

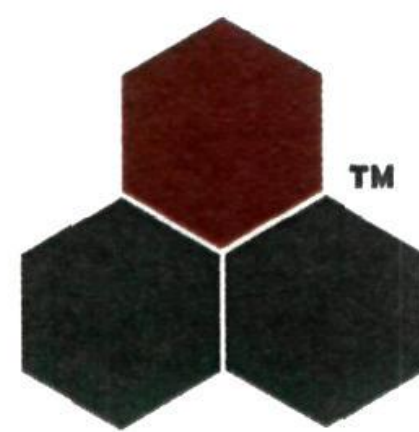


"When will you be an IPexpert?"



IPexpert's CCIE™ Security Proctor Guide (Version 4.0)

A companion to IPexpert's CCIE™ Security Preparation Workbook



ipexpert

powered by **PROCTOR**
LABS



NOT FOR RESALE - THIS IS AN INDIVIDUALLY LICENSED PRODUCT
For use with Proctor Labs, Inc. equipment.
Copyright 2001 - 2007 IPexpert, Inc.
All Rights Reserved. Additional copyrights and trademarks may apply.

For technical support peer groups, subscribe for free to:

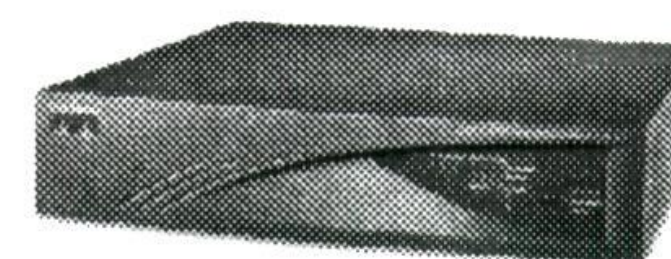
CertificationTalk 

www.certificationtalk.com

ONLINE 
study list
www.onlinestudylist.com

IPexpert's CCIE Security Proctor Guide (Version 4.0)

(To be used in conjunction with IPexpert's Ultimate Preparation Workbook for the Cisco® CCIE™ Security Laboratory Exam, Version 4.0)



Before We Begin

This guide was created to provide you with not only a hand-holding walk-through, but also to provide you with a “Proctor Like” experience. Used in conjunction with our CCIE Security Lab Preparation Workbook (Version 4.0), you're guaranteed a real self-paced learning experience like no other!

Technical Support

CertificationTalk  (<http://www.CertificationTalk.com>)

ONLINE
study list  (<http://www.OnlineStudyList.com>)

IPexpert is proud to lead the industry with multiple support options at your disposal free of charge. Our online forums (www.CertificationTalk.com) have attracted a membership of nearly 20,000 of your peers from around the world! At www.OnlineStudyList.com, you may subscribe to multiple “SPAM-free” email lists. Also, if you are an IPexpert Elite Member and need support for your IPexpert products, simply open a support ticket at www.IPexpert.com and it will be addressed promptly.

Copyright

IPEXPERT'S CCIE™ SECURITY PROCTOR GUIDE (VERSION 4.0). Copyright © 2007 by IPexpert, Inc. All rights reserved. Printed in the United States of America. No part of this book may be used or reproduced in any manner whatsoever without written permission. Protected by End-User License Agreement on Pages 5 and 6.

ISBN 978-1-934344-07-1

About IPexpert's Authors

IPexpert employs only the best and brightest CCIE developers and instructors in the industry. Our celebrated team of diverse experts holds multiple CCIE certifications gained from substantial and highly relevant real-world experience. These key attributes give IPexpert the leading edge for delivering the most effective training possible.

Wayne A. Lawson II

CCIE #5244 (R&S), CCNA, CCDA, Nortel NCSE, MCP, MCSE (NT 4.0), MCSE +I, CNA, CNE (4.0), CNX Ethernet, Cisco Wireless LAN Design Specialist, Cisco IP Telephony Design Specialist
Founder & President – IPexpert, Inc.

With 15 years of networking, sales and marketing experience, Mr. Lawson possesses the technical competency, leadership and visionary talent possessed only by the most successful entrepreneurs around the globe. Wayne has served as a highly effective contributing member of five major organizations, including the United States Marine Corps (USMC), International Network Services (INS), Cisco Systems, Vertical Networks and IPexpert, Inc. He has been published on the topics of "Building Cisco Remote Access Networks" (ISBN: 1-928993-13-X) and "Configuring Cisco AVVID" (ISBN: 1-928994-14-8), and has written for various technical and entrepreneurial magazines. Mr. Lawson founded IPexpert in 2001 and continues to revolutionize the way engineers prepare for the coveted CCIE Lab certification. Wayne's unique visionary approach to cutting-edge technologies and enterprise network solutions, coupled with a fanatical dedication to customer satisfaction, propel the engine of success at IPexpert. With a talent for revolutionizing products, services and solutions, and a drive to achieve perfection, his leadership and business ethics have molded IPexpert into the clear leader in CCIE Lab training. In addition to acting as the President and Senior Director of IPexpert, Inc., Wayne is also preparing for his CCIE Voice Lab exam.

Scott Morris

Quad CCIE #4713 (R&S, ISP-Dial, Security and Service Provider), CCDP, CCSP, Cisco Cable Communications Specialist, Cisco IP Telephony Support Specialist, Cisco IP Telephony Design Specialist, CCNA (WAN Switching), MCSE (NT 4.0), Juniper Networks JNCIE (#153) and JCNIS, RiverStone Networks RCNP, NSA/CNSS INFOSEC Professional, TIA Convergence Technology Professional (CTP), and CISSP #37445.

Senior Technical Instructor and Developer – IPexpert, Inc.

Boasting more than 18 years of technical training and consulting experience and a wealth of technical certifications, Scott Morris has proven himself among the elite in the technical training industry. Scott is one of the few people in the world currently holding four separate CCIE certifications, and he is actively preparing for his fifth – the CCIE Voice. Scott has an outstanding track record of success in editing, writing and reviewing training books for Cisco Press, Wylie, Sybex, Que Publishing and McGraw-Hill, and teaching CCIE lab preparation materials. He has served as a contributing author for works including Cisco Press' Managing Cisco Network Security book (ISBN: 1578701031) - Chapters on the PIX Firewall; and Cisco Press' CCIE Practical Studies, Vol. 2 (ISBN: 1587050722) - Chapter on Multicast. Scott has also written various articles for Packet Magazine and TCP Mag.

Marvin Greenlee

CCIE #12237 (Security, Service Provider, Routing and Switching), Cisco IP Communications Express Specialist, Cisco IP Telephony Express Specialist, Cisco VPN/Security Sales Specialist, CCDP, CCNP, MCSE (NT4.0,2000), Juniper Networks JNCIA-M.

Sr. Technical Instructor and Developer – IPexpert, Inc.

Joining IPexpert in 2007, Marvin Greenlee brings years of valuable experience in technical consulting and training. In addition to his on-the-job experience employed at Cisco, he has written, edited, and reviewed several books and training materials focused on CCIE certification topics. Mr. Greenlee has earned a favorable reputation in the CCIE Lab training community as an active participant on various message boards and email lists. Marvin is responsible for instructor-led training, self-study product development and support, with a focus on the CCIE Security track.

Mark Snow

CCIE #14073 (Voice, Security), CCVP, CCNP, CCDP, CSE, CQS-CIPCCES, CQS-CIPTDS, CQS-CIPTOS, CQS-CIPTSS, MCSE.

Sr. Voice Technical Instructor and Developer – IPexpert, Inc.

From an early age when his father, a patented inventor with Bell Labs®, first started him on Unix System V, Mark Snow's passion for technology has not yet stopped growing. With over 12 years working professionally in the IT industry and over 7 years spent consulting internationally with a focus on Cisco IP Telephony and Security, Mark brings a wealth of knowledge to the training arena. Mark plans to begin working on his next CCIE in Storage. With IPexpert for 2 years, Mark is responsible for instructor-led training, self-study product development and support, with a focus on the CCIE Voice and Security tracks.

Vik Malhi

CCIE #13890 Voice, CCVP, Cisco IP Telephony Support Specialist, Cisco IP Telephony Operations Specialist, Cisco IP Telephony Design Specialist and Cisco Wireless LAN Design Specialist.

Sr. Voice Technical Instructor and Developer – IPexpert, Inc.

With nearly 10 years of IP Telephony training and consulting experience and a wealth of technical certifications, Vik Malhi has proven that he's one of the top Cisco voice instructors and consultants in the world! Vik was the first engineer to install CM 3.0 in Europe, Has over 6 years of AVVID consulting and implementation experience and has taught CCIE Voice Lab classes for the past several months. Vik has joined IPexpert's accredited team of experts and will be in charge of updating, supporting and teaching IPexpert's CCIE Voice-related products, services and classes.

Feedback

Do you have a suggestion or other feedback regarding this book or other IPexpert products? At IPexpert, we look to you – our valued clients – for the real world, frontline evaluation that we believe is necessary to improve continually. Please send an email with your thoughts to feedback@ipexpert.com or call 1.866.225.8064 (international callers dial +1.810.326.1444).

In addition, when you pass the CCIE™ Lab exam, we want to hear about it! Email your CCIE™ number to success@ipexpert.com and let us know how IPexpert helped you succeed. We would like to send you a gift of thanks and congratulations.

Additional CCIE™ Preparation Material

IPexpert, Inc. is committed to developing the most effective Cisco CCIE™ R&S, Security, Service Provider, and Voice Lab certification preparation tools available. Our team of certified networking professionals develops the most up-to-date and comprehensive materials for networking certification, including self-paced workbooks, online Cisco hardware rental, classroom training, online (distance learning) instructor-led training, audio products, and video training materials. Unlike other certification-training providers, we employ the most experienced and accomplished team of experts to create, maintain, and constantly update our products. At IPexpert, we are focused on making your CCIE™ Lab preparation more effective.

IPexpert features a variety of CCIE™ training materials to suit your needs and learning preferences. Please review the catalog that has been incorporated into this book for additional products that are available to you!

Command Syntax

Command syntax in this book confirms to the following conventions:

Technical Notes:

NOTE:

Please reference your R&S Workbook for all diagrams and tables.

R&S Workbook Tasks:

Task 1.1

Technical tasks taken from the R&S Workbook will be displayed in this same font (Arial). The text will hug the left column and be normal (not bold, italicized or underlined). The task will follow a **Bold** heading which will display the Lab number–dot-Task number (i.e. Lab 3 Task 7 = **Task 3.7**)

Notes from the Instructor / Proctor:

- Notes from the Instructor / Proctor will be displayed in the following font (Arial) and be bold. There will also be an arrow pointing to the text as displayed within this statement.

Commands:

R4(config)#**command that you need to type will be displayed as follows**

or

R2:

```
int fa1/0
no switchport
ip address 150.50.17.2 255.255.255.0
```

Router Output / Output Notes:

Important command output will be displayed as such ← Notes regarding the command or router output will be displayed as such

Standard Router or Switch Prompt:

```
Cat3550-1(config)#
```


IPEXPERT END-USER LICENSE AGREEMENT

END USER LICENSE FOR ONE (1) PERSON ONLY

IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, DO NOT OPEN OR USE THE TRAINING MATERIALS.

This is a legally binding agreement between you and IPEXPERT, the "Licensor," from whom you have licensed the IPEXPERT training materials (the "Training Materials"). By using the Training Materials, you agree to be bound by the terms of this License, except to the extent these terms have been modified by a written agreement (the "Governing Agreement") signed by you (or the party that has licensed the Training Materials for your use) and an executive officer of Licensor. If you do not agree to the License terms, the Licensor is unwilling to license the Training Materials to you. In this event, you may not use the Training Materials, and you should promptly contact the Licensor for return instructions.

The Training Materials shall be used by only **ONE (1) INDIVIDUAL** who shall be the sole individual authorized to use the Training Materials throughout the term of this License.

Copyright and Proprietary Rights

The Training Materials are the property of IPEXPERT, Inc. ("IPEXPERT") and are protected by United States and International copyright laws. All copyright, trademark, and other proprietary rights in the Training Materials and in the Training Materials, text, graphics, design elements, audio, and all other materials originated by IPEXPERT at its site, in its workbooks, scenarios and courses (the "IPEXPERT Information") are reserved to IPEXPERT.

The Training Materials cannot be used by or transferred to any other person. You may not rent, lease, loan, barter, sell or time-share the Training Materials or accompanying documentation. You may not reverse engineer, decompile, or disassemble the Training Materials. You may not modify, or create derivative works based upon the Training Materials in whole or in part. You may not reproduce, store, upload, post, transmit, download or distribute in any form or by any means, electronic, mechanical, recording or otherwise any part of the Training Materials and IPEXPERT Information other than printing out or downloading portions of the text and images for your own personal, non-commercial use without the prior written permission of IPEXPERT.

You shall observe copyright and other restrictions imposed by IPEXPERT. You may not use the Training Materials or IPEXPERT Information in any manner that infringes the rights of any person or entity.

Exclusions of Warranties

THE TRAINING MATERIALS AND DOCUMENTATION ARE PROVIDED "AS IS." LICENSOR HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE LIMITATION OF INCIDENTAL DAMAGES OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. This agreement gives you specific legal rights, and you may have other rights that vary from state to state.

Choice of Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of the State of Michigan, without reference to any conflict of law principles. You agree that any litigation or other proceeding between you and Licensor in connection with the Training Materials shall be brought in the Michigan state or courts located in Port Huron, Michigan, and you consent to the jurisdiction of such courts to decide the matter. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods shall not apply to this License. If any provision of this Agreement is held invalid, the remainder of this License shall continue in full force and effect.

Limitation of Claims and Liability

ANY ACTION ON ANY CLAIM AGAINST IPEXPERT MUST BE BROUGHT BY THE USER WITHIN ONE (1) YEAR FOLLOWING THE DATE THE CLAIM FIRST ACCRUED, OR SHALL BE DEEMED WAIVED. IN NO EVENT WILL THE LICENSOR'S LIABILITY UNDER, ARISING OUT OF, OR RELATING TO THIS AGREEMENT EXCEED THE AMOUNT PAID TO LICENSOR FOR THE TRAINING MATERIALS. LICENSOR SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, REGARDLESS OF WHETHER LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITHOUT LIMITING THE FOREGOING, LICENSOR WILL NOT BE LIABLE FOR LOST PROFITS, LOSS OF DATA, OR COSTS OF COVER.

Entire Agreement

This is the entire agreement between the parties and may not be modified except in writing signed by both parties.

U.S. Government - Restricted Rights

The Training Materials and accompanying documentation are "commercial computer Training Materials" and "commercial computer Training Materials documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction release, performance, display, or disclosure of the Training Materials and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

IF YOU DO NOT AGREE WITH THE ABOVE TERMS AND CONDITIONS, DO NOT OPEN OR USE THE TRAINING MATERIALS AND CONTACT LICENSOR FOR INSTRUCTIONS ON RETURN OF THE TRAINING MATERIALS.

IPexpert's CCIE Security Proctor Guide (Version 4.0)

Table of Contents

Section 1: Access Control Lists (ACLs) and Filters for IP	Page 9
Section 2: Network Attacks and Advanced Filtering	Page 25
Section 3: GRE and NAT	Page 35
Section 4: Authentication, Authorization and Accounting (AAA) on a Router	Page 55
Section 5: PIX Firewall	Page 75
Section 6: PIX Firewall / ASA	Page 117
Section 7: IPsec	Page 131
Section 7B: DMVPN	Page 147
Section 8: VPN Concentrator	Page 155
Section 9: Switching	Page 179
Section 10: IDS	Page 203
Section 10B: IPS	Page 217
Section 10C: IDS	Page 229
Section 11: Router Management IOS Services	Page 243
Section 12: Multiprotocol Challenge A (One Day Lab Experience)	Page 257
Section 13: Multiprotocol Challenge B (One Day Lab Experience)	Page 285
Section 14: Multiprotocol Challenge C (One Day Lab Experience)	Page 315
Section 15: Multiprotocol Challenge D (One Day Lab Experience)	Page 339
Section 16: Multiprotocol Challenge E (One Day Lab Experience)	Page 365
Section 17: Multiprotocol Challenge F (One Day Lab Experience)	Page 391
Section 18: Multiprotocol Challenge G (One Day Lab Experience)	Page 439

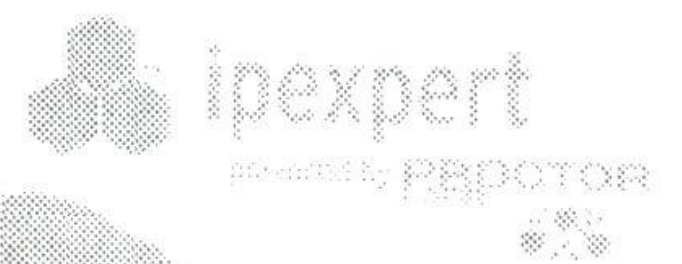
This page left intentionally blank.

Section 1: Access Control Lists (ACLs) and Filters for IP

Estimated Time to Complete: 4 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 1 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 1-A.
- The Routers are running the following protocols:
 - RIP – R2, R4 and R5 (Frame Network)
 - OSPF – R5 and R7 (Ethernet Network)
 - EIGRP – R7 and R8 (Serial Connection)
- Redistribution of the Routing protocols will be done on the appropriate Routers (R5 and R7).
- This lab will focus strictly on ACLs. You will need to pre-configure the network with the base Frame Relay, IP Addressing, OSPF, RIP and EIGRP. The pre-configuration will include the Redistribution of the Routing Protocols. Prior to starting this lab, be sure you pre-load the "Initial Configuration" for each router used in this lab scenario. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 1 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.
- Configure the Clock and Time zone on all the routers based on Local Time. This is required for the Time Based Access Lists to work properly.

R2 Filtering Section

Task 1-1

Allow traffic destined to a Web Server located at 150.50.2.80 from anywhere coming in through the Frame Relay interface. Traffic Filtering should be done on the Frame Relay interface in the inbound direction for all incoming traffic.

- It is necessary to first define an access list "infilter" that will eventually be applied to the serial interface. Then you want to permit the traffic going to www with IP as shown above.

```
r2(config)#ip access-list extended infilter
r2(config-ext-nacl)#permit tcp any host 150.50.2.80 eq www
```

Task 1-2

Users from the 150.50.2.0 network should be able to go to the outside networks and return. This should be allowed for TCP based traffic.

- Add additional line for this IP address and use the "established" keyword.

```
r2(config-ext-nacl)#permit tcp any 150.50.2.0 0.0.0.255 established
```


Task 1-3

DNS queries will be sent to a DNS Server located at 150.50.57.53. Allow the DNS query replies to come back thru the Frame Relay network. The ACL entry should be as specific as possible.

- In here, you need to make sure that the DNS server can be connected.

```
r2(config-ext-nacl)#permit udp host 150.50.57.53 eq domain 150.50.2.0
0.0.0.255
```

Task 1-4

The users on the 150.50.2.0 networks should access the Web. The access list should be created on the Frame Relay interface in the outbound direction. They are only allowed to browse during the following times:

- 12:00 to 1:00 PM on Weekdays
 - 5:00 PM to Midnight on Weekdays
 - All day on Saturday and Sunday.
- The following commands can be used to apply the time ranged access list.

```
r2(config)#time-range web-access
r2(config-time-range)#periodic weekdays 12:00 to 13:00
r2(config-time-range)#periodic weekdays 17:00 to 23:59
r2(config-time-range)#periodic weekend 0:00 to 23:59
```

- Different time would mean that the time range access list would be active or not. After entering the command for Task 1-4, you can have the display as shown below. First, the time is outside of the time range and that's why the access list is inactive.

```
r2#sh clock
02:00:13.671 UTC Fri Dec 23 2005
r2#sh ip access
Extended IP access list infilter
 10 permit tcp any host 150.50.2.80 eq www
 20 permit tcp any 150.50.2.0 0.0.0.255 established
 30 permit udp host 150.50.57.53 eq domain 150.50.2.0 0.0.0.255
 40 permit udp host 150.50.25.5 host 224.0.0.9 eq rip
 50 deny ip any any log
Extended IP access list outfilter
 10 permit tcp 150.50.2.0 0.0.0.255 any eq www time-range web-access
(inactive)
 20 deny tcp 150.50.2.0 0.0.0.255 any eq www
 30 permit ip any any
```

- With the time within the range, the time access list is active.

```
r2#sh clock
*14:09:43.383 UTC Sat Dec 24 2005
```



```
r2#sh ip access-lists
```

```
Extended IP access list infilter
```

```
10 permit tcp any host 150.50.2.80 eq www
```

```
20 permit tcp any 150.50.2.0 0.0.0.255 established
```

```
30 permit udp host 150.50.57.53 eq domain 150.50.2.0 0.0.0.255
```

```
40 permit udp host 150.50.25.5 host 224.0.0.9 eq rip
```

```
50 deny ip any any log
```

```
Extended IP access list outfilter
```

```
10 permit tcp 150.50.2.0 0.0.0.255 any eq www time-range web-access  
(active)
```

```
20 deny tcp 150.50.2.0 0.0.0.255 any eq www
```

```
30 permit ip any any
```

Task 1-5

All the ACLs in this section should be named. You cannot use Reflexive or CBAC to accomplish the tasks in this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. . Be sure to log any traffic that violates these rules.

- You have already defined the name access list in Task 1-1. And now you want to allow RIP to go through and deny anything else. It is always a good idea to explicitly deny ip any any with a log statement so that you know exactly what is allowed and what is not.

```
r2(config-ext-nacl)#permit udp host 150.50.25.5 host 224.0.0.9 eq rip  
r2(config-ext-nacl)#deny ip any any log
```

R4 Filtering Section

Task 1-6

Allow users on 150.50.4.0 network to browse the WAN. The users should be able to go out from the following traffic:

- Telnet
- SMTP
- DNS
- HTTP
- HTTPS

- Same as the previous task, you should define an outfilter that eventually will be applied to the serial interface with the following commands:

```
r4(config)#ip access-list extended outfilter  
r4(config-ext-nacl)#permit tcp 150.50.4.0 0.0.0.255 any eq telnet  
reflect racl timeout 180  
r4(config-ext-nacl)#permit tcp 150.50.4.0 0.0.0.255 any eq smtp  
reflect racl timeout 180  
r4(config-ext-nacl)#permit tcp 150.50.4.0 0.0.0.255 any eq www  
reflect racl timeout 180  
r4(config-ext-nacl)#permit tcp 150.50.4.0 0.0.0.255 any eq 443  
reflect racl timeout 180  
r4(config-ext-nacl)#permit udp 150.50.4.0 0.0.0.255 any eq domain  
reflect racl timeout 60  
r4(config-ext-nacl)#deny ip any any log
```


Task 1-7

The return entries should be automatically created on the return.

- The “reflect racl” option listed in the commands above would automatically accomplish the requirement stated here. This racl access list will be used in the infiltrer access list later.

Task 1-8

The return entries should expire after 3 minutes for TCP based protocols. DNS entries should expire after 1 minute. Use minimum configuration lines to accomplish this.

- The keyword “timeout 180” in the statement above would automatically accomplish the requirement.

Task 1-9

There is a Web Server located at 150.50.4.80. Access should be allowed to this server for regular and secure web traffic.

- Once again, we want to define an access list infiltrer that can accomplish these requirement. Reading ahead to the next section however, we realize that we need to explicitly deny traffic to the web server during maintenance hours and permit it at all other times.

```
r4(config)#ip access-list extended infiltrer
r4(config-ext-nacl)#deny tcp any host 150.50.4.80 eq www time-range
web-maintenance
r4(config-ext-nacl)#deny tcp any host 150.50.4.80 eq 443 time-range
web-maintenance
r4(config-ext-nacl)#permit tcp any host 150.50.4.80 eq www
r4(config-ext-nacl)#permit tcp any host 150.50.4.80 eq 443
r4(config-ext-nacl)#permit udp host 150.50.45.5 host 224.0.0.9 eq rip
r4(config-ext-nacl)#evaluate racl
r4(config-ext-nacl)#deny ip any any log
```

Task 1-10

The above mentioned Web Server will be taken down for Maintenance and Backups between 1:00 AM and 3:00 AM every Wednesday. The Maintenance schedule should come into effect from the 1st of next month for a duration of 6 months.

- The time-range keyword in the above statement would accomplish this requirement. In addition, we need to add the time limit too.

```
r4(config)#time-range web-maintenance
r4(config-time-range)#absolute start 00:00 01 April 2005 end 23:59 30
September 2005
r4(config-time-range)#periodic Wednesday 1:00 to 3:00
```


- Same as the last section, when the time range is within the range, the access list would be active.

```
R4#sh clock
02:00:11.587 PST Wed Aug 24 2005
R4#sh ip access
Extended IP access list infilter
 10 deny tcp any host 150.50.4.80 eq www time-range web-maintenance
(active)
 20 deny tcp any host 150.50.4.80 eq 443 time-range web-maintenance
(active)
 30 permit tcp any host 150.50.4.80 eq www
 40 permit tcp any host 150.50.4.80 eq 443
 50 permit udp host 150.50.45.5 host 224.0.0.9 eq rip
 60 evaluate racl
 70 deny ip any any log
Reflexive IP access list racl
```

- When the time range is outside the range, the access-list is inactive.

```
R4#sh clock
02:00:06.603 PST Thu Aug 25 2005
R4#sh ip access
Extended IP access list infilter
 10 deny tcp any host 150.50.4.80 eq www time-range web-maintenance
(inactive)
 20 deny tcp any host 150.50.4.80 eq 443 time-range web-maintenance
(inactive)
 30 permit tcp any host 150.50.4.80 eq www
 40 permit tcp any host 150.50.4.80 eq 443
 50 permit udp host 150.50.45.5 host 224.0.0.9 eq rip
 60 evaluate racl
 70 deny ip any any log
Reflexive IP access list racl
```

Task 1-11

CBAC is not allowed to accomplish the objectives of this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. Be sure to log any traffic that violates these rules

- Since CBAC is not used, we have to use the reflective Access list. In order to test the result, we can add R1's Fast Ethernet to the VLAN 4. Then we can telnet it from that interface and you can see an additional line of reflexive access list below.

```
R4#sh ip access
Extended IP access list infilter
 10 deny tcp any host 150.50.4.80 eq www time-range web-maintenance
(inactive)
 20 deny tcp any host 150.50.4.80 eq 443 time-range web-maintenance
(inactive)
 30 permit tcp any host 150.50.4.80 eq www
 40 permit tcp any host 150.50.4.80 eq 443
 50 permit udp host 150.50.45.5 host 224.0.0.9 eq rip
 60 evaluate racl
 70 deny ip any any log
Extended IP access list outfilter
 10 permit icmp any any (5 matches)
 20 permit tcp any any reflect racl (30 matches)
```



```

30 permit tcp 150.50.4.0 0.0.0.255 any eq telnet reflect racl
40 permit tcp 150.50.4.0 0.0.0.255 any eq smtp reflect racl
50 permit tcp 150.50.4.0 0.0.0.255 any eq www reflect racl
60 permit tcp 150.50.4.0 0.0.0.255 any eq 443 reflect racl
70 permit udp 150.50.4.0 0.0.0.255 any eq domain reflect racl
80 deny ip any any log
Reflexive IP access list racl
  permit tcp host 150.50.45.5 eq telnet host 150.50.4.1 eq 21201 (54
matches) (time left 287)

```

R5 Filtering Section

Task 1-12

Allow all TCP and UDP based traffic to go out and return from the Frame Relay network on R5.

→ We will use the CBAC access list and it will be defined as below.

Task 1-13

For web traffic, only allow Java applets to be downloaded from Web servers 150.50.4.80 and 150.50.2.80.

→ We will define an access list with these two IP address and apply this to the java list.

```

r5(config)#access-list 1 permit 150.50.4.80
r5(config)#access-list 1 permit 150.50.2.80
r5(config)#ip inspect name FW http java-list 1

```

Task 1-14

Create inbound filter on the Frame Relay interface. Log all the Denies.

→ The access list infilter is created that will be applied to the FR interface. The command is as shown below. This command will add more entry in the upcoming tasks.

```

r5(config)#ip access-list extended infilter
r5(config-ext-nacl)#remark Deny Spoofed Packets

```

Task 1-15

The router should act as a Firewall and protect the internal network against Syn-floods. It should start deleting half open connections if they are at 800. It should stop deleting half open connections when they reach 600.

→ This is for fine tuning the CBAC access list parameters.

```

r5(config)#ip inspect max-incomplete high 800
r5(config)#ip inspect max-incomplete low 600

```


Task 1-16

It should further protect the internal network by starting to delete half-open connections at 600 if there have been 600 new connections created within the last one minute and stop deleting at 400.

- **Continue to fine tune the CBAC parameters.**

```
r5(config)#ip inspect one-minute high 600
r5(config)#ip inspect one-minute low 400
```

Task 1-17

Configure the Router to delete TCP connections if the connection has been idle for 10 minutes.

- **This command is for preventing a lot of half open TCP sessions. We change the time to 10 minutes, which is 600 seconds.**

```
r5(config)#ip inspect tcp idle-time 600
```

Task 1-18

Do not allow traffic with source IP address from the RFC 1918 address space to come in thru the Frame Relay interface.

- **The RFC 1918 address are listed below.**

```
r5(config)#ip access-list extended infiltrer
r5(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 any log
r5(config-ext-nacl)#deny ip 172.16.0.0 0.15.255.255 any log
r5(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255 any log
```

Task 1-19

Also block any address that should never be in the source address field.

- **The “Strange” addresses, such as multicast, loopback, broadcast addresses are listed below.**

```
r5(config)#ip access-list extended infiltrer
r5(config-ext-nacl)#deny ip 127.0.0.0 0.255.255.255 any log
r5(config-ext-nacl)#deny ip 169.254.0.0 0.0.255.255 any log
r5(config-ext-nacl)#deny ip 224.0.0.0 15.255.255.255 any log
r5(config-ext-nacl)#deny ip host 0.0.0.0 any log
r5(config-ext-nacl)#deny ip host 255.255.255.255 any log
r5(config-ext-nacl)#permit udp host 150.50.25.2 host 224.0.0.9 eq rip
r5(config-ext-nacl)#permit udp host 150.50.45.4 host 224.0.0.9 eq rip
```


Task 1-20

Turn on an audit trail messages which will be displayed on the console after each CBAC session closes.

- You turn on audit trail with the following command.

```
r5(config)#ip inspect audit trail
```

Task 1-21

Globally specify the TCP session will still be managed after the firewall detects a FIN-exchange to be 10 seconds for all TCP sessions.

- This is for specifying the time limit for the FIN exchange.

```
r5(config)#ip inspect tcp finwait-time 10
```

Task 1-22

Changes the max-incomplete host number to 35 half-open sessions, and changes the block-time timeout to 3 minutes.

- Similar to the command previously defined, this one prevents a lot of half-open sessions because this could be a DoD attack.

```
r5(config)#ip inspect tcp max-incomplete host 35 block-time 3
```

Task 1-23

Set the global UDP idle timeout to 100 seconds.

- The UDP idle timeout is not as frequent of an attack, but this is also a good habit to turn on.

```
r5(config)#ip inspect udp idle-time 100
```

- In order to test this section, we can temporarily remove the access list in R2. And then, we can telnet from R7 to R2 through R5's FR interface. The result is shown below:

```
R5#show ip inspect config
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:600] connections
max-incomplete sessions thresholds are [600:800]
max-incomplete tcp connections per host is 35. Block-time 3 minutes.
tcp synwait-time is 30 sec -- tcp finwait-time is 10 sec
tcp idle-time is 600 sec -- udp idle-time is 100 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name FW
    tcp alert is on audit-trail is off timeout 600
    udp alert is on audit-trail is off timeout 100
    http java-list 1 alert is on audit-trail is off timeout 600
```



```

R5#show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [6:65]
Interfaces configured for inspection 2
Session creations since subsystem startup or last reset 6
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:1]
Last session created 00:01:12
Last statistic reset never
Last session creation rate 0
Last half-open session total 0

R5#show ip inspect sessions detail
Established Sessions
  Session 467F02AC (150.50.57.7:31659)=>(150.50.25.2:23) tcp SIS_OPEN
    Created 00:01:18, Last heard 00:00:17
    Bytes sent (initiator:responder) [30:155]
    In  SID 150.50.25.2[23:23]=>150.50.57.7[31659:31659] on ACL infilter  (10
matches)
R5#

```

Task 1-24

Prevent IP Spoofing using Reverse Path Forwarding.

- Even though this is only one command, this seems to be a popular topic discussed on Cisco's NetPro Security Forums.

```
r5(config-if)#ip verify unicast reverse-path
```

R7 Filtering Section

Task 1-25

Allow users on 150.50.57.0 to go out to R8 using the following protocols:

- Telnet
- SMTP
- DNS
- HTTP
- HTTPS
- We will define a filter "outfilter" and apply it to the serial interface with the following commands:

```

R7(config)#ip access-list extended outfilter
R7(config-ext-nacl)#permit tcp 150.50.57.0 0.0.0.255 any eq telnet
reflect racl timeout 180
R7(config-ext-nacl)#permit tcp 150.50.57.0 0.0.0.255 any eq smtp
reflect racl timeout 180
R7(config-ext-nacl)#permit tcp 150.50.57.0 0.0.0.255 any eq www
reflect racl timeout 180

```



```
R7(config-ext-nacl)#permit tcp 150.50.57.0 0.0.0.255 any eq 443
reflect racl timeout 180
R7(config-ext-nacl)#permit udp 150.50.57.0 0.0.0.255 any eq domain
reflect racl timeout 60
R7(config-ext-nacl)#deny ip any any log
```

Task 1-26

The return entries should be automatically created on the return.

- The “reflect racl” and “evaluate racl-in” keywords in the above command automatically accomplish these tasks. In addition, we will use the established keyword

```
R7(config)#ip access-list extended infilter
R7(config-ext-nacl)#evaluate racl
R7(config-ext-nacl)#deny ip any any log
```

Task 1-27

The return entries should expire after 3 minutes for TCP based protocols. DNS entries should expire after 1 minute. Use minimum configuration lines to accomplish this.

- The “timeout 180” would make the return entries after 180 seconds. And the “timeout 60” is for the DNS entries.

Task 1-28

Do not allow traffic with source IP address from the RFC 1918 address space to come in thru the Serial interface.

- We will create an access list to block the RFC 1918. Blocking of the RFC1918 addressing space means that we will block all the private IP addresses.

```
r7(config)#ip access-list extended infilter
r7(config-ext-nacl)#deny ip 10.0.0.0 0.255.255.255 any log
r7(config-ext-nacl)#deny ip 172.16.0.0 0.15.255.255 any log
r7(config-ext-nacl)#deny ip 192.168.0.0 0.0.255.255 any log
```

Task 1-29

Also block any address that should never be in the source address field.

- We will continue to use the access list above to block the other strange source addresses such as loopback or multicast addresses.

```
r7(config)#ip access-list extended infilter
r7(config-ext-nacl)#deny ip 127.0.0.0 0.255.255.255 any log
r7(config-ext-nacl)#deny ip 169.254.0.0 0.0.255.255 any log
r7(config-ext-nacl)#deny ip 224.0.0.0 15.255.255.255 any log
r7(config-ext-nacl)#deny ip host 0.0.0.0 any log
r7(config-ext-nacl)#deny ip host 255.255.255.255 any log
```


Task 1-30

Prevent IP Spoofing using Reverse Path Forwarding.

- Same as Task 1-24, this command would prevent IP Spoofing using reverse path forwarding.

```
r5(config-if)#ip verify unicast reverse-path
```

Task 1-31

Allow R8 users to access the 150.50.57.0 and the Frame Relay networks thru R7 based on successful authentication. They should only be allowed to come in for TCP based protocols.

- We will assign three VTY line to let them telnet and then for the authentication. We will also use the local user database that we will define later. Don't forget to allow the R8 users to have access to telnet to R7 to perform authentication. This requires an explicit line on the infilter ACL. Since this traffic is destined to the router, the return traffic would not be affected by the outfilter.

```
r7(config)#line vty 0 2
r7(config-line)#login local
r7(config-line)#autocommand access-enable host timeout 2

r7(config)#ip access-list extended infilter
r7(config-ext-nacl)#permit tcp any host 150.50.78.7 eq telnet
```

Task 1-32

Create an access list entry that is only effective after successful authentication by the host.

- The dynamic access-list entry that is created when the user authenticated satisfies this requirement. Notice the keyword "HOST" in the question. This should tell you to use the host option of the access-enable autocommand such that the dynamically generated acl entry specifies a specific host address.

Task 1-33

Create the username as **ipexpert** with a password of **cisco** on the router.

- You create the user password with the following command.

```
r7(config)#username ipexpert password 0 cisco
```

Task 1-34

The user should use Telnet for the authentication.

- The user needs to telnet to our vty line, therefore, this requirement is also satisfied.
- This is how we can test it:

→ We need to first telnet from R8 to R7 in order to telnet to R5.

→ At first, we cannot telnet to R5.

```
r8#150.50.57.5
Trying 150.50.57.5 ...
% Destination unreachable; gateway or host down
```

→ Telnet to R7 and authenticate myself first.

```
r8#150.50.78.7
Trying 150.50.78.7 ... Open

User Access Verification

Username: ipexpert
Password:
[Connection to 150.50.78.7 closed by foreign host]
```

→ Now I can telnet to R5.

```
r8#150.50.57.5
Trying 150.50.57.5 ... Open
```

User Access Verification

```
Password:
R5#
```

→ Notice the new entry below line 120 of the ACL. This shows that the host 150.50.78.8 now has access to any destination using tcp.

```
R7#sh ip access
Standard IP access list 1
 10 permit 150.50.78.8
Extended IP access list infiltrer
 10 permit eigrp host 150.50.78.8 host 224.0.0.10
 20 deny ip 10.0.0.0 0.255.255.255 any log
 30 deny ip 172.16.0.0 0.15.255.255 any log
 40 deny ip 192.168.0.0 0.0.255.255 any log
 50 deny ip 127.0.0.0 0.255.255.255 any log
 60 deny ip 169.254.0.0 0.0.255.255 any log
 70 deny ip 224.0.0.0 15.255.255.255 any log
 80 deny ip host 0.0.0.0 any log
 90 deny ip host 255.255.255.255 any log
100 permit tcp any host 150.50.78.7 eq telnet
110 permit tcp any host 150.50.78.7 eq 3050
120 Dynamic dyn permit tcp any any
    permit tcp host 150.50.78.8 any (28 matches) (time left 95)
130 evaluate racl
140 deny ip any any log
```


Task 1-35

The dynamic entry created should remain in effect for a maximum of 1 hour and should get deleted after 2 minutes of no activity.

- The “timeout 2” command would make sure that the dynamic entry will be deleted after 2 minutes of no activity.

Task 1-36

Make sure you leave at least 2 lines open for Telnet Management access to the router. The administrators should use 3050 as the telnet port for management.

- We only use VTY 0 2 above so we still have VTY 3 4 open.

```
r7(config-line)#line vty 3 4
r7(config-line)#rotary 50
```

Task 1-37

Allow 150.50.78.8 to telnet into R7 for Management access. Allow the appropriate entries in the access list.

- In order to restrict access to management access, we need to define an access list and apply it to the VTY. For the telnet access management, we have to specify “line vty 0 2” and “line vty 3 4” because of the requirement. We also need to create an entry in the infiltrer ACL to allow R8 to have inbound telnet access to R7 on port 3050. Make sure this is before the *evaluate* command.

```
r7(config)#access-list 1 permit 150.50.78.8
r7(config-line)#line vty 3 4
r7(config-line)#access-class 1 in
r7(config)#ip access-list extended infiltrer
r7(config-ext-nacl)#permit tcp any host 150.50.78.7 eq 3050
```

Task 1-38

CBAC is not allowed to accomplish the objectives of this section. Allow relevant traffic coming in. Make sure Routing is still working after you are done with this section. Be sure to log any traffic that violates these rules.

- The following command for the infiltrer access list would permit EIGRP traffic.

```
r7(config-ext-nacl)#permit eigrp host 150.50.78.8 host 224.0.0.10
```


R8 Filtering

Task 1-39

Create a lock-and-key access-list for R8's Fast Ethernet 0/0 and require users to authentication prior to accessing a web server located at 150.50.57.5

- The lock-and-key access list can be accomplished below. It satisfies the requirement by the next few tasks.

```
r8(config)# access-list 123 dynamic mydynlist timeout 100 permit tcp  
any host 150.50.57.5 eq www  
r8(config)# access-list 123 deny tcp any host 150.50.57.5 eq www  
r8(config)# access-list 123 permit ip any any
```

```
r8(config)# interface f0/0  
r8(config-if)# ip access-group 123 in
```

```
r8(config-line)# line vty 0 4  
r8(config-line)# login local  
r8(config-line)# autocmd access-enable host timeout 10
```

Task 1-40

The session will be open at most for 100 mins.

- The timeout 100 would accomplish this requirement.

Task 1-41

The session will timeout after 10 mins of idleness.

- The timeout 10 would accomplish this requirement.

Task 1-42

The username and password for the user is **ccie** and **ccie**.

- You use this standard technique to define the username and password

```
r8(config)# username ccie password ccie
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

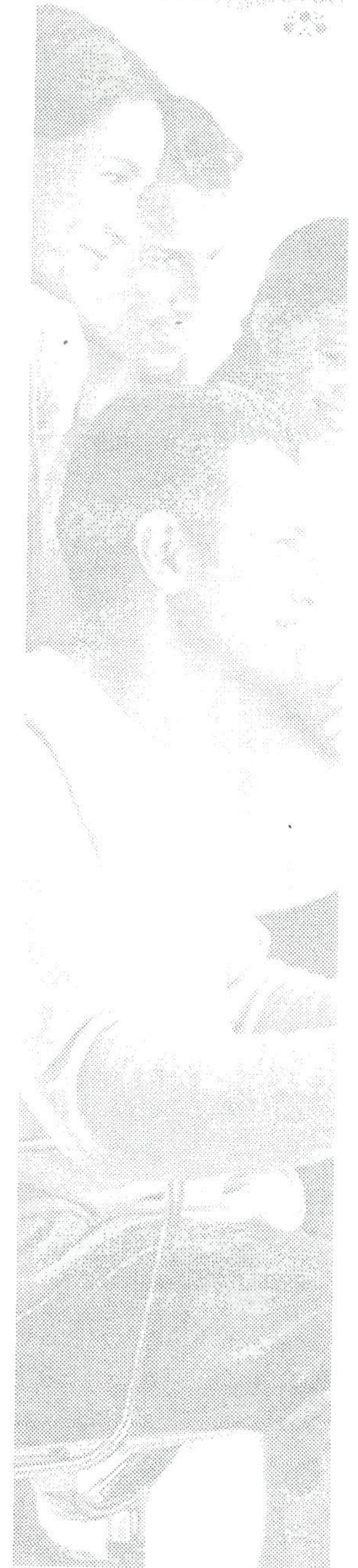
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 2: Network Attacks and Advanced Filtering

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 2 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 2-A.
- The Routers are running the following protocols:
 - OSPF as the routing protocol
- This lab will focus strictly on Network attacks and Advanced Filtering. You will need to pre-configure the network with the base Frame Relay, IP Addressing and OSPF configuration. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs* → Section 2 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Route Maps

Task 2-1

R2 has detected attacks coming in from the Ethernet segment.

- Applying a route map with the following information would be ok to solve the problem. The access list and also the size of the packet is specified as well.

```
R2(config)#access-list 101 permit tcp any any eq www
```

```
R2(config)#route-map BlackHole permit 10  
R2(config-route-map)#match ip address 101
```

Task 2-2

All the packets are HTTP packets with a size of 115 bytes.

- Use the following command to make sure that the HTTP packet has the size of 115.

```
R2(config-route-map)#match length 115 115
```

Task 2-3

Use Policy Based Routing (PBR) to block this attack by Black Holing the packets.

- The PBR is used in this task and the attack would go to Null0 interface.

```
R2(config-route-map)#set interface Null0
```

After the routemap is applied, the result will be shown below:


```
R2#sh route-map
route-map BlackHole, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
    length 115 115
  Set clauses:
    interface Null0
  Policy routing matches: 0 packets, 0 bytes
route-map BlackHole, permit, sequence 20
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

```
R2#sh ip policy
Interface      Route map
Fa1/0          BlackHole
```

```
R2#sh ip access-lists 101
Extended IP access list 101
  10 permit tcp any any eq www
```

Smurf Attack

Task 2-4

You are also the administrator for R5. You want to block a smurf attack from the Ethernet segment.

- You want to have a access list applied to the Ethernet interface with the following command:

```
r5(config)#access-list 101 deny icmp any any echo
r5(config)#access-list 101 deny icmp any any echo-reply
r5(config)#access-list 101 permit ip any any
```

Task 2-5

Using an access-list block this type of attack on R5.

- In order to prevent this problem, the access list can be applied. Then the output can be shown below:

```
R5#sh ip access-lists
Extended IP access list 101
  10 deny icmp any any echo
  20 deny icmp any any echo-reply
  30 permit ip any any (26 matches)
```


IP Spoofing

Task 2-6

Remove problems caused by the introduction of malformed or forged IP source addresses into a network by discarding IP packets that lack a verifiable IP source address in R2's F1/0.

- We want to verify the reverse path info, specifically with the info from the next task.

```
R2(config-if)#ip verify unicast reverse-path 160
```

Task 2-7

An application server on the 150.50.56.0/24 network is sending out packets with a source address of 192.168.24.20. Make sure that only spoofed packets from this server are dropped.

- Normally, having the verify reverse-path command is enough. However, in order to be more specific for that IP address, the following access list is needed.
- The following command would allow you to drop the packet to the IP address specified above.

```
R2(config)#access-list 160 deny ip host 192.168.24.20 any log-input
R2(config)#access-list 160 permit ip any any
```

- The output can be verified below:

```
R2#sh ip access-lists 160
Extended IP access list 160
 10 deny ip host 192.168.24.20 any log-input
 20 permit ip any any
```

- Therefore, the resulting command is as follows:

```
R2(config-if)#ip verify unicast reverse-path 160
```

- If and only if a packet fails the uRPF check will the ACL be checked. Packets that are denied by the ACL will be dropped, while packets that are permitted will be forwarded.

Preventing attacks on the Switch

Task 2-8

You do not want a device with a MAC address of 0015.12AB.BAD0 to send AppleTalk and Vines traffic into port F 0/6 on Switch 1.

- You need to establish a CAT MAC Access list to block the appletalk and vines traffic.

```
sw1(config)#mac access-list extended macfilter
sw1(config-ext-macl)#deny host 0015.12ab.bad0 any vines-echo
sw1(config-ext-macl)#deny host 0015.12ab.bad0 any vines-ip
sw1(config-ext-macl)#deny host 0015.12ab.bad0 any appletalk
sw1(config-ext-macl)#permit any any
```


Task 2-9

Filter the preceding traffic coming into port F 0/6 on Switch 1. Allow all other traffic.

- You are applying the access list to the F0/6 interface.

```
sw1(config-ext-macl)#int fa0/6
sw1(config-if)#mac access-group macfilter in
```

Task 2-10

Use a Mac address list to block this type of traffic.

- You can define the action for the MAC access list with the following commands.

```
sw1(config)#vlan access-map block_arp 10
sw1(config-access-map)#action forward
sw1(config-access-map)#match mac address ARP-Packet
sw1(config-access-map)#vlan access-map block_arp 20
sw1(config-access-map)#action block
sw1(config-access-map)#vlan filter block_arp vlan-list 20
```

Task 2-11

Configure MAC address filtering and only permit MAC address from 0000.1111.2222 to 0000.2222.1111 for Vlan 20.

- The following command can help to set the MAC address filter required above. In addition, the 0x806 is used in order to notify this is for the ARP table conversion.

```
sw1(config)#mac access-list extended ARP_Packet
sw1(config-ext-macl)#permit host 0000.1111.2222 host 0000.2222.1111
0x806 0x0
```

- In order to verify the requirement, the following commands can be used:

```
Sw1#sh access-lists
Extended MAC access list ARP-Packet
Extended MAC access list ARP_Packet
    permit host 0000.1111.2222 host 0000.2222.1111 0x806 0x0
Extended MAC access list macfilter
    deny host 0015.12ab.bad0 any vines-echo
    deny host 0015.12ab.bad0 any vines-ip
    deny host 0015.12ab.bad0 any appletalk
    permit any any
```



```

Sw1#sh mac access-group
Interface FastEthernet0/1:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/2:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/3:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/4:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/5:
  Inbound access-list is not set
  Outbound access-list is not set
Interface FastEthernet0/6:
  Inbound access-list is macfilter
  Outbound access-list is not set
Interface FastEthernet0/7:
  Inbound access-list is not set

```

IP TCP Intercept

Task 2-12

The 150.50.24.0 network is experiencing syn attacks from the Frame cloud to your web servers.

- This is for preparing you to use the TCP intercept commands listed in the following requirements.

Task 2-13

R4 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets.

- You use the following command to define the watch timer.

```
r4(config)#ip tcp intercept watch-timeout 20
```

Task 2-14

Limit IP TCP intercept to only watch packets coming from 150.50.46.0 or the 150.50.56.0 networks for Web traffic.

- You want to define the access list to specify what packets to watch, and then apply this to the TCP intercept list.

```

r4(config)#access-list 101 permit tcp 150.50.46.0 0.0.0.255 any eq
www
r4(config)#access-list 101 permit tcp 150.50.56.0 0.0.0.255 any eq
www
r4(config)#ip tcp intercept list 101

```


Task 2-15

Configure IP TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850.

- The following command can set the embryonic connection between 1050 and 850.

```
r4(config)#ip tcp intercept max-incomplete low 850
r4(config)#ip tcp intercept max-incomplete high 1050
```

Task 2-16

Set the software to manage the connection for 12 hours after no activity.

- This would timeout after 43200 seconds.

```
r4(config)#ip tcp intercept connection-timeout 43200
```

Task 2-17

Configure the router such that it will enter aggressive mode when 1400 connections are made within 60 seconds.

- This can allow the one minute high to be 1400 connections.

```
r4(config)#ip tcp intercept one-minute high 1400
```

Task 2-18

Configure the router such that it will leave aggressive mode when the number of connections drop below 850 in a 60 second window.

- This can limit the one minute low to be 850 connections.

```
r4(config)#ip tcp intercept one-minute low 850
```

- In a network where the above limit is exceeded, the following two commands would show valuable information for network debugging.

```
R4#sh tcp intercept statistics
Watching new connections using access-list 101
0 incomplete, 0 established connections (total 0)
0 connection requests per minute
```

```
R4#sh tcp intercept connections
Incomplete:
Client          Server          State    Create    Timeout    Mode

Established:
Client          Server          State    Create    Timeout    Mode
R4#
```

```
R4#sh ip access-lists
Extended IP access list 101
 10 permit ip 150.50.46.0 0.0.0.255 any
 20 permit ip 150.50.56.0 0.0.0.255 any
```


Network Based Application Recognition

Task 2-19

You are under the Code Red and Nimda attacks from the Frame Cloud on R4.

- You need to define what is a code red attack, with URL of *.ida, cmd.exe, root.exe, readme.eml and then match it with the policy map -red attack.

```
r4(config)#class-map match-any nimda-code-red
r4(config-cmap)#match protocol http url "*.ida*"
r4(config-cmap)#match protocol http url "*cmd.exe*"
r4(config-cmap)#match protocol http url "*root.exe*"
r4(config-cmap)#match protocol http url "*readme.eml*"
r4(config-cmap)#policy-map nimda-code-red
r4(config-pmap)#class nimda-code-red
r4(config-pmap-c)#set ip dscp 1
```

Task 2-20

Using NBAR classify the traffic on the inbound on S 0/0/0.

- You want to apply the previous policy map to S0/0/0 with the following command.

```
r4(config-if)#service-policy input nimda-code-red
```

- There are several steps that are always necessary to perform QoS. First, we should define the class map Then we should define the policy map so that we will know what policy should be applied to what kind of traffic. Lastly, the policy map should be applied to the interface.

Task 2-21

Drop the classified traffic on an outbound ACL on the F 0/0 interface. Use DSCP to classify Code Red traffic.

- You need to define an out access list ACL 102 and then drop everything with DSCP equal to 1.

```
r4(config)#access-list 102 deny ip any any dscp 1
r4(config)#access-list 102 permit ip any any
r4(config)#interface f0/0
r4(config-if)#ip access-group 102 out
```


- As shown here, this step first defines the class-map as the protocol with HTTP url as required. Then it would apply the DSCP 1 as the policy. All traffic that matches would have DSCP of 1 and the rest would remain as default DSCP. Lastly, the policy is applied to the interface.

```
R4#show class-map
Class Map match-any nimda-code-red (id 1)
  Match protocol http url "*.ida*"
  Match protocol http url "*cmd.exe*"
  Match protocol http url "*root.exe*"
  Match protocol http url "*readme.eml*"

Class Map match-any class-default (id 0)
  Match any
```

```
R4#show policy-map
Policy Map nimda-code-red
  Class nimda-code-red
    set ip dscp 1
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

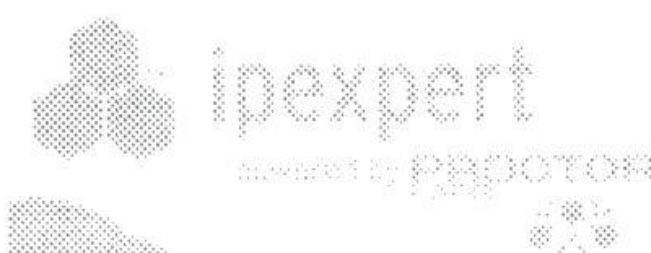
This page left intentionally blank.

Section 3: GRE and NAT

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 3 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 3-A.
- This lab will focus strictly on GRE and NAT. You will need to pre-configure the network with the base Frame Relay, IP Addressing and VLAN configuration. The pre-configuration will not include configuration of Routing Protocols. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 3 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Base Routing Configuration

Task 3-1

Routers R1, R2, R4 and R5 need to be configured with EIGRP as the routing protocol in AS 1245 with the following networks advertised:

- R1 – 150.50.1.0/24 and 150.50.12.0/24
 - R2 – 150.50.12.0/24, 150.50.24.0/24 and 150.50.25.0/24
 - R4 – 150.50.4.0/24, 150.50.24.0/24 and 150.50.45.0/24
 - R5 – 150.50.25.0/24 and 150.50.45.0/24.
- **First, setup the EIGRP process to run on all of the routers listed above. You will use the `router eigrp as-number` command for this.**
- **Auto summary allows the automatic summarization of subnet routes into network-level routes and is enabled by default. To disable this, use the `no auto-summary` command under the EIGRP process.**
- **To advertise a network under EIGRP use the `network network-number [network-mask]` command. The network command also enables EIGRP to send updates to the interfaces in the specified networks. This means that EIGRP will send out routing updates and try to form adjacencies over interfaces that are defined with the network command.**
- **Following are the configuration examples for each router:**

```
r1(config)#router eigrp 1245
r1(config-router)#no auto-summary
r1(config-router)#network 150.50.1.0 0.0.0.255
r1(config-router)#network 150.50.12.0 0.0.0.255
```

```
r2(config)#router eigrp 1245
r2(config-router)#no auto-summary
r2(config-router)#network 150.50.12.0 0.0.0.255
r2(config-router)#network 150.50.24.0 0.0.0.255
r2(config-router)#network 150.50.25.0 0.0.0.255
```



```

r4(config)#router eigrp 1245
r4(config-router)#no auto-summary
r4(config-router)#network 150.50.4.0 0.0.0.255
r4(config-router)#network 150.50.24.0 0.0.0.255
r4(config-router)#network 150.50.45.0 0.0.0.255

r5(config)#router eigrp 1245
r5(config-router)#no auto-summary
r5(config-router)#network 150.50.25.0 0.0.0.255
r5(config-router)#network 150.50.45.0 0.0.0.255

```

- Verify the neighbor relationships with the `show ip eigrp neighbor` command.

```

R2#sh ip eigrp neighbor
IP-EIGRP neighbors for process 1245
H   Address                Interface      Hold Uptime    SRTT   RTO   Q   Seq
                               (sec)          (ms)          Cnt  Num
2   150.50.25.5             Se0/1/0.5      12 00:00:35     48    288   0   4
1   150.50.24.4             Se0/1/0.4      13 00:01:06     29    200   0   5
0   150.50.12.1             Fa1/0          12 00:01:35      1    200   0   3

```

- This output on R2 verifies the neighbor relationships in AS1245 to R1, R4 and R5.
- At this point, check the routing table on any router to make sure that you see all of the configured networks properly. Routes marked with a code of 'D' are those learned via EIGRP.

```

R2#sh ip route

Gateway of last resort is not set

    150.50.0.0/24 is subnetted, 6 subnets
D       150.50.45.0 [90/2681856] via 150.50.25.5, 00:04:20, Serial0/1/0.5
          [90/2681856] via 150.50.24.4, 00:04:20, Serial0/1/0.4
D       150.50.4.0 [90/2297856] via 150.50.24.4, 00:04:20, Serial0/1/0.4
D       150.50.1.0 [90/156160] via 150.50.12.1, 00:04:19, FastEthernet1/0
C       150.50.12.0 is directly connected, FastEthernet1/0
C       150.50.24.0 is directly connected, Serial0/1/0.4
C       150.50.25.0 is directly connected, Serial0/1/0.5

```

Task 3-2

Do not advertise any of the RFC 1918 networks under EIGRP 1245.

- EIGRP only advertises those networks specified with the `network network-number [network-mask]` command. Since none of the RFC 1918 networks were specified in the previous task, they will not be advertised.

- Verify that the RFC 1918 networks are not being advertised by reviewing the routing table displayed in task 3-1, and check the routing tables on each of the other routers running EIGRP. Use the command `show ip route eigrp` to display only those routes learned via EIGRP.

```
R4#sh ip route eigrp
      150.50.0.0/24 is subnetted, 6 subnets
D       150.50.1.0 [90/2300416] via 150.50.24.2, 00:08:09, Serial0/0/0.2
D       150.50.12.0 [90/2172416] via 150.50.24.2, 00:08:09, Serial0/0/0.2
D       150.50.25.0 [90/2681856] via 150.50.45.5, 00:08:13, Serial0/0/0.5
                        [90/2681856] via 150.50.24.2, 00:08:13, Serial0/0/0.2
```

Configuring GRE Tunnels

Task 3-3

Configure a GRE tunnel between R1 and R5. The Tunnel Network should be set to 10.15.15.0/24. Make sure the tunnel is authenticated.

- Most dynamic routing protocols use broadcast or IP multicast packets for operation. GRE tunnels can be utilized to create a virtual point-to-point link between sites that have only IP unicast connectivity, such as VPN connections. These tunnels are capable of handling the transportation of broadcast or IP multicast traffic, enabling dynamic routing protocols to operate across encrypted links.
- Define a virtual tunnel interface on each router endpoint with the command `interface tunnel number`.
- Specify a source IP address for the each tunnel interface with the interface configuration command `tunnel source {ip-address | interface}`. The IP address specified as the source address must be an address of an interface on the router, or you may specify an interface on the router that has IP enabled.
- Specify a destination IP address for each tunnel interface with the interface configuration command `tunnel destination {ip-address | hostname}`. The IP address specified as the destination address must be an address of an interface on the destination router, or you may specify a hostname that resolves to the IP address of an interface on the destination router.
- Enable IP on each tunnel interface with the interface configuration command `ip address ip-address netmask`. The IP addresses specified for each end of the tunnel must be within the same subnet.
- Following are the configuration examples for each router:

```
r1(config)#interface tunnel 15
r1(config-router)#tunnel source 150.50.12.1
r1(config-router)#tunnel destination 150.50.25.5
r1(config-router)#ip address 10.15.15.1 255.255.255.0
```



```
r5(config)#interface tunnel 15
r5(config-router)#tunnel source 150.50.25.5
r5(config-router)#tunnel destination 150.50.12.1
r5(config-router)#ip address 10.15.15.5 255.255.255.0
```

Task 3-4

Configure a GRE tunnel between R1 and R4. The Tunnel Network should be set to 10.14.14.0/24. Make sure the tunnel is authenticated.

→ Following are the configuration examples for each router:

```
r1(config)#interface tunnel 14
r1(config-router)#tunnel source 150.50.12.1
r1(config-router)#tunnel destination 150.50.24.4
r1(config-router)#ip address 10.14.14.1 255.255.255.0

r4(config)#interface tunnel 14
r4(config-router)#tunnel source 150.50.24.4
r4(config-router)#tunnel destination 150.50.12.1
r4(config-router)#ip address 10.14.14.4 255.255.255.0
```

Task 3-5

Configure a GRE tunnel between R4 and R5. The Tunnel Network should be set to 10.45.45.0/24. Make sure the tunnel is authenticated.

→ Following are the configuration examples for each router:

```
r4(config)#interface tunnel 45
r4(config-router)#tunnel source 150.50.45.4
r4(config-router)#tunnel destination 150.50.45.5
r4(config-router)#ip address 10.45.45.4 255.255.255.0

r5(config)#interface tunnel 45
r5(config-router)#tunnel source 150.50.45.5
r5(config-router)#tunnel destination 150.50.45.4
r5(config-router)#ip address 10.45.45.5 255.255.255.0
```

Task 3-6

Make sure you can ping the Tunnel interfaces of directly connected tunnels. For example, you should be able to ping 10.15.15.1 from R5 and you should also be able to ping 10.14.14.4 from R1.

→ At this point all tunnel interfaces created in this lab should be reachable from directly connected routers. Test this by pinging.

Routing RFC 1918 using Static Routes

Task 3-7

R1 should be able to route to the following networks:

- 10.57.57.0 /24
- 192.168.5.0 /24
- 192.168.4.0 /24

- Task 3-11 states that no routing protocols are to be used to advertise these routes to other routers. Static routes can be configured to manually add routes to a routing table of a router.
- To configure a static route, use the command `ip route prefix mask {ip-address / interface}`. Static routes that point to an interface will be advertised via dynamic routing protocols.

```
r1(config)#ip route 10.57.57.0 255.255.255.0 Tunnel15
r1(config)#ip route 192.168.5.0 255.255.255.0 Tunnel14
r1(config)#ip route 192.168.4.0 255.255.255.0 Tunnel15
```

- Verify the routing table entries with the `show ip route static` command.

```
R1#sh ip route static
S    192.168.4.0/24 is directly connected, Tunnel15
S    192.168.5.0/24 is directly connected, Tunnel14
     10.0.0.0/24 is subnetted, 3 subnets
S        10.57.57.0 is directly connected, Tunnel15
```

Task 3-8

R4 should be able to route to the following networks:

- 10.57.57.0 /24
- 192.168.5.0 /24
- 172.16.1.0 /24

- Following are the static route commands for R4:

```
r4(config)#ip route 10.57.57.0 255.255.255.0 Tunnel45
r4(config)#ip route 192.168.5.0 255.255.255.0 Tunnel45
r4(config)#ip route 172.16.1.0 255.255.255.0 Tunnel14
```

- Verify the routing table entries with the `show ip route static` command.

```
R4#sh ip route stat
     172.16.0.0/24 is subnetted, 1 subnets
S        172.16.1.0 is directly connected, Tunnel14
S    192.168.5.0/24 is directly connected, Tunnel45
     10.0.0.0/24 is subnetted, 3 subnets
S        10.57.57.0 is directly connected, Tunnel45
```


Task 3-9

R5 should be able to route to the following networks:

- ➔ 192.168.4.0 /24
- ➔ 172.16.1.0 /24

➔ **Following are the static route commands for R5:**

```
r5(config)#ip route 192.168.4.0 255.255.255.0 Tunnel45
r5(config)#ip route 172.16.1.0 255.255.255.0 Tunnel15
```

➔ **Verify the routing table entries with the show ip route static command.**

```
R5#sh ip route static
      172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0 is directly connected, Tunnel15
S       192.168.4.0/24 is directly connected, Tunnel45
```

Task 3-10

R7 should also be able to connect to any of the RFC 1918 networks. You can only use one **ip route** command to accomplish this.

➔ **In order to accomplish this using only one static route statement, you will need to configure a static route on R7 to a destination network that includes all of the RFC 1918 networks. There are several RFC 1918 networks utilized in this lab example, but these network addresses are not contiguous. Since R7 has only one path to the rest of the network, the best method, then, would be to create a static default route pointing to R5.**

```
r7(config)#ip route 0.0.0.0 0.0.0.0 10.57.57.5
```

➔ **Verify the routing table entries with the show ip route command.**

```
R7#sh ip route

Gateway of last resort is 10.57.57.5 to network 0.0.0.0

      10.0.0.0/24 is subnetted, 1 subnets
C       10.57.57.0 is directly connected, Ethernet0/0
S*     0.0.0.0/0 [1/0] via 10.57.57.5
```


Task 3-11

No routing protocols can be used for this section. No configuration should be done on R2 to accomplish this section.

- Only static route commands were used for this section. Specifying the tunnel interfaces as the destination rather than the next hop IP address was necessary, otherwise packets with a destination address on the 172.16.1.0/24 network would have been routed to R2, and then dropped, since R2 was not changed and does not have routes to the destination networks used in this section. Use of the GRE tunnels encapsulates the packets in a tunnel header with a destination IP address of the tunnel endpoint, thus allowing the packets to be routed through R2.

Routing RFC 1918 using RIP

Task 3-12

Remove all the Static Routes configured in the previous section.

- Remove each of the static routes entered in the previous section using the command `no ip route prefix mask` for each static route that was configured. For example,

```
r1(config)#no ip route 10.57.57.0 255.255.255.0
```

Task 3-13

R1, R4, R5 and R7 should be able to route to the RFC 1918 networks.

- RIP routing will be used to advertise the RFC 1918 networks amongst the routers. To enable the RIP routing process, use the command `router rip` on the specified routers.
- To advertise networks under RIP use the `network network-number` command. The `network` command also enables RIP to send updates to the interfaces in the specified networks.
- Be sure to include the tunnel interface networks in order to send RIP advertisements across the GRE tunnels.
- Following are the configuration examples for each router:

```
r1(config)#router rip
r1(config-router)#network 172.16.1.0
r1(config-router)#network 10.0.0.0
```

```
r4(config)#router rip
r4(config-router)#network 192.168.4.0
r4(config-router)#network 10.0.0.0
```

```
r5(config)#router rip
r5(config-router)#network 192.168.5.0
r5(config-router)#network 10.0.0.0
```



```
r7(config)#router rip
r7(config-router)#network 10.0.0.0
```

Task 3-14

Configure RIP V2 as the routing protocols to accomplish this task.

- ➔ To specify a RIP version to be used globally by the router, use the version 2 command in router configuration mode.
- ➔ Auto summary allows the automatic summarization of subnet routes into network-level routes and is enabled by default. To disable this, use the no auto-summary command under the RIP process, for each router.

```
r1(config-router)#version 2
r1(config-router)#no auto-summary
```

Task 3-15

Do not use any Static Routes to accomplish this section.

- ➔ All static routes were removed, and RIPv2 dynamic routing configured. Verify the routing table entries with the show ip route command on each router. Look for the 'R' code in the first position of each routing table entry that specifies the route was learned via RIP.

```
R7#sh ip route
```

Gateway of last resort is not set

```

      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
R       172.16.0.0/16 [120/2] via 10.57.57.5, 00:00:16, Ethernet0/0
R       172.16.1.0/24 [120/2] via 10.57.57.5, 00:00:16, Ethernet0/0
R      192.168.4.0/24 [120/2] via 10.57.57.5, 00:00:16, Ethernet0/0
R      192.168.5.0/24 [120/1] via 10.57.57.5, 00:00:16, Ethernet0/0
      10.0.0.0/24 is subnetted, 4 subnets
R       10.45.45.0 [120/1] via 10.57.57.5, 00:00:16, Ethernet0/0
R       10.15.15.0 [120/1] via 10.57.57.5, 00:00:16, Ethernet0/0
R       10.14.14.0 [120/2] via 10.57.57.5, 00:00:17, Ethernet0/0
C       10.57.57.0 is directly connected, Ethernet0/0
```

Routing RFC 1918 using OSPF

Task 3-16

Remove RIP as the Routing protocol on R1, R4, R5 and R7.

- ➔ Remove the RIP routing process from each router using the command no router rip.

Task 3-17

Run OSPF as the routing protocol to route the RFC 1918 networks.

- OSPF routing will be used to advertise the RFC 1918 networks amongst the routers. To enable the OSPF routing process, use the command `router ospf process-number` on the specified routers. The *process-number* argument is locally significant only, in cases of running multiple processes, so for this exercise, the value is unimportant.
- To advertise networks under OSPF use the `network ip-address wildcard-mask area area-id` command. For OSPF to operate on the interface, the primary address of the interface must be covered by the combination *ip-address wildcard-mask* arguments. For this exercise, use *area-id* of 0 for all interfaces, since no requirements were specified.
- Be sure to include the tunnel interface networks in order to send OSPF advertisements across the GRE tunnels.
- Following are the configuration examples for each router:

```
r1(config)#router ospf 1
r1(config-router)#network 172.16.1.0 0.0.0.255 area 0
r1(config-router)#network 10.0.0.0 0.255.255.255 area 0

r4(config)#router ospf 1
r4(config-router)#network 192.168.4.0 0.0.0.255 area 0
r4(config-router)#network 10.0.0.0 0.255.255.255 area 0

r5(config)#router ospf 1
r5(config-router)#network 192.168.5.0 0.0.0.255 area 0
r5(config-router)#network 10.0.0.0 0.255.255.255 area 0

r7(config)#router ospf 1
r7(config-router)#network 10.0.0.0 0.255.255.255 area 0
```

Task 3-18

Do not use any Static Routes to accomplish this section.

- All static routes were removed, and OSPF dynamic routing configured. Verify the routing table entries with the `show ip route` command on each router. Look for the 'O' code in the first position of each routing table entry that specifies the route was learned via OSPF.

```
R7#sh ip route
```

```
Gateway of last resort is not set
```

```

    172.16.0.0/32 is subnetted, 1 subnets
O       172.16.1.1 [110/11122] via 10.57.57.5, 00:00:08, Ethernet0/0
    192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.4 [110/11122] via 10.57.57.5, 00:00:08, Ethernet0/0
    192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.5 [110/11] via 10.57.57.5, 00:00:08, Ethernet0/0
    10.0.0.0/24 is subnetted, 4 subnets
O       10.45.45.0 [110/11121] via 10.57.57.5, 00:00:08, Ethernet0/0
```



```

O      10.15.15.0 [110/11121] via 10.57.57.5, 00:00:09, Ethernet0/0
O      10.14.14.0 [110/22232] via 10.57.57.5, 00:00:09, Ethernet0/0
C      10.57.57.0 is directly connected, Ethernet0/0

```

Routing RFC 1918 using EIGRP

Task 3-19

Remove OSPF as the Routing protocol on R1, R4, R5 and R7.

- Remove the OSPF routing process from each router using the command `no router ospf 1`.

Task 3-20

Run EIGRP 1457 as the routing protocol to route the RFC 1918 networks.

- A separate EIGRP routing process from that which was configured in task 3-1 will be used to advertise the RFC 1918 networks amongst the routers. To enable the EIGRP routing process, use the command `router eigrp as-number` on the specified routers.
- Auto summary allows the automatic summarization of subnet routes into network-level routes and is enabled by default. To disable this, use the `no auto-summary` command under the EIGRP process.
- To advertise a network under EIGRP use the `network network-number [network-mask]` command. The network command also enables EIGRP to send updates to the interfaces in the specified networks. This means that EIGRP will send out routing updates and try to form adjacencies over interfaces that are defined with the network command.
- Be sure to include the tunnel interface networks in order to send EIGRP advertisements across the GRE tunnels.
- Following are the configuration examples for each router:

```

r1(config)#router eigrp 1457
r1(config-router)#no auto-summary
r1(config-router)#network 172.16.1.0 0.0.0.255
r1(config-router)#network 10.0.0.0 0.255.255.255

```

```

r4(config)#router eigrp 1457
r4(config-router)#no auto-summary
r4(config-router)#network 192.168.4.0 0.0.0.255
r4(config-router)#network 10.0.0.0 0.255.255.255

```

```

r5(config)#router eigrp 1457
r5(config-router)#no auto-summary
r5(config-router)#network 192.168.5.0 0.0.0.255
r5(config-router)#network 10.0.0.0 0.255.255.255

```

```

r7(config)#router eigrp 1457
r7(config-router)#no auto-summary
r7(config-router)#network 10.0.0.0 0.255.255.255

```


Task 3-21

Do not use any Static Routes to accomplish this section.

- All static routes were removed, and an additional EIGRP dynamic routing process configured. Verify the routing table entries with the `show ip route` command on each router. Look for the 'D' code in the first position of each routing table entry that specifies the route was learned via EIGRP.

```
R5#sh ip route
```

```
Gateway of last resort is not set
```

```

      172.16.0.0/24 is subnetted, 1 subnets
D       172.16.1.0 [90/297372416] via 10.15.15.1, 00:00:32, Tunnel15
D     192.168.4.0/24 [90/297372416] via 10.45.45.4, 00:00:32, Tunnel45
C     192.168.5.0/24 is directly connected, Loopback0
      10.0.0.0/24 is subnetted, 4 subnets
C       10.57.57.0 is directly connected, FastEthernet0/0
C       10.45.45.0 is directly connected, Tunnel45
C       10.15.15.0 is directly connected, Tunnel15
D       10.14.14.0 [90/310044416] via 10.45.45.4, 00:00:32, Tunnel45
              [90/310044416] via 10.15.15.1, 00:00:33, Tunnel15
      150.50.0.0/24 is subnetted, 6 subnets
C       150.50.45.0 is directly connected, Serial0/1/0.4
D       150.50.4.0 [90/2297856] via 150.50.45.4, 00:02:53, Serial0/1/0.4
D       150.50.1.0 [90/2300416] via 150.50.25.2, 00:02:55, Serial0/1/0.2
D       150.50.12.0 [90/2172416] via 150.50.25.2, 00:02:55, Serial0/1/0.2
D       150.50.24.0 [90/2681856] via 150.50.45.4, 00:02:55, Serial0/1/0.4
              [90/2681856] via 150.50.25.2, 00:02:55, Serial0/1/0.2
C       150.50.25.0 is directly connected, Serial0/1/0.2

```

NAT

Task 3-22

Configure R5 such that the 10.57.57.0/24 network can reach non RFC 1918 networks using a pool of either 150.50.25.0/24 or 150.50.45.0/24.

- Setup R5 for NAT – Network Address Translation. First, create the two NAT pools using the `ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}` command. Because the networks that are to be used for the two NAT pools are the same /24 networks as used for the frame-relay links, and thus contain existing hosts, use a *start-ip* address of x.x.x.11 for each pool, to prevent use of the addresses already configured for the frame-relay sub-interfaces.

```

r5(config)#ip nat pool pool25 150.50.25.11 150.50.25.254 netmask
255.255.255.0
r5(config)#ip nat pool pool45 150.50.45.11 150.50.45.254 netmask
255.255.255.0

```


- **Identify which interfaces to treat as inside and outside for the NAT process.**

```
r5(config)#int FastEthernet0/0
r5(config-if)#ip nat inside
r5(config-if)#int Serial0/1/0.2 point-to-point
r5(config-if)#ip nat outside
r5(config-if)#int Serial0/1/0.4 point-to-point
r5(config-if)#ip nat outside
```

Task 3-23

Make sure pools are chosen in an efficient manner. When 10.57.57.0 communicates to 150.50.12.0 it should use the 150.50.25.0 pool and when it communicates to 150.50.4.0 it should use the 150.50.45.0 pool. 150.50.24.0 should be reachable via either pool. Make sure to allow for failover in case of a problem with either PVC going to R2 and R4

- **Create access-lists defining the 'interesting traffic' that is to be NAT'd. We are going to use a single access-list to define traffic from the 10.57.57/24 network to any 150.50 network. We will use this access-list along with the outgoing interface to help determine which pool to use. By using the outgoing interface, and allowing the 10.57.57/24 network to reach any 150.50 network via either interface, a failure of either PVC will allow for traffic to still have reachability. First we define the ACL.**

```
r5(config)#access-list 100 permit ip 10.57.57.0 0.0.0.255 150.50.0.0
0.0.0.255
```

Task 3-24

R7 should be able to connect to the non RFC 1918 networks as well.

- **R7's only interface is in the 10.57.57.0/24 network, so packets sourced from R7 will be NAT'd on R5, without any additional configuration. Since R7 has no routes to the non-RFC 1918 networks, a static default route must be configured on R7.**

Task 3-25

One static route is allowed for this section.

- **A static default route will be necessary on R7, as configured in Task 3-10.**

Task 3-26

Route Maps are allowed for this section.

- **To enable NAT of inside source IP addresses, you will use the `ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface type number | pool pool-name} [overload]` command.**

- You have defined a single ACL to match outgoing traffic, however we still need two separate route-maps, each relating to the outgoing interface. Define two route-maps, to match the destination addresses specified in each ACL. Also define the outgoing interface that should be matched.

```
r5(config)#route-map nat25 permit 10
r5(config-route-map)#match ip address 100
r5(config-route-map)#match interface Serial0/1/0.2

r5(config)#route-map nat45 permit 10
r5(config-route-map)#match ip address 100
r5(config-route-map)#match interface Serial0/1/0.4
```

- Enable the NAT of the inside source IP addresses, using the route-map arguments. If the destination addresses match those specified in route-map nat25, (acl 101), then use the NAT pool nat25. If the destination addresses match those specified in route-map nat45, (acl 102), then use the NAT pool nat45.

```
r5(config)#ip nat inside source route-map nat25 pool pool25
r5(config)#ip nat inside source route-map nat45 pool pool45
```

Task 3-27

Make sure when 10.57.57.0 network is communicating to other RFC 1918 networks it does not get translated.

- The ACLs created are extended ACLs, and specify the destination addresses for the interesting traffic to be NAT'd. Since no RFC 1918 addresses were specified in the ACLs, traffic to these destinations will not be NAT'd.
- Test with an extended ping from R5. Run `debug ip nat` during the ping test.

```
r5#debug ip nat
```

- First, verify that packets destined to 150.50.12.0 use the NAT pool 150.50.25.0.

```
R5#ping
Protocol [ip]:
Target IP address: 150.50.12.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.57.57.5
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.50.12.1, timeout is 2 seconds:
Packet sent with a source address of 10.57.57.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
R5#
```



```
*Oct 21 01:55:15.513: NAT: s=10.57.57.5->150.50.25.11, d=150.50.12.1 [20]
*Oct 21 01:55:15.573: NAT*: s=150.50.12.1, d=150.50.25.11->10.57.57.5 [20]
*Oct 21 01:55:15.573: NAT: s=10.57.57.5->150.50.25.11, d=150.50.12.1 [21]
*Oct 21 01:55:15.629: NAT*: s=150.50.12.1, d=150.50.25.11->10.57.57.5 [21]
*Oct 21 01:55:15.629: NAT: s=10.57.57.5->150.50.25.11, d=150.50.12.1 [22]
*Oct 21 01:55:15.685: NAT*: s=150.50.12.1, d=150.50.25.11->10.57.57.5 [22]
*Oct 21 01:55:15.689: NAT: s=10.57.57.5->150.50.25.11, d=150.50.12.1 [23]
*Oct 21 01:55:15.745: NAT*: s=150.50.12.1, d=150.50.25.11->10.57.57.5 [23]
*Oct 21 01:55:15.745: NAT: s=10.57.57.5->150.50.25.11, d=150.50.12.1 [24]
*Oct 21 01:55:15.801: NAT*: s=150.50.12.1, d=150.50.25.11->10.57.57.5 [24]
```

R5#**sh ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	150.50.25.11:5	10.57.57.5:5	150.50.12.1:5	150.50.12.1:5

→ **Next, verify that packets destined to 150.50.4.0 use the NAT pool 150.50.45.0.**

R5#**ping**

```
Protocol [ip]:
Target IP address: 150.50.4.4
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.57.57.5
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.50.4.4, timeout is 2 seconds:
Packet sent with a source address of 10.57.57.5
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
R5#
*Oct 21 02:01:38.125: NAT: s=10.57.57.5->150.50.45.11, d=150.50.4.4 [35]
*Oct 21 02:01:38.153: NAT*: s=150.50.4.4, d=150.50.45.11->10.57.57.5 [35]
*Oct 21 02:01:38.157: NAT: s=10.57.57.5->150.50.45.11, d=150.50.4.4 [36]
*Oct 21 02:01:38.185: NAT*: s=150.50.4.4, d=150.50.45.11->10.57.57.5 [36]
*Oct 21 02:01:38.185: NAT: s=10.57.57.5->150.50.45.11, d=150.50.4.4 [37]
*Oct 21 02:01:38.217: NAT*: s=150.50.4.4, d=150.50.45.11->10.57.57.5 [37]
*Oct 21 02:01:38.217: NAT: s=10.57.57.5->150.50.45.11, d=150.50.4.4 [38]
*Oct 21 02:01:38.249: NAT*: s=150.50.4.4, d=150.50.45.11->10.57.57.5 [38]
*Oct 21 02:01:38.249: NAT: s=10.57.57.5->150.50.45.11, d=150.50.4.4 [39]
*Oct 21 02:01:38.281: NAT*: s=150.50.4.4, d=150.50.45.11->10.57.57.5 [39]
```

R5#**sh ip nat trans**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	150.50.45.11:7	10.57.57.5:7	150.50.4.4:7	150.50.4.4:7

→ **Last, verify that packets destined to RFC 1918 addresses are not NAT'd. The ping should succeed, but the debug should not produce any entries. Also, the display of the show ip nat translations command should not have any entries for the ping to the RFC 1918 address.**

PAT

Task 3-28

Configure R1 such that the 172.16.1.0/24 network can reach non RFC 1918 networks without configuring a pool.

- To configure NAT without configuring a pool of NAT addresses, setup R1 for NAT using the interface option, along with the overload option, or PAT – Port Address Translation. Multiple inside addresses can be mapped to one outside address, such as the outside interface. The router uses the TCP or UDP port numbers of each inside host to distinguish between the local addresses.
- Identify which interfaces to treat as inside and outside for the NAT process.

```
r1(config)#int Loopback1
r1(config-if)#ip nat inside
r1(config-if)#int FastEthernet0/0
r1(config-if)#ip nat outside
```

- Create an access-list defining the 'interesting traffic' that is to be NAT'd. The ACL can be defined so as to permit, (define as interesting), that traffic that is to be NAT'd, or it can be defined so as to deny, (define as non-interesting), that traffic that should not be NAT'd, and then permit, (define as interesting), all other traffic. Following is an example configuration using the latter scenario:

```
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 192.168.5.0
0.0.0.255
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 192.168.4.0
0.0.0.255
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 10.57.57.0
0.0.0.255
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 10.14.14.0
0.0.0.255
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 10.15.15.0
0.0.0.255
r1(config)#access-list 101 deny ip 172.16.1.0 0.0.0.255 10.45.45.0
0.0.0.255
r1(config)#access-list 101 deny eigrp any any
r1(config)#access-list 101 permit ip any any
```

- Enable the NAT of the inside source IP addresses, using the interface option with overload.

```
r1(config)#ip nat inside source list 101 interface FastEthernet0/0
overload
```


- **Test and verify with an extended ping from R1. Run debug ip nat during the ping test.**

```
R1#ping
Protocol [ip]:
Target IP address: 150.50.25.5
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.50.25.5, timeout is 2 seconds:
Packet sent with a source address of 172.16.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
R1#
*Oct 21 02:19:29.929: NAT: s=172.16.1.1->150.50.12.1, d=150.50.25.5 [10]
*Oct 21 02:19:29.989: NAT*: s=150.50.25.5, d=150.50.12.1->172.16.1.1 [10]
*Oct 21 02:19:29.989: NAT: s=172.16.1.1->150.50.12.1, d=150.50.25.5 [11]
*Oct 21 02:19:30.045: NAT*: s=150.50.25.5, d=150.50.12.1->172.16.1.1 [11]
*Oct 21 02:19:30.045: NAT: s=172.16.1.1->150.50.12.1, d=150.50.25.5 [12]
*Oct 21 02:19:30.105: NAT*: s=150.50.25.5, d=150.50.12.1->172.16.1.1 [12]
*Oct 21 02:19:30.105: NAT: s=172.16.1.1->150.50.12.1, d=150.50.25.5 [13]
*Oct 21 02:19:30.161: NAT*: s=150.50.25.5, d=150.50.12.1->172.16.1.1 [13]
*Oct 21 02:19:30.161: NAT: s=172.16.1.1->150.50.12.1, d=150.50.25.5 [14]
*Oct 21 02:19:30.221: NAT*: s=150.50.25.5, d=150.50.12.1->172.16.1.1 [14]

R1#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 150.50.12.1:2      172.16.1.1:2      150.50.25.5:2      150.50.25.5:2
```

Task 3-29

Configure R4 such that the 192.168.4.0/24 network can reach the 150.50.12/24 and 150.50.24/24 networks. You should use a pool to accomplish this. Make sure the address is translated using IP address and Port number combination.

- **Setup R4 for NAT – Network Address Translation, using a NAT pool with the overload option. First, create a NAT pool using the `ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}` command. Since we want to use the overload option, we create a small NAT pool, with as little as one address, selecting an address other than the interface address.**
- `r4(config)#ip nat pool mypool 150.50.24.11 150.50.24.11 netmask 255.255.255.0`

- Identify which interfaces to treat as inside and outside for the NAT process.

```
r4(config)#int Loopback1
r4(config-if)#ip nat inside
r4(config-if)#int Serial0/0/0.2
r4(config-if)#ip nat outside
```

- Create an access-list as before as to deny, (define as non-interesting), that traffic that should not be NAT'd, and then permit, (define as interesting), all other traffic.

```
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255
192.168.5.0 0.0.0.255
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 172.16.1.0
0.0.0.255
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 10.14.14.0
0.0.0.255
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 10.15.15.0
0.0.0.255
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 10.45.45.0
0.0.0.255
r4(config)#access-list 101 deny ip 192.168.4.0 0.0.0.255 10.57.57.0
0.0.0.255
r4(config)#access-list 101 deny eigrp any any
r4(config)#access-list 101 permit ip any any
```

- Enable the NAT of the inside source IP addresses, specifying the pool with overload.

```
r4(config)#ip nat inside source list 101 pool mypool overload
```

- Test with an extended ping from R4. Run debug ip nat during the ping test.

```
R4#ping 150.50.24.4 source 192.168.4.4
Sending 5, 100-byte ICMP Echos to 150.50.24.4, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.4
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/68 ms
R4#
R4#show logg
<snip>
*Mar 18 19:09:39.431: NAT: s=192.168.4.4->150.50.24.11, d=150.50.24.4 [55]
*Mar 18 19:09:39.487: NAT: s=150.50.24.4, d=150.50.24.11->192.168.4.4 [55]
*Mar 18 19:09:39.491: NAT: s=192.168.4.4->150.50.24.11, d=150.50.24.4 [56]
*Mar 18 19:09:39.547: NAT: s=150.50.24.4, d=150.50.24.11->192.168.4.4 [56]
*Mar 18 19:09:39.547: NAT: s=192.168.4.4->150.50.24.11, d=150.50.24.4 [57]
*Mar 18 19:09:39.603: NAT: s=150.50.24.4, d=150.50.24.11->192.168.4.4 [57]
*Mar 18 19:09:39.603: NAT: s=192.168.4.4->150.50.24.11, d=150.50.24.4 [58]
*Mar 18 19:09:39.659: NAT: s=150.50.24.4, d=150.50.24.11->192.168.4.4 [58]
*Mar 18 19:09:39.659: NAT: s=192.168.4.4->150.50.24.11, d=150.50.24.4 [59]
*Mar 18 19:09:39.715: NAT: s=150.50.24.4, d=150.50.24.11->192.168.4.4 [59]
R4#
R4#sho ip nat trans
Pro Inside global      Inside local          Outside local          Outside global
icmp 150.50.24.11:9    192.168.4.4:9         150.50.24.4:9         150.50.24.4:9
R4#
```


Task 3-30

Make sure when the RFC 1918 network communicates to other RFC 1918 networks, they do not get translated.

- All access lists were created in such a way so that RFC 1918 to RFC 1918 traffic would not be translated. Test this with extended pings from R1 and R4. Run `debug ip nat` during the ping tests.

Static NAT**Task 3-31**

There is a Web server at 10.57.57.80. This Web server should be visible to the outside networks as 150.50.25.80.

- Configure a static NAT entry on R5 using the `ip nat inside source static local-ip global-ip` command. The NAT inside and outside interfaces have already been configured in an earlier step.

```
r5(config)#ip nat inside source static 10.57.57.80 150.50.25.80
```

- You can add the IP address of the Web server as a secondary address on the LAN interface, so that it can be pinged.

```
r5(config)#interface FastEthernet0/0
r5(config-if)#ip address 10.57.57.80 255.255.255.0 secondary
```

- You can test the translation with a ping from R1, R2, or R4. Run `debug ip nat` on R5 during the ping test. If you did not create the secondary address as above, the ping will fail, since the Web server host does not exist, but the debug display will show that the packets arrived at R5 and translation did occur.

```
R5#debug ip nat
*Oct 21 02:27:37.508: NAT*: s=150.50.25.2, d=150.50.25.80->10.57.57.80 [10]
*Oct 21 02:27:39.508: NAT*: s=150.50.25.2, d=150.50.25.80->10.57.57.80 [11]
*Oct 21 02:27:41.508: NAT*: s=150.50.25.2, d=150.50.25.80->10.57.57.80 [12]
*Oct 21 02:27:43.508: NAT*: s=150.50.25.2, d=150.50.25.80->10.57.57.80 [13]
*Oct 21 02:27:45.508: NAT*: s=150.50.25.2, d=150.50.25.80->10.57.57.80 [14]
R5#
R5#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 150.50.25.80:2    10.57.57.80:2    150.50.25.2:2    150.50.25.2:2
```

Task 3-32

There is a Web server at 172.16.1.80. This web server should be visible to the outside networks as 150.50.12.80.

- Configure a static NAT entry on R1 using the `ip nat inside source static local-ip global-ip` command. The NAT inside and outside interfaces have already been configured in an earlier step.

```
r1(config)#ip nat inside source static 172.16.1.80 150.50.12.80
```


- You can add the IP address of the Web server as a secondary address on the loopback interface, so that it can be pinged.

```
r1(config)#interface Loopback1
r1(config-if)#ip address 172.16.1.80 255.255.255.0 secondary
```

- You can test the translation with an extended ping from R2, R4, R5 or R7. Run debug ip nat on R1 during the ping test. If you did not create the secondary address as above, the ping will fail, since the Web server host does not exist, but the debug display will show that the packets arrived at R1 and translation did occur.

```
R1#debug ip nat
*Oct 21 02:35:48.932: %SYS-5-CONFIG_I: Configured from console by console
*Oct 21 02:36:23.296: NAT*: s=150.50.12.2, d=150.50.12.80->172.16.1.80 [16]
*Oct 21 02:36:25.296: NAT*: s=150.50.12.2, d=150.50.12.80->172.16.1.80 [17]
*Oct 21 02:36:27.296: NAT*: s=150.50.12.2, d=150.50.12.80->172.16.1.80 [18]
*Oct 21 02:36:29.296: NAT*: s=150.50.12.2, d=150.50.12.80->172.16.1.80 [19]
```

```
R1#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
icmp 150.50.12.80:3    172.16.1.80:3    150.50.12.2:3      150.50.12.2:3
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

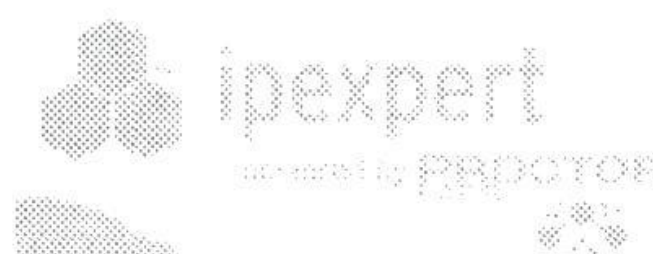
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 4: Authentication, Authorization and Accounting (AAA) on a Router

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 4 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 4-A.
- The Routers are running RIP V2 as the routing protocol.
- This lab will focus strictly on AAA. You will need to pre-configure the network with the base IP Addressing, HDLC and VLAN configuration. The pre-configuration files will be used to initially configure the router. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 4 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Configuring R7 and R8 for AAA

Task 4-1

AAA Server is located at 10.1.1.100. Configure the ACS server for a Username U1 with password cisco. Configure the ACS server for a username U2 with password cisco.

- **Select User setup, and enter the users. All that really needs to be configured for this step is username and password setup.**

209.124.41.89 - Remote Desktop

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://127.0.0.1:2052/

CISCO SYSTEMS

User Setup

Edit

User: U1 (New User)

☐ Account Disabled

Supplementary User Info

Real Name

Description Section4_User_U1

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

☐ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Default Group

Callback

Submit Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

http://127.0.0.1:2052/users/sh_edit_help_page.htm#Client_IP_Address

Internet

→ Repeat the process for user U2.

Task 4-2

Configure the ACS server to communicate with R7, using the key Tipexpert and TACACS+ as the authentication protocol. Verify that the ACS server can ping R7's loopback address.

- To configure the router as a AAA client, select **Network Configuration**, and **Add AAA Client**. Select **TACACS** as the protocol, and enter the address for R7, and the key.

CiscoSecure ACS - Microsoft Internet Explorer

Address: <http://127.0.0.1:2052/>

Network Configuration

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

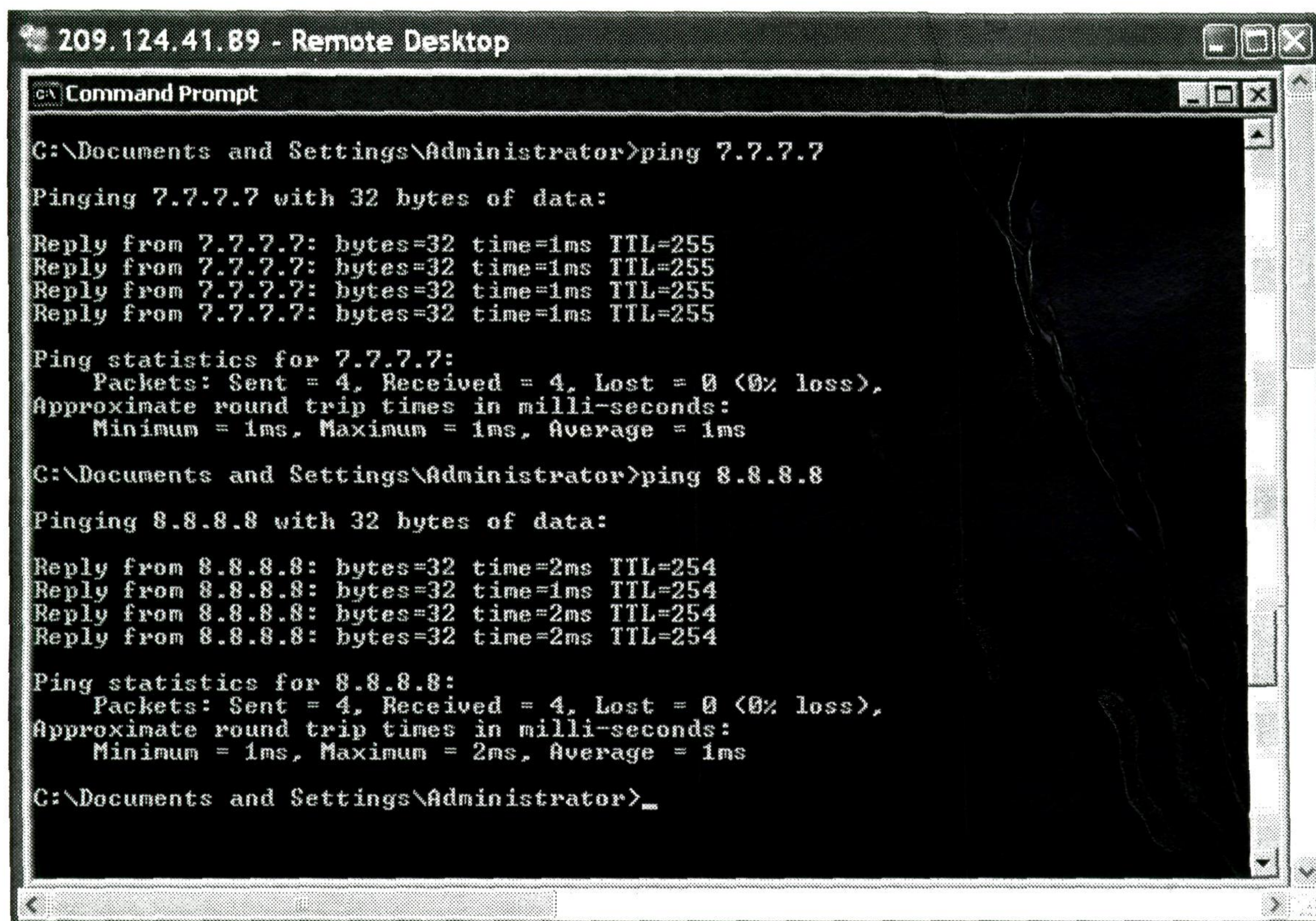
If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.1 and 192.168.13.255, enter 192.168.13.1-255 in the AAA Client IP Address box.

Applet encryptor started

Internet



```
C:\Documents and Settings\Administrator>ping 7.7.7.7

Pinging 7.7.7.7 with 32 bytes of data:

Reply from 7.7.7.7: bytes=32 time=1ms TTL=255
Reply from 7.7.7.7: bytes=32 time=1ms TTL=255
Reply from 7.7.7.7: bytes=32 time=1ms TTL=255
Reply from 7.7.7.7: bytes=32 time=1ms TTL=255

Ping statistics for 7.7.7.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=2ms TTL=254
Reply from 8.8.8.8: bytes=32 time=1ms TTL=254
Reply from 8.8.8.8: bytes=32 time=2ms TTL=254
Reply from 8.8.8.8: bytes=32 time=2ms TTL=254

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

→ Verify connectivity to the router loopbacks by pinging R7 and R8 from the ACS server.

Task 4-3

Configure the ACS server to communicate with R8, using the key Ripexpert and RADIUS as the authentication protocol. Verify that the ACS server can ping R8's loopback address.

→ The setup for R8 is similar, except that the protocol used is RADIUS.

209.124.41.89 - Remote Desktop

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://127.0.0.1:2052/

CISCO SYSTEMS

Network Configuration

Edit Help

Add AAA Client

AAA Client Hostname: R8

AAA Client IP Address: 8.8.8.8

Key: Ripexpert

Authenticate Using: RADIUS (IETF)

☐ Single Connect TACACS+ AAA Client (Record statistics on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this Client

Submit Submit + Apply Cancel

? Back to Help

Applet startStop started

Internet

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

[Back to Top](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

Task 4-4

Configure R7 to communicate to the AAA Server. The AAA Server is configured to communicate to R7 using its Loopback 0 address of 7.7.7.7. The Secret key is **Tipexpert**. Use TACACS+ as the Protocol.

- To enable the authentication, authorization, and accounting (AAA) access control model, issue the `aaa new-model` command on each router.

```
R7(config)#aaa new-model
```

- To specify a TACACS+ AAA server host, use the `tacacs-server host` command in global configuration mode.
- To set the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ server, use the `tacacs-server key` command in global configuration mode. The key entered must match the key used on the TACACS+ server.
- To use the IP address of a specified interface for all outgoing TACACS+ packets, use the `ip tacacs source-interface` command in global configuration mode.
- Configure the TACACS+ server as specified.

```
R7(config)#tacacs-server host 10.1.1.100
R7(config)#tacacs-server key Tipexpert
R7(config)#ip tacacs source-interface Loopback0
```

Task 4-5

Verify connectivity by testing Users U1 with a password of cisco.

- Test the TACACS+ server connectivity using the `test aaa group tacacs username password` command. This command allows you to run a quick test of the connectivity between the router and the AAA server, by sending a test TACACS+ record to the server.

```
R7#test aaa group tacacs+ U1 cisco legacy
```

```
Attempting authentication test to server-group tacacs+ using tacacs
User was successfully authenticated.
```

Task 4-6

Configure R8 to communicate to the AAA Server. The AAA Server is configured to communicate to R8 using its Loopback 0 address of 8.8.8.8. The Secret key is **Ripexpert**. Use RADIUS as the protocol.

- To specify a RADIUS AAA server host, use the `radius-server host` command in global configuration mode.
- To set the authentication encryption key used for all RADIUS communications between the router and the RADIUS server, use the `radius-server key` command in global configuration mode. The key entered must match the key used on the RADIUS server.

- To use the IP address of a specified interface for all outgoing RADIUS packets, use the `ip radius source-interface` command in global configuration mode.
- Configure the radius server as specified.

```
R8(config)#radius-server host 10.1.1.100
R8(config)#radius-server key Ripexpert
R8(config)#ip radius source-interface Loopback0
```

Task 4-7

Verify connectivity by testing Users U1 with a password of **cisco**.

- Test the RADIUS server connectivity using the `test aaa group username password new-code` command. This command allows you to run a quick test of the connectivity between the router and the AAA server, by sending a test RADIUS record to the server. This command was introduced in 12.2(4)T.

```
R8#test aaa group radius U1 cisco legacy
```

```
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

Configuring Login Authentication for Telnet, Console and Aux ports

Task 4-8

Configure R7 such that the AUX and Console ports are not authenticated. Make sure of it.

- For AAA authentication, you first must create named lists of authentication methods, and then apply a list to one or more line interfaces. Method lists define the types of authentication to be performed and the sequence in which they will be performed.
- To create an authentication method list, use the `aaa authentication login {default | list-name} method1 [method2...]` command. Specify either 'default' or a list-name to be referenced on the command applying the authentication to a line interface.
- The method specified can be one or more of the following authentication methods. If more than one are specified, the additional methods are used only if the previous method receives an error, not if it simply fails authentication.

enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.

none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group group-name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

- To apply a method list to a line, use the `login authentication {default | list-name}` command in line configuration mode.
- Following is a configuration example that sets the aux and console ports to no authentication.

```
R7(config)#aaa authentication login no-authen none
R7(config)#line con 0
R7(config-line)#login authentication no-authen
R7(config-line)#line aux 0
R7(config-line)#login authentication no-authen
```

- Test the access to the console port by logging out, and then by logging back in. It is generally best practice to first start another inbound session, such as a telnet session, before you log out, so that in the event your changes were not correct, you could remove those changes without inadvertently locking out your access. Otherwise, you would need to reboot the router, assuming that you did not save the changes before logging out.

Task 4-9

Configure R7 such that the Telnet connections are authenticated against the AAA server using TACACS+. Do not use the default list. Provide for a way to authenticate the user locally if the AAA server is unavailable.

- Create an authentication method list, specifying a list-name to be referenced on the command that will apply the authentication to the vty lines.
- For the first method, choose `group tacacs+`, and for the second method, specify `local`. The login authentication will first try the TACACS+ server, and if it receives an error message, then it will try the local database.
- Following is a configuration example that sets the telnet lines to use TACACS+ for authentication, with the local database as a backup.

```
R7(config)#aaa authentication login taclist group tacacs+ local
R7(config)#line vty 0 15
R7(config-line)#login authentication taclist
```


Task 4-10

Create a User for backup authentication as admin with a password of admin.

- In order for the backup authentication to succeed, you will need to create a username in the local database of the router, using the `username name password password` command.

```
R7(config)#username admin password admin
```

- Verify your changes by telnetting from R8 into R7, and use the TACACS+ username U1 and password cisco.

```
R8#telnet 150.50.78.7
Trying 150.50.78.7 ... Open
```

```
User Access Verification
```

```
Username: U1
Password:
```

```
R7>exit
```

```
[Connection to 150.50.78.7 closed by foreign host]
R8#
```

- Shutdown interface e0/0 on R7, (the interface to the ACS server), and attempt the telnet again. You should find that username U1 fails, but you will be able to log in with username admin, password admin.

```
R8#telnet 150.50.78.7
Trying 150.50.78.7 ... Open
Username: U1
Password:
```

```
% Authentication failed.
```

```
Username: admin
Password:
```

```
R7>exit
```

```
[Connection to 150.50.78.7 closed by foreign host]
R8#
```

Task 4-11

Configure R8 such that the AUX and Console ports are not authenticated. Make sure of it.

- Perform the same steps as in Task 4-6, this time on R8.

```
R8(config)#aaa authentic login noauth none
R8(config)#line con 0
R8(config-line)#login authentic noauth
R8(config-line)#line aux 0
R8(config-line)#login authentic noauth
```


Task 4-12

Configure R8 such that the Telnet connections are authenticated against the AAA server using RADIUS. Do not use the default list. Provide for a way to authenticate the user locally if the AAA server is unavailable.

- Create an authentication method list, specifying a list-name to be referenced on the command that will apply the authentication to the vty lines.
- For the first method, choose group radius, and for the second method, specify local. The login authentication will first try the RADIUS server, and if it receives an error message, then it will try the local database.
- Following is a configuration example that sets the telnet lines to use TACACS+ for authentication, with the local database as a backup.

```
R8(config)#aaa authentication login radlist group radius local
R8(config)#line vty 0 15
R8(config-line)#login authentication radlist
```

Task 4-13

Create a User for backup authentication as admin with a password of admin.

- Perform the same step as in Task 4-8, this time on R8. Verify the RADIUS authentication and local database authentication in the same manner as in Task 4-8.

```
R8(config)#username cisco password cisco
```

Configuring Local Authorization on R7

Task 4-14

Allow User **User1** access to all commands.

- By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15).
- Define User1 in the local database, and assign a privilege level of 15, using the `username name privilege privilege-level password password` command.

```
R7(config)#username User1 privilege 15 password cisco
```

Task 4-15

Allow User **User2** access to a user-defined privilege 5. Privilege 5 should have the following capabilities:

- It should allow users to be able to go into Global Config Mode.
- It should allow users to be able to configure a hostname
- It should allow users to be able to configure a routing and advertise networks.
- It should allow users to be able to configure all snmp related commands in global config mode.

- A new privilege level will need to be created, with the capabilities listed above. Use the `privilege` command to create privilege level 5.

- To allow a user to enter Global Config mode, configure the following privilege:

```
R7(config)#privilege exec level 5 configure terminal
```

- To allow a user configure a hostname, configure the following privilege:

```
R7(config)#privilege configure level 5 hostname
```

- To allow a user configure a routing protocol and advertise networks, configure the following privilege:

```
R7(config)#privilege configure level 5 router
R7(config)#privilege router all level 5 network
```

- To allow a user to configure all snmp related commands, configure the following privilege:

```
R7(config)#privilege configure all level 5 snmp
R7(config)#privilege configure all level 5 snmp-server
```

- Define User2 in the local database, and assign a privilege level of 5.

```
R7(config)#username User2 privilege 5 password cisco
```

Task 4-16

Authorization should only be done on the Telnet Connections. Make sure of it.

- AAA authorization enables you to limit the services available to a user. You first must create named lists of authorization methods, and then apply a list to one or more line interfaces. Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed.
- To create an authorization method list, use the `aaa authorization {auth-proxy | network | exec | commands level | reverse-access | configuration | ipmobile} {default | list-name} [method1 [method2...]]` command. Specify either 'default' or a list-name to be referenced on the command applying the authentication to a line interface.
- The method specified can be one or more of the following authorization methods. If more than one are specified, the additional methods are used only if the previous method receives no response.

group group-name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the <code>aaa group server radius</code> or <code>aaa group server tacacs+</code> command.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
krb5-instance	Uses the instance defined by the <code>kerberos instance map</code> command.
local	Uses the local database for authorization.
none	No authorization is performed.

- To perform authorization for users to run an EXEC shell, use the 'exec' argument on the `aaa authorization` command. The following example creates a list named `lauthor` that will check the local user database, and a list named `no-author` that will not require authorization.

```
R7(config)#aaa authorization exec lauthor local
R7(config)#aaa authorization exec no-author none
```

- To perform authorization for users to enter commands at a certain privilege level, use the 'commands level' argument on the `aaa authorization` command. The following example creates a list named `lauthor` that will check the local user database for privilege levels 1, 5 and 15, and a list named `no-author` that will not require authorization for privilege levels 1, 5 and 15.
- Use the `authorization exec {default | list-name}` command in line configuration mode to determine if the user is allowed to run an EXEC shell on the selected lines.

```
R7(config)#line vty 0 15
R7(config-line)#authorization exec lauthor
```

- Use the `authorization command level {default | list-name}` command in line configuration mode to allow the user to enter all commands at the specified privilege level on the selected lines.

```
R7(config)#line vty 0 15
R7(config-line)#authorization commands 1 lauthor
R7(config-line)#authorization commands 5 lauthor
R7(config-line)#authorization commands 15 lauthor
```

- Following is a configuration example that sets the aux and console ports to no authorization. (AAA authorization is disabled on the console port by default. For this example, we have enabled authorization on the console, and then set the method to no authorization, to show how it can be done).

```
R7(config)#line con 0
R7(config-line)#authorization exec no-author
R7(config-line)#authorization commands 1 no-author
R7(config-line)#authorization commands 5 no-author
R7(config-line)#authorization commands 15 no-author
R7(config-line)#exit
R7(config)#aaa authorization console
R7(config-line)#line aux 0
R7(config-line)#authorization exec no-author
R7(config-line)#authorization commands 1 no-author
R7(config-line)#authorization commands 5 no-author
R7(config-line)#authorization commands 15 no-author
```


Task 4-17

The password for both users is **cisco**.

- The passwords were entered with the **username** command in Tasks 4-14 and 4-15.
- Verify that authorization is not performed on the console port. Log out and log back in. You should be able to enter configuration mode, and enter any configuration command.
- Verify that the telnet authorization is working . Telnet into R7 from R8. Log in as User1, and display your privilege level. Then log out, and log back in as User2. Display your privilege level, and then attempt some allowed commands, and some commands that are not allowed, for that privilege level.

```
R8#telnet 150.50.78.7
Trying 150.50.78.7 ... Open
```

```
Username: User1
Password:
```

```
R7#show privilege
Current privilege level is 15
R7#exit
```

[Connection to 150.50.78.7 closed by foreign host]

```
R8#telnet 150.50.78.7
Trying 150.50.78.7 ... Open
```

```
Username: User2
Password:
```

```
R7#show privilege
Current privilege level is 5
R7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R7(config)#hostname r7
r7(config)#router rip
r7(config-router)#exit
r7(config)#snmp-server host 1.1.1.1 string
r7(config)#
r7(config)#interface e0/0
^
```

% Invalid input detected at '^' marker. ← Note that you cannot get into interface config mode.

```
r7(config)#access-list 1 permit 150.50.0.0 0.0.255.255
^
```

```
% Invalid input detected at '^' marker.
r7(config)#^Z
r7#exit
```

[Connection to 150.50.78.7 closed by foreign host]
R8#

- **Note:** If you still have the AAA authentication configured from the earlier steps, it has the potential to cause problems here. If the AAA server is not available, and the local authentication is used, everything works fine. When the AAA server is available, however, you will run into a conflict. If you use the users defined on the AAA server,

you will receive an error when logging in for an authorization failure. If you use the users defined locally, authentication will fail because those users are not configured on the AAA server. You can easily add user1 and user2 to the AAA server, and add the users U1 and U2 locally. Authentication and authorization do NOT have to be done in the same location. The router can authenticate user and password off of the AAA server, and use the local information for that username to determine access rights for authorization.

Accounting

Task 4-18

On R7, Log all logins and logout to track usage for Telnet connections only.

- Like authentication and authorization method lists, method lists for accounting define the way accounting will be performed and the sequence in which these methods are performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for accounting services.

- To create an accounting method list, use the `aaa accounting {auth-proxy | system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [broadcast] group groupname` command. Specify either 'default' or a list-name to be referenced on the command applying the accounting to a line interface.

- AAA supports the following accounting types:

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests.
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the <code>autocommand</code> command.
connection	Provides information about all outbound connections made from the network access server.
commands level	Runs accounting for all commands at the specified.

- You must also specify the accounting record type; select either `start-stop`, `stop-only`, or `none`. For minimal accounting, use the `stop-only` keyword, which instructs the specified method, (RADIUS or TACACS+), to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the `start-stop` keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the `none` keyword.
- To apply a method list to a line, use the `accounting` command in line configuration mode.

- Following is a configuration example that sends accounting records for all login and logouts for Telnet sessions only..

```
R7(config)#aaa accounting exec taclist start-stop group tacacs+
R7(config)#line vty 0 15
R7(config-line)#accounting exec taclist
```

Task 4-19

On R7, Log all commands typed by users when on the router through Telnet only.

- You will need to enter an accounting method list for each command privilege level configured on the router. Privilege levels 0,1, and 15 are default, and in a previous task, you had configured privilege level 5. So, you will need 4 accounting method lists, one for each command level.
- Following is a configuration example that sends accounting records for commands typed by users for Telnet sessions only..

```
R7(config)#aaa accounting commands 0 taclist start-stop group tacacs+
R7(config)#aaa accounting commands 1 taclist start-stop group tacacs+
R7(config)#aaa accounting commands 5 taclist start-stop group tacacs+
R7(config)#aaa accounting commands 15 taclist start-stop group tacacs+
R7(config)#line vty 0 15
R7(config-line)#accounting commands 0 taclist
R7(config-line)#accounting commands 1 taclist
R7(config-line)#accounting commands 5 taclist
R7(config-line)#accounting commands 15 taclist
```

Task 4-20

On R8, Log all logins and logout to track usage for Telnet connection only.

- Enter the same commands as in Task 4-18, but remember to specify group radius for R8.
- Following is a configuration example that sends accounting records for all login and logouts for Telnet sessions only..

```
R8(config)#aaa accounting exec radlist start-stop group radius
R8(config)#line vty 0 15
R8(config-line)#accounting exec radlist
```


Task 4-21

Verify the logging on the ACS Server.

- For RADIUS, select RADIUS Accounting under the Reports and Activity tab. For TACACS, select TACACS+ Accounting for the login information, and TACACS+ Administration for the command logging.

The screenshot shows the CiscoSecure ACS web interface in Microsoft Internet Explorer. The browser address bar shows <http://127.0.0.1:2052/>. The page title is "CiscoSecure ACS - Microsoft Internet Explorer". The main content area is titled "Reports and Activity". On the left, there is a sidebar with various configuration and monitoring options. The main content area is divided into two sections: "Select" and "Reports".

The "Select" section shows "RADIUS Accounting active.csv" with "Refresh" and "Download" buttons. Below this, there are input fields for "Regular Expression", "Start Date & Time", and "End Date & Time". The "Start Date & Time" field contains "mm/dd/yyyy, hh:mm:ss". The "End Date & Time" field contains "mm/dd/yyyy, hh:mm:ss". There are "Apply Filter" and "Clear Filter" buttons. Below these, it says "Filtering is not applied."

The "Reports" section displays a table of session data. The table has the following columns: Date, Time, User-Name, Group-Name, Calling-Station-Id, Acct-Status-Type, Acct-Session-Id, Acct-Session-Time, Service-Type, Framed-Protocol, and Acct-Input-Octet. The table contains one row of data:

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octet
01/24/2007	01:29:16	User1	Default Group	8.8.8.8	Start	00000001	...	NAS Prompt

At the bottom of the sidebar, there is a "Back to Help" button.

209.124.41.89 - Remote Desktop
CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://127.0.0.1:2052/ Go Links

Cisco Systems Reports and Activity

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

Network Access Profiles

Reports and Activity

Online Documentation

Select Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Administration Audit
- User Password Changes
- ACS Service Monitoring

Back to Help

Select

TACACS+ Accounting active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time

mm/dd/yyyy, hh:mm:ss mm/dd/yyyy, hh:mm:ss

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed time	service	bytes in	bytes out
01/24/2007	01:33:07	user1	Default Group	150.50.78.8	stop	21	shell
01/24/2007	01:32:46	user1	Default Group	150.50.78.8	start	..	shell

209.124.41.89 - Remote Desktop

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://127.0.0.1:2052/

Reports and Activity

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Porting Validation

Network Access Profiles

Reports and Activity

Online Documentation

Select Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Administration Audit
- User Password Changes
- ACS Service Monitoring

[Back to Help](#)

Select

Tacacs+ Administration active.csv [Refresh](#) [Download](#)

Regular Expression Start Date & Time End Date & Time

Filtering is not applied.

Date	Time	User-Name	Group-Name	cmd	priv-lev	service	NAS-Portname	task id	NAS-IP-Address	reason
01/24/2007	01:33:07	user1	Default Group	exit	0	shell	tty322	16	7.7.7.7	..
01/24/2007	01:32:49	user1	Default Group	show running-config	15	shell	tty322	15	7.7.7.7	..

Task 4-22

Configure a backup of the ACS database.

- For ACS, backup the system under System Configuration, ACS Backup. Select 'Backup Now' at the bottom of the page.

System Configuration

ACS System Backup Setup

ACS Backup Scheduling

☒ Manual
☐ Every 60 minutes
☐ At specific times

	00:00	06:00	12:00	18:00	24:00
Mon					
Tue					
Wed					
Thu					
Fri					
Sat					
Sun					

Backup Location

Directory
 C:\Program Files\CiscoSecure ACS v4.0\CSA

☐ Manage Directory

☐ Keep only the last 7 files
☒ Delete files older than 7 days

Help

- [ACS Backup Scheduling](#)
- [Backup Location](#)
- [Backup Now](#)

ACS System Backup Setup

This page enables you to set the parameters for backing up your user and group databases and your ACS system configuration information.

[\[Back to Top\]](#)

ACS Backup Scheduling

Set the time-of-day and day-of-week during which backup is to take place.

- **Manual.** Do not backup automatically.
- **Every X Minutes.** The frequency between backups. The default is 60 minutes. If this value is set too high, backup might be incomplete. Because ACS momentarily shuts down during backup, if this value is set too low, backup might interfere with users' ability to authenticate.
- **At specific times.** At user-definable times during the week. This option enables the administrator to define when backup will take place. The minimum is one hour, and backup takes place on the hour selected. In the day and hour graph, click the times at which you want backup performed or prevented. Times during which backup will occur are highlighted in green. Click **Set All** to select all hours of every day. Click **Clear All** to clear all hours.

[\[Back to Top\]](#)

Backup Location

This section enables you to configure the parameters for the ACS system backup files.

Directory

Type the name of the directory in which to place the backup files.

Manage Directory

To configure parameters for the directory for the backup files, select the **Manage Directory** check box and click one of the following options.

- **Keep only the last X files.** Click this option and type the maximum number of backup files to keep in the backup directory. The default is 7 files.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 5: PIX Firewall

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.

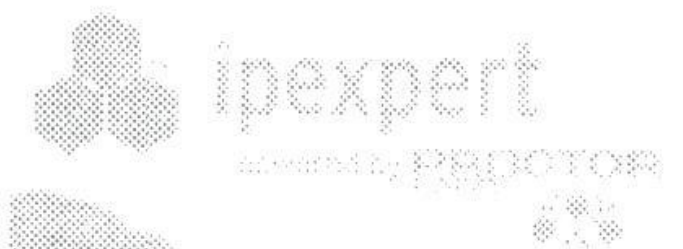
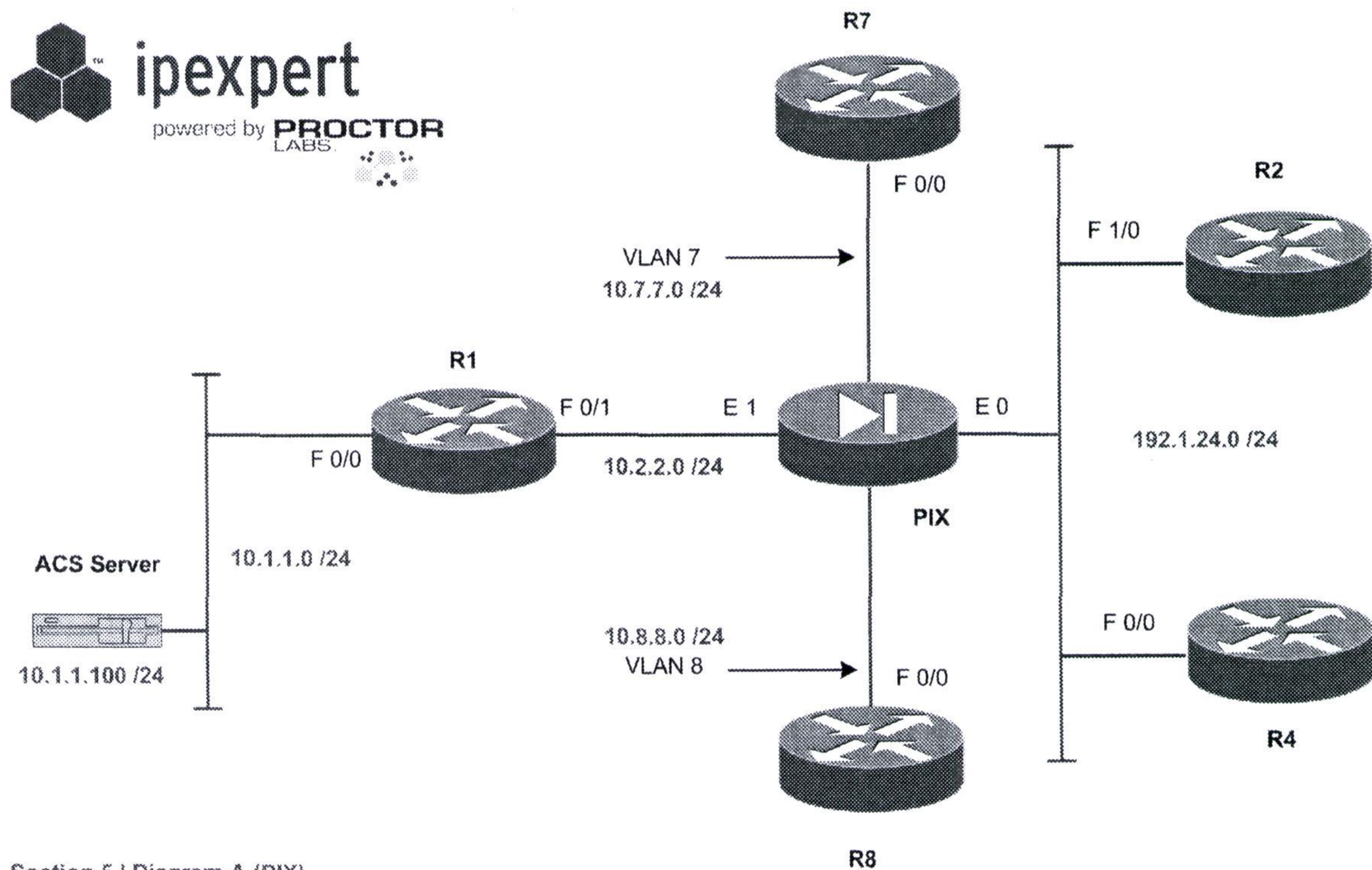


Diagram 5-A



Section 5 | Diagram A (PIX)

Section 5 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 5-A.
- This lab will focus strictly on PIX you will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 5 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Section 5 Configuration Tasks

Basic PIX Configuration

Task 5-1

Create 2 subinterfaces off of E0, 0.7 and 0.8. VLAN24 is the primary untagged VLAN.

Task 5-2

Assign them names and security levels as follows:

- Eth0.7 – DMZ7 - 25
- Eth0.8 – DMZ8 – 50

- Each interface has a unique name and security level that you can change using the `nameif` command.

- Security levels let you control access between systems on different interfaces and the way you enable or restrict access depends on the relative security level of the interfaces:
 - To enable access to a higher security level interface from a lower-level interface, use the `static` and `access-list` commands
 - To enable access to a lower-level interface from a higher-level interface, use the `nat` and `global` commands if NAT-control is enabled. If NAT-control is not enabled, NAT statements are not required to pass traffic.

```
pixfirewall(config)#int eth0.7
pixfirewall(config-subif)#vlan 7
pixfirewall(config-subif)#nameif DMZ7
pixfirewall(config-subif)#security 25
pixfirewall(config)#int eth0.8
pixfirewall(config-subif)#vlan 8
pixfirewall(config-subif)#security 50
pixfirewall(config-subif)#nameif DMZ8
pixfirewall(config)#hostname PIX
PIX(config)#int eth0
PIX(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
PIX(config-if)#int eth1
PIX(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
```

Task 5-3

Also configure the PIX outside port on the switch to allow VLAN7 and VLAN8 to communicate to the rest of the network.

- As long as the VLANs are active on the switch, and the port is configured as a trunk, there is nothing to configure for this step.

Task 5-4

Assign the following addresses to the PIX and bring all PIX interfaces up:

- Inside – 10.2.2.10/24
- Outside – 192.1.24.10/24
- DMZ7 – 10.7.7.10/24
- DMZ8 – 10.8.8.10/24

```
PIX(config)#int eth0
PIX(config-if)#ip address 192.1.24.10 255.255.255.0
PIX(config-if)#int eth1
PIX(config-if)#ip address 10.2.2.10 255.255.255.0
PIX(config-if)#int eth0.7
PIX(config-subif)#ip address 10.7.7.10 255.255.255.0
PIX(config-subif)#int eth0.8
PIX(config-subif)#ip address 10.8.8.10 255.255.255.0
```

```
PIX(config)#int eth0
PIX(config-if)#no shut
PIX(config-if)#int eth1
PIX(config-if)#no shut
```

- If you don't enable the physical interfaces with "no shut", the subinterfaces will not come up.

Task 5-5

Verify connectivity by pinging the directly connected devices around the PIX.

```
PIX(config)#ping 10.7.7.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PIX(config)#ping 10.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
PIX(config)#ping 192.1.24.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.24.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PIX(config)#ping 192.1.24.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.24.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
PIX(config)#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
PIX(config)#
```


Translations and Connections

Task 5-6

Configure the PIX for NAT-Control. Use a NAT/PAT combination to allow inside networks to outside using the following range of address:

→ 192.1.24.51 – 192.1.24.150

- Inside networks are generally configured with a higher security level than outside networks or DMZ networks. The default security level for the inside network is 100. To enable access to a lower-level interface from a higher-level interface, use the `nat` and `global` commands.
- Here, you will use Inside Dynamic NAT, which translates addresses on a secure interface to a range of addresses on a less secure interface in a one-to-one mapping between the internal and external addresses.
- The task also specifies that you use Inside Dynamic PAT, which translates multiple addresses to a single address on the lower security interface in a many-to-one mapping between the internal addresses and the single external address. The purpose for using a NAT/PAT combination is so that the NAT range does not limit the translations to 100 one-to-one mappings. NAT should be configured for the first 99 external addresses in the range, and PAT for the final external address.
- Use the `global` command to create the pool of addresses to be used on the lower security interface. The "2" after the interface specifier is the NAT ID, which will be specified also on the corresponding `nat` command. Specify the range 192.1.24.51-192.1.24.149 for the NAT pool, and 192.1.24.150 for the PAT address.
- To let all inside users start connections, use the `nat (inside) 2 0 0` command. The "0 0" after the NAT ID is the network/mask identifier, with 0 0 specifying any address.
- Following is an example configuration for configuring a NAT/PAT combination:

```
PIX(config)#nat (inside) 2 0 0 0 0
PIX(config)#global (outside) 2 192.1.24.51-192.1.24.149
PIX(config)#global (outside) 2 192.1.24.150
INFO: Global 192.1.24.150 will be Port Address Translated
```

- Nat Control will cause the PIX to use the NAT behavior seen in earlier PIX versions, where a translation was required for the PIX to pass traffic.

```
PIX(config)#nat-control
```

Task 5-7

If more than 99 simultaneous connections are received, the PIX uses PAT to translate. Do not use NAT-ID 1

- The previous task accomplished this, given that the requirement was to use a NAT/PAT combination.

Task 5-8

R2 should be able to Manage R7 using Telnet. R2 should see R7 as 192.1.24.7. Allow the appropriate filtering on the PIX. Do not use conduits.

- Access from R2 to R7 requires you to enable access from a lower security level interface, (outside), to a higher-level interface, (VLAN 7). To enable this, use the `static` and `access-list` commands.
- Static NAT addressing creates a permanent one-to-one mapping of an internal address to an external address. You will use the `static` command to map the internal address of R7 to the specified external address of 192.1.24.7.
- You also must use the `access-list` command to allow access from the external interface to the higher security level interface. The access-list should allow only Telnet inbound to the Static NAT address from R2.
- The access-list will need to be applied to the external interface using the `access-group` command.
- Following is an example configuration for configuring the access to R7:

```
PIX(config)#static (DMZ7,outside) tcp 192.1.24.7 telnet 10.7.7.7
telnet netmask 255.255.255.255 0 0
PIX(config)#access-list infilter permit tcp host 192.1.24.2 gt 1024
host 192.1.24.7 eq telnet
PIX(config)#access-group infilter in interface outside
```

- R7 will need to be configured to accept telnet connections. This is done by configuring a login password for the vty lines on R7.

```
R7(config)#line vty 0 15
R7(config-line)#password ipexpert
```

- Verify your configuration by telnetting from R2 to R7 at 192.1.24.2:

```
R2#telnet 192.1.24.7
Trying 192.1.24.7 ... Open

User Access Verification

Password:
R7>quit

[Connection to 192.1.24.7 closed by foreign host]
R2#
```

Task 5-9

R4 should be able to Manage R8 using Telnet. R4 should see R8 as 192.1.24.8. Allow the appropriate filtering on the PIX. Do not use conduits.

- The same set of commands as in Task 5-8 must be configured to allow access from R4 on the external interface to R8 on a higher security level interface.

- Only one access-list can be applied to an interface, so the previously created access-list, “infilter”, can be added to by simply entering another access control entry.
- The access-group command does not need to be entered, as it is already applied to the outside interface.
- Following is an example configuration for configuring the access to R8:

```
PIX(config)#static (DMZ8,outside) tcp 192.1.24.8 telnet 10.8.8.8
telnet netmask 255.255.255.255 0 0
PIX(config)#access-list infilter permit tcp host 192.1.24.4 host
192.1.24.8 eq telnet
```

- R8 will need to be configured to accept telnet connections. This is done by configuring a login password for the vty lines on R8.

```
R8(config)#line vty 0 15
R8(config-line)#password ipexpert
```

- Verify your configuration by telnetting from R4 to R8 at 192.1.24.8:

```
R4#telnet 192.1.24.8
Trying 192.1.24.8 ... Open

User Access Verification

Password:
R8>quit

[Connection to 192.1.24.8 closed by foreign host]
R4#
```

Task 5-10

If an outside user Telnets or HTTPs to 192.1.24.10, he should be redirected to a server at 10.7.7.100. This server is not there. But your company will be putting this server up in the future. Allow the appropriate entries in your filter list.

- You again will use the static command to map the internal address of the server to the specified external address of 192.1.24.10. Since the address of the new server is from the VLAN 7 subnet, the static command will specify the DMZ7 interface as the inside interface.
- Because the redirection requirement is for Telnet and HTTPs access only, you will need to specify those ports on the static command.
- Configure additional access control entries to the existing access-list, “infilter”.
- Following is an example configuration for configuring the access to the new server:

```
PIX(config)#static (DMZ7,outside) tcp 192.1.24.10 telnet 10.7.7.100
telnet netmask 255.255.255.255 0 0
PIX(config)#static (DMZ7,outside) tcp 192.1.24.10 https 10.7.7.100
https netmask 255.255.255.255 0 0
```



```
PIX(config)#access-list infilter permit tcp any host 192.1.24.10 eq
telnet
PIX(config)#access-list infilter permit tcp any host 192.1.24.10 eq
https
```

Task 5-11

R7 should be able to ping R2 and R4's Loopback addresses using its own IP Address 10.7.7.7. You cannot use the static command to accomplish this. Allow the appropriate entries in the access list. You are allowed to create a single route on both R2 and R4. You may also create a single route on the PIX

- Access for this task will be from a higher security level interface to a lower-level interface, therefore the `nat` and `global` commands are necessary.
- In order to use R7's IP address to ping the external routers, you will need to disable NAT for the pings. One method is to use a NAT ID of 0 to specify that NAT translation will be disabled. Because you only want to disable NAT specifically for pings from R7 to the loopback addresses of R2 and R4, you will need to create an access-list for these source/destination addresses, and specify the access-list on the NAT 0 command.

- Following is an example configuration for the NAT 0 requirement:

```
PIX(config)#access-list nonat permit ip host 10.7.7.7 host 2.2.2.2
PIX(config)#access-list nonat permit ip host 10.7.7.7 host 4.4.4.4
PIX(config)#nat (DMZ7) 0 access-list nonat
```

- Configure additional access control entries to the existing access-list, "infilter".

```
PIX(config)#access-list infilter permit icmp host 2.2.2.2 host
10.7.7.7 echo-reply
PIX(config)#access-list infilter permit icmp host 4.4.4.4 host
10.7.7.7 echo-reply
```

- The PIX does not know the routes to the loopback addresses of R2 and R4. You must enter a default route, specifying the outside interface of the PIX as the gateway address. If the route command statement uses the IP address from one interface of the PIX as the gateway IP address, the PIX will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address. Any Cisco router on the outside interface LAN which has a route to address X, (Cisco IOS software has proxy ARP enabled by default), replies back to the PIX with its own MAC address as the next hop.

```
PIX(config)#route outside 0 0 192.1.24.10
```

- In order for R2 and R4 to respond to the ping request from R7, each router will need a route to the internal address for R7, 10.7.7.7. Configure a static route on R2 and R4 to point to the PIX as the route to 10.7.7.7:

```
R2(config)#ip route 10.7.7.7 255.255.255.255 192.1.24.10
```

```
R4(config)#ip route 10.7.7.7 255.255.255.255 192.1.24.10
```


- **Test the ping from R7 to R2 and R4's Loopback addresses. In order to verify that R7's address was not NAT'd, run an ICMP debug on the target router before starting the ping:**

```
R7#ping 2.2.2.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:  
!!!!
```

```
R2#debug ip icmp
```

```
*Nov 17 02:10:11.775: ICMP: echo reply sent, src 2.2.2.2, dst 10.7.7.7  
*Nov 17 02:10:11.779: ICMP: echo reply sent, src 2.2.2.2, dst 10.7.7.7  
*Nov 17 02:10:11.783: ICMP: echo reply sent, src 2.2.2.2, dst 10.7.7.7  
*Nov 17 02:10:11.791: ICMP: echo reply sent, src 2.2.2.2, dst 10.7.7.7  
*Nov 17 02:10:11.795: ICMP: echo reply sent, src 2.2.2.2, dst 10.7.7.7
```

Access List and Object Groups on the PIX

Task 5-12

Your company will be putting in 2 application servers. One of the application servers will be in DMZ7 with an IP Address of 10.7.7.21, and the other will be in DMZ8 with an IP Address of 10.8.8.22.

- **Object grouping provides a way to reduce the number of access rules required to describe complex security policies by grouping objects of a similar type so that a single access rule can apply to all the objects in the group.**
- **Object Groups can be created for the following types:**
- **protocol**—Group of IP protocols. It can be one of the keywords `icmp`, `ip`, `tcp`, or `udp`, or an integer in the range 1 to 254 representing an IP protocol number.
 - **service**—Group of TCP or UDP port numbers assigned to different services.
 - **icmp-type**—Group of ICMP message types to which you permit or deny access.
 - **network**—Group of hosts or subnets
- **Because the access rule for each of these servers is similar, you can group them into a Network Object Group. Be sure to use the external global addresses for the host addresses.**
- **Following is an example configuration for the Network Object Group:**

```
PIX(config)#object-group network pn-servers  
PIX(config-network)#network-object host 192.1.24.21  
PIX(config-network)#network-object host 192.1.24.22
```


Task 5-13

Create a static translation for them on the outside so that 10.7.7.21 is seen as 192.1.24.21 on the outside and 10.8.8.22 is seen as 192.1.24.22 on the outside.

→ **Following is an the configuration for the static translations:**

```
PIX(config)#static (DMZ7,outside) 192.1.24.21 10.7.7.21 netmask
255.255.255.255 0 0
PIX(config)#static (DMZ8,outside) 192.1.24.22 10.8.8.22 netmask
255.255.255.255 0 0
```

Task 5-14

These servers are going to be access by partner organizations. The IP Addresses of these partner organizations are as follows:

- 205.15.25.0/24
- 207.215.1.0/24
- 210.208.15.16/28
- 211.0.15.32/27
- 192.1.150.112/28

→ **Create a Network Object Group for these network addresses:**

```
PIX(config)#object-group network pn-networks
PIX(config-network)#network-object 205.15.25.0 255.255.255.0
PIX(config-network)#network-object 207.215.1.0 255.255.255.0
PIX(config-network)#network-object 210.208.15.16 255.255.255.240
PIX(config-network)#network-object 211.0.15.32 255.255.255.224
PIX(config-network)#network-object 192.1.150.112 255.255.255.240
```

Task 5-15

The applications on the servers are as follows:

- TFTP
- FTP
- HTTP
- SMTP
- DNS
- Custom Application at UDP 50000

→ **Create a Service Object Group for the specified services. You will need to create a group for the TCP services and a group for the UDP services.**

```
PIX(config)#object-group service pn-tcp tcp
PIX(config-service)#port-object eq ftp
PIX(config-service)#port-object eq www
PIX(config-service)#port-object eq smtp
PIX(config-service)#port-object eq domain
PIX(config-service)#exit
```



```
PIX(config)#object-group service pn-udp udp
PIX(config-service)#port-object eq tftp
PIX(config-service)#port-object eq domain
PIX(config-service)#port-object eq 50000
```

Task 5-16

Allow all the partner organizations access to all the applications on the 2 servers. You are allowed 2 lines in the Access List to accomplish this.

- Because you have created Object Groupings, the required Access Control Entries need only reference the Object Group names, and not the individual hosts and services, which would require several entries.
- Replace the parameters of the `access-list` commands with the corresponding object group:
 - Replace the protocol parameter with a protocol object group.
 - Replace local and remote IP addresses and subnet masks with a network object group.
 - Replace the port parameter with a service object group.
 - Replace the icmp-type parameter with an icmp-type object group.
- Use the `object-group` keyword in the `access-list` command to specify that access list search is performed on object groups that are contained in the access list instead of searching the entire expanded access list.
- You will need two Access Control entries, one for the TCP service group, and one for the UDP service group.
- Following is an example configuration for the Access List entries:

```
PIX(config)#access-list infilter permit tcp object-group pn-networks
object-group pn-servers object-group pn-tcp
PIX(config)#access-list infilter permit udp object-group pn-networks
object-group pn-servers object-group pn-udp
```

- Looking at the output of `show access-list`, you can see that there are a lot of lines entered, but the items added with the object groups only show up as lines 7 and 8.

```
PIX#show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list infilter; 76 elements
access-list infilter line 1 extended permit tcp host 192.1.24.2 gt 1024 host
192.1.24.7 eq telnet (hitcnt=2) 0x1725857a
access-list infilter line 2 extended permit tcp host 192.1.24.4 gt 1024 host
192.1.24.8 eq telnet (hitcnt=4) 0x47328282
access-list infilter line 3 extended permit tcp any host 192.1.24.10 eq
telnet (hitcnt=0) 0xf8386f55
access-list infilter line 4 extended permit tcp any host 192.1.24.10 eq https
(hitcnt=0) 0xaa50fcea
access-list infilter line 5 extended permit icmp host 2.2.2.2 host 10.7.7.7
echo-reply (hitcnt=1) 0xc91e1d61
access-list infilter line 6 extended permit icmp host 4.4.4.4 host 10.7.7.7
echo-reply (hitcnt=1) 0xa375177b
access-list infilter line 7 extended permit tcp object-group pn-networks
object-group pn-servers object-group pn-tcp 0x5e3bcbb7
```



```
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq ftp (hitcnt=0) 0x3f909c21
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq www (hitcnt=0) 0x3212134b
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq smtp (hitcnt=0) 0x79eb2c2a
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq domain (hitcnt=0) 0x323e05d9
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq ftp (hitcnt=0) 0x89fe3a87
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq www (hitcnt=0) 0x719fa1af
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq smtp (hitcnt=0) 0x2f2a5684
access-list infilter line 7 extended permit tcp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq domain (hitcnt=0) 0x7ae562c2
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq ftp (hitcnt=0) 0x3080b478
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq www (hitcnt=0) 0x85291025
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq smtp (hitcnt=0) 0xb8e15a9a
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq domain (hitcnt=0) 0x1315b2ce
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq ftp (hitcnt=0) 0xe71ce344
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq www (hitcnt=0) 0xfe6a90d9
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq smtp (hitcnt=0) 0xcd63034c
access-list infilter line 7 extended permit tcp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq domain (hitcnt=0) 0xcd490981
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq ftp (hitcnt=0) 0xb9028eef
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq www (hitcnt=0) 0x75ab1b49
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq smtp (hitcnt=0) 0xc2b7826b
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq domain (hitcnt=0) 0xf454cbb6
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq ftp (hitcnt=0) 0x75e444b5
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq www (hitcnt=0) 0xf03f9f58
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq smtp (hitcnt=0) 0xeb20882b
access-list infilter line 7 extended permit tcp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq domain (hitcnt=0) 0x199b6dce
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq ftp (hitcnt=0) 0x24a63fe
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq www (hitcnt=0) 0xab4537c3
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq smtp (hitcnt=0) 0x6cf7a42
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq domain (hitcnt=0) 0x52fd819a
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq ftp (hitcnt=0) 0xca25a1c
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq www (hitcnt=0) 0x4140b907
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq smtp (hitcnt=0) 0xbdcdcf23bf
```



```
access-list infilter line 7 extended permit tcp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq domain (hitcnt=0) 0x3659a4f8
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq ftp (hitcnt=0) 0xa2a455ee
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq www (hitcnt=0) 0xe308521d
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq smtp (hitcnt=0) 0xa7e5841
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq domain (hitcnt=0) 0x105413c2
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq ftp (hitcnt=0) 0x70ffb863
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq www (hitcnt=0) 0xc3e1aa92
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq smtp (hitcnt=0) 0x193d499d
access-list infilter line 7 extended permit tcp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq domain (hitcnt=0) 0xab15e733
access-list infilter line 8 extended permit udp object-group pn-networks
object-group pn-servers object-group pn-udp 0x340083ab
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq tftp (hitcnt=0) 0x4324a66a
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq domain (hitcnt=0) 0xaebc7e47
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.21 eq 50000 (hitcnt=0) 0xc40aa3dd
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq tftp (hitcnt=0) 0xc5548003
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq domain (hitcnt=0) 0x8b81a11
access-list infilter line 8 extended permit udp 205.15.25.0 255.255.255.0
host 192.1.24.22 eq 50000 (hitcnt=0) 0x3dd64d65
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq tftp (hitcnt=0) 0x937baed1
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq domain (hitcnt=0) 0x190c55cf
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.21 eq 50000 (hitcnt=0) 0xda1fb08d
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq tftp (hitcnt=0) 0x59119642
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq domain (hitcnt=0) 0xe69b85d6
access-list infilter line 8 extended permit udp 207.215.1.0 255.255.255.0
host 192.1.24.22 eq 50000 (hitcnt=0) 0xc1abac9f
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq tftp (hitcnt=0) 0xa753bc21
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq domain (hitcnt=0) 0x8025d00c
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.21 eq 50000 (hitcnt=0) 0xd04bd9ed
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq tftp (hitcnt=0) 0x94e8f93e
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq domain (hitcnt=0) 0x4e87325c
access-list infilter line 8 extended permit udp 210.208.15.16 255.255.255.240
host 192.1.24.22 eq 50000 (hitcnt=0) 0xfeca0428
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq tftp (hitcnt=0) 0xc56e4b59
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq domain (hitcnt=0) 0xa1450ce7
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.21 eq 50000 (hitcnt=0) 0x7434cd7c
```



```
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq tftp (hitcnt=0) 0xa9d24b60
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq domain (hitcnt=0) 0x5dfdc645
access-list infilter line 8 extended permit udp 211.0.15.32 255.255.255.224
host 192.1.24.22 eq 50000 (hitcnt=0) 0x9cacf9df
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq tftp (hitcnt=0) 0x81093951
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq domain (hitcnt=0) 0x2350e78a
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.21 eq 50000 (hitcnt=0) 0xd1e72720
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq tftp (hitcnt=0) 0xe64cb33a
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq domain (hitcnt=0) 0x372130f8
access-list infilter line 8 extended permit udp 192.1.150.112 255.255.255.240
host 192.1.24.22 eq 50000 (hitcnt=0) 0x48eae304
```

Authentication Proxy

Task 5-17

The AAA server is located at 10.1.1.100. Create a static route for the AAA server on the PIX pointing towards R1. Configure the AAA server to communicate with the PIX using TACACS+ and a key of **ipexpert**. Configure a user named **pixuser** with a password of **ipexpert**.

- **Configure the static route on the PIX to point to the AAA server.**

```
PIX(config)#route inside 10.1.1.100 255.255.255.255 10.2.2.1
```


→ On the ACS server, under user setup, add the user pixuser as shown below:

Task 5-18

All outbound Telnet and HTTP Requests have to authenticate against the AAA server. The Username to use is **pixuser** with a password of **ipexpert**. Use the same username and password for all authentication passwords.

- Proxy authentication can be used to control access for specific users or groups. The PIX can communicate with RADIUS and TACACS+ servers to proxy for authentication and authorization for users of Telnet, HTTP or FTP.
- You must identify the server that handles authentication or authorization using the `aaa-server` command. First, create a unique server group name, and specify the use of TACACS+ authentication. Then, specify that the TACACS+ server is on the inside interface, and provide the IP address and key.

```
PIX(config)#aaa-server TAC protocol tacacs+
PIX(config)#aaa-server TAC host 10.1.1.100 ipexpert
```

- In the new PIX 7.x code, the default is for the authentication server to be on the inside interface. Also, when you add the key, the PIX will configure it as a second line in the running config, and the key will show up on a second line.

- We need to add the user, and also need to add the PIX as a Network device on the ACS server under Network configuration.

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address <http://10.1.1.100:2954/>

CISCO SYSTEMS

User Setup

Edit

User: pixuser (New User)

☐ Account Disabled

Supplementary User Info ?

Real Name

Description

User Setup ?

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

☐ Separate (CHAP/MS-CHAP/ARAP)

Password

- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

Applet nas_filter started

Internet

CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://10.1.1.100:2954/

CISCO SYSTEMS

Network Configuration

Edit

Add AAA Client

AAA Client Hostname:

AAA Client IP Address:

Key:

Authenticate Using:

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Help

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update / Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client

Appllet startStop started

Internet

- Finally, we need to add the aaa authentication commands on the PIX.
- Enable authentication for each desired service with the aaa authentication command. The format of the command is:

```
aaa authentication include authen_service if_name local_ip local_mask
[foreign_ip foreign_mask] server_tag
```

where:

- **authen_service** specifies the desired service.
- **if_name** specifies the name of the interface on which to enable the authentication.
- **local_ip, local_mask** specifies the host(s) and mask to be authenticated. Use '0 0' to specify any.
- **foreign_ip, foreign_mask** specifies the destination host(s) and mask. Use '0 0' to specify any.
- **server_tag** specifies the server group name configured on the aaa-server command.

- Following is an example configuration for enabling the authentication service:

```
PIX(config)#aaa authentication include telnet inside 0 0 0 0 TAC
PIX(config)#aaa authentication include http inside 0 0 0 0 TAC
```

- Test by trying to telnet to R2. The proxy authentication will prompt you for username and password. Afterwards, the connection will fail, since R2 does not have a password set.

```
R1#telnet 192.1.24.2
Trying 192.1.24.2 ... Open
```

```
Username: pixuser
```

```
Password:
```

```
Password required, but none set
```

```
[Connection to 192.1.24.2 closed by foreign host]
R1#
```

- On the ACS server, you should see the successful authentication request, and on the PIX, you can see that the user was authenticated in the output of show uauth.

```
PIX#show uauth
```

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1
user 'pixuser' at 10.2.2.1, authenticated (idle for 0:01:45)		
absolute timeout:	0:05:00	
inactivity timeout:	0:00:00	

```
PIX#
```

Task 5-19

Enable Telnet on R1 with a password of ipexpert.

- R1 will need to be configured to accept telnet connections. This is done by configuring a login password for the vty lines on R1.

```
R1(config)#line vty 0 4
R1(config-line)#password ipexpert
```

Task 5-20

Make R1 appear as 192.1.24.15 on the outside. Allow R4 to telnet into R1 through the PIX.

- Access from R4 to R1 requires you to enable access from a lower security level outside interface to the higher-level inside interface. To enable this, use the static and access-list commands.

```
PIX(config)#static (inside,outside) 192.1.24.15 10.2.2.1 netmask
255.255.255.255 0 0
```



```
PIX(config)#access-list infilter permit tcp host 192.1.24.4 gt 1024  
host 192.1.24.15 eq telnet
```

- **Test by telnetting to R1's translated address from R4.**

```
R4#telnet 192.1.24.15  
Trying 192.1.24.15 ... Open
```

User Access Verification

Password:
R1>

Task 5-21

All inbound traffic for Telnet should be authenticated against the AAA server. Allow any networks to telnet into R1's outside address in the Access List.

- **Enable authentication for telnet from the outside interface with the aaa authentication command.**

```
PIX(config)#aaa authentication include telnet outside 0 0 0 0 TAC
```

- **Add an access-list entry to allow any network to telnet to R1's outside address.**

```
PIX(config)#access-list infilter permit tcp any host 192.1.24.15 eq  
telnet
```

- **If you try to telnet to R1 from R4 now, you will see that you are prompted for the proxy authentication first.**

```
R4#telnet 192.1.24.15  
Trying 192.1.24.15 ... Open
```

Username: **pixuser**

Password:

User Access Verification

Password:
R1>

Task 5-22

All outbound TFTP and RSH traffic should be authenticated against the AAA server. Use 192.1.24.9 for the virtual address and telnet as the authentication protocol.

- **To enable authentication for non-standard protocols that do not support authentication, use the virtual telnet command. This command allows the PIX Virtual Telnet server to provide a way to pre-authenticate users who require connections through the PIX Firewall using services or protocols that do not support authentication. Users first**

connect to the Virtual Telnet server IP address, where the user is prompted for a username and password.

- When an unauthenticated user Telnets to the virtual IP address, they are challenged for their username and password, and then authenticated with the TACACS+ or RADIUS server. Once authenticated, they see the message "Authentication Successful" and their authentication credentials are cached in the PIX Firewall for the duration of the uauth timeout.
- Following is an example configuration for specifying authentication for TFTP, (UDP/69), and RSH, (TCP/514), and specifying the virtual address of the Virtual Telnet server:

```
PIX(config)#aaa authentication include udp/69 inside 0 0 0 0 TAC
PIX(config)#aaa authentication include tcp/514 inside 0 0 0 0 TAC
PIX(config)#virtual telnet 192.1.24.9
```

- Because the address of the Virtual Telnet server is on the external interface, you will need to enter an access-control entry to the access-list applied to the outside interface allowing telnet to the Virtual Telnet server address. You will also need to configure an identity static command, which specifies the same address of the Virtual Telnet server as the global and local addresses.

```
PIX(config)#access-list infilter permit tcp any host 192.1.24.9 eq
telnet
PIX(config)#static (inside,outside) 192.1.24.9 192.1.24.9 netmask
255.255.255.255 0 0
```

- Test the virtual telnet authentication by telnetting from R1 to the virtual server address, and entering the username/password. (You could also test the TFTP by configuring either R2 or R4 as a tftp server, and entering the tftp command from R1). Verify that the authentication is cached on the PIX with the show uauth command.

```
R1#telnet 192.1.24.9
Trying 192.1.24.9 ... Open
```

```
LOGIN Authentication
```

```
Username: pixuser
```

```
Password:
```

```
Authentication Successful
```

```
PIX#show uauth
```

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

```
user 'pixuser' at 10.2.2.1, authenticated (idle for 0:00:11)
  absolute timeout: 0:05:00
  inactivity timeout: 0:00:00
PIX#
```


- If you telnet to the virtual telnet address again, you can log out, and close the open authentication.

```
R1#telnet 192.1.24.9
Trying 192.1.24.9 ... Open
```

```
LOGOUT Authentication
```

```
Username: pixuser
```

```
Password:
```

```
Logout Successful
```

Task 5-23

R2 should be able to Telnet into 192.1.24.15 (R1's translated address). Configure R1 such that it should allow R2 to telnet into port 3025. Allow the appropriate entries in the access-list.

- Access from R2 to R1 requires you to enable access from a lower security level outside interface to the higher-level inside interface. To enable this, use the `static` and `access-list` commands. The `static` command was entered already in Task 5-20.
- Be sure to enter the source port of 3025 on the access-control entry.

```
PIX(config)#access-list infilter permit tcp host 192.1.24.2 host
192.1.24.15 eq 3025
```

- R1 must be configured to accept telnet connections on port 3025.

```
R1(config)#line vty 16
R1(config)#rotary 25
```

Task 5-24

Authenticate all Telnet traffic to port 3025 from R2 to R1 using the AAA Server.

- Enable authentication for telnet on port 3025 from the outside interface with the `aaa authentication` command.

```
PIX(config)#aaa authentication include tcp/3025 outside 0 0 0 0 TAC
```

- Verify your configuration. Because `tcp/3025` is not a protocol supported by authentication, you will need to use the Virtual Telnet server to authenticate. Then, attempt to telnet to R1 on port 3025. If you try to connect to port 3025 without authenticating first, you will receive an error message.

NOTE

Please use `Clear uauth` on the PIX after every authentication step to clear the authentication.


```
R2#telnet 192.1.24.15 3025
Trying 192.1.24.15, 3025 ... Open

Error: Must authenticate before using this service.

[Connection to 192.1.24.15 closed by foreign host]
R2#telnet 192.1.24.9
Trying 192.1.24.9 ... Open

LOGIN Authentication

Username: pixuser

Password:

Authentication Successful

[Connection to 192.1.24.9 closed by foreign host]
R2#telnet 192.1.24.15 3025
Trying 192.1.24.15, 3025 ... Open

User Access Verification

Password:
R1>
```

Advanced Filtering on the PIX

Task 5-25

You want to block Java and ActiveX applets from 2.2.2.2.

- You can disable ActiveX objects and remove Java applets with the `filter` command. Specify either Java or ActiveX, the port number, and the local and foreign IP addresses/mask. '0 0' is used for any.

```
PIX(config)#filter java 80 0 0 2.2.2.2 255.255.255.255
PIX(config)#filter activex 80 0 0 2.2.2.2 255.255.255.255
```

Task 5-26

Configure the Firewall to support protection against SMTP attacks by restricting the types of SMTP commands allowed.

- ESMTP inspection adds on to the commands allowed in previous versions with the "fixup smtp" command. 8 additional ESMTP commands are supported. It is configured using the command `inspect esmtp` under a policy map.

```
PIX(config)#policy-map global_policy
PIX(config-pmap)#class inspection_default
PIX(config-pmap-c)#inspect esmtp
```


Task 5-27

There is a WebSense server located at 10.1.1.101.

- To identify the address of a WebSense filtering server, use the `url-server` command. Specify the interface on which filtering is enabled, and the IP address of the server.

```
PIX(config)#url-server (inside) host 10.1.1.101
```

Task 5-28

Before a HTTP request is allowed to go out, the PIX should verify with the WebSense server if the website is allowed or not. Configure the PIX such that traffic will be allowed to pass if the WebSense server is down.

- Use the `filter url` command to configure the policy for filtering URLs. The syntax of the command for filtering URLs is as follows:

```
filter url port local_ip local_mask foreign_ip foreign_mask [allow]
```

- The `[allow]` keyword is optional and is used to tell the PIX to allow traffic to pass if the WebSense server is unreachable or unresponsive.

```
PIX(config)#filter url http 0 0 0 0 allow
```

Running RIP as the Routing Protocol on the PIX

Task 5-29

Remove all static routes from R1, R7, R8 and the PIX.

- Use the `no ip route` command to remove each static route from the specified routers. This is an example statement showing how to remove a static route from R7:

```
R7(config)#no ip route 0.0.0.0 0.0.0.0 10.7.7.10
```

- Use the `no route` command to remove each static route from the PIX. This is an example statement to show how to remove a static route from the PIX:

```
PIX(config)#no route inside 10.1.1.100 255.255.255.255 10.2.2.1 1
```

```
R1(config)#no ip route 0.0.0.0 0.0.0.0 10.2.2.10
```

```
R2(config)#no ip route 10.7.7.7 255.255.255.255 192.1.24.10
```

```
R4(config)#no ip route 10.7.7.7 255.255.255.255 192.1.24.10
```


Task 5-30

Run RIP V2 as your routing protocol on R1, R2, R4, R7 and R8. Advertise all networks on each router.

- To enable the RIP routing process, use the command `router rip` on the specified routers.
- To specify a RIP version to be used globally by the router, use the `version 2` command in router configuration mode.
- To advertise networks under RIP use the `network network-number` command. The `network` command also enables RIP to send updates to the interfaces in the specified networks.
- When RIP advertises a network across a different major net boundary, by default, RIP summarizes the advertised network at the major net boundary. Some environments may contain one or more discontinuous networks, which are comprised of a major net separated by another major net. The automatic summarization would prevent the routing of traffic from one portion of the discontinuous network to the other. To disable the automatic summarization of subnet routes into network-level routes, use the `no auto-summary` command under the RIP process, for each router.
- Here are the configuration examples for each router:

```
R1 (config) #router rip
R1 (config-router) #version 2
R1 (config-router) #network 1.0.0.0
R1 (config-router) #network 10.0.0.0
R1 (config-router) #no auto-summary
```

```
R2 (config) #router rip
R2 (config-router) #version 2
R2 (config-router) #network 2.0.0.0
R2 (config-router) #network 192.1.24.0
R2 (config-router) #no auto-summary
```

```
R4 (config) #router rip
R4 (config-router) #version 2
R4 (config-router) #network 4.0.0.0
R4 (config-router) #network 192.1.24.0
R4 (config-router) #no auto-summary
```

```
R7 (config) #router rip
R7 (config-router) #version 2
R7 (config-router) #network 7.0.0.0
R7 (config-router) #network 10.0.0.0
R7 (config-router) #no auto-summary
```

```
R8 (config) #router rip
R8 (config-router) #version 2
R8 (config-router) #network 8.0.0.0
R8 (config-router) #network 10.0.0.0
R8 (config-router) #no auto-summary
```


Task 5-31

Configure routing protocol authentication using a key of 1 and key-string of **ipexpert**.

- **RIP route authentication provides either plain text authentication or MD5 authentication of routing updates to prevent the introduction of unauthorized or false routing messages from unapproved sources. You must specify RIP version 2 to run authentication.**
- **You first must specify a text key string that is identical on each RIP router. Use the key-chain configuration mode to specify the text string. The format of the key-chain configuration is:**

```
key-chain name-of-chain
      key number
            key-string text
```

- **Following is an example of specifying a key for R1. These commands will need to be entered on ALL routers participating in RIP route authentication.**

```
R1(config)#key chain rip
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string ipexpert
```

- **Use the show key chain command to see the key-string:**

```
R1#show key chain
Key-chain rip:
  key 1 -- text "ipexpert"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
```

- **To enable route authentication, you must enable authentication of RIP packets on each interface which is sending and receiving RIP packets, and identify the key-chain to use. You can allow the authentication mode to default to plain text, or specify MD5. You should not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet.**
- **The interface command to enable route authentication is ip rip authentication key-chain key-chain.**
- **The interface command to specify MD5 authentication is ip rip authentication mode md5.**

```
R1(config)#key chain rip
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string ipexpert
```

```
R1(config)#int fa0/1
R1(config-if)#ip rip authent key-chain rip
```

```
R2(config)#key chain rip
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string ipexpert
```

```
R2(config)#int fa1/0
R2(config-if)#ip rip authent key-chain rip
```



```
R4(config)#key chain rip
R4(config-keychain)#key 1
R4(config-keychain-key)#key-string ipexpert

R4(config)#int fa0/0
R4(config-if)#ip rip authent key-chain rip

R7(config-router)#key chain rip
R7(config-keychain)#key 1
R7(config-keychain-key)#key-string ipexpert

R7(config)#int fa0/0
R7(config-if)#ip rip authent key-chain rip

R8(config)#key chain rip
R8(config-keychain)#key 1
R8(config-keychain-key)#key-string ipexpert

R8(config)#int fa0/0
R8(config-if)#ip rip authentication key-chain rip
```

Task 5-32

Run RIP V2 on the PIX to inject a default route to R1, R7 and R8. Make sure to use RIP authentication to match the Routers.

- If you configured MD5 authentication on the routers, you will need to match with MD5 authentication on the PIX. If you configured the routers for plain text authentication, configure plain text authentication on the PIX.

```
PIX(config)#router rip
PIX(config-router)#version 2
PIX(config-router)#redistribute static metric 1
PIX(config-router)#network 10.0.0.0

PIX(config)#interface eth1
PIX(config-if)#rip authentication key ipexpert key_id 1

PIX(config)#int eth0.7
PIX(config-subif)#rip authentication key ipexpert key_id 1

PIX(config)#int eth0.8
PIX(config-subif)#rip authentication key ipexpert key_id 1
```

Task 5-33

Run RIP to receive routes from all the routers. Make sure to use RIP authentication to match the Routers.

- The PIX is not yet configured for the outside network for RIP. Add the network to RIP, and add the authentication on the interface.

```
PIX(config)#router rip
PIX(config-router)#network 192.1.24.0
```



```
PIX(config)#interface eth0
PIX(config-if)#rip authentication key ipexpert key 1
```

Task 5-34

Verify that the appropriate routes are propagating in the routing tables of all routers and the PIX Firewall.

→ Check the routing tables on the routers and the PIX.

```
R1#show ip route rip
R    2.0.0.0/8 [120/2] via 10.2.2.10, 00:00:08, FastEthernet0/1
R    4.0.0.0/8 [120/2] via 10.2.2.10, 00:00:08, FastEthernet0/1
R   192.1.24.0/24 [120/1] via 10.2.2.10, 00:00:08, FastEthernet0/1
R    7.0.0.0/8 [120/2] via 10.2.2.10, 00:00:08, FastEthernet0/1
R    8.0.0.0/8 [120/2] via 10.2.2.10, 00:00:08, FastEthernet0/1
    10.0.0.0/24 is subnetted, 4 subnets
R      10.8.8.0 [120/1] via 10.2.2.10, 00:00:08, FastEthernet0/1
R      10.7.7.0 [120/1] via 10.2.2.10, 00:00:08, FastEthernet0/1
R*   0.0.0.0/0 [120/1] via 10.2.2.10, 00:00:08, FastEthernet0/1
R1#

PIX#show route | i R
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       * - candidate default, U - per-user static route, o - ODR
R    1.0.0.0 255.0.0.0 [120/1] via 10.2.2.1, 0:00:11, inside
R    2.0.0.0 255.0.0.0 [120/1] via 192.1.24.2, 0:00:07, outside
R    4.0.0.0 255.0.0.0 [120/1] via 192.1.24.4, 0:00:23, outside
R    7.0.0.0 255.0.0.0 [120/1] via 10.7.7.7, 0:00:21, DMZ7
R    8.0.0.0 255.0.0.0 [120/1] via 10.8.8.8, 0:00:03, DMZ8
R   10.1.1.0 255.255.255.0 [120/1] via 10.2.2.1, 0:00:11, inside
PIX#
```

Running OSPF as the Routing Protocol on the PIX

Task 5-35

Remove RIP from all Routers and the PIX Firewall.

→ Remove the RIP routing process from each router using the command `no router rip`.

```
PIX(config)#no router rip

R1(config)#no router rip

R2(config)#no router rip

R4(config)#no router rip

R7(config)#no router rip

R8(config)#no router rip
```


Task 5-36

Run OSPF as your routing protocol on R1, R2, R4, R7 and R8. Advertise all networks on each router.

- To enable the OSPF routing process, use the command `router ospf process-number` on the specified routers. The *process-number* argument is locally significant only, in cases of running multiple processes, so for this exercise, the value is unimportant.
- To advertise networks under OSPF use the `network ip-address wildcard-mask area area-id` command. For OSPF to operate on the interface, the primary address of the interface must be covered by the combination *ip-address wildcard-mask* arguments. For this exercise, use *area-id* of 0 for all interfaces, since no requirements were specified.
- Since we are advertising all interfaces into OSPF, we can use a network of 0.0.0.0 with a wildcard mask of 255.255.255.255.

```
R1(config)#router ospf 1
R1(config-router)#network 0.0.0.0 255.255.255.255 area 0

R2(config)#router ospf 1
R2(config-router)#network 0.0.0.0 255.255.255.255 area 0

R4(config)#router ospf 1
R4(config-router)#network 0.0.0.0 255.255.255.255 area 0

R7(config)#router ospf 1
R7(config-router)#network 0.0.0.0 255.255.255.255 area 0

R8(config)#router ospf 1
R8(config-router)#network 0.0.0.0 255.255.255.255 area 0
```

Task 5-37

Configure routing protocol authentication using a key of 1 and key-string of **ipexpert**. Do not use the AREA authentication command under the ospf process.

- OSPF route authentication provides either plain text authentication or MD5 authentication of routing updates to prevent the introduction of unauthorized or false routing messages from unapproved sources.
- To enable route authentication, you must identify the key to use and enable authentication either on each interface or for the OSPF area. The same key identifier must be used on all neighbor routers. To enable OSPF Message Digest 5 (MD5) authentication, use the `ip ospf message-digest-key` command in interface configuration mode.

```
R1(config-int)#ip ospf message-digest-key 1 md5 ipexpert
```

- You can allow the authentication mode to default to plain text, or specify MD5. You should not use plain text authentication for security purposes, because the unencrypted authentication key is sent in every OSPF header. To specify the authentication type for an interface, use the `ip ospf authentication` command in interface configuration mode.


```
R1(config-int)#ip ospf authentication message-digest

R1(config)#int fa0/1
R1(config-if)#ip ospf message-digest-key 1 md5 ipexpert
R1(config-if)#ip ospf authentication message-digest

R2(config)#int fa1/0
R2(config-if)#ip ospf message-digest-key 1 md5 ipexpert
R2(config-if)#ip ospf authentication message-digest

R4(config-router)#int fa0/0
R4(config-if)#ip ospf message-digest-key 1 md5 ipexpert
R4(config-if)#ip ospf authentication message-digest

R7(config)#int fa0/0
R7(config-if)#ip ospf message-digest-key 1 md5 ipexpert
R7(config-if)#ip ospf authentication message-digest

R8(config)#int fa0/0
R8(config-if)#ip ospf message-digest-key 1 md5 ipexpert
R8(config-if)#ip ospf authentication message-digest
```

Task 5-38

Run OSPF in Process ID 1 for the outside network. Make sure to use OSPF authentication to match the Routers on the outside.

- ➔ To enable the OSPF routing process, use the command `router ospf process-number`.
- ➔ To advertise networks under OSPF use the `network ip-address wildcard-mask area area-id` command. For OSPF to operate on the interface, the primary address of the interface must be covered by the combination `ip-address wildcard-mask` arguments. For this exercise, use `area-id` of 0, since no requirements were specified.
- ➔ Following is a configuration example for enabling OSPF on the outside interface of the PIX:

```
PIX(config)#router ospf 1
PIX(config-router)#network 192.1.24.0 255.255.255.0 area 0
```

- ➔ To enable route authentication, you must configure the interface-specific OSPF authentication mode and key. To specify the desired interface, use the `routing interface` command.
- ➔ The same key identifier must be used on all neighbor routers. To enable OSPF Message Digest 5 (MD5) authentication; use the `ospf message-digest-key` command in OSPF interface submode.

- You can allow the authentication mode to default to plain text, or specify MD5. You should not use plain text authentication for security purposes, because the unencrypted authentication key is sent in every OSPF header. To specify the authentication type for an interface, use the `ospf authentication` command in OSPF interface submode.

```
PIX(config)#router ospf 1
PIX(config-router)#network 192.1.24.0 255.255.255.0 area 0

PIX(config)#int eth0
PIX(config-if)#ospf message-digest-key 1 md5 ipexpert
PIX(config-if)#ospf authentication message-digest
```

- Check the routing table with `show route` and make sure that you can see the routes for the loopbacks of R2 and R4.

```
PIX#show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    2.2.2.2 255.255.255.255 [110/11] via 192.1.24.2, 0:00:41, outside
O    4.4.4.4 255.255.255.255 [110/11] via 192.1.24.4, 0:00:41, outside
C    192.1.24.0 255.255.255.0 is directly connected, outside
C    10.2.2.0 255.255.255.0 is directly connected, inside
C    10.8.8.0 255.255.255.0 is directly connected, DMZ8
C    10.7.7.0 255.255.255.0 is directly connected, DMZ7
PIX#
```

Task 5-39

Run OSPF in Process ID 2 for the inside and the 2 DMZ networks. Make sure to use OSPF authentication to match the Routers on the inside and the DMZ networks.

- When NAT is used and OSPF is operating on public and private areas you need to run two OSPF processes to prevent the advertising of private networks in public areas. This lets you use NAT and OSPF, without advertising private networks.
- With the PIX, the wildcard mask is reversed. You can still use a range, just like on a router. Just reverse the mask. Since the two DMZ networks and the Inside use 10.x.x.x addressing, a network of 10.0.0.0 with a mask of 255.0.0.0 will cover all the address space with a first octet of 10.

```
PIX(config)#router ospf 2
PIX(config-router)#network 10.0.0.0 255.0.0.0 area 0

PIX(config)#int eth1
PIX(config-if)#ospf message-digest-key 1 md5 ipexpert
PIX(config-if)#ospf authentication message-digest
```



```

PIX(config)#int eth0.7
PIX(config-subif)#ospf message-digest-key 1 md5 ipexpert
PIX(config-subif)#ospf authentication message-digest

PIX(config)#int eth0.8
PIX(config-subif)#ospf message-digest-key 1 md5 ipexpert
PIX(config-subif)#ospf authentication message-digest

```

Task 5-40

Verify that the appropriate routes are propagating in the routing tables of all routers and the PIX Firewall.

```
PIX#sh ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	0:00:37	192.1.24.2	outside
4.4.4.4	1	FULL/DROTHER	0:00:32	192.1.24.4	outside
7.7.7.7	1	FULL/BDR	0:00:35	10.7.7.7	DMZ7
8.8.8.8	1	FULL/BDR	0:00:30	10.8.8.8	DMZ8
1.1.1.1	1	FULL/BDR	0:00:35	10.2.2.1	inside

```
PIX#
```

```
PIX#show route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

O    1.1.1.1 255.255.255.255 [110/11] via 10.2.2.1, 0:04:45, inside
O    2.2.2.2 255.255.255.255 [110/11] via 192.1.24.2, 0:07:02, outside
O    4.4.4.4 255.255.255.255 [110/11] via 192.1.24.4, 0:07:02, outside
C    192.1.24.0 255.255.255.0 is directly connected, outside
O    7.7.7.7 255.255.255.255 [110/11] via 10.7.7.7, 0:04:45, DMZ7
O    8.8.8.8 255.255.255.255 [110/11] via 10.8.8.8, 0:04:45, DMZ8
O    10.1.1.0 255.255.255.0 [110/11] via 10.2.2.1, 0:04:45, inside
C    10.2.2.0 255.255.255.0 is directly connected, inside
C    10.8.8.0 255.255.255.0 is directly connected, DMZ8
C    10.7.7.0 255.255.255.0 is directly connected, DMZ7
PIX#

```

Task 5-41

You want routes from the outside routers to propagate to R1, R7 and R8 and vice versa.

- To propagate the routes, you will need to enable redistribution on the PIX under each OSPF process. Use the `redistribute ospf` command. Specify the argument `subnets` to also redistribute routes that are subnetted.

```

PIX(config)#router ospf 1
PIX(config-router)#redistribute ospf 2 subnets

```



```
PIX(config)#router ospf 2
PIX(config-router)#redistribute ospf 1 subnets
```

- Check the routing tables on the routers with the command `show ip route ospf`.

```
R2#show ip route ospf
 1.0.0.0/32 is subnetted, 1 subnets
O E2   1.1.1.1 [110/11] via 192.1.24.10, 00:01:09, FastEthernet1/0
 4.0.0.0/32 is subnetted, 1 subnets
O      4.4.4.4 [110/2] via 192.1.24.4, 00:01:09, FastEthernet1/0
 7.0.0.0/32 is subnetted, 1 subnets
O E2   7.7.7.7 [110/11] via 192.1.24.10, 00:01:09, FastEthernet1/0
 8.0.0.0/32 is subnetted, 1 subnets
O E2   8.8.8.8 [110/11] via 192.1.24.10, 00:01:09, FastEthernet1/0
10.0.0.0/24 is subnetted, 4 subnets
O E2   10.8.8.0 [110/10] via 192.1.24.10, 00:01:09, FastEthernet1/0
O E2   10.7.7.0 [110/10] via 192.1.24.10, 00:01:09, FastEthernet1/0
O E2   10.2.2.0 [110/10] via 192.1.24.10, 00:01:09, FastEthernet1/0
O E2   10.1.1.0 [110/11] via 192.1.24.10, 00:01:09, FastEthernet1/0
R2#
```

```
R7#show ip route ospf
 1.0.0.0/32 is subnetted, 1 subnets
O      1.1.1.1 [110/12] via 10.7.7.10, 00:00:34, FastEthernet0/0
 2.0.0.0/32 is subnetted, 1 subnets
O E2   2.2.2.2 [110/11] via 10.7.7.10, 00:00:34, FastEthernet0/0
 4.0.0.0/32 is subnetted, 1 subnets
O E2   4.4.4.4 [110/11] via 10.7.7.10, 00:00:34, FastEthernet0/0
O E2 192.1.24.0/24 [110/10] via 10.7.7.10, 00:00:34, FastEthernet0/0
 8.0.0.0/32 is subnetted, 1 subnets
O      8.8.8.8 [110/12] via 10.7.7.10, 00:00:34, FastEthernet0/0
10.0.0.0/24 is subnetted, 4 subnets
O      10.8.8.0 [110/11] via 10.7.7.10, 00:00:34, FastEthernet0/0
O      10.2.2.0 [110/11] via 10.7.7.10, 00:00:34, FastEthernet0/0
O      10.1.1.0 [110/12] via 10.7.7.10, 00:00:34, FastEthernet0/0
R7#
```

Running OSPF thru the PIX

Task 5-42

Remove OSPF process ID 1 from the PIX Firewall.

- To remove the OSPF routing process, use the command `no router ospf process-number`.

```
PIX(config)#no router ospf 1
```

Task 5-43

You want R2 to peer with R1 for OSPF.

- OSPF uses multicast to establish neighbor relationships and advertise routes. R2 and R1 are on opposite sides of the PIX. The PIX does not forward multicast traffic. You will need to setup a GRE tunnel to pass the OSPF multicast traffic through the PIX.

Task 5-44

Configure a GRE Tunnel to accomplish this. Make sure the 192.1.24.0 network is advertised to R1 and the 10.2.2.0 network is advertised to R2.

- Define a tunnel interface on each router endpoint with the command `interface tunnel number`.
- Specify a source IP address for the each tunnel interface with the interface configuration command `tunnel source {ip-address | interface}`. The IP address specified as the source address must be an address of an interface on the router, or you may specify an interface on the router that has IP enabled.
- Specify a destination IP address for each tunnel interface with the interface configuration command `tunnel destination {ip-address | hostname}`. The IP address specified as the destination address must be an address of an interface on the destination router, or you may specify a hostname that resolves to the IP address of an interface on the destination router.
- Because NAT is enabled, the destination addresses must be global NAT addresses. The internal address of R1 already has a static NAT entry defined on the PIX from an earlier task. The local address of 10.2.2.1 translates to the global address 192.1.24.15, so this address must be specified as the tunnel destination on R2. For the tunnel destination on R1, you will need to create a new static entry on the PIX and use that global address for the tunnel destination.

```
PIX(config)#static (outside,inside) 10.2.2.15 192.1.24.2 netmask  
255.255.255.0 0
```

- Enable IP on each tunnel interface with the interface configuration command `ip address ip-address netmask`. The IP addresses specified for each end of the tunnel should be within the same subnet.
- Following are configuration examples for each router:

```
R1(config)#interface tunnel 12  
R1(config-if)#ip address 10.12.12.1 255.255.255.0  
R1(config-if)#tunnel source 10.2.2.1  
R1(config-if)#tunnel destination 10.2.2.15  
R1(config-if)#ip ospf authentication message-digest  
R1(config-if)#ip ospf message-digest-key 1 md5 ipexpert
```

```
R2(config)#interface tunnel 12  
R2(config-if)#ip address 10.12.12.2 255.255.255.0  
R2(config-if)#tunnel source 192.1.24.2  
R2(config-if)#tunnel destination 192.1.24.15  
R2(config-if)#ip ospf authentication message-digest  
R2(config-if)#ip ospf message-digest-key 1 md5 ipexpert
```


- You will also need to enable OSPF operation on the tunnel interfaces:

```
R1(config)#router ospf 1
R1(config-router)#network 10.12.12.0 0.0.0.255 area 0

R2(config)#router ospf 1
R2(config-router)#network 10.12.12.0 0.0.0.255 area 0
```

Task 5-45

Allow the appropriate entries in the Access List.

- You will need to add an access control entry to the inbound access list that allows GRE from the R2 tunnel interface address to the R1 tunnel interface global address. All the traffic passing through the tunnel will be encapsulated, so GRE is all that needs to be allowed between the two hosts.

```
PIX(config)#access-list infilter permit gre host 192.1.24.2 host
192.1.24.15
```

Task 5-46

You cannot use Static routes to accomplish this task.

- Because the tunnel destination addresses were configured to be global NAT addresses on the PIX, static routes are not necessary. The destination addresses appear to be on the local subnet.

Task 5-47

You should see all routes in R2's routing table, including the 10.1.1.0 and 10.2.2.0.

```
R2#show ip route
*Jan 27 07:08:55.069: %SYS-5-CONFIG_I: Configured from console by consoleospf
  1.0.0.0/32 is subnetted, 1 subnets
O    1.1.1.1 [110/11112] via 10.12.12.1, 00:01:47, Tunnel12
  4.0.0.0/32 is subnetted, 1 subnets
O    4.4.4.4 [110/2] via 192.1.24.4, 00:01:47, FastEthernet1/0
  7.0.0.0/32 is subnetted, 1 subnets
O    7.7.7.7 [110/11123] via 10.12.12.1, 00:01:47, Tunnel12
  8.0.0.0/32 is subnetted, 1 subnets
O    8.8.8.8 [110/11123] via 10.12.12.1, 00:01:47, Tunnel12
 10.0.0.0/24 is subnetted, 5 subnets
O    10.8.8.0 [110/11122] via 10.12.12.1, 00:01:47, Tunnel12
O    10.7.7.0 [110/11122] via 10.12.12.1, 00:01:47, Tunnel12
O    10.2.2.0 [110/11112] via 10.12.12.1, 00:01:47, Tunnel12
O    10.1.1.0 [110/11112] via 10.12.12.1, 00:01:47, Tunnel12
R2#
```


Running BGP thru the PIX

Task 5-48

This lab will start with a fresh config. Erase the configs and reload R1, R2, R4, the switches and the PIX.

- To erase the configs on each router, switch and the PIX, use the `write erase` command.
- Use the `reload` command to reload each device.

Task 5-49

Load the initial configs for R1, R2, R4 and the switches.

- Load the initial configs for each device using the provided text files, and save the configurations with the `write memory` command.

Task 5-50

Bring the E0 and E1 interfaces up on the PIX. Configure them with the following IP addresses:

- Outside: 192.1.24.10 /24
- 10.2.2.10 /24

```
pixfirewall(config)#hostname PIX
PIX(config)#interface eth0
PIX(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
PIX(config-if)#ip address 192.1.24.10 255.255.255.0
PIX(config-if)#no shut
PIX(config-if)#int eth1
PIX(config-if)#no shut
PIX(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
PIX(config-if)#ip address 10.2.2.10 255.255.255.0
```

Task 5-51

Run RIP v2 as the routing protocol on R1, R2 and R4. Advertise all directly connected networks.

```
R1(config)#router rip
R1(config-router)#ver 2
R1(config-router)#no auto-sum
R1(config-router)#network 1.0.0.0
R1(config-router)#network 10.0.0.0

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 2.0.0.0
R2(config-router)#network 192.1.24.0
```



```
R4(config)#router rip
R4(config-router)#version 2
R4(config-router)#no auto-summary
R4(config-router)#network 192.1.24.0
R4(config-router)#network 4.0.0.0
```

Task 5-52

Run RIP on the PIX to receive the RIP routes on the inside and outside interfaces.

```
PIX(config)#router rip
PIX(config-router)#version 2
PIX(config-router)#no auto-summary
PIX(config-router)#network 10.0.0.0
PIX(config-router)#network 192.1.24.0
```

- **Verify that R1 sees the routes for R2 and R4's loopback networks.**

```
R1#show ip route rip
R    2.0.0.0/8 [120/2] via 10.2.2.10, 00:00:17, FastEthernet0/1
R    4.0.0.0/8 [120/2] via 10.2.2.10, 00:00:17, FastEthernet0/1
R    192.1.24.0/24 [120/1] via 10.2.2.10, 00:00:17, FastEthernet0/1
R1#
```

Task 5-53

Configure the following loopbacks on R1, R2 and R4:

- R1 Loopback 55: 55.1.1.1 /24
 - R2 Loopback 55: 55.2.2.2 /24
 - R4 Loopback 55: 55.4.4.4 /24
- **To specify a loopback interface and enter interface configuration mode, use the interface loopback command. Assign the IP address with the ip address command in interface configuration mode.**

```
R1(config)#int loop55
R1(config-if)#ip address 55.1.1.1 255.255.255.0

R2(config)#int loop55
R2(config-if)#ip address 55.2.2.2 255.255.255.0

R4(config)#int loop55
R4(config-if)#ip address 55.4.4.4 255.255.255.0
```


Task 5-54

Run IBGP between R1 and R2. They should be in AS 12. Peer R2 with 1.1.1.1. Peer R1 with 2.2.2.2. Configure the PIX with the appropriate statics and access-lists. Create host routes on R1 and R2 for each other.

- To enable the BGP routing process, use the `router bgp as-number` command. The `as-number` argument specifies an Autonomous System (AS) number that identifies the router to other BGP routers.

```
R1(config)#router bgp 12
```

- It is generally best practice to disable auto-summary, unless told otherwise. This disables the automatic summarization of subnet routes into network-level routes.

```
R1(config-router)#no auto-summary
```

- The BGP router ID defaults to the IP address of a loopback interface, or lacking one, to the highest IP address configured on a physical interface. It is best practice to configure a fixed router ID for a BGP-speaking router specifying a loopback interface, using the `bgp router-id` command in router configuration mode.

```
R1(config-router)#bgp router-id 1.1.1.1
```

- Next, configure R1 to peer to R2 in AS12. Use the `neighbor {ip-address | peer-group-name} remote-as as-number` command.

```
R1(config-router)#neighbor 2.2.2.2 remote-as 12
```

- BGP defaults to use the IP address of the closest interface to the neighbor for TCP connections. Use the `neighbor update-source` command in router configuration mode to specify the loopback address as the source address for TCP.

```
R1(config-router)#neighbor 2.2.2.2 update-source loopback0
```

- Now, configure R2 to peer to R1 in AS12. For IBGP, each router must use the same AS number.

```
R2(config)#router bgp 12
R2(config-router)#no auto-summary
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 1.1.1.1 remote-as 12
R2(config-router)#neighbor 1.1.1.1 update-source loopback0
```

- You can create an access-list applied to the outside interface allowing the BGP to the R1 address.

```
PIX(config)#access-list infiltrer permit tcp host 2.2.2.2 gt 1024 host 1.1.1.1 eq bgp
PIX(config)#access-group infiltrer in interface outside
```


- **Note:** It is not completely necessary to configure this access list for the adjacency to form. By default, both routers will try to establish the connection. If the connection is established from the inside to the outside, the PIX will automatically allow the return traffic back in. This access list allows the outside router to initiate the connection to the inside router. If unsure about whether a BGP connection should be able to be established in either direction, make sure to ask the proctor.

Task 5-55

Run EBGP between R1 and R4. R4 is in AS4. Peer R4 with 10.2.2.1. Peer R1 with 192.1.24.4. Configure the PIX with the appropriate statics and access-lists. Create host routes on R1 and R4 for each other.

- **EBGP connections generally are with peers that are directly connected. For this lab, the PIX is located between the peers, so they are not directly connected. To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the `neighbor ebgp-multihop` command in router configuration mode.**

```
R1(config)#router bgp 12
R1(config-router)#neighbor 192.1.24.4 remote-as 4
R1(config-router)#neighbor 192.1.24.4 ebgp-multihop
```

```
R4(config)#router bgp 4
R4(config-router)#no auto-summary
R4(config-router)#bgp router-id 4.4.4.4
R4(config-router)#neighbor 10.2.2.1 remote-as 12
R4(config-router)#neighbor 10.2.2.1 ebgp-multihop
```

- **In earlier PIX versions, a NAT translation was required for traffic to pass. By default, NAT control is disabled in version 7.x, and so a static translation is not necessary.**
- **You can create an access-list applied to the outside interface allowing the BGP to the R1 address. Again, this may not be necessary, depending on the desired direction of the BGP adjacency.**

```
PIX(config)#access-list infilter permit tcp host 192.1.24.4 gt 1024
host 10.2.2.1 eq bgp
```

Task 5-56

Advertise the new loopbacks in BGP.

- **To specify the networks to be advertised by the BGP routing processes, use the `network` command in router configuration mode.**

```
R1(config)#router bgp 12
R1(config-router)#network 55.1.1.0 mask 255.255.255.0
```

```
R2(config)#router bgp 12
R2(config-router)#network 55.2.2.0 mask 255.255.255.0
R4(config)#router bgp 4
R4(config-router)#network 55.4.4.0 mask 255.255.255.0
```



```
R4#show ip bgp
```

```
BGP table version is 4, local router ID is 4.4.4.4
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
               r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 55.1.1.0/24	10.2.2.1	0		0 12	i
*> 55.2.2.0/24	10.2.2.1			0 12	i
*> 55.4.4.0/24	0.0.0.0	0		32768	i

```
R4#
```

Task 5-57

Authenticate the EBGP neighbors.

- To enable MD5 authentication on a TCP connection between two BGP peers, use the `neighbor password` command in router configuration mode on each peer router. R1 and R4 are the EBGP neighbors.

```
R1(config)#router bgp 12
```

```
R1(config-router)#neighbor 192.1.24.4 password ipexpert
```

```
R4(config)#router bgp 4
```

```
R4(config-router)#neighbor 10.2.2.1 password ipexpert
```

- Verify that the routers remain peered. (The routers will attempt to maintain the peer session until the BGP holddown timer expires, which defaults to 180 seconds). You also can force a reset with the `clear ip bgp` command.
- When configuring BGP peers with MD5 authentication that pass through a PIX firewall you must also disable the TCP random sequence number feature on the PIX firewall because this feature will prevent the BGP peers from successfully negotiating a connection. The BGP neighbor authentication fails because the PIX firewall changes the TCP sequence number for IP packets before it forwards them. When the BGP peer receiving the authentication request runs the MD5 algorithm, it will detect that the TCP sequence number has been changed and reject the authentication request. To prevent the TCP sequence number change, use the `nonrandomseq` keyword in the PIX configuration. This can be done either on a translation command, or on a policy. The PIX 7.x code also handles TCP options a bit differently, and will clear the options by default. Option 19 is used for MD5. By default, the PIX will clear this option, and the router will display an error message of "No MD5 digest". Both of these items can be addressed in a single policy.

```
PIX(config)#class-map BGPCCLASS
```

```
PIX(config-cmap)#match port tcp eq 179
```

```
PIX(config-pmap)#tcp-map MYMAP
```

```
PIX(config-tcp-map)#tcp-options range 19 19 allow
```

```
PIX(config)#policy-map global_policy
```

```
PIX(config-pmap)#class BGPCCLASS
```

```
PIX(config-pmap-c)#set connection random-sequence-number disable
```

```
PIX(config-pmap-c)#set connection advanced-options MYMAP
```


→ **Verify that the neighbor relationship comes up.**

```
R1#show ip bgp
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop              Metric LocPrf Weight Path
*> 55.1.1.0/24            0.0.0.0                  0         32768 i
*>i55.2.2.0/24            2.2.2.2                  0        100      0 i
*> 55.4.4.0/24            192.1.24.4               0         0 4 i
R1#
```

Remote Management of the PIX

Task 5-58

Allow the ACS Server to Manage the PIX Firewall.

→ **This will be configured in the next few steps.**

Task 5-59

The ACS Server should be able to use either ssh or telnet for management.

→ **The commands SSH and Telnet allow you to specify from what addresses you want to allow management.**

```
PIX(config)#ssh 10.1.1.100 255.255.255.255 inside
PIX(config)#telnet 10.1.1.100 255.255.255.255 inside
```

```
PIX(config)#domain-name ipexpert.com
PIX(config)#crypto key generate rsa
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: yes
Keypair generation process begin. Please wait...
PIX(config)#
```

→ **Note: In older PIX versions you needed to manually save with 'ca save all'. With the newer versions, the key pairs are saved when you do a write mem.**

Task 5-60

The user authentication should be done based on TACACS+.

→ **You must identify the server that handles authentication or authorization using the aaa-server command. First, create a unique server group name, and specify the use of TACACS+ authentication. Then, specify the TACACS+ IP address and key.**

```
PIX(config)#aaa-server TAC protocol tacacs+
PIX(config)#aaa-server TAC host 10.1.1.100 ipexpert
```


- To protect access to the console with an authentication server, use the `aaa authentication telnet | ssh console` command.

```
PIX(config)#aaa authentication telnet console TAC
PIX(config)#aaa authentication ssh console TAC
```

Task 5-61

The ACS Server should already been setup for this communication.

- This was done in an earlier step.

Task 5-62

The username for management is `pixuser` with a password of `ipexpert`.

- You can verify your remote management configuration by opening a telnet session and an ssh session from the ACS server desktop to 10.2.2.10, or by adding R1's address for SSH and telnet and testing from R1.

```
R1#ssh -l pixuser 10.2.2.10
```

Password:

Type help or '?' for a list of available commands.

PIX>

Enabling the PIX firewall as a DHCP Server

Task 5-63

Configure the PIX firewall as a DHCP Server.

Task 5-64

It should assign IP configuration on the inside interface based on the following information:

- IP ADDRESS : 10.2.2.51 – 10.2.2.100
 - WINS ADDRESS : 10.2.2.135
 - DNS ADDRESS : 150.50.24.53
 - DEFAULT GATEWAY : 10.2.2.10
 - LEASE TIME : 3 Days 12 hours
 - Excluded Addresses : 10.2.2.1 – 10.2.2.50
- Specify a DHCP address pool using the `dhcpd address` command. Only those addresses specified are included in the pool, so there is no need to configure excluded addresses.

```
PIX(config)#dhcpd address 10.2.2.51-10.2.2.100 inside
```


- Specify the IP address(es) of the WINS server(s) the client will use. You can specify up to two DNS servers.

```
PIX(config)#dhcpd wins 10.2.2.135
```

- Specify the IP address(es) of the DNS server(s) the client will use. You can specify up to two DNS servers.

```
PIX(config)#dhcpd dns 150.50.24.53
```

- Specify the lease length to be granted to the client. This lease equals the amount of time (in seconds) the client can use its allocated IP address before the lease expires.

```
PIX(config)#dhcpd lease 302400
```

- The DHCP daemon on the PIX firewall provides the IP address of the interface on which it receives the DHCP client request as the default gateway address.

- Enable the DHCP daemon within the PIX Firewall to listen for DHCP client requests on the enabled interface.

```
PIX(config)#dhcpd enable inside
```

- Verify the DHCP server configuration with the `show run | i dhcpd` command.

```
PIX(config)#show run | i dhcpd
dhcpd dns 150.50.24.53
dhcpd wins 10.2.2.135
dhcpd lease 302400
dhcpd address 10.2.2.51-10.2.2.100 inside
dhcpd enable inside
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

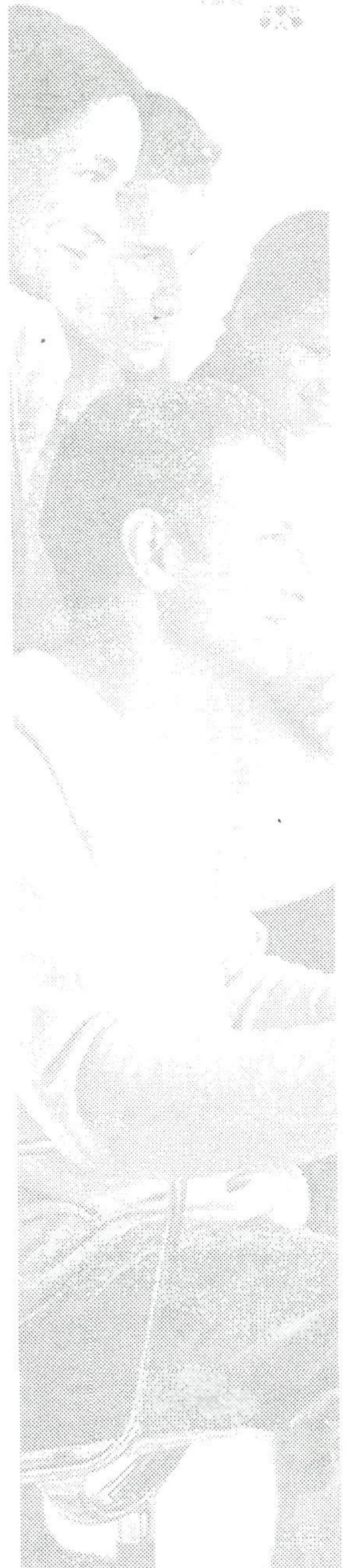
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 6: PIX Firewall / ASA

Estimated Time to Complete: 2 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 6 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 5-A.
- This lab will focus strictly on PIX you will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs → Section 5 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Section 6 Configuration Tasks

Transparent Firewall Configuration

Task 6-1

Configure the PIX for transparent firewall mode. Use the management IP address of 56.56.56.55/24. Configure the firewall to allow telnet and SSH for management from R5's interface connected to VLAN 5.

```

pixfirewall(config)#firewall transparent
pixfirewall(config)#ip address 56.56.56.55 255.255.255.0

pixfirewall(config)#interface eth0
pixfirewall(config-if)#no shut
pixfirewall(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)#interface eth1
pixfirewall(config-if)#no shut
pixfirewall(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.

pixfirewall(config)#telnet 56.56.56.5 255.255.255.255 inside
pixfirewall(config)#ssh 56.56.56.5 255.255.255.255 inside

pixfirewall(config)#username cisco password cisco
pixfirewall(config)#aaa authentication ssh console LOCAL

```

→ Verify by testing from R5.

```

R5#ssh -l cisco 56.56.56.55

Password:
Type help or '?' for a list of available commands.
pixfirewall>

```

→ In order to be able to ping from R5 to R6, you can permit ICMP traffic entering the outside interface.

```

pixfirewall#conf t
pixfirewall(config)#access-list OUTSIDE permit icmp any any
pixfirewall(config)#access-group OUTSIDE in interface outside

```


Task 6-2

R6 and R5 are preconfigured for OSPF and EIGRP adjacencies. Configure the PIX to allow these adjacencies to form. Permit only ICMP and the necessary routing protocol traffic to pass through the firewall.

- If you turn on the debug for OSPF hellos, you will see that they are sent out the interfaces, but not received back. If you permit the OSPF traffic to the all OSPF routers group 224.0.0.5 and the host on the other side, the adjacency can form.

```
R6#deb ip ospf hello
OSPF hello events debugging is on
R6#
*Jan 14 06:38:45.244: OSPF: Send hello to 224.0.0.5 area 0 on FastEthernet0/0
from 56.56.56.6
```

```
pixfirewall(config)#access-list OUTSIDE permit ospf host 56.56.56.6
host 224.0.0.5
pixfirewall(config)#access-list OUTSIDE permit ospf host 56.56.56.6
host 56.56.56.5
```

```
pixfirewall(config)#access-list INSIDE permit ospf host 56.56.56.5
host 224.0.0.5
pixfirewall(config)#access-group INSIDE in interface inside
```

```
pixfirewall(config)#access-list INSIDE permit ospf host 56.56.56.5
host 56.56.56.6
```

```
pixfirewall(config)#access-list OUTSIDE permit eigrp host 56.56.56.6
host 224.0.0.10
pixfirewall(config)#access-list OUTSIDE permit eigrp host 56.56.56.6
host 56.56.56.5
```

```
pixfirewall(config)#access-list INSIDE permit eigrp host 56.56.56.5
host 224.0.0.10
pixfirewall(config)#access-list INSIDE permit eigrp host 56.56.56.5
host 56.56.56.6
```

- Verify that you can ping the networks learned.

```
R6#ping 192.168.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/156/176 ms
R6#ping 192.168.54.5
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.54.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/157/176 ms
R6#
```


Task 6-3

Configure an ethertype access list on both interfaces to block BPDUs. All other Ethertypes should be explicitly permitted.

→ Here, we are just configuring a basic ACL and applying to the interfaces.

```
pixfirewall(config)#access-list NOBPDU ether type deny bpu
pixfirewall(config)#access-list NOBPDU ether type permit any
pixfirewall(config)#access-group NOBPDU in interface outside
pixfirewall(config)#access-group NOBPDU in interface inside
```

ASA Contexts

Task 6-4

Configure ASA1 for context "left". Assign IP addresses and security levels to the interfaces as shown in the diagram. Configure the switch to allow traffic to pass on the VLANs shown, for the interface connecting to the ASA. Verify that R1 can ping R7. Do not configure any NAT or STATIC statements for context "left".

→ Start by changing to multiple context mode with the command mode multi. This will require a reload and will clear the configuration.

```
SA1(config)#mode multi
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!!
The old running configuration file will be written to disk0

The admin context configuration will be written to disk0

The new running configuration file was written to disk0
Security context mode: multiple
```

```
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
*** change mode
```

Rebooting....

Booting system, please wait...

- **Make sure that your interfaces are enabled globally, configure the VLANs for the subinterfaces, and then create the context.**

```
ASA1(config)#interface eth0/0
ASA1(config-if)#no shut
ASA1(config-if)#int eth0/1
ASA1(config-if)#no shut
ASA1(config-if)#int eth0/2
ASA1(config-if)#no shut
```

```
ASA1(config)#interface eth0/1.1
ASA1(config-subif)#vlan 101
ASA1(config-subif)#int eth0/1.2
ASA1(config-subif)#vlan 102
ASA1(config-subif)#int eth0/1.7
ASA1(config-subif)#vlan 107
ASA1(config-subif)#int eth0/1.4
ASA1(config-subif)#vlan 104
```

```
ASA1(config)#context left
Creating context 'left'... Done. (2)
ASA1(config-ctx)#config-url disk0:/left.cfg
```

```
WARNING: Could not fetch the URL disk0:/left.cfg
INFO: Creating context with default config
ASA1(config-ctx)#
ASA1(config-ctx)#allocate-interface eth0/1.1
ASA1(config-ctx)#allocate-interface eth0/1.7
```

- **Change to the context, and configure the IP addresses and security levels for the interfaces.**

```
ASA1#changeto context left
ASA1/left#conf t
ASA1/left(config)#interface eth0/1.1
ASA1/left(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA1/left(config-if)#ip address 10.1.1.55 255.255.255.0
```

```
ASA1/left(config-if)#interface eth0/1.3
ASA1/left(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA1/left(config-if)#ip address 10.7.7.55 255.255.255.0
```

- **Add an access-list for the outside interface and apply. To allow the ping through, permit ICMP. To be more granular, you could explicitly specify echo and echo-reply, as well as the source/destination address, but this section is really just looking for basic connectivity.**

```
ASA1/left(config)#access-list leftoutside permit icmp any any
ASA1/left(config)#access-group leftoutside in interface outside
```



```
R1#ping 10.7.7.7
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.7.7.7, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/150/168 ms
```

```
R1#
```

Task 6-5

Configure context “left” for TCP normalization to verify TCP checksums. Do not apply the policy globally.

- **Configuring a service policy on the PIX is very similar to MQC on a router. Start with a class map to match traffic, configure a policy map and then apply to the interface. In order to verify the checksums, configure a TCP map and assign it to the class in the policy map.**

```
ASA1/left(config)#tcp-map MYMAP
```

```
ASA1/left(config-tcp-map)#checksum-verification
```

```
ASA1/left(config)#class MYCLASS
```

```
ASA1/left(config-cmap)#match any
```

```
ASA1/left(config-cmap)#exit
```

```
ASA1/left(config)#policy-map MYPOLICY
```

```
ASA1/left(config-pmap)#class MYCLASS
```

```
ASA1/left(config-pmap-c)#set connection advanced-options MYMAP
```

```
ASA1/left(config)#service-policy MYPOLICY interface inside
```

```
ASA1/left(config)#service-policy MYPOLICY interface outside
```

- **Verify with show service policy.**

```
ASA1/left#show service-policy
```

```
Global policy:
```

```
Service-policy: global_policy
```

```
Class-map: inspection_default
```

```
Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
```

```
Inspect: ftp, packet 0, drop 0, reset-drop 0
```

```
Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
```

```
Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
```

```
Inspect: netbios, packet 0, drop 0, reset-drop 0
```

```
Inspect: rsh, packet 0, drop 0, reset-drop 0
```

```
Inspect: rtsp, packet 0, drop 0, reset-drop 0
```

```
Inspect: skinny, packet 0, drop 0, reset-drop 0
```

```
Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
```

```
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
```

```
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
```

```
Inspect: tftp, packet 0, drop 0, reset-drop 0
```

```
Inspect: sip, packet 0, drop 0, reset-drop 0
```

```
Inspect: xdmcp, packet 0, drop 0, reset-drop 0
```



```

Interface outside:
  Service-policy: MYPOLICY
  Class-map: MYCLASS
    Set connection policy:
    Set connection advanced-options: MYMAP
      Retransmission drops: 0          TCP checksum drops : 0
      Exceeded MSS drops : 0          SYN with data drops: 0
      Out-of-order packets: 0        No buffer drops : 0
      Reserved bit cleared: 0        Reserved bit drops : 0
      IP TTL modified : 0            Urgent flag cleared: 0
      Window varied resets: 0
    TCP-options:
      Selective ACK cleared: 0        Timestamp cleared : 0
      Window scale cleared : 0
      Other options cleared: 0
      Other options drops: 0

Interface inside:
  Service-policy: MYPOLICY
  Class-map: MYCLASS
    Set connection policy:
    Set connection advanced-options: MYMAP
      Retransmission drops: 0          TCP checksum drops : 0
      Exceeded MSS drops : 0          SYN with data drops: 0
      Out-of-order packets: 0        No buffer drops : 0
      Reserved bit cleared: 0        Reserved bit drops : 0
      IP TTL modified : 0            Urgent flag cleared: 0
      Window varied resets: 0
    TCP-options:
      Selective ACK cleared: 0        Timestamp cleared : 0
      Window scale cleared : 0
      Other options cleared: 0
      Other options drops: 0

ASA1/left#

```

Task 6-6

Configure ASA2 for context "right". Assign IP addresses to the interfaces as shown in the diagram. Configure the switch to allow traffic to pass on the VLANs shown, for the interface connecting to the ASA. Verify that R2 can ping R4.

- **Make sure to read the whole lab. Since we are configuring failover in the next section, it is easier to just create the context on ASA1 and then let the failover handle the configuration replication.**

```

ASA1(config)#context right
Creating context 'right'... Done. (3)
ASA1(config-ctx)#config-url disk0:/right.cfg

WARNING: Could not fetch the URL disk0:/right.cfg
INFO: Creating context with default config
ASA1(config-ctx)#
ASA1(config)#context right
ASA1(config-ctx)#allocate eth0/1.2
ASA1(config-ctx)#allocate eth0/1.4

ASA1(config)#changeto context right
ASA1/right(config)#interface eth0/1.2
ASA1/right(config-if)#ip address 10.2.2.55 255.255.255.0

```



```

ASA1/right(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA1/right(config-if)#interface eth0/1.4
ASA1/right(config-if)#ip address 10.4.4.55 255.255.255.0
ASA1/right(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA1/right(config-if)#

ASA1/right(config-if)#access-list rightoutside permit icmp any any
ASA1/right(config)#access-group rightoutside in interface outside

```

Task 6-7

R2 and R4 are preconfigured for a BGP peering. Make sure that this peering is allowed to form without adjusting the configuration of R2 or R4.

- There are a few things to watch for here. By default, the pix will randomize the TCP sequence numbers for traffic. Since the MD5 hash uses the sequence number, the hash fails at the other end. In order to work around this, the ASA can be configured to leave the sequence numbers alone with the "norandomseq" option on a static translation. If the peering is established inside to outside, the ASA will pass traffic normally. If the peering is initiated by the router on the outside, it will need to be permitted in the ACL on the outside interface. The source TCP port will be greater than 1024, and the destination port will be 179.

```

ASA1/right(config)#access-list rightoutside permit tcp host 10.2.2.2
gt 1024 host 10.4.4.4 eq 179
ASA1/right(config)#static (inside,outside) 10.4.4.4 10.4.4.4 netmask
255.255.255.255 norandom

```

- In addition, the ASA treats the TCP packet a little differently. By default, some of the TCP options that were allowed through in earlier PIX versions are now removed. This includes TCP option 19, which is the MD5 Signature option. As a result, the router on the other side of the firewall may see a message similar to the one shown below.

```

*Jan 14 03:29:21.407: %TCP-6-BDAUTH: No MD5 digest from 10.2.2.2(18652) to
10.4.4.4(179)

```

- In order to work around this, a TCP map can be configured to allow option 19. You may need to remove the default global policy before applying the new policy.

```

ASA1/right(config)#tcp-map FIXBGP
ASA1/right(config-tcp-map)#tcp-options range 19 19 allow
ASA1/right(config-tcp-map)#exit
ASA1/right(config)#class-map MYBGPFIX
ASA1/right(config-cmap)#match port tcp eq 179
ASA1/right(config-cmap)#exit
ASA1/right(config)#policy-map BGPPOLICY
ASA1/right(config-pmap)#class MYBGPFIX
ASA1/right(config-pmap-c)#set connection advanced-options FIXBGP

ASA1/right(config)#service-policy BGPPOLICY global
ERROR: Policy map global_policy is already configured as a service policy
ASA1/right(config)#no service-policy global_policy global
ASA1/right(config)#service-policy BGPPOLICY global

```


Failover

Task 6-8

If ASA1 fails, ASA2 should take over for context 'left'. If ASA2 fails, ASA1 should take over for context 'right'. Configure the failover as LAN-based, using interface Eth0/2 on both devices. Verify by shutting down the port on the switch, connected to each ASA. Failover should also be stateful. Configure the standby addresses to be .56 on the respective subnets. The inside and outside interfaces should NOT show us "Not-Monitored" or "waiting" in the output of 'show failover', they should show up as "Normal".

→ **Configure the standby addresses for the failover in the individual contexts.**

```
ASA1/left(config)#int eth0/1.1
ASA1/left(config-if)#ip address 10.1.1.55 255.255.255.0 standby
10.1.1.56
ASA1/left(config-if)#int eth0/1.7
ASA1/left(config-if)#ip address 10.7.7.55 255.255.255.0 standby
10.7.7.56
ASA1/left(config)#changeto cont right
ASA1/right(config)#int eth0/1.2
ASA1/right(config-if)#ip address 10.2.2.55 255.255.255.0 standby
10.2.2.56
ASA1/right(config-if)#int eth0/1.4
ASA1/right(config-if)#ip address 10.4.4.55 255.255.255.0 standby
10.4.4.56

ASA1/right#changeto system
ASA1(config)#interface eth0/2
ASA1(config-if)#description LAN Failover/State link

ASA1(config)#failover lan unit primary
ASA1(config)#failover lan interface failoverint eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its sub-
interfaces
ASA1(config)#failover link failoverint eth0/2
ASA1(config)#failover interface ip failoverint 55.55.55.55
255.255.255.0 standby 55.55.55.56

ASA1(config)#failover group 1
ASA1(config-fover-group)#primary
ASA1(config-fover-group)#preempt
ASA1(config-fover-group)#exit
ASA1(config)#failover group 2
ASA1(config-fover-group)#secondary
ASA1(config-fover-group)#preempt

ASA1(config)#context left
ASA1(config-ctx)#join-failover-group 1
ASA1(config-ctx)#context right
ASA1(config-ctx)#join-failover-group 2

ASA1(config)#failover
```


→ Check the output of “show failover”.

```

ASA1(config)#show failover
Failover On
Failover unit Primary
Failover LAN Interface: failoverint Ethernet0/2 (Configuration incomplete)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Version: Ours 7.2(2), Mate Unknown
Last Failover at: 18:35:24 UTC Jan 22 2007
  This host: Primary - Disabled
    Active time: 0 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
      left Interface outside (10.1.1.55): Normal (Not-Monitored)
      left Interface inside (10.7.7.55): Normal (Not-Monitored)
      right Interface outside (10.2.2.55): Normal (Not-Monitored)
      right Interface inside (10.4.4.55): Normal (Not-Monitored)
    slot 1: empty
  Other host: Secondary - Not Detected
    Active time: 0 (sec)
    slot 0: empty
      left Interface outside (10.1.1.56): Unknown (Not-Monitored)
      left Interface inside (10.7.7.56): Unknown (Not-Monitored)
      right Interface outside (10.2.2.56): Unknown (Not-
Monitored)
      right Interface inside (10.4.4.56): Unknown (Not-Monitored)
    slot 1: empty

Stateful Failover Logical Update Statistics
Link : failoverint Ethernet0/2 (Configuration incomplete)
Stateful Obj      xmit      xerr      rcv      rerr
General           0          0          0          0
sys cmd           0          0          0          0
up time           0          0          0          0
RPC services      0          0          0          0
TCP conn          0          0          0          0
UDP conn          0          0          0          0
ARP tbl           0          0          0          0
Xlate_Timeout     0          0          0          0

Logical Update Queue Information
                  Cur      Max      Total
Recv Q:          0        0        0
Xmit Q:           0        0        0
ASA1(config)#

```

→ By default, physical interfaces will be monitored, subinterfaces will not. In order to monitor the subinterfaces, use the command ‘monitor-interface’ under the contexts.

```

ASA1(config)#changeto cont right
ASA1/right(config)#monitor-interface ?

configure mode commands/options:
Current available interface(s):
  inside  Name of interface Ethernet0/1.4
  outside Name of interface Ethernet0/1.2
ASA1/right(config)#monitor-interface inside
ASA1/right(config)#monitor-interface outside

```



```
ASA1(config)#changeto context left
ASA1/left(config)#monitor-interface inside
ASA1/left(config)#monitor-interface outside
```

- On the secondary unit, we just need to configure the failover link, configure the ASA as secondary, and enable failover.

```
ASA2(config)#failover lan interface failoverint eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its sub-
interfaces
ASA2(config)#failover interface ip failoverint 55.55.55.55
255.255.255.0 standby 55.55.55.56
ASA2(config)#failover lan unit secondary
ASA2(config)#failover

ASA2(config)#int eth0/2
ASA2(config-if)#no shut
```

- You may see an error message on the console display:

```
ASA1#Mate's operating mode (Single) is not compatible with my mode
(Multi). Failover will be disabled.
```

- Configure ASA2 for multiple mode, and allow it to reload. After ASA2 comes back online, reenables failover, and ASA2 will replicate the configuration. Make sure to enable failover on ASA1 FIRST.

```
ASA2(config)#mode multi
```

```
ASA1(config)#failover
```

```
ASA2(config)#failover
ASA2(config)#.
```

```

    Detected an Active mate
Beginning configuration replication from mate.
Removing context 'admin' (1)... Done
INFO: Admin context is required to get the interfaces
Creating context 'admin'... Done. (2)

WARNING: Skip fetching the URL disk0:/admin.cfg
INFO: Creating context with default config
INFO: Admin context will take some time to come up .... please wait.
Creating context 'left'... Done. (3)

WARNING: Skip fetching the URL disk0:/left.cfg
INFO: Creating context with default config
Creating context 'right'... Done. (4)

WARNING: Skip fetching the URL disk0:/right.cfg
INFO: Creating context with default config
End configuration replication from mate.
```

```
Group 2 No Response from Mate
```

```
Group 1 Detected Active mate
```


→ On ASA2, the output should show the failover status.

```

ASA1#show failover
Failover On
Failover unit Secondary
Failover LAN Interface: failoverint Ethernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Group 1 last failover at: 21:22:56 UTC Jan 22 2007
Group 2 last failover at: 21:35:22 UTC Jan 22 2007

This host:      Secondary
Group 1         State:          Standby Ready
                Active time:    0 (sec)
Group 2         State:          Active
                Active time:    424 (sec)

slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
  left Interface outside (10.1.1.56): Normal
  left Interface inside (10.7.7.56): Normal
  right Interface outside (10.2.2.55): Normal
  right Interface inside (10.4.4.55): Normal
slot 1: empty

Other host:     Primary
Group 1         State:          Active
                Active time:    2080 (sec)
Group 2         State:          Standby Ready
                Active time:    1658 (sec)

slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
  left Interface outside (10.1.1.55): Normal
  left Interface inside (10.7.7.55): Normal
  right Interface outside (10.2.2.56): Normal
  right Interface inside (10.4.4.56): Normal
slot 1: empty

Stateful Failover Logical Update Statistics
Link : failoverint Ethernet0/2 (up)
Stateful Obj    xmit      xerr      rcv       rerr
General         114        0        133        0
sys cmd         111        0        111        0
up time         0          0         0         0
RPC services    0          0         0         0
TCP conn        2          0        14         0
UDP conn        0          0         0         0
ARP tbl         1          0         8         0
Xlate_Timeout   0          0         0         0

Logical Update Queue Information
                Cur      Max      Total
Recv Q:         0        1       133
Xmit Q:         0        1       114

```

ASA1#

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

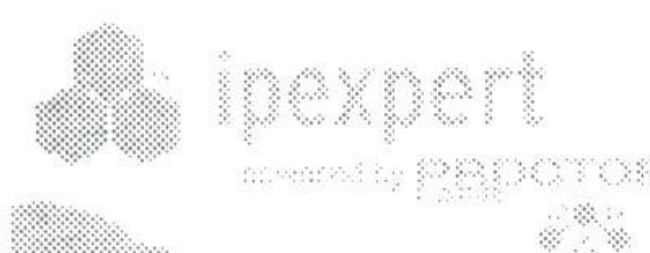
This page left intentionally blank.

Section 7: IPSec

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 7 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 7-A.
- This lab will focus strictly on IPSec. You will need to pre-configure the network with the base IP Addressing, VLAN and PIX configuration. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 7 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Section 7 Configuration Tasks

Router-to-Router IPSec Tunnel

Task 7-1

Create a static mapping for R5 as 192.1.24.5.

- You need to put a mapping statement for the PIX.

```
pixfirewall(config)#static (DMZ5,outside) 192.1.24.5 10.5.5.5 netmask
255.255.255.255 0 0
```

Task 7-2

You are allowed a static route on R2.

- You need to make sure that R2 can reach R5's loopback. Therefore, you need to use the following static route:

```
r2(config)#ip route 5.0.0.0 255.0.0.0 192.1.24.10
```

Task 7-3

Configure an IPSec tunnel encrypting traffic from the Loopbacks behind R2 and R5.

- First, configure the access list between R2 and R5's loopback. Then create the crypto map and lastly apply it to the interface as shown below:

```
r2(config)#access-list 101 permit ip 2.0.0.0 0.255.255.255 5.0.0.0
0.255.255.255
r2(config)#crypto map secure 10 ipsec-isakmp
r2(config-crypto-map)#set peer 192.1.24.5
r2(config-crypto-map)#set transform-set secure
r2(config-crypto-map)#match address 101
r2(config-crypto-map)#interface FastEthernet1/0
r2(config-if)#crypto map secure
R5(config)#access-list 101 permit ip 5.0.0.0 0.255.255.255 2.0.0.0
0.255.255.255
R5(config)#crypto map secure 10 ipsec-isakmp
R5(config-crypto-map)#set peer 192.1.24.2
R5(config-crypto-map)#set transform-set secure
```



```
R5(config-crypto-map)#match address 101
R5(config-crypto-map)#interface FastEthernet0/0
R5(config-if)#crypto map secure
```

Task 7-4

Use R2 E 0/0 and the static translation of R5 as the Tunnel Endpoints.

- As shown above, the peer address is 192.1.24.2 and 192.1.24.5.

Task 7-5

Use the following Parameters for the Tunnel:

- Authentication – Pre-shared
- Group – 2
- Key – ccie
- Transform-set – esp-des and esp-md5-hmac
- Interesting Traffic – Network 2.0.0.0 to Network 5.0.0.0 and vice versa.
- The following can define the ISAKMP policy that is required above:

```
r2(config)#crypto isakmp policy 10
r2(config-isakmp)#authentication pre-share
r2(config-isakmp)#group 2
r2(config-isakmp)#crypto isakmp key ccie address 192.1.24.5
```

Task 7-6

Allow the appropriate entries through the PIX Firewall. Use minimum number of entries in the PIX access-list.

- Please be sure that the ISAKMP traffic is allowed.

```
pixfirewall(config)#access-list infilter permit udp host 192.1.24.2
host 192.1.24.5 eq isakmp
pixfirewall(config)#access-list infilter permit udp host 192.1.24.2
host 192.1.24.5 eq 4500
```

- The most challenging part for this exercise is that it is passing through the PIX firewall. Therefore, it is necessary to check that whether ISAKMP and IPSec traffic are allowed to go through the PIX firewall.
- To allow IPSec NAT transparency, you need to permit UDP 4500 through the firewall.
- We used the debug command “debug crypto isakmp” and “debug crypto ipsec” and arrived with the following output:

→ **First we ping from R5 to R2's loopback to start the channel.**

R5#**ping 2.2.2.2 source 5.5.5.5**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

Packet sent with a source address of 5.5.5.5

```
*Dec 25 17:22:23: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.5.5.5, remote= 192.1.24.2,
  local_proxy= 5.0.0.0/255.0.0.0/0/0 (type=4),
  remote_proxy= 2.0.0.0/255.0.0.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x7A130E44(2048069188), conn_id= 0, keysize= 0, flags= 0x400A
*Dec 25 17:22:23: ISAKMP: received ke message (1/1)
*Dec 25 17:22:23: ISAKMP: set new node 0 to QM_IDLE
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): sitting IDLE. Starting QM immediately
(QM_IDLE)
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):beginning Quick Mode exchange, M-ID of -
921870906
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.2 my_port
4500 peer_port 4500 (I) QM_IDLE
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):Node -921870906, Input =
IKE_MSG_INTERNAL, IKE_INIT_QM
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY New State =
IKE_QM_I_QM1
*Dec 25 17:22:23: ISAKMP (0:134217729): received packet from 192.1.24.2 dport
4500 sport 4500 Global (I) QM_IDLE
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = -
921870906
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): processing SA payload. message ID = -
921870906
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1
*Dec 25 17:22:23: ISAKMP: transform 1, ESP_DES
*Dec 25 17:22:23: ISAKMP: attributes in transform:
*Dec 25 17:22:23: ISAKMP: encaps is 3 (Tunnel-UDP)
*Dec 25 17:22:23: ISAKMP: SA life type in seconds
*Dec 25 17:22:23: ISAKMP: SA life duration (basic) of 3600
*Dec 25 17:22:23: ISAKMP: SA life type in kilobytes
*Dec 25 17:22:23: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Dec 25 17:22:23: ISAKMP: authenticat.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms (There is
only one packet lost during the tunnel establishment stage)
R5#or is HMAC-MD5
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):atts are acceptable.
*Dec 25 17:22:23: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 10.5.5.5, remote= 192.1.24.2,
  local_proxy= 5.0.0.0/255.0.0.0/0/0 (type=4),
  remote_proxy= 2.0.0.0/255.0.0.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x400
*Dec 25 17:22:23: Crypto mapdb : proxy_match
  src addr      : 5.0.0.0
  dst addr      : 2.0.0.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = -
921870906
```



```

*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): processing ID payload. message ID = -
921870906
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): processing ID payload. message ID = -
921870906
*Dec 25 17:22:23: ISAKMP: Locking peer struct 0x47395C20, IPSEC refcount 1
for for stuff_ke
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): Creating IPsec SAs
*Dec 25 17:22:23: inbound SA from 192.1.24.2 to 10.5.5.5 (f/i) 0/ 0
(proxy 2.0.0.0 to 5.0.0.0)
*Dec 25 17:22:23: has spi 0x7A130E44 and conn_id 0 and flags 400
*Dec 25 17:22:23: lifetime of 3600 seconds
*Dec 25 17:22:23: lifetime of 4608000 kilobytes
*Dec 25 17:22:23: has client flags 0x10
*Dec 25 17:22:23: outbound SA from 10.5.5.5 to 192.1.24.2 (f/i) 0/0
(proxy 5.0.0.0 to 2.0.0.0)
*Dec 25 17:22:23: has spi 1387719574 and conn_id 0 and flags 408
*Dec 25 17:22:23: lifetime of 3600 seconds
*Dec 25 17:22:23: lifetime of 4608000 kilobytes
*Dec 25 17:22:23: has client flags 0x10
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.2 my_port
4500 peer_port 4500 (I) QM_IDLE
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):deleting node -921870906 error FALSE
reason "No Error"
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):Node -921870906, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Dec 25 17:22:23: ISAKMP:(0:1:SW:1):Old State = IKE_QM_I_QM1 New State =
IKE_QM_PHASE2_COMPLETE
*Dec 25 17:22:23: IPSEC(key_engine): got a queue event with 2 kei messages
*Dec 25 17:22:23: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.5.5.5, remote= 192.1.24.2,
local_proxy= 5.0.0.0/255.0.0.0/0/0 (type=4),
remote_proxy= 2.0.0.0/255.0.0.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
lifedur= 3600s and 4608000kb,
spi= 0x7A130E44(2048069188), conn_id= 0, keysize= 0, flags= 0x400
*Dec 25 17:22:23: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.5.5.5, remote= 192.1.24.2,
local_proxy= 5.0.0.0/255.0.0.0/0/0 (type=4),
remote_proxy= 2.0.0.0/255.0.0.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel-UDP),
lifedur= 3600s and 4608000kb,
spi= 0x52B6EB96(1387719574), conn_id= 0, keysize= 0, flags= 0x408
*Dec 25 17:22:23: Crypto mapdb : proxy_match
src addr : 5.0.0.0
dst addr : 2.0.0.0
protocol : 0
src port : 0
dst port : 0
*Dec 25 17:22:23: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and 192.1.24.2
*Dec 25 17:22:23: IPsec: Flow_switching Allocated flow for sibling 80000003
*Dec 25 17:22:23: IPSEC(policy_db_add_ident): src 5.0.0.0, dest 2.0.0.0,
dest_port 0

*Dec 25 17:22:23: ISAKMP: Locking peer struct 0x47395C20, IPSEC refcount 2
for from create_transforms

```



```
*Dec 25 17:22:23: IPSEC(create_sa): sa created,
(sa) sa_dest= 10.5.5.5, sa_proto= 50,
sa_spi= 0x7A130E44(2048069188),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3002
*Dec 25 17:22:23: IPSEC(create_sa): sa created,
(sa) sa_dest= 192.1.24.2, sa_proto= 50,
sa_spi= 0x52B6EB96(1387719574),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3001
*Dec 25 17:22:23: ISAKMP: Unlocking IPSEC struct 0x47395C20 from
create_transforms, count 1
```

→ The tunnel has been established. Therefore, the ping goes through.

```
R5#ping 2.2.2.2 source 5.5.5.5
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 5.5.5.5
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

→ Check the IPSec SA information below. It has the source and destination address, as well as the peer and transform info.

```
R5#show crypto ipsec sa
```

```
interface: FastEthernet0/0
  Crypto map tag: secure, local addr 10.5.5.5

  protected vrf: (none)
  local ident (addr/mask/prot/port): (5.0.0.0/255.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (2.0.0.0/255.0.0.0/0/0)
  current_peer 192.1.24.2 port 4500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

  local crypto endpt.: 10.5.5.5, remote crypto endpt.: 192.1.24.2
  path mtu 1500, ip mtu 1500
  current outbound spi: 0x52B6EB96(1387719574)

inbound esp sas:
  spi: 0x7A130E44(2048069188)
    transform: esp-des esp-md5-hmac ,
    in use settings = {Tunnel UDP-Encaps, }
    conn id: 3002, flow_id: NETGX:2, crypto map: secure
    sa timing: remaining key lifetime (k/sec): (4493257/3545)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:
```



```

outbound esp sas:
spi: 0x52B6EB96(1387719574)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 3001, flow_id: NETGX:1, crypto map: secure
sa timing: remaining key lifetime (k/sec): (4493257/3543)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcp sas:
```

- This command can quickly check what channels there are.

```
R5#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	10.5.5.5	set	HMAC_SHA+DES_56_CB	0	0
3001	FastEthernet0/0	10.5.5.5	set	DES+MD5	9	0
3002	FastEthernet0/0	10.5.5.5	set	DES+MD5	0	9

Router-to-Router using a GRE Tunnel

Task 7-7

Create a GRE tunnel from R2 to R4. Use 10.24.24.0 /24 as the tunnel address.

- It is very simple to create two tunnel interfaces with the source and destination address as 192.1.24.2 and 192.1.24.4.

```

r2(config)#interface Tunnel24
r2(config-if)#ip address 10.24.24.2 255.255.255.0
r2(config-if)#tunnel source 192.1.24.2
r2(config-if)#tunnel destination 192.1.24.4

```

```

r4(config)#interface Tunnel24
r4(config-if)#ip address 10.24.24.4 255.255.255.0
r4(config-if)#tunnel source 192.1.24.4
r4(config-if)#tunnel destination 192.1.24.2

```

Task 7-8

Create a loopback on R2 and R4 as follows:

- R2 Loopback: 22.2.2.2 /8
- R4 Loopback: 44.4.4.4 /8

- Once again, this is simple to create a loopback address.

```

r2(config)#interface Loopback0
r2(config-if)#ip address 2.2.2.2 255.0.0.0

```

```

r4(config)#interface Loopback0
r4(config-if)#ip address 4.4.4.4 255.0.0.0

```


Task 7-9

Run EIGRP in AS 24 as the routing protocol to route the GRE networks. Advertise the new loopbacks on R2 and R4 in EIGRP 24.

→ The EIGRP is running between the two loopback with the following commands.

```
r2(config)#router eigrp 24
r2(config-router)#network 10.24.24.0 0.0.0.255
r2(config-router)#network 22.0.0.0
r2(config-router)#no auto-summary

r4(config)#router eigrp 24
r4(config-router)#network 10.24.24.0 0.0.0.255
r4(config-router)#network 44.0.0.0
r4(config-router)#no auto-summary
```

Task 7-10

Configure a IPSec tunnel between R2 and R4 using the following parameters:

- Authentication: Pre-shared
- Group: 2
- Key: ccie
- Transform-set: esp-des
- Mode: transport
- Interesting Traffic: Any traffic that goes over the GRE tunnel between R2 and R4 including the EIGRP traffic.

→ The following commands define the ISAKMP policy:

```
r2(config)#access-list 124 permit gre host 192.1.24.2 host 192.1.24.4
r2(config)#crypto isakmp policy 10
r2(config-isakmp)#authentication pre-share
r2(config-isakmp)#group 2
r2(config-isakmp)#crypto isakmp key ccie address 192.1.24.4
r2(config)#crypto ipsec transform-set secure2 esp-des
r2(cfg-crypto-trans)#mode transport
r2(cfg-crypto-trans)#crypto map secure 20 ipsec-isakmp
r2(config-crypto-map)#set peer 192.1.24.4
r2(config-crypto-map)#set transform-set secure2
r2(config-crypto-map)#match address 124
r2(config-crypto-map)#interface FastEthernet1/0
r2(config-if)#crypto map secure

r4(config)#access-list 142 permit gre host 192.1.24.4 host 192.1.24.2
r4(config)#crypto map secure 10 ipsec-isakmp
r4(config-crypto-map)#set peer 192.1.24.2
r4(config-crypto-map)#set transform-set secure
r4(config-crypto-map)#match address 142
r4(config-crypto-map)#crypto isakmp policy 10
r4(config-isakmp)#authentication pre-share
r4(config-isakmp)#group 2
r4(config-isakmp)#crypto isakmp key ccie address 192.1.24.2
r4(config)#crypto ipsec transform-set secure esp-des
```



```

r4(cfg-crypto-trans)#mode transport
r4(cfg-crypto-trans)#interface FastEthernet0/0
r4(config-if)#crypto map secure

```

- The GRE tunnel uses IPSec as shown in the access list. Then the crypto engine shows that the IPSec tunnel is activated. If you want to confirm it, you can clear the crypto sa and then observe the establishment of the tunnel again.

```

R2#show ip access-lists
Extended IP access list 101
  10 permit ip 2.0.0.0 0.255.255.255 5.0.0.0 0.255.255.255 (10 matches)
Extended IP access list 124
  10 permit gre host 192.1.24.2 host 192.1.24.4 (171 matches)

```

```
R2#show crypto engine connections active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet1/0	192.1.24.2	set	HMAC_SHA+DES_56_CB	0	0
3002	FastEthernet1/0	192.1.24.2	set	DES	0	13
3003	FastEthernet1/0	192.1.24.2	set	DES	13	0

```
R2#show crypto ipsec sa
```

```

interface: FastEthernet1/0
  Crypto map tag: secure, local addr 192.1.24.2

protected vrf: (none)
local ident (addr/mask/prot/port): (2.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (5.0.0.0/255.0.0.0/0/0)
current_peer 192.1.24.5 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 192.1.24.2, remote crypto endpt.: 192.1.24.5
  path mtu 1500, ip mtu 1500
  current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (192.1.24.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.1.24.4/255.255.255.255/47/0)
current_peer 192.1.24.4 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
  #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14

```



```

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.1.24.2, remote crypto endpt.: 192.1.24.4
path mtu 1500, ip mtu 1500
current outbound spi: 0xEB3B7339(3946541881)

inbound esp sas:
spi: 0x111C7526(287077670)
transform: esp-des ,
in use settings ={Transport, }
conn id: 3002, flow_id: Onboard VPN:2, crypto map: secure
sa timing: remaining key lifetime (k/sec): (4555011/3532)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xEB3B7339(3946541881)
transform: esp-des ,
in use settings ={Transport, }
conn id: 3003, flow_id: Onboard VPN:3, crypto map: secure
sa timing: remaining key lifetime (k/sec): (4555011/3531)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

R4#show ip access-lists

```

Extended IP access list 110
 10 permit ip 4.0.0.0 0.255.255.255 10.2.2.0 0.0.0.255
Extended IP access list 142
 10 permit gre host 192.1.24.4 host 192.1.24.2 (1642 matches)

```

R4#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0
3003	FastEthernet0/0	192.1.24.4	set	DES	18	0
3006	FastEthernet0/0	192.1.24.4	set	DES	0	18

R4#show crypto ipsec sa

```

interface: FastEthernet0/0
Crypto map tag: secure, local addr 192.1.24.4

protected vrf: (none)
local ident (addr/mask/prot/port): (192.1.24.4/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.1.24.2/255.255.255.255/47/0)
current_peer 192.1.24.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 837, #pkts encrypt: 837, #pkts digest: 837

```



```
#pkts decaps: 771, #pkts decrypt: 771, #pkts verify: 771
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 8, #recv errors 0

local crypto endpt.: 192.1.24.4, remote crypto endpt.: 192.1.24.2
path mtu 1500, ip mtu 1500
current outbound spi: 0x111C7526(287077670)

inbound esp sas:
  spi: 0xEB3B7339(3946541881)
    transform: esp-des ,
    in use settings ={Transport, }
    conn id: 3006, flow_id: NETGX:6, crypto map: secure
    sa timing: remaining key lifetime (k/sec): (4581604/3501)
    IV size: 8 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x111C7526(287077670)
    transform: esp-des ,
    in use settings ={Transport, }
    conn id: 3003, flow_id: NETGX:3, crypto map: secure
    sa timing: remaining key lifetime (k/sec): (4581604/3499)
    IV size: 8 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (4.0.0.0/255.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer 192.1.24.10 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```



```

local crypto endpt.: 192.1.24.4, remote crypto endpt.: 192.1.24.10
path mtu 1500, ip mtu 1500
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcg sas:

outbound esp sas:

outbound ah sas:

outbound pcg sas:

```

Router-to-PIX Firewall Tunnel

Task 7-11

Configure an IPSec tunnel encrypting traffic from the 10.2.2.0 network to the 4.0.0.0 network.

→ We need to encrypt all the IP traffic.

```

r4(config)#access-list 110 permit ip 4.0.0.0 0.255.255.255 10.2.2.0
0.0.0.255
r4(config)#crypto isakmp key ccie address 192.1.24.10
r4(config)#crypto ipsec transform-set secure2 esp-des esp-md5-hmac
r4(cfg-crypto-trans)#crypto map secure 20 ipsec-isakmp
r4(config-crypto-map)#set peer 192.1.24.10
r4(config-crypto-map)#set transform-set secure2
r4(config-crypto-map)#match address 110
r4(config-crypto-map)#interface FastEthernet0/0
r4(config-if)#crypto map secure

```

Task 7-12

Use the PIX outside and the R4 E 0/0 as the Tunnel endpoints.

→ The PIX firewall should have these commands to make the tunnel works:

```

pixfirewall(config)#crypto ipsec transform-set secure esp-des esp-
md5-hmac
pixfirewall(config)#crypto map secure 10 match address 1022-4
pixfirewall(config)#crypto map secure 10 set peer 192.1.24.4
pixfirewall(config)#crypto map secure 10 set transform-set secure
pixfirewall(config)#crypto map secure interface outside

```


Task 7-13

Use the following Parameters for the Tunnel:

- Authentication – Pre-shared
- Group – 2
- Key – ccie
- Transform-set – esp-des and ah-md5-hmac
- Interesting Traffic – Network 10.2.2.0 to Network 4.0.0.0 and vice versa.

- You can define the ISAKMP policy with these commands:

```

pixfirewall(config)#crypto isakmp enable outside
pixfirewall(config)#crypto isakmp policy 10
pixfirewall(config-isakmp-policy)#auth pre-share
pixfirewall(config-isakmp-policy)#encr des
pixfirewall(config-isakmp-policy)#hash sha
pixfirewall(config-isakmp-policy)#group 2
pixfirewall(config-isakmp-policy)#lifetime 86400

pixfirewall(config)#tunnel-group 192.1.24.4 type ipsec-l2l
pixfirewall(config)#tunnel-group 192.1.24.4 ipsec-attributes
pixfirewall(config-tunnel-ipsec)#pre-shared-key ccie

```

- You need to be sure and add an entry in to your access-list that you defined for bypassing NAT translation. This entry should define the inside networks as the source and the remote network as the destination. After you have created this access-list, you need to apply it to NAT 0.
- Even if identical to the ACL used in the crypto setup, it must be a different name.

```

pixfirewall(config)#access-list nonat permit ip 10.2.2.0
255.255.255.0 4.0.0.0 255.0.0.0

pixfirewall(config)#nat (inside) 0 access-list nonat

```

Task 7-14

You are allowed a static route on R4 to accomplish this task.

- We need to make sure that we can reach the destination network with the following command:

```

r4(config)#ip route 10.2.2.0 255.255.255.0 192.1.24.10

```

- Originally, the crypto engine command indicates that the tunnel is not up. Then, when I ping it, it is up, as seen by the “Debug crypto isakmp” and “debug crypto ipsec” commands. The debug commands contain the source and destination address.

```

R4#show crypto engine connection active

```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0
3	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0

R4#ping 10.2.2.1 source 4.4.4.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

```
*Dec 25 05:05:19: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 192.1.24.4, remote= 192.1.24.10,
  local_proxy= 4.0.0.0/255.0.0.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0xFDBEAFA7(4257132455), conn_id= 0, keysize= 0, flags= 0x400A
*Dec 25 05:05:19: ISAKMP: received ke message (1/1)
*Dec 25 05:05:19: ISAKMP: set new node 0 to QM_IDLE
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): sitting IDLE. Starting QM immediately
(QM_IDLE)
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):beginning Quick Mode exchange, M-ID of -
320828851
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): sending packet to 192.1.24.10 my_port
500 peer_port 500 (I) QM_IDLE
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):Node -320828851, Input =
IKE_MESG_INTERNAL, IKE_INIT_QM
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):Old State = IKE_QM_READY New State =
IKE_QM_I_QM1
*Dec 25 05:05:19: ISAKMP (0:134217731): received packet from 192.1.24.10
dport 500 sport 500 Global (I) QM_IDLE
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): processing HASH payload. message ID = -
320828851
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): processing SA payload. message ID = -
320828851
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):Checking IPsec proposal 1
*Dec 25 05:05:19: ISAKMP: transform 1, ESP_DES
*Dec 25 05:05:19: ISAKMP: attributes in transform:
*Dec 25 05:05:19: ISAKMP: encaps is 1 (Tunnel)
*Dec 25 05:05:19: ISAKMP: SA life type in seconds
*Dec 25 05:05:19: ISAKMP: SA life duration (basic) of 3600
*Dec 25 05:05:19: ISAKMP: SA life type in kilobytes
*Dec 25 05:05:19: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Dec 25 05:05:19: ISAKMP: authenticator is HMAC-MD5
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):atts are acceptable.
*Dec 25 05:05:19: IPSEC!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
R4#(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 192.1.24.4, remote= 192.1.24.10,
  local_proxy= 4.0.0.0/255.0.0.0/0/0 (type=4),
  remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Dec 25 05:05:19: Crypto mapdb : proxy_match
  src addr      : 4.0.0.0
  dst addr      : 10.2.2.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): processing NONCE payload. message ID = -
320828851
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): processing ID payload. message ID = -
320828851
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): processing ID payload. message ID = -
320828851
```



```

*Dec 25 05:05:19: ISAKMP: Locking peer struct 0x47351B60, IPSEC refcount 1
for for stuff_ke
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): Creating IPsec SAs
*Dec 25 05:05:19:      inbound SA from 192.1.24.10 to 192.1.24.4 (f/i)  0/
0
      (proxy 10.2.2.0 to 4.0.0.0)
*Dec 25 05:05:19:      has spi 0xFDBEAFA7 and conn_id 0 and flags 2
*Dec 25 05:05:19:      lifetime of 3600 seconds
*Dec 25 05:05:19:      lifetime of 4608000 kilobytes
*Dec 25 05:05:19:      has client flags 0x0
*Dec 25 05:05:19:      outbound SA from 192.1.24.4 to 192.1.24.10 (f/i)
0/0
      (proxy 4.0.0.0 to 10.2.2.0)
*Dec 25 05:05:19:      has spi 211559672 and conn_id 0 and flags A
*Dec 25 05:05:19:      lifetime of 3600 seconds
*Dec 25 05:05:19:      lifetime of 4608000 kilobytes
*Dec 25 05:05:19:      has client flags 0x0
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1): sending packet to 192.1.24.10 my_port
500 peer_port 500 (I) QM_IDLE
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):deleting node -320828851 error FALSE
reason "No Error"
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):Node -320828851, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Dec 25 05:05:19: ISAKMP:(0:3:SW:1):Old State = IKE_QM_I_QM1 New State =
IKE_QM_PHASE2_COMPLETE
*Dec 25 05:05:19: IPSEC(key_engine): got a queue event with 2 kei messages
*Dec 25 05:05:19: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 192.1.24.4, remote= 192.1.24.10,
      local_proxy= 4.0.0.0/255.0.0.0/0/0 (type=4),
      remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
      protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
      lifedur= 3600s and 4608000kb,
      spi= 0xFDBEAFA7(4257132455), conn_id= 0, keysize= 0, flags= 0x2
*Dec 25 05:05:19: IPSEC(initialize_sas): ,
      (key eng. msg.) OUTBOUND local= 192.1.24.4, remote= 192.1.24.10,
      local_proxy= 4.0.0.0/255.0.0.0/0/0 (type=4),
      remote_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
      protocol= ESP, transform= esp-des esp-md5-hmac (Tunnel),
      lifedur= 3600s and 4608000kb,
      spi= 0xC9C24F8(211559672), conn_id= 0, keysize= 0, flags= 0xA
*Dec 25 05:05:19: Crypto mapdb : proxy_match
      src addr      : 4.0.0.0
      dst addr      : 10.2.2.0
      protocol      : 0
      src port      : 0
      dst port      : 0
*Dec 25 05:05:19: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and 192.1.24.10
*Dec 25 05:05:19: IPsec: Flow_switching Allocated flow for sibling 8000000A
*Dec 25 05:05:19: IPSEC(policy_db_add_ident): src 4.0.0.0, dest 10.2.2.0,
dest_port 0

*Dec 25 05:05:19: ISAKMP: Locking peer struct 0x47351B60, IPSEC refcount 2
for from create_transforms
*Dec 25 05:05:19: IPSEC(create_sa): sa created,
      (sa) sa_dest= 192.1.24.4, sa_proto= 50,
      sa_spi= 0xFDBEAFA7(4257132455),
      sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3005
*Dec 25 05:05:19: IPSEC(create_sa): sa created,
      (sa) sa_dest= 192.1.24.10, sa_proto= 50,
      sa_spi= 0xC9C24F8(211559672),
      sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3001

```



```
*Dec 25 05:05:19: ISAKMP: Unlocking IPSEC struct 0x47351B60 from
create_transforms, count 1
```

→ After the establishment of the IPsec tunnel, we can ping successfully.

```
R4#ping 10.2.2.1 source 4.4.4.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 4.4.4.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

The command below shows that IPsec tunnel is being established.

```
R4#show crypto engine connection active
```

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
2	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0
3	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0
3001	FastEthernet0/0	192.1.24.4	set	DES+MD5	9	0
3004	FastEthernet0/0	192.1.24.4	set	DES	11	0
3005	FastEthernet0/0	192.1.24.4	set	DES+MD5	0	9
3006	FastEthernet0/0	192.1.24.4	set	DES	0	12

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

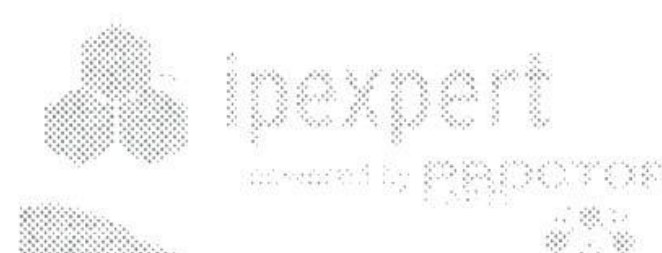
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 7B: DMVPN

Estimated Time to Complete: 1 Hour

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 7B Pre-Lab Setup

- Physically connect and configure your network according to Diagram 6-B.
- This lab will focus strictly on IPsec. You will need to pre-configure the network with the base IP Addressing, VLAN and PIX configuration. You will find these configurations in the “Initial Configurations” subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs → Section 7B → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the “MY CONFIGS” area of your *www.IPexpert.com Member's Area*.

Section 7B Configuration Tasks

DMVPN for R2, R5, R6

Task 7-15

Create a tunnel with the network of 100.0.0.x/24 where x is the router number.

- **Basic tunnel configuration just requires configuring the source and the address on the tunnel. Since we are using a multipoint GRE tunnel, do not specify a destination. There are a few parameters that should be the same on the devices, including NHRP network-id, holdtime, and key.**

```
R6(config)#int tun100
R6(config-if)#ip address 100.0.0.6 255.255.255.0
R6(config-if)#tun source ser0/1/0
R6(config-if)#tun mode gre multipoint
```

```
R6(config-if)#ip nhrp map multicast dynamic
R6(config-if)#ip nhrp network-id 1
R6(config-if)#ip nhrp holdtime 300
R6(config-if)#tunnel key 12345
```

- **The configuration on the spokes will be similar. The spokes include a mapping to the hub with the NHRP map command to map the hub NBMA address to the physical address for the hub. The spokes also include a mapping for multicast, telling them to send it to the tunnel address of the hub, and a mapping to the hub as a next-hop server**

```
R2(config)#int tun100
R2(config-if)#ip address 100.0.0.2 255.255.255.0
R2(config-if)#tun source ser0/1/0
R2(config-if)#tun mode gre multipoint
R2(config-if)#ip nhrp network-id 1
R2(config-if)#ip nhrp holdtime 300
R2(config-if)#tunnel key 12345
R2(config-if)#ip nhrp map 100.0.0.6 150.50.99.6
R2(config-if)#ip nhrp map multicast 150.50.99.6
R2(config-if)#ip nhrp nhs 100.0.0.6
```



```
R5(config)#int tun100
R5(config-if)#ip address 100.0.0.5 255.255.255.0
R5(config-if)#tun source ser0/1/0
R5(config-if)#tun mode gre multi
R5(config-if)#ip nhrp network-id 1
R5(config-if)#ip nhrp holdtime 300
R5(config-if)#tunnel key 12345
R5(config-if)#ip nhrp map multicast 150.50.99.6
R5(config-if)#ip nhrp nhs 100.0.0.6
R5(config-if)#ip nhrp map 100.0.0.6 150.50.99.6
```

Task 7-16

Activate the Frame Relay interfaces should have IP address 150.50.99.x/24.

- **Make sure that the serial interfaces are not shut down. They should be configured via the initial configuration files.**
- **At this point you should have active tunnels, and should be able to ping the other tunnel interfaces.**

Task 7-17

Running a separate EIGRP process for the tunnel interface.

- **In this particular case, there is not an underlying routing protocol running in the topology. With DMVPN, you want a separate routing process as the encryption process uses routing.**
- **Configure the tunnel interfaces and the Ethernet interfaces for EIGRP.**

```
R2(config)#router eigrp 7
R2(config-router)#network 100.0.0.0 0.0.0.255
R2(config-router)#network 192.1.24.0 0.0.0.255
R2(config-router)#no auto-summary
```

```
R5(config)#router eigrp 7
R5(config-router)#network 100.0.0.0 0.0.0.255
R5(config-router)#network 155.55.55.0 0.0.0.255
R5(config-router)#no auto-summary
```

```
R6(config)#router eigrp 7
R6(config-router)#network 100.0.0.0 0.0.0.255
R6(config-router)#network 60.0.0.0 0.0.0.255
R6(config-router)#no auto-summary
```

```
R6(config)#int tun100
R6(config-if)#no ip split-horizon eigrp 7
```


- **Verify that R5 has reachability to R4's Ethernet network, and check the routing table for the EIGRP routes.**

```
R5#ping 192.1.24.4 source fa0/1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.1.24.4, timeout is 2 seconds:

Packet sent with a source address of 155.55.55.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/61/64 ms

```
R5#show ip route eigrp
```

```
D    192.1.24.0/24 [90/28162560] via 100.0.0.6, 00:01:40, Tunnel100
      60.0.0.0/24 is subnetted, 1 subnets
```

```
D          60.0.0.0 [90/15362560] via 100.0.0.6, 00:01:40, Tunnel100
```

```
R5#
```

- **Next, we can configure the crypto for the DMVPN. R2 and R5 will be similar.**

```
R5(config)#crypto isakmp pol 10
```

```
R5(config-isakmp)#hash md5
```

```
R5(config-isakmp)#auth pre-share
```

```
R5(config)#crypto isakmp key ccie address 0.0.0.0 0.0.0.0
```

```
R5(config)#crypto ipsec transform-set TRANS esp-3des esp-md5-hmac
```

```
R5(cfg-crypto-trans)#exit
```

```
R5(config)#crypto ipsec profile MYPROF
```

```
R5(ipsec-profile)#set security-association lifetime seconds 120
```

```
R5(ipsec-profile)#set transform-set TRANS
```

```
R2(config)#crypto isakmp pol 10
```

```
R2(config-isakmp)#hash md5
```

```
R2(config-isakmp)#auth pre-share
```

```
R2(config)#crypto isakmp key ccie address 0.0.0.0 0.0.0.0
```

```
R2(config)#crypto ipsec transform-set TRANS esp-3des esp-md5-hmac
```

```
R2(config)#crypto ipsec profile MYPROF
```

```
R2(ipsec-profile)#set security-association lifetime seconds 120
```

```
R2(ipsec-profile)#set transform-set TRANS
```

- **R6 will be slightly different, since it is will also be authenticating Easy VPN clients.**

```
R6(config)#crypto keyring SPOKES
```

```
R6(conf-keyring)#pre-shared-key address 0.0.0.0 0.0.0.0 key ccie
```

```
R6(config)#crypto isakmp policy 10
```

```
R6(config-isakmp)#hash md5
```

```
R6(config-isakmp)#authentication pre-share
```

```
R6(config)#crypto ipsec trans TRANS esp-3des esp-md5-hmac
```

```
R6(config)#crypto ipsec profile SECUREME
```

```
R6(ipsec-profile)#set security-association lifetime seconds 120
```

```
R6(ipsec-profile)#set transform-set TRANS
```

```
R6(ipsec-profile)#set isakmp-profile ISAKPROF
```



```
R6(config)#crypto isakmp profile ISAKPROF
% A profile is deemed incomplete until it has match identity statements
R6(conf-isa-prof)#keyring SPOKES
R6(conf-isa-prof)#match identity address 0.0.0.0

R6(config)#int tun100
R6(config-if)#tunnel protection ipsec profile SECUREME

R2(config)#int tun100
R2(config-if)#tun prot ipsec profile MYPROF

R5(config)#int tun 100
R5(config-if)#tun prot ipsec profile MYPROF
```

Task 7-18

Use XAUTH for local configuration, with username and password is ccie.

```
R6(config)#aaa new-model
R6(config)#aaa authentication login USERS local
R6(config)#aaa authorization network NETW local
R6(config)#aaa authentication login default none

R6(config)#username ccie password ccie

R6(config)#crypto isakmp profile XVPN
% A profile is deemed incomplete until it has match identity statements
R6(conf-isa-prof)#match identity group MYGROUP
R6(conf-isa-prof)#client authentication list USERS
R6(conf-isa-prof)#isakmp authorization list NETW
R6(conf-isa-prof)#client config address respond
```

Task 7-19

The default pre-shared key should be ccie.

- The default key is configured for the DMVPN spokes.

Task 7-20

Easy VPN Clients should use Diffie-Hellman group 2.

- Configure another ISAKMP policy for the Easy VPN clients.

```
R6(config)#crypto isak policy 30
R6(config-isakmp)#hash md5
R6(config-isakmp)#authent pre-share
R6(config-isakmp)#group 2
```


Task 7-21

The dynamic address pool should be 60.0.0.10 to 60.0.0.20.

→ **Configure a local pool on R6.**

```
R6 (config) #ip local pool vpnclients 60.0.0.10 60.0.0.20
```

Task 7-22

Client should response to the address.

→ **This was configured under the ISAKMP profile.**

Task 7-23

Create a VPN client group that uses DNS at 60.0.0.1, 60.0.0.2 and WINS at 60.0.0.3 and 60.0.0.4.

```
R6 (config-isakmp) #crypto isakmp client config group MYGROUP
R6 (config-isakmp-group) #key MYPASSWORD
A key already exists for group MYGROUP

R6 (config-isakmp-group) #dns 60.1.1.1 60.1.1.2
R6 (config-isakmp-group) #wins 60.1.1.3 60.1.1.4
R6 (config-isakmp-group) #domain cisco.com
```

Task 7-24

Phase 2 policy should be esp-3des esp-md5-hmac.

→ **Configure to use the same transform set as the DMVPN.**

```
R6 (config) #crypto dynamic-map dyna 10
R6 (config-crypto-map) #set isakmp-profile XVPN
R6 (config-crypto-map) #set transform TRANS
R6 (config-crypto-map) #reverse-route

R6 (config) #int fa0/0
R6 (config-if) #crypto map MYMAP
```

Task 7-25

NHRP authentication should use ccie.

```
R2 (config) #int tun100
R2 (config-if) #ip nhrp authent ccie

R6 (config) #int tun100
R6 (config-if) #ip nhrp authent ccie

R5 (config) #int tun100
R5 (config-if) #ip nhrp authent ccie
```


Task 7-26

Reverse route injection should be used to provide the DMVPN networks access to any Easy VPN Client network.

→ This was configured under the dynamic crypto map.

Task 7-27

R6 will be the hub.

→ This is informational only. R6 was configured as the hub in earlier steps.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

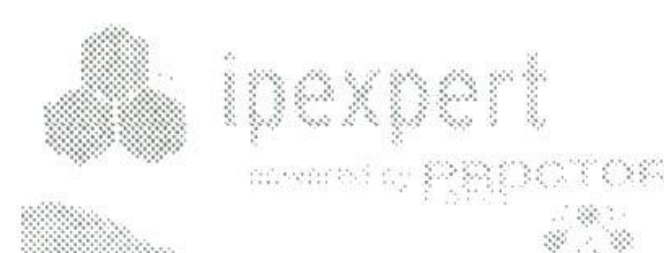
This page left intentionally blank.

Section 8: VPN Concentrator

Estimated Time to Complete: 3 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 8 Pre-Lab Setup

- Physically connect and configure your network according to the Diagram 8-A.
- This lab will focus strictly on the Concentrator. You will need to pre-configure the network with the base IP Addressing on the Routers. The pre-configuration files will be used to initially configure the routers. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs → Section 7 → Initial Configurations → Router X.txt*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Basic Configuration of the VPN Concentrator from the CLI and the Graphical Interface

Task 8-1

Configure the VPN Concentrator from the CLI. Assign it an IP Address on the Private interface of 10.2.2.5 with a Mask of 255.255.255.0.

- The basic config is set through the CLI command. You can telnet to the concentrator with username / password of admin / admin. Then you just follow the prompt and specify the IP address and also the mask. Then you have access to GUI from the ACS server.

Task 8-2

Allow the Inside PC to connect to the VPN Concentrator for Administrator from the inside address.

- Try to see whether you can ping the VPN concentrator from R1. If it is ok, then you can try to ping it from the ACS server.

Task 8-3

You are allowed a single static route on the VPN Concentrator.

- You are adding a route from 10.1.1.0/24 to go through 10.2.2.1 and it can be done in the prompt.

Configuration – System Management – IP Routing – Static Routes – Add Static Route

Routing -> 1

Static Routes

Destination	Mask	Metric	Destination

No Static Routes Configured			

No Static Routes Configured

- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

Routing ->1

> Net Address

Routing ->10.1.1.0

> Subnet Mask

Routing ->255.255.255.0

- 1) Destination is Router
- 2) Destination is Interface

Routing ->1

> Router Address

Routing ->10.2.2.1

> Route Metric (1 - 16)

Routing ->[1]

Static Routes

Destination	Mask	Metric	Destination
10.1.1.0	255.255.255.0	1	10.2.2.1

- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

Routing ->

→ If you ping from the ACS server now, you should get a response.

Task 8-4

Configure the Public interface of the Concentrator using the Graphical Interface.

→ You use the <http://10.2.2.5> to access to the GUI interface and then click the public interface such that you can set the address.

Task 8-5

Assign it an IP Address of 192.1.24.5 with a mask of 255.255.255.0.

→ As mentioned from the previous task, you can set the public interface IP address from the GUI interface. Just simply click to the Public interface.

- This task is relatively simple. You should be able to complete it with minimal help. Just remember that the username and password for VPN is admin/admin.

Configuration: Interfaces: Ethernet 2

Configuring Ethernet Interface 2 (Public).

General RIP OSPF Bandwidth WebVPN

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask.
	IP Address	192.1.24.5	Enter the IP Address and Subnet Mask for this interface.
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address		The MAC address for this interface.
	Interface Name		Enter the textual name of the interface.
	Filter	2: Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPsec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation, fragment prior to interface transmission <input type="radio"/> Fragment prior to IPsec encapsulation with Path MTU Discovery (ICMP) <input type="radio"/> Fragment prior to IPsec encapsulation without Path MTU Discovery (Clear DF bit)	

Apply Cancel

Configuring RIP and OSPF on the Concentrator

Task 8-6

Configure OSPF on R2 and R4 in Area 0. Advertise all directly connected networks.

- You need to use the following commands for the routing protocol:

```
r2(config)#router ospf 1
r2(config-router)#router-id 2.2.2.2
r2(config-router)#log-adjacency-changes
r2(config-router)#network 2.2.2.2 0.0.0.0 area 0
r2(config-router)#network 192.1.24.2 0.0.0.0 area 0
```

```
r4(config)#router ospf 1
r4(config-router)#router-id 4.4.4.4
r4(config-router)#log-adjacency-changes
r4(config-router)#network 4.4.4.4 0.0.0.0 area 0
r4(config-router)#network 192.1.24.4 0.0.0.0 area 0
```


Task 8-7

Configure OSPF on the Public Interface of the Concentrator in Area 0.

- You need to go to the public interface and click on the tab for OSPF and then set OSPF to the Area 0. Click enable under System → IP Routing for the OSPF.
- Also, remember to check for the filter for the public interface so that you would know whether the OSPF packet is filtered. Configuration – Policy Management – Traffic Management – Filters – Public – Assign Rules. Select OSPF in and OSPF out.
- Configuration – Interfaces – Private – OSPF Tab, check 'OSPF Enabled'.
- Something to notice is that the concentrator will not advertise its inside network of 10.2.2.0/24 into OSPF. There are two ways of allowing this network to be reachable from the outside. The first is to enable OSPF on the private interface. The second would be change the static route you created for 10.1.1.0/24 to include the 10.2.2.0/24 network. If you don't advertise this network address to R2 and R4, they will not know how to route packets to this network and therefore your IPsec VPN and your EZVPN configuration that you will do later will fail.

Task 8-8

Configure RIP V2 on R1. Advertise all directly connected networks.

- The following commands can be used for R1 to run RIP. To specify it as version 2, then RIP v2 is being used.

```
r1(config)#router rip
r1(config-router)#version 2
r1(config-router)#network 1.0.0.0
r1(config-router)#network 10.0.0.0
r1(config-router)#no auto-summary
```

Task 8-9

Configure RIP V2 on the Private interface of the Concentrator.

- Go to the tab RIP under interface Private Interface. Then the Inbound RIP and Outbound RIP should be set to RIP v2. Note: Inbound RIP will be on by default.

Task 8-10

Redistribute the OSPF Routes into RIP and vice versa.

- To redistribute the route, go to System → IP Routing → OSPF and click on Autonomous system then the VPN concentrator would redistribute the routes.

- You can check the routing table under “monitoring”. It should look something like this:

Address	Mask	Next Hop	Interface	Protocol	Age	Metric
1.0.0.0	255.0.0.0	10.2.2.1	1	RIP	3	2
2.2.2.2	255.255.255.255	192.1.24.2	2	OSPF	0	2
4.4.4.4	255.255.255.255	192.1.24.4	2	OSPF	0	2
10.1.1.0	255.255.255.0	10.2.2.1	1	Static	0	1
10.2.2.0	255.255.255.0	0.0.0.0	1	Local	0	1
192.1.24.0	255.255.255.0	0.0.0.0	2	Local	0	1

- We can also check OSPF is neighboring between the routers and the VPN by the following command:

R2#**sh ip ospf neighbor**

```
Neighbor ID    Pri  State           Dead Time   Address      Interface
4.4.4.4        1    FULL/BDR        00:00:31    192.1.24.4   FastEthernet1/0
5.5.5.5        1    FULL/DROTHER    00:00:30    192.1.24.5   FastEthernet1/0
```

R4#**sh ip ospf neighbor**

```
Neighbor ID    Pri  State           Dead Time   Address      Interface
2.2.2.2        1    FULL/DR         00:00:35    192.1.24.2   FastEthernet0/0
5.5.5.5        1    FULL/DROTHER    00:00:35    192.1.24.5   FastEthernet0/0
```

- From the “show ip route”, you can see that the RIP routes are treated as external routes, meaning that the concentrator is doing redistribution. You can also see that the 10.2.2.0/24 network has been included in the 10/8 network advertisement.

R4#**show ip route**

```
2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 192.1.24.2, 00:05:36, FastEthernet0/0
C       4.0.0.0/8 is directly connected, Loopback0
C       192.1.24.0/24 is directly connected, FastEthernet0/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O E2    10.1.1.0/24 [110/20] via 192.1.24.5, 00:05:36, FastEthernet0/0
O E2    10.0.0.0/8 [110/20] via 192.1.24.5, 00:05:36, FastEthernet0/0
192.168.3.0/32 is subnetted, 1 subnets
C       192.168.3.1 is directly connected, Loopback1
```

- We can also check the RIP debug commands - “debug ip rip events” and “debug ip rip”.

R1#**clear ip route ***

```
*Dec 25 19:00:55: RIP: received v2 update from 10.2.2.5 on FastEthernet0/1
*Dec 25 19:00:55:      2.2.2.2/32 via 0.0.0.0 in 8 hops
*Dec 25 19:00:55:      4.4.4.4/32 via 0.0.0.0 in 8 hops
*Dec 25 19:00:55:      192.1.24.0/24 via 0.0.0.0 in 1 hops
*Dec 25 19:00:55: RIP: Update contains 3 routes
*Dec 25 19:00:56: RIP: sending request on FastEthernet0/0 to 224.0.0.9
*Dec 25 19:00:56: RIP: sending request on FastEthernet0/1 to 224.0.0.9
*Dec 25 19:00:56: rip_route_adjust for FastEthernet0/0 coming up
*Dec 25 19:00:56: rip_route_adjust for FastEthernet0/1 coming up
*Dec 25 19:00:56: RIP: sending request on Loopback0 to 224.0.0.9
*Dec 25 19:00:56: rip_route_adjust for Loopback0 coming up
*Dec 25 19:00:56: RIP: remove FastEthernet0/0 from RIP idb list
```



```
*Dec 25 19:00:56: RIP: remove FastEthernet0/1 from RIP idb list
*Dec 25 19:00:56: RIP: remove Loopback0 from RIP idb list
*Dec 25 19:00:56: RIP: add Loopback0 to RIP idb list
*Dec 25 19:00:56: RIP: add FastEthernet0/0 to RIP idb list
*Dec 25 19:00:56: RIP: add FastEthernet0/1 to RIP idb list

*Dec 25 19:00:56: RIP: ignored v2 packet from 1.1.1.1 (sourced from one of
our addresses)
*Dec 25 19:00:58: RIP: sending v2 flash update to 224.0.0.9 via
FastEthernet0/0 (10.1.1.1)
*Dec 25 19:00:58: RIP: build flash update entries
*Dec 25 19:00:58:      1.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Dec 25 19:00:58:      2.2.2.2/32 via 0.0.0.0, metric 9, tag 0
*Dec 25 19:00:58:      4.4.4.4/32 via 0.0.0.0, metric 9, tag 0
*Dec 25 19:00:58:      10.2.2.0/24 via 0.0.0.0, metric 1, tag 0
*Dec 25 19:00:58:      192.1.24.0/24 via 0.0.0.0, metric 2, tag 0
*Dec 25 19:00:58: RIP: Update contains 5 routes
*Dec 25 19:00:58: RIP: Update queued
```

Concentrator Administration

Task 8-11

Admin access should be restricted to the inside PC.

- ➔ **Go to Administration → Access Right → Access Control List and define 10.1.1.100. Then go to Interface → Public interface → WebVPN click the “Allow Management HTTPS sessions” and “Redirect HTTP to HTTPS”.**

Task 8-12

Also allow HTTP management from the Public Interface using HTTPS. This should be limited to network 192.1.24.0.

- ➔ **Go to Administration → Access right → Access Control List and define 192.1.24.0/24 Then go to Interface → Public interface → WebVPN click the “Allow Management HTTPS sessions” and “Redirect HTTP to HTTPS”.**

→ We can check the HTTP from the “monitoring → statistic → http”.

	Sent	Received
Octets	272440	291264
Packets	758	558
	Sockets	Sessions
Active	2	1
Peak	2	1
Total	4	2

HTTP Sessions

Login Name	IP Address	Login Time	Encryption	Octets		Packets		Sockets		
				Sent	Received	Sent	Received	Active	Peak	Total
admin	10.1.1.100	Dec 25 11:12:47	None	91808	119795	297	233	2	2	2

Max Connections: 2

→ We can also check the session under “monitoring → session”.

Management Sessions

[[LAN-to-LAN Sessions](#) | [Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	10.1.1.100	HTTP	None	Dec 25 11:12:50	0:03:02

LAN-to-LAN IPSec Tunnel to a Router

Task 8-13

Configure an IPSec tunnel between R2 and the Concentrator using the following information:

- ISAKMP Hash – MD5
- ISAKMP Authentication – Pre-shared
- IPSec – ESP-DES, ESP-MD5-HMAC
- Interesting Traffic – 10.2.2.0 to 2.0.0.0
- For the VPN concentrator, you go to the Tunneling and Security --> IPSec --> LAN to LAN and enable it with the peer of 192.1.24.2. The Local Network IP address is 10.2.2.0 with mask 0.0.0.255 and the remote network is 2.0.0.0 with mask 0.255.255.255.
- The following commands configure R2 to build an IPSEC tunnel to the concentrator

```
r2(config)#access-list 151 permit ip 2.0.0.0 0.255.255.255 10.2.2.0
0.0.0.255
r2(config)#crypto isakmp policy 10
r2(config-isakmp)#hash md5
r2(config-isakmp)#authentication pre-share
r2(config-isakmp)#crypto isakmp key ipexpert address 192.1.24.5
r2(config)#crypto ipsec transform-set tset esp-des esp-md5-hmac
r2(cfg-crypto-trans)#crypto map secure 10 ipsec-isakmp
r2(config-crypto-map)#set peer 192.1.24.5
r2(config-crypto-map)#set transform-set tset
```



```

r2(config-crypto-map)#match address 151
r2(config-crypto-map)#interface FastEthernet1/0
r2(config-if)#crypto map secure

```

→ The “monitoring → session” gives the IPSec session as follows:

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
1	0	1	2	2	1	1.00%	100	4

LAN-to-LAN Sessions

[Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
R2	192.1.24.2	IPSec/LAN-to-LAN	DES-56	Dec 25 14:19:22	0:00:37	416	416

→ In addition, under “statistic → IPSec”, there is the traffic generated by IKE. Sometimes, if the tunnel is not working, this may be a good place to check. We would know whether there is any traffic in the IKE Phase 2. If not, then check whether there is any traffic for IKE Phase 1. Then we roughly would know where the IPSec has problem.

Reset 

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	1188
Sent Bytes	1092
Received Packets	11
Sent Packets	10
Received Packets Dropped	0
Sent Packets Dropped	0
Received Notifies	6
Sent Notifies	12
Received Phase-2 Exchanges	1
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	0
Initiated Tunnels	0
Failed Initiated Tunnels	0

IPSec (Phase 2) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	416
Sent Bytes	416
Received Packets	4
Sent Packets	4
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	4
Failed Inbound Authentications	0
Outbound Authentications	4
Failed Outbound Authentications	0
Decryptions	4
Failed Decryptions	0
Encryptions	4
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

→ R2's show command would also shows the IPSec info:

R2#**show crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet1/0	192.1.24.2	set	HMAC_MD5+DES_56_CB	0	0
3001	FastEthernet1/0	192.1.24.2	set	DES+MD5	0	4
3002	FastEthernet1/0	192.1.24.2	set	DES+MD5	4	0

R2#**show crypto ipsec sa**

interface: **FastEthernet1/0**

Crypto map tag: secure, local addr **192.1.24.2**

protected vrf: (none)

local ident (addr/mask/prot/port): (2.0.0.0/255.0.0.0/0/0)

remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)

current_peer **192.1.24.5** port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4

#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: **192.1.24.2**, remote crypto endpt.: **192.1.24.5**

path mtu 1500, ip mtu 1500

current outbound spi: 0x2A088DF7(705203703)

inbound esp sas:

spi: 0x55DE0486(1440613510)

transform: esp-des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 3001, flow_id: Onboard VPN:1, crypto map: secure

sa timing: remaining key lifetime (k/sec): (4494227/3250)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

spi: 0x2A088DF7(705203703)

transform: esp-des esp-md5-hmac ,

in use settings ={Tunnel, }

conn id: 3002, flow_id: Onboard VPN:2, crypto map: secure

sa timing: remaining key lifetime (k/sec): (4494227/3248)

IV size: 8 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcsp sas:

Remote Access Tunnel Using IPSec and PPTP

Task 8-14

Create a Group called RA with a password of **abcd**.

- You click on the Tunnel and Security --> PPTP and Enable it. Then you go to System --> Address Management --> Address assignment and use the pool. And you add a group under User Management --> Group and define the name and password.

Task 8-15

Allow IPSec and PPTP as the Access Protocol.

- The previous step and upcoming steps would allow IPSec and PPTP as the access protocol.

Task 8-16

Create a Pool of IP Address 192.168.1.1-192.168.1.254. This pool should be specific to this group.

- You need to go to the group and click on the Address Pool and specify the address range as 192.168.1.1 to 192.168.1.254 with mask 255.255.255.0.

*** IMPORTANT NOTE ***

- In order to allow address pools to be used you also need to go and globally enable address pools.

Configuration->System->Address Management->Assignments. Place a check in the "Use Address Pools" box.

Task 8-17

Make sure this network gets propagated to R1.

- In the IP Routing --> Reverse Route Injection, you would click the "Generate Hold Down route" and then you would see the network 192.168.1.0/0.0.0.255.
- The "Monitoring → Statistics → Address Pools" command displays the valid address pool. The "Available" and "Allocated" would be changed when the user is using this.

Group	IP Address Range		Addresses				
	Start	End	Total	Available	Allocated	Held	Max Allocated
RA	192.168.1.1	192.168.1.254	254	254	0	0	0
webvpn	192.168.2.1	192.168.2.254	254	254	0	0	0

→ R1 would also see the route injected.

R1#**show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
```

→ Gateway of last resort is not set.

```
C    1.0.0.0/8 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
R    2.2.2.2 [120/8] via 10.2.2.5, 00:00:15, FastEthernet0/1
    4.0.0.0/32 is subnetted, 1 subnets
R    4.4.4.4 [120/8] via 10.2.2.5, 00:00:15, FastEthernet0/1
R    192.1.24.0/24 [120/1] via 10.2.2.5, 00:00:15, FastEthernet0/1
    10.0.0.0/24 is subnetted, 2 subnets
C    10.2.2.0 is directly connected, FastEthernet0/1
C    10.1.1.0 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/1] via 10.2.2.5, 00:00:16, FastEthernet0/1
```

Task 8-18

Allow users of this group to also connect to the 4.0.0.0 network when they are connected to the VPN Concentrator.

- Go to Policy Management --> Traffic Management --> Network List and define a list with name Net4 and 4.0.0.0/0.255.255.255.
- Then, User Management --> Group, click the RA group that we previously defined. And click the "Client config" tab. For the Split tunnel Policy, click "allow the networks in list to bypass the tunnel". Then for the Split Tunneling Network List, choose "Net4" that we defined earlier. Then click Apply".

Task 8-19

Create a user **RAUser** with a password of **RAUser12**. Assign the user to the **RA** group.

- User Management --> User, define a user with the username RAUser as required. Place this user to the group RA.

Web VPN

Task 8-20

Enable HTTP Services on R1.

- The following command enable HTTP service for R1:

```
r1(config)#ip http server
```


Task 8-21

Create a Telnet Password of **telnet** on R1.

- **The password for the vty line is changed to telnet.**

```
r1(config)#line vty 0 4
r1(config-line)#password telnet
r1(config-line)#login
```

Task 8-22

Create a Group called **WebVPN** with a password of **abcd**.

- **User Management -> Group, create a group name WebVPN.**

Task 8-23

Allow WebVPN as the protocol for this group.

Task 8-24

Create a Pool of IP Address 192.168.2.1-192.168.2.254. This pool should be specific to this group.

- **Click on the Address Pools and Add an address pool with IP address 192.168.2.1 to 192.168.2.254 and mask 255.255.255.0.**

Task 8-25

Make sure this network gets propagated to R1.

- **Under IP Routing --> Reverse Route Injection, click on "Generate route" and you should see the address pool hold down routes is changed to 192.168.0.0/255.255.252.0. You should be able to check it from R1's routing table.**
- **The following is the "show ip route" from R1. Notice that the route is propagated.**

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
```


Gateway of last resort is not set

```
C    1.0.0.0/8 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
R    2.2.2.2 [120/8] via 10.2.2.5, 00:00:27, FastEthernet0/1
    4.0.0.0/32 is subnetted, 1 subnets
R    4.4.4.4 [120/8] via 10.2.2.5, 00:00:27, FastEthernet0/1
R    192.1.24.0/24 [120/1] via 10.2.2.5, 00:00:27, FastEthernet0/1
    10.0.0.0/24 is subnetted, 2 subnets
C    10.2.2.0 is directly connected, FastEthernet0/1
C    10.1.1.0 is directly connected, FastEthernet0/0
R    192.168.0.0/22 [120/1] via 10.2.2.5, 00:00:28, FastEthernet0/1
```

Task 8-26

Enable the Concentrator to redirect HTTP requests to HTTPS.

- **Go to Public Interface --> WebVPN and click on Allow WebVPN HTTPS Session.**

Task 8-27

Disable the ability of the users to enter a URL.

- **UserManagement --> Group --> Click on the WebVPN group that we defined earlier and the tab WebVPN. Uncheck the URL Entry.**

Task 8-28

Create a URL Link for the HTTP Server on R1 such that when a user part of this group logs in, he has the ability to click on a Link to connect to the HTTP server on R1.

- **Go back to the group WebVPN and click on the "WebVPN Servers and URLs". Add a name R1-HTTP with remote as `http://10.2.2.1` and then click apply and done.**

Task 8-29

Create a custom application that allows the user to telnet into R1 using port 20000.

- **Go back to the group WebVPN and click on WebVPN Port Forwarding. Add a name R1-Telnet with local TCP port as 20000 and Remote Server 102.2.1 and Remote TCP port 23. Click apply and done.**

Task 8-30

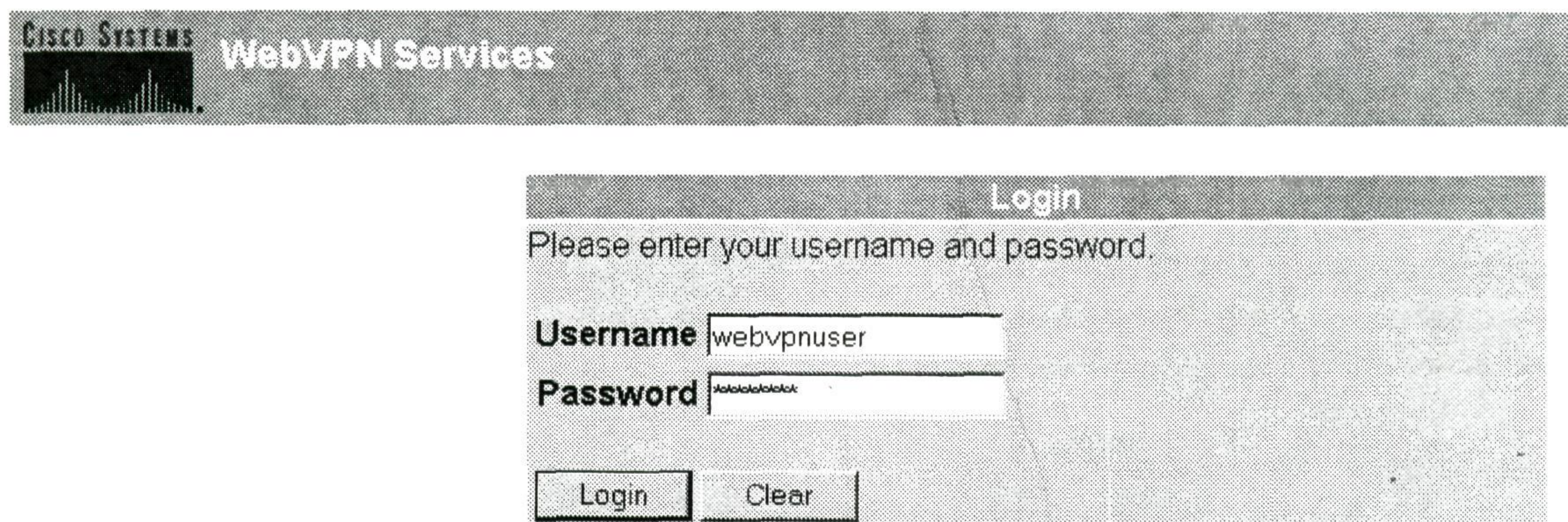
Create a user **webvpnuser** with a password of **webvpn12**. Assign the user to the **WebVPN** group.

- **Click on User Management --> Users and add a new user webvpnuser and place it under the group of WebVPN.**

Task 8-31

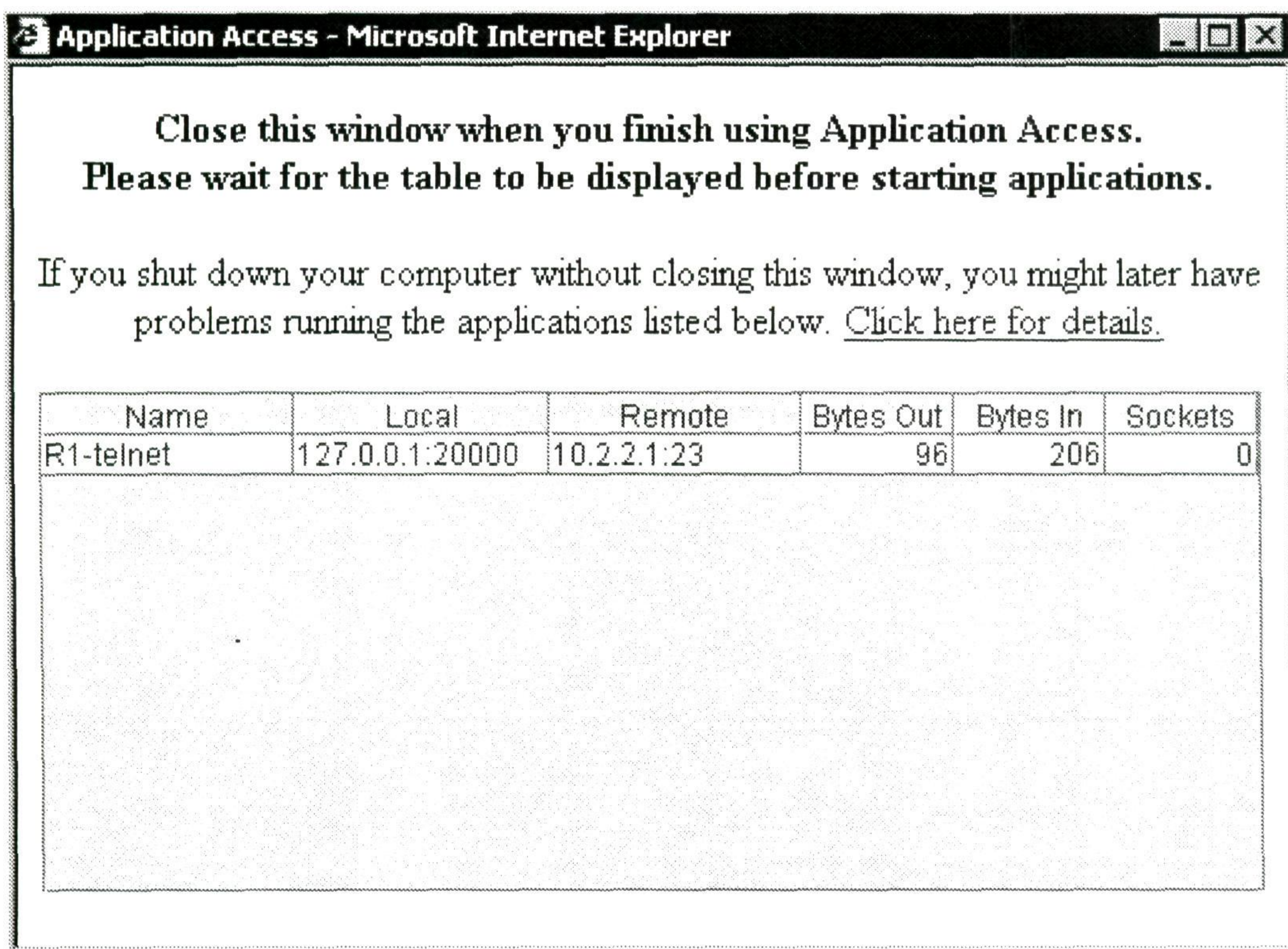
Verify the config by logging on and verifying the configuration.

→ After you have configured this, you would see the following screen:



The image shows a web browser window titled "Cisco Systems WebVPN Services". The main heading is "WebVPN Services". Below this is a "Login" section with the instruction "Please enter your username and password." There are two input fields: "Username" with the value "webvpnuser" and "Password" with masked characters. At the bottom of the login section are two buttons: "Login" and "Clear".

→ You should close this window after finishing the application process, as indicated in the warning below.



The image shows a Microsoft Internet Explorer window titled "Application Access - Microsoft Internet Explorer". The main content area contains the following text:

**Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.**

If you shut down your computer without closing this window, you might later have problems running the applications listed below. [Click here for details.](#)

Name	Local	Remote	Bytes Out	Bytes In	Sockets
R1-telnet	127.0.0.1:20000	10.2.2.1:23	96	206	0

→ Then open a DOS window and enter the command "telnet 127.0.0.1 20000" and you would get to router 1.

EZVPN

Task 8-32

Configure an IPSec tunnel between R4 and the Concentrator using EZVPN.

→ **Nothing is needed for this step.**

Task 8-33

The Concentrator should act as the EZVPN Server and R4 should be the client.

→ **Nothing is needed for this step.**

Task 8-34

Create a separate group for the EZVPN Configuration called EZVPN with a password of **abcd**.

→ **Click User Management --> Group and add a group EZVPN.**

Task 8-35

Create a Pool of IP Address 192.168.3.1-192.168.3.254. This pool should be specific to this group.

→ **Click on the EZVPN group EZVPN that we defined above and the Address Pools --> Add a pool of 192.168.3.1 to 192.168.3.254.**

Task 8-36

Make sure this network gets propagated to R1.

→ **Click on IP Routing --> Reverse Route Injection and Generate Hold Down Routes.**

Task 8-37

Create a User **EZ** with a password of **ezvpn123**.

→ **Click on User Management --> Users and add a new username of EZ and place it under the group of EZVPN that we defined earlier.**

Task 8-38

Make this user a member of the EZVPN group.

→ **This step is performed in the previous task.**

Task 8-39

Configure R4 to act as the EZVPN Client with the following parameters:

- ➔ Peer: 192.1.24.5
- ➔ Connect: Auto
- ➔ Mode: client
- ➔ Group: EZVPN
- ➔ Key: abcd
- ➔ Outside Interface: F 0/0
- ➔ Inside Interface: Loopback 0

```
r4(config)#crypto ipsec client ezvpn ez
r4(config-crypto-ezvpn)#connect auto
r4(config-crypto-ezvpn)#group EZVPN key abcd
r4(config-crypto-ezvpn)#mode client
r4(config-crypto-ezvpn)#peer 192.1.24.5
r4(config-crypto-ezvpn)#username EZ password ezvpn123
r4(config-crypto-ezvpn)#xauth userid mode local
```

```
r4(config)#interface Loopback0
r4(config-if)#ip address 4.4.4.4 255.0.0.0
r4(config-if)#crypto ipsec client ezvpn ez inside
```

```
r4(config)#interface FastEthernet0/0
r4(config-if)#crypto ipsec client ezvpn ez
```

Task 8-40

Connect from R4 to the Concentrator to verify the configuration.

- ➔ **The EZVPN is established and we ran the two debug “debug crypto ipsec” and “debug crypto isakmp”. Repeated entries are deleted, and the important points are highlighted.**

```
R4#crypto ipsec client ezvpn connect
*Dec 25 23:19:58: ISAKMP:isadb_key_addr_delete: no key for address 192.1.24.5
(NULL root)
*Dec 25 23:19:58: ISAKMP: Created a peer struct for 192.1.24.5, peer port 500
*Dec 25 23:19:58: ISAKMP: received ke message (1/1)
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0): SA request profile is (NULL)
*Dec 25 23:19:58: ISAKMP: Found a peer struct for 192.1.24.5, peer port 500
*Dec 25 23:19:58: ISAKMP: Locking peer struct 0x46564E80, IKE refcount 1 for
isakmp_initiator
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0):Setting client config settings 46564C3C
*Dec 25 23:19:58: ISAKMP: local port 500, remote port 500
*Dec 25 23:19:58: insert sa successfully sa = 4620B514
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0): client mode configured.
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-07 ID
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-03 ID
*Dec 25 23:19:58: ISAKMP:(0:0:N/A:0): constructed NAT-T vendor-02 ID
*Dec 25 23:19:58: ISKAMP: growing send buffer from 1024 to 3072
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):SA is doing pre-shared key authentication
plus XAUTH using id type ID_KEY_ID
*Dec 25 23:19:58: ISAKMP (0:134217729): ID payload
      next-payload : 13
      type          : 11
```



```

group id      : EZVPN
protocol      : 17
port          : 0
length        : 13
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):Total payload length: 13
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_IPSEC,
IKE_SA_REQ_AM
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):Old State = IKE_READY New State =
IKE_I_AM1

*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): beginning Aggressive Mode exchange
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) AG_INIT_EXCH
*Dec 25 23:19:58: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) AG_INIT_EXCH
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing SA payload. message ID = 0
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing ID payload. message ID = 0
*Dec 25 23:19:58: ISAKMP (0:134217729): ID payload
next-payload : 8
type          : 1
address       : 192.1.24.5
protocol      : 17
port          : 500
length        : 12
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):: peer matches *none* of the profiles
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing vendor id payload
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): vendor ID is Unity
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing vendor id payload
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): vendor ID seems Unity/DPD but major 215
mismatch
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): vendor ID is XAUTH
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing vendor id payload
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): vendor ID is DPD
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): local preshared key found
*Dec 25 23:19:58: ISAKMP : Scanning profiles for xauth ...
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): Authentication by xauth preshared
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):Checking ISAKMP transform 14 against
priority 65515 policy
*Dec 25 23:19:58: ISAKMP:          encryption 3DES-CBC
*Dec 25 23:19:58: ISAKMP:          hash MD5
*Dec 25 23:19:58: ISAKMP:          default group 2
*Dec 25 23:19:58: ISAKMP:          auth XAUTHInitPreShared
*Dec 25 23:19:58: ISAKMP:          life type in seconds
*Dec 25 23:19:58: ISAKMP:          life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):Encryption algorithm offered does not
match policy!
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):atts are not acceptable. Next payload is
0
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1):atts are acceptable. Next payload is 0
*Dec 25 23:19:58: ISAKMP:(0:1:SW:1): processing KE payload. message ID = 0
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID = 0
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):SKEYID state generated
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1): processing HASH payload. message ID = 0
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):SA has been authenticated with 192.1.24.5
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Send initial contact
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) AG_INIT_EXCH
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_AM_EXCH
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Old State = IKE_I_AM1 New State =
IKE_P1_COMPLETE

```



```

*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Need XAUTH
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 25 23:19:59: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) CONF_XAUTH
*Dec 25 23:19:59: ISAKMP: set new node -1462071336 to CONF_XAUTH
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):processing transaction payload from
192.1.24.5. message ID = -1462071336
*Dec 25 23:19:59: ISAKMP: Config payload REQUEST
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):checking request:
*Dec 25 23:19:59: ISAKMP: XAUTH_TYPE_V2
*Dec 25 23:19:59: ISAKMP: XAUTH_USER_NAME_V2
*Dec 25 23:19:59: ISAKMP: XAUTH_USER_PASSWORD_V2
*Dec 25 23:19:59: ISAKMP: XAUTH_MESSAGE_V2
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Xauth process request
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER,
IKE_CFG_REQUEST
*Dec 25 23:19:59: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_XAUTH_REPLY_AWAIT

*Dec 25 23:20:10: EZVPN(ez): Pending XAuth Request, Please enter the
following command:
*Dec 25 23:20:10: EZVPN: crypto ipsec client ezvpn xauth

R4#crypto ipsec client ezvpn xauth
Enter Username and Password.: EZ
Password:
R4#
*Dec 25 23:20:46: xauth-type: 0
*Dec 25 23:20:46: username: EZ
*Dec 25 23:20:46: password: <omitted>
*Dec 25 23:20:46: message <Enter Username and Password.>
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1): responding to peer config from
192.1.24.5. ID = -1628483708
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) CONF_XAUTH
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):deleting node -1628483708 error FALSE
reason "Done with xauth request/reply exchange"
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Input = IKE_MESG_INTERNAL,
IKE_XAUTH_REPLY_ATTR
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Old State = IKE_XAUTH_REPLY_AWAIT New
State = IKE_XAUTH_REPLY_SENT

*Dec 25 23:20:46: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) CONF_XAUTH
*Dec 25 23:20:46: ISAKMP: set new node 2026872836 to CONF_XAUTH
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):processing transaction payload from
192.1.24.5. message ID = 2026872836
*Dec 25 23:20:46: ISAKMP: Config payload SET
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Xauth process set, status = 1
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):checking SET:
*Dec 25 23:20:46: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):attributes sent in message:
*Dec 25 23:20:46: Status: 1
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) CONF_XAUTH
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):deleting node 2026872836 error FALSE
reason "No Error"
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Input = IKE_MESG_FROM_PEER, IKE_CFG_SET

```



```

*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Old State = IKE_XAUTH_REPLY_SENT New
State = IKE_P1_COMPLETE

*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Need config/address
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Need config/address
*Dec 25 23:20:46: ISAKMP: set new node -785696602 to CONF_ADDR
*Dec 25 23:20:46: ISAKMP: Sending APPLICATION_VERSION string: Cisco IOS
Software, 2800 Software (C2800NM-ADVENTERPRISEK9-M), Version 12.4(3a),
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 30-Sep-05 13:24 by hqluong
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1): initiating peer config to 192.1.24.5. ID
= -785696602
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) CONF_ADDR
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_CONFIG_MODE_REQ_SENT

*Dec 25 23:20:46: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) CONF_ADDR
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):processing transaction payload from
192.1.24.5. message ID = -785696602
*Dec 25 23:20:46: ISAKMP: Config payload REPLY
*Dec 25 23:20:46: ISAKMP(0:134217729) process config reply
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):deleting node -785696602 error FALSE
reason "Transaction mode done"
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Old State = IKE_CONFIG_MODE_REQ_SENT New
State = IKE_P1_COMPLETE

*Dec 25 23:20:46: insert of map into mapdb AVL failed, map + ace pair already
exists on the mapdb
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Input = IKE_MSG_INTERNAL,
IKE_PHASE1_COMPLETE
*Dec 25 23:20:46: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 25 23:20:46: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 192.1.24.4, remote= 192.1.24.5,
local_proxy= 192.168.3.1/255.255.255.255/0/0 (type=1),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
protocol= ESP, transform= esp-aes esp-sha-hmac (Tunnel),
lifedur= 2147483s and 4608000kb,
spi= 0x7C5C8CA2(2086440098), conn_id= 0, keysize= 128, flags= 0x400A

*Dec 25 23:20:46: ISAKMP: received ke message (1/18)
*Dec 25 23:20:47: ISAKMP: set new node 0 to QM_IDLE
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): sitting IDLE. Starting QM immediately
(QM_IDLE )
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):beginning Quick Mode exchange, M-ID of
381558818
*Dec 25 23:20:47: ISKAMP: growing send buffer from 1024 to 3072
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) QM_IDLE
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Node 381558818, Input =
IKE_MSG_INTERNAL, IKE_INIT_QM
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Old State = IKE_QM_READY New State =
IKE_QM_I_QM1
*Dec 25 23:20:47: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) QM_IDLE

```



```

*Dec 25 23:20:47: ISAKMP: set new node 1370878221 to QM_IDLE
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing HASH payload. message ID =
1370878221
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing NOTIFY RESPONDER_LIFETIME
protocol 1
spi 0, message ID = 1370878221, sa = 4620B514
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing responder lifetime
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): start processing isakmp responder
lifetime
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): restart ike sa timer to 86400 secs
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): deleting node 1370878221 error FALSE
reason "Informational (in) state 1"
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Input = IKE_MSG_FROM_PEER,
IKE_INFO_NOTIFY
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE

*Dec 25 23:20:47: ISAKMP (0:134217729): received packet from 192.1.24.5 dport
500 sport 500 Global (I) QM_IDLE
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing HASH payload. message ID =
381558818
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing SA payload. message ID =
381558818
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Checking IPsec proposal 1
*Dec 25 23:20:47: ISAKMP: transform 1, ESP_3DES
*Dec 25 23:20:47: ISAKMP: attributes in transform:
*Dec 25 23:20:47: ISAKMP: SA life type in seconds
*Dec 25 23:20:47: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
*Dec 25 23:20:47: ISAKMP: SA life type in kilobytes
*Dec 25 23:20:47: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Dec 25 23:20:47: ISAKMP: encaps is 1 (Tunnel)
*Dec 25 23:20:47: ISAKMP: authenticator is HMAC-MD5
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):atts are acceptable.
*Dec 25 23:20:47: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 192.1.24.4, remote= 192.1.24.5,
local_proxy= 192.168.3.1/255.255.255.255/0/0 (type=1),
remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
*Dec 25 23:20:47: Crypto mapdb : proxy_match
src addr : 192.168.3.1
dst addr : 0.0.0.0
protocol : 0
src port : 0
dst port : 0
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing NONCE payload. message ID =
381558818
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing ID payload. message ID =
381558818
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing ID payload. message ID =
381558818
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing NOTIFY RESPONDER_LIFETIME
protocol 3
spi 46397355, message ID = 381558818, sa = 4620B514
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):SA authentication status:
authenticated
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): processing responder lifetime
*Dec 25 23:20:47: ISAKMP (134217729): responder lifetime of 28800s
*Dec 25 23:20:47: ISAKMP: Locking peer struct 0x46564E80, IPSEC refcount 1
for for stuff_ke

```



```

*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): Creating IPsec SAs
*Dec 25 23:20:47:      inbound SA from 192.1.24.5 to 192.1.24.4 (f/i)  0/
0
      (proxy 0.0.0.0 to 192.168.3.1)
*Dec 25 23:20:47:      has spi 0xEA2A7A38 and conn_id 0 and flags 2
*Dec 25 23:20:47:      lifetime of 28790 seconds
*Dec 25 23:20:47:      lifetime of 4608000 kilobytes
*Dec 25 23:20:47:      has client flags 0x0
*Dec 25 23:20:47:      outbound SA from 192.1.24.4 to 192.1.24.5 (f/i) 0/0
      (proxy 192.168.3.1 to 0.0.0.0)
*Dec 25 23:20:47:      has spi 46397355 and conn_id 0 and flags A
*Dec 25 23:20:47:      lifetime of 28790 seconds
*Dec 25 23:20:47:      lifetime of 4608000 kilobytes
*Dec 25 23:20:47:      has client flags 0x0
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1): sending packet to 192.1.24.5 my_port 500
peer_port 500 (I) QM_IDLE
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):deleting node 381558818 error FALSE
reason "No Error"
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Node 381558818, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Dec 25 23:20:47: ISAKMP:(0:1:SW:1):Old State = IKE_QM_I_QM1  New State =
IKE_QM_PHASE2_COMPLETE
*Dec 25 23:20:47: IPSEC(key_engine): got a queue event with 2 kei messages
*Dec 25 23:20:47: IPSEC(initialize_sas): ,
      (key eng. msg.) INBOUND local= 192.1.24.4, remote= 192.1.24.5,
      local_proxy= 192.168.3.1/0.0.0.0/0/0 (type=1),
      remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
      protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
      lifedur= 28790s and 4608000kb,
      spi= 0xEA2A7A38(3928652344), conn_id= 0, keysize= 0, flags= 0x2
*Dec 25 23:20:47: Crypto mapdb : proxy_match
      src addr      : 192.168.3.1
      dst addr      : 0.0.0.0
      protocol      : 0
      src port      : 0
      dst port      : 0
*Dec 25 23:20:47: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and 192.1.24.5
*Dec 25 23:20:47: IPsec: Flow_switching Allocated flow for sibling 80000002
*Dec 25 23:20:47: IPSEC(policy_db_add_ident): src 192.168.3.1, dest 0.0.0.0,
dest_port 0

*Dec 25 23:20:47: ISAKMP: Locking peer struct 0x46564E80, IPSEC refcount 2
for from create_transforms
*Dec 25 23:20:47: IPSEC(create_sa): sa created,
      (sa) sa_dest= 192.1.24.4, sa_proto= 50,
      sa_spi= 0xEA2A7A38(3928652344),
      sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 3001
*Dec 25 23:20:47: IPSEC(create_sa): sa created,
      (sa) sa_dest= 192.1.24.5, sa_proto= 50,
      sa_spi= 0x2C3F7AB(46397355),
      sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 3002
*Dec 25 23:20:47: ISAKMP: Unlocking IPSEC struct 0x46564E80 from
create_transforms, count 1
*Dec 25 23:20:47: %CRYPTO-6-EZVPN_CONNECTION_UP: (Client) User= Group=EZVPN
Client_public_addr=192.1.24.4 Server_public_addr=192.1.24.5
Assigned_client_addr=192.168.3.1
*Dec 25 23:20:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
*Dec 25 23:20:47: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0,
changed state to up

```


→ It automatically created two interfaces:

R4#**show ip int brief**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.1.24.4	YES	NVRAM	up	up
FastEthernet0/1	unassigned	YES	NVRAM	administratively down	down
Serial0/0/0	unassigned	YES	NVRAM	administratively down	down
NVI0	unassigned	YES	unset	up	up
Loopback0	4.4.4.4	YES	NVRAM	up	up
Loopback1	192.168.3.1	YES	manual	up	up

→ Afterward, when you issue a ping packet “ping 10.2.2.1 source 4.4.4.4”, you can see that the following command increment itself.

→ This command can quickly check what channels there are.

R4#**show crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
1	FastEthernet0/0	192.1.24.4	set	HMAC_SHA+DES_56_CB	0	0
3001	FastEthernet0/0	192.1.24.4	set	DES+MD5	9	0
3002	FastEthernet0/0	192.1.24.4	set	DES+MD5	0	9

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

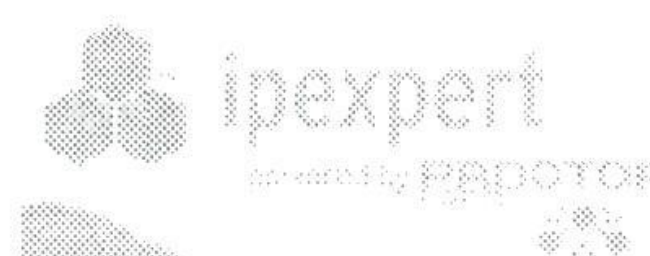
This page left intentionally blank.

Section 9: Switching

Estimated Time to Complete: 2 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 9 Pre-Lab Setup

- Physically connect and configure your network according to the Lab Topology provided above.
- This lab will focus on the Switches. You will need to pre-configure the network with the base IP Addressing using the pre-configuration files. You will find these configurations in the “Initial Configurations” subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs → Section 8 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the “MY CONFIGS” area of your *www.IPexpert.com* Member’s Area.

Configuring a Trunk and VTP Domains

Task 9-1

F 0/23 and F 0/24 are connected to each other on both switches. Configure both these links as trunk links. Set the encapsulation as ISL. Make sure the switches do not negotiate the trunk.

- Before we start the configuration let’s look at the trunk status.

```
Sw1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	desirable	n-isl	trunking	1
Fa0/24	desirable	n-isl	trunking	1

Port	Vlans allowed on trunk
Fa0/23	1-4094
Fa0/24	1-4094

Port	Vlans allowed and active in management domain
Fa0/23	1
Fa0/24	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/23	1
Fa0/24	none

- Note that the switch will automatically negotiate the port as a trunk port if the device on the other end can become a trunk port. We see that the encapsulation is n-isl and that status is trunking. The protocol that is used for automatic trunk negotiation is DTP (dynamic trunking protocol). The n-isl indicates that the trunk is using a negotiated encapsulation of ISL. You will also see that all of the VLANs are allowed across each trunk port. Lastly note that each link is a separate trunk.
- Use the `interface range` command to configure both interfaces at the same time. This will save you time when configuring more than 1 interface with identical commands. Use the same commands for both switches.
- Set the trunk encapsulation with the `switchport trunk encapsulation` command. Use `isl` encapsulation as specified.

- Set the port to be a trunk with the `switchport mode trunk` command.

```
Sw1(config)#interface range f0/23 -24
Sw1(config-if-range)#switchport trunk encapsulation isl
Sw1(config-if-range)#switchport mode trunk
```

- Configure the 2nd switch with the same commands.
- Now examine the trunk status with the `show interface trunk` command.

```
Sw1#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/23	on	isl	trunking	1
Fa0/24	on	isl	trunking	1

Port	Vlans allowed on trunk
Fa0/23	1-4094
Fa0/24	1-4094

Port	Vlans allowed and active in management domain
Fa0/23	1
Fa0/24	1

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/23	1
Fa0/24	none

Task 9-2

Configure a VTP Domain as **ipexpert** with a password of **ipexpert**. Do not use the VLAN database to accomplish this. Set Switch 1 as the Server and Switch 2 as the Client.

- Setup VTP, (VLAN Trunking Protocol), and set the VTP mode. A switch can be in one of 3 VTP modes:
- **Server** – this is the default mode for the switch. A VTP server can create, modify and delete VLANs locally. The server will propagate its VLANs throughout the network.
 - **Client** – a client will receive VLAN configuration from a VTP server in the same VTP domain and then modify its configuration. When a switch is in VTP client mode, you cannot change its VLAN configuration locally.
 - **Transparent** – when you configure a switch to be in the transparent mode – VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switches. VTP Version 2 will forward received VTP advertisements on all of its trunk links.
- To view VTP settings, use the `show vtp status` command.

```
Sw1#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 5
VTP Operating Mode          : Server
```



```

VTP Domain Name          :
VTP Pruning Mode         : Disabled
VTP V2 Mode              : Disabled
VTP Traps Generation     : Disabled
MD5 digest               : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

```

→ **VTP characteristics for a switch can be configured in either of 2 modes:**

- **VLAN Database Configuration Mode**
- **Config Mode**

→ **The requirements for this step specify that you should not use the VLAN database mode. From config mode, set the VTP mode on switch 1 to Server with the `vtp mode` command.**

```

Sw1(config)#vtp mode server
Device mode already VTP SERVER

```

→ **Configure the vtp domain name. The command used is `vtp domain`.**

```

Sw1(config)#vtp domain ipexpert
Changing VTP domain name from NULL to ipexpert

```

→ **This requirement calls for the vtp password to be set. This is an optional step for setting up vtp.**

→ **The password can be from 8 to 64 characters. When a VTP password is configured, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.**

→ **To configure the VTP password in the global config mode:**

```

Sw1(config)#vtp password ipexpert
Setting device VLAN database password to ipexpert

```

→ **To view VTP settings, use the `show vtp status` command.**

```

Sw1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            : ipexpert
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xD9 0x41 0x71 0x01 0x39 0x52 0x18 0x86
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

```

→ **To see the vtp password we have to use the `show vtp password` command.**

```

Sw1#show vtp password
VTP Password:ipexpert

```


- Set the VTP mode on switch 2 to Client with the `vtp mode` command.

```
Sw2(config)#vtp mode client
Setting device to VTP CLIENT mode
```

- Configure the vtp domain name. The command used is `vtp domain`.

```
Sw2(config)#vtp domain ipexpert
Changing VTP domain name from NULL to ipexpert
```

- Set the VTP password with the `vtp password` command.

```
Sw2(config)#vtp password ipexpert
Setting device VLAN database password to ipexpert
```

- To view VTP settings, use the `show vtp status` command.

```
Sw2#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 5
VTP Operating Mode          : Client
VTP Domain Name             : ipexpert
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xD9 0x41 0x71 0x01 0x39 0x52 0x18 0x86
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Creating VLANs and Assigning Ports to them

Task 9-3

Create the following three VLANs on Switch 1:

- 111 with a name of VLAN_Sales.
 - 112 with a name of VLAN_Finance.
 - 100 with a name of Trunk_VLAN.
- Create the VLANs on switch 1. We can create VLANs in either of 2 modes:
 - VLAN Configuration Mode
 - Config-vlan Mode
 - The commands are very close between the 2 modes. To save time, use the `vlan configuration` mode due to the fact that the VLAN can be created and named with one line. In `config-vlan` mode, two lines are necessary.

- First, an example using the vlan database mode.

```

Cat#vlan database
Sw1(vlan)#vlan 111 name VLAN_Sales
VLAN 111 added:
    Name: VLAN_Sales

Sw1(vlan)#vlan 112 name VLAN_Finance
VLAN 112 added:
    Name: VLAN_Finance

Sw1(vlan)#vlan 100 name Trunk_VLAN
VLAN 100 added:
    Name: Trunk_VLAN

Sw1(vlan)#exit
APPLY completed.
Exiting....
Sw1#

```

- Here is the config-vlan configuration mode.

```

Sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw1(config)#vlan 111
Sw1(config-vlan)#name VLAN_Sales
Sw1(config-vlan)#vlan 112
Sw1(config-vlan)#name VLAN_Finance
Sw1(config-vlan)#vlan 100
Sw1(config-vlan)#name Trunk_VLAN

```

- As you can see, it is easier to use the vlan database mode.
- Verify the vlan creation and naming with the show vlan command.

```

Sw1#show vlan

```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Gi0/1, Gi0/2
100	Trunk_VLAN	active	
111	VLAN_Sales	active	
112	VLAN_Finance	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

*****Rest of output omitted*****

Task 9-4

Make sure the VLANs are propagating to Switch 2 using VTP.

- Assuming that the VTP configuration was done properly, switch 1 should propagate the vlans and vlan names to switch 2. Verify the vlans appear on switch 2 with the `show vlan` command.

```
Sw2#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Gi0/1, Gi0/2
100	Trunk_VLAN	active	
111	VLAN_Sales	active	
112	VLAN_Finance	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

*****Rest of output omitted*****

Task 9-5

Assign R1 to VLAN 111 and R6 to VLAN 112.

- By default, a port will try to “auto” negotiate itself to be either a trunk port or an access port. To change this behavior, use the `switchport mode access` interface command.
- To assign a port to a specific VLAN, use the `switchport mode vlan interface` command, specifying the desired vlan. For this lab, R1 connects to port F 0/1 on switch 1, and R6 connects to port F 0/6 on switch 2.

```
Sw1(config)#interface f0/1
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 111
```

```
Sw2(config)#interface f0/6
Sw2(config-if)#switchport mode access
Sw2(config-if)#switchport access vlan 112
```


Creating VLAN Interfaces on the Switches

Task 9-6

Create a VLAN Interface on Switch 1 to connect to R1. Assign it an IP Address of 10.1.1.35/24.

- Create an SVI, (switch virtual interface), on switch 1 for VLAN 111, and assign it a layer 3 IP address. Use the `interface vlan` and the `ip address` commands. Applying an IP address to a SVI enables the routing of IP packets for that VLAN.

```
Sw1(config)#interface vlan 111
Sw1(config-if)#ip address 10.1.1.35 255.255.255.0
```

- You can verify this with the `show ip interface brief vlan 111` command.

```
Sw1#show ip interface brief vlan 111
Interface                IP-Address OK? Method Status    Protocol
Vlan111                  10.1.1.35  YES manual up        up
```

Task 9-7

Create a VLAN Interface on Switch 2 to connect to R6. Assign it an IP Address of 150.50.112.100/24.

- Create an SVI, (switch virtual interface), on switch 2 for VLAN 112, and assign it a layer 3 IP address. Use the `interface vlan` and the `ip address` commands.

```
Sw2(config)#interface vlan 112
Sw2(config-if)#ip address 150.50.112.100 255.255.255.0
```

- You can verify this with the `show ip interface brief vlan 112` command.

```
Sw1#show ip interface brief vlan 112
Interface                IP-Address OK? Method Status    Protocol
Vlan112                  150.50.112.100 YES manual up        up
```

Task 9-8

Create a VLAN interface on both switches to connect to each other over VLAN 100. Assign it an IP Address of 150.50.100.1/24 for Switch 1 and 150.50.100.2/24 for Switch.

- Create an SVI, (switch virtual interface), on each switch for VLAN 100, and assign layer 3 IP addresses. Use the `interface vlan` and the `ip address` commands.

```
Sw1(config)#interface vlan 100
Sw1(config-if)#ip address 150.50.100.1 255.255.255.0
```

```
Sw2(config)#interface vlan 100
Sw2(config-if)#ip address 150.50.100.2 255.255.255.0
```


- You can verify this with the `show ip interface brief vlan 100` command.

```
Sw1#show ip interface brief vlan 100
Interface          IP-Address      OK? Method Status  Protocol
Vlan100            150.50.100.1    YES manual up      up
```

Task 9-9

Make sure you can ping all directly connected devices.

- Verify by pinging R1 and Switch 2 from Switch 1. Ping R6 from switch 2.

```
Sw1#ping 150.50.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.50.100.2, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

Sw1#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/201/1000 ms

Sw2#ping 150.50.112.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.50.112.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1004 ms
```

Port Security

Task 9-10

An Application server connects to port 6 on Switch 1.

- Because this port connects to an application server, it is best practice to statically change the port to access mode, so that trunk auto-negotiation is disabled. Also, to enable port security, the port cannot be in the default dynamic mode.

```
Sw1(config)#interface f0/6
Sw1(config-if)#switchport mode access
```

Task 9-11

You want to make sure that no other device connects into that port. If another device connects into the port, you should shut the port down.

- Use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.

- To enable port security on a port, use the `switchport port-security interface` command.
- When the number of secure MAC addresses reaches the limit allowed on the port, a security violation occurs. There are 3 possible settings that can be configured to instruct the switch what action to take in the event of a security violation on a port.
 - Protect – drop packets from unknown source addresses
 - Restrict – drop packets from unknown source addresses, with logging and SNMP trap sent
 - Shutdown – interface becomes error-disabled, with logging and SNMP trap sent
- Shutdown mode is the default for port security violations. It can be changed with the `switchport port-security violation {protect | restrict | shutdown}` command.

```
Sw1(config)#interface f0/6
Sw1(config-if)#switchport port-security
```

Task 9-12

The MAC address of the port is 002A.115C.13DA.

- The default number of allowable MAC addresses for a port configured with port-security is one. If more were necessary, this could be configured with the `switchport port-security maximum value` command.
- To specify the allowed MAC address, use the `switchport port-security mac-address interface` command.

```
Sw1(config)#interface f 0/6
Sw1(config-if)#switchport port-security mac-address 002A.115C.13DA
```

- Verify port-security with the `show port-security address` and `show port-security interface` commands.

```
Sw1#sh port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
1       002a.115c.13da   SecureConfigured   Fa0/6    -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 5120

Sw1#show port-security interface f0/6
Port Security          : Enabled
Port Status            : Secure-down
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
```



```

Configured MAC Addresses      : 1
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0

```

VMPS Server Configuration

Task 9-13

There is a VMPS server at 10.1.1.150.

- **VMPS dynamically assigns dynamic access port VLAN membership. The 3550 switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it. The Catalyst 5000 and Catalyst 6000 switches can be a VMPS server.**
- **To configure the switch as a client, identify the VMPS server with the `vmmps server ipaddress` command. Task 9-16 states to configure switch 1 for VMPS.**

```
Sw1(config)#vmmps server 10.1.1.150 primary
```

Task 9-14

You would like to get VLAN assignment for all ports on switch 1 in dynamic mode from the VMPS server.

- **To specify that the access mode VLAN is dependent on the VLAN Membership Policy Server (VMPS) protocol, you must first configure the port to access mode. Then, use the `switchport access vlan dynamic` interface command.**
- **Use the `port-range` command in order to enter the VMPS interface commands for the appropriate ports. Only configure VMPS for those interfaces not statically assigned to a VLAN elsewhere in this lab.**

```

Sw1(config)#interface range f0/2 -5 , f0/7 , f0/9 -22 , g0/1 -2
Sw1(config-if-range)#switchport mode access
Sw1(config-if-range)#switchport access vlan dynamic

```

- **Verify your configuration with the `show interface interface-id switchport` command. Look in the Operational Mode field of the display.**

```

Sw1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic access
Operational Mode: dynamic access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: unassigned
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
*****Rest of output omitted*****

```


Task 9-15

You would like to reconfirm the assignment every 20 minutes.

- **VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs. Use the `vmps reconfirm minutes` global command.**

```
Sw1(config)#vmps reconfirm 20
```

Task 9-16

Configure Switch 1 for VMPS.

- **All VMPS commands were entered on Switch 1. Verify your configuration with the `show vmps` command.**

```
Sw1#show vmps
VQP Client Status:
-----
VMPS VQP Version:    1
Reconfirm Interval:  20 min
Server Retry Count:  3
VMPS domain server:  10.1.1.150 (primary, current)

Reconfirmation status
-----
VMPS Action:          other
```

Dot1x Authentication

Task 9-17

Configure Port 8 on Switch 1 for Dot1x authentication.

- **802.1x port-based authentication is a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.**
- **To enable 802.1x port-based authentication, you first must enable authentication, authorization, and accounting (AAA) and specify the authentication method. Currently, only RADIUS is supported as the authentication method.**
- **To enable AAA on the switch, use the `aaa new-model` command. To specify the authentication method, use the `aaa authentication dot1x default group radius` command.**
- **After enabling AAA, enable dot1x on the switch with the `dot1x system-auth-control` command.**

- Following is the global configuration for dot1x on switch 1:

```
Sw1(config)#aaa new-model
Sw1(config)#aaa authentication dot1x default group radius
Sw1(config)#dot1x system-auth-control
```

Task 9-18

Any device that connects to Port 8 should be authenticated by a RADIUS server located at 10.1.1.100. The RADIUS server uses **ipexpert** as the key and 1645 as the Authentication port.

- The RADIUS server host(s) used for authentication must be identified by hostname or IP address. Multiple servers can be configured for failover purposes; the entries are tried in the order that they were configured. Each server uses the `radius server host {hostname | ip-address} auth-port port-number key string command`.
- To specify an interface to be enabled for dot1x authentication, use the `dot1x port-control auto` command. The switchport mode cannot be dynamic.
- Here is the configuration for specifying the RADIUS server, and enabling dot1x on port 8 of switch 1:

```
Sw1(config)#radius-server host 10.1.1.100 key ipexpert
Sw1(config)#interface F 0/8
Sw1(config-if)#switchport mode access
Sw1(config-if)#dot1x port-control auto
01:02:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
changed state to down
```


CiscoSecure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://127.0.0.1:1152/

CISCO SYSTEMS

Network Configuration

Edit

Add AAA Client

AAA Client Hostname: Sw1

AAA Client IP Address: 10.1.1.35

Key: ipexpert

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Submit Submit + Apply Cancel

Back to Help

Help

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

AAA Client IP Address

The AAA Client IP Address is the IP

Applet encryptor started Internet

- You must specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.
- The port-number may default to a value of 1812. If the RADIUS server uses a different port number for UDP authentication requests, you can enter that value on the radius server host command.
- Re-enter the radius server host command using the required values if necessary:

```
Sw1(config)#radius-server host 10.1.1.100 auth-port 1645 key ipexpert
```

Task 9-19

- Configure a username of sales with a password of x1todsales. Configure a username of finance with a password of x1todfinance. User sales should be assigned to VLAN_Sales upon authentication. User finance should be assigned to VLAN_Finance upon authentication.

- In order for different users to have different Radius attributes, we have two options. We can either assign the users to different radius groups, or assign separate Radius attributes per user. If using multiple groups, the radius attributes are applied to the group, and the user is assigned to the group. If using per-user attributes, this needs to be enabled under interface configuration – advanced options – per-user TACACS+/RADIUS Attributes. Individual attributes also need to be enabled for users under interface configuration – RADIUS.

CiscoSecure ACS – Microsoft Internet Explorer

Address: <http://127.0.0.1:3971/>

User Setup

Edit

User: sales

☐ Account Disabled

Supplementary User Info

Real Name: sales user

Description:

User Setup

Password Authentication:

☐ ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

☐ Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

Deleting a Username

The Delete button appears only when you are editing an existing user account, not when you are adding a new user.

Applet has failed to start

Cisco Systems

User Setup

Edit **Help**

User: finance

☐ Account Disabled

Supplementary User Info ?

Real Name:

Description:

User Setup ?

Password Authentication:

(Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

☐ Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card may allow CHAP

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top](#)

Deleting a Username

Applet nas_filter started Internet

- In order for the switch to allow dynamic VLAN changes from the RADIUS server, add network authorization to the switch configuration.

```
Sw1(config)#aaa authorization network default group radius
```

- If you have configured for per-user attributes, you will see them available at the bottom of the user setup page.

Task 9-20

The Switch should re-authenticate every 2 hours.

- ➔ You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600.
- ➔ To enable re-authentication, use the `dot1x reauthentication` interface command.
- ➔ To change the re-authentication timeout value, use the `dot1x timeout reauth-period seconds` interface command.
- ➔ Following is the configuration to meet the requirements of this task:

```
Sw1(config)#interface f0/8
Sw1(config-if)#dot1x reauthentication
Sw1(config-if)#dot1x timeout reauth-period 7200
```


→ **Verify the dot1x configuration:**

```
Sw1#show dot1x
Sw1#show dot1x
Sysauthcontrol           = Enabled
Supplicant Allowed In Guest Vlan = Disabled
Dot1x Protocol Version   = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

```
Sw1#show dot1x interface f0/8
PortStatus               = UNAUTHORIZED
MaxReq                   = 2
MaxAuthReq               = 2
HostMode                 = Single
PortControl              = Auto
QuietPeriod              = 60 Seconds
Re-authentication        = Enabled
ReAuthPeriod             = 7200 Seconds
ServerTimeout            = 30 Seconds
SuppTimeout              = 30 Seconds
TxPeriod                 = 30 Seconds
Guest-Vlan               = 0
```

Routing on the Switch

Task 9-21

Configure EIGRP in AS 1 as the routing protocol between R6, Sw2 and Sw1.

- **By default, IP routing is disabled on the 3550 switch. In order to enable Layer 3 services, you must enable IP routing. Use the `ip routing` command to enable routing on each switch.**

```
Sw1(config)#ip routing
```

```
Sw2(config)#ip routing
```

- **Now setup the EIGRP routing process to run on the switches and on R6. You will use the `router eigrp as-number` command for this.**
- **Auto summary allows the automatic summarization of subnet routes into network-level routes and is enabled by default. To disable this, use the `no auto-summary` command under the EIGRP process.**
- **Enter the following configuration commands on each switch and on R6.**

```
Sw1(config)#router eigrp 1
Sw1(config-router)#no auto-summary
```

- **Use the `network` command to enable EIGRP to send updates to the interfaces that connect R6, Sw2 and Sw1. This means that EIGRP will send out routing updates and try to form adjacencies over interfaces that are defined with the `network` command.**

```
R6(config)#router eigrp 1
R6(config-router)#network 150.50.112.0 0.0.0.255
```



```
Sw2 (config)#router eigrp 1
Sw2 (config-router)#network 150.50.112.0 0.0.0.255
Sw2 (config-router)#network 150.50.100.0 0.0.0.255

Sw1 (config)#router eigrp 1
Sw1 (config-router)#network 150.50.100.0 0.0.0.255
Sw1 (config-router)#network 150.50.111.0 0.0.0.255
```

Task 9-22

Advertise the Loopback on R6 in EIGRP 1.

- To advertise a network under EIGRP use the `network network-number [network-mask]` command. The network command also enables EIGRP to send updates to the interfaces in the specified networks. This means that EIGRP will send out routing updates and try to form adjacencies over interfaces that are defined with the network command.

```
r6 (config-router)#network 6.0.0.0
```

Task 9-23

Authenticate all EIGRP devices using MD5 authentication and key of `ipexpert`.

- EIGRP route authentication provides MD5 authentication of routing updates to prevent the introduction of unauthorized or false routing messages from unapproved sources.
- You first must specify a text key string that is identical on each EIGRP neighbor router. Use the key-chain configuration mode to specify the text string. The format of the key-chain configuration is:

```
key-chain name-of-chain
      key number
            key-string text
```

- Following is an example of specifying a key for R6. These commands will need to be entered on ALL routers participating in EIGRP route authentication.

```
R6 (config)#key chain EIGRP
R6 (config-keychain)#key 1
R6 (config-keychain-key)#key-string ipexpert
```

- Use the `show key chain` command to see the key-string:

```
R6#show key chain
Key-chain EIGRP:
  key 1 -- text "ipexpert"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
```

- To enable route authentication, you must enable authentication of EIGRP packets on each interface which is sending and receiving EIGRP packets, and identify the key-chain to use. You must also specify the authentication mode, of which MD5 is the only choice for EIGRP.

- The interface command to enable route authentication is `ip authentication key-chain eigrp autonomous-system key-chain`.
- The interface command to specify MD5 authentication is `ip authentication mode eigrp autonomous-system md5`.
- Following is an example of the necessary configuration for each of the devices, R6, Sw1 and Sw2 that are participating in EIGRP route authentication.

```
R6(config)#interface FastEthernet0/0
R6(config-if)#ip authentication mode eigrp 1 md5
R6(config-if)#ip authentication key-chain eigrp 1 EIGRP
```

```
Sw1(config)#interface Vlan100
Sw1(config-if)#ip authentication mode eigrp 1 md5
Sw1(config-if)#ip authentication key-chain eigrp 1 EIGRP
```

```
Sw2(config)#interface Vlan100
Sw2(config-if)#ip authentication mode eigrp 1 md5
Sw2(config-if)#ip authentication key-chain eigrp 1 EIGRP
Sw2(config)#interface Vlan112
Sw2(config-if)#ip authentication mode eigrp 1 md5
Sw2(config-if)#ip authentication key-chain eigrp 1 EIGRP
```

- Verify the neighbor relationships with the `show ip eigrp neighbors` command from Sw2. The display should show both R6 and Sw1 as neighbors.

```
Sw2#show ip eigrp neighbor
```

```
IP-EIGRP neighbors for process 1
H   Address                Interface      Hold Uptime    SRTT   RTO   Q   Seq Type
                               (sec)          (ms)
1   150.50.112.6            Vl112         13 00:00:24     4    200   0    5
0   150.50.100.1            Vl100         11 00:00:36   1536   5000   0    7
```

- Check the routing table on Sw1 to make sure that you see all of the configured networks and loopbacks properly.

```
Sw1#show ip route eigrp
D    6.0.0.0/8 [90/131072] via 150.50.100.2, 00:01:18, Vlan100
    150.50.0.0/24 is subnetted, 3 subnets
D      150.50.112.0 [90/3072] via 150.50.100.2, 00:01:33, Vlan100
```

Task 9-24

Run BGP between R1 and Sw1. Sw1 should be AS 100 and R1 should be AS 1.

- To configure the BGP process use the `router bgp as-number` command on each device.

```
r1(config)#router bgp 1
```


- It is generally best practice to disable auto-summary, unless told otherwise. This disables the automatic summarization of subnet routes into network-level routes.

```
r1(config-router)#no auto-summary
```

- Next, configure R1 to peer to Sw1 in AS100. Use the `neighbor {ip-address | peer-group-name} remote-as as-number` command.

```
r1(config-router)#neighbor 150.50.111.100 remote-as 100
```

- Now, configure Sw1 to peer to R1 in AS100.

```
Sw1(config)#router bgp 100
```

```
Sw1(config-router)#no auto-summary
```

```
Sw1(config-router)#neighbor 150.50.111.1 remote-as 1
```

- Use the `show ip bgp summary` command to check the configuration:

```
r1#sh ip bgp summary
```

```
BGP router identifier 1.1.1.1, local AS number 1
```

```
BGP table version is 1, main routing table version 1
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
150.50.111.100	4	100	2	2	0	0	0	00:00:21	0

Task 9-25

Advertise the Loopback on R1 in BGP.

- To advertise a network in BGP, use the `network network-number` command to specify a network as local to this AS.

```
R1(config)#router bgp 1
```

```
R1(config-router)#network 1.0.0.0
```

- Check that the route is now in the routing tables of Sw1.

```
Sw1#sh ip bgp
```

```
BGP table version is 2, local router ID is 150.50.111.100
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,  
r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 1.0.0.0	150.50.111.1	0		0	1 i

Task 9-26

Configure mutual redistribution on Sw1 between EIGRP in AS 1 and BGP.

- To redistribute routes from one routing protocol to another, use the `redistribute` command in router configuration mode. For mutual distribution, as specified in this task, you will need to redistribute the EIGRP-learned routes into BGP, and redistribute the BGP-learned routes into EIGRP.

```
Sw1(config)#router bgp 100
Sw1(config-router)#redistribute eigrp 1
Sw1(config)#router eigrp 1
Sw1(config-router)#redistribute bgp 100 metric 1544 20000 255 1 1500
```

- When any routing protocol is redistributed into EIGRP, an EIGRP metric must be assigned to all the networks from the routing protocol that is being redistributed.

Task 9-27

All devices should see all routes in their routing tables.

- Check the routing tables on R1 and R6 to make sure that you see all of the configured networks and loopbacks properly.
- On R6, check for network 1.0.0.0, since this is advertised by BGP on R1, redistributed into EIGRP by Sw1, and R6 is running EIGRP.

```
R6#show ip route
D EX 1.0.0.0/8 [170/6780672] via 150.50.112.100, 00:00:31, FastEthernet0/0
C    6.0.0.0/8 is directly connected, Loopback0
    150.50.0.0/24 is subnetted, 2 subnets
D      150.50.100.0 [90/28416] via 150.50.112.100, 00:19:13, FastEthernet0/0
D      150.50.111.0 [90/28672] via 150.50.112.100, 00:19:13, FastEthernet0/0

C      150.50.112.0 is directly connected, FastEthernet0/0
```

- On R1, check for network 6.0.0.0, since this is advertised by EIGRP on R6, redistributed into BGP by Sw1, and R1 is running BGP.

```
R1#show ip route
C    1.0.0.0/8 is directly connected, Loopback0
B    6.0.0.0/8 [20/131072] via 150.50.111.100, 00:02:40
    150.50.0.0/24 is subnetted, 3 subnets
B      150.50.100.0 [20/0] via 150.50.111.100, 00:02:40
C      150.50.111.0 is directly connected, FastEthernet0/0
B      150.50.112.0 [20/3072] via 150.50.111.100, 00:02:40
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

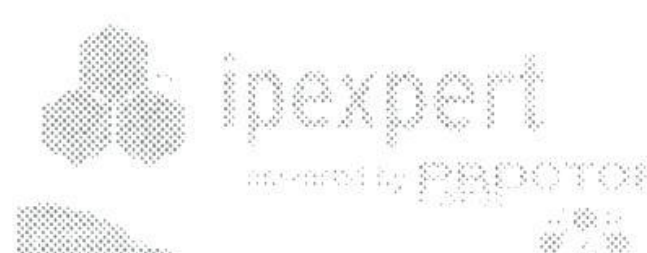
This page left intentionally blank.

Section 10: IDS

Estimated Time to Complete: 4 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 10 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 10-A.
- This lab will focus strictly on IDS. You will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers and the PIX. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 9 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Section 10 Configuration Tasks

IDS on a PIX

Task 10-1

Configure a Syslog Server at 10.1.1.100. Configure the PIX to send message to the Syslog server.

- You are setting the syslog server with the command required as shown below:

```
pixfirewall(config)#logging host inside 10.1.1.100
```

Task 10-2

Configure Console Logging to level 4. Configure Trap logging level to debugging.

- We can set the logging for trap to be debugging, and the console to be level 4, which is warning.

```
pixfirewall(config)#logging console warnings  
pixfirewall(config)#logging trap debugging
```

Task 10-3

Configure the PIX IDS with the following parameters:

- Send an alarm for Info signatures
 - Send an alarm and drop packets for Attack signatures
- We define the audit name to be PIX-INFO and PIX-ATTACK for the two required action.

```
pixfirewall(config)#ip audit name PIX-INFO info action alarm  
pixfirewall(config)#ip audit name PIX-ATTACK attack action alarm drop  
pixfirewall(config)#ip audit info action alarm  
pixfirewall(config)#ip audit attack action alarm drop
```


Task 10-4

You do not want signature 2004 to fire at all.

- **We can disable the 2004 signature with this command.**

```
pixfirewall(config)#ip audit signature 2004 disable
```

Task 10-5

Protect the PIX from the outside interface.

- **We can protect the outside interface from the two audits we defined previously.**

```
pixfirewall(config)#ip audit interface outside PIX-INFO
pixfirewall(config)#ip audit interface outside PIX-ATTACK
```

- **Show ip audit count can be used to check the output:**

```
pixfirewall#show ip audit count interface outside
IP AUDIT INTERFACE COUNTERS: outside
```

1000	I	Bad IP Options List	0
1001	I	Record Packet Route	0
1002	I	Timestamp	0
1003	I	Provide s,c,h,tcc	0
1004	I	Loose Source Route	0
1005	I	SATNET ID	0
1006	I	Strict Source Route	0
1100	A	IP Fragment Attack	0
1102	A	Impossible IP Packet	0
1103	A	IP Teardrop	0
2000	I	ICMP Echo Reply	0
2001	I	ICMP Unreachable	0
2002	I	ICMP Source Quench	0
2003	I	ICMP Redirect	0
2004	I	ICMP Echo Request	0
2005	I	ICMP Time Exceed	0
2006	I	ICMP Parameter Problem	0
2007	I	ICMP Time Request	0
2008	I	ICMP Time Reply	0
2009	I	ICMP Info Request	0
2010	I	ICMP Info Reply	0
2011	I	ICMP Address Mask Request	0
2012	I	ICMP Address Mask Reply	0
2150	A	Fragmented ICMP	0
2151	A	Large ICMP	0
2154	A	Ping of Death	0
3040	A	TCP No Flags	0
3041	A	TCP SYN & FIN Flags Only	0
3042	A	TCP FIN Flag Only	0
3153	A	FTP Improper Address	0
3154	A	FTP Improper Port	0
4050	A	Bomb	0
4051	A	Snork	0
4052	A	Chargen	0
6050	A	DNS Host Info	0
6051	A	DNS Zone Xfer	0
6052	A	DNS Zone Xfer High Port	0


```

6053 A DNS All Records 0
6100 I RPC Port Registration 0
6101 I RPC Port Unregistration 0
6102 I RPC Dump 0
6103 A Proxied RPC 0
6150 I ypserv Portmap Request 0
6151 I ypbind Portmap Request 0
6152 I yppasswdd Portmap Request 0
6153 I ypupdated Portmap Request 0
6154 I ypxfrd Portmap Request 0
6155 I mountd Portmap Request 0
6175 I rexd Portmap Request 0
6180 I rexd Attempt 0
6190 A statd Buffer Overflow 0

```

```
pixfirewall#
```

IDS on a Router

Task 10-6

Configure the IOS IDS on R6 with the following parameters:

- Name the rule set IOS-IDS
- Send the alarm to a syslog server
- Configure the router with the syslog server's translation address.
- You would set the default actions for the attack and info signatures by configuring it as below. Since the default for info signatures is alarm, you will not see anything in the configuration. You also need to set the notification configurations globally.
- Remember to set these values in your named IDS configuration as well.

```

R6(config)#ip ips notify log <--- (For older IOS versions, the
command syntax is ip audit notify log.)
R6(config)#logging host 192.1.24.100

```

Task 10-7

The logging server is located at 10.1.1.100. Translate that address to 192.1.24.100 for the outside networks on the PIX. Allow appropriate entries in the Access List of the PIX.

- Define the logging with the logging command. On the PIX, we need a translation, and permit the syslog traffic in the outside interface. Also from the PIX, we need to translate it to 192.1.24.100 and permit the syslog data to go through.

```

r6(config)#logging 192.1.24.100

pixfirewall(config)#static (inside,outside) 192.1.24.100 10.1.1.100
netmask 255.255.255.255 0 0
pixfirewall(config)#access-list infilter permit udp host 192.1.24.6
host 192.1.24.100 eq syslog

```


Task 10-8

You do not want signatures to fire from 192.1.24.10 for the IOS-IDS Rule Set.

```
R6(config)#access-list 8 deny 192.1.24.10
R6(config)#access-list 8 permit any
R6(config)#ip ips name IOS-IPS list 8
```

Task 10-9

You do not want signatures 2150 to fire from 192.1.24.4.

```
R6(config)#access-list 9 deny 192.1.24.4
R6(config)#access-list 9 permit any
R6(config)#ip ips signature 2150 list 9
%IPS Signature 2150:0 will use acl
```

Task 10-10

You do not want signature 2004 to fire at all

```
R6(config)#ip ips signature 2004 disable
%IPS Signature 2004:0 is disabled
```

Task 10-11

On R6, Protect traffic coming in thru the Fa 0/0 interface.

```
R6(config)#int fa0/0
R6(config-if)#ip ips IOS-IPS in
```

- **Signature 2004 is the signature for echo request. Pinging R6 from the PIX or R4 will not fire the signature. Pinging R4 from R6 should cause the signature 2000 to fire, and pinging the PIX should not cause the signature to fire.**

```
R6#ping 192.1.24.4
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.24.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R6#
*Jan 27 19:19:55.606: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo
Rply [192.1.24.4:0 -> 192.1.24.6:0]
*Jan 27 19:19:55.610: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo
Rply [192.1.24.4:0 -> 192.1.24.6:0]
*Jan 27 19:19:55.610: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo
Rply [192.1.24.4:0 -> 192.1.24.6:0]
*Jan 27 19:19:55.614: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo
Rply [192.1.24.4:0 -> 192.1.24.6:0]
*Jan 27 19:19:55.614: %IPS-4-SIGNATURE: Sig:2000 Subsig:0 Sev:2 ICMP Echo
Rply [192.1.24.4:0 -> 192.1.24.6:0]ping 192.1.24.10
```



```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.24.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R6#
```

- **Note:** Depending on how new the IOS version is that you are using, the command syntax could be either IP IPS or IP audit (older).
- **For verification, use the commands show ip audit interfaces, show ip audit configuration, and show ip audit statistics.**

```
R6#show ip audit interfaces
Interface Configuration
  Interface FastEthernet0/0
    Inbound IPS rule is IOS-IPS
    acl list 8
    Outgoing IPS rule is not set
R6#show ip audit configuration
Configured SDF Locations: none
Builtin signatures are enabled and loaded
Last successful SDF load time: 19:11:27 UTC Jan 27 2007
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is disabled
Total Active Signatures: 132
Total Inactive Signatures: 0
Signature 2004:0 disable
Signature 2150:0 list 9
Signature 1107:0 disable
IPS Rule Configuration
  IPS name IOS-IPS
  acl list 8
Interface Configuration
  Interface FastEthernet0/0
    Inbound IPS rule is IOS-IPS
    acl list 8
    Outgoing IPS rule is not set

R6#show ip audit statistics
Signature statistics [process switch:fast switch]
  signature 2000:0 packets checked: [0:22]
  signature 2001:0 packets checked: [0:128]
  signature 2150:0 packets checked: [0:3]
  signature 2151:0 packets checked: [0:21]
Interfaces configured for ips 1
Session creations since subsystem startup or last reset 0
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:0:0]
Last session created never
Last statistic reset never

R6#
```


Basic configuration and IDS Sensor Configuration from the CLI

Task 10-12

Configure RSPAN on the Switch to copy all traffic from R6, R4 and PIX outside to the Monitoring Interface on the IDS Sensor.

- First we need to create the remote-span vlan on the VTP server

```
Sw1(config)#vlan 50
Sw1(config-vlan)#remote-span
```

- Next we need to configure switch 1 to monitor both the remote-span VLAN as well as the VLAN ports on this switch and to send the traffic to the port that the IDS sensing interface is connected to.

```
Sw1(config)#monitor session 1 destination interface Fa0/7
Sw1(config)#monitor session 1 source vlan 24 , 50 rx
```

- Finally we configure switch 2 to monitor the vlan and mirror the traffic to the remote-span VLAN. For the reflector port you can use any *UNUSED* port on the 3550. Make sure that this port is not in use as its ASICs will be used to send this data and the port will no longer be able to service clients until the monitor session is removed.

```
Sw2(config)#monitor session 1 source vlan 24 rx
Sw1(config)#monitor session 1 destination remote vlan 50 reflector-
port Fa0/18
```

Task 10-13

Configure Telnet on R1.

Here, we just need to set a password for any telnet to R1.

```
R1(config)#line vty 0 4
R1(config-line)#password telnet
R1(config-line)#login
```

Task 10-14

Create a Static for R1 on the PIX to 192.1.24.11. Allow the outside network to Telnet into R1.

- We configure a static translation on the PIX, and create an entry in the acl to allow the outside network to telnet to this external address.

```
pixfirewall(config)#static (inside,outside) 192.1.24.11 10.2.2.1
netmask 255.255.255.255 0 0
pixfirewall(config)#access-list infilter permit tcp 192.1.24.0
255.255.255.0 host 192.1.24.11 eq telnet
```


Task 10-15

Allow the Inside Networks to Telnet into the PIX.

- **We allow the telnet from the inside network 10.1.1.0/24 and 10.2.2.0/24 to telnet to the PIX.**

```
pixfirewall(config)#telnet 10.1.1.0 255.255.255.0 inside
pixfirewall(config)#telnet 10.2.2.0 255.255.255.0 inside
```

Task 10-16

Configure the IDS Sensor with an IP Address of 10.1.1.15 and a default gateway of 10.1.1.1 (R1) from the CLI.

```
Continue with configuration dialog?[yes]:
Enter host name[sensor]: IPS
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.15/24,10.1.1.1
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
    No entries
Permit: 10.1.1.0/24
Permit:
Modify system clock settings?[no]:
Modify virtual sensor "vs0" configuration?[no]:
```

The following configuration was entered.

```
service host
network-settings
host-ip 10.1.1.15/24,10.1.1.1
host-name IPS
telnet-option disabled
access-list 10.1.1.0/24
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

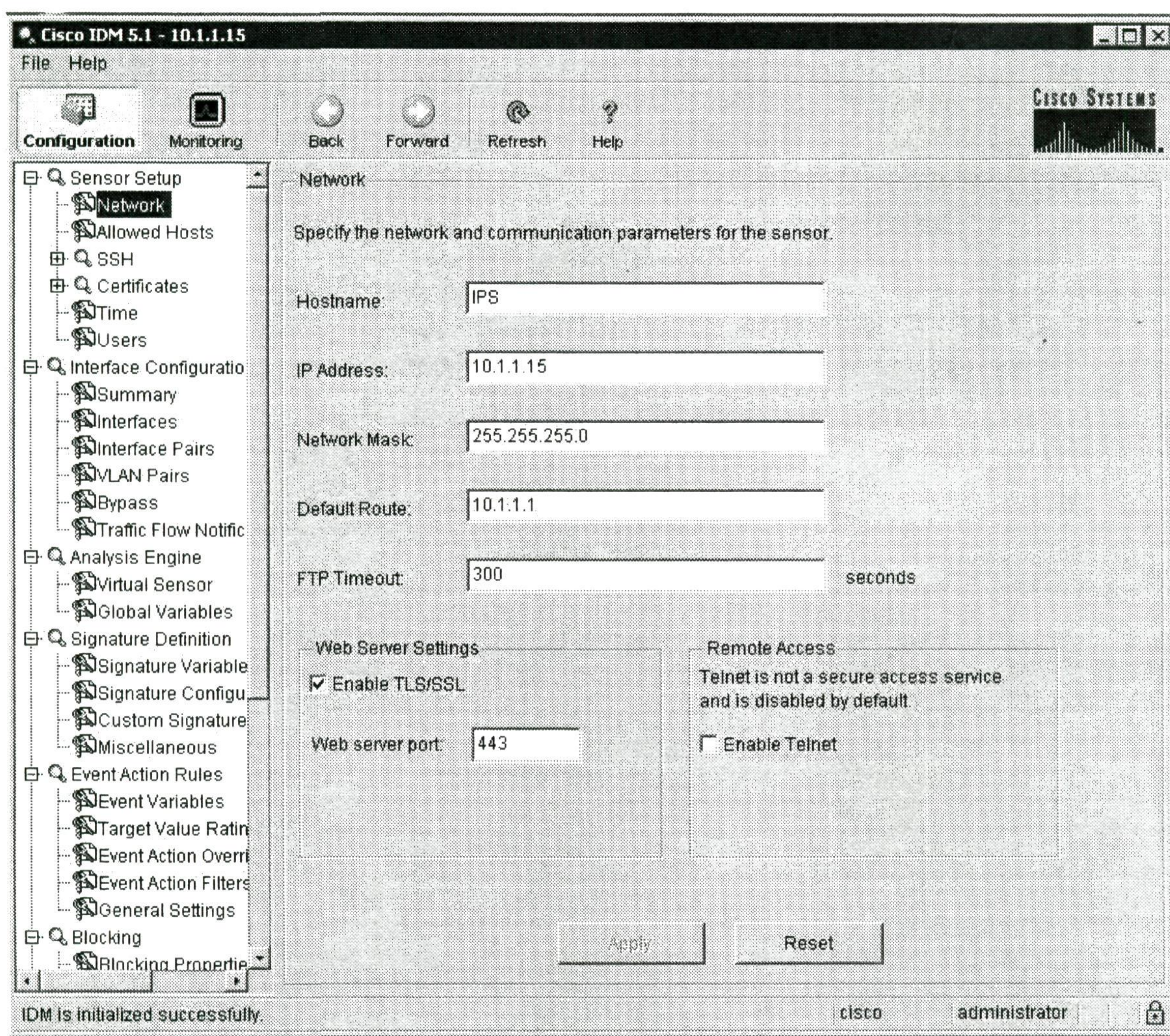
- [0] Go to the command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration and exit setup.

```
Enter your selection[2]: 2
```


Task 10-17

Verify that you can open the device manager from the ACS server.

- ➔ **Connect to the IPS Device manager by opening a browser window to <https://10.1.1.15>. Select Yes when prompted for security warnings.**

**Signature and Sensor Tuning****Task 10-18**

Enable the ICMP Echo Signature 2004.

- ➔ **Select Signature configuration, scroll down to 2004, select, and click Enable.**

Task 10-19

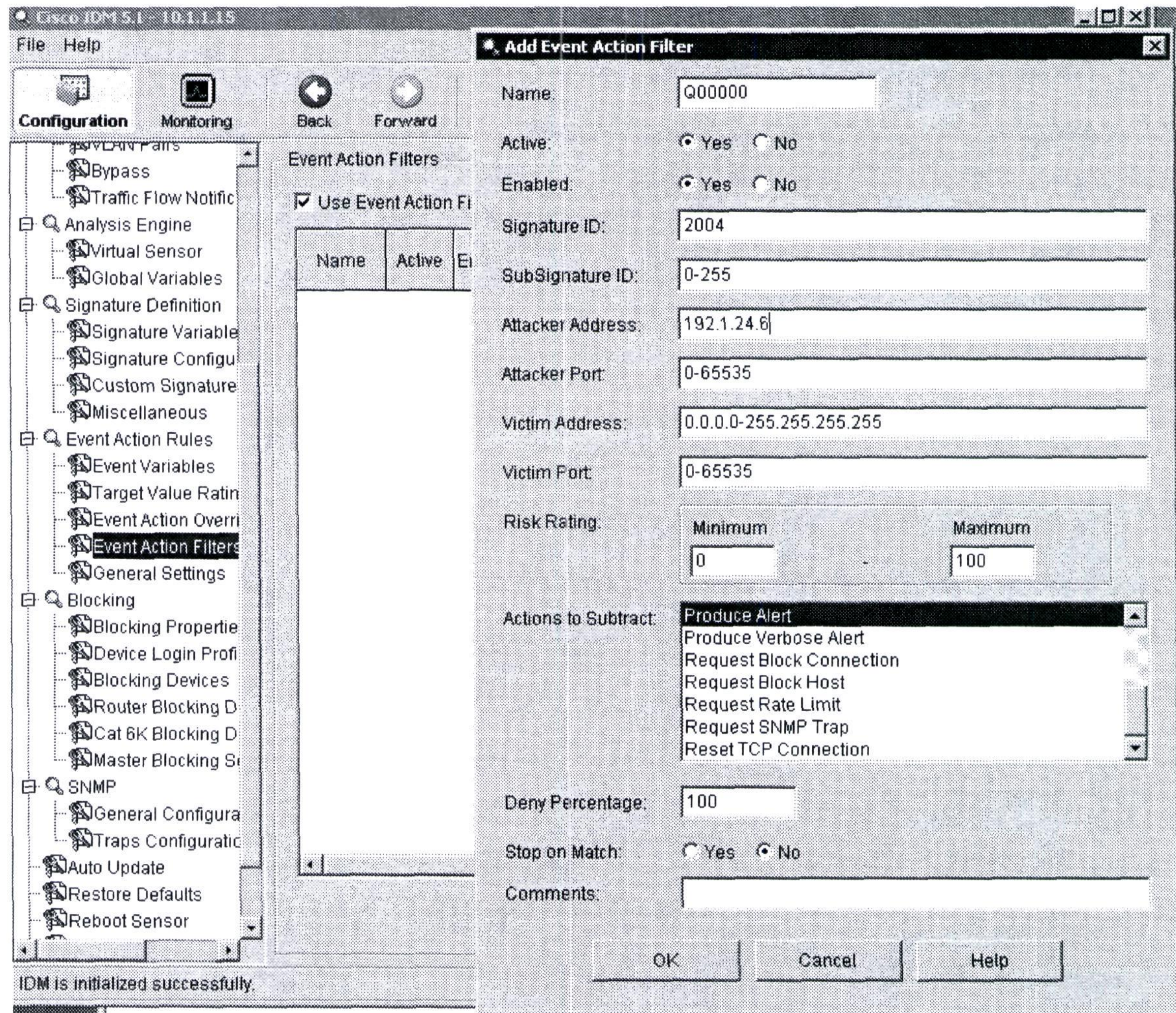
Configure the Alarm severity to Medium.

- ➔ **Right click on the signature, and select "Set severity to.. Medium"**

Task 10-20

You don't want the 2004 signature to fire from R6.

- **Configure an event action filter for signature 2004, using the event action filters option under Event action rules as shown below. Select OK and apply to sensor.**

**Task 10-21**

Configure IDS for BSD reassembly.

- **Under Signature Definition, Miscellaneous, select BSD for Fragment Reassembly.**

Task 10-22

Configure the fa0/1 interface for monitoring traffic.

- **Select Edit virtual sensor, and assign Fa0/1 to the virtual sensor. Also make sure you enable the Fa0/1 interface under Interface configuration, interfaces.**

- ➔ Ping from R6 to the PIX and from the PIX to R6. When the PIX pings R6, the event should fire. When R6 pings the PIX, the event should not show up in the event viewer, due to the filter configured. If you look at the event details for the Alert, you can see what source and destination triggered the Alert.

The screenshot shows the Cisco IDM 5.1 - 10.3.1.15 Event Viewer interface. The main window displays a table of events with the following data:

#	Type	Sensor UTC Time	Event ID	Events	Sig ID
1	error:warning	January 27, 2007 12:15:48 ...	1166453279279743020	New host ip [10.1.1.15]	
2	alert:medium...	January 27, 2007 12:51:20 ...	1166453279279743075	ICMP Echo Request	2004
3	alert:medium...	January 27, 2007 12:51:50 ...	1166453279279743092	ICMP Echo Request	2004

A detailed view for event ID 1166453279279743092 is shown in a separate window. The details include:

```

evIdsAlert: eventId=1166453279279743092 vendor=Cisco severity=medium
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 343
time: January 27, 2007 12:51:50 PM UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=$1
  subSigId: 0
interfaceGroup:
  vlan: 0
participants:
  attacker:
    addr: 192.1.24.10 locality=OUT
  target:
    addr: 192.1.24.6 locality=OUT
summary: 5 final=true initialAlert=1166453279279743075 summaryType=Regular
alertDetails: Regular Summary: 5 events this interval ;
riskRatingValue: 75
interface: fe0_1
protocol: icmp
  
```

Configuring a Custom Signature

Task 10-23

Create a custom signature to fire if a packet is received for Telnet with the word "attack" in it.

- ➔ Signature Definition, Custom Signature Wizard,
- ➔ Select STRING TCP as the engine, next, next
- ➔ Enter attack as the regex string, and select port 23 for service ports, next.
- ➔ Select HIGH for severity, next
- ➔ Select Finish

Task 10-24

Set the Severity level to high.

- ➔ **This task has already been completed in step 23.**

Task 10-25

Configure it send an alarm if the signature is detected.

- ➔ **This task has already been completed in step 23.**

Task 10-26

Telnet into R1 from the outside to test it by typing in the word "attack".

- ➔ **Verify that the alert fires by checking the event viewer.**

Configuring the IDS to shun the connection on the PIX**Task 10-27**

Configure IP Blocking on the IDS Sensor.

- ➔ **Under Blocking, Device Login Profiles, add a profile with password cisco and enable password cisco, apply.**

Task 10-28

Configure the PIX firewall as a Managed Device under IDS Sensor. Use the Telnet password as **cisco**.

- ➔ **Under Blocking devices, add the PIX as a blocking device, using the login profile created in the prior step. Select Telnet as the communication protocol.**

Task 10-29

Change the Signature action for ICMP 2004 to shun.

- ➔ **Select Block Host as an action for the signature.**

Task 10-30

Verify by pinging the outside interface of the PIX.

→ **Check the PIX after pinging, and you should see the SHUN.**

```
R4#ping 192.1.24.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.1.24.10, timeout is 2 seconds:
```

```
!!!!.
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

```
R4#
```

```
pixfirewall#show shun
```

```
shun (outside) 192.1.24.4 0.0.0.0 0 0 0.
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

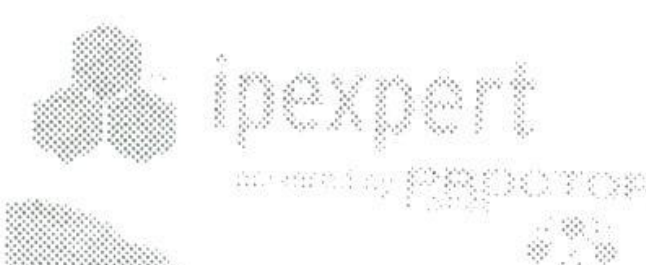
This page left intentionally blank.

Section 10B: IPS

Estimated Time to Complete: 1 Hour

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 10B Pre-Lab Setup

- Physically connect and configure your network according to Diagram 10B-1.
- This lab will focus strictly on IDS. You will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers and the PIX. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs* → *Section 10* → *Initial Configurations* → *Router X.txt*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

Section 10B Configuration Tasks

IDS using interface pairs

Task 10-31

Configure the IDS from the CLI for initial setup. Configure the IP address for the command and control interface to 10.1.1.55. Configure the access-list to allow the address of the ACS server. Configure a default gateway of 10.1.1.100, the address of the ACS server.

```
IDSsensor#setup
```

```
--- System Configuration Dialog ---
```

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

```
Continue with configuration dialog?[yes]: yes
Enter host name[sensor]: IDSsensor
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.55/24,10.1.1.100
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.0/24
Permit:
Modify system clock settings?[no]:
Modify virtual sensor "vs0" configuration?[no]:
```

The following configuration was entered.

```
service host
network-settings
host-ip 10.1.1.55/24,10.1.1.100
host-name IDSsensor
telnet-option disabled
access-list 10.1.1.0/24
ftp-timeout 300
no login-banner-text
exit
```



```

time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit

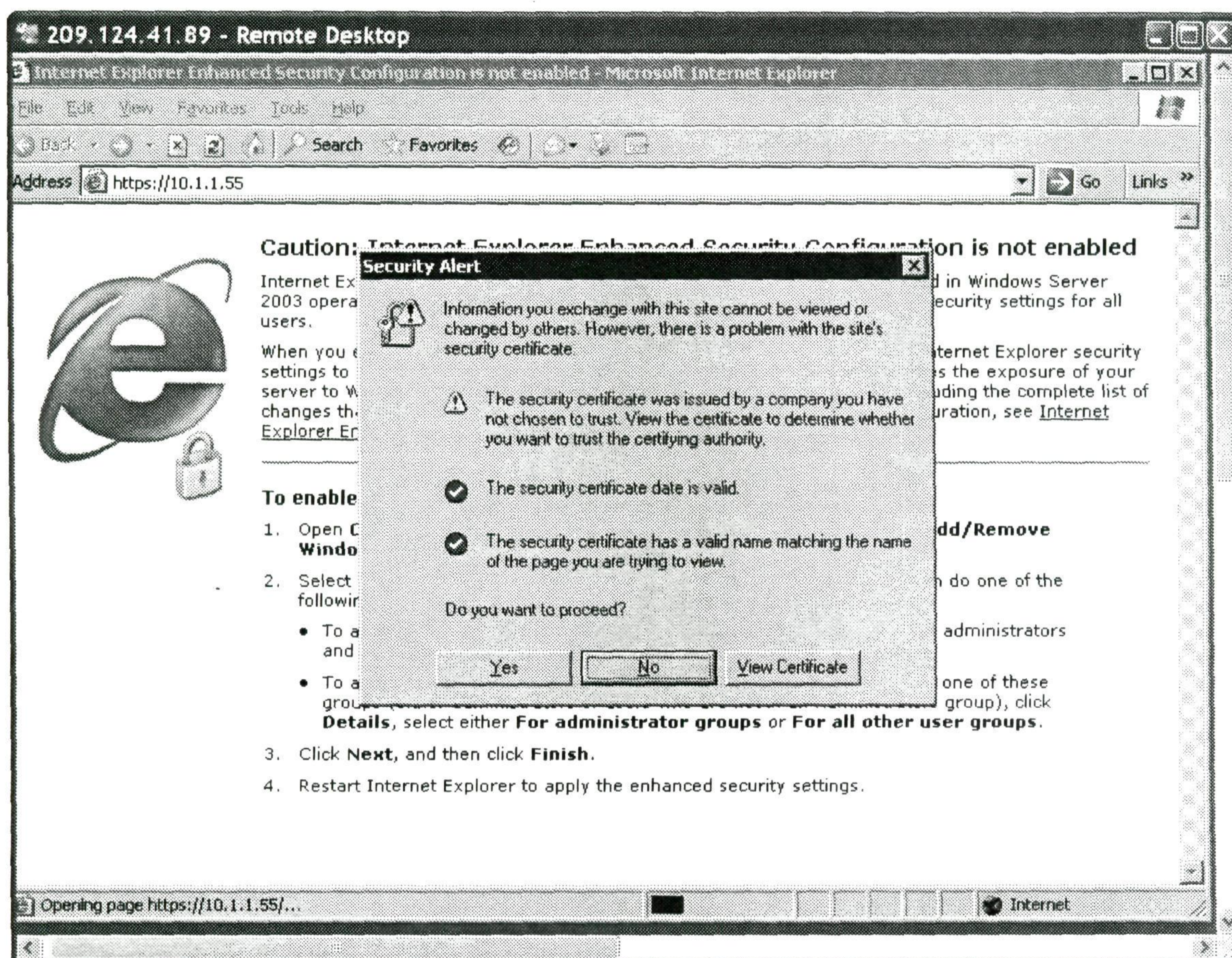
```

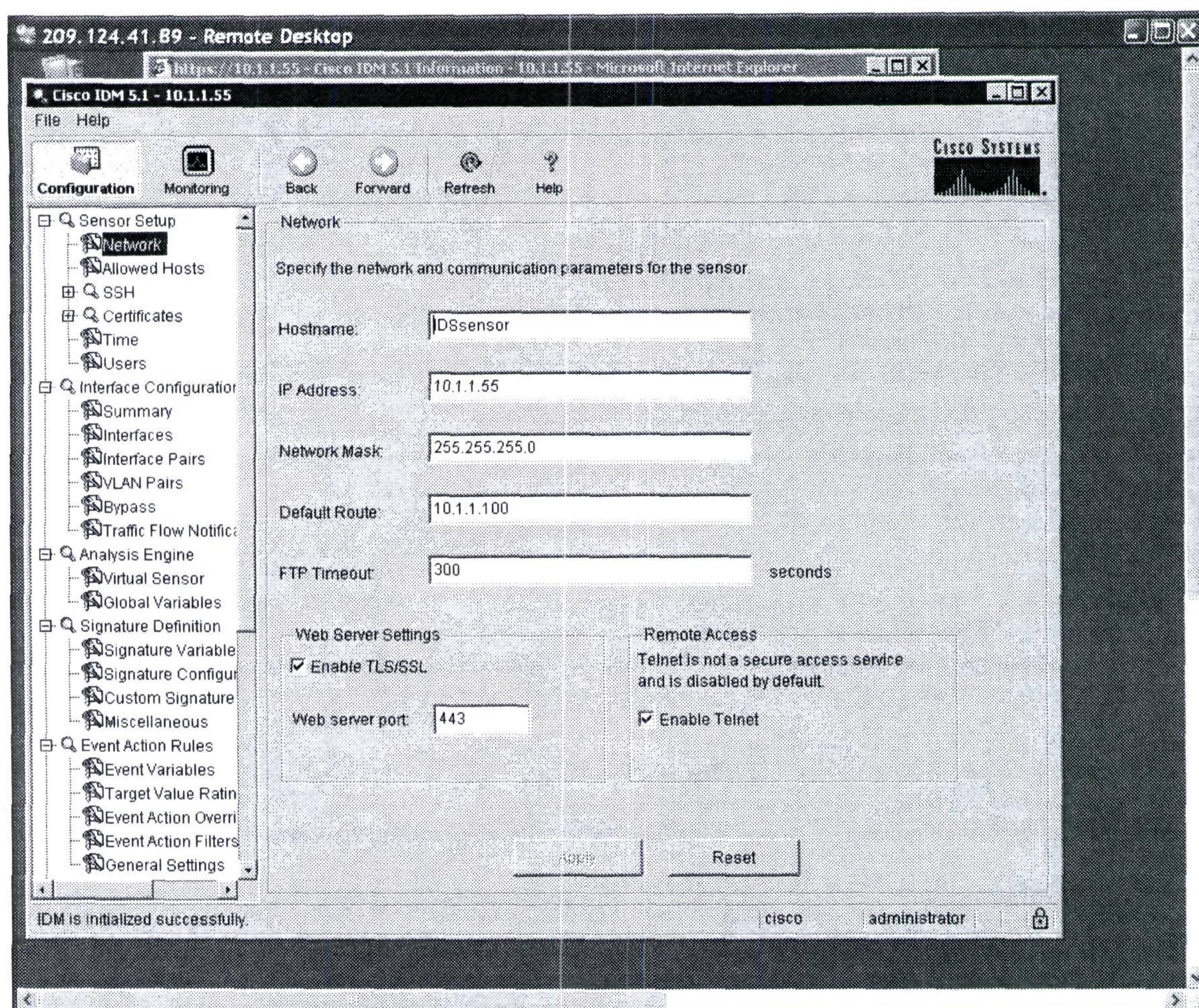
- [0] Go to the command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration and exit setup.

Enter your selection[2]: 2
 Configuration Saved.

Task 10-32

Open a web browser on the ACS server, and connect to the IDS GUI interface at <https://10.1.1.55>

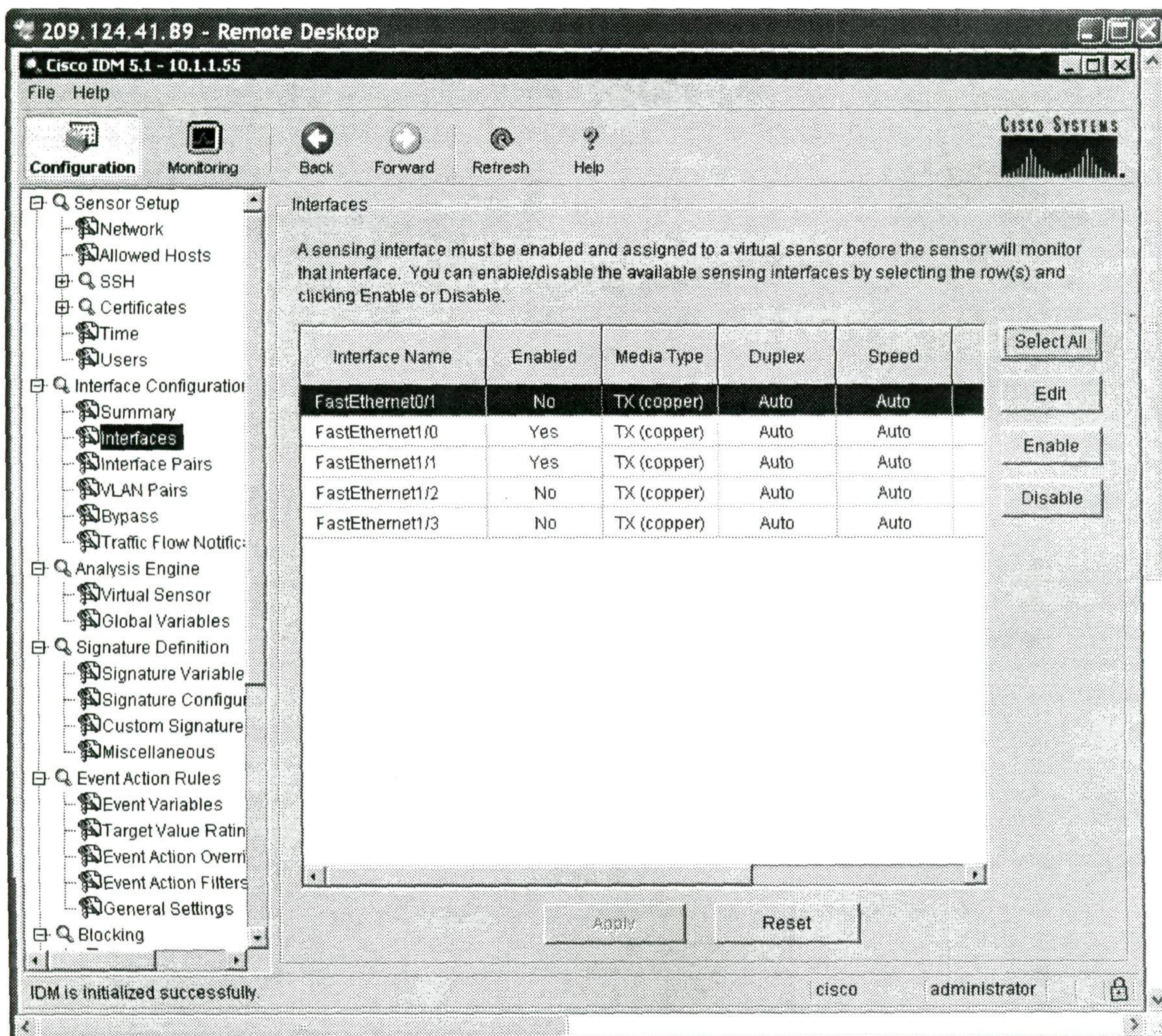




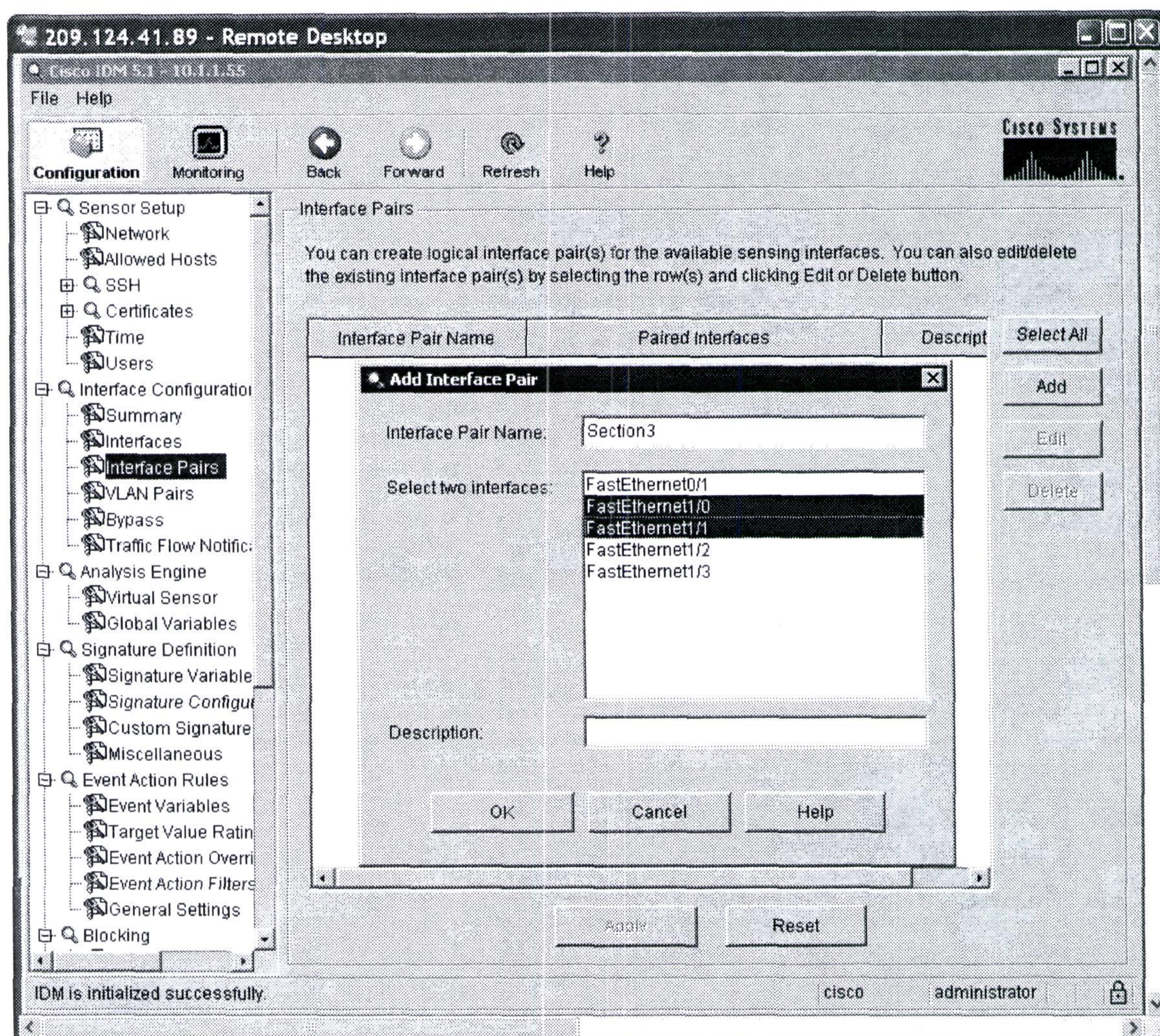
Task 10-33

Configure the IDS for inline mode using interfaces, as shown in the diagram. Interface Fa1/0 should be on VLAN 10 and interface Fa1/1 should be on VLAN 20. Verify that R1 can ping R2.

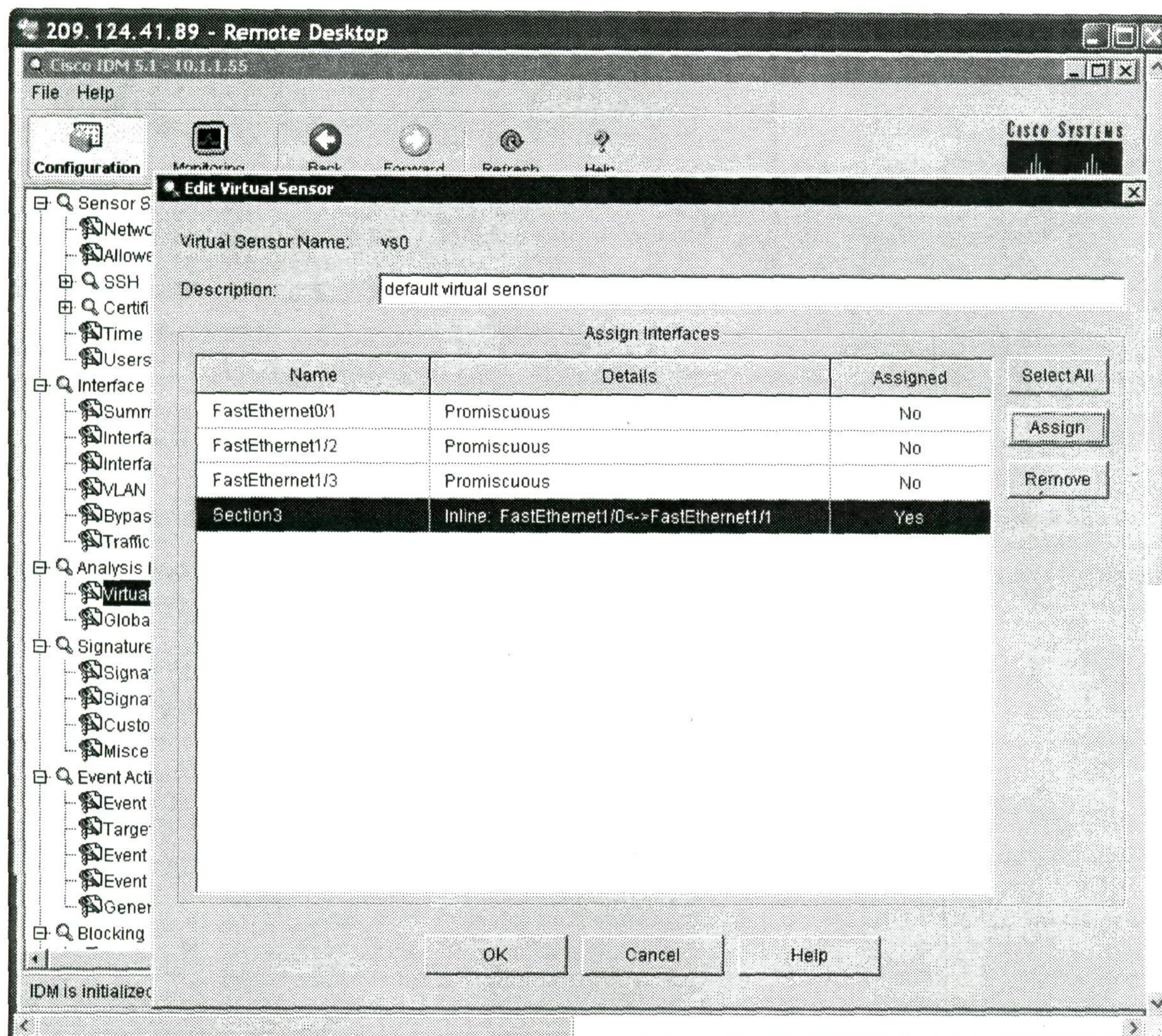
→ Start by enabling the FastEthernet interfaces on the IDS.



→ Add the interface pair under interface pairs.



→ Add the interface pair to the virtual sensor.



R4#ping 12.12.12.2

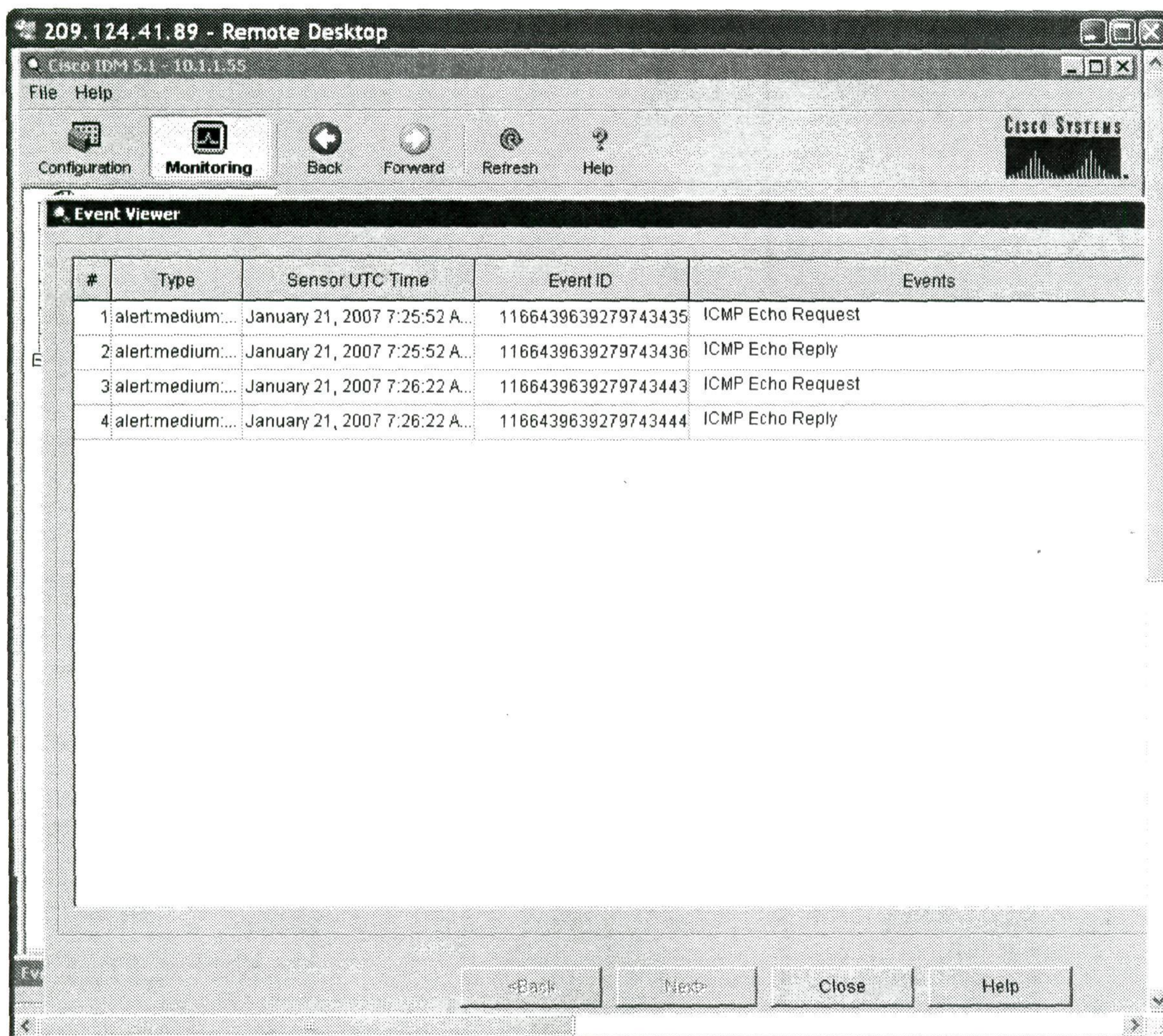
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/28/132 ms

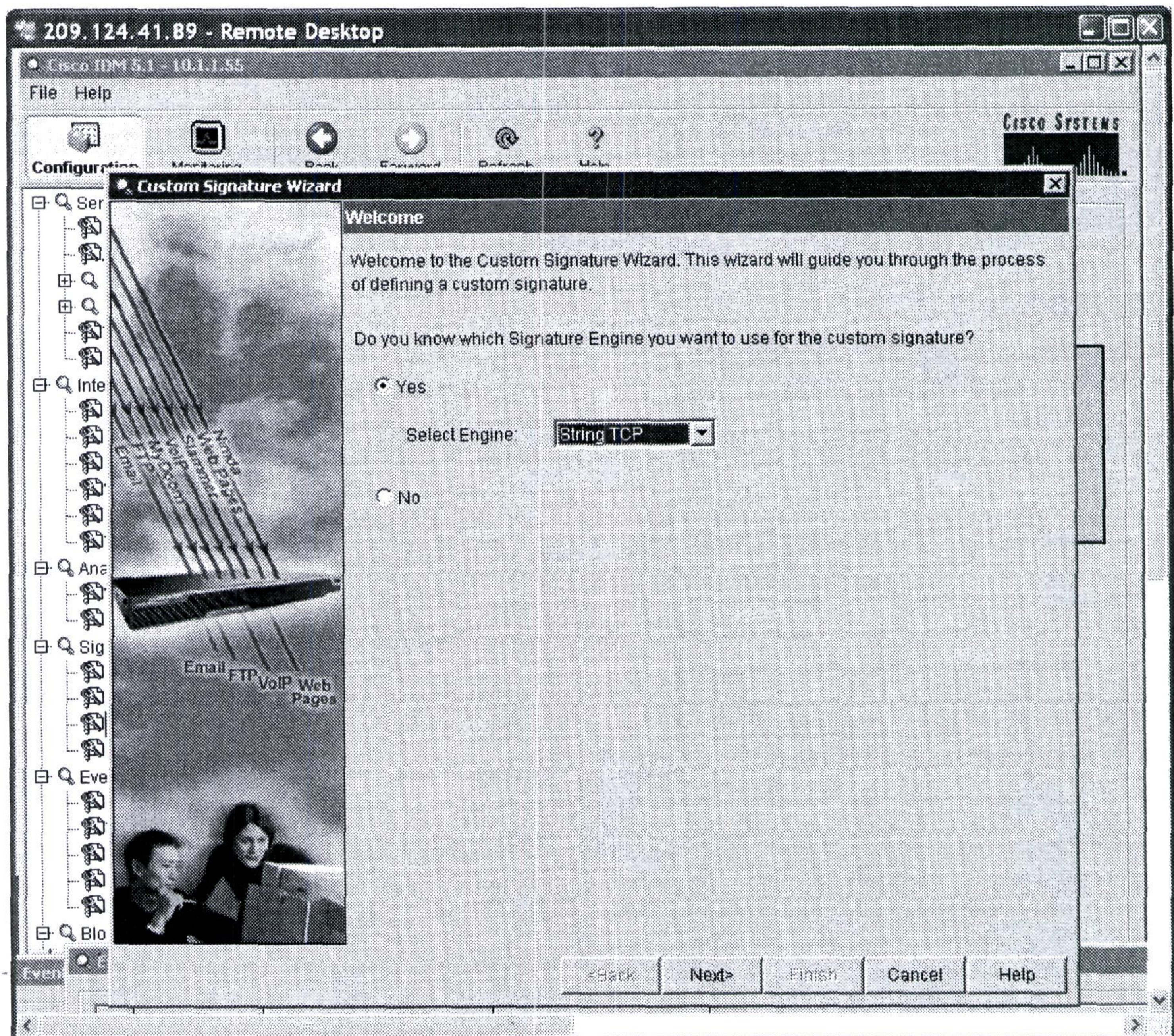
R4#



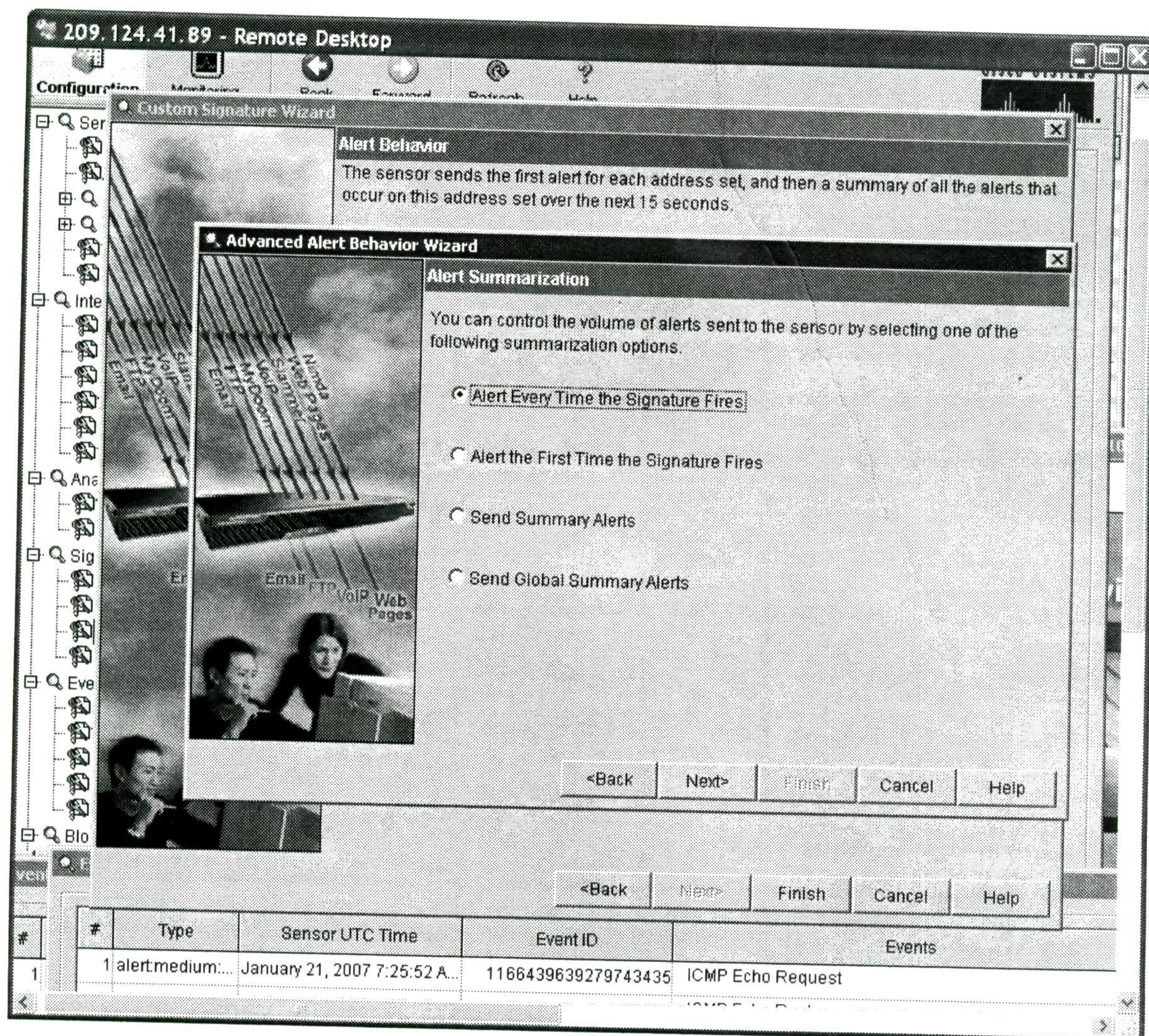
Task 10-35

Create a custom signature with the following properties:

- If a telnet session is established, and the word “password” is typed, the connection should be reset.
- Severity level for this signature should be set to medium.
- The signature should fire each time this occurs.



- Select both produce alert and reset TCP connection for event actions. The regular expression string that we are looking for is the word password.
- Alert severity is medium by default. Under alert behavior, select advanced to tune the summarization.



Task 10-36

Test by telnetting from R4 to R2, and entering the word password.

```
R4#telnet 12.12.12.2
Trying 12.12.12.2 ... Open
```

User Access Verification

Password:

```
R2>en
```

Password:

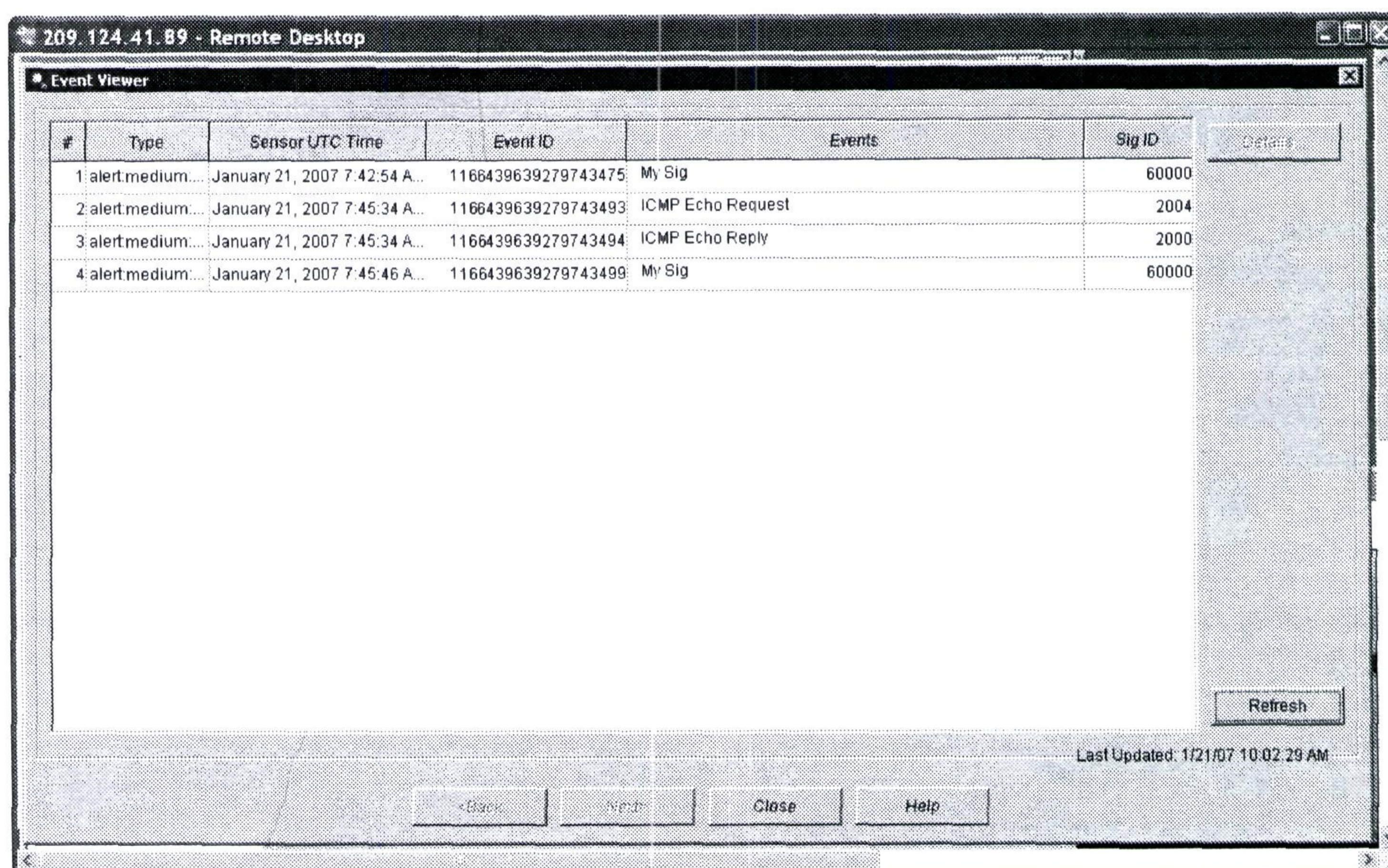
R2#password

```
[Connection to 12.12.12.2 closed by foreign host]
```

R4#

Task 10-37

Verify that the events show up in the event viewer.



Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 10C: IDS

Estimated Time to Complete: 1 Hour

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 10C Pre-Lab Setup

- Physically connect and configure your network according to Diagram 10C-1.
- This lab will focus strictly on IDS. You will need to pre-configure the network with the base IP Addressing and VLAN configuration. The pre-configuration files will be used to initially configure the routers and the PIX. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs* → *Section 10* → *Initial Configurations* → *Router X.txt*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your *www.IPexpert.com Member's Area*.

Section 10C Configuration Tasks

IPS using VLAN pairs

Task 10-38

Configure the IPS from the CLI for initial setup. Configure the IP address for the command and control interface to 10.1.1.55. Configure the access-list to allow the address of the ACS server. Configure a default gateway of 10.1.1.100, the address of the ACS server

```
IDSensor#setup
```

```
--- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

```
Continue with configuration dialog?[yes]: yes
Enter host name[sensor]: IDSsensor
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.55/24,10.1.1.100
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.0/24
Permit:
Modify system clock settings?[no]:
Modify virtual sensor "vs0" configuration?[no]:
```

```
The following configuration was entered.
```

```
service host
network-settings
host-ip 10.1.1.55/24,10.1.1.100
host-name IDSsensor
telnet-option disabled
access-list 10.1.1.0/24
ftp-timeout 300
no login-banner-text
```



```

exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit

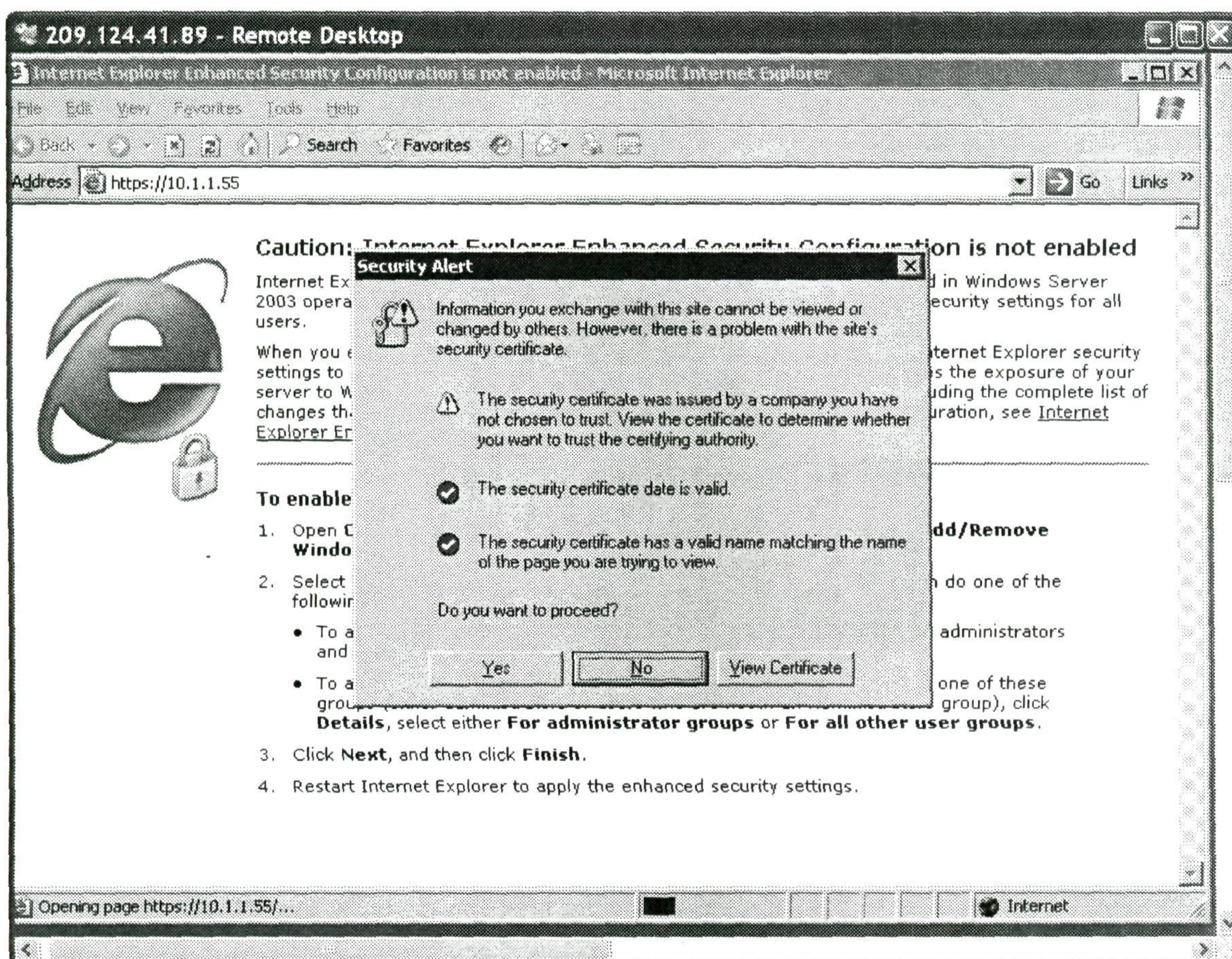
```

- [0] Go to the command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration and exit setup.

Enter your selection[2]: 2
 Configuration Saved.

Task 10-39

Open a web browser on the ACS server, and connect to the IPS GUI interface at 10.1.1.55

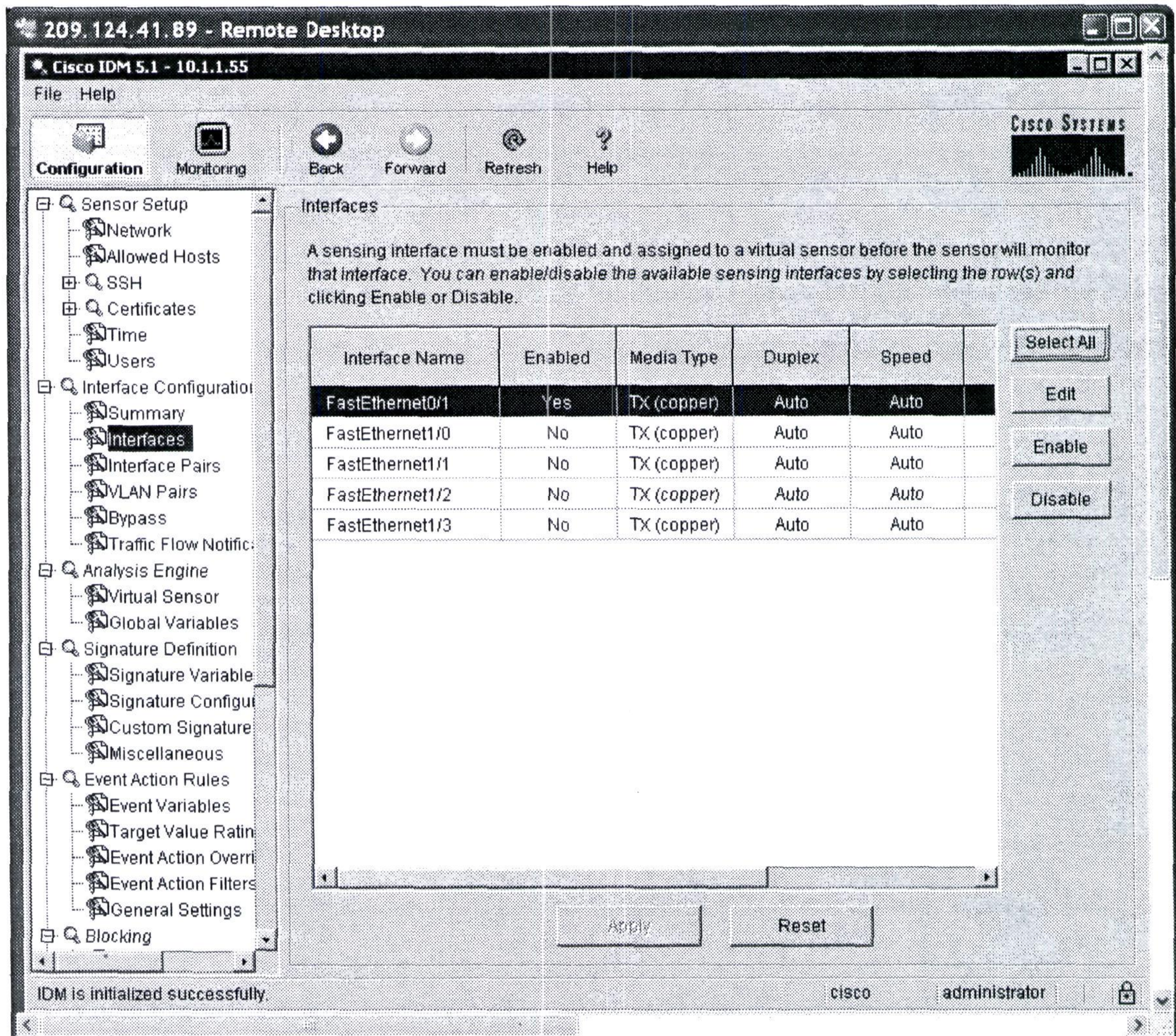


- Select Yes for the Security warnings, and log in with the username/password for the IPS.

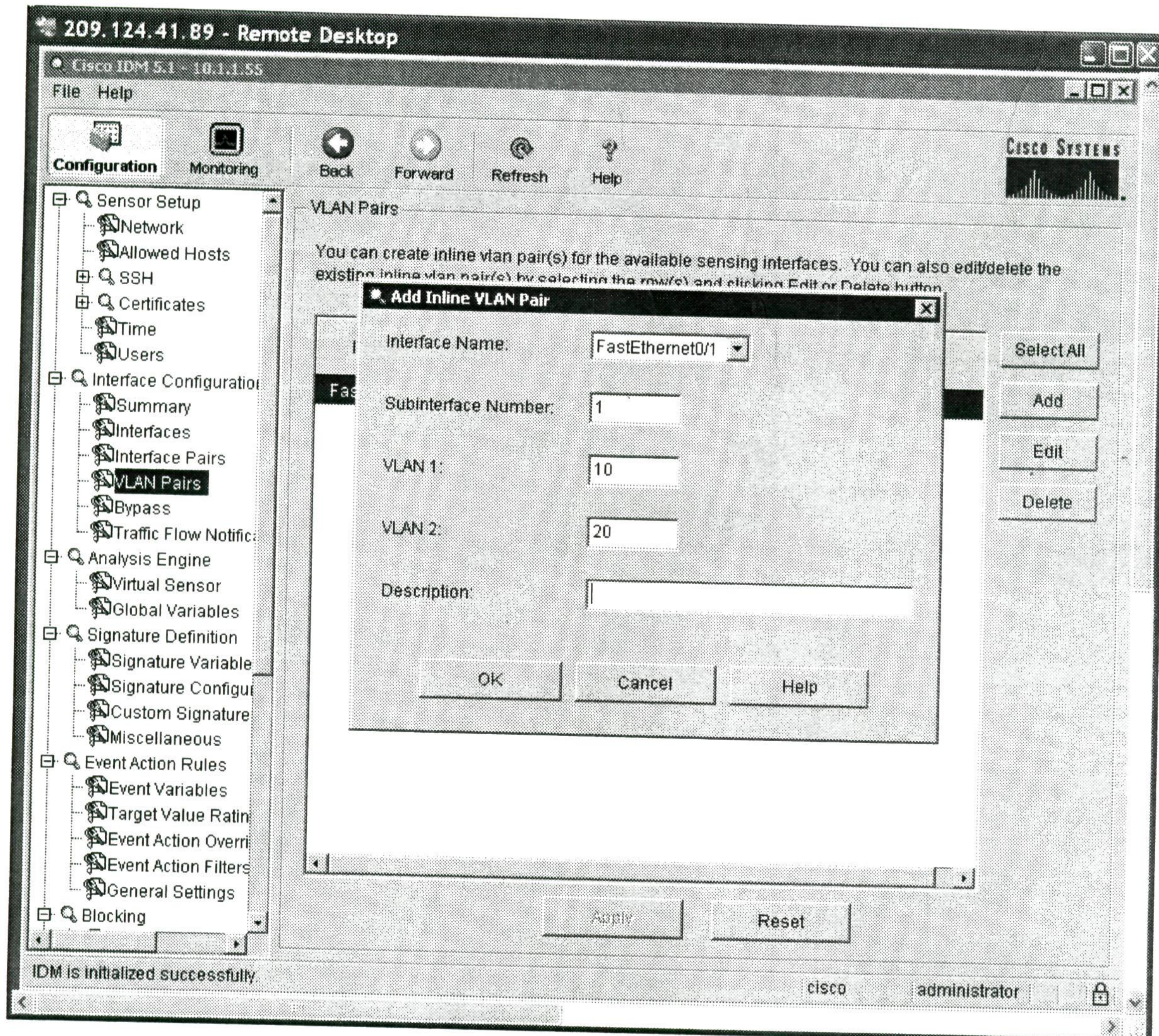
Task 10-40

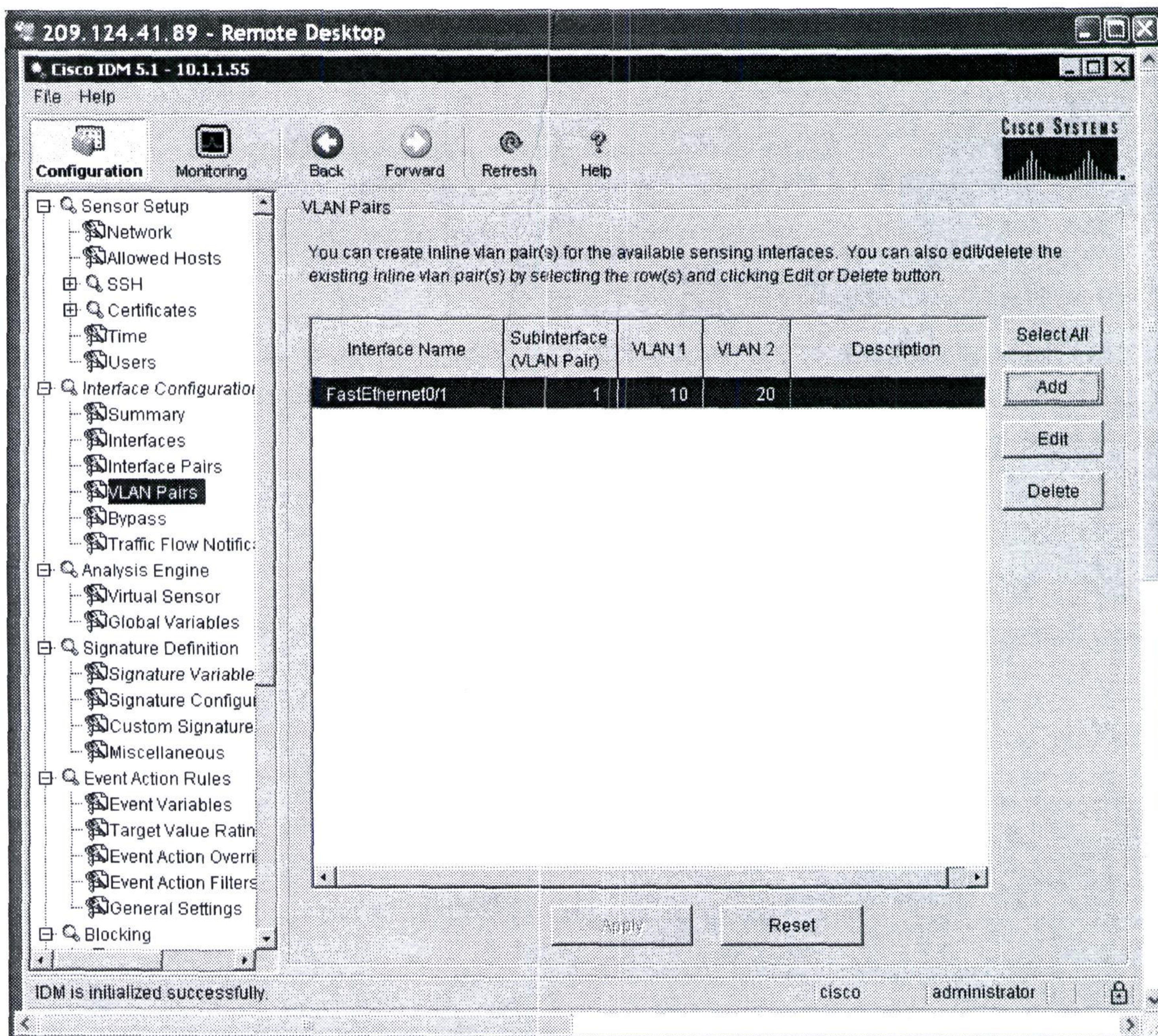
Configure the IPS for inline mode using VLAN pairs, as shown in the diagram. Interface Eth0/1 should be connected to VLANs 10 and 20. Configure the switch to allow the IPS to pass traffic for these interfaces on interface Ethernet 0/1. Verify that R4 can ping R2.

- Under Interfaces, enable the FastEthernet0/1 interface. Make sure to apply your settings to the sensor as you move through the sections.



- Under VLAN Pairs, add a VLAN pair, entering the two VLANs. Make sure to select the correct interface, Fa0/1





R4#ping 12.12.12.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 12.12.12.2, timeout is 2 seconds:

!!!!

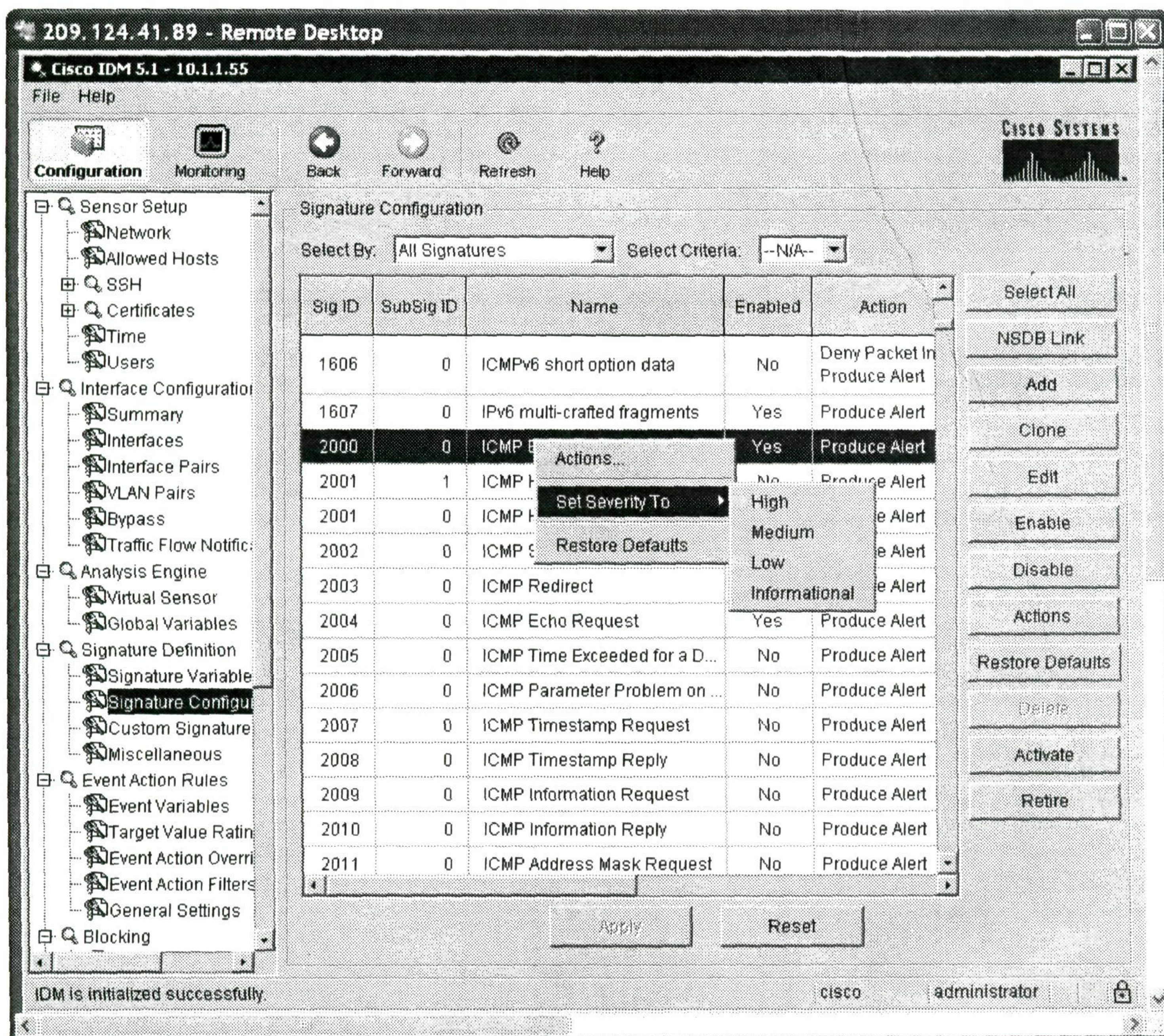
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R4#

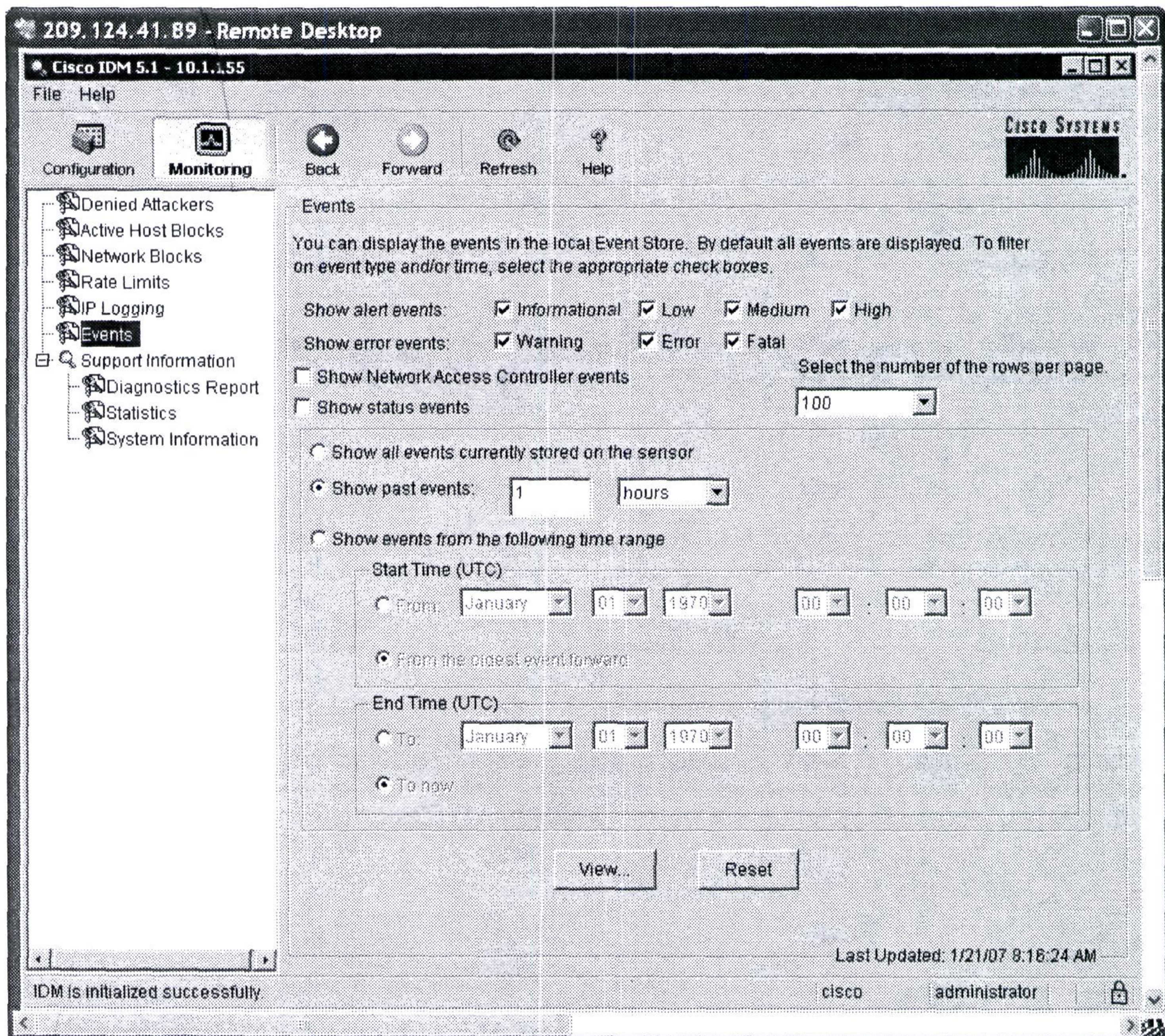
Task 10-41

Tune the signatures for echo and echo-reply to medium severity. Verify that pings from R4 to R2 and from R2 to R4 cause the signatures to fire.

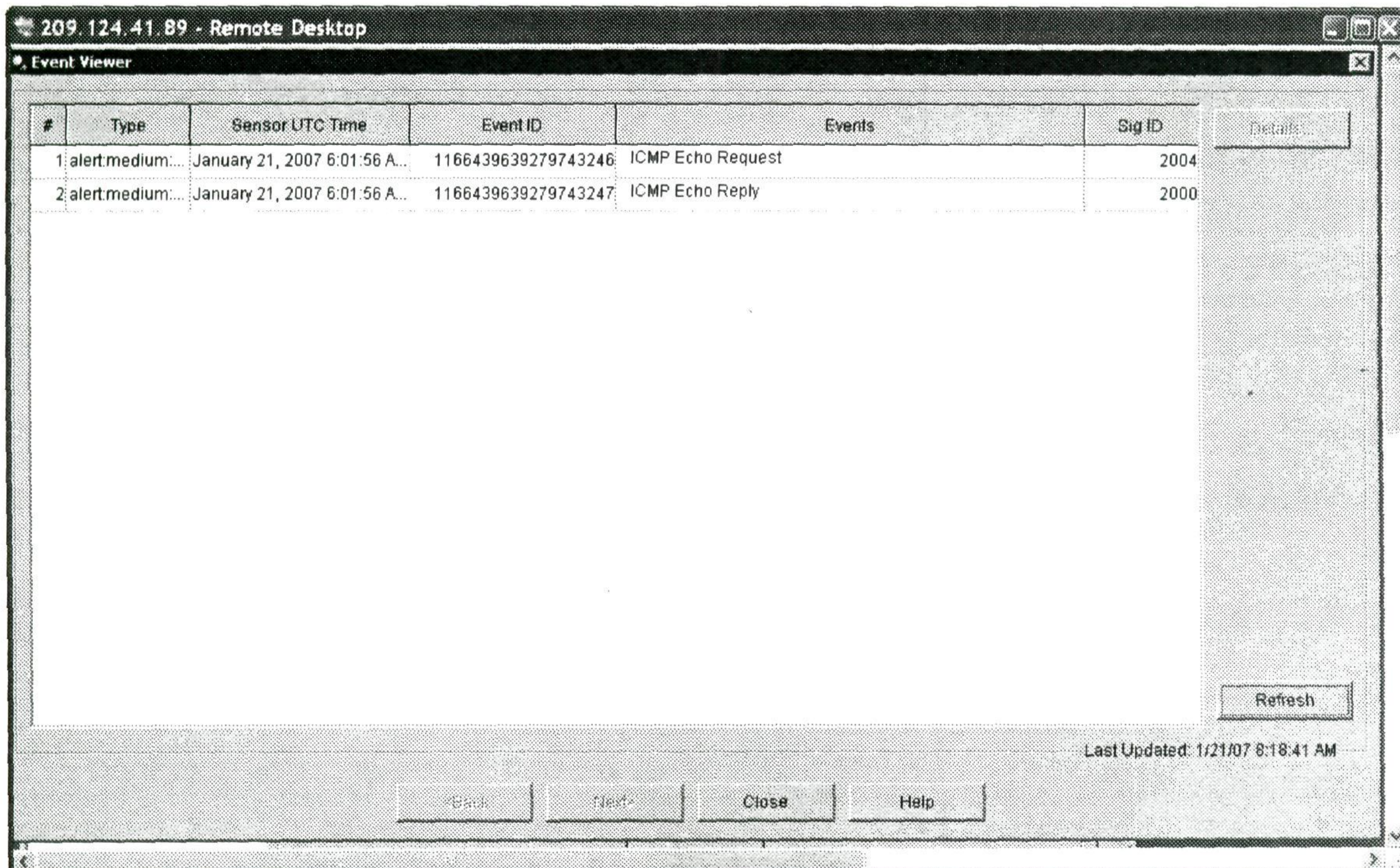
- **ICMP signatures start at 2000, so scroll down, and click enable for signatures 2000 and 2004. To change severity, right-click on the signature and choose “set severity to”. Make sure to apply your changes to the sensor.**



- To monitor the events, select the monitoring tab, and events. Selecting View will open the event viewer.



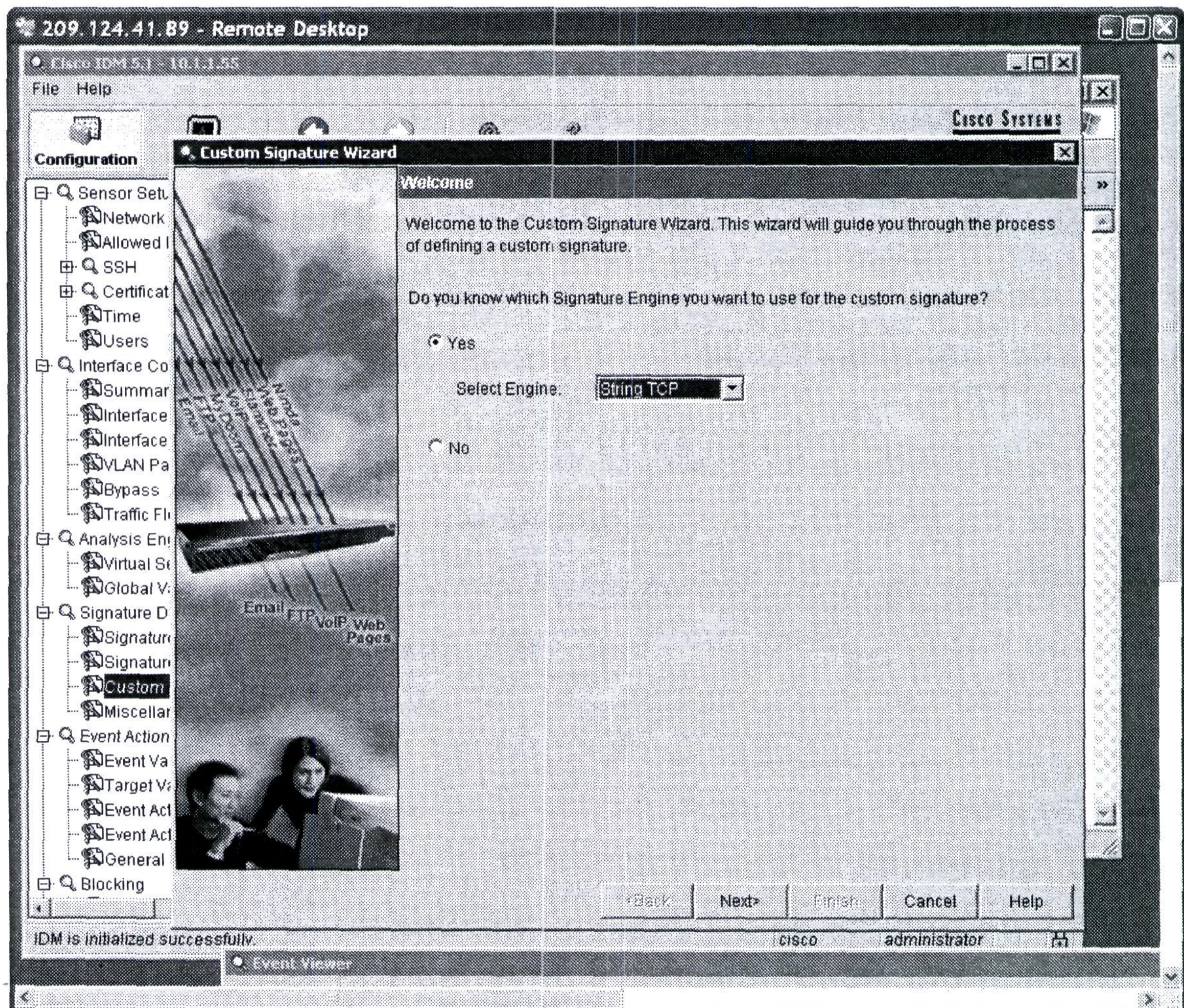
- As you can see in the output of the event viewer, the alert shows as medium and shows that both signatures 2000 and 2004 have fired. Note that there is only one alert for each. If you need each ping to fire, you may need to adjust the summarization information for the signature. Since this section doesn't specify that the signature should fire each time, the summarization is fine. When in doubt, however, it is best to ask the proctor.



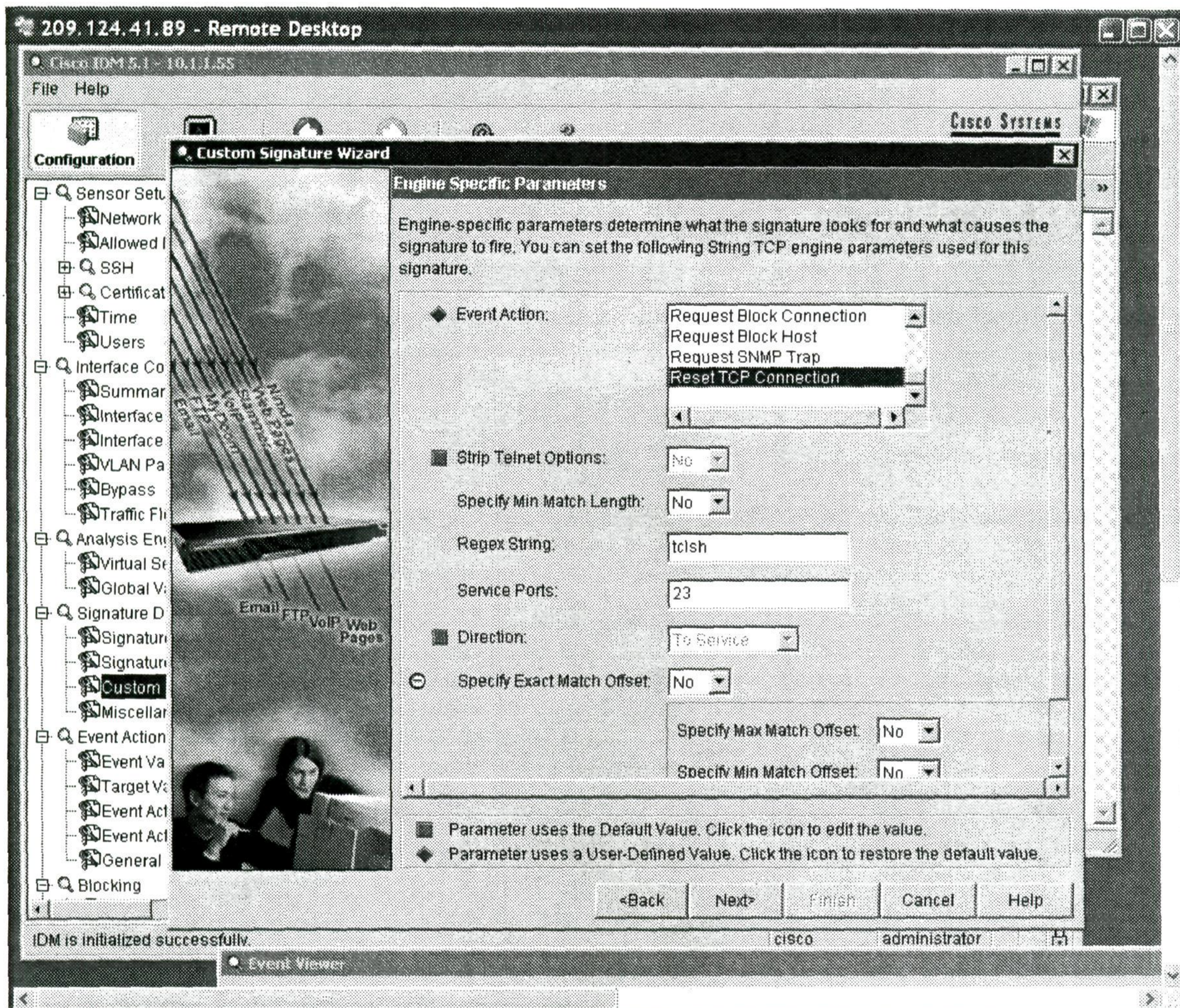
Task 10-42

Create a custom signature with the following properties:

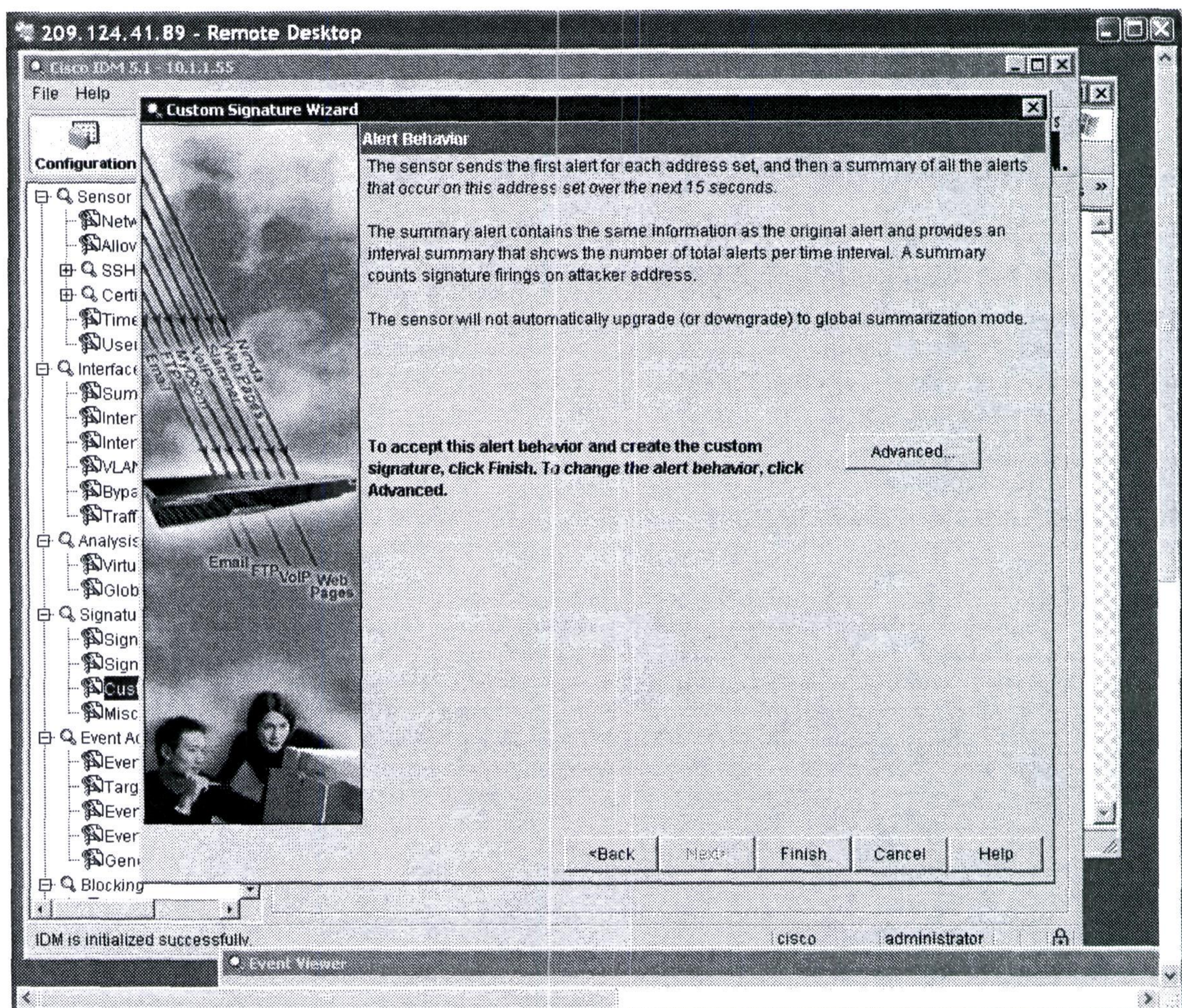
- ➔ If a telnet session is established, and the word "tclsh" is typed, the signature should fire. The connection should not be reset.
- ➔ Severity level for this signature should be set to medium.
- ➔ The signature should fire each time this occurs.



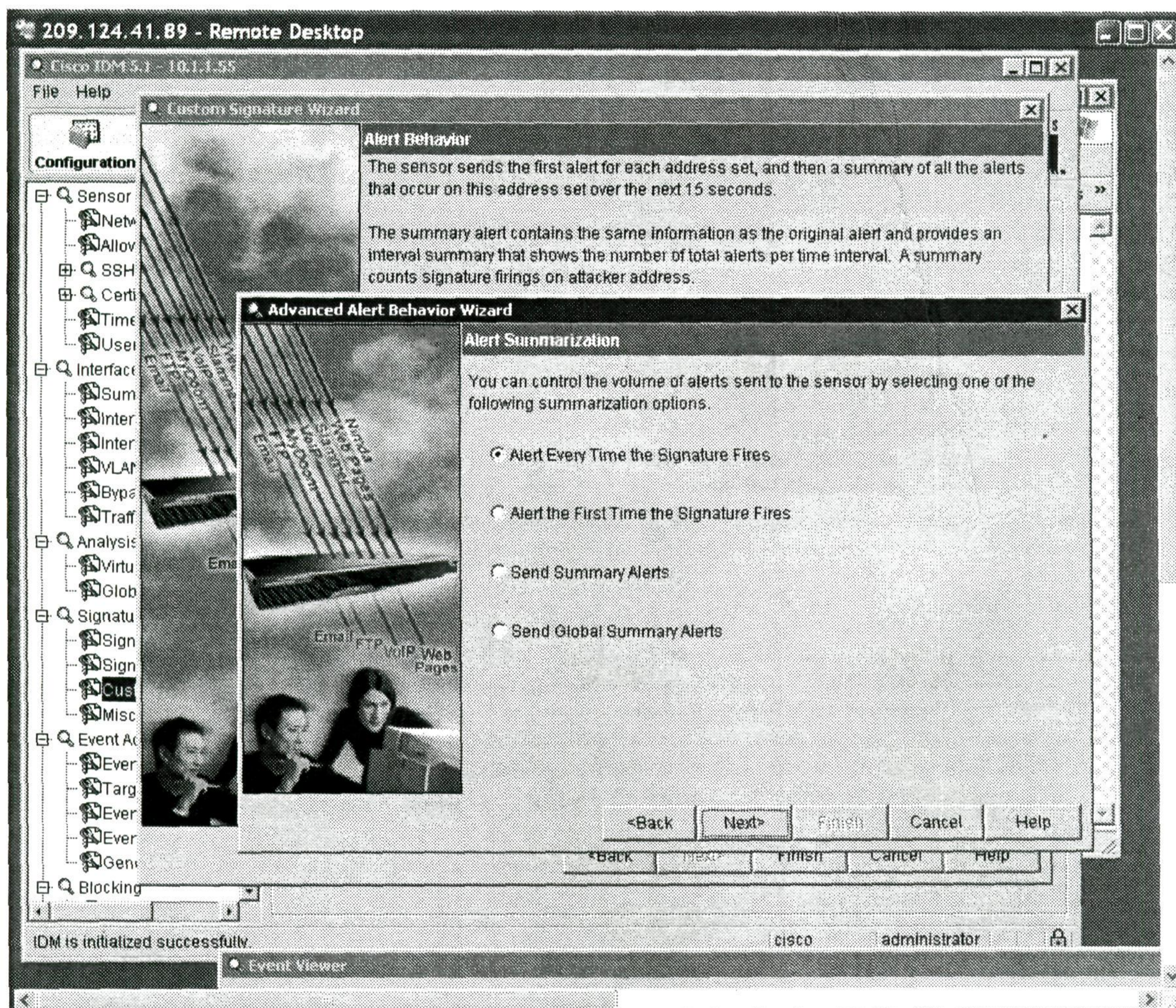
- Start by selecting the custom signature wizard, and selecting String.TCP as the signature engine to use. We aren't given a specific signature ID or name to use, so you may enter a name if you wish.



- Since we are looking at Telnet, the service port will be 23. Select event action, and scroll down to Reset TCP connection. When finished, select next to continue to the next page. The default severity is medium, so continue to the next page.



- Here we see alert behavior. Since the default is to summarize, we need to adjust this. Click on the Advanced tab. On the event count and interval page, select next. On the alert summarization page, select Alert Every Time. Select next, and then select finish.



Task 10-43

Test by telnetting from R4 to R2, and entering the command tclsh.

```
R4#telnet 12.12.12.2
Trying 12.12.12.2 ... Open

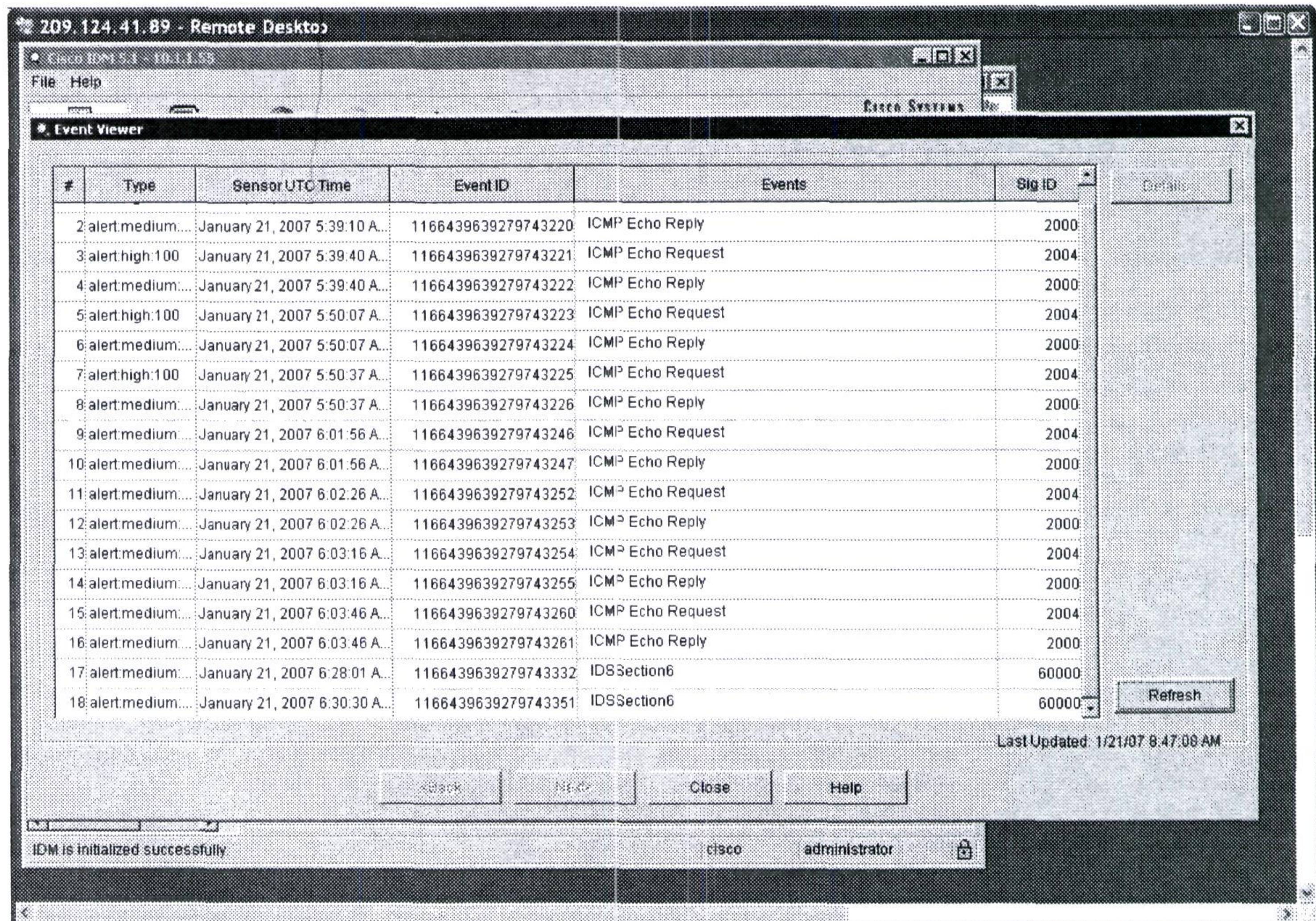
User Access Verification

Password:
R2>tclsh
[Connection to 12.12.12.2 closed by foreign host]
R4#
```

- You may test more than one time.

Task 10-44

Verify that the events show up in the event viewer.



- Make sure that you have the custom signature configured to produce an alert. If you just have it configured for reset, the signature will fire, and will reset the connection, but will not show up in the event viewer.

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

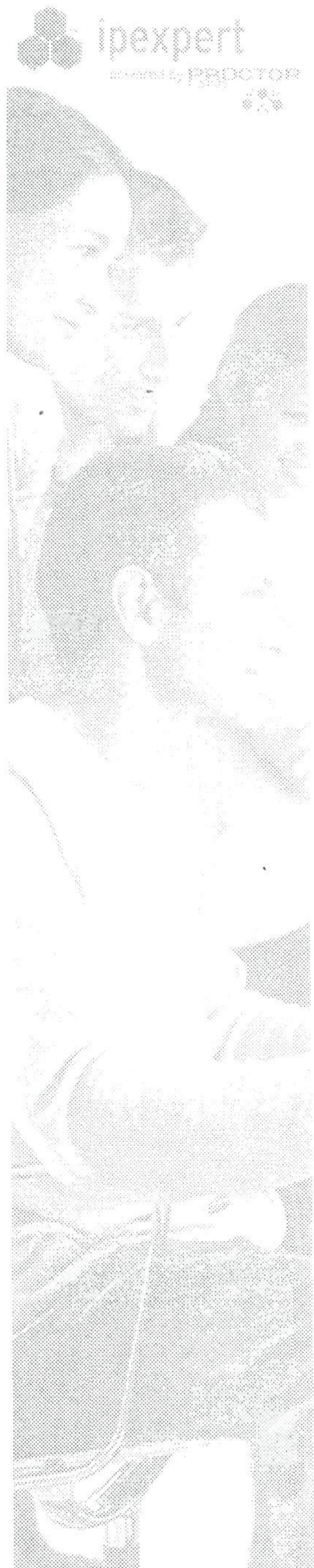
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 11: Router Management | IOS Services

Estimated Time to Complete: 2 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 11 Pre-Lab Setup

- Physically connect and configure your network according to Diagram 11-A.
- The Routers are running the following protocols:
 - OSPF as the routing protocol
- This lab will focus strictly on IOS Services. You will need to pre-configure the network with the base Frame Relay, IP Addressing and OSPF configuration. You will find these configurations in the “Initial Configurations” subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 11 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the “MY CONFIGS” area of your www.IPexpert.com Member's Area.

Telnet Configurations

Task 11-1

The administrator of R2 wants to reserve a Telnet line for himself.

- **No command is needed here.**

Task 11-2

Accomplish this by changing the telnet port for the last vty line to 3045.

- **The rotary command would automatically add 3000 to the required value. And we just want to apply it to the last line, so the command of line vty 4.**
- **By default, whenever there is a person telnetting to a router, it takes up a vty line. Therefore, it is always a good idea to reserve one for the administrator, using a different setting than otherwise available.**

```
R2(config)#line vty 4
R2(config-line)#rotary 45
```

Task 11-3

The administrator of R2 does not want anybody to telnet from R2. Disable the Telnet client on R2. You cannot use an Access List to accomplish this task.

- **The transport output none will stop any outbound telnet sessions from being established. Be sure to use this command on all interfaces including the aux and console.**

```
R2(config-line)#transport output none
```


Task 11-4

When users Telnet into the normal Telnet port on R2, they should not have the ability to access the command prompt. Instead, they should receive a menu that only allows them the ability to perform the following commands:

- SH IP INT BRIEF
- SH IP ROUTE
- SH IP OSPF NEIGHBOR
- EXIT

- **The menu command is a very convenient command because you can limit the user to exactly what you want him or her to access.**

```
R2(config)#menu IPEXPERT title ^CIPEXPERT TELNET MENU^C
R2(config)#menu IPEXPERT prompt ^CPlease Enter Your Selection : ^C
R2(config)#menu IPEXPERT text 1 SH IP INT BRIEF
R2(config)#menu IPEXPERT command 1 SH IP INT BRIEF
R2(config)#menu IPEXPERT options 1 pause
R2(config)#menu IPEXPERT text 2 SH IP ROUTE
R2(config)#menu IPEXPERT command 2 SH IP ROUTE
R2(config)#menu IPEXPERT options 2 pause
R2(config)#menu IPEXPERT text 3 SH IP OSPF NEIGHBOR
R2(config)#menu IPEXPERT command 3 SH IP OSPF NEIGHBOR
R2(config)#menu IPEXPERT options 3 pause
R2(config)#menu IPEXPERT text 4 EXIT
R2(config)#menu IPEXPERT command 4 EXIT
R2(config)#menu IPEXPERT line-mode
```

- **This will be the output when you telnet from R4 to R2:**

R4#10.1.1.2

Trying 10.1.1.2 ... Open

User Access Verification

Password: CIPEXPERT TELNET MENU

- | | |
|---|---------------------|
| 1 | SH IP INT BRIEF |
| 2 | SH IP ROUTE |
| 3 | SH IP OSPF NEIGHBOR |
| 4 | EXIT |

CPlease Enter Your Selection : 1

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	manual	administratively down	down
GigabitEthernet0/1	unassigned	YES	manual	administratively down	down
BRI0/0/0	unassigned	YES	manual	administratively down	down
BRI0/0/0:1	unassigned	YES	unset	administratively down	down
BRI0/0/0:2	unassigned	YES	unset	administratively down	down
Serial0/1/0	unassigned	YES	manual	administratively down	down
Serial0/2/0	unassigned	YES	unset	administratively down	down
FastEthernet1/0	10.1.1.2	YES	manual	up	up
FastEthernet1/1	unassigned	YES	unset	administratively down	down
FastEthernet1/2	unassigned	YES	unset	administratively down	down
FastEthernet1/3	unassigned	YES	unset	administratively down	down
FastEthernet1/4	unassigned	YES	unset	administratively down	down
FastEthernet1/5	unassigned	YES	unset	administratively down	down
FastEthernet1/6	unassigned	YES	unset	administratively down	down
FastEthernet1/7	unassigned	YES	unset	administratively down	down


```

FastEthernet1/8          unassigned      YES unset  administratively down down

1          SH IP INT BRIEF
2          SH IP ROUTE
3          SH IP OSPF NEIGHBOR
4          EXIT

```

CPlease Enter Your Selection : **2**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

```

C    2.0.0.0/8 is directly connected, Loopback0
    4.0.0.0/32 is subnetted, 1 subnets
O    4.4.4.4 [110/2] via 10.1.1.4, 00:01:12, FastEthernet1/0
    10.0.0.0/24 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, FastEthernet1/0

```

```

1          SH IP INT BRIEF
2          SH IP ROUTE
3          SH IP OSPF NEIGHBOR
4          EXIT

```

CPlease Enter Your Selection : **3**

Neighbor ID	Pri	State	Dead Time	Address	Interface
4.4.4.4	1	FULL/BDR	00:00:32	10.1.1.4	FastEthernet1/0

```

1          SH IP INT BRIEF
2          SH IP ROUTE
3          SH IP OSPF NEIGHBOR
4          EXIT

```

CPlease Enter Your Selection : **4**

[Connection to 10.1.1.2 closed by foreign host]

DHCP Server

Task 11-5

Enable R4 as a DHCP Server with the following information:

- ➔ IP ADDRESS : 10.1.1.0 255.255.255.0
- ➔ WINS ADDRESS : 10.1.1.135
- ➔ DNS ADDRESS : 10.1.1.53
- ➔ DEFAULT GATEWAY : 10.1.1.4
- ➔ LEASE TIME : 3 Days 12 hours
- ➔ Excluded Addresses: 10.1.1.1 – 10.1.1.20, 10.1.1.53 – 10.1.1.100, 10.1.1.135

→ The following commands are for the basic DHCP commands:

```
R4 (config) #ip dhcp excluded-address 10.1.1.1 10.1.1.20
R4 (config) #ip dhcp excluded-address 10.1.1.135
R4 (config) #ip dhcp excluded-address 10.1.1.53 10.1.1.100
R4 (config) #ip dhcp pool IPEXPERT
R4 (dhcp-config) #network 10.1.1.0 255.255.255.0
R4 (dhcp-config) #netbios-name-server 10.1.1.135
R4 (dhcp-config) #dns-server 10.1.1.53
R4 (dhcp-config) #default-router 10.1.1.4
R4 (dhcp-config) #lease 3 12
```

Task 11-6

Disable any DHCP Related services on R2.

→ Use the No Service command to disable DHCP services on a router.

```
R2 (config) #no ip bootp server
R2 (config) #no service dhcp
```

Task 11-7

Enable conflict logging on R4.

→ This would prevent enable the conflict logging by issuing the following command:

```
R4 (dhcp-config) #ip dhcp conflict logging
```

Task 11-8

Configure option 19 to tell the client should configure its IP layer for packet forwarding.

→ This should be entered under the IP DHCP pool and this would fine tune the DHCP pool:

```
R4 (dhcp-config) #option 19 hex 01
```

Task 11-9

Specifies five ping attempts by the DHCP server before ceasing any further ping attempts.

→ And this would specify five ping attempts:

```
R4 (config) #ip dhcp ping packets 5
```


- The two commands below are good to check whether DHCP is working probably. Since this is a small scale network, there is very few traffic. However, if you check these commands in a real network, the statistics can be huge.

```
R4#show ip dhcp server statistics
```

```
Memory usage          24444
Address pools         1
Database agents       0
Automatic bindings    1
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0
```

```
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         2
DHCPREQUEST          1
DHCPDECLINE          0
DHCPRELEASE          0
DHCPIFORM            0
```

```
Message              Sent
BOOTREPLY            0
DHCPOFFER            2
DHCPACK              1
DHCPNAK              0
```

```
R4#sh ip dhcp binding
```

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
10.1.1.21	0100.508b.eca7.b6	Dec 28 2005 05:38 AM	Automatic

NTP

Task 11-10

Configure the timezone on R2 as PST -8. Set the clock to the current time on R2.

- The PST-8 timezone can be configured. This is always good to have the right time zone or else the debugging would be a bit confusing when routers are across continents.

```
R2(config)#clock timezone PST -8
```

Task 11-11

Set R2 as the NTP Master with a stratum of 2. NTP should require MD5 authentication with a key 1.

- This can define the R2 as the NTP router and ensure that all the NTP packets are transmitted securely.

```
R2(config)#ntp authentication-key 1 md5 151B1B091C3A2E363C 7
R2(config)#ntp master 2
```


Task 11-12

Configure R6 as the client for R2. R6 should point to R2 using the NTP Server command. Configure the timezone to PST -8 on R6.

- **The R6 can use R2 as the NTP server and with the right timezone. Also, the communication between the NTP packets is secured.**

```
R6(config)#clock timezone PST -8
R6(config)#ntp authentication-key 1 md5 141E020E14142F3930 7
R6(config)#ntp authenticate
R6(config)#ntp trusted-key 1
R6(config)#ntp clock-period 17179952
R6(config)#ntp server 10.1.1.2 key 1
```

Task 11-13

Configure R4 to peer with R6. R4 should get its clock from R6. Use the Peer command to accomplish this. Configure the timezone to PST -8 on R4.

- **This would cause R4 to peer with R6. You don't always need to peer with the master. The clock can be relayed from one to the other and the accuracy is pretty good.**

```
R4(config)#ntp authentication-key 1 md5 121015120A1B09163E 7
R4(config)#ntp authenticate
R4(config)#ntp trusted-key 1
R4(config)#ntp clock-period 17179903
R4(config)#ntp peer 150.50.46.6 key 1
```

Task 11-14

Configure R6 to periodically update the hardware clock from NTP time source.

- **Some routers has internal clock, such as this one. Then even when you reboot the router, the time is still there.**

```
R6(config)#ntp update-calendar
```

Task 11-15

Configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the Aux0 port for R6.

- **This would cause R6 to check the aux 0 port for a GPS clock source:**

```
R6(config)#line aux 0
R6(config-line)#ntp refclock trimble pps none
```


→ This is for the NTP master router R2:

```
R2#show ntp associations detail
127.127.7.1 configured, our_master, sane, valid, stratum 1
ref ID .LOCL., time C75840BB.9438CFFD (13:48:43.578 PST Sat Dec 24 2005)
our mode active, peer mode passive, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.00, reach 377, sync dist 0.015
delay 0.00 msec, offset 0.0000 msec, dispersion 0.02
precision 2**18, version 3
org time C75840BB.9438CFFD (13:48:43.578 PST Sat Dec 24 2005)
rcv time C75840BB.9438CFFD (13:48:43.578 PST Sat Dec 24 2005)
xmt time C75840BB.9438981D (13:48:43.578 PST Sat Dec 24 2005)
filtdelay =      0.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00
filtoffset =      0.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00
filtererror =      0.02      0.99      1.97      2.94      3.92      4.90      5.87      6.85
Reference clock status:  Running normally
Timecode:
```

→ As you can see here, the ntp status is synchronized. It does not take much to make the master clock synchronize. As long as you have set the clock, then you should have this synchronized.

```
R2#show ntp status
Clock is synchronized, stratum 2, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is C75840BB.9438CFFD (13:48:43.578 PST Sat Dec 24 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

→ This is for the NTP peer. Notice that the peers show as authenticated

```
R6#sho ntp associations detail
10.1.1.2 configured, authenticated, our_master, sane, valid, stratum 2
ref ID 127.127.7.1, time C7D9D819.0726F3EB (20:56:57.027 PST Sat Apr 1 2006)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 377, sync dist 11.261
delay 17.64 msec, offset 15.9397 msec, dispersion 2.41
precision 2**24, version 3
org time C7D9D81C.00EACC68 (20:57:00.003 PST Sat Apr 1 2006)
rcv time C7D9D81B.FF187799 (20:56:59.996 PST Sat Apr 1 2006)
xmt time C7D9D81B.FA88974B (20:56:59.978 PST Sat Apr 1 2006)
filtdelay =      17.64      17.75      17.68      17.59      17.73      17.59      17.70      17.78
filtoffset =      15.94      14.94      13.67      11.98      10.30      8.02      5.50      5.66
filtererror =      0.02      0.99      1.97      2.94      3.92      4.90      5.87      6.85

127.127.8.1 configured, insane, invalid, unsynced, stratum 0
ref ID .GPS., time 00000000.00000C00 (16:00:00.000 PST Wed Dec 31 1899)
our mode active, peer mode unspec, our poll intvl 32, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 0, sync dist 39.230
delay 0.00 msec, offset 0.0000 msec, dispersion 16000.00
precision 2**20, version 3
org time 00000000.00000000 (16:00:00.000 PST Wed Dec 31 1899)
rcv time 00000000.00000000 (16:00:00.000 PST Wed Dec 31 1899)
xmt time C7D9D826.FAA82C06 (20:57:10.979 PST Sat Apr 1 2006)
filtdelay =      0.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00
filtoffset =      0.00      0.00      0.00      0.00      0.00      0.00      0.00      0.00
filtererror = 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0 16000.0
Reference clock status:  Reply timeout
Timecode:
```



```

150.50.46.4 configured, authenticated, insane, invalid, stratum 4
ref ID 150.50.46.6, time C7D9D7DB.FCA0B358 (20:55:55.986 PST Sat Apr 1 2006)
our mode active, peer mode active, our poll intvl 64, peer poll intvl 64
root delay 42.62 msec, root disp 395.16, reach 76, sync dist 1305.725
delay 25.39 msec, offset -2.2856 msec, dispersion 876.08
precision 2**24, version 3
org time C7D9D7FB.138AB6DE (20:56:27.076 PST Sat Apr 1 2006)
rcv time C7D9D7FB.1760CB57 (20:56:27.091 PST Sat Apr 1 2006)
xmt time C7D9D81B.FAA0050B (20:56:59.979 PST Sat Apr 1 2006)
filtdelay =    25.39    25.41    25.16    25.28    24.81    0.00    0.00    0.00
filtoffset =   -2.29   -1.83   -1.51   -1.20   -1.76    0.00    0.00    0.00
filtererror =    0.50    1.48    2.46    3.43    4.41 16000.0 16000.0 16000.0

```

R6#

- As you can see below, the clock is synchronized with the master clock R2. The UDP port 123 packet is exchanged about once per minute. You can try some debug command to view this packet. In the future, if you run any access list, beware that you are not filtering the NTP packet, or else it would change to unsynchronized.

R6#**sho ntp stat**

```

Clock is synchronized, stratum 3, reference is 10.1.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9989 Hz, precision is 2**18
reference time is C7D9D89C.00875D6A (20:59:08.002 PST Sat Apr 1 2006)
clock offset is 17.5773 msec, root delay is 17.58 msec
root dispersion is 19.32 msec, peer dispersion is 1.72 msec

```

IP Accounting

Task 11-16

You would like to gather traffic statistics about the traffic that transits thru R6. Configure R6 for IP accounting on both interfaces.

- The commands below would enable accounting on both the Fast Ethernet and also the Serial interfaces:

```

R6(config)#interface FastEthernet0/0
R6(config-if)#ip accounting output-packets
R6(config)#interface Serial0/1/0.4 point-to-point
R6(config-if)#ip accounting output-packets

```

Task 11-17

The maximum number of accounting entries to be created should be 500.

- This can make sure that the maximum accounting entry to be 500:

```

R6(config)#ip accounting-threshold 500

```


Task 11-18

IP accounting should be based on IP precedence for received and transmitted packets

- To enable IP accounting on any interface based on IP precedence, use the **ip accounting precedence interface configuration** command.

```
R6(config)#interface f0/0
R6(config-if)# ip accounting precedence input
R6(config-if)# ip accounting precedence output

R6(config)#interface s0/1/0.4
R6(config-if)# ip accounting precedence input
R6(config-if)# ip accounting precedence output
```

Privilege**Task 11-19**

Configure a user (username = "user"/password = none) in R2 that can set the clock.

- We are using the standard way to create a user. Without specifying the privilege level, it is assumed to be one, and without specifying the password, it is assumed that there is no password.

```
R2(config)#username user privilege 3
R2(config)#username manager privilege 7 password manager
```

Task 11-20

Configure a user (username = "manager"/password = "manager") in R2 such that he inherit the privilege of user "user" but he can also set the ip address and shut down any interface.

- In this case, the privilege level can set different users with different capabilities.

```
R2(config)#privilege interface level 7 shutdown
R2(config)#privilege interface level 7 ip address
R2(config)#privilege configure level 7 interface
R2(config)#privilege exec level 7 configure terminal
R2(config)#privilege exec level 3 clock set
```

- First, I disable it back to the user's privilege:

```
R2#disable
R2>show privilege
Current privilege level is 1
I cannot set the clock or go to the configure terminal mode:
R2>clock
% Unknown command or computer name, or unable to find computer address
R2>configure
% Unknown command or computer name, or unable to find computer address
```


- Then I login with “user/none”:

```
R2>login
Username: user
Password:
```

- The privilege level is three:

```
R2#show privilege
Current privilege level is 3
```

- I can set the clock but not going to the configure terminal mode:

```
R2#clock set 1:1:1 25 dec 2005
R2#
.Dec 25 09:01:01: %SYS-6-CLOCKUPDATE: System clock has been updated from
13:58:03 PST Sat Dec 24 2005 to 01:01:01 PST Sun Dec 25 2005, configured from
console by user on console.
R2#show clock
.01:01:04.711 PST Sun Dec 25 2005
```

```
R2#configure
% Unknown command or computer name, or unable to find computer address
```

- Finally, I log on as “manager/manager”:

```
R2#login
Username: manager
Password:
```

- The privilege level is 7:

```
R2#show privilege
Current privilege level is 7
```

- I can set the clock, just as “user/none” can:

```
R2#clock set 2:2:2 25 dec 2005
R2#
.Dec 25 10:02:02: %SYS-6-CLOCKUPDATE: System clock has been updated from
01:01:41 PST Sun Dec 25 2005 to 02:02:02 PST Sun Dec 25 2005, configured from
console by manager on console.
```

- I can also go to configure terminal mode:

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- However, I cannot set the routing protocol or any other thing:

```
R2(config)#router rip
^
% Invalid input detected at '^' marker.
```

- I can go to the interface:

```
R2(config)#interface fastEthernet 1/0
```


- I cannot change the encapsulation or anything else in the interface:

```
R2(config-if)#encap frame
% Invalid input detected at '^' marker.
```

- I can set the IP address and also shut down the interface:

```
R2(config-if)#ip address 1.1.1.1 255.255.255.0
Dec 25 10:02:52: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on FastEthernet1/0
from FULL to DOWN, Neighbor Down: Interface down or detached

R2(config-if)#shutdown
R2(config-if)#
Dec 25 10:02:58: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to
administratively down
Dec 25 10:02:59: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0, changed state to down
```

Core Dump to a RCP Server

Task 11-21

Configure R5 to send a Core Dump to a RCP Server located at 10.1.1.15.

- We want to create a core dump and send that to a RCP server. Therefore, we use the commands as shown below:

```
R5(config)#exception protocol rcp
R5(config)#exception dump 10.1.1.15
```

Task 11-22

The router logs into the RCP Server using a username of ipexpert.

- With the ip rcmd command, then we specify which server username the router should use.

```
R5(config)#ip rcmd remote-username ipexpert
```

Task 11-23

Set the Dump size to 32768.

- The size of 32768 is the size that I usually set in real life too.

```
R5(config)#exception region-size 32768
```


Task 11-24

The router should use the source address of 5.5.5.5, the Loopback address on R5.

- **Remember that the 5.5.5.5 is the loopback address and we are using that one as the source.**

```
R5(config)#ip rcmd source-interface Loopback0
```

- **In the production network, you are going to see a lot of output for the core dump. However, in this small network, you can still check whether you have program correctly with the following command:**

```
R5#sh exception
```

```
10.1.1.15
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

This page left intentionally blank.

Section 12: Multiprotocol Challenge A (One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 12 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 12 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

1 - Layer 2 Configuration (8 Points)

1.1 - Switch Management and Traffic control (4 Points)

- a) Create a Management interface on the Switch1 belonging to VLAN 6. Set the IP Address as .20 on that network.

```
Sw1(config)#int vlan 6
Sw1(config-if)#ip address 192.1.6.20 255.255.255.0
```

- b) Allow Management access to this switch from VLAN 6 only.

```
Sw1(config)#access-list 23 permit 192.1.6.0 0.0.0.255
Sw1(config)#line vty 0 15
Sw1(config-line)#access-class 23 in
```

- c) Port F 0/15 on the Switch1 is experiencing Broadcast and Multicast problems. Configure it so that broadcasts do not take more than 30% of the bandwidth and Multicast does not take more than 20% of the bandwidth. For broadcast traffic, the port should forward again when it falls below 25%. For Multicast traffic, the port should forward again when it falls below 15%.

→ **Storm control allows you to set levels for traffic. Newer code versions allow the setting of rising and falling thresholds.**

```
Sw1(config)#int fa0/15
Sw1(config-if)#storm-control broadcast level 30 25
Sw1(config-if)#storm-control multicast level 20 15
```

- d) Set the Port to Access Mode so that it does not negotiate the Port mode.

```
Sw1(config-if)#switchport mode access
```

- e) Configure port F0/15 on Switch1 to block inbound traffic with an ethertype value of 0x1234.

→ **A MAC access list will allow traffic filtering at layer 2, including Ethertype values.**

```
Sw1(config)#mac access-list extended NO1234
Sw1(config-ext-macl)#deny any any 0x1234 0
Sw1(config-ext-macl)#permit any any
```

```
Sw1(config)#int fa0/15
Sw1(config-if)#mac access-group NO1234 in
```


1.2 - Catalyst Security (4 Points)

- a) Add VLAN 123 to Cat1. Configure MAC address filtering and only permit MAC address from 0000.1234.4321 to 0000.4321.1234 for Vlan 123.

→ For more granular control, vlan maps can be used to restrict traffic. Setup is similar to a route map, where individual clauses match, and can either permit (forward) or deny (drop). Start with a mac access-list to match the traffic that you want to permit in the filter.

```
Sw1(config)#vlan 123
Sw1(config-vlan)#state active

Sw2(config)#mac access-list extended from1234
Sw2(config-ext-macl)#permit host 0000.1234.4321 host 0000.4321.1234
Sw2(config-ext-macl)#exit
Sw2(config)#vlan access-map VLAN123filter 10
Sw2(config-access-map)#match mac address from1234
Sw2(config-access-map)#action forward
Sw2(config-access-map)#exit
Sw2(config)#vlan access-map VLAN123filter 20
Sw2(config-access-map)#action drop
Sw2(config-access-map)#exit
Sw2(config)#vlan filter VLAN123filter vlan-list 123
```

2 - PIX Firewall / ASA Configuration (17 Points)

2.1 - PIX IP Address (3 Points)

- a) Assign IP Addresses to the PIX Firewall interfaces as shown in the diagram. Eth0 is the outside interface, and should have a security level of 0. Eth1 is the inside interface and should have a security level of 100.

→ Configure the interface names, and apply the addresses.

```
pixfirewall(config)#int eth0
pixfirewall(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)#ip address 192.1.12.10 255.255.255.0
pixfirewall(config-if)#no shut
pixfirewall(config-if)#int eth1
pixfirewall(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)#ip address 10.2.2.10 255.255.255.0
pixfirewall(config-if)#no shut
```

2.2 - Routing (3 Points)

- a) Run RIP as the routing protocol on the PIX Firewall. Configure RIP such that it only receives routes from the outside interface.

```
pixfirewall(config)#router rip
pixfirewall(config-router)#version 2
pixfirewall(config-router)#no auto-summary
```



```

pixfirewall(config-router)#network 10.0.0.0
pixfirewall(config-router)#network 192.1.12.0
pixfirewall(config-router)#passive outside

```

- b) Configure RIP such that it receives routes from the inside interface and also injects a default route from the inside interface.

→ Since the network statement was already added in the previous step, we just need to configure the PIX to send a default route.

```

pixfirewall(config)#router rip
pixfirewall(config-router)#default-information originate

```

2.3 - Address Translation (4 Points)

- a) There is a Web/SMTP/DNS Server at 10.1.1.55. Create a Static Mapping to 192.1.12.55. Allow the appropriate entries in the access-list.

→ Web servers use TCP ports 80 for http and 443 for HTTPS. SMTP is TCP port 25. DNS uses UDP port 53 for lookups and TCP port 53 for zone transfers. When allowing access, remember to configure the access-list using the translated address.

```

pixfirewall(config)#static (inside,outside) 192.1.12.55 10.1.1.55
netmask 255.255.255.255

```

```

pixfirewall(config)#access-list outsideint permit tcp any host
192.1.12.55 eq 25
pixfirewall(config)#access-list outsideint permit tcp any host
192.1.12.55 eq 53
pixfirewall(config)#access-list outsideint permit tcp any host
192.1.12.55 eq 80
pixfirewall(config)#access-list outsideint permit tcp any host
192.1.12.55 eq 443
pixfirewall(config)#access-list outsideint permit udp any host
192.1.12.55 eq 53
pixfirewall(config)#access-group outsideint in interface outside

```

- b) Also create a static mapping to R1. Create a static mapping to 192.1.12.15. Allow Telnet access to R1 from R2 only in the access-list.

```

pixfirewall(config)#static (inside,outside) 192.1.12.15 10.2.2.1
netmask 255.255.255.255
pixfirewall(config)#access-list outsideint permit tcp host 192.1.12.2
host 192.1.12.15 eq 23

```

- c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow the appropriate entries in the access-list for TACACS+. Only allow R2 to communicate to the TACACS+ server. R2 should communicate to the TACACS+ server using its loopback0 interface.

```

pixfirewall(config)#static (inside,outside) 192.1.12.100 10.1.1.100
netmask 255.255.255.255
pixfirewall(config)#access-list outsideint permit tcp host 2.2.2.2
host 192.1.12.100 eq 49

```

```

R2(config)#ip tacacs source-int lo0

```


- d) Enable Nat-control on the PIX.

```
pixfirewall(config)#nat-control
```

2.4 – Transparent Firewall (2 points)

- a) Configure ASA1 in transparent firewall mode for the VLANs connecting R4 and R9. Make sure that the routing protocol adjacencies between R4 and R9 work after completing this step. Do not configure contexts for this step.

```
ciscoasa(config)#firewall transparent
ciscoasa(config)#hostname ASA1
ASA1(config)#int eth0/0
ASA1(config-if)#no shut
ASA1(config-if)#int eth0/1
ASA1(config-if)#no shut

ASA1(config)#int eth0/0
ASA1(config-if)#nameif outside
IICMP: icmp_open Entry for context 0
NFO: Security level for "outside" set to 0 by default.
ASA1(config-if)#int eth0/1
ASA1(config-if)#nameif inside
IICMP: icmp_open Entry for context 0
NFO: Security level for "inside" set to 100 by default.

ASA1(config)#ip address 192.1.49.55 255.255.255.0
```

- At a minimum, we need to allow OSPF and BGP traffic, and possibly ICMP echo and echo-reply for ping testing. Since we are not given any restrictions on what traffic to allow, we can just allow all IP traffic.

```
ASA1(config)#access-list ROUTING permit ip any any
ASA1(config)#access-group ROUTING in interface outside
ASA1(config)#access-group ROUTING in interface inside
```

2.5 – Contexts (2points)

- a) Configure ASA2 in transparent firewall mode for the VLANs connecting R5 and BB2, using contexts. Use the context name r5tobb2. Configure interfaces eth0/0 and eth0/1 for a security level of 100.

- Configuration for ASA2 will be similar, but we will be using contexts. Start by switching to multiple context mode.

```
ciscoasa(config)#mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
```


- **Enable the interfaces, create the context, and allocate the interfaces. We need to also create an admin context, but we do not have to assign it any interfaces.**

```
ciscoasa(config)#firewall transparent

ciscoasa(config)#int eth0/0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#int eth0/1
ciscoasa(config-if)#no shut

ciscoasa(config)#admin-context MYADMIN
ciscoasa(config)#context MYADMIN
ciscoasa(config-ctx)#config-url disk0:MYADMIN
INFO: Converting disk0:MYADMIN to disk0:/MYADMIN

WARNING: Could not fetch the URL disk0:/MYADMIN
INFO: Creating context with default config
INFO: Admin context will take some time to come up .... please wait.
ciscoasa(config-ctx)#exit
ciscoasa(config)#

ciscoasa(config)#context r5tobb2
Creating context 'r5tobb2'... Done. (5)
ciscoasa(config-ctx)#config-url disk0:r5tobb2
INFO: Converting disk0:r5tobb2 to disk0:/r5tobb2

WARNING: Could not fetch the URL disk0:/r5tobb2
INFO: Creating context with default config
ciscoasa(config-ctx)#allocate-interface eth0/0
ciscoasa(config-ctx)#allocate-interface eth0/1

ciscoasa(config)#hostname ASA2
ASA2(config)#
ASA2(config)#changeto context r5tobb2
ASA2/r5tobb2(config-if)#int eth0/0
ASA2/r5tobb2(config-if)#nameif outside
ASA2/r5tobb2(config-if)#int eth0/1
ASA2/r5tobb2(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA2/r5tobb2(config-if)#exit
ASA2/r5tobb2(config)#ip address 10.5.5.55 255.255.255.0

ASA2/r5tobb2(config)#route outside 0 0 10.5.5.5
```

- **To allow traffic to pass between interfaces with the same security level, use the same-security-traffic command. Again, we are not given traffic restrictions, so we can permit everything. At a minimum, EIGRP and BGP need to be allowed for the routing protocol adjacencies, and possibly ICMP for testing.**

```
ASA2/r5tobb2(config)#same-security-traffic permit inter-interface

ASA2/r5tobb2(config)#access-list ROUTING permit ip any any
ASA2/r5tobb2(config)#access-group ROUTING in interface outside
ASA2/r5tobb2(config)#access-group ROUTING in interface inside
```


2.6 – Management / Filtering (3 points)

- a) Configure ASA1 to allow management access via SSH on the interface connecting to R4.

- **Add a username and password, and add local authentication for SSH. Allow ssh on the outside interface.**

```
ASA1(config)#ssh 192.1.49.0 255.255.255.0 outside
ASA1(config)#username cisco password cisco
```

```
ASA1(config)#aaa authentication ssh console LOCAL
```

- **Verify by connecting from R4.**

```
R4#ssh -l cisco 192.1.49.55
```

Password:

Type help or '?' for a list of available commands.

```
ASA1>
```

- b) Configure ASA1 to block ICMP type 0 traffic with a source of R9's Ethernet interface, and a destination of R4's Ethernet interface. ICMP type 8 traffic should not be affected.

- **Type 8 is echo, type 0 is echo reply.**

```
ASA1(config)#access-list INSIDE deny icmp host 192.1.49.9 host
192.1.49.4 ech$
```

```
ASA1(config)#access-list INSIDE permit ip any any
```

```
ASA1(config)#access-group INSIDE in interface inside
```

3 - IDS Configuration (16 Points)

3.1 - Basic Configuration of IDS (4 Points)

- a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the AAA server based on the Network Diagram.

- **Run Setup from the command line.**

```
Continue with configuration dialog?[yes]:
```

```
Enter host name[sensor]: IDS
```

```
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.15/24,10.1.1.1
```

```
Enter telnet-server status[disabled]:
```

```
Enter web-server port[443]:
```

```
Modify current access list?[no]: yes
```

```
Current access list entries:
```

```
No entries
```

```
Permit: 10.1.1.0/24
```

```
Permit:
```

```
Modify system clock settings?[no]:
```

```
Modify virtual sensor "vs0" configuration?[no]:
```


→ **Verify that you can ping the ACS server.**

```
IDS#ping 10.1.1.100
PING 10.1.1.100 (10.1.1.100): 56 data bytes
64 bytes from 10.1.1.100: icmp_seq=0 ttl=127 time=4.4 ms
64 bytes from 10.1.1.100: icmp_seq=1 ttl=127 time=0.6 ms
64 bytes from 10.1.1.100: icmp_seq=2 ttl=127 time=2.4 ms
64 bytes from 10.1.1.100: icmp_seq=3 ttl=127 time=1.2 ms

--- 10.1.1.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.6/2.1/4.4 ms
IDS#
```

b) You would like to monitor all traffic received in the outside VLAN of the PIX.

→ **The IDS Sensing interface is connected to port fa0/7 on Cat1. The devices connected to the outside VLAN are the PIX outside interface on port fa0/2 on cat2 and R2's interface fa1/0 connected to fa0/2 on Cat1.**

```
Sw1(config)#monitor session 1 source vlan 12 , 555 rx
Sw1(config)#monitor session 1 dest int fa0/7

Sw1(config)#vlan 555
Sw1(config-vlan)#remote-span

Sw2(config)#monitor session 1 source vlan 12 rx
Sw2(config)#monitor session 1 dest remote vlan 555
```

c) Configure the Switch to copy all relevant traffic to the monitoring port.

→ **This was accomplished in the previous step.**

3.2 - Enabling and Fine tuning the ICMP Echo Request Signature (4 Points)

a) Enable the ICMP Echo Request Signature.

b) Set the Alarm Severity to High.

c) Verify the Alarm by pinging the outside Interface of the PIX from R2.

```
IDS(config)#service interface
IDS(config-int)#physical-interfaces FastEthernet0/1
IDS(config-int-phy)#admin-state enabled

IDS(config)#service analysis-engine
IDS(config-ana)#virtual-sensor vs0
IDS(config-ana-vir)#physical-interface FastEthernet0/1 subinterface-
number 0
```



```
IDS (config) #service signature-definition sig0
IDS (config-sig) #signatures 2004 0
IDS (config-sig-sig) #alert-severity high
IDS (config-sig-sig) #status
IDS (config-sig-sig-sta) #enabled true
```

- For an example of how to configure via the GUI, see the IDS section in this Proctor Guide.

3.3 - Creating a Custom Signature (4 Points)

- Create a custom string signature
- Set the Alarm Severity to High.
- If sensor detects telnet traffic with a string of "admin", it should fire this alarm.
- Enable telnet on R1 by assigning it a password of telnet. Configure a static route on R1 for the 192.1.12.0 network via the PIX. It is learning this route through the concentrator.
- Verify the Alarm by connecting into R1 for Telnet and typing the work "admin" after you are connected.

```
IDS (config) #service signature-definition sig0
```

```
IDS (config-sig) #
IDS (config-sig) #no signatures 60000 0
IDS (config-sig) #signatures 60000 0
IDS (config-sig-sig) #alert-severity high
IDS (config-sig-sig) #engine string-tcp
IDS (config-sig-sig-str) #regex-string admin
IDS (config-sig-sig-str) #service-ports 23
```

```
R1 (config) #line vty 0 15
R1 (config-line) #password telnet
```

```
R1 (config-line) #ip route 192.1.12.0 255.255.255.0 10.2.2.10
```

- **Note:** The static NAT and access list for the telnet connection from R2 to R1 was configured in an earlier step.
- Verify the signature fires and is visible on the event viewer.

3.4 - IOS IDS (4 Points)

- Configure IDS on R6 for attacks from the Frame Relay clouds.
- Configure the IOS IDS with the following parameters:
 - Send the alarm to a syslog server.
 - Configure the Router with the Syslog Server's Address at 192.1.12.65.

- Pretty straightforward, configure logging, and apply the inspection to the interface.

```
R6(config)#ip ips name MYIDS
R6(config)#ip ips notify log
R6(config)#logging host 192.1.12.65
R6(config)#int ser0/1/0
R6(config-if)#ip ips MYIDS in
```

- c) Configure Static mappings and access-list entries on the PIX to allow this type of traffic. The syslog is at 10.1.1.65.

```
pixfirewall(config)#static (inside,outside) 192.1.12.65 10.1.1.65
netmask 255.255.255.255
pixfirewall(config)#access-list outsideint permit udp host 192.1.26.6
host 192.1.12.65 eq 514
```

4 - BGP Routing Configuration (4 Points)

4.1 – BGP Traffic Policy (4 Points)

- a) Configure R2 to dynamically propagate information for static routes added to R2 with the following parameters:

- If a static route is added with tag 12345, the network should be advertised into BGP.
- The routes should be seen on R4 and R5 with a next-hop address of 192.0.0.1.
- Traffic destined to these networks should be dropped locally by R4 and R5, and not forwarded to R2.
- Routing information for these networks should not be propagated beyond AS 245. Do not use any distribute-lists or route-maps to filter outbound to BB2 or R9.
- In order to prevent the information from being sent further, you can use the no-export community. On R4 and R5, drop the traffic locally with a route to Null0 for 192.0.0.1. R4 and R5 would still send an ICMP unreachable message (backscatter) back to the source address, unless you configured the command “no ip unreachable” on the Null0 interface. This is not required for the section, however.

```
R2(config)#route-map TRAFPOLICY
R2(config-route-map)#match tag 12345
R2(config-route-map)#set ip next-hop 192.0.0.1
R2(config-route-map)#set community no-export
```

```
R2(config)#router bgp 245
R2(config-router)#redist static route-map TRAFPOLICY
R2(config-router)#neighbor 4.4.4.4 send-community
R2(config-router)#neighbor 5.5.5.5 send-community
```

```
R2(config)#ip route 155.55.55.55 255.255.255.255 192.0.0.1 tag 12345
R2(config)#ip route 192.0.0.1 255.255.255.255 null0
```

```
R4(config)#ip route 192.0.0.1 255.255.255.255 null0
R5(config)#ip route 192.0.0.1 255.255.255.255 null0
```


5 - Access Management Configuration (9 Points)

5.1 - Management of R2 using Telnet (5 Points)

- a) Setup R2 with AAA access.

→ On the ACS server, configure R2 as a AAA client under Network configuration.

```
R2(config)#ip tacacs source-int lo0
```

- b) No Authentication or authorization should be done on the Console or AUX lines.

```
R2(config)#aaa new-model
R2(config)#aaa authentication login default none
R2(config)#tacacs-server host 192.1.12.100 key cisco
```

- c) Setup Authentication based on TACACS+ for the VTY lines.

```
R2(config)#aaa authentication login VTYMETHOD group tacacs
R2(config)#line vty 0 15
R2(config-line)#login authentic VTYMETHOD
```

- d) Create 2 users on the AAA server, User1 and User2. Both the users should have cisco as their password.

→ Create the users on both the ACS server, and locally on R2.

```
R2(config)#username User1 priv 15 password cisco
R2(config)#username User2 priv 7 password cisco
```

→ Use the TEST AAA command to verify that the users were successfully added on the ACS server.

```
R2#test aaa group tacacs+ User1 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2#test aaa group tacacs+ User2 cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

```
R2#
```

- e) Setup Authorization based on Local Privilege Levels defined as follows:

- Setup authorization for User1 such that the user can type all commands. User1 should be in Privilege Exec mode when logged in.
- Setup authorization for User2 such that the user can type all commands specified in Privilege Level 7. Privilege Level 7 should allow the user to type all commands for snmp-server in global configuration mode. This privilege level should also allow the user to change the hostname of the Router.

→ **Configure the commands for snmp, hostname, and config for privilege level 7.**

```
R2(config)#privilege configure all level 7 snmp-server
R2(config)#privilege configure level 7 hostname
R2(config)#privilege exec level 7 configure terminal
R2(config)#privilege exec level 7 configure
R2(config)#aaa authorization commands 1 NO none
R2(config)#aaa authorization commands 7 NO none
R2(config)#aaa authorization commands 15 NO none
R2(config)#aaa authorization commands 1 YES local
R2(config)#aaa authorization commands 7 YES local
R2(config)#aaa authorization commands 15 YES local
```

```
R2(config)#line aux 0
R2(config-line)#authorization commands 1 NO
R2(config-line)#authorization commands 7 NO
R2(config-line)#authorization commands 15 NO
R2(config-line)#line vty 0 15
R2(config-line)#authorization commands 1 YES
R2(config-line)#authorization commands 7 YES
R2(config-line)#authorization commands 15 YES
```

```
R2(config)#line aux 0
R2(config-line)#authorization exec NO
R2(config-line)#line vty 0 15
R2(config-line)#authorization exec YES
```

→ **Verify by telnetting to R2 and logging in as one of the new users.**

```
R2#telnet 2.2.2.2
Trying 2.2.2.2 ... Open
```

```
Username: User2
Password:
```

```
R2#show priv
Current privilege level is 7
R2
```

- f) Configure Accounting for all commands typed by users from Telnet. You should be able to charge the users based on usage times.

```
R2(config)#aaa accounting exec YES start-stop group tacacs+
R2(config)#aaa accounting commands 1 YES start-stop group tac
R2(config)#aaa accounting commands 7 YES start-stop group tac
R2(config)#aaa accounting commands 15 YES start-stop group tac
```

```
R2(config)#line vty 0 15
R2(config-line)#accounting exec YES
R2(config-line)#accounting commands 1 YES
R2(config-line)#accounting commands 7 YES
R2(config-line)#accounting commands 15 YES
```


- g) Only allow VLAN 6 to be able to telnet into R2.

```
R2 (config)#access-list 23 permit 192.1.6.0 0.0.0.255
R2 (config)#line vty 0 15
R2 (config-line)#access-class 23 in
```

5.2 - HTTP Management (2 Points)

- a) Configure HTTP Management on R2.

```
R2 (config)#ip http server
```

- b) Only Users from the VLAN 49 should be able to manage this router through HTTP.

```
R2 (config)#ip http authentication local
R2 (config)#ip http access-class 49
R2 (config)#access-list 49 permit 192.1.49.0 0.0.0.255
```

- c) HTTP should authenticate to the already configured AAA.

```
R2 (config)#ip http authentication local
```

5.3 – ASA Management (2 points)

- a) ASA1 is configured to allow SSH management. Configure ASA1 to authenticate SSH sessions via TACACS+. Create a user asamgr with password !p3xp3rt on the ACS server. Verify that you can connect to ASA1 via SSH from R2.

➔ On the PIX, configure to allow the inbound TACACS traffic from ASA1. On the ASA, configure to permit SSH from R2. Since the ACS server is reached via the outside interface, make sure that you specify the outside interface in the server definition.

```
pixfirewall (config)#access-list outsideint permit tcp host
192.1.49.55 host 192.1.12.100 eq tacacs
```

```
ASA1 (config)#ssh 192.1.24.2 255.255.255.255 outside
```

```
ASA1 (config)#aaa-server TAC prot tacacs+
ASA1 (config)#aaa-server TAC (outside) host 192.1.12.100
ASA1 (config-aaa-server-host)#key cisco
```

```
ASA1 (config)#no aaa authent ssh console LOCAL
ASA1 (config)#aaa authent ssh console TAC
```


→ **Verify that you can log in from R2.**

```
R2#ssh -l asamgr 192.1.49.55
```

```
Password:
Type help or '?' for a list of available commands.
ASA1> en
Password: *****
Invalid password
Password:
ASA1#
```

6 - IP Services Configuration (8 Points)

6.1 - Creating Core Dumps (2 Points)

- Configure R5 to send a Core Dump to a TFTP Server located at 192.1.12.100.
- Set the Dump size to 32768.
- The router should use the source address of 5.5.5.5, the Loopback address on R5.

→ **Since 192.1.12.100 is the translated address of the ACS server, make sure that you also allow the traffic to pass through the PIX.**

```
R5(config)#exception dump 192.1.12.100
R5(config)#exception prot tftp
R5(config)#exception region-size 32768
R5(config)#ip tftp source-int loop0
```

```
pixfirewall(config)#access-list outsideint permit udp host 5.5.5.5
host 192.1.12.100 eq 69
```

6.2 - DHCP Server (4 Points)

- Enable R4 as a DHCP Server with the following information:

- IP ADDRESS : 192.1.49.0/24
- WINS ADDRESS : 192.1.49.135
- DNS ADDRESS : 192.1.49.53
- DEFAULT GATEWAY : 192.1.49.4
- LEASE TIME : 6 Days

- Enable conflict logging on R4.

```
R4(config)#no ip dhcp conflict logging
R4(config)#ip dhcp excluded-address 192.1.49.53
R4(config)#ip dhcp excluded-address 192.1.49.135
R4(config)#ip dhcp pool R4
R4(dhcp-config)#network 192.1.49.0 255.255.255.0
R4(dhcp-config)#netbios-name-server 192.1.49.135
R4(dhcp-config)#dns-server 192.1.49.53
R4(dhcp-config)#default-router 192.1.49.4
R4(dhcp-config)#option 19 hex 01
```


- c) Configure option 19 to tell the client should configure its IP layer for packet forwarding.

→ This was configured in the previous step.

- d) Specifies four ping attempts by the DHCP server before ceasing any further ping attempts.

```
R4 (config) #ip dhcp ping packets 4
```

- e) Configure switch1 for DHCP snooping for this VLAN.

```
Sw1 (config) #ip dhcp snooping
Sw1 (config) #ip dhcp snooping vlan 49

Sw1 (config) #int fa0/4
Sw1 (config-if) #ip dhcp snooping trust
```

→ Verify with show ip dhcp snooping:

```
Sw1 #show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
49
Insertion of option 82 is enabled
  circuit-id format: vlan-mod-port
  remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/4          yes         unlimited
Sw1 #
```

6.3 - NTP (2 Points)

- a) Configure R2 as the NTP clock master.

```
R2 (config) #ntp master
```

- b) Configure R6 to use NTP clock from R2 in a secured way. R2 should not have any NTP authentication keys configured to achieve this task.

```
R2 (config) #int tunnel26
R2 (config-if) #ip address 192.168.26.2 255.255.255.0
R2 (config-if) #tun source ser0/1/0.6
R2 (config-if) #tun dest 192.1.26.6

R6 (config) #int tun26
R6 (config-if) #ip address 192.168.26.6 255.255.255.0
R6 (config-if) #tun source ser0/1/0
R6 (config-if) #tun dest 192.1.26.2

R6 (config) #ntp server 192.168.26.2
```


7 - Virtual Private Networks Configuration (18 Points)

7.1 - Basic Concentrator Configuration (3 Points)

a) Configure the IP Address of the Private Interface through the CLI.

→ The basic setup through the CLI prompts you for basic setup information. After you have configured the private IP address, make sure to save changes and then you can access the GUI for the remainder of the setup.

b) The Public interface should be configured from the Graphical interface.

→ You can configure the public interface from either the GUI or from the command line.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager GUI. The left sidebar contains a navigation tree with categories like Configuration, Administration, and Monitoring. The main content area is titled 'Configuring Ethernet Interface 2 (Public)'. It features a 'General' tab and a table of 'General Parameters'.

Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask.
	IP Address	192.1.12.5	Enter the IP Address and Subnet Mask for this interface.
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address		The MAC address for this interface.
	Interface Name		Enter the textual name of the interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPsec Fragmentation Policy	<input checked="" type="radio"/> Do not fragment prior to IPsec encapsulation; fragment prior to interface transmission <input type="radio"/> Fragment prior to IPsec encapsulation with Path MTU Discovery (ICMP) <input type="radio"/> Fragment prior to IPsec encapsulation without Path MTU Discovery (Clear DF bit)	

At the bottom of the configuration window are 'Apply' and 'Cancel' buttons.

c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

→ In this setup, a static route is not necessary on the concentrator. You should be familiar with how to add a static route to the concentrator, if needed, from the command line interface.

→ From the main menu on the CLI, the path to follow is:

Configuration – System Management – IP Routing – Static Routes – Add Static route.

d) Configure the concentrator to send routes using RIP on the private interface.

→ By default, RIP is enabled on the private interface to receive routes. Outbound RIP is disabled by default. In order for later sections to work, you need to enable it outbound on the private interface.

Configuration – Interfaces – Private – Outbound RIP.

e) Configure a Default Route on the Public Interface pointing towards R2.

→ The concentrator is learning a default route from the PIX. Configuring a static route, will allow R2 to be preferred

→ Under Configuration-system- IP Routing – Default Gateways, add the router address or 192.1.12.2 as a default gateway.

7.2 - Setup a Site-to-Site IPsec VPN between the Concentrator and R5 (4 Points)

a) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- For IPsec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

b) You can use static routes on R5 and R1 to accomplish this.

```
R5(config)#crypto isakmp key ccie address 192.1.12.5
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#hash md5
R5(config-isakmp)#authent pre-share

R5(config)#crypto ipsec transform-set VPNC esp-des esp-sha-hmac
R5(cfg-crypto-trans)#mode tunnel

R5(config)#access-list 172 permit ip 10.5.5.0 0.0.0.255 10.2.2.0
0.0.0.255
R5(config)#crypto map R5MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R5(config-crypto-map)#match address 172
R5(config-crypto-map)#set peer 192.1.12.5
R5(config-crypto-map)#set transform VPNC

R5(config)#int ser0/1/0
R5(config-if)#crypto map R5MAP

R5(config)#ip route 10.2.2.0 255.255.255.0 192.1.25.2
```


- Add a static route to the VPN concentrator for the 10.5.5.0/24 network, with a destination of R2.
- Check the routing table on the VPN Concentrator. Depending on how you set up the routing on the PIX, you may also need to add a route to 192.1.25.0/24 via the public interface.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logged in

Configuration | Administration | Monitoring

Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - IPsec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

Configuration: Tunneling and Security: IPsec: LAN-to-LAN: Add

Add a new IPsec LAN-to-LAN connection.

Enable ☒

Name

Interface

Connection Type

Peers

Digital Certificate

Certificate Transmission ☐ Entire certificate chain ☐ Identity certificate only

Preshared Key

Authentication

Encryption

IKE Proposal

Filter

Check to enable this LAN-to-LAN connection.

Enter the name for this LAN-to-LAN connection.

Select the interface for this LAN-to-LAN connection.

Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.

Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

Select the digital certificate to use.

Choose how to send the digital certificate to the IKE peer.

Enter the preshared key for this LAN-to-LAN connection.

Specify the packet authentication mechanism to use.

Specify the encryption mechanism to use.

Select the IKE Proposal to use for this LAN-to-LAN connection.

Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection.

CISCO SYSTEMS

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin

Configuration | Administration | Monitoring

Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

Encryption: DES-56
IKE Proposal: IKE-DES-MD5
Filter: -None-
IPSec NAT-T: ☐
Bandwidth Policy: -None-
Routing: None

Specify the encryption mechanism to use.
Select the IKE Proposal to use for this LAN-to-LAN connection.
Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Choose the routing mechanism to use. **Parameters below are ignored if Network Autodiscovery is chosen.**

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.
Network List: Use IP Address/Wildcard-mask below
IP Address: 10.2.2.0
Wildcard Mask: 0.0.0.255
Note: Enter a **wildcard** mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.
Network List: Use IP Address/Wildcard-mask below
IP Address: 10.5.5.0
Wildcard Mask: 0.0.0.255
Note: Enter a **wildcard** mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

Add Cancel

Cisco Systems, Inc. VPN 3000 Concentrator [10.2.2.5] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Go Links

Address http://10.2.2.5/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin

Configuration | Administration | Monitoring

Configuration | Tunneling and Security | IPSec LAN-to-LAN | Add | Done

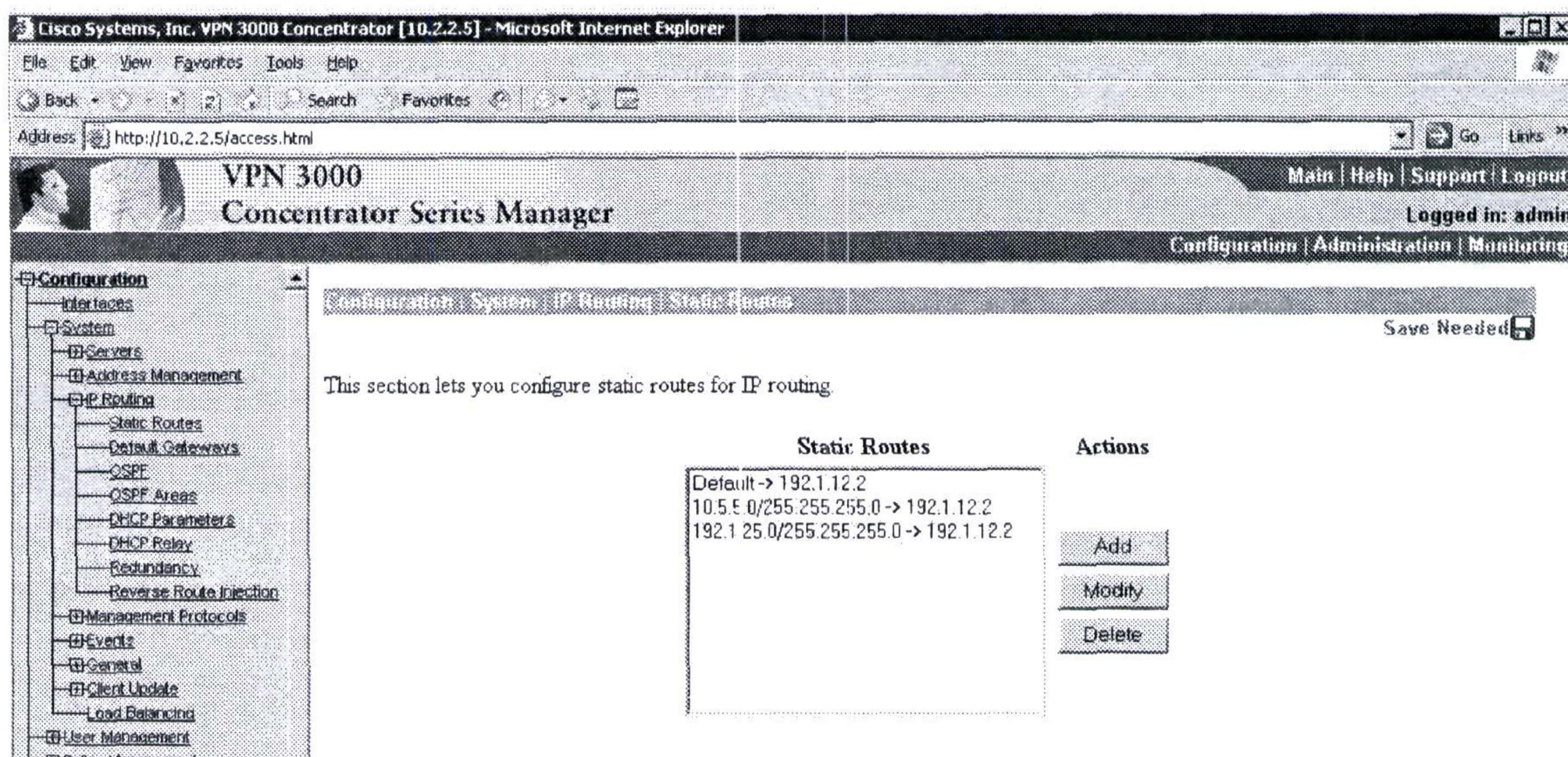
Save Needed

An IPSec LAN-to-LAN connection has been successfully configured. The following have been added to your configuration:

Authentication Server Internal
Group 192.1.25.5
Security Association L2L: R5
Filter Rules L2L: R5 Out
L2L: R5 In

Modifying any of these items will affect the LAN-to-LAN configuration. The **Group** is the same as your LAN-to-LAN peer. The **Security Association** and **Filter Rules** all start with "L2L:" to indicate that they form a LAN-to-LAN configuration.

OK



→ Verify that you can ping R1's address with a source of R5's Ethernet address.

```
R5#ping 10.2.2.1 source 10.5.5.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.5.5.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R5#

7.3 - Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

a) Use the following parameters to setup Concentrator with the following options:

- Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created on the Concentrator.
- Set the username as VPNUser with a password of **ccie1234**.
- Create a group called Remote with a password of **ccie**.

b) The network 10.3.3.0 should be propagated to R1 through RIP.

- Add the group under User Management - Groups – Add Group.
- Add the address pool for the group, by selecting the group and “add address pool”
- Add the user under Configuration – User Management – Users.
- Under system – IP routing, select Generate holddown routes, and apply.
- Under system – address management -- assignment, select use address pools.
- You can verify by connecting from the Test PC, however since split tunneling is not configured, you will may lose your connection to the Test PC.

VPN 3000 Concentrator Series Manager

Logged in: admin

Configuration | Administration | Monitoring

session, click on that session's name.

Group:

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
1	1	1	3	3	2	1.00%	200	8

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	1	1

LAN-to-LAN Sessions

[Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
R5	192.125.5	IPSec/LAN-to-LAN	DES-56	Feb 3 13:42:33	1:42:28	1456	1456

Remote Access Sessions

[LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
VPNUser	10.3.3.1 192.1.12.33	Remote	IPSec 3DES-168	Feb 3 15:24:33 0:00:28	WinNT 4.8.0.10300	0 3072	N/A

Management Sessions

[LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	10.1.1.100	HTTP	None	Feb 03 14:01:38	0:23:22

Overall System Status

- Make sure that R1 sees the route for the 10.3.3.0/24 network. If you did not enable outbound RIP updates on the VPN concentrator's private interface, R1 will not receive the update from the concentrator.

R1#show ip route 10.3.3.0

Routing entry for 10.3.3.0/24

Known via "rip", distance 120, metric 1

Redistributing via rip

Last update from 10.2.2.5 on FastEthernet0/0, 00:00:16 ago

Routing Descriptor Blocks:

* 10.2.2.5, from 10.2.2.5, 00:00:16 ago, via FastEthernet0/0

Route metric is 1, traffic share count is 1

R1#

7.4 - Setup a Site-to-Site IPsec VPN between the R2 and R6 (4 Points)

- a) Create the following loopbacks on R2 and R6:

- R2 - Int loo 10 : 192.168.102.2/24
- R6 - Int loo 10 : 192.168.106.6/24

- b) Create a GRE tunnel from R2 S 0/1/0.6 to R6 S 0/1/0. Route the newly created loopbacks over the tunnel using EIGRP in AS 26.

- Depending on how you configured step 6.3, it is possible that you already have the tunnel created. If so, just add the networks to EIGRP.

```
R2 (config) #router eigrp 26
R2 (config-router) #network 192.168.26.0
R2 (config-router) #network 192.168.102.0
```

```
R6 (config) #router eigrp 26
R6 (config-router) #network 192.168.26.0
R6 (config-router) #network 192.168.106.0
```

- c) Encrypt traffic going on the GRE tunnel including the EIGRP traffic using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm and Group 2 for the Diffie-Hellman key exchange. Use defaults for the rest of the parameters.
- For IPsec, use ESP-DES for encryption and ESP-MD5-HMAC for Authentication in Transport Mode.

- Start with the key on both sides:

```
R2 (config) #crypto isakmp key ccie address 192.1.26.6
```

```
R6 (config) #crypto isakmp key ccie address 192.1.26.2
```

- Configure the isakmp policies:

```
R2 (config) #crypto isakmp policy 10
R2 (config-isakmp) #hash md5
R2 (config-isakmp) #authent pre-share
R2 (config-isakmp) #group 2
```

```
R6 (config) #crypto isakmp policy 10
R6 (config-isakmp) #hash md5
R6 (config-isakmp) #authent pre-share
R6 (config-isakmp) #group 2
```

- Configure the transform sets:

```
R2 (config) #crypto ipsec transform-set R2R6 esp-des esp-md5-hmac
R2 (cfg-crypto-trans) #mode transport
```

```
R6 (config) #crypto ipsec transform-set R2R6 esp-des esp-md5-hmac
R6 (cfg-crypto-trans) #mode transport
```


→ **Configure the access lists:**

```
R2(config)#access-list 151 permit gre host 192.1.26.2 host 192.1.26.6
```

```
R6(config)#access-list 151 permit gre host 192.1.26.6 host 192.1.26.2
```

→ **Configure the crypto maps:**

```
R2(config)#crypto map secure 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

```
R2(config-crypto-map)#set peer 192.1.26.6
```

```
R2(config-crypto-map)#set transform-set R2R6
```

```
R2(config-crypto-map)#match address 151
```

```
R6(config)#crypto map secure 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

```
R6(config-crypto-map)#set peer 192.1.26.2
```

```
R6(config-crypto-map)#set transform-set R2R6
```

```
R6(config-crypto-map)#match address 151
```

→ **Apply to the interfaces:**

```
R2(config-crypto-map)#int ser0/1/0.6
```

```
R2(config-subif)#crypto map secure
```

```
R6(config)#int ser0/1/0
```

```
R6(config-if)#crypto map secure
```

→ **Verify with show crypto ipsec sa:**

```
R6#show crypto ipsec sa
```

```
interface: Serial0/1/0
```

```
  Crypto map tag: secure, local addr 192.1.26.6
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (192.1.26.6/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (192.1.26.2/255.255.255.255/47/0)
```

```
current_peer 192.1.26.2 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 165, #pkts encrypt: 165, #pkts digest: 165
```

```
  #pkts decaps: 165, #pkts decrypt: 165, #pkts verify: 165
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

```
  #pkts not compressed: 0, #pkts compr. failed: 0
```

```
  #pkts not decompressed: 0, #pkts decompress failed: 0
```

```
  #send errors 1, #recv errors 0
```

```
local crypto endpt.: 192.1.26.6, remote crypto endpt.: 192.1.26.2
```

```
path mtu 1500, ip mtu 1500
```

```
current outbound spi: 0x8AE41CB5(2330205365)
```


8 - IOS Firewall Configuration (8 Points)

8.1 - Cisco IOS Firewall (4 Points)

- a) On R4, inspect all tcp, udp and icmp traffic from the Ethernet segment going towards the Frame networks.

→ Start by configuring the inspection, and apply to the interface.

```
R4(config)#ip inspect name MYFW tcp
R4(config)#ip inspect name MYFW udp
R4(config)#ip inspect name MYFW icmp
```

```
R4(config)#int ser0/0/0
R4(config-if)#ip inspect MYFW out
```

- b) Only allow relevant traffic coming in.

→ We have BGP and OSPF sessions to permit.

```
R4(config)#ip access-list extended 121
R4(config-ext-nacl)#permit tcp host 2.2.2.2 host 4.4.4.4 eq bgp
R4(config-ext-nacl)#permit tcp host 2.2.2.2 eq bgp host 4.4.4.4 est
R4(config-ext-nacl)#permit ospf host 192.1.24.2 host 224.0.0.5
R4(config-ext-nacl)#permit ospf host 192.1.24.2 host 192.1.24.4
R4(config-ext-nacl)#deny ip any any log
```

- c) ACL should be set to inbound on the Serial interface.

```
R4(config)#int ser0/0/0
R4(config-if)#ip access-group 121 in
```

8.2 - Cisco IOS Firewall tuning (2 Points)

- a) Set the IOS Firewall such that it blocks half-open connections if they exceed 1000 and stop deleting the connections if they reach 800.
- b) Also set it for a one-minute high.
- c) Set the TCP idle time to 30 Minutes.

```
R4(config)#ip inspect max-incomplete high 1000
R4(config)#ip inspect max-incomplete low 801
R4(config)#ip inspect one-minute high 1000
R4(config)#ip inspect one-minute low 801

R4(config)#ip inspect tcp idle-time 1800
```


8.3 - Cisco IOS Firewall on R4 (2 points)

- a) Set the global UDP idle timeout to 110 seconds.

```
R4(config)#ip inspect udp idle-time 110
```

- b) Changes the max-incomplete host number to 32 half-open sessions, and changes the block-time timeout to 1 minute.

```
R4(config)#ip inspect tcp max-incomplete host 32 block 1
```

- c) Turn on an audit trail messages which will be displayed on the console after each CBAC session closes.

```
R4(config)#ip inspect audit-trail
```

- d) Globally specify the TCP session will still be managed after the firewall detects a FIN-exchange to be 15 seconds for all TCP sessions.

```
R4(config)#ip inspect tcp finwait-time 15
```

➔ **Double check your settings with show ip inspect all**

```
R4#show ip inspect all
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [801:1000] connections
max-incomplete sessions thresholds are [801:1000]
max-incomplete tcp connections per host is 32. Block-time 1 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 15 sec
tcp idle-time is 1800 sec -- udp idle-time is 110 sec
dns-timeout is 5 sec
Inspection Rule Configuration
  Inspection name MYFW
    tcp alert is on audit-trail is on timeout 1800
    udp alert is on audit-trail is on timeout 110
    icmp alert is on audit-trail is on timeout 10

Interface Configuration
Interface Serial0/0/0
  Inbound inspection rule is not set
  Outgoing inspection rule is MYFW
    tcp alert is on audit-trail is on timeout 1800
    udp alert is on audit-trail is on timeout 110
    icmp alert is on audit-trail is on timeout 10
  Inbound access list is 121
  Outgoing access list is not set

R4#
```


9 - Advanced Security and Attacks Configuration (12 Points)

9.1 - Filtering Java and ActiveX applets (2 Points)

- a) Setup the PIX to block the downloading of Java and ActiveX applets from anywhere.

```
pixfirewall(config)#filter java 80 0 0 0 0
pixfirewall(config)#filter activex 80 0 0 0 0
```

9.2 - Allow Remote Management of the PIX (2 Points)

- a) Setup the PIX firewall so that the PC at 10.1.1.100 can telnet into the PIX for remote management. Change the default Telnet password to ccie.

```
pixfirewall(config)#telnet 10.1.1.100 255.255.255.255 inside
pixfirewall(config)#passwd ccie
```

→ Verify by telnetting from the ACS server.

9.3 - Time-Based Access List (2 Points)

- a) You do not want users on R6 Ethernet Network access a special application that uses TCP port 25000, during the Weekdays between 9:00 AM to 4:00 PM.
- b) It is OK for them to use the application at other times.

```
R6(config)#time-range WEEKDAYS
R6(config-time-range)#periodic weekdays 09:00 to 15:59

R6(config)#access-list 131 deny tcp 192.1.6.0 0.0.0.255 any eq 25000
time-range WEEKDAYS
R6(config)#access-list 131 permit ip any any

R6(config)#int fa0/0
R6(config-if)#ip access-group 131 in
```

9.4 - Time-Based Access List (2 Points)

- a) You do not want users on R6 Ethernet Network to use a customized application that uses UDP port 20000, on the Weekend between 10:00 AM to 3:00 PM.
- b) It is OK for them to use the application at other times.

→ Since this is on the same interface, make sure to merge this into the existing access-list.

```
R6(config)#time-range WEEKEND
R6(config-time-range)#periodic weekend 10:00 to 14:59
R6(config)#ip access-list extended 131
R6(config-ext-nacl)#no permit ip any any
```



```

R6(config-ext-nacl)#deny udp 192.1.6.0 0.0.0.255 any eq 20000 time-
range WEEKEND
R6(config-ext-nacl)#permit ip any any

R6#show access-list 131
Extended IP access list 131
  10 deny tcp 192.1.6.0 0.0.0.255 any eq 25000 time-range WEEKDAYS
(inactive)
  20 deny udp 192.1.6.0 0.0.0.255 any eq 20000 time-range WEEKEND
(inactive)
  30 permit ip any any
R6#show time-range
time-range entry: WEEKDAYS (inactive)
  periodic weekdays 9:00 to 15:59
  used in: IP ACL entry
time-range entry: WEEKEND (inactive)
  periodic weekend 10:00 to 14:59
  used in: IP ACL entry
R6#

```

9.5 - Disable Unnecessary Services (2 Points)

- Disable the DHCP Service on R6.
- Verify that it is disabled by typing Show ip socket.

```

R6#show ip socket

```

Proto	Remote	Port	Local	Port	In	Out	Stat	TTY	OutputIF
17	0.0.0.0	0	6.6.6.6	5060	0	0	211	0	
17	--listen--		6.6.6.6	68	0	0	1	0	
17	--listen--		6.6.6.6	2887	0	0	11	0	
17	0.0.0.0	0	6.6.6.6	67	0	0	2211	0	
17	0.0.0.0	0	6.6.6.6	2517	0	0	11	0	
88	--listen--		6.6.6.6	26	0	0	0	0	
17	192.1.12.65	514	6.6.6.6	56286	0	0	211	0	
17	--listen--		6.6.6.6	123	0	0	1	0	

```

R6#

```

```

R6(config)#no service dhcp

```

```

R6#show ip socket

```

Proto	Remote	Port	Local	Port	In	Out	Stat	TTY	OutputIF
17	0.0.0.0	0	6.6.6.6	5060	0	0	211	0	
17	--listen--		6.6.6.6	68	0	0	1	0	
17	--listen--		6.6.6.6	2887	0	0	11	0	
17	0.0.0.0	0	6.6.6.6	2517	0	0	11	0	
88	--listen--		6.6.6.6	26	0	0	0	0	
17	192.1.12.65	514	6.6.6.6	56286	0	0	211	0	
17	--listen--		6.6.6.6	123	0	0	1	0	

```

R6#

```


9.6 - Spoofing (2 Points)

- a) Remove problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address in R2's F1/0. Only packets with a source address of 10.5.5.100 arriving at interface FastEthernet0/0 are verified and dropped if needed.

```
R2(config)#access-list 96 deny 10.5.5.100
```

```
R2(config-if)#ip verify unicast reverse-path 96
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

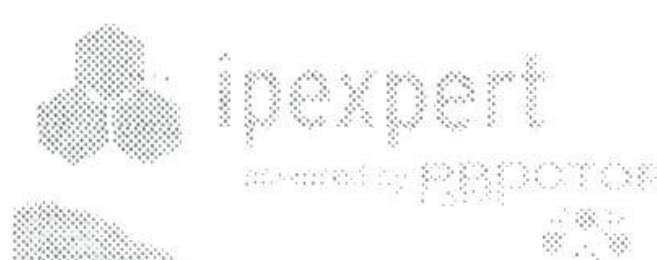
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 13: Multiprotocol Challenge B (One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 13 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the “Initial Configurations” subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs → Section 13 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the “MY CONFIGS” area of your www.IPexpert.com Member’s Area.

1 – Layer 2 Configuration (3 Points)

1.1 – Switch Management (3 Points)

- a) Create a Management interface on the Switch1 belonging to VLAN 6.
- b) Set the IP Address as .20 on that network.

```
Sw1(config)#int vlan 6
Sw1(config-if)#ip address 192.1.6.20 255.255.255.0
```

- c) Allow Management access to this switch from VLAN 6 only.

```
Sw1(config)#access-list 23 permit 192.1.6.0 0.0.0.255
Sw1(config)#line vty 0 15
Sw1(config-line)#access-class 23 in
```

- d) Reserve the 15 Telnet Line for the administrator using Port number 3005.

→ **Configuring the VTY interface as a rotary line allows specification of a particular port, starting at 3001. Rotary 5 would be port 3005.**

```
Sw1(config)#line vty 15
Sw1(config-line)#rotary 5
```

- e) You want to make sure that only the PIX inside interface can connect to port F 0/3 on Switch 2. Configure the Switch to send a trap if more than 3 MAC addresses are connected.

→ **Check the firewall first, to see what the MAC address is for that interface. Setting the port to restrict mode, will send a trap, but will not shut the port down.**

```
pixfirewall#show int eth1
Interface Ethernet1 "", is administratively down, line protocol is up
  Hardware is i82559, BW 100 Mbps
    Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
    Available but not configured via nameif
    MAC address 0019.2f6b.4526, MTU not set
```

```
Sw2(config)#int fa0/3
Sw2(config-if)#switchport port-security mac-address 0019.2f6b.4526

Sw2(config-if)#switchport port-security violation restrict
```


2 – Basic PIX Firewall Configuration (16 Points)

2.1 – ASA IP Address (4 Points)

- a) Create a Logical Interface off of E0 interface on the ASA1.
- b) The subinterface E0/0.55 should belong to VLAN 55.
- c) The physical interface belongs to the outside VLAN. Assign the subinterface 0/0.55 a name of DMZ55 using and a security level of 55.

```
ASA1(config)#int eth0/0.55
ASA1(config-subif)#vlan 55
ASA1(config-subif)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ASA1(config-subif)#security 55
ASA1(config-subif)#ip address 192.168.5.55 255.255.255.0
```

- d) Configure switch1 as needed to allow ASA1 to communicate to the rest of the network.

→ **Make sure that the port connected to ASA1 is configured as a trunk. Also make sure that VLANs 55 and 12 are active on the switches.**

- e) Assign IP Addresses to ASA1's Interfaces.

```
ASA1(config)#int eth0/0
ASA1(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA1(config-if)#ip address 192.1.12.10 255.255.255.0
ASA1(config-if)#no shut
ASA1(config-if)#int eth0/1
ASA1(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA1(config-if)#ip address 10.2.2.10 255.255.255.0
ASA1(config-if)#no shut
```

- f) Enable NAT-control on ASA1.

```
ASA1(config)#nat-control
```

2.2 – Routing (2 Points)

- a) Run RIP as the routing protocol on ASA1.
- b) Configure RIP such that it receives routes from the inside interface and also injects a default route from the inside interface.

```
ASA1(config)#router rip
ASA1(config-router)#version 2
ASA1(config-router)#no auto-summary
```



```
ASA1(config-router)#network 10.0.0.0
ASA1(config-router)#default
ASA1(config-router)#default-information originate
```

- c) ASA1 should be able to reach the rest of the network on the outside interface.
- d) You are allowed a single route command to accomplish this task.

```
ASA1(config)#route outside 0 0 192.1.12.2
```

2.3 – Static Translation (4 Points)

- a) Create a static mapping to R1. Create a Static Mapping to 192.1.12.15. Allow Web Access to R1 from R6 Loopback 0 address.

```
ASA1(config)#static (inside,outside) 192.1.12.15 10.2.2.1 netmask
255.255.255.255
ASA1(config)#access-list outsideacl permit tcp host 6.6.6.6 host
192.1.12.15 eq www
ASA1(config)#access-group outsideacl in interface outside
```

- b) Allow R1 Loopback 0 to ping R2 using its own IP Address. You are allowed a static route on R2.

→ Without address translation, R2 will need a route to R1's loopback.

```
ASA1(config)#access-list nonat permit ip host 1.1.1.1 host 192.1.12.2
ASA1(config)#nat (inside) 0 access-list nonat
ASA1(config)#access-list outsideacl permit icmp host 192.1.12.2 host
1.1.1.1 echo-reply
```

```
R2(config)#ip route 1.1.1.1 255.255.255.255 192.1.12.10
```

- c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

```
ASA1(config)#static (inside,outside) 192.1.12.100 10.1.1.100 netmask
255.255.255.255
ASA1(config)#access-list outsideacl permit tcp host 4.4.4.4 host
192.1.12.100 eq tacacs
ASA1(config)#access-list outsideacl permit tcp host 192.1.12.2 host
192.1.12.100 eq tacacs
```

2.4 – Advanced Protocol Handling on the PIX (2 Points)

- a) There is a FTP Server at a Partner Network that uses 2020 for the Data port and 2021 for the command port. The inside users should be able to connect to this server using Standard FTP.

b) You are allowed one command to accomplish this.

- Although there are technically multiple commands added to the config, this can be configured just by adding the command to watch FTP traffic on port 2021, using the legacy command `fixup protocol ftp 2021`

```
ASA1(config)#fixup prot ftp 2021
```

- The ASA will convert this to the modular framework, and the additions to the config will include the following:

```
class-map class ftp
match port tcp eq 2021
policy-map global_policy
class class ftp
inspect ftp
```

2.5 – Failover (2 points)

a) Configure ASA2 as a standby for ASA1. Use the eth0/2 interfaces for failover. Make sure that subinterface 0/0.55 is shown as a monitored interface in the output of `show failover`.

```
ASA1(config)#failover lan unit primary
ASA1(config)#failover lan interface MYFAILOVER eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its
sub-interfaces
ASA1(config)#failover key MYKEY
ASA1(config)#failover interface ip MYFAILOVER 55.55.55.1
255.255.255.0 standby 55.55.55.2
ASA1(config)#failover
ASA1(config)#monitor-interface DMZ
ciscoasa(config)#failover lan unit secondary
ciscoasa(config)#failover lan interface MYFAILOVER eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its
sub-interfaces
ciscoasa(config)#failover key MYKEY
ciscoasa(config)#failover interface ip MYFAILOVER 55.55.55.1
255.255.255.0 standby 55.55.55.2
ciscoasa(config)#failover
ciscoasa(config)#int eth0/2
ciscoasa(config-if)#no shut
```

- In order for the failover to show “normal” status, rather than “Waiting”, configure standby addresses for the interfaces.

```
ASA1(config)#int eth0/0
ASA1(config-if)#ip address 192.1.12.10 255.255.255.0 standby
192.1.12.11
ASA1(config-if)#int eth0/0.55
ASA1(config-subif)#ip address 192.168.5.55 255.255.255.0 standby
192.168.5.56
ASA1(config-subif)#int eth0/1
ASA1(config-if)#ip address 10.2.2.10 255.255.255.0 standby 10.2.2.11
```


→ **Verify with show failover:**

```
ASA1#show failover
Failover On
Failover unit Primary
Failover LAN Interface: MYFAILOVER Ethernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Last Failover at: 21:33:31 UTC Feb 3 2007
  This host: Primary - Active
    Active time: 580 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
      Interface DMZ (192.168.5.55): Normal
      Interface outside (192.1.12.10): Normal
      Interface inside (10.2.2.10): Normal
    slot 1: empty
  Other host: Secondary - Standby Ready
    Active time: 85 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
      Interface DMZ (192.168.5.56): Normal
      Interface outside (192.1.12.11): Normal
      Interface inside (10.2.2.11): Normal
    slot 1: empty

Stateful Failover Logical Update Statistics
Link : Unconfigured.

ASA1#
```

2.6 – Transparent Firewall (2 points)

- a) Configure the PIX as a transparent firewall between VLANs 50 and 51. After the IPS section has been completed, verify that the routing adjacencies between R5 and BB2 are established.

→ **Start by making the PIX firewall to transparent, and enable the interfaces. Revisit after finishing the IDS section.**

```
PIX(config)#firewall transparent

pixfirewall(config)#hostname PIX
PIX(config)#int eth0
PIX(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
PIX(config)#int eth1
PIX(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
PIX(config-if)#no shut

PIX(config)#ip address 10.5.5.55 255.255.255.0

PIX(config)#access-list ALLOW permit ip any any
PIX(config)#access-group ALLOW in interface inside
PIX(config)#access-group ALLOW in interface outside
```


3 – Routing Using Interior Gateway Protocols Configuration (4 Points)

3.1 – Routing protocol authentication (4 Points)

- a) R1 and BB1 should authenticate to each other using the highest level of authentication with a password of ccie.

→ If you look at the output of debug ip rip events, you can see that the update from the backbone is being ignored. After configuring the key chain, and applying to the interface, the update is accepted.

```
*Jan 4 15:07:14.812: RIP: ignored v2 packet from 10.1.1.200 (invalid authentication)
R1#
```

```
R1(config)#key chain 1
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string ccie
```

```
R1(config-if)#ip rip authentication key-chain 1
R1(config-if)#ip rip authentication mode md5
```

```
*Jan 4 15:08:41.084: RIP: received v2 update from 10.1.1.200 on FastEthernet0/1
*Jan 4 15:08:41.084: RIP: Update contains 4 routes
```

- b) All OSPF routers should exchange packets based on the most secure Authentication method. Use a password of ccie. You cannot use Area x authentication message-digest command to complete this task.

```
R2(config)#int ser0/1/0.4
R2(config-subif)#ip ospf message-digest-key 1 md5 ccie
R2(config-subif)#ip ospf authentication message-digest
R2(config-subif)#int ser0/1/0.5
R2(config-subif)#ip ospf message-digest-key 1 md5 ccie
R2(config-subif)#ip ospf authentication message-digest
R2(config-subif)#int ser0/1/0.6
R2(config-subif)#ip ospf message-digest-key 1 md5 ccie
R2(config-subif)#ip ospf authentication message-digest
```

```
R4(config)#int fa0/0
R4(config-if)#ip ospf message-digest-key 1 md5 ccie
R4(config-if)#ip ospf authentication message-digest
R4(config-if)#int ser0/0/0
R4(config-if)#ip ospf message-digest-key 1 md5 ccie
R4(config-if)#ip ospf authentication message-digest
```

```
R5(config)#int ser0/1/0
R5(config-if)#ip ospf message-digest-key 1 md5 cisco
R5(config-if)#ip ospf authentication message-digest
```

```
R9(config)#int fa0/0
R9(config-if)#ip ospf message-digest-key 1 md5 ccie
R9(config-if)#ip ospf authentication message-digest
```



```
R6(config)#int ser0/1/0
R6(config-if)#ip ospf message-digest-key 1 md5 ccie
R6(config-if)#ip ospf authentication mess
```

```
R2#show ip ospf interface | i protocol|authentication|key
Serial0/1/0.6 is up, line protocol is up
  Message digest authentication enabled
    Youngest key id is 1
Serial0/1/0.5 is up, line protocol is up
  Message digest authentication enabled
    Youngest key id is 1
Serial0/1/0.4 is up, line protocol is up
  Message digest authentication enabled
    Youngest key id is 1
Loopback0 is up, line protocol is up
R2#show ip ospf neigh
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
6.6.6.6	0	FULL/ -	00:00:31	192.1.26.6	Serial0/1/0.6
5.5.5.5	0	FULL/ -	00:00:35	192.1.25.5	Serial0/1/0.5
4.4.4.4	0	FULL/ -	00:00:38	192.1.24.4	Serial0/1/0.4

R2#

- c) All routers in EIGRP should authentication with each other using a password of ccie with a key id of 1.

```
R5(config)#key chain 1
R5(config-keychain)#key 1
R5(config-keychain-key)#key-string ccie
R5(config-keychain-key)#int fa0/0

R5(config-if)#ip authentication mode eigrp 100 md5
R5(config-if)#ip authentication key-chain eigrp 100 1
```

- d) Authenticate all IBGP Peerings using MD5 authentication with a password of ccie.

```
R5(config)#router bgp 245
R5(config-router)#neighbor 2.2.2.2 password ccie

R4(config)#router bgp 245
R4(config-router)#neighbor 2.2.2.2 password ccie

R2(config)#router bgp 245
R2(config-router)#neighbor 4.4.4.4 password ccie
R2(config-router)#neighbor 5.5.5.5 password ccie
```


4 – Access Management Configuration (7 Points)

4.1 – Configuring AAA Authentication on R4 for Telnet (4 Points)

- a) Configure R4 with AAA access. TACACS+ server sees R4 with its Loopback 0 address. The secret key is ccie.

```
R4(config)#aaa new-model  
  
R4(config)#aaa new-model  
R4(config)#aaa authentication login default none  
R4(config)#aaa authentication login TAC group tacacs  
  
R4(config)#tacacs-server host 192.1.12.100 key ccie  
R4(config)#ip tacacs source-int loop0
```

- b) No Authentication should be done on the Console or AUX lines.

→ This is handled by setting the default method list to none.

- c) Setup Authentication based on TACACS+ for the VTY lines.

```
R4(config)#line vty 0 15  
R4(config-line)#login authentic TAC
```

- d) Create 2 users on the AAA server, User1 and User2. Both the users should have cisco as their password. Configure the AAA server for R4 as a network device.

→ Add the two users on the AAA server, also add R4 as a Network AAA client, using the key ccie and the loopback address of R4.

- e) Verify that authentication does not affect the console, and verify that the ACS logs show successful authentication when connecting to R4 via telnet.

→ Check the logs on the ACS server for failed attempts. You can also check the authentication from R4 with the test aaa command.

```
R4#test aaa group tacacs User1 ccie legacy  
Attempting authentication test to server-group tacacs+ using tacacs+  
User was successfully authenticated.
```

4.2 – Configuring AAA Authorization on R4 for Telnet (3 Points)

- a) Setup Authorization based on Local Privilege Levels defined as follows:

```
R4(config)#username User1 priv 15 password ccie  
R4(config)#username User2 priv 5 password ccie
```


- b) Setup authorization for User1 such that the user can type all commands. User1 should be in Privilege Exec mode when logged in.

```
R4(config)#aaa authorization exec VTY local
R4(config)#line vty 0 15
R4(config-line)#authorization exec VTY
```

- c) Setup authorization for User2 such that the user can type all commands specified in Privilege Level 5. Privilege Level 5 should allow the user to type the following commands:

- Configure or change IP Addresses for the Interfaces.
- Configure a Routing Protocol. Allow the user to advertise and redistribute networks.
- Set the Clock and configure the time zone for the router.

```
R4(config)#privilege router level 5 redistribute
R4(config)#privilege router level 5 network
R4(config)#privilege interface level 5 ip address
R4(config)#privilege interface level 5 ip
R4(config)#privilege configure all level 5 router
R4(config)#privilege configure level 5 interface
R4(config)#privilege configure level 5 clock timezone
R4(config)#privilege configure level 5 clock
R4(config)#privilege exec level 5 clock set
R4(config)#privilege exec level 5 clock
R4(config)#privilege exec level 5 configure terminal
R4(config)#privilege exec level 5 configure
```

- d) Configure Accounting for all commands typed by users from Telnet. You should be able to charge the users based on usage times.

```
R4(config)#aaa accounting commands 0 VTYACCT start-stop group tacacs+
R4(config)#aaa accounting commands 1 VTYACCT start-stop group tacacs+
R4(config)#aaa accounting commands 5 VTYACCT start-stop group tacacs+
R4(config)#aaa accounting commands 15 VTYACCT start-stop group tacacs+
```

```
R4(config)#line vty 0 15
R4(config-line)#accounting commands 0 VTYACCT
R4(config-line)#accounting commands 1 VTYACCT
R4(config-line)#accounting commands 5 VTYACCT
R4(config-line)#accounting commands 15 VTYACCT
```

```
R4(config)#aaa accounting exec VTYACCT start-stop group tacacs
R4(config)#line vty 0 15
R4(config-line)#accounting exec VTYACCT
```

- e) Verify the logging on the ACS server.

- **Logging for the session start-stops will appear under TACACS Accounting. Logging for the commands will appear under TACACS Administration.**

Address: http://127.0.0.1:4891/

Cisco Systems Reports and Activity

Select

Reports

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in Users
- Disabled Accounts
- ACS Backup And Restore
- Administration Audit
- User Password Changes
- ACS Service Monitoring

[Back to Help](#)

Select

Tacacs+ Administration active.csv [Refresh](#) [Download](#)

Regular Expression: Start Date & Time: End Date & Time: Rows per Page:

[Apply Filter](#) [Clear Filter](#)

Filtering is not applied.

[Next](#)

Date	Time	User-Name	Group-Name	cmd	priv-lev	service	NAS Port
02/04/2007	12:19:04	User2	Default Group	exit <cr>	0	shell	tty324
02/04/2007	12:18:42	User2	Default Group	configure terminal <cr>	5	shell	tty324
02/04/2007	12:18:26	User1	Default Group	telnet 4.4.4.4	15	shell	tty323
02/04/2007	12:18:26	User1	Default Group	telnet 4.4.4.4 <cr>	1	shell	tty323
02/04/2007	12:18:22	User1	Default Group	telnet 4.4.4.4	15	shell	tty323
02/04/2007	12:18:22	User1	Default Group	exit <cr>	0	shell	tty324
02/04/2007	12:18:12	User1	Default Group	ping 4.4.4.4 <cr>	15	shell	tty324
02/04/2007	12:18:09	User1	Default Group	telnet 4.4.4.4 <cr>	15	shell	tty324
02/04/2007	12:17:48	User1	Default Group	ping 4.4.4.4 <cr>	15	shell	tty324
02/04/2007	12:17:11	User1	Default Group	telnet 4.4.4.4 <cr>	1	shell	tty323
02/04/2007	12:17:11	User1	Default Group	telnet 4.4.4.4	15	shell	tty323
02/04/2007	12:17:08	User1	Default Group	exit <cr>	0	shell	tty323
02/04/2007	12:17:06	User1	Default Group	exit <cr>	0	shell	tty323

5 – IP Services Configuration (6 points)

5.1 – Configuring NTP between R5 and R2 (3 Points)

- a) Configure the timezone on R5 as PST -8. Set the clock to the current time on R5.

```
R5(config)#clock timezone PST -8
R5#clock set 01:00:00 1 Jan 2007
```

- b) Set R5 as the NTP Master with a stratum of 2. NTP should require MD5 authentication with a key 1.

```
R5(config)#ntp master 2
R5(config)#ntp authentication-key 1 md5 ipexpert
```

- c) Configure the timezone on R2 as PST -8. Configure R2 as the client for R5. R2 should point to R5 using the NTP Server command.

```
R2(config)#clock timezone PST -8
R2(config)#ntp authentication-key 1 md5 ipexpert
R2(config)#ntp server 192.1.25.5 key 1
R2(config)#ntp authenticate
```

→ Verify the output of show ntp association detail shows AUTHENTICATED

```
R2#show ntp assoc det
192.1.25.5 configured, authenticated, our_master, sane, valid, stratum 2
```


- d) R5 should only allow R2 to get the clock from it.

```
R5(config)#access-list 2 permit 192.1.25.2
R5(config)#ntp access-group serve-only 2
```

- **Configure R4 with “ntp server 192.1.25.5” and then look at the output of DEBUG NTP PACKET. Packets are received and transmitted to R2, but only received from R4.**

```
.Jan  1 09:15:58.651: NTP: rcv packet from 192.1.25.2 to 192.1.25.5 on
Serial0/1/0:
.Jan  1 09:15:58.651: leap 0, mode 3, version 3, stratum 3, ppoll 64

.Jan  1 09:15:58.651: NTP: stateless xmit packet to 192.1.25.2:
.Jan  1 09:15:58.651: leap 3, mode 4, version 3, stratum 0, ppoll 64
R5#
.Jan  1 09:16:10.895: NTP: rcv packet from 192.1.24.4 to 192.1.25.5 on
Serial0/1/0:
.Jan  1 09:16:10.895: leap 3, mode 3, version 3, stratum 0, ppoll 64
```

5.2 – NAT (3 Points)

- a) Configure a loopback 15 interface on R6. Assign it an IP Address of 192.168.15.1/24.

```
R6(config)#int loop15
R6(config-if)#ip address 192.168.15.1 255.255.255.0
```

- b) Configure NAT such that if loopback 15 network wants to go to 9.0.0.0 or 4.0.0.0 networks, it should use the interface IP address of the Serial0/1/0 interface as the translated address. Configure PAT for this entry.

- **Since the only egress point for those networks is via R2, only the Ser0/1/0 network needs to be configured as an outside NAT interface. The overload keyword will PAT the entries.**

```
R6(config)#access-list 162 permit ip host 192.168.15.1 9.0.0.0
0.255.255.255
R6(config)#access-list 162 permit ip host 192.168.15.1 4.0.0.0
0.255.255.255
R6(config)#int loop15
R6(config-if)#ip nat inside
R6(config-if)#int ser0/1/0
R6(config-if)#ip nat outside

R6(config)#ip nat inside source list 162 interface ser0/1/0 overload
```

- c) Configure NAT such that if loopback 15 network wants to go to 2.0.0.0 or 5.0.0.0 networks, it should use 192.1.26.15 as the translated address. Configure PAT for this entry.

```
R6(config)#access-list 163 permit ip host 192.168.15.1 2.0.0.0
0.255.255.255
R6(config)#access-list 163 permit ip host 192.168.15.1 5.0.0.0
0.255.255.255
```



```
R6(config)#ip nat pool NAT 192.1.26.15 192.1.26.15 prefix 24
R6(config)#ip nat inside source list 163 pool NAT overload
```

- To verify, turn on DEBUG IP ICMP and DEBUG IP NAT, and look at the output when you ping with a source of the loopback address.

```
R6#ping 5.5.5.5 source loop15
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 5.5.5.5, timeout is 2 seconds:

Packet sent with a source address of 192.168.15.1

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms

```
R6#
```

```
*Feb 4 19:16:56.775: NAT: s=192.168.15.1->192.1.26.15, d=5.5.5.5 [600]
*Feb 4 19:16:56.811: NAT*: s=5.5.5.5, d=192.1.26.15->192.168.15.1 [600]
*Feb 4 19:16:56.811: ICMP: echo reply rcvd, src 5.5.5.5, dst 192.168.15.1
*Feb 4 19:16:56.811: NAT: s=192.168.15.1->192.1.26.15, d=5.5.5.5 [601]
*Feb 4 19:16:56.847: NAT*: s=5.5.5.5, d=192.1.26.15->192.168.15.1 [601]
*Feb 4 19:16:56.847: ICMP: echo reply rcvd, src 5.5.5.5, dst 192.168.15.1
*Feb 4 19:16:56.847: NAT: s=192.168.15.1->192.1.26.15, d=5.5.5.5 [602]
*Feb 4 19:16:56.883: NAT*: s=5.5.5.5, d=192.1.26.15->192.168.15.1 [602]
*Feb 4 19:16:56.883: ICMP: echo reply rcvd, src 5.5.5.5, dst 192.168.15.1
```

```
R6#
```

```
*Feb 4 19:16:56.887: NAT: s=192.168.15.1->192.1.26.15, d=5.5.5.5 [603]
*Feb 4 19:16:56.919: NAT*: s=5.5.5.5, d=192.1.26.15->192.168.15.1 [603]
*Feb 4 19:16:56.923: ICMP: echo reply rcvd, src 5.5.5.5, dst 192.168.15.1
*Feb 4 19:16:56.923: NAT: s=192.168.15.1->192.1.26.15, d=5.5.5.5 [604]
*Feb 4 19:16:56.959: NAT*: s=5.5.5.5, d=192.1.26.15->192.168.15.1 [604]
*Feb 4 19:16:56.959: ICMP: echo reply rcvd, src 5.5.5.5, dst 192.168.15.1
```

```
R6#ping 4.4.4.4 source loop15
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

Packet sent with a source address of 192.168.15.1

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms

```
R6#
```

```
*Feb 4 19:17:11.359: NAT: s=192.168.15.1->192.1.26.6, d=4.4.4.4 [605]
*Feb 4 19:17:11.379: NAT*: s=4.4.4.4, d=192.1.26.6->192.168.15.1 [605]
*Feb 4 19:17:11.379: ICMP: echo reply rcvd, src 4.4.4.4, dst 192.168.15.1
*Feb 4 19:17:11.383: NAT: s=192.168.15.1->192.1.26.6, d=4.4.4.4 [606]
*Feb 4 19:17:11.403: NAT*: s=4.4.4.4, d=192.1.26.6->192.168.15.1 [606]
*Feb 4 19:17:11.403: ICMP: echo reply rcvd, src 4.4.4.4, dst 192.168.15.1
*Feb 4 19:17:11.403: NAT: s=192.168.15.1->192.1.26.6, d=4.4.4.4 [607]
*Feb 4 19:17:11.423: NAT*: s=4.4.4.4, d=192.1.26.6->192.168.15.1 [607]
*Feb 4 19:17:11.423: ICMP: echo reply rcvd, src 4.4.4.4, dst 192.168.15.1
```

```
R6#
```

```
*Feb 4 19:17:11.423: NAT: s=192.168.15.1->192.1.26.6, d=4.4.4.4 [608]
*Feb 4 19:17:11.443: NAT*: s=4.4.4.4, d=192.1.26.6->192.168.15.1 [608]
*Feb 4 19:17:11.447: ICMP: echo reply rcvd, src 4.4.4.4, dst 192.168.15.1
*Feb 4 19:17:11.447: NAT: s=192.168.15.1->192.1.26.6, d=4.4.4.4 [609]
*Feb 4 19:17:11.467: NAT*: s=4.4.4.4, d=192.1.26.6->192.168.15.1 [609]
*Feb 4 19:17:11.467: ICMP: echo reply rcvd, src 4.4.4.4, dst 192.168.15.1
```


6 –Virtual Private Networks Configuration (16 Points)

6.1 – Basic Concentrator Configuration (2 Points)

- a) Configure the IP Address of the Private Interface thru the CLI.

→ **When you get to the IP portion of setup, configure the address and subnet mask for the private interface.**

> Enter IP Address

Quick Ethernet 1 -> [0.0.0.0] **10.2.2.5**

Waiting for Network Initialization...

> Enter Subnet Mask

Quick Ethernet 1 -> [255.0.0.0] **255.255.255.0**

> Enter Interface Name

Quick Ethernet 1 ->

- b) The Public interface should be configured from the Graphical interface.

Configuration – interfaces – Public – configure the IP address and subnet mask

- c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

→ **Since inbound RIP is enabled on the private interface by default, you should be able to connect to the concentrator from the PC. Since RIP will be disabled in the next step, make sure that you had a static route configured.**

Configuration – System – IP Routing – Static Routes – add a route to 10.1.1.0/24 via 10.2.2.1

6.2 – Routing Protocols on the Concentrator (2 Points)

- a) Disable RIP on the private interface.

Configuration – Interfaces – Private – RIP tab.

- b) Configure the Concentrator to run RIP V2 on the Public Interface.

Configuration – Interfaces – Public – RIP tab – enable RIP

- c) Configure the ASA to send a default route to the Concentrator on the DMZ55 interface using RIP V2.

```
ASA1(config)#router rip
ASA1(config-router)#network 192.168.5.0
```

- On the concentrator, you also need to adjust the interface filter.

Configuration – Policy Management – Traffic Management – Filters – Assign Rules to Filter.

- Verify that the default route shows up in your routing table on the concentrator.

Monitoring – Routing Table

6.3 – Setup a Site-to-Site IPsec VPN between the Concentrator and R5 (4 Points)

- a) The concentrator should be seen as 192.1.12.5 on the outside network. Configure the ASA to accomplish this.

```
ASA1(config)#static (DMZ,outside) 192.1.12.5 192.168.5.5 netmask
255.255.255.255
```

- b) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- For IPsec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.
- Start with the configuration on R5.

```
R5(config)#crypto isakmp key ccie address 192.1.12.5
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#hash md5
R5(config-isakmp)#authent pre-share
```

```
R5(config)#crypto ipsec transform-set VPNC esp-des esp-sha-hmac
R5(cfg-crypto-trans)#mode tunnel
```

```
R5(config)#access-list 173 permit ip 10.5.5.0 0.0.0.255 10.2.2.0
0.0.0.255
```

```
R5(config)#crypto map R5MAP 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

```
R5(config-crypto-map)#match address 173
R5(config-crypto-map)#set peer 192.1.12.5
R5(config-crypto-map)#set transform VPNC
R5(config-crypto-map)#int ser0/1/0
R5(config-if)#crypto map R5MAP
```

- On the VPN concentrator, add a new Lan to Lan tunnel under Configuration – Tunneling and Security – IPsec – LAN to LAN.

- Set the peer address to 192.1.25.5

Configure the preshared key, set authentication to ESP/SHA/HMAC, set encryption to DES, and set the IKE proposal to IKE-DES-MD5.

- Check the box for NAT-T.

- Set the local and remote networks.

- Globally enable IPsec over NAT-T under Tunnelling and Security – IPsec – NAT Transparency.

c) You can use static routes on R5 and R1 to accomplish this.

- R5 will need a static route to the 10.2.2.0 network. R1 will need a static route to the 10.5.5.0 network.

```
R5(config-if)#ip route 10.2.2.0 255.255.255.0 192.1.25.2
```

```
R1(config)#ip route 10.5.5.0 255.255.255.0 10.2.2.5
```

d) Create the appropriate entries in the PIX firewall to accomplish this.

```
ASA1(config)#access-list infilter permit udp host 192.1.25.5 eq 4500  
host 192.1.12.5 eq 4500
```

```
ASA1(config)#access-list infilter permit udp host 192.1.25.5 host  
192.1.12.5 eq 500
```

- Verify that you can ping R1 with a source of R5's Ethernet interface, and verify the output of your show crypto ipsec sa.

```
R5#ping 10.2.2.1 source 10.5.5.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.5.5.5

!!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms

R5#

```
R5#show crypto ipsec sa
```

```
interface: Serial0/1/0
```

```
  Crypto map tag: R5MAP, local addr 192.1.25.5
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/pctr): (10.5.5.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/pctr): (10.2.2.0/255.255.255.0/0/0)
```

```
current_peer 192.1.12.5 port 4500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
```

```
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```


6.4 – Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

a) Use the following parameters to setup Concentrator with the following options:

- Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote**.
- Set the username as VPNUser with a password of **ccie1234**.
- Create a group called Remote with a password of **ccie**.
- When the user connects in, he should also be allowed to connect to the 192.1.49.0/24 networks.
- **Add the group under User Management - Groups – Add Group.**
- **Add the address pool for the group, by selecting the group and “address pool”**
- **Add the user under Configuration – User Management – Users.**
- **Under system – address management – assignment, select use address pools.**
- **Under Configuration – User Management – Groups – Modify the remote access group. Select the client config tab. Under split tunneling policy, select “Only tunnel networks in the list”. Under Split Tunneling Network List, select VPN client local lan.**
- **On the PIX, make sure to allow the incoming connections for remote access.**

```
ASA1(config)#access-list outsideacl permit udp any host 192.1.12.5 eq 4500
```

```
ASA1(config)#access-list outsideacl permit udp any host 192.1.12.5 eq 500
```

```
ASA1(config)#route inside 10.3.3.0 255.255.255.0 10.2.2.5
```

```
R1(config)#ip route 10.3.3.0 255.255.255.0 10.2.2.5
```

- **Note: On the client PC, you may need to add a route to 192.1.49.0/24.**

```
route ADD 192.1.49.0 mask 255.255.255.0 192.1.12.2
```

- **Test your configuration from the Client PC.**

6.5 – Configure a Remote Access VPN using IOS Easy VPN (R2) and Cisco Secure VPN Client (4 Points)

a) Configure R2 as the Easy VPN Server using the following parameters:

- Group name and password : Name : **EZGroup** Password : **abcd1234**
- DNS and WINS Address : 192.1.12.175
- Domain Name : ipexpert.com
- Address Pool (Local) : 192.168.22.1 192.168.22.16

```
R2(config)#ip local pool dynpool 192.168.22.1 192.168.22.16
```

```
R2(config)#crypto isakmp client configuration group EZGroup
```

```
R2(config-isakmp-group)#key abcd1234
```

```
R2(config-isakmp-group)#dns 192.1.12.175
```



```
R2(config-isakmp-group)#wins 192.1.12.175
R2(config-isakmp-group)#domain ipexpert.com
R2(config-isakmp-group)#pool dynpool
```

- The Address should be assigned to the client from the pool above. This network should be propagated to all the other routers.

```
R2(config)#crypto isakmp client configuration address-pool local
dynpool
```

```
R2(config)#crypto ipsec transform-set transform-1 esp-des esp-md5-
hmac
```

```
R2(config)#crypto dynamic-map dynmap 10
R2(config-crypto-map)#set transform-set transform-1
R2(config-crypto-map)#reverse-route
```

- On the router Reverse Route Injection adds the networks locally as Statics, but does not propagate them to the rest of the topology until you redistribute the statics into a routing protocol.

```
R2(config)#access-list 75 permit 192.168.22.0 0.0.0.31
R2(config)#route-map RRI
R2(config-route-map)#match address 75
```

```
R2(config)#router ospf 1
R2(config-router)#redist static route-map RRI subnets
```

- Verify that the route shows up on another box.

```
R6#show ip route 192.168.22.1
Routing entry for 192.168.22.1/32
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward metric
  64
  Last update from 192.1.26.2 on Serial0/1/0, 00:01:06 ago
  Routing Descriptor Blocks:
    * 192.1.26.2, from 2.2.2.2, 00:01:06 ago, via Serial0/1/0
      Route metric is 20, traffic share count is 1
```

- The Authentication and Authorization should be done locally.

```
R2(config)#username VPNUser password ccie1234
```

```
R2(config)#aaa new-model
R2(config)#aaa authentication login USERS local
R2(config)#aaa authorization network EZGroup local
```

```
R2(config)#crypto map dynmap client authentication list USERS
R2(config)#crypto map dynmap isakmp authorization list EZGroup
```

```
R2(config)#crypto map dynmap 1 ipsec-isakmp dynamic dynmap
```


- Hashing for the ISAKMP Policy should be done based on MD5.
- Authentication for the ISAKMP Policy should be done based on Pre-shared keys.
- **Make sure that you set the policy to DH group 2, or the VPN client will not connect.**

```
R2 (config)#crypto isakmp policy 10
R2 (config-isakmp)#hash md5
R2 (config-isakmp)#group 2
R2 (config-isakmp)#authentication pre-share
```

- Set the authentication to XAUTH.

```
R2 (config)#crypto map dynmap client configuration address respond
```

- Use ESP-DES and ESP-MD5-HMAC for your transform set.
- **Verify by connecting from the VPN client. Since this section does not include split tunneling, you may lose your connection when the VPN connects. Clear the connection on R2 with the command CLEAR CRYPTO SA to be able to reconnect.**

7 - DMVPN, Easy VPN for R4 and R9's LAN Configuration (6 Points)

7.1 – Configure a DMVPN and Easy VPN (6 Points)

- a) Configure DMVPN and Easy VPN with XAUTH on R9. Configure R4 as a DMVPN spoke. Add a loopback 49 on R4 with the address 49.4.4.4/24. Add a loopback 49 on R9 with the address 49.9.9.9/24. These networks should be advertised via the new EIGRP process in step c.

```
R4 (config)#int loop49
R4 (config-if)#ip address 49.4.4.4 255.255.255.0

R9 (config)#int loop49
R9 (config-if)#ip address 49.9.9.9 255.255.255.0
```

- b) Create a tunnel with the network of 49.0.0.x/24 with x is the router number.

- **Start on R4 with the ISAKMP key and policy.**

```
R4 (config)#crypto isakmp key 0 ccie address 192.1.49.9
R4 (config)#crypto isakmp policy 10
R4 (config-isakmp)#hash md5
R4 (config-isakmp)#authentication pre-share
```

- **Configure the transform set and a crypto profile.**

```
R4 (config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac
R4 (config)#crypto ipsec profile cisco
R4 (ipsec-profile)#set security-association lifetime seconds 120
R4 (ipsec-profile)#set transform-set strong
```


→ **Configure the tunnel, and apply the profile.**

```
R4(config)#interface Tunnel0
R4(config-if)#ip address 49.0.0.4 255.255.255.0
R4(config-if)#no ip redirects
R4(config-if)#ip mtu 1440
R4(config-if)#ip nhrp authentication ccie
R4(config-if)#ip nhrp map multicast dynamic
R4(config-if)#ip nhrp map 49.0.0.9 192.1.49.9
R4(config-if)#ip nhrp map multicast 192.1.49.9
R4(config-if)#ip nhrp network-id 1
R4(config-if)#ip nhrp holdtime 300
R4(config-if)#ip nhrp nh 49.0.0.9
R4(config-if)#tunnel source FastEthernet0/0
R4(config-if)#tunnel mode gre multipoint
R4(config-if)#tunnel key 0
R4(config-if)#tunnel protection ipsec profile cisco
```

→ **On R9, the configuration will be slightly different, as we will be using ISAKMP profiles.**

```
R9(config)#crypto isakmp policy 10
R9(config-isakmp)#hash md5
R9(config-isakmp)#authentication pre-share

R9(config-isakmp)#crypto ipsec transform-set strong esp-3des esp-md5-
hmac

R9(config)#crypto keyring dmvpnspokes
R9(conf-keyring)#pre-shared-key address 192.1.49.4 key ccie

R9(conf-keyring)#crypto isakmp profile DMVPN
% A profile is deemed incomplete until it has match identity
statements
R9(conf-isa-prof)#keyring dmvpnspokes
R9(conf-isa-prof)#match identity address 0.0.0.0

R9(conf-isa-prof)#crypto ipsec profile cisco
R9(ipsec-profile)#set security-association lifetime seconds 120
R9(ipsec-profile)#set transform-set strong
R9(ipsec-profile)#set isakmp-profile DMVPN
R9(ipsec-profile)#
R9(ipsec-profile)#interface Tunnel0
R9(config-if)#ip address 49.0.0.9 255.255.255.0
R9(config-if)#no ip redirects
R9(config-if)#ip mtu 1440
R9(config-if)#ip nhrp authentication ccie
R9(config-if)#ip nhrp map multicast dynamic
R9(config-if)#ip nhrp network-id 1
R9(config-if)#ip nhrp holdtime 300
R9(config-if)#tunnel source FastEthernet0/0
R9(config-if)#tunnel mode gre multipoint
R9(config-if)#tunnel key 0
R9(config-if)#tunnel protection ipsec profile cisco
R9(config-if)#
```


- c) Running a separate EIGRP process for the tunnel interface.

```
R4(config)#router eigrp 49
R4(config-router)#network 49.0.0.0 0.0.0.255
R4(config-router)#network 49.4.4.0 0.0.0.255
R4(config-router)#no auto-summary
R9(config)#router eigrp 49
R9(config-router)#network 49.0.0.0 0.0.0.255
R9(config-router)#network 49.9.9.0 0.0.0.255
R9(config-router)#no auto-summary
```

→ At this point R4 and R9 should be able to ping the 49.4.4.4 and 49.9.9.9 loopbacks.

- d) Use XAUTH for local configuration, with username and password is ccie.

```
R9(config)#username ccie password 0 ccie
R9(config)#aaa new-model
R9(config)#
R9(config)#aaa authentication login remoteusers local
R9(config)#aaa authorization network remotegroup local
```

- e) The default pre-shared key should be ccie.

- f) Easy VPN Clients should use Diffie-Hellman group 2.

```
R9(config)#crypto isakmp policy 20
R9(config-isakmp)#hash md5
R9(config-isakmp)#authentication pre-share
R9(config-isakmp)#group 2
```

- g) The dynamic address pool should be 123.0.0.10 to 123.0.0.20.

```
R9(config)#ip local pool dynpool 123.0.0.10 123.0.0.20
```

- h) Client should respond to the address.

```
R9(config)#crypto isakmp profile VPNclient
% A profile is deemed incomplete until it has match identity
statements
R9(conf-isa-prof)#match identity group myvpngroup
R9(conf-isa-prof)#client authentication list remoteusers
R9(conf-isa-prof)#isakmp authorization list remotegroup
R9(conf-isa-prof)#client configuration address respond
```

- i) Create a VPN client group that uses DNS at 123.1.1.1 and WINS at 123.1.1.2.

```
R9(config)#crypto isakmp client configuration group myvpngroup
R9(config-isakmp-group)#key ipexpert
R9(config-isakmp-group)#dns 123.1.1.1
```



```
R9(config-isakmp-group)#wins 123.1.1.2
R9(config-isakmp-group)#domain cisco.com
R9(config-isakmp-group)#pool dynpool
```

- j) Phase 2 policy should be esp-3des esp-md5-hmac.

```
R9(config)#crypto ipsec transform-set strong esp-3des esp-md5-hmac
```

- k) NHRP authentication should use ccie.

- l) Reverse route injection should be used to provide the DMVPN networks access to any Easy VPN Client network.

```
R9(config)#crypto dynamic-map dynmap 10
R9(config-crypto-map)#set isakmp-profile VPNclient
R9(config-crypto-map)#set transform-set strong
R9(config-crypto-map)#reverse-route
```

```
R9(config)#router eigrp 49
R9(config-router)#redist static metric 1 1 1 1 1
```

- **Connect from the Test PC and verify that R4 can ping the address assigned to the VPN client.**

```
R9#show crypto ipsec sa
```

```
interface: FastEthernet0/0
  Crypto map tag: MYMAP, local addr 192.1.49.9

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (123.0.0.11/255.255.255.255/0/0)
  current_peer 192.1.6.33 port 500
    PERMIT, flags={}
    #pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18
    #pkts decaps: 27, #pkts decrypt: 27, #pkts verify: 27
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 192.1.49.9, remote crypto endpt.: 192.1.6.33
    path mtu 1500, ip mtu 1500
    current outbound spi: 0x2F682B9F(795356063)

  inbound esp sas:
    spi: 0x25B69924(632723748)
      transform: esp-3des esp-md5-hmac ,
```

```
R9#
R9#ping 123.0.0.11
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.0.0.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms
R9#
```



```
R4#ping 123.0.0.11 source 49.4.4.4
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 123.0.0.11, timeout is 2 seconds:
Packet sent with a source address of 49.4.4.4

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
R4#

8 – IOS Firewall Configuration (12 Points)

8.1 – Cisco IOS Firewall on R4 (4 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- All TCP Based traffic.
- All UDP Based traffic.
- Netmeeting Traffic.
- SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in.

```
R4(config)#ip inspect name MYFW tcp
R4(config)#ip inspect name MYFW udp
R4(config)#ip inspect name MYFW h323
R4(config)#ip inspect name MYFW smtp
```

```
R4(config-if)#int ser0/0/0
R4(config-if)#ip inspect MYFW out
```

b) Only allow Java applets from 2.0.0.0 to be downloaded.

```
R4(config)#access-list 80 permit 2.0.0.0
R4(config)#ip inspect name MYFW http java-list 80
```

c) Only allow relevant traffic coming in.

- **Whenever configuring IOS firewall, watch the access-list very carefully.**

```
R4(config)#access-list 121 permit ospf host 192.1.24.2 host 224.0.0.5
R4(config)#access-list 121 permit ospf host 192.1.24.2 host
192.1.24.4
R4(config)#access-list 121 permit tcp host 2.2.2.2 host 4.4.4.4 eq
bgp
R4(config)#access-list 121 permit esp any host 192.1.49.9
R4(config)#access-list 121 permit udp any host 192.1.49.9 eq 500
R4(config)#access-list 121 permit tcp any host 192.1.24.4 eq telnet
R4(config)#access-list 121 permit tcp host 192.1.12.100 eq 49 host
4.4.4.4
```

d) ACL should be set to inbound on the Serial interface.

```
R4(config)#int ser0/0/0
R4(config-if)#ip access-group 121 in
```


8.2 – Cisco IOS Firewall on R4 (4 Points)

- a) Set the IOS Firewall such that it blocks half-open connections if they exceed 800 and stop deleting the connections if they reach 600.
- b) Also set it for a one-minute high.

```
R4(config)#ip inspect max-incomplete high 800
R4(config)#ip inspect max-incomplete low 601
R4(config)#ip inspect one-minute high 800
R4(config)#ip inspect one-minute low 601
```

- c) Configure the Router such that it waits for 10 seconds for a connection to complete before tearing it down.

```
R4(config)#ip inspect tcp synwait-time 10
```

- d) Configure the dns-timeout to 30 seconds.
- e) Configure the udp idle timeout to 25 seconds.

```
R4(config)#ip inspect dns-timeout 30
R4(config)#ip inspect udp idle-time 25
```

8.3 - TCP Intercept (4 points)

- a) The 9.9.9.0 network is experiencing syn attacks. R9 should watch the traffic and if it does not complete the TCP handshake in 15 seconds, it should drop the packets.

```
R9(config)#access-list 193 permit tcp any 9.9.9.0 0.0.0.255
R9(config)#ip tcp intercept list 193
R9(config)#ip tcp intercept mode watch
R9(config)#ip tcp intercept watch-timeout 15
```

- b) Limit IP TCP intercept to only watch packets going to 9.9.9.0.
- c) Configure IP TCP intercept such that the router drops embryonic connections if they reach 1250. It should stop dropping the embryonic connections once the number reaches 800.

```
R9(config)#ip tcp int max-inc high 1250
R9(config)#ip tcp int max-inc low 800
```

- d) Set the software to manage the connection for 12 hours after no activity.

```
R9(config)#ip tcp int connection-timeout 43200
```

- e) Allows 1450 connection requests before the software enters aggressive mode.

```
R9(config)#ip tcp int one-minute high 1450
```


- f) Sets the software to leave aggressive mode when the number of connection requests falls below 1050.

```
R9(config)#ip tcp int one-minute low 1050
```

9 – Advanced Security and Attacks Configuration (14 Points)

9.1 – Allow Remote Management of the ASA (4 Points)

- a) Setup the ASA so that the PC at 10.1.1.100 can Telnet into the ASA for remote management.

```
ASA1(config)#telnet 10.1.1.100 255.255.255.255 inside
```

- b) Add the ASA as a device on the ACS server.

The screenshot shows the Cisco ACS 5.0 Network Configuration interface. On the left is a navigation pane with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area has a title bar 'Edit' and a header 'Add AAA Client'. The form contains the following fields and options:

- AAA-Client Hostname:
- AAA-Client IP Address:
- Key:
- Authenticate Using:
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure): ☐
- Log Update/Watchdog Packets from this AAA Client: ☐
- Log RADIUS Tunneling Packets from this AAA Client: ☐
- Replace RADIUS Port info with Username from this AAA Client: ☐

At the bottom of the form are three buttons: 'Submit', 'Submit + Apply', and 'Cancel'. Below these buttons is a link with a question mark icon and the text 'Back to Help'.

- c) The TACACS+ Server should authenticate telnet requests.
- d) The ASA communicates to the ACS server using TACACS+ with a secret key of ipexpert.

```
ASA1(config)#aaa-server TAC prot tacacs+
ASA1(config)#aaa-server TAC host 10.1.1.100
ASA1(config-aaa-server-host)#key ipexpert
ASA1(config)#aaa authentication telnet console TAC
```

- **Verify by connecting to the PIX from the ACS box. You don't have to add another user, you can use one of the existing users created in an earlier step.**

9.2 – Reflexive Access List (4 Points)

- a) You should allow HTTP, Telnet, SMTP, ICMP Pings and DNS traffic from VLAN 50 to go out of R5 and return back.
- b) Allow ICMP traffic sourced from R2's frame-relay interface. Do not allow any other traffic into VLAN 50 from outside of R5. You may allow relevant traffic in as needed for routing protocol adjacencies.
- c) Use a Reflexive Access List to accomplish it.

- **Evaluate the traffic leaving, and allow it to return with the evaluate keyword in the inbound ACL.**

```
R5(config)#ip access-list extended outfilter
R5(config-ext-nacl)#permit ospf host 192.1.25.5 host 224.0.0.5
R5(config-ext-nacl)#permit tcp host 5.5.5.5 host 2.2.2.2 eq bgp
R5(config-ext-nacl)#permit udp any any eq 4500
R5(config-ext-nacl)#permit udp any eq 4500 any
R5(config-ext-nacl)#permit udp host 192.1.25.5 host 192.1.12.5 eq
isakmp
R5(config-ext-nacl)#permit tcp any any eq www reflect RACL
R5(config-ext-nacl)#permit tcp any any eq telnet reflect RACL
R5(config-ext-nacl)#permit tcp any any eq smtp reflect RACL
R5(config-ext-nacl)#permit udp any any eq domain reflect RACL
R5(config-ext-nacl)#permit icmp any any reflect RACL
R5(config-ext-nacl)#permit udp host 192.1.25.2 host 192.1.25.5 eq ntp
R5(config-ext-nacl)#deny ip any any log
```

```
R5(config)#ip access-list extended infilter
R5(config-ext-nacl)#permit ospf host 192.1.25.2 host 224.0.0.5
R5(config-ext-nacl)#permit tcp host 2.2.2.2 host 5.5.5.5 eq bgp
R5(config-ext-nacl)#permit udp host 192.1.12.5 host 192.1.25.5 eq
isakmp
R5(config-ext-nacl)#permit udp host 192.1.25.2 host 192.1.25.5 eq ntp
R5(config-ext-nacl)#$host 192.1.12.5 eq 4500 host 192.1.25.5 eq 4500
R5(config-ext-nacl)#permit tcp host 2.2.2.2 eq bgp host 5.5.5.5
R5(config-ext-nacl)#evaluate RACL
R5(config-ext-nacl)#deny ip any any log
```


9.3 – Black Holing (3 Points)

- a) R9 has detected attacks coming in from the Ethernet segment.
 - b) All the packets are HTTP packets with a size ranging from 40 bytes to 100 bytes.
 - c) Use Policy Based Routing (PBR) to block this attack by Black Holing the packets.
- **Configure a route-map to match the traffic, and set the next hop to Null0. Configure the Null0 interface to not send ICMP unreachable, and apply the policy to the Fa0/0 interface on R9.**

```
R9(config)#route-map BADTRAFFIC
R9(config-route-map)#match address 191
R9(config-route-map)#match length 40 100
R9(config-route-map)#set interface null0

R9(config)#access-list 191 permit tcp any any eq 80

R9(config)#int null0
R9(config-if)#no ip unreachable
R9(config)#int fa0/0
R9(config-if)#ip policy route-map BADTRAFFIC
```

9.4 - IP Accounting (3 points)

- a) You would like to gather traffic statistics about the traffic that transits thru R9. Configure R9 for IP accounting on both interfaces.
- b) The maximum number of accounting entries to be created should be 500.
- c) IP accounting should be based on IP precedence for received and transmitted packets.

```
R9(config)#int fa0/0
R9(config-if)#ip accounting output-packets
R9(config-if)#ip accounting precedence input
R9(config-if)#ip accounting precedence output
R9(config-if)#int tun0
R9(config-if)#ip accounting output-packets
R9(config-if)#ip accounting precedence input
R9(config-if)#ip accounting precedence input
R9(config-if)#ip accounting precedence output
```

10 – IDS Configuration (16 Points)

10.1 – Basic Configuration of IPS (2 Points)

- a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the ACS server.

```
sensor#setup
Continue with configuration dialog?[yes]:
Enter host name[sensor]: IPS
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.15/24,10.1.1.1
```



```

Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.100
% The ip network address, 10.1.1.100, format is invalid
Please enter a valid IP address and netmask in the form x.x.x.x/nn.

Permit: 10.1.1.100/32
Permit:

```

10.2 – IPS Configuration (3 Points)

- a) Configure the IPS inline to monitor traffic between VLANs 51 and 52, using a single interface for monitoring.

- Enable the Fa0/1 interface under interface configuration – interfaces
- Add a VLAN pair for VLANs 51 and 52.
- Assign the VLAN pair to the virtual sensor under Analysis Engine – Virtual Sensor
- Make sure that the sniffing interface is configured as a trunk.

```

Sw1(config)#int fa0/7
Sw1(config-if)#swit trunk encap dot1q
Sw1(config-if)#swit mode trunk

```

10.3 – Signature Tuning (3 Points)

- a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.

Signature Definition – Signature Configuration, enable Echo (2004) and Echo Reply (2000)

- b) Set the Alarm Severity to Medium.

- Right Click the signature and set severity.

- c) The alarms should not fire when traffic is sourced from R2. They should fire from any other device.

Event Action Rules – Event action Filter – add a filter for signatures 2000 and 2004.

- Select Produce Alert as the Action to Subtract. Configure 192.1.25.2 as the attacker address.

- d) Verify the Alarm by pinging BB2's Ethernet interface from R2 and R5.

- Verify that the alarms show up in the Event Viewer.

10.4 – Creating a Custom Signature (4 Points)

- a) Create a custom string signature. The alarm should fire if a telnet connection types the words “admin” or “Admin”.

→ **Configure the Signature using the Signature Configuration Wizard. For telnet, use the String TCP engine with a service port of 23.**

- b) Set the Alarm Severity to High.

- c) Verify the Alarm by telnetting into BB2 from R2 and typing the word “Admin” after you have connected.

→ **In order to telnet to BB2 from R2, you will need to adjust your access list on R5.**

```
R5 (config) #ip access-list extended infiltrer
R5 (config-ext-nacl) #permit tcp host 192.1.25.2 host 10.5.5.100
```

- d) You are only allowed to create one alarm.

10.5 – PIX IDS (4 Points)

- a) Configure a Syslog Server at 10.1.1.100. Configure the ASA to send message to the Syslog server.

```
ASA1 (config) #logging host inside 10.1.1.100
```

- b) Configure Console Logging to level 4. Configure Trap logging level to debugging.

```
ASA1 (config) #logging console 4
ASA1 (config) #logging trap debugging
```

- c) Configure the ASA IDS with the following parameters:

- Send an alarm for Info signatures.
- Send an alarm and drop packets for Attack signatures.

```
ASA1 (config) #ip audit name INFO info action alarm
ASA1 (config) #ip audit name ATTACK attack action alarm drop
```

- d) You do not want signature 2004 to fire at all.

```
ASA1 (config) #ip audit signature 2004 disable
```

- e) Enable IDS on the outside interface.

```
ASA1 (config) #ip audit interface outside INFO
ASA1 (config) #ip audit interface outside ATTACK
```


Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

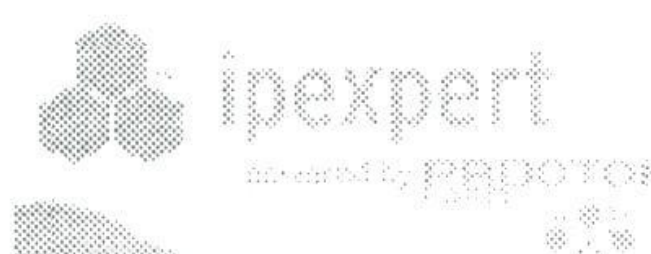
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 14: Multiprotocol Challenge C (One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 14 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 14 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

1 – Layer 2 (4 Points)

1.1 – Switch Management (2 Points)

- a) Create a Management interface on Switch1 belonging to VLAN 6.
- b) Set the IP Address as .20 on that network.

```
sw1(config)#int vlan 6
sw1(config-if)#ip address 192.1.6.6 255.255.255.0
```

- c) Allow Management access to this switch from VLAN 6 and VLAN 11.

```
sw1(config)#access-list 23 permit 192.1.6.0 0.0.0.255
sw1(config)#access-list 23 permit 10.2.2.0 0.0.0.255
```

1.2 – VLAN Interfaces (2 Points)

- a) Create a couple of Management interfaces on Sw2. It should be able to communicate to VLAN 49 and VLAN 5.
- b) Set the IP Address as .20 on both networks.

```
Sw2(config)#int vlan 49
Sw2(config-if)#ip address 192.1.49.20 255.255.255.0
Sw2(config-if)#int vlan 5
Sw2(config-if)#ip address 10.5.5.20 255.255.255.0
```

2 – Basic PIX Firewall (16 Points)

2.1 – PIX IP Address (4 Points)

- a) Create a Logical Interface off of E0 interface on the PIX.
- b) The logical interface should belong to VLAN 55.
- c) The Physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.

```
pixfirewall(config)#int eth0.55
pixfirewall(config-subif)#vlan 55
pixfirewall(config-subif)#nameif DMZ55
INFO: Security level for "DMZ55" set to 0 by default.
```



```
pixfirewall(config-subif)#security 50
pixfirewall(config-subif)#ip address 192.168.5.10 255.255.255.0
```

- d) Configure the Switch to allow the PIX to communicate to the rest of the network.

→ In order to connect to both the outside VLAN and the DMZ VLAN on the same interface, the switch needs to be configured to carry both VLANs.

```
Sw2(config)#int fa0/2
Sw2(config-if)#swit mode trunk
Sw2(config-if)#swit trunk encap dot1q
Sw2(config-if)#swit trunk native vlan 12
```

- e) Assign IP Addresses to the PIX Interfaces.

```
pixfirewall(config)#int eth0
pixfirewall(config-if)#nameif outside
pixfirewall(config-if)#ip address 192.1.12.10 255.255.255.0
pixfirewall(config-if)#no shut
pixfirewall(config-if)#int eth1
pixfirewall(config-if)#nameif inside
pixfirewall(config-if)#ip address 10.2.2.10 255.255.255.0
```

2.2 – Routing (3 Points)

- a) Run OSPF as the routing protocol on the PIX Firewall.
- b) Configure Process ID 1 and advertise the inside network in area 0.

```
pixfirewall(config)#router ospf 1
pixfirewall(config-router)#network 10.2.2.0 255.255.255.0 area 0
```

- c) Configure Process ID 10 and advertise the outside network in area 0.

```
pixfirewall(config)#router ospf 10
pixfirewall(config-router)#network 192.1.12.0 255.255.255.0 area 0
```

2.3 – Static Translation (3 Points)

- a) Allow R1 Loopback 0 to ping R2 using its own IP Address. Do not use an access-list to accomplish this. You might have to wait until a later step to verify this step. You are not allowed any static routes.

```
pixfirewall(config)#access-list outsideint permit icmp host
192.1.12.2 host 1.1.1.1 echo-reply
pixfirewall(config)#access-group outsideint in interface outside
```


- Without a static route, R2 needs to know how to return traffic to R1.

```
pixfirewall(config)#router ospf 1
pixfirewall(config-router)#redist ospf 10 subnets
pixfirewall(config-router)#exit
pixfirewall(config)#router ospf 10
pixfirewall(config-router)#redist ospf 1 subnets
```

- b) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

```
pixfirewall(config)#static (inside,outside) 192.1.12.100 10.1.1.100
netmask 255.255.255.255
pixfirewall(config)#access-list outsideint permit tcp host 4.4.4.4
host 192.1.12.100 eq 49
pixfirewall(config)#access-list outsideint permit tcp host 191.1.12.2
host 192.1.12.100 eq 49
```

2.4 – Advanced Access Lists (6 Points)

- a) Your company will be putting in 2 application servers. One of the application servers will be in DMZ55 with IP Addresses of 192.168.5.21 and 192.168.5.22.
- b) Create a static translation for them on the outside so that 192.168.5.21 is seen as 192.1.12.21 on the outside and 192.168.5.22 is seen as 192.1.12.22 on the outside. You might have to wait until a later step to verify this step. You are not allowed any static routes.

- Object groups will allow you to group items together, so that you can administer them together. Start with the static translations for the servers.

```
pixfirewall(config)#static (inside,outside) 192.1.12.21 192.168.5.21
netmask 255.255.255.255
pixfirewall(config)#static (inside,outside) 192.1.12.22 192.168.5.22
netmask 255.255.255.255
pixfirewall(config)#object-group network servers
pixfirewall(config-network)#network-object host 192.1.12.21
pixfirewall(config-network)#network-object host 192.1.12.22
```

- c) These servers are going to be access by partner organizations. The IP Addresses of these partner organizations are as follows:

- 205.15.25.0/24
- 207.215.1.0/24
- 210.208.15.16/28
- 211.0.15.32/27
- 192.1.150.112/28

```
pixfirewall(config)#object-group network partners
pixfirewall(config-network)#network-object 205.15.25.0 255.255.255.0
pixfirewall(config-network)#network-object 207.215.1.0 255.255.255.0
pixfirewall(config-network)#network-object 210.208.15.16 255.255.255.240
```



```
pixfirewall(config-network)#network-object 211.0.15.32 255.255.255.224
pixfirewall(config-network)#network-object 192.1.150.112 255.255.255.240
```

d) The applications on the servers are as follows:

- TFTP
- FTP
- HTTP
- SMTP
- DNS
- Custom Application at UDP 50000

→ For the Applications, create one group for TCP and one group for UDP ports.

```
pixfirewall(config)#object-group service srvtcp tcp
pixfirewall(config-service)#port-object eq ftp
pixfirewall(config-service)#port-object eq www
pixfirewall(config-service)#port-object eq ftp-data
pixfirewall(config-service)#port-object eq smtp
pixfirewall(config-service)#port-object eq 53
```

```
pixfirewall(config)#object-group service srvudp udp
pixfirewall(config-service)#port-obj eq tftp
pixfirewall(config-service)#port-obj eq 53
pixfirewall(config-service)#port-obj eq 50000
```

e) Allow all the partner organizations access to all the applications on the 2 servers. You are allowed 2 lines in the Access List to accomplish this.

```
pixfirewall(config)#access-list outsideint permit tcp object-group
partners object-group servers object-group srvtcp
pixfirewall(config)#access-list outsideint permit udp object-group
partners object-group servers object-group srvudp
```

→ If you use the command `show access-list`, the access-list will be expanded. If you use the command `show run access-list`, you can see that there are two lines.

3 – IDS (17 Points)

3.1 – Basic Configuration of IDS through IDS, IDM and IEV (2 Points)

a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

→ Run through setup from the CLI, and configure the IP address and netmask.

3.2 – Switch Configuration (2 Points)

a) You would like to monitor all traffic received in the outside VLAN of the PIX.

b) Configure the Switch to copy all relevant traffic to the monitoring port.


```
sw1(config)#vlan 123
sw1(config-vlan)#remote-span

Sw2(config)#monitor session 1 source vlan 12 rx
Sw2(config)#monitor session 1 dest remote vlan 123 reflector-port
fa0/20

sw1(config)#monitor session 1 source vlan 12 , 123 rx
sw1(config)#monitor session 1 dest int fa0/7
```

3.3 – Fine tuning the ICMP Signature (4 Points)

- a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.
 - Enable interface Fa0/1 under Interface Configuration – Interfaces
 - Assign to the virtual sensor under Analysis Engine – Virtual Sensor
- b) Set the Alarm Severity to Medium.
 - Enable and set severity under Signature Definition –Signature Configuration.
- c) The alarms should not fire when they are sent by R2. They should fire from any other device.
 - Under Event Action Rules configure a filter under Event Action Filters. Add the address for R2. Make sure to select “Produce Alert” under actions to subtract, or the alarm will still fire. You may want to add filters for ALL the addresses on R2, not just the address for the Ethernet interface. If unsure about a section, be sure to ask the proctor for clarification.
- d) Verify the Alarm by pinging the outside Interface of the PIX from R2 and R5.

3.4 – IP Blocking on the PIX (5 Points)

- a) Configure the IDS Sensor to block the Connection if the ICMP Echo Request or Reply signature is detected.
- b) The Blocking should be done on the PIX firewall.
- c) Configure the PIX to allow the IDS Sensor to Telnet into it.

```
pixfirewall(config)#telnet 10.1.1.15 255.255.255.255 inside
```
- d) Authenticate the Telnet connection using AAA server. Configure the ACS server as needed.
 - Setup User1 on the ACS server, with a password of ccie.

- **Configure the PIX as a network device on the ACS server, using the key ipexpert.**

```
pixfirewall(config)#aaa-server TAC protocol TACACS
pixfirewall(config)#aaa-server TAC host 10.1.1.100
pixfirewall(config-aaa-server-host)#key ipexpert
```

- e) Configure the Sensor with the appropriate information to Telnet into the PIX. Use User1 as the username and cisco as the password to allow the IDS to connect into the PIX.

- **Add the device login profile under blocking, using user User1 and password cisco.**

- **Under Blocking, add the PIX as a blocking device, using telnet as the protocol.**

- **Under the signatures, add “request block connection” as an action.**

- f) Set the Block time to 20 Minutes.

- **Under Event Action rules, General settings, configure the block duration to 20 minutes.**

3.5 – IOS IDS on R6 (4 Points)

- a) Configure the router to send alarms to a Syslog Server. Configure the PIX to allow the alarms from R6 to the Syslog Server at 10.1.1.100. The Syslog server is seen as 192.1.12.100 on the outside of the PIX. This static translation should have been done in an earlier step.

```
pixfirewall(config)#access-list outsideint permit udp host 6.6.6.6
host 192.1.12.100 eq 514
R6(config)#logging source-int lo0
R6(config)#ip ips notify log
R6(config)#logging host 192.1.12.100
```

- b) You do not want signatures to fire from a specific address. (200.0.0.2) for this IDS Rule Set.

```
R6(config)#access-list 35 deny 200.0.0.2
R6(config)#access-list 35 permit any
R6(config)#ip ips name MYIPS list 35
```

- c) Attacks should be detected from the Frame cloud.

```
R6(config)#int ser0/1/0
R6(config-if)#ip ips MYIPS in
```


4 – ASA (6 Points)

4.1 – ASA Configuration (3 Points)

- a) Configure ASA2 with IP addresses as shown in the diagram. ASA2 should learn route information from R6, but should not give R6 information about VLAN 6.

- **Start with basic configuration of interfaces and IP addresses. In order to learn route information from R6, configure a routing protocol on the ASA. Since R6 is running OSPF, enable OSPF on the outside interface.**

```
ASA1(config)#int eth0/0
ASA1(config-if)#ip address 192.1.66.55 255.255.255.0
ASA1(config-if)#no shut
ASA1(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.

ASA1(config)#int eth0/1
ASA1(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA1(config-if)#ip address 192.1.6.55 255.255.255.0
ASA1(config-if)#no shut

ASA1(config)#router ospf 1
ASA1(config-router)#network 192.1.66.0 255.255.255.0 area 10
```

4.2 – ASA Failover (3 points)

- a) Configure ASA2 to act as a failover in case ASA1 fails.

- **Since we aren't given any specific parameters to use, we can pick any values we want. The Eth0/2 interfaces are unused, and are both configured for VLAN 555 on the switch.**

```
ASA1(config)#failover lan unit primary
ASA1(config)#failover lan interface MYFAILOVER eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its
sub-interfaces
ASA1(config)#failover key IPEXPERT
ASA1(config)#failover interface ip MYFAILOVER 192.55.55.55
255.255.255.0 standby 192.55.55.56
ASA1(config)#int eth0/0
ASA1(config-if)#ip address 192.1.66.55 255.255.255.0 standby
192.1.66.56
ASA1(config-if)#int eth0/1
ASA1(config-if)#ip address 192.1.6.55 255.255.255.0 standby
192.1.6.56
ASA1(config-if)#failover
```

- **Start on ASA2 by checking the mode. The mode needs to match for failover to be successful.**

```
ciscoasa(config)#show mode
Security context mode: single
```


→ **Verify that the failover interface is not shut down.**

```
ciscoasa(config)#int eth0/2
ciscoasa(config-if)#no shut

ciscoasa(config)#failover lan unit secondary
ciscoasa(config)#failover lan interface MYFAILOVER eth2
Invalid interface
ciscoasa(config)#failover lan interface MYFAILOVER eth0/2
INFO: Non-failover interface config is cleared on Ethernet0/2 and its
sub-interfaces
ciscoasa(config)#failover key IPEXPERT
ciscoasa(config)#failover interface ip MYFAILOVER 192.55.55.55
255.255.255.0 standby 192.55.55.56
```

→ **Enable failover on ASA-2.**

```
ciscoasa(config)#failover
```

→ **Verify with show failover**

```
ASA1#show failover
Failover On
Failover unit Secondary
Failover LAN Interface: MYFAILOVER Ethernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Last Failover at: 17:40:58 UTC Feb 6 2007
    This host: Secondary - Standby Ready
        Active time: 609 (sec)
        slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
            Interface outside (192.1.55.56): Normal
            Interface inside (192.1.6.56): Normal
        slot 1: empty
    Other host: Primary - Active
        Active time: 1095 (sec)
        slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
            Interface outside (192.1.55.55): Normal
            Interface inside (192.1.6.55): Normal
        slot 1: empty

Stateful Failover Logical Update Statistics
Link : Unconfigured.
```

```
ASA1#
```


5 – Access Management (8 Points)

5.1 – Configuring AAA Authentication on R4 for Telnet (4 Points)

- a) Configure R4 with AAA access. TACACS+ server sees R4 with its Loopback 0 address. The secret key is cisco.

```
R4(config)#aaa new-model
R4(config)#tacacs-server host 192.1.12.100
R4(config)#tacacs-server key cisco
R4(config)#ip tacacs source-int lo0
```

- b) No Authentication should be done on the Console or AUX lines.

```
R4(config)#aaa authentication login default none
```

- c) Setup Authentication based on TACACS+ for the VTY lines.

```
R4(config)#aaa authentication login VTY group tacacs
R4(config)#line vty 0 15
R4(config-line)#login authentication VTY
```

- d) Create 2 users created on the AAA server, User 1 and User2. Both the users have ccie as their password.

5.2 – Configuring Controlled Telnet Access (4 Points)

- a) Configure Telnet on R4 such that when Users login, they see a menu that only allows them the ability to execute the following commands by using a menu:

- Show IP interface Brief
- Show IP Route
- Show IP Protocol
- Show Run
- Exit

- b) The Users should not to able to get a command prompt if they login using the default port (23).

- **Configure the text lines for the menu, and configure the commands that correspond.**

```
R4(config)#menu MYMENU text 1 "Show IP interface Brief"
R4(config)#menu MYMENU command 1 Show IP interface Brief
R4(config)#menu MYMENU text 2 "Show IP Route"
R4(config)#menu MYMENU command 2 Show IP Route
R4(config)#menu MYMENU text 3 "Show IP Protocol"
R4(config)#menu MYMENU command 3 Show IP Protocol
R4(config)#menu MYMENU text 4 "Show Run"
R4(config)#menu MYMENU command 4 Show Run
R4(config)#menu MYMENU text 5 "Exit"
R4(config)#menu MYMENU command 5 Exit
```


- **Apply the menu to the VTY lines with the autocommand.**

```
R4(config)#line vty 0 15
R4(config-line)#autocommand menu MYMENU
```

- c) Configure local authorization for exec, command 1 and command 15 privilege levels. Assign User1 and User2 to privilege level 15.

- **Configuring the user privileges just requires configuring the users locally. For authorization, configure a method list and apply to the VTY lines.**

```
R4(config)#username User1 priv 15 password ccie
R4(config)#username User2 priv 15 password ccie
R4(config)#aaa authorization exec LOCAUTH local
R4(config)#aaa authorization commands 1 LOCAUTH local
R4(config)#aaa authorization commands 15 LOCAUTH local
R4(config)#line vty 0 1180
R4(config-line)#authorization exec LOCAUTH
R4(config-line)#authorization commands 1 LOCAUTH
R4(config-line)#authorization commands 15 LOCAUTH
```

- d) The administrator should be given the ability to login and get a prompt without the menu. The administrator to connect using port 3099. Set aside one Telnet line for the Administrator.

- **Configuring a rotary group allows the use of a range of ports above 3000. For port 3099, use rotary 99.**

```
R4(config)#line vty 1180
R4(config-line)#rotary 99
R4(config)#line vty 1180
R4(config-line)#login authentic VTY
```

6 – Network Attacks (12 Points)

6.1 – Network Attacks (12 Points)

- a) Configure R4's Ethernet interface for PBR, to mitigate against the Nachi worm. Any inbound ICMP type 8 or type 0 with a packet length of 92 should be dropped. Disable unreachable on both the Ethernet interface, and the null0 interface.

- **ICMP type 8 is echo request, ICMP type 0 is echo reply. Policy routing just needs a route-map to match the traffic and send it to Null0. Ordinarily an ICMP unreachable message would be generated, but will be disabled for this step.**

```
R4(config)#access-list 161 permit icmp any any echo
R4(config)#access-list 161 permit icmp any any echo-reply

R4(config)#route-map NACHI
R4(config-route-map)#match ip address 161
R4(config-route-map)#match length 92 92
R4(config-route-map)#set interface null0
```



```

R4(config)#int null0
R4(config-if)#no ip unreach
R4(config)#int fa0/0
R4(config-if)#ip policy route-map NACHI
R4(config-if)#no ip unreachable

```

- b) Configure R6's Ethernet interface to drop inbound malicious traffic. The malicious traffic has been identified as using TCP port 15796 with a packet length of 142 bytes. Do not configure an access-list for this step. Other traffic using TCP port 15796 should not be affected.

→ **NBAR will allow you to match protocols based on port number. Since we don't have a protocol predefined for TCP port 15796, we can use a custom mapping. By matching the undesired traffic first, we can drop it, and allow other traffic to pass freely.**

```

R6(config)#ip nbar port-map custom-01 tcp 15796

R6(config)#class-map BAD
R6(config-cmap)#match prot custom-01

R6(config-cmap)#match packet length min 142 max 142

R6(config)#policy-map ATTACK
R6(config-pmap)#class BAD
R6(config-pmap-c)#drop

R6(config)#int fa0/0
R6(config-if)#service-policy input ATTACK

```

- c) Configure R5's Ethernet interface to deny any ICMP traffic inbound, other than type 8 and type 0.

```

R5(config)#access-list 163 permit icmp any any echo
R5(config)#access-list 163 permit icmp any any echo-reply
R5(config)#access-list 163 deny icmp any any
R5(config)#access-list 163 permit ip any any
R5(config)#int fa0/0
R5(config-if)#ip access-group 163 in

```

- d) Configure R2's serial interface to block inbound traffic on tcp ports 8000 to 8005. Other traffic should not be affected. Use an access-list to accomplish this.

→ **Since we are not told which subinterface, apply the access-list on all the subinterfaces.**

```

R2(config)#access-list 164 deny tcp any any range 8000 8005
R2(config)#access-list 164 permit ip any any
R2(config)#int ser0/1/0.6
R2(config-subif)#ip access-group 164 in
R2(config-subif)#int ser0/1/0.5
R2(config-subif)#ip access-group 164 in
R2(config)#int ser0/1/0.4
R2(config-subif)#ip access-group 164 in

```


7 –Virtual Private Networks (20 Points)

7.1 – Basic Concentrator Configuration (3 Points)

- a) Configure the IP Address of the Private Interface thru the CLI.
- b) The Public interface should be configured from the Graphical interface.
- c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.
 - **Configure the private interface address through setup on the CLI. Since R1 is running RIP on both interfaces, a static route is not necessary.**
 - **For the Public interface, add the IP address and mask under Configuration – Interfaces.**

7.2 – Static Routes on the Concentrator (2 Points)

- a) Configure a Default Route on the Concentrator pointing towards the DMZ55 interface on the PIX.

Configuration (1) – System Management (2) – IP Routing (3) – Default Gateway (2) -

7.3 – Setup a Site-to-Site IPSec VPN between the PIX and R5 (4 Points)

- a) Configure a LAN to LAN tunnel between the PIX and R5 to encrypt traffic from 10.2.2.0/24 to 10.5.5.0/24.
- b) Use the following parameters:
 - Authentication is based on Pre-shared key of **ccie**.
 - Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
 - For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.
 - **Start with the access list for interesting traffic:**

```
pixfirewall(config)#access-list R5L2L extended permit ip 10.2.2.0
255.255.255.0 10.5.5.0 255.255.255.0
```

- **Configure the ISAKMP policy, using preshared key, and MD5.**

```
pixfirewall(config)#crypto isak policy 10
pixfirewall(config-isakmp-policy)#auth pre-share
pixfirewall(config-isakmp-policy)#hash md5
```

- **Enable ISAKMP on the outside interface, and configure the key under tunnel group.**

```
pixfirewall(config)#crypto isakmp enable outside
pixfirewall(config)#tunnel-group 192.1.25.5 type ipsec-l2l
pixfirewall(config)#tunnel-group 192.1.25.5 ipsec-attributes
pixfirewall(config-tunnel-ipsec)#pre-shared-key ccie
```


- **Configure the IPSec transform, and configure the crypto map.**

```
pixfirewall(config)#crypto ipsec transform-set MYTRANSFORM esp-des
esp-sha-hmac
```

```
pixfirewall(config)#crypto map MYMAP 10 match address R5L2L
pixfirewall(config)#crypto map MYMAP 10 set transform-set MYTRANSFORM
pixfirewall(config)#crypto map MYMAP 10 set peer 192.1.25.5
```

```
pixfirewall(config)#crypto map MYMAP interface outside
```

- **The PIX has a route for the remote network learned from R2, so adding a route is not necessary.**
- **Tunnel mode is the default for the transform set. If we needed to use a transport tunnel, it would be specified on the transform set as “crypto ipsec transform-set MYTRANSFORM mode transport”**
- **Configuration is similar on R5. Start with the key and access list.**

```
R5(config)#crypto isak key 0 ccie address 192.1.12.10
```

```
R5(config)#ip access-list extended R5L2L
R5(config-ext-nacl)#permit ip 10.5.5.0 0.0.0.255 10.2.2.0 0.0.0.255
```

- **Configure the ISAKMP policy.**

```
R5(config)#crypto isak pol 10
R5(config-isakmp)#auth pre-share
R5(config-isakmp)#hash md5
R5(config-isakmp)#group 2
R5(config-isakmp)#encr 3des
```

- **Configure the Transform set and crypto map, and apply map to the interface.**

```
R5(config)#crypto ipsec transform MYTRANSFORM esp-des esp-sha-hmac
```

```
R5(config)#crypto map MYMAP 10 ipsec-isakmp
```

% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

```
R5(config-crypto-map)#match address R5L2L
R5(config-crypto-map)#set peer 192.1.12.10
R5(config-crypto-map)#set transform MYTRANSFORM
R5(config-crypto-map)#exit
R5(config)#int ser0/1/0
R5(config-if)#crypto map MYMAP
```

- **Note: The section asks that you configure ISAKMP parameters at the “default values”. The default values for the PIX are not the same as the defaults for a router. Depending on whether you choose the router defaults or the PIX defaults, they need to match on both sides. When in doubt, ask the proctor for clarification.**

- **Verify that you can ping across, and that the crypto counters show values for encapsulation and decapsulation.**

R5#**ping 10.2.2.1 source 10.5.5.5**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.5.5.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 24/27/28 ms

R5#**show cry ipsec sa**

interface: Serial0/1/0

Crypto map tag: MYMAP, local addr 192.1.25.5

protected vrf: (none)

local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)

current_peer 192.1.12.10 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9

#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 11, #recv errors 0

local crypto endpt.: 192.1.25.5, remote crypto endpt.: 192.1.12.10

path mtu 1500, ip mtu 1500

7.4 – Setup a Remote Access VPN from the Cisco Secure Client and the Concentrator (4 points)

- a) Use the following parameters to setup the Concentrator with the following options:

- Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote**.
- Set the username as VPNUser with a password of **ccie1234**.
- Create a group called Remote with a password of **ccie**.
- Only allow PPTP and IPsec for the group. Configure it such that only MSCHAP V2 is allowed as the authentication protocol for PPTP.

Configuration – User Management – Base Group – select PPTP and enable MSCHAPv2.

Configuration – User Management – Groups – Add a group with name Remote and password ccie.

- On the General tab for the group, uncheck L2TP and WebVPN.
- On the PPTP tab uncheck Inherit for PPTP authentication, and make sure that only MSCHAP v2 is selected for PPTP authentication protocols.
- Select apply to take you back to the Groups page.
- Select Address pools, add a pool 10.3.3.1 to 10.3.3.254 with 24 bit mask.

Configuration – System – Address Management – Assignment, select “use address pools”.

Under Configuration – User Management - Users, add a user VPNUser with password ccie1234.

→ Testing:

→ On the PIX, allow ESP and ISAKMP traffic to the concentrator address.

```
pixfirewall(config)#access-list outsideint permit esp any host 192.168.5.5
pixfirewall(config)#access-list outsideint permit udp any host 192.168.5.5 eq$
```

→ Configure the Test PC for VLAN 12 by adding the interface on Cat2 (Fa0/10) to vlan 12.

→ On the Test PC, configure an IP address unused on VLAN 12, and add a route to 192.168.5.5.

```
C:\ >route add 192.168.5.5 mask 255.255.255.255 192.1.12.10
```

→ On the VPN Concentrator, add a route to 192.1.12.0/24 via the DMZ interface if you did not disable RIP on the Private interface.

→ Create a connection entry on the VPN client, with group/password as specified above and connect. When the authentication box pops up, enter the username VPNUser with password ccie1234.

7.5 – Configure a Remote Access VPN using Easy VPN Concentrator and R4 (5 Points)

a) Configure the Concentrator as the Easy VPN Server using the following parameters:

- Group name and password : Name : **EZGroup** Password : **abcd1234**
- Domain Name : ipexpert.com
- Address Pool (Local) : 192.168.22.1 192.168.22.16
- The Address should be assigned to the client from the pool above. Create a static route on R1 for this network. The Authentication should be done locally.
- Create a User called **EZUser** with a password of **ccie1234**. Make this user a member of the **EZGROUP**.

Configuration – User Management – Groups – Add a group EZGroup with password abcd1234.

→ Under the Client Config tab, add the domain name ipexpert.com.

→ Add the address pool to the group, under address pools.

```
R1(config)#ip route 192.168.22.0 255.255.255.224 10.2.2.5
```

→ Under users, configure the EZUser, select only IPSec for tunneling protocols under the general tab.

→ You can test this first part by adding a connection entry on the test PC and log in with the username of EZUser. By testing from the test PC, you can eliminate the possibility of configuration issues on the VPN Concentrator.

- **Note:** On the VPN Concentrator, make sure you have also selected “Allow Network Extension Mode” under the HW Client tab of the Group setup, or the negotiation will fail.
- For the split tunneling in the next section, select the option “only tunnel networks in the list” on the Client Config tab. You can use the existing network, or add a network list for 10.2.2.0/24 under configuration – policy management – traffic management – network lists.

b) Configure R4 as the EZVPN Client:

- Create a Loopback 100 on R4. Assign it an IP address of 172.16.0.1 255.255.0.0.
- Configure R4 such that when this Loopback connects to the Network, it is translated to the Serial interface of R4 except when it tries to connect to 10.2.2.0/24.
- When Loopback 100 tries to connect to 10.2.2.0/24 network, the Router should initiate an EZVPN session with the Concentrator.
- It should match the group name and username of the Concentrator.
- Configure it in network extension mode.

→ **Configure the Group on R4**

```
R4(config)#crypto ipsec client ezvpn EZGroup
R4(config-crypto-ezvpn)#group EZGroup key abcd1234
R4(config-crypto-ezvpn)#mode network-extension
R4(config-crypto-ezvpn)#peer 192.168.5.5
R4(config-crypto-ezvpn)#username EZUser password 0 cciel234 <--This
command will not be accepted, if the concentrator is not
configured to allow the client to save the password under the
client config tab of Group setup.)
```

```
R4(config)#int loop100
```

```
R4(config-if)#ip nat inside
```

```
R4(config)#access-list 176 permit ip 172.16.0.0 0.0.255.255 10.2.2.0
0.0.0.255
```

```
R4(config-if)#crypto ipsec client ezvpn EZGroup inside
```

```
R4(config-if)#int ser0/0/0
```

```
R4(config-if)#ip nat outside
```

```
R4(config-if)#crypto ipsec client ezvpn EZGroup
```

```
R4(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 10.2.2.0
0.0.0.255
```

```
R4(config)#access-list 175 permit ip 172.16.0.0 0.0.255.255 any
```

```
R4(config)#ip nat inside source list 175 interface ser0/0/0 overload
```

→ **Routing – R4 and R2 need a route to 192.168.5.0 to pass the tunnel traffic.**

```
R4(config)#ip route 192.168.5.0 255.255.255.0 192.1.24.2
```

```
R2(config)#ip route 192.168.5.0 255.255.255.0 192.1.12.10
```



```
R4#ping 10.2.2.1 source loop100
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
R4#
```

```
R4#show cry ipsec sa
```

```
interface: Serial0/0/0
  Crypto map tag: Serial0/0/0-head-0, local addr 192.1.24.4

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.22.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 192.168.5.5 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

- **Debug NAT translations, and verify that R4 can ping other addresses and be NATed to the interface address.**

```
R4#ping 10.5.5.5 source lo100
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
Packet sent with a source address of 172.16.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
R4#
*Feb  7 23:09:57.987: NAT: s=172.16.0.1->192.1.24.4, d=10.5.5.5 [6659]
*Feb  7 23:09:58.007: NAT*: s=10.5.5.5, d=192.1.24.4->172.16.0.1 [6659]
*Feb  7 23:09:58.011: NAT: s=172.16.0.1->192.1.24.4, d=10.5.5.5 [6660]
*Feb  7 23:09:58.031: NAT*: s=10.5.5.5, d=192.1.24.4->172.16.0.1 [6660]
*Feb  7 23:09:58.031: NAT: s=172.16.0.1->192.1.24.4, d=10.5.5.5 [6661]
*Feb  7 23:09:58.051: NAT*: s=10.5.5.5, d=192.1.24.4->172.16.0.1 [6661]
*Feb  7 23:09:58.055: NAT: s=172.16.0.1->192.1.24.4, d=10.5.5.5 [6662]
*Feb  7 23:09:58.075: NAT*: s=10.5.5.5, d=192.1.24.4->172.16.0.1 [6662]
*Feb  7 23:09:58.075: NAT: s=172.16.0.1->192.1.24.4, d=10.5.5.5 [6663]
*Feb  7 23:09:58.095: NAT*: s=10.5.5.5, d=192.1.24.4->172.16.0.1 [6663]
```

7.6 – Management VPN (2 Points)

- a) Configure a Lan-to-lan IPSec connection from ASA1 to the PIX. Traffic from 10.2.2.0 to 192.168.6.0 should be encrypted.

- **Since we already have a VPN configured on the PIX, we can use the same parameters for this VPN.**

```
pixfirewall(config)#access-list ASAL2L extended permit ip 10.2.2.0
255.255.255.0 192.1.6.0 255.255.255.0

pixfirewall(config)#tunnel-group 192.1.66.55 type ipsec-l2l
pixfirewall(config)#tunnel-group 192.1.66.55 ipsec-attributes
pixfirewall(config-tunnel-ipsec)#pre-shared-key ccie
```



```

pixfirewall(config)#crypto map MYMAP 20 match address ASAL2L
WARNING: The crypto map entry is incomplete!
pixfirewall(config)#crypto map MYMAP 20 set transform MYTRANSFORM
WARNING: The crypto map entry is incomplete!
pixfirewall(config)#crypto map MYMAP 20 set peer 192.1.66.55

```

- On ASA1 configure the parameters to match.

```

ASA1(config)#access-list ASAL2L extended permit ip 192.1.6.0
255.255.255.0 10$
ASA1(config)#crypto isak pol 10
ASA1(config-isakmp-policy)#auth pre-share
ASA1(config-isakmp-policy)#hash md5

ASA1(config)#crypto isakmp enable outside
ASA1(config)#tunnel-group 192.1.12.10 type ipsec-l2l
ASA1(config)#tunnel-group 192.1.12.10 ipsec-attributes
ASA1(config-tunnel-ipsec)#pre-shared-key ccie

ASA1(config)#crypto ipsec transform MYTRANSFORM esp-des esp-sha-hmac
ASA1(config)#crypto map MYMAP 10 match address ASAL2L
ASA1(config)#crypto map MYMAP 10 set transform MYTRANSFORM
ASA1(config)#crypto map MYMAP 10 set peer 192.1.12.10
ASA1(config)#crypto map MYMAP interface outside

```

- The ASA is learning a route for the 10.2.2.0 network, but the PIX is not learning a route for the 192.1.6.0 network. Add a static route on the PIX. Redistributing the static route into OSPF for the inside interface will tell R1 about the 192.1.6.0 network.

```

pixfirewall(config)#route outside 192.1.6.0 255.255.255.0 192.1.12.2

pixfirewall(config)#router ospf 1
pixfirewall(config-router)#redist static

```

- Add a static route on Cat1 pointing to ASA1.

```

sw1(config)#ip route 0.0.0.0 0.0.0.0 192.1.6.55

```

- If you tested by pinging from R1 to Cat1 before adding the static route, it is possible that you will see a difference in the packets encapsulated and decapsulated as shown below since Cat1 did not have a route to send the traffic back.

```

ASA1#show cry ipsec sa
interface: outside
  Crypto map tag: MYMAP, seq num: 10, local addr: 192.1.66.55

    access-list ASAL2L permit ip 192.1.6.0 255.255.255.0 10.2.2.0
    255.255.255.0
    local ident (addr/mask/prot/port): (192.1.6.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
    current_peer: 192.1.12.10

    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

```



```

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly:
0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.1.66.55, remote crypto endpt.: 192.1.12.10

path mtu 1500, ipsec overhead 58, media mtu 1500

current outbound spi: 24054858

```

8 – IOS Firewall (9 Points)

8.1 – Cisco IOS Firewall on R4 with non-standard ports (5 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- All TCP Based traffic
- All UDP Based traffic
- Netmeeting Traffic
- SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in.

```

R4(config)#ip inspect name MYFW tcp
R4(config)#ip inspect name MYFW udp
R4(config)#ip inspect name MYFW h323
R4(config)#ip inspect name MYFW smtp

```

- **Note: Newer IOS versions (12.3T4 and later) allow ESMTP inspection as well.**

b) FTP should be inspected on the Standard port and also on port 2021.

```

R4(config)#ip port-map ftp port 2021

```

c) HTTP should also be inspected for a non-standard port of 8000.

```

R4(config)#ip port-map http port 8000
R4(config)#ip inspect name MYFW http

```

d) Only allow relevant traffic coming in.

- **When creating an ACL, make sure to go back through the lab, and see what sections have asked you to do. The biggest thing to remember is that CBAC is intended for TRANSIT traffic, so any traffic terminating or originating on the router may need to be permitted in your access list.**

- **Allow routing traffic.**

```

R4(config)#access-list 182 permit ospf host 192.1.24.2 host 224.0.0.5

```

- **Allow return traffic from the TACACS server:**

```

R4(config)#access-list 182 permit tcp host 192.1.12.100 host 4.4.4.4
eq 49

```


→ **Allow return traffic from the concentrator for the VPN traffic.**

```
R4(config)#access-list 182 permit udp host 192.168.5.5 host
192.1.24.4 eq isak
R4(config)#access-list 182 permit esp host 192.168.5.5 host
192.1.24.2
```

→ **Allow telnet on both normal port and 3099.**

```
R4(config)#access-list 182 permit tcp any host 192.1.24.2 eq telnet
R4(config)#access-list 182 permit tcp any host 4.4.4.4 eq telnet
R4(config)#access-list 182 permit tcp any host 192.1.24.2 eq 3099
R4(config)#access-list 182 permit tcp any host 4.4.4.4 eq 3099
```

→ **Allow traffic from VLAN 11 to loopback 11.**

```
R4(config)#access-list 182 permit ip 10.2.2.0 0.0.0.255 host
172.16.0.1
```

→ **In general, it is usually safe to allow ICMP echo and echo reply for ping testing. If not stated, or you are not sure if it is OK to add, make sure to ask the proctor.**

```
R4(config)#access-list 182 permit icmp any any echo
R4(config)#access-list 182 permit icmp any any echo-reply
```

e) **ACL should be set to inbound on the Serial interface.**

```
R4(config)#int ser0/0/0
R4(config-if)#ip access-group 182 in
R4(config-if)#ip inspect MYFW out
```

8.2 – URL Filtering (4 Points)

- Configure R4 to inspect all HTTP traffic from the Ethernet segment towards the Frame networks for urls.
- The url server is a Web Sense server located at 192.1.49.52.
- Configure the Router to point to the Web Sense server.
- The router should always block requests going towards xxx.com. The router should always permit requests to cisco.com.
- If the Web Sense server is down, the HTTP requests should be allowed to go out.

→ **These are just modifications to the HTTP inspection.**

```
R4(config)#access-list 80 permit any
R4(config)#ip inspect name MYFW http java-list 80 urlfilter

R4(config)#ip urlfilter allow-mode on
R4(config)#ip urlfilter exclusive-domain deny xxx.com
R4(config)#ip urlfilter exclusive-domain permit cisco.com
R4(config)#ip urlfilter server vendor websense 192.1.49.52
```


9 – Advanced Security and Attacks (8 Points)

9.1 – SSH into PIX (4 Points)

- Setup the PIX firewall so that the PC at 10.1.1.100 can ssh into the PIX for remote management.
- Have the TACACS Server authenticate ssh Requests.
- The PIX communicates to the TACACS Server using TACACS+ with a secret key of ipexpert.

```
pixfirewall(config)#ssh 10.1.1.100 255.255.255.255 inside
pixfirewall(config)#ssh 10.1.1.1 255.255.255.255 inside
pixfirewall(config)#aaa-server TAC host 10.1.1.100
pixfirewall(config-aaa-server-host)#key ipexpert
pixfirewall(config)#aaa authentication ssh console TAC
```

→ On the ACS server, create a user, and configure the PIX as a network device with the key ipexpert. Verify that you can log in from the PC at 10.1.1.100.

9.2 – Dynamic Access Lists (4 Points)

- R5 should allow access from the frame networks only if users are authenticated.
- Once Authenticated, the user should be allowed full access.
- The authentication should be done locally.
- Allow Administrator to Manage the Router from the Frame Relay interface. They should use a non-default port for this. Dedicated only one Telnet line for this.
- Apply the ACL on the Frame Relay Interface.
- Allow relevant traffic to come in including return traffic. You are also allowed to create a reflexive ACL for this task.
- Create a couple of local users to test the config (U1 with a password of u1 and U2 with a password of U2).

→ Two separate pieces here, allowing local login, and configuring a reflexive access list.

→ Start with the reflexive access list.

```
R5(config)#ip access-list extended OUTBOUND
R5(config-ext-nacl)#permit ip any any reflect BACK
R5(config-ext-nacl)#exit
R5(config)#ip access-list extended INBOUND

R5(config-ext-nacl)#permit esp host 192.1.12.10 host 192.1.25.5
R5(config-ext-nacl)#permit udp host 192.1.12.10 eq 500 host
192.1.25.5 eq 500
R5(config-ext-nacl)#permit ospf host 192.1.25.2 host 192.1.25.5
R5(config-ext-nacl)#permit icmp any any echo
R5(config-ext-nacl)#permit icmp any any echo-reply
```



```
R5(config-ext-nacl)#permit tcp any host 192.1.25.5 eq 3001
R5(config-ext-nacl)#permit tcp any host 192.1.25.5 eq telnet
R5(config-ext-nacl)#evaluate RACL
```

```
R5(config)#int ser0/1/0
R5(config-if)#ip access-group INBOUND in
R5(config-if)#ip access-group OUTBOUND out
```

- Use a rotary line to give the administrators a high numbered port to connect to.

```
R5(config)#line vty 1180
R5(config-line)#rotary 1
```

- For the host portion, add a dynamic line to the access list, and the autocommand access enable under the VTY lines.

```
R5(config)#ip access-list extended INBOUND
R5(config-ext-nacl)#dynamic IPEXPERT permit ip any any
```

```
R5(config)#line vty 0 15
R5(config-line)#login local
R5(config-line)#autocommand access-enable host
```

```
R5(config)#username U1 password u1
R5(config)#username U2 password U2
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

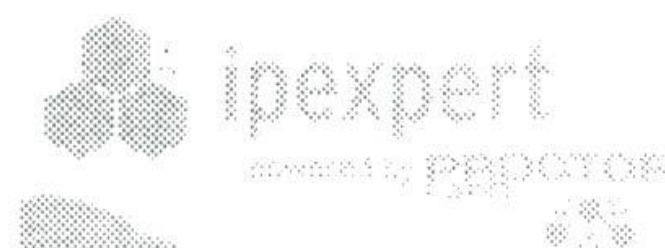
This page left intentionally blank.

Section 15: Multiprotocol Challenge D (One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 15 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the “Initial Configurations” subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 15 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the “MY CONFIGS” area of your www.IPexpert.com Member's Area.

1 – Layer 2 (7 Points)

1.1 – Switch Management (2 Points)

- Create a Management interface on the Switch1 belonging to VLAN 6.
- Set the IP Address as .20 on that network.
- Allow Management access to this switch from VLAN 6 only.

→ **Basic configuration for the switch, assign an address to the VLAN, and configure an access class to restrict traffic.**

```
Sw1(config)#int vlan 6
Sw1(config-if)#ip address 1
Sw1(config)#access-list 23 permit 192.1.6.0 0.0.0.255
Sw1(config)#line vty 0 15
Sw1(config-line)#access-class 23 in
```

1.2 – Switch Security (5 Points)

- You want to make sure that only PIX Inside interface can connect to the respective port on Switch 2.
- Make sure only PIX inside MAC can communicate on that port.

→ **Just looking for port security here. Look at the PIX to see what its mac address is and configure it on the switch. Eth1 is the PIX inside interface.**

```
Sw2(config)#int fa0/3
Sw2(config-if)#switchport port-security mac-address 0019.2f6b.4514
```

- All ports on switch 1 and switch 2 that do not need trunking should be set as access ports, to minimize the risk of a rogue device connecting and establishing a trunk connection.

→ **Ports 21-24 and the Gig ports are trunking, per the topology diagram. Also port E0 on the Pix will be trunking.**

```
Sw1(config)#int range fa0/1 - 20
Sw1(config-if-range)#swit mode acc
Sw1(config-if-range)#swit noneg
```



```
Sw2(config)#int range fa0/1 , fa0/3 - 20
Sw2(config-if-range)#swit mode acc
Sw2(config-if-range)#swit noneg

Sw2(config)#int gi0/2
Sw2(config-if)#swit mode acc
Sw2(config-if)#swit noneg
```

- d) Configure Cat1 and Cat2 to add a dot1q tag to traffic in the native vlan. Configure any unused ports on Cat1 and Cat2 to use VLAN 37.

→ Check your topology diagram to see what ports are not in use.

```
Sw1(config)#vlan dot1q tag native
Sw2(config)#vlan dot1q tag native

Sw1(config)#int fa0/3
Sw1(config-if)#swit acc vl 37
Sw1(config-if)#int fa0/6
Sw1(config-if)#swit acc vl 37
```

- e) Configure VLAN 37 for DHCP snooping. Rate limit ports fa0/23 and Fa0/24 on switch 1 to 12 DHCP messages per second. A DHCP server will be added in the future on port Fa0/3 on switch 1, configure this port to be trusted.

→ DHCP snooping just needs to be enabled on the interface.

```
Sw1(config)#ip dhcp snooping
Sw1(config)#ip dhcp snooping vlan 37
Sw1(config-if)#int fa0/23
Sw1(config-if)#ip dhcp snooping limit rate 12
Sw1(config-if)#int fa0/24
Sw1(config-if)#ip dhcp snooping limit rate 12

Sw1(config)#int fa0/3
Sw1(config-if)#ip dhcp snooping trust
```

→ Verify with show ip dhcp snooping.

```
Sw1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
37
Insertion of option 82 is enabled
  circuit-id format: vlan-mod-port
  remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
```

Interface	Trusted	Rate limit (pps)
FastEthernet0/3	yes	unlimited
FastEthernet0/23	no	12
FastEthernet0/24	no	12

```
Sw1#
```


- f) Ports Fa0/1 to Fa0/20 on Cat1 should be configured to shut down the port, if a BPDU is received on the port.

→ **BPDUGuard can prevent the switch from accepting BPDUs on the port.**

```
Sw1(config)#int range fa0/1 - 20
Sw1(config-if-range)#spanning bpduguard enable
```

2 – Basic PIX Firewall (14 Points)

2.1 – PIX IP Address (4 Points)

- a) Create a Logical Interface off of E0 interface on the PIX.

```
pixfirewall(config)#int eth0.55
pixfirewall(config-subif)#vlan 55
pixfirewall(config-subif)#security 50
pixfirewall(config-subif)#nameif DMZ55
pixfirewall(config-subif)#ip address 192.168.5.10 255.255.255.0
```

- b) The logical interface should belong to VLAN 55.
- c) The Physical interface belongs to the outside VLAN. Assign the new VLAN interface a name of DMZ55 and a security level of 50.
- d) Configure the Switch to allow the PIX to communicate to the rest of the network.

→ **On the switch, the port needs to be able to pass traffic on more than one VLAN.**

- e) Assign IP Addresses to the PIX Interfaces.

```
pixfirewall(config)#int eth0
pixfirewall(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
pixfirewall(config-if)#ip address 192.1.12.10 255.255.255.0
pixfirewall(config-if)#no shut
pixfirewall(config-if)#int eth1
pixfirewall(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
pixfirewall(config-if)#ip address 10.2.2.10 255.255.255.0
pixfirewall(config-if)#no shut
```

2.2 – Routing (2 Points)

- a) Run OSPF as the routing protocol on the outside interface of the PIX Firewall.
- b) Configure Process ID 10 and advertise the outside network in area 0.

```
pixfirewall(config)#router ospf 10
pixfirewall(config-router)#network 192.1.12.0 255.255.255.0 area 0
```


- c) Configure static routes for the 10.1.1.0 and 1.0.0.0 networks on the PIX.

```
pixfirewall(config)#route inside 10.1.1.0 255.255.255.0 10.2.2.1
pixfirewall(config)#route inside 1.0.0.0 255.255.255.0 10.2.2.1
```

2.3 – Static Translation (3 Points)

- a) Allow all networks behind the PIX to get out with translation.

- b) Use PAT without using any unused address.

→ **NAT just requires a nat statement and a global statement. In order to not use any addresses, we can overload to the interface using the interface keyword.**

```
pixfirewall(config)#nat (inside) 1 0 0
pixfirewall(config)#nat (DMZ55) 1 0 0
pixfirewall(config)#global (outside) 1 interface
```

- c) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

→ **Configure an access list and apply to the interface. Configure a static translation for the ACS server. Make sure that your access list entries reference the translated address.**

```
pixfirewall(config)#static (inside,outside) 192.1.12.100
10.1.1.100 netmask 255.255.255.255
pixfirewall(config)#access-list outsideacl permit tcp host
4.4.4.4 host 192.1.12.100 eq 49
pixfirewall(config)#access-list outsideacl permit tcp host
192.1.12.2 host 192.1.12.100 eq 49
pixfirewall(config)#access-group outsideacl in interface outside
R4(config)#ip tacacs source-int lo0
```

- d) Create a Static entry for R1 F 0/0 at 10.2.2.1. Translate it to 192.1.12.15.

```
pixfirewall(config)#static (inside,outside) 192.1.12.15 10.2.2.1
netmask 255.255.255.255
```

2.4 – Advanced Filtering (3 Points)

- a) Configure URL Filtering on the PIX. The url server is a Web Sense server located at 10.2.2.52.

- b) Configure the PIX to point to the Web Sense server.

```
pixfirewall(config)#url-server (inside) host 10.2.2.52
pixfirewall(config)#filter url 80 0 0 0 0
```


2.5 – Authentication Proxy (2 points)

- a) Configure the PIX to perform proxy-authentication for telnet connections passing through the PIX. Use TACACS+ as the protocol. Configure the ACS server as needed.

→ On the PIX, configure the tacacs server and key.

```
pixfirewall(config)#aaa-server TAC protocol TACACS
pixfirewall(config-aaa-server-group)#exit
pixfirewall(config)#aaa-server TAC host 10.1.1.100
pixfirewall(config-aaa-server-host)#key pixkey
pixfirewall(config)#aaa authentication include telnet inside 0 0
0 0 TAC
```

→ On the ACS server, create a new user, and add the PIX as a network device. Since you are not given a specific username to use, choose one.

→ Test from R1, by telnetting to R2's address. You may need to add a static route to R1 pointing towards the PIX.

```
R1#telnet 192.1.12.2
Trying 192.1.12.2 ... Open
```

```
Username: pixuser
```

```
Password:
```

3 – ASA / PIX (12 Points)

3.1 – Transparent Firewall (4 points)

- Configure ASA1 as a transparent firewall for the VLANs between R4 and R9.
- Configure a management address of .55 for the subnet.
- Make sure that the routing protocol adjacencies between R4 and R9 form.
- Statically add the MAC addresses for R4 and R9 to the MAC address table on the ASA.
- Configure the timeout value for dynamic MAC address table entries to 15 minutes.

```
ciscoasa(config)#firewall transparent
```

→ Add the address, name the interfaces, and make sure they are enabled

```
ciscoasa(config)#ip address 192.1.49.55 255.255.255.0
```

```
ciscoasa(config)#int eth0/0
```

```
ciscoasa(config-if)#nameif outside
```

```
INFO: Security level for "outside" set to 0 by default.
```

```
ciscoasa(config-if)#no shut
```

```
ciscoasa(config-if)#int eth0/1
```

```
ciscoasa(config-if)#nameif inside
```

```
INFO: Security level for "inside" set to 100 by default.
```

```
ciscoasa(config-if)#no shut
```


→ **Configure the aging time and apply a hostname.**

```
ciscoasa(config)#mac-address-table aging-time 15
```

```
ciscoasa(config)#hostname ASA1
```

→ **For the routing protocols. OSPF is used, so we need to allow it in an access list. Apply the access list to the interfaces.**

```
ASA1(config)#access-list ALLOW permit ospf any any
```

```
ASA1(config)#access-list ALLOW permit icmp any any echo
```

```
ASA1(config)#access-list ALLOW permit icmp any any echo-reply
```

```
ASA1(config)#access-group ALLOW in interface outside
```

```
ASA1(config)#access-group ALLOW in interface inside
```

→ **Add the static MAC entries, and add a route for management traffic.**

```
ASA1(config)#mac-address-table static inside 0018.731d.bdf0
```

```
ASA1(config)#mac-address-table static outside 0012.8031.cd08
```

```
ASA1(config)#route outside 0 0 192.1.49.4
```

→ **Verify your routing protocol adjacency.**

```
R4#show ip ospf neigh
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
9.9.9.9	1	FULL/DR	00:00:39	192.1.49.9	FastEthernet0/0
2.2.2.2	0	FULL/ -	00:00:35	192.1.24.2	Serial0/0/0

```
R4#
```

3.2 – Transparent Firewall (4 Points)

- Configure ASA2 as a transparent firewall for the VLANs between R5 and BB2.
- Configure a management address of .55 for the subnet.
- Make sure that the routes are exchanged between R5 and BB2.
- Configure static ARP entries for the addresses of R5 and BB2 on the VLANs connected to the ASA.
- Configure ARP inspection for the inside and outside interfaces. Non-matching ARP packets should be dropped.

→ **Configure the firewall for transparent mode, also you should verify that you are in single context mode with the command show mode. For transparent firewall, the address is configured globally.**

```
ciscoasa#conf t
```

```
ASA2(config)#firewall transparent
```

```
ciscoasa(config)#ip address 10.5.5.55 255.255.255.0
```


→ **Configure an access list to apply to the interfaces.**

```
ciscoasa(config)#access-list ALLOW permit icmp any any echo
ciscoasa(config)#access-list ALLOW permit icmp any any echo-reply
ciscoasa(config)#access-list ALLOW permit eigrp any any
```

```
ciscoasa(config)#access-group ALLOW in interface inside
ciscoasa(config)#access-group ALLOW in interface outside
```

→ **Make sure your interface are not shut down, and have the names configured.**

```
ciscoasa(config)#int eth0/0
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#int eth0/1
ciscoasa(config-if)#no shut
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
```

→ **Configure hostname and a route for management traffic.**

```
ciscoasa(config)#hostname ASA2
ASA2(config)#route outside 0 0 10.5.5.5
```

→ **Configure ARP inspection for the interfaces and add static ARP entries for the addresses of the neighboring routers.**

```
ASA2(config)#arp-inspection inside enable no-flood
ASA2(config)#arp-inspection outside enable no-flood

ASA2(config)#arp outside 10.5.5.5 0012.8031.e118
ASA2(config)#arp inside 10.5.5.100 0003.6beb.1360
```

3.3 – Management (4 points)

- Configure ASA1 and ASA2 for management via SSH, using local authentication. Use a username of ipexpert and a password of ccie.
- SSH access should only be allowed from devices on VLAN 10, including R1.

→ **Configuring SSH support on the ASA just needs a few things:**

Username / Password
Configure network to allow SSH from
Configure authentication for SSH
Create key

```
ASA1(config)#username ipexpert password ccie

ASA1(config)#ssh 10.1.1.0 255.255.255.0 outside

ASA1(config)#aaa authentication ssh console LOCAL
```



```
SA1(config)#crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ASA1(config)#
```

```
ASA2(config)#username ipexpert password ccie
ASA2(config)#ssh 10.1.1.0 255.255.255.0 outside
ASA2(config)#aaa authentication ssh console LOCAL
```

```
ASA2(config)#crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ASA2(config)#
```

4 – IDS (17 Points)

4.1 – Basic Configuration of IDS through IDS, IDM and IEV (2 Points)

- a) Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.

→ Run setup from the CLI, and configure the IP address and default gateway. Configure the access list to permit the PC so that you have GUI access.

4.2 – Switch Configuration (2 Points)

- a) You would like to monitor all traffic between VLAN 12 connected to the outside of the PIX, and VLAN 102 connected to R2.

→ On the switch, verify that the sensor ports are in the correct VLANs.

```
Sw1(config)#int fa0/7
Sw1(config-if)#swit acc vlan 12
Sw1(config-if)#int fa0/17
Sw1(config-if)#swit access vlan 102
```

→ On the GUI, enable the ports F0/1 and F1/0 under interfaces and apply.

→ Under interface pairs, add the two interfaces and apply

→ Under Analysis Engine – Virtual Sensor – assign the pair to the virtual sensor.

→ Verify that you can pass traffic by pinging R2 from the PIX.

```
pixfirewall#ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
pixfirewall#
```


4.3 – Fine tuning the ICMP Signature (3 Points)

- a) Enable the ICMP Echo Request and ICMP Echo Reply Signatures.
- b) Set the Alarm Severity to Medium.
 - Under signature configuration, enable signatures 2000 and 2004, and set the severity to Medium.

4.4 – IP Blocking on the Router (6 Points)

- a) Configure the IDS Sensor to block the Connection if the ICMP Echo Request or Reply signature is detected
 - Right click on the signature, and select actions. Add block connection.
- b) The blocking should be done on the R2 S0/1/0.4 and R2 S0/1/0.5 sub-interfaces.
 - Under device login profiles, create a profile, and add the user ids.
- c) Configure the Router to allow the IDS Sensor to Telnet into it.
- d) Authenticate the Telnet connection locally. Create a username of ids with a password of ids.

```
R2(config)#username ids password ids
R2(config)#line vty 0 15
R2(config-line)#login local
R2(config)#enable password cisco
```

- e) Configure the Sensor with the appropriate information to Telnet into the R2.
 - Under blocking, blocking devices, configure the IP address and name for R2.
 - Under router blocking devices, add the interfaces for blocking.
- f) Set the Block time to 20 Minutes.
 - Under event action rules, General Settings, configure the block time.
- g) Sensor should be seen as 192.1.12.77 on the outside. IDS should not use the tunnel to connect to R2. You are allowed a static route to accomplish this step.
 - Add a static on the firewall to adjust how the address appears on the outside. Also, configure an exclusion from the proxy authentication configured earlier.

```
pixfirewall(config)#static (inside,outside) 192.1.12.77 10.1.1.15
netmask 255.255.255.255
pixfirewall(config)#aaa authentication exclude telnet inside
10.1.1.15 255.255.255.255 192.1.12.2 255.255.255.255 TAC
```


- h) The sensor should never block itself. Make sure the entry in the access list reflects the correct IP address for the Sensor.

→ **Under Blocking, Blocking properties, add the translated address to the sensor to the list of never block addresses.**

4.5 - IDS tuning (4 points)

- a) Configure the maximum number of open log files on the sensor to 21.

→ **Under analysis engine – global variables, adjust the max number of open log files from the default of 20. This will require a reboot to take effect.**

- b) The sensor should be able to ping R1 and get 100% response. If R1 pings the sensor command interface, it should receive 0% response. This task should be configured on the IDS sensor.

→ **The sensor will not respond to pings unless the address is in the access list. If you configured the access list as a /32 for the PC, there is nothing to configure here. If you allowed the entire /24 network, then you need to adjust your ACL.**

- c) Configure the SNMP Read-only community as ipexpert. Configure the read-write community as not4u!

→ **SNMP configuration is under SNMP – General Configuration**

- d) Configure the sensor to issue a status event if more than 5 percent of packets are missed over a 60 second interval. The sensor should also issue a status event if the interface does not receive packets for a 5 minute time period.

→ **The threshold for missed traffic is under Interface Configuration – Traffic Flow Notifications.**

5 – Access Management (6 Points)

5.1 – Configuring AAA Authentication on Switch 1 for Telnet Management (4 Points)

- a) Configure Switch 1 with AAA access using TACACS+. The secret key is ccie. Configure the switch with a default route to communicate to the AAA server. Allow the appropriate entries in the access list of the PIX. You are allowed a static route to make this work.

```
Sw1(config)#ip route 0.0.0.0 0.0.0.0 192.1.6.6
```

```
Sw1(config)#aaa new-model
```

```
Sw1(config)#tacacs host 192.1.12.100 key ccie
```

```
pixfirewall(config)#access-list outsideacl permit tcp host  
192.1.6.20 host 192.1.12.100 eq tacacs
```



```
Sw1(config)#aaa authentication login default none
Sw1(config)#aaa authentication login VTY group tacacs
Sw1(config)#line vty 0 15
Sw1(config-line)#login authentic VTY

Sw1(config)#enable password cisco
```

b) No Authentication should be done on the Console or AUX lines.

→ By setting the default method to none, console and AUX will not be affected.

c) Setup Authentication based on TACACS+ for the VTY lines.

→ This was accomplished by assigning the VTY method to the vty lines.

d) Create 2 users on the AAA server, User 1 and User2. Both the users have cisco as their password.

→ Add the two users on the AAA server under User setup. Add the switch as a device under network configuration.

→ Verify that you have IP connectivity by pinging the address of the switch from the ACS server. You may need to allow the return ICMP through the PIX if you want to test this connectivity.

5.2 –Controlled Telnet Access (2 Points)

a) You want User1 and User2 to have full privilege on the router. When User1 and User2 login, they should be in Privilege Exec mode.

→ You can either configure the authorization locally or via the TACACS+ server.

→ Under Interface Configuration, TACACS, select shell under the user column to allow user specific options.

→ Select Shell, and set the privilege level to 15 for the users, under User setup.

→ On the switch, configure

```
Sw1(config)#aaa authorization exec VTY group tacacs
Sw1(config)#line vty 0 15
Sw1(config-line)#authoriz exec VTY
```

→ Verify by telnetting from R6.

```
R6#telnet 192.1.6.20
Trying 192.1.6.20 ... Open
```

```
Username: user1
Password:
```



```
Sw1#show priv
Current privilege level is 15
Sw1#
```

- b) You would like to reserve the last telnet line for yourself. Do this by changing the default port to 3099.

```
Sw1(config)#line vty 15
Sw1(config-line)#rotary 99
```

- c) Disable the telnet client on the switch.

```
Sw1(config)#line vty 0 15
Sw1(config-line)#transport output none
Sw1(config)#line con 0
Sw1(config-line)#transport output none
```

→ If you try to telnet from the router you should receive an error message.

```
Sw1#telnet 1.1.1.1
% telnet connections not permitted from this terminal
Sw1
```

6 – IP Services (5 Points)

6.1 – NAT on R5 (3 Points)

- a) Configure NAT such that if F0/0 network wants to go to 1.0.0.0, 4.0.0.0 or 9.0.0.0 networks, it should use the interface IP address of the S0/1/0 interface as the translated address. Configure PAT for this entry.

```
R5(config)#int fa0/0
R5(config-if)#ip nat inside
R5(config-if)#int ser0/1/0
R5(config-if)#ip nat outside

R5(config)#access-list 161 permit ip 10.5.5.0 0.0.0.255 1.0.0.0
0.255.255.255
R5(config)#access-list 161 permit ip 10.5.5.0 0.0.0.255 4.0.0.0
0.255.255.255
R5(config)#access-list 161 permit ip 10.5.5.0 0.0.0.255 9.0.0.0
0.255.255.255

R5(config)#ip nat inside source list 161 int ser0/1/0 overload
```


- b) Configure NAT such that if F0/0 network wants to go to 2.0.0.0 or 6.0.0.0 networks, it should use a pool of 192.1.25.151 – 192.1.25.199 as the translated address.

```
R5(config)#access-list 162 permit ip 10.5.5.0 0.0.0.255 2.0.0.0
4.255.255.255
R5(config)#ip nat pool SECTION61 192.1.25.151 192.1.25.199
prefix-length 24
R5(config)#ip nat inside source list 162 pool SECTION61 overload
```

- Verify by enabling debug ip nat while pinging with a source of the fa0/0 network.

```
R5#ping 9.9.9.9 source 10.5.5.5
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
Packet sent with a source address of 10.5.5.5
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/87/88 ms
R5#
*Jan  9 02:13:01.142: NAT: s=10.5.5.5->192.1.25.5, d=9.9.9.9 [30]
*Jan  9 02:13:01.226: NAT*: s=9.9.9.9, d=192.1.25.5->10.5.5.5 [30]
*Jan  9 02:13:01.230: NAT: s=10.5.5.5->192.1.25.5, d=9.9.9.9 [31]
*Jan  9 02:13:01.314: NAT*: s=9.9.9.9, d=192.1.25.5->10.5.5.5 [31]
*Jan  9 02:13:01.314: NAT: s=10.5.5.5->192.1.25.5, d=9.9.9.9 [32]
*Jan  9 02:13:01.402: NAT*: s=9.9.9.9, d=192.1.25.5->10.5.5.5 [32]
```

- c) There is a Web Server at 10.5.5.80. The Web server should be seen as 192.1.25.80.

```
R5(config)#ip nat inside source static 10.5.5.80 192.1.25.80
```

6.2 – SNMP Configuration on R2 (2 Points)

- a) Configure R2 to allow the management station at 192.1.12.30 to manage R2.
b) Configure the Read-only community as CCIERO and Read-write community as CCIERW.

```
R2(config)#access-list 62 permit 192.1.12.30

R2(config)#snmp-server community CCIERO ro
R2(config)#snmp-server community CCIERW rw 62

R2(config)#snmp-server host 192.1.12.30 CCIERW
```

7 – Virtual Private Networks (22 Points)

7.1 – Basic Concentrator Configuration (4 Points)

- a) Configure the IP Address on the Private and Public Interfaces.

- Configure the addresses through the CLI.

- b) Do not configure any static routes for the 10.1.1.0 network on the Concentrator.
- c) Management of the Concentrator should be done thru the Public interface.
- d) Configure the PIX firewall to allow traffic from the Management PC at 10.1.1.100 to communicate to the Concentrator from the Public Interface. You are allowed a static route on R1 to accomplish this.

→ **R1 does not know about the network 192.168.5.0. Configure a static route pointing to the PIX, so that R1 can reach the Concentrator. On the PIX, configure NAT to translate traffic from the inside network to the DMZ.**

```
R1(config)#ip route 192.168.5.0 255.255.255.0 10.2.2.10
```

```
pixfirewall(config)#global (DMZ55) 1 interface
```

- e) Configure the Concentrator such that it allows management from the Public Interface.

→ **On the concentrator, enable management from the public interface.**

Configuration - interface - public interface - WebVPN parameters - HTTP/ HTTPS Management – Enable

→ **You may need to add a route on the PC so that it has a route to the concentrator as well.**

```
C:\ >route add 192.168.5.0 mask 255.255.255.0 10.1.1.1
```

- f) Disable RIP on the concentrator and configure a default gateway pointing towards the PIX.

→ **Disabling RIP is accomplished under interface config.**

Interface configuration – private interface – set port routing config – set inbound RIP options – disable inbound.

→ **Configuring a gateway is under System management**

System management – ip routing – default gateways – set default gateway

→ **Verify that you can connect to the concentrator from the management PC.**

7.2 – Setup a Site-to-Site IPSec VPN between the Concentrator and R5 (4 Points)

- a) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- For IPSec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.

- Add a new Lan to Lan under configuration – tunneling and security – IPSec – LAN to LAN

Enter the Peer ID 192.1.25.5
 Enter the preshared key ccie
 Authentication for ipsec is esp/sha/hmac
 Encryption is DES
 IKE Proposal is IKE-DES-MD5
 Enable IPSec NAT-T
 Configure the local network as 10.2.2.0 with a wildcard mask of 0.0.0.255
 Configure the remote network as 10.5.5.0 with a wildcard mask of 0.0.0.255

- On R5 – start with a crypto key and isakmp policy:

```
R5(config)#crypto isakmp key 0 ccie address 192.1.12.5
```

```
R5(config)#crypto isak policy 10
R5(config-isakmp)#hash md5
R5(config-isakmp)#authent pre-share
```

- Add a transform and access list, and configure the crypto MAP. Apply the map to the interface.

```
R5(config)#crypto ipsec transform-set R5CONC esp-des esp-sha-hmac

R5(config)#access-list 151 permit ip 10.5.5.0 0.0.0.255 10.2.2.0
0.0.0.255
```

```
R5(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R5(config-crypto-map)#set peer 192.1.12.5
R5(config-crypto-map)#set transform R5CONC
R5(config-crypto-map)#match address 151

R5(config)#int ser0/1/0
R5(config-if)#crypto map MYMAP
```

- b) You can use static routes on R5 and R1 to accomplish this.

- R5 needs a static for the 10.2.2.0 network pointing out the serial interface.
- R1 needs a static for the 10.5.5.0 network pointing to the concentrator.

```
R5(config)#ip route 10.2.2.0 255.255.255.0 192.1.25.2
R1(config)#ip route 10.5.5.0 255.255.255.0 10.2.2.5
```

- c) The concentrator is seen on the outside as 192.1.12.5. Configure the PIX to translate the concentrator and allow appropriate entries for the IPSec traffic from R5 to the concentrator.

```
pixfirewall(config)#static (DMZ55,outside) 192.1.12.5 192.168.5.5
netmask 255.255.255.255
pixfirewall(config)#access-list outsideacl permit udp host
192.1.25.5 eq 4500 host 192.1.12.5 eq 4500
```



```

pixfirewall(config)#access-list outsideacl permit udp host
192.1.25.5 eq 500 host 192.1.12.5 eq 500
pixfirewall(config)#access-list dmzacl permit esp host
192.168.5.5 host 192.1.25.5
pixfirewall(config)#access-list dmzacl permit udp host
192.168.5.5 host 192.1.25.5 eq 500

```

```
R5#ping 10.2.2.1 source 10.5.5.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:

Packet sent with a source address of 10.5.5.5

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 88/88/88 ms

```
R5#
```

```
R5#show cry ipsec sa
```

```
interface: Serial0/1/0
```

```
  Crypto map tag: MYMAP, local addr 192.1.25.5
```

```
  protected vrf: (none)
```

```
  local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
```

```
  remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
```

```
  current_peer 192.1.12.5 port 500
```

```
    PERMIT, flags={origin_is_acl,}
```

```
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
```

```
    #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
```

7.3 – Setup a Remote Access VPN between the Concentrator and the Cisco Secure Client using External Authentication (4 Points)

a) Use the following parameters to setup Concentrator with the following options:

- Assign IP Address in the range of 10.3.3.1 – 10.3.3.254. The pool should be created specific to the group **Remote**.
- Create a group called Remote with a password of **ccie**.
- The group should do authentication based on a RADIUS server located at 10.2.2.99. It communicates to the Concentrator using Port 1812 for Authentication and 1813 for Accounting. The secret key is **Ripexpert**.
- Only allow PPTP and IPSec for the group. Configure it such that only MSCHAP V2 is allowed as the authentication protocol for PPTP.
- **Configuration – User Management – Base Group – select MSCHAPv2 as an available protocol.**
- **Add the group Remote – configuration – user management – groups – add group**
- **Under the General Tab for the group, unselect L2TP and WebVPN**
- **Under IPSec, select RADIUS for authentication.**
- **Add a Radius server under configuration – system – servers – authentication**

Enter 10.2.2.99 as the IP address and 1812 as the server port.

Enter a server secret of Ripexpert

- On the ACS server, add a AAA client for the VPN Concentrator, using the host address 10.2.2.5.
- On R1, configure address translation for the RADIUS requests.

```
R1(config)#int fa0/1
R1(config-if)#ip nat inside
```

```
R1(config-if)#int fa0/0
R1(config-if)#ip nat outside
```

```
R1(config)#ip nat inside source static udp 10.1.1.100 1645
10.2.2.99 1812
```

```
R1(config)#ip nat inside source static udp 10.1.1.100 1646
10.2.2.99 1813
```

- Make sure that you also allow address assignment. – Configuration – system – address management – assignment – Use address pools.
- Enable traffic to reach the concentrator.

```
pixfirewall(config)#access-list outsideacl permit esp any host
192.1.12.5
```

```
pixfirewall(config)#access-list outsideacl permit udp any eq 500
host 192.1.12.5 eq 500
```

```
pixfirewall(config)#access-list dmzacl permit esp host
192.168.5.5 any
```

```
pixfirewall(config)#access-list dmzacl permit udp host
192.168.5.5 eq 500 any
```

7.4 – Setup a Site-to-Site IPSec VPN between the PIX and R4 (4 Points)

- a) Create the following loopback on R4:

- R4 - Int loop 10 : 192.168.104.4/24

```
R4(config)#int loop10
R4(config-if)#ip address 192.168.104.4 255.255.255.0
```

- b) Encrypt traffic between the 192.168.104.0/24 and 10.2.2.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**
- Use MD5 for the Hashing algorithm and Group 2 for the Diffie-Hellman key exchange. Use defaults for the rest of the ISAKMP parameters
- For IPSec, use ESP-DES for encryption and ESP-MD5-HMAC for Data Authentication in Tunnel Mode

- c) Use the PIX outside and R4 S 0/0 as the Tunnel Endpoints.

- d) You are allowed a static route on the PIX, R1 and R4.


```

pixfirewall(config)#tunnel-group 192.1.24.4 type ipsec-l2l
pixfirewall(config)#tunnel-group 192.1.24.4 ipsec-attributes
pixfirewall(config-tunnel-ipsec)#pre-shared-key ccie

pixfirewall(config)#access-list R4L2L extended permit ip 10.2.2.0
255.255.255 192.168.104.0 255.255.255.0
pixfirewall(config)#crypto isakmp pol 10
pixfirewall(config-isakmp-policy)#auth pre-share
pixfirewall(config-isakmp-policy)#encr des
pixfirewall(config-isakmp-policy)#hash md5
pixfirewall(config-isakmp-policy)#group 2
pixfirewall(config)#crypto isakmp enable outside
pixfirewall(config)#crypto ipsec transform MYTRANS esp-des esp-
md5-hmac
pixfirewall(config)#crypto map MYMAP 10 match address R4L2L
pixfirewall(config)#crypto map MYMAP 10 set transform MYTRANS
pixfirewall(config)#crypto map MYMAP 10 set peer 192.1.24.4
pixfirewall(config)#crypto map MYMAP interface outside

pixfirewall(config)#route outside 192.168.104.0 255.255.255.0
192.1.12.2

R1(config)#ip route 192.168.104.0 255.255.255.0 10.2.2.10

R4(config)#crypto ipsec transform-set PIXL2L esp-des esp-md5-hmac

R4(config)#crypto isakmp pol 10
R4(config-isakmp)#hash md5
R4(config-isakmp)#auth pre-share
R4(config-isakmp)#group 2
R4(config)#crypto isakmp key 0 ccie address 192.1.12.10
R4(config)#ip access-list ext PIXL2L
R4(config-ext-nacl)#permit ip 192.168.104.0 0.0.0.255 10.2.2.0
0.0.0.255
R4(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R4(config-crypto-map)#set peer 192.1.12.10
R4(config-crypto-map)#set transform PIXL2L
R4(config-crypto-map)#match address PIXL2L
R4(config)#int ser0/0/0
R4(config-if)#crypto map MYMAP

```

→ At this point, pings will fail, when testing from R4.

```
R4#ping 10.2.2.1 source 1010
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.104.4
.....
Success rate is 0 percent (0/5)

```


- Take a look at the crypto to see why. ISAKMP looks OK, and shows QM_IDLE.

```
R4#show cry isak sa
dst          src          state          conn-id slot status
192.1.12.10  192.1.24.4  QM_IDLE          1      0 ACTIVE
```

- IPsec shows traffic encapsulated, but not decapsulated. Something is blocking the return traffic.

```
R4#show cry ipsec sa

interface: Serial0/0/0
  Crypto map tag: MYMAP, local addr 192.1.24.4

  protected vrf: (none)
  local ident (addr/mask/prot/port): (192.168.104.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
  current_peer 192.1.12.10 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 192.1.24.4, remote crypto endpt.: 192.1.12.10
    path mtu 1500, ip mtu 1500
    current outbound spi: 0x58474BFD(1481067517)
```

- Earlier, NAT was configured for all traffic from the inside interface. Since we want this traffic to keep the same address, we can bypass nat for the lan to lan traffic on the PIX, using NAT 0.

```
pixfirewall(config)#access-list NONAT permit ip 10.2.2.0
255.255.255.0 192.168.104.0 255.255.255.0
pixfirewall(config)#nat (inside) 0 access-list NONAT
```

- Ping again, and you can see the ping is successful.

```
R4#ping 10.2.2.1 source 10.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.104.4
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 132/162/172
ms
R4#
```

7.5 – QoS on the VPN Concentrator (3 Points)

- a) Create a bandwidth policy for the public interface giving it minimum of 1 Mbps and a maximum of 100 Mbps. Assign a burst of 16000 bytes.

- b) You want to limit the amount of bandwidth allocated to the LAN to LAN tunnel between the Concentrator and R5 based on the following:

- Minimum Bandwidth allocated – 1 Mbps
- Maximum Bandwidth allowed – 3 Mbps
- Burst – 16000 bytes

Configuration – Policy Management – Traffic Management- BW Policies – add

- **Configure minimum bandwidth of 1000kbps, policing of 100000kbps, and normal burst size of 16000.**
- **Select interfaces – public – bandwidth tab.**

**Enable bandwidth management by the checkbox.
Set the link rate to 100000 kbps
Apply the named policy that you just configured.**

7.6 – Management VPN (3 points)

- a) Configure a secure method of management for configuring ASA1.
 - b) Configure a secure method of management for configuring ASA2.
 - c) R1 should be able to connect to ASA1 and ASA2, and the traffic should not be sent in cleartext.
- **For the most part, this section is just configuring two lan to lan VPNs, and configuring R1 as an SSH client**
 - **R1's configuration for ISAKMP and crypto is straightforward.**

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#hash md5
R1(config-isakmp)#encr 3des
R1(config-isakmp)#authent pre-share
R1(config-isakmp)#exit
R1(config)#crypto isakmp key 0 ccie address 192.1.49.55
R1(config)#crypto isakmp key 0 ccie address 10.5.5.55
R1(config)#crypto ipsec transform-set ASA esp-3des esp-sha-hmac
R1(config)#ip access-list extended ASA1
R1(config-ext-nacl)#permit ip 10.1.1.0 0.0.0.255 host 192.1.49.55
R1(config)#ip access-list extended ASA2
R1(config-ext-nacl)#permit ip host 10.1.1.0 0.0.0.255 host
10.5.5.55
```

- **Configure two MAP clauses, one for each firewall, and apply the MAP to the interface.**

```
R1(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 192.1.49.55
R1(config-crypto-map)#set transform ASA
R1(config-crypto-map)#match address ASA1
R1(config)#crypto map MYMAP 20 ipsec-isakmp
```


% NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.

```
R1(config-crypto-map)#set peer 10.5.5.55
R1(config-crypto-map)#set transform ASA
R1(config-crypto-map)#match address ASA2
R1(config)#int fa0/0
R1(config-if)#crypto map MYMAP
```

- On ASA1, the termination point used will be R1's Fa0/0 interface, which has an existing NAT to 192.1.12.15 on the PIX.

```
ASA1(config)#tunnel-group 192.1.12.15 type ipsec-l2l
ASA1(config)#tunnel-group 192.1.12.15 ipsec-attributes
ASA1(config-tunnel-ipsec)#pre-shared-key ccie
ASA1(config)#crypto ipsec transform MYTRANS esp-3des esp-sha-hmac
ASA1(config)#access-list L2L permit ip host 192.1.49.55 10.1.1.0
255.255.255.0
ASA1(config)#crypto map MYMAP 10 match address L2L
ASA1(config)#crypto map MYMAP 10 set peer 192.1.12.15
ASA1(config)#crypto map MYMAP 10 set transform MYTRANS
ASA1(config)#crypto map MYMAP interface outside
ASA1(config)#crypt isakmp enable outside
ASA1(config)#crypto isak pol 10
ASA1(config-isakmp-policy)#hash md5
ASA1(config-isakmp-policy)#encr 3des
ASA1(config-isakmp-policy)#authent pre-share
```

- On R1, configure a domain name and generate keys for SSH:

```
R1(config)#ip domain name ipexpert.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ipexpert.com
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.
```

```
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#ip ssh source-in fa0/1
```

- On R2, there is an existing VPN connecting 10.2.2.0/24 and 10.5.5.0/24, so ASA2 will use the original address of R1's FA0/0 interface.

```
ASA2(config)#tunnel-group 10.2.2.1 type ipsec-l2l
ASA2(config)#tunnel-group 10.2.2.1 ipsec-attrib
ASA2(config-tunnel-ipsec)#pre-shared-key ccie

ASA2(config)#crypto ipsec transform MYTRANS esp-3des esp-sha-hmac
ASA2(config)#access-list L2L permit ip host 10.5.5.55 10.1.1.0
255.255.255.0

ASA2(config)#crypto map MYMAP 10 match address L2L
ASA2(config)#crypto map MYMAP 10 set peer 10.2.2.1
ASA2(config)#crypto map MYMAP 10 set transform MYTRANS
ASA2(config)#crypto map MYMAP interface outside
```



```
ASA2 (config)#crypto isakmp enable outside
```

```
ASA2 (config)#crypt isak pol 10
```

```
ASA2 (config-isakmp-policy)#authent pre-share
```

```
ASA2 (config-isakmp-policy)#encr 3des
```

```
ASA2 (config-isakmp-policy)#hash md5
```

→ **Verify that R1 can connect to ASA1 and ASA2.**

```
R1#ssh -l ipexpert 192.1.49.55
```

Password:

Type help or '?' for a list of available commands.

```
ASA1> exit
```

Logoff

[Connection to 192.1.49.55 closed by foreign host]

```
R1#ssh -l ipexpert 10.5.5.55
```

Password:

Type help or '?' for a list of available commands.

```
ASA2>
```

8 – IOS Firewall (5 Points)

8.1 – Cisco IOS Firewall on R4 with non-standard ports (5 Points)

a) Inspect the following traffic from the Ethernet segment going towards the Frame networks:

- All TCP Based traffic
- All UDP Based traffic
- Netmeeting Traffic
- SMTP traffic should be inspected so that only a limited number of SMTP commands are allowed in

b) FTP should be inspected on the Standard port and also on port 2021.

c) HTTP should also be inspected for a non-standard port of 8000.

d) Only allow Java applets from 2.0.0.0 to be downloaded.

```
R4 (config)#ip inspect name MYFW tcp
```

```
R4 (config)#ip inspect name MYFW udp
```

```
R4 (config)#ip inspect name MYFW ftp
```

```
R4 (config)#access-list 81 permit 2.0.0.0
```

```
R4 (config)#ip inspect name MYFW http java-list 81
```

```
R4 (config)#ip inspect name MYFW smtp
```

```
R4 (config)#ip port-map ftp port 2021
```

```
R4 (config)#ip port-map HTTP port 8000
```


- e) Only allow relevant traffic coming in.

→ Go back through the entire lab carefully to determine what traffic is necessary.

```
R4(config)#access-list 181 permit ospf host 192.1.24.2 host 224.0.0.5
R4(config)#access-list 181 permit esp host 192.1.12.10 host 192.1.24.4
R4(config)#access-list 181 permit udp host 192.1.12.10 eq 500 host 192.1.24.4 eq 500
R4(config)#access-list 181 permit esp host 192.1.12.15 host 192.1.49.55
R4(config)#access-list 181 permit udp host 192.1.12.15 eq 500 host 192.1.49.55 eq 500
R4(config)#access-list 181 permit tcp host 192.1.12.100 host 4.4.4.4 eq 49
```

- f) ACL should be set to inbound on the Serial interface.

```
R4(config)#int ser0/0/0
R4(config-if)#ip access-group 181 in
R4(config-if)#ip inspect MYFW out
```

9 – Advanced Security and Attacks (12 Points)

9.1 – ICMP (4 Points)

- a) Only R2 F 1/0 should be allowed to ping the outside interface of the PIX.
- b) Also allow R4 S0/0.0 and R5 S0/1/0 to ping the PIX outside interface.

```
pixfirewall(config)#icmp permit 0 0 inside
pixfirewall(config)#icmp permit 0 0 DMZ55
pixfirewall(config)#icmp permit 192.1.12.2 255.255.255.255 outside
pixfirewall(config)#icmp permit 192.1.25.5 255.255.255.255 outside
pixfirewall(config)#icmp permit 192.1.24.4 255.255.255.255 outside
```

→ On the IDS, under Event Action Rules, Event Action filters, add two filters to allow R4 S0/0/0 and R5 S0/1/0 to ping the PIX without being blocked.

- c) Deny any non-initial ICMP fragments entering R4's Ethernet interface. Other traffic should not be affected.

```
R4(config)#access-list 191 deny icmp any any fragments
R4(config)#access-list 191 permit ip any any
R4(config)#int fa0/0
R4(config-if)#ip access-group 191 in
```


- d) Disable ICMP unreachable on R2 and R6.

```
R2(config)#int fa1/0
R2(config-if)#no ip unreachable
R2(config-if)#int ser0/1/0.4
R2(config-subif)#no ip unreachable
R2(config-subif)#int null0
R2(config-if)#no ip unreachable
R2(config-if)#int ser0/1/0.5
R2(config-subif)#no ip unreachable
R2(config-subif)#int ser0/1/0.6
R2(config-subif)#no ip unreachable
R2(config-subif)#int lo0
R2(config-if)#no ip unreachable
```

```
R6(config)#int loop0
R6(config-if)#no ip unreachable
R6(config-if)#int lo16
R6(config-if)#no ip unreachable
R6(config-if)#int fa0/0
R6(config-if)#no ip unreachable
R6(config-if)#int ser0/1/0
R6(config-if)#no ip unreachable
R6(config-if)#int null0
R6(config-if)#no ip unreachable
```

9.2 – Preventing the Nimda attack (3 Points)

- R6 is experiencing the Nimda attack from the Frame Cloud.
- Classify the attack on the outside interfaces.
- Drop the packets using an ACL on the Inside interface.

→ **Nimda is an attack against certain web servers.**

```
R6(config)#class-map match-any nimda
R6(config-cmap)#match protocol http url "*.ida*"
R6(config-cmap)#match protocol http url "*cmd.exe*"
R6(config-cmap)#match protocol http url "*root.exe*"
R6(config-cmap)#match protocol http url "*readme.eml*"
R6(config-cmap)#policy-map mark-nimda
R6(config-pmap)#class nimda
R6(config-pmap-c)#set ip dscp 1
R6(config)#access-list 192 deny ip any any dscp 1
R6(config)#access-list 192 permit ip any any

R6(config)#int ser0/1/0
R6(config-if)#service-policy input mark-nimda
R6(config-if)#int fa0/0
R6(config-if)#ip access-group 192 out
```


9.3 – Preventing the W32.Blaster Worm attack (2 Points)

- a) R9 is experiencing the W32.Blaster worm attack on the Ethernet link.
- b) Use ACL to block this attack.

→ Blaster predominantly uses ports TCP/UDP 135, UDP port 69, and TCP port 4444.

9.4 – Preventing the Smurf and Fraggle attacks (3 Points)

- a) R9 is experiencing the smurf and fraggle attacks from the Ethernet link.
- b) Use a Named ACL to block the attack.
- c) Allow all other traffic coming in.

→ Smurf attacks are mainly ICMP echo and echo-reply traffic. By blocking echo and echo reply traffic, you will be unable to ping the router.

→ Fraggle attacks are similar, but use UDP echo.

```
R9(config)#ip access-list extended SECT93
R9(config-ext-nacl)#deny tcp any any eq 135
R9(config-ext-nacl)#deny udp any any eq 135
R9(config-ext-nacl)#deny tcp any any eq 4444
R9(config-ext-nacl)#deny udp any any eq tftp
R9(config-ext-nacl)#deny udp any eq echo any
R9(config-ext-nacl)#deny udp any any eq echo
R9(config-ext-nacl)#deny icmp any any echo
R9(config-ext-nacl)#deny icmp any any echo-reply
R9(config-ext-nacl)#permit ip any any
R9(config)#int fa0/0
R9(config-if)#ip access-group SECT93 in
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

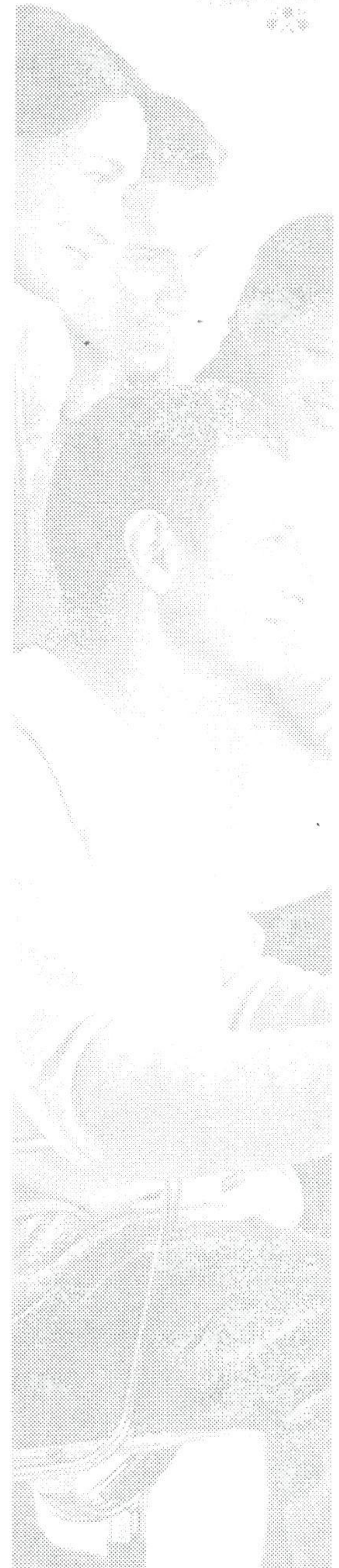
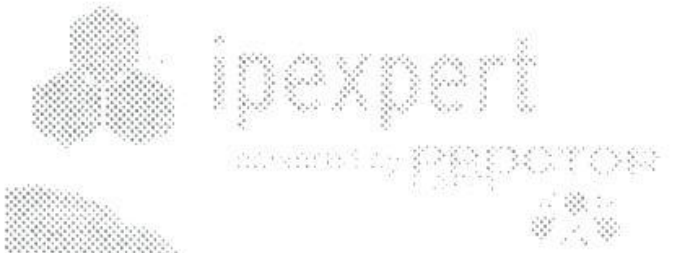
- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 16: Multiprotocol Challenge E One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 16 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the "Initial Configurations" subfolder within each section (*i.e. IPexpert CCIE Security 4.0 WB Configs → Section 16 → Initial Configurations → Router X.txt.*). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

1 – Layer 2 (5 Points)

1.1 – Switch Management (2 Points)

- a) Create a Management interface on Switch1 belonging to VLAN 6.
- b) Set the IP Address as .20 on that network.
- c) Allow management access to this switch from VLAN 6 only.

```
Cat1(config)#int vlan6
Cat1(config-if)#ip address 192.1.6.20 255.255.255.0

Cat1(config)#line vty 0 15
Cat1(config-line)#access-class 23 in
```

1.2 – Port Security (3 Points)

- a) Configure Port F 0/19 on Switch 1 for Dot1x authentication.
- b) Any device that connects to Port F 0/19 should be authenticated by a RADIUS server located at 192.1.12.100. Configure the firewall for the translation and access list accordingly.
- c) The RADIUS server uses ipexpert as the key and 1645 as the Authentication port.
- d) The Switch should re-authenticate every 2 hours.
- e) This port is connected to a hub. Once a port on that hub authenticates, all devices should be allowed.

```
Cat1(config)#aaa new-model
Cat1(config)#aaa authentication dot1x default group radius
Cat1(config)#radius-server host 192.1.12.100 key ipexpert
Cat1(config)#dot1x system-auth-control
Cat1(config)#int fa0/19
Cat1(config-if)#swit mode acc
Cat1(config-if)#dot1x port-control auto
Cat1(config-if)#dot1x host-mode multi
Cat1(config-if)#dot1x timeout reauth-period 7200
Cat1(config-if)#dot1x reauth
```


- **Configure R1 with a static for the 192.1.6.0 network pointing at the PIX. Configure Cat1 with a static route pointing at R6.**

```
R1(config)#ip route 192.1.6.0 255.255.255.0 10.2.2.10
```

```
Cat1(config)#ip route 0.0.0.0 0.0.0.0 192.1.6.6
```

- **On the ACS server, configure the Switch as a network device, and add a user to test. You will not be able to test this until you have routing connectivity, and the firewall is configured for the translation. Make sure to come back and test this section after you have connectivity.**
- **VLAN assignment information is not given. If it was specified what VLAN the Radius server was handing out, you would need to assign the attributes 64, 65, and 81 to VLAN, 802, and the VLAN name.**

```
Cat1#test aaa group radius user1 cisco legacy
```

```
Attempting authentication test to server-group radius using radius
```

```
User was successfully authenticated.
```

2 – Basic PIX Firewall (20 Points)

2.1 – PIX IP Address (4 Points)

- Create a Subinterface off of E0/0 interface on the ASA1, 0/0.55.
- The interface should belong to VLAN 55.
- The main interface belongs to the outside VLAN. Assign the new subinterface a name of DMZ55 and a security level of 50.

```
ciscoasa(config)#int eth0/0.55
ciscoasa(config-subif)#vlan 55
ciscoasa(config-subif)#nameif DMZ55
INFO: Security level for "DMZ55" set to 0 by default.
ciscoasa(config-subif)#security 50
ciscoasa(config-subif)#ip address 192.168.5.10 255.255.255.0
```

- Configure the switch to allow the ASA1 to communicate to the rest of the network.

- **The switch needs to be configured to allow traffic for both VLANs on the same port.**

```
Cat3(config-if)#int fa0/10
Cat3(config-if)#swit trunk encap dot1q
Cat3(config-if)#swit trunk native vlan 12
Cat3(config-if)#swit mode trunk
```

```
Cat4(config)#int fa0/10
Cat4(config-if)#swit trunk encap dot1q
Cat4(config-if)#swit trunk native vlan 12
Cat4(config-if)#swit mode trunk
```


- e) Assign IP Addresses to the ASA1 Interfaces.

```
ciscoasa(config)#int eth0/0
ciscoasa(config-if)#ip address 192.1.12.10 255.255.255.0
ciscoasa(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)#no shut
ciscoasa(config-if)#int eth0/1
ciscoasa(config-if)#ip address 10.2.2.10 255.255.255.0
ciscoasa(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)#no shut
```

2.2 – Routing (2 Points)

- a) Configure a default route on the ASA1 pointing towards R2.
b) Configure a static route for the network behind R1.

```
ciscoasa(config)#route outside 0 0 192.1.12.2
ciscoasa(config)#route inside 10.1.1.0 255.255.255.0 10.2.2.1
```

2.3 – Static Translation (4 Points)

- a) Configure a Loopback 125 on R1. It should be assigned an IP Address of 195.1.1.1/24. This is a network with a public address. Create a static route on R1 for the 192.1.12.0 network towards the ASA.

```
R1(config)#int loop125
R1(config-if)#ip address 195.1.1.1 255.255.255.0
R1(config-if)#ip route 192.1.12.0 255.255.255.0 10.2.2.10
```

- b) Allow this network to go out without getting translated. You cannot use the static command to accomplish this.
c) R2 should be able to ping this network. You are allowed a static route on R2 and the PIX to accomplish this step.

```
ciscoasa(config)#route inside 195.1.1.0 255.255.255.0 10.2.2.1
ciscoasa(config)#access-list outacl permit icmp any any echo
ciscoasa(config)#access-list outacl permit icmp any any echo-reply
ciscoasa(config)#access-group outacl in interface outside

R2(config)#ip route 195.1.1.0 255.255.255.0 192.1.12.10
```


- **Note: R2 will not be able to ping this network until after section 2.6 is completed. Verify after you have 2.6 completed.**

```
R2#ping 195.1.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 195.1.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
R2#
```

- d) Create a Static entry for the AAA server at 10.1.1.100. Translate it to 192.1.12.100. Allow R4 Loopback 0 to communicate to the TACACS+ server. Also allow R2 F 1/0 interface to communicate to the TACACS+ server.

```
ciscoasa(config)#hostname ASA1
ASA1(config)#static (inside,outside) 192.1.12.100 10.1.1.100
netmask 255.255.255.255
ASA1(config)#access-list outacl permit udp host 192.1.6.20 host
192.1.12.100 eq 1645
ASA1(config)#access-list outacl permit udp host 192.1.6.20 host
192.1.12.100 eq 1646
ASA1(config)#access-list outacl permit tcp host 4.4.4.4 host
192.1.12.100 eq 49
ASA1(config)#access-list outacl permit tcp host 192.1.12.2 host
192.1.12.100 eq 49
```

- e) Create a Static entry for R1 E 0/0 at 10.2.2.1. Translate it to 192.1.12.15.

```
ASA1(config)#static (inside,outside) 192.1.12.15 10.2.2.1 netmask
255.255.255.255
```

2.4 – Authentication Proxy (4 Points)

- a) The AAA server is located at 10.1.1.100. It communicates to the PIX using TACACS+ and a key of ipexpert.

```
ASA1(config)#aaa-server TAC prot tacacs
ASA1(config-aaa-server-group)#exit
ASA1(config)#aaa-server TAC host 10.1.1.100
ASA1(config-aaa-server-host)#key ipexpert
```

- **On the ACS server, create the PIX as a network device.**

- b) All outbound Telnet and HTTP Requests have to authenticate against the AAA server. The username to use is pixuser with a password of ipexpert. Use the same username and password for all authentication passwords.

- **Configure the user on the ACS sever, under User setup.**

```
ASA1(config)#aaa authent include telnet inside 0 0 0 0 TAC
ASA1(config)#aaa authent include http inside 0 0 0 0 TAC
```


- **Test by telnetting to R2 from R1. You should see the proxy authentication.**

```
R1#telnet 192.1.12.2
Trying 192.1.12.2 ... Open
Username: pixuser
Password:
Password required, but none set
[Connection to 192.1.12.2 closed by foreign host]
R1#
```

- **On the ASA, show uauth will show the authenticated user.**

```
ASA1#show uauth

Current      Most Seen
Authenticated Users      1          1
Authen In Progress      0          1
user 'pixuser' at 10.2.2.1, authenticated (idle for 0:00:38)
    absolute timeout: 0:05:00
    inactivity timeout: 0:00:00
ASA1#
```

- c) Allow R2 to telnet into R1 through the PIX.

```
ASA1(config)#access-list outacl permit tcp host 192.1.12.2 host
192.1.12.15 eq 23
```

- d) All inbound traffic for Telnet should be authenticated against the AAA server.

```
ASA1(config)#aaa authent include telnet outside 0 0 0 0 TAC
```

- e) All outbound traffic destined for a custom TCP application should be authenticated against the AAA server. The TCP application uses port 4515. Use virtual telnet and an IP address of 192.1.12.1.

- **Virtual telnet allows authentication for other ports.**

```
ASA1(config)#aaa authent include tcp/4515 inside 0 0 0 0 TAC
ASA1(config)#virtual telnet 192.1.12.1
```

- **From R1, telnet to R2 on port 4515. You will receive an error from the ASA. After authenticating to the virtual server address, you will be able to connect through. (You will receive a connection refused because R2 is not listening on 4515.)**

```
R1#telnet 192.1.12.2 4515
Trying 192.1.12.2, 4515 ... Open
Error: Must authenticate before using this service.
[Connection to 192.1.12.2 closed by foreign host]
R1#telnet 192.1.12.1
Trying 192.1.12.1 ... Open
LOGIN Authentication
Username: pixuser
Password:
Authentication Successful
[Connection to 192.1.12.1 closed by foreign host]
```



```
R1#telnet 192.1.12.2 4515
Trying 192.1.12.2, 4515 ...
% Connection refused by remote host

R1#
```

2.5 – Failover (2 points)

- Configure ASA2 as a failover device for ASA1.
- Use the Ethernet 0/2 interface for state information and failover.

```
ASA1(config-if)#ip address 192.1.12.10 255.255.255.0 standby
192.1.12.11
ASA1(config-if)#int eth0/0.55
ASA1(config-subif)#ip address 192.168.5.10 255.255.255.0 standby
192.168.5.11
ASA1(config-subif)#int eth0/1
ASA1(config-if)#ip address 10.2.2.10 255.255.255.0 standby
10.2.2.11
```

- In order to use the Eth0/2 interface for both state and failover, use two subinterfaces.

```
ASA1(config)#int eth0/2.10
ASA1(config-subif)#vlan 550
ASA1(config-subif)#int eth0/2.20
ASA1(config-subif)#vlan 560
```

```
ASA1(config)#failover lan interface FAILOVERINT eth0/2.10
INFO: Non-failover interface config is cleared on Ethernet0/2 and
its sub-interfaces
ASA1(config)#failover link state eth0/2.20
INFO: Non-failover interface config is cleared on Ethernet0/2 and
its sub-interfaces
```

- Make sure the switches are also configured for the ports as trunks.

```
Cat3(config)#int fa0/12
Cat3(config-if)#swit trunk encap dot1q
Cat3(config-if)#swit mode trunk
```

```
Cat4(config)#int fa0/12
Cat4(config-if)#swit trunk encap dot1q
Cat4(config-if)#swit mode trunk
Cat4(config-if)#
```

```
ASA1(config)#failover lan unit primary
ASA1(config)#failover key ipexpert
ASA1(config)#failover interface ip FAILOVERINT 192.168.55.1
255.255.255.0 standby 192.168.55.2
ASA1(config)#failover interface ip state 192.168.56.1
255.255.255.0 standby 192.168.56.2
ASA1(config)#failover
```


- On ASA2, enable the interface, configure the subinterface for the VLAN

```
ciscoasa(config)#int eth0/2
ciscoasa(config-if)#no shut

ciscoasa(config)#int eth0/2.10
ciscoasa(config-subif)#vlan 550
ciscoasa(config-subif)#exit
ciscoasa(config)#failover lan unit secondary

ciscoasa(config)#failover key ipexpert
ciscoasa(config)#failover lan int FAILOVERINT eth0/2.10
INFO: Non-failover interface config is cleared on Ethernet0/2 and
its sub-interfaces
ciscoasa(config)#failover interface ip FAILOVERINT 192.168.55.1
255.255.255.0 standby 192.168.55.2
ciscoasa(config)#failover
```

- Check the output of show failover. Notice that the interfaces show as “normal”. If the interfaces show “waiting”, the ASA is not receiving traffic from the mate.

```
ASA1#show failover
Failover On
Failover unit Primary
Failover LAN Interface: FAILOVERINT Ethernet0/2.10 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 7.2(2), Mate 7.2(2)
Last Failover at: 15:08:47 UTC Feb 10 2007
  This host: Primary - Active
    Active time: 850 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
      Interface DMZ55 (192.168.5.10): Normal (Not-Monitored)
      Interface outside (192.1.12.10): Normal
      Interface inside (10.2.2.10): Normal
    slot 1: empty
  Other host: Secondary - Standby Ready
    Active time: 448 (sec)
    slot 0: ASA5510 hw/sw rev (1.1/7.2(2)) status (Up Sys)
      Interface DMZ55 (192.168.5.11): Normal (Not-Monitored)
      Interface outside (192.1.12.11): Normal
      Interface inside (10.2.2.11): Normal
    slot 1: empty

Stateful Failover Logical Update Statistics
ASA1#
```

- Notice that the DMZ interface shows as Not-monitored. By default subinterfaces are not monitored. If you want to monitor a subinterface, use the command monitor-interface under global configuration mode.

```
ASA1(config)#monitor-interface DMZ55
```


2.6 – Transparent Firewall (3 points)

- a) Configure the PIX as a transparent Firewall between VLAN 11 and VLAN 111. Deny all ICMP traffic, other than echo and echo reply. Allow all other traffic.

- **Configure the mode as transparent, enable the interfaces, and assign names and security levels.**

```
pixfirewall(config)#firewall transparent
pixfirewall(config)#
```

```
pixfirewall(config)#int eth0
pixfirewall(config-if)#nameif outside
pixfirewall(config-if)#no shut
pixfirewall(config-if)#int eth1
pixfirewall(config-if)#no shut
pixfirewall(config-if)#nameif inside
```

- **Configure an access-list to allow the traffic specified, and apply to the interfaces.**

```
pixfirewall(config)#access-list ALLOW permit icmp any any echo
pixfirewall(config)#access-list ALLOW permit icmp any any echo-
reply
```

```
pixfirewall(config)#access-list ALLOW deny icmp any any
pixfirewall(config)#access-list ALLOW permit ip any any
```

```
pixfirewall(config)#access-group ALLOW in interface inside
pixfirewall(config)#access-group ALLOW in interface outside
```

- **Verify that you can ping through the transparent firewall.**

```
ASA1#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA1#
```

3 – Routing Using Interior Gateway Protocols (4 Points)

3.1 – GRE thru PIX (4 Points)

- a) Configure a GRE Tunnel from R1 F 0/0 to R2 F 1/0. Use 172.16.12.0/24 as the Tunnel IP Address.

```
R1(config)#interface Tunnel12
R1(config-if)#ip address 172.16.12.1 255.255.255.0
R1(config-if)#tunnel source 10.2.2.1
R1(config-if)#tunnel destination 10.2.2.2
```

```
R2(config)#int tunnel 12
R2(config-if)#ip address 172.16.12.1 255.255.255.0
R2(config-if)#tunnel source 192.1.12.2
R2(config-if)#tunnel dest 192.1.12.15
```


b) Run OSPF over the GRE tunnel. Advertise the following networks over the GRE Tunnel:

- R1 – Loopback 0, Tunnel and F 0/0
- R2 – Advertise the Tunnel and F 1/0 interface in OSPF. The other interfaces should already have been advertised into OSPF. Use the same process ID.

```
R2(config)#router ospf 1
R2(config-router)#network 172.16.12.0 0.0.0.255 area 0
R2(config-router)#network 192.1.12.0 0.0.0.255 area 0
```

```
R1(config)#router ospf 1
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1(config-router)#network 172.16.12.0 0.0.0.255 area 0
R1(config-router)#network 10.2.2.0 0.0.0.0 area 0
```

c) Allow the Tunnel thru the PIX Firewall.

d) Make sure that there is no Recursive Routing issue. You can use the static command on the PIX.

```
ASA1(config)#static (outside,inside) 10.2.2.2 192.1.12.2 netmask
255.255.255.255
```

```
ASA1(config)#access-list outacl permit gre host 192.1.12.2 host
192.1.12.15
```

- **Recursive routing happens when the destination for the tunnel is learned via the tunnel. Since the destination network is being advertised via the tunnel, NAT can allow us to use a different address that the router thinks is local. The ASA already has a translation for R1's address to 192.1.12.15. By adding a translation for R2's network, R1 will send traffic to a local destination.**

- **Verify that the OSPF neighbor relationship has established.**

```
R2#show ip ospf neigh
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	0	FULL/ -	00:00:33	172.16.12.1	Tunnel12

```
R2#
```

4 – BGP Routing (8 Points)

4.1 – Authentication (2 Points)

a) Authenticate all IBGP Peerings using MD5 authentication with a password of ccie.

```
R2(config)#router bgp 245
R2(config-router)#neighbor 4.4.4.4 password ccie
R2(config-router)#neighbor 5.5.5.5 password ccie
R4(config)#router bgp 245
R4(config-router)#neighbor 2.2.2.2 password ccie
R5(config)#router bgp 245
R5(config-router)#neighbor 2.2.2.2 password ccie
```


4.2 – EBGW thru the PIX (2 Points)

- a) Configure EBGW peering between R1 and R2 thru the PIX. R1 sees R2 as 192.1.12.2 and R2 should see R1 as 192.1.12.15. The Static should have been created in the previous step.
- R1 has a static route to the 192.1.12.0 network. As the traffic passes through the PIX, it will be translated to address 192.1.12.15. The only thing to do is to allow the BGP in the outside ACL in case R2 wants to initiate the BGP connection.

```
ASA1 (config) #access-list outacl permit tcp host 192.1.12.2 host 192.1.12.15 eq 179
```

4.3 – BGP Filtering - I (4 Points)

- a) R5 should be receiving the following routes from the BB2:
- 200.1.4.0 /24
 - 200.1.5.0 /24
 - 200.1.6.0 /24
 - 200.1.7.0 /24
- b) Devices within your topology should see the routes learned from BB2 with a next hop of 192.0.1.5, and if traffic is directed to these networks, should be dropped locally.
- c) ICMP unreachables should not be sent out for traffic that the routers drop.

```
BB2 (config) #route-map SETHOP
BB2 (config-route-map) #set ip next-hop 192.0.1.5
BB2 (config) #router bgp 100
BB2 (config-router) #neighbor 10.5.5.5 route-map SETHOP out

R5 (config) #ip route 192.0.1.5 255.255.255.255 null0
```

- On each of the other BGP routers, add a local route to Null0 for the address 192.0.1.5. In order to prevent unreachables, disable them under the interfaces.

```
R1 (config) #ip route 192.0.1.5 255.255.255.255 null0
R2 (config) #ip route 192.0.1.5 255.255.255.255 null0
R4 (config) #ip route 192.0.1.5 255.255.255.255 null0
R9 (config) #ip route 192.0.1.5 255.255.255.255 null0
```

```
R1 (config) #int fa0/0
R1 (config-if) #no ip unreachable
R1 (config-if) #int fa0/1
R1 (config-if) #no ip unreachable
```

```
R2 (config) #int fa1/0
R2 (config-if) #no ip unreachable
R2 (config-if) #int ser0/1/0.4
R2 (config-subif) #no ip unreachable
R2 (config-subif) #int ser0/1/0.5
R2 (config-subif) #no ip unreachable
R2 (config-subif) #int ser0/1/0.6
R2 (config-subif) #no ip unreachable
```



```
R4(config)#int ser0/0/0
R4(config-if)#no ip unreachable
R4(config-if)#int fa0/0
R4(config-if)#no ip unreachable
```

```
R5(config)#int fa0/0
R5(config-if)#no ip unreachable
R5(config-if)#int ser0/1/0
R5(config-if)#no ip unreachable
```

```
R9(config)#int fa0/0
R9(config-if)#no ip unreachable
```

- **R2 has an ebgp peering to R1, and R4 has a peering to R9. By default, the router will set the next hop to the peer address with an EBGP connection. Configure a route-map on R2 and R4 to set the next hop for these routes.**

```
R2(config)#access-list 44 permit 200.1.4.0 0.0.3.0
```

```
R2(config)#route-map SETHOP
R2(config-route-map)#match address 44
R2(config-route-map)#set ip next-hop 192.0.1.5
R2(config-route-map)#router bgp 245
R2(config-router)#neighbor 192.1.12.15 route-map SETHOP out
```

```
R4(config)#access-list 44 permit 200.1.4.0 0.0.3.0
R4(config)#route-map SETHOP
R4(config-route-map)#match address 44
R4(config-route-map)#set ip next-hop 192.0.1.5
```

5 – Access Management (4 Points)

5.1 – Configuring SSH on R4 (4 Points)

- Configure SSH on R4.
- SSH authentication should be done locally.
- Create a user admin with a password of ipexpert.

- **Configure the username and domain name, and generate RSA keys. Configure the VTY lines to allow local login.**

```
R4(config)#username admin password ipexpert
R4(config)#ip domain name ipexpert.com
R4(config)#crypto key generate ?
    rsa    Generate RSA keys
    <cr>
```



```
R4(config)#crypto key generate rsa ?
  general-keys  Generate a general purpose RSA key pair for
signing and
                  encryption
  usage-keys    Generate separate RSA key pairs for signing and
encryption
  <cr>
```

```
R4(config)#crypto key generate rsa
The name for the keys will be: R4.ipexpert.com
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.
```

```
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

```
R4(config)#
R4(config)#line vty 0 15
R4(config-line)#login local
```

- You can test from the ACS box, using the SSH client. Connect to the address 4.4.4.4, R4's loopback. The firewall should already have a translation for the ACS server to 192.1.12.100, so no other routes should be necessary.

6 – IP Services (5 Points)

6.1 – DHCP Server and Relay Agent (5 Points)

- a) Enable R2 as a DHCP Server with the following information:

- IP ADDRESS : 192.1.49.0/24
- WINS ADDRESS : 192.1.49.135
- DNS ADDRESS : 192.1.49.53
- DEFAULT GATEWAY : 192.1.49.4
- LEASE TIME : 6 Days

- b) Enable R4 to forward DHCP requests to R2.

- c) Configure Cat1 for DHCP snooping for R2.

```
R2(config)#no ip dhcp conflict logging
R2(config)#
R2(config)#ip dhcp excluded-address 192.1.49.4
R2(config)#ip dhcp excluded-address 192.1.49.9
R2(config)#ip dhcp excluded-address 192.1.49.53
R2(config)#ip dhcp excluded-address 192.1.49.135
R2(config)#
R2(config)#ip dhcp pool CCIE
```



```
R2(dhcp-config)#network 192.1.49.0 255.255.255.0
R2(dhcp-config)#netbios-name-server 192.1.49.135
R2(dhcp-config)#dns-server 192.1.49.53
R2(dhcp-config)#default-router 192.1.49.4
R2(dhcp-config)#lease 6
```

- **R4 just needs a helper address to forward the requests.**

```
R4(config)#int fa0/0
R4(config-if)#ip helper-address 192.1.24.2
```

- **To test, add an interface to vlan 49 with a DHCP negotiated address.**

```
Cat1(config)#int vlan 49
Cat1(config-if)#ip address dhcp
```

- **Interface Vlan49 assigned DHCP address 192.1.49.1, mask 255.255.255.0**

```
Cat1(config)#ip dhcp snooping
Cat1(config)#ip dhcp snooping vlan 49
Cat1(config-if)#int fa0/4
Cat1(config-if)#ip dhcp snooping trust
```

7 –Virtual Private Networks (20 Points)

7.1 – Basic Concentrator Configuration (3 Points)

- a) Configure the IP Address of the Private Interface thru the CLI.

```
> Enter IP Address

Quick Ethernet 1 -> [ 192.168.5.5 ] 10.2.2.5

> Enter Subnet Mask

Quick Ethernet 1 -> [ 255.255.255.0 ]
```

- b) The Public interface should be configured from the Graphical interface.
- c) Make sure the PC can access the Concentrator. You are allowed a static route on the Concentrator to accomplish this.

Configuration – system management – ip routing – static routes – add static route.

No Static Routes Configured

- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

```
Routing -> 1
> Net Address
Routing -> 10.1.1.0
```



```

> Subnet Mask
Routing -> 255.255.255.0
1) Destination is Router
2) Destination is Interface
Routing -> 1
> Router Address
Routing -> 10.2.2.1

```

→ From the GUI, configure the address for the public interface under configuration – interfaces.

d) Configure a Default Route on the Concentrator pointing towards the DMZ55 interface on the PIX. You are allowed a static route on R1 to accomplish this.

→ Configure the default gateway under configuration – system – ip routing – default gateways.

7.2 – Configure a Remote Access Easy VPN using ASA as a Server and Cisco Secure VPN Client (5 Points)

a) Configure the ASA as the Easy VPN Server using the following parameters:

- Group name and password: Name: **EZGroup**, Password: **abcd1234**
- DNS and WINS Address: 10.2.2.175
- Domain Name: ipexpert.net
- Address Pool (local): 10.3.3.1 – 10.3.3.253
- The address should be assigned to the client from the pool above.
- The authentication should be done locally.
- Hashing for the ISAKMP policy should be done based on MD5.
- Authentication for ISAKMP policy should be done based on a pre-shared key.
- Use ESP-DS and ESP-MD5-HMAC for your transform set.

→ Configure the group policy:

```

ASA1(config)#group-policy EZGroup internal
ASA1(config)#group-policy EZGroup attributes
ASA1(config-group-policy)#wins-server value 10.2.2.175
ASA1(config-group-policy)#dns-server value 10.2.2.175
ASA1(config-group-policy)#vpn-idle-timeout 30
ASA1(config-group-policy)#default-domain value ipexpert.net
ASA1(config)#tunnel-group EZGroup type ipsec-ra

```

→ Configure the address pool.

```

ASA1(config)#ip local pool MYpool 10.3.3.1-10.3.3.253

```

→ Configure the tunnel group.

```

ASA1(config)#tunnel-group EZGroup general-attributes
ASA1(config-tunnel-general)#address-pool MYpool
ASA1(config-tunnel-general)#default-group-policy EZGroup

```


→ **Configure the ISAKMP policy**

```
ASA1(config)#crypto isak enable outside
ASA1(config)#crypto isakmp policy 10
ASA1(config-isakmp-policy)#authentication pre-share
ASA1(config-isakmp-policy)#encryption 3des
ASA1(config-isakmp-policy)#hash md5
ASA1(config-isakmp-policy)#group 2
ASA1(config-isakmp-policy)#lifetime 86400
```

→ **Configure the transform and the crypto map.**

```
ASA1(config)#crypto ipsec transform MYTRANSFORM esp-des esp-md5-
hmac
ASA1(config)#crypto dynamic-map MYDYN 5 set transform MYTRANSFORM
ASA1(config)#crypto map MYMAP 50 ipsec-isakmp dynamic MYDYN

ASA1(config)#crypto map MYMAP interface outside

ASA1(config)#username cisco password cisco
```

→ **On the Test PC, connect to the server using the group EZGroup and password abcd1234. Verify that you can ping the client from the ASA.**

```
ASA1#ping 10.3.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
ASA1#
```

→ **If you add a static route on R1, you should be able to ping from R1 as well.**

```
R1(config)#ip route 10.3.3.0 255.255.255.0 10.2.2.10

R1#ping 10.3.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```

7.3 – Setup a Site-to-Site IPsec VPN between the Concentrator and R5 (4 Points)

- a) The concentrator should be seen as 192.1.12.5 on the outside network. Configure the PIX to accomplish this.

```
ASA1(config)#static (DMZ55,outside) 192.1.12.5 192.168.5.5
netmask 255.255.255.255
```


- b) Encrypt traffic between the 10.2.2.0/24 and 10.5.5.0/24 networks using the following parameters:

- Authentication is based on Pre-shared key of **ccie**.
- Use MD5 for the Hashing algorithm. Use defaults for the rest of the ISAKMP parameters.
- For IPsec, use ESP-DES for encryption and ESP-SHA-HMAC for Data Authentication in Tunnel Mode.
- **On the concentrator:**

Configuration – tunneling and security – IPsec – Lan to Lan

Add new entry

Set peer as 192.1.25.5

Configure the preshared key of ccie

Authentication should be ESP/SHA/HMAC-160

Encryption should be DES-56

IKE should be IKE-DES-MD5

Add 10.2.2.0 as the local network

Add 10.5.5.0 as the remote network

```
R5(config)#crypto isakmp policy 10
R5(config-isakmp)#hash md5
R5(config-isakmp)#auth pre-share

R5(config)#crypto isakmp key ccie address 192.1.12.5
R5(config)#crypt ipsec transform-set R5TRANS esp-des esp-sha-hmac

R5(config)#access-list 175 permit ip 10.5.5.0 0.0.0.255 10.2.2.0
0.0.0.255
R5(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R5(config-crypto-map)#match address 175
R5(config-crypto-map)#set peer 192.1.12.5
R5(config-crypto-map)#set transform R5TRANS

R5(config)#int ser0/1/0
R5(config-if)#crypto map MYMAP
```

- c) You can use static routes on R5 and R1 to accomplish this.

```
R1(config)#ip route 10.5.5.0 255.255.255.0 10.2.2.5
R5(config)#ip route 10.2.2.0 255.255.255.0 192.1.25.2
```

- d) Create the appropriate entries in the PIX firewall to accomplish this.

```
ASA1(config)#access-list outacl permit esp host 192.1.25.5 host
192.1.12.5
ASA1(config)#access-list outacl permit udp host 192.1.25.5 eq 500
host 192.1.12.5
```


- **Verify that you can ping R1 from R5.**

```
R5#ping 10.2.2.1 source fa0/0
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:  
Packet sent with a source address of 10.5.5.5  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/87/88 ms  
R5#
```

7.4 – Event Management on the Concentrator (3 Points)

- a) Configure the Concentrator to send e-mail messages to concadmin@ipexepert.com.

→ **Configuration – system – events – Email Recipients**

- b) The SMTP Server to be used for sending messages is located at 10.2.2.25.

→ **Configuration – system – events – SMTP servers – Add**

- c) Disable the ability of users to Telnet into the Concentrator.

→ **Configuration – management – telnet, uncheck enable.**

7.5 – Web VPN on the Concentrator (5 Points)

- a) Enable HTTP Services on R1.

- b) Create a Group called WebVPN with a password of abcd.

→ **User Management – groups – add group.**

- c) Enable WebVPN for the public interface.

→ **Configuration – interfaces – Public – WebVPN tab.**

→ **Select WebVPN HTTPS sessions and Redirect http to HTTPS.**

- d) Create a Pool of IP Address 192.168.2.1-192.168.2.254. This pool should be specific to this group.

→ **Add the pool under the group. – Configuration – user management – Groups – add address pool.**

→ **Configuration – System – Address Management – Assignment – select use address pools**

- e) Allow the Inside PC to connect to the Public interface of the Concentrator thru the PIX Firewall. Use the Static command to accomplish this on the PIX.
- f) Create a static route for the 192.168.2.0 network on R1 pointing towards the Concentrator. Also create a static route on R1 for the 192.168.5.0 /24 network thru the PIX. The user at 10.1.1.100 should be able to Web VPN into the concentrator from the public interfaces thru the PIX.
- g) Enable the Concentrator to redirect HTTP requests to HTTPS.
- h) Disable the ability of the users to enter a URL.
 - ➔ **Under the group setup, webvpn tab, uncheck the box :enable url entry.**
- i) Create a URL Link for the HTTP Server on R1 such that when a user part of this group logs in, he has the ability to click on a Link to connect to the HTTP server on R1.
 - ➔ **Under the group setup – WebVPN Servers and URLs – add a URL for R1.**
- j) Also allow the Client to use a Custom application that allows the user to connect into R1 using a port 3001.
 - ➔ **Under group setup – WebVPN port forwarding – add – configure a forwarding for R1.**
- k) Create a user webvpnuser with a password of webvpn12. Assign the user to the WebVPN group.
 - ➔ **Configuration – user management – users – create and add to the group.**
- l) Verify the config by logging on and verifying the configuration from the Inside PC. Delete the static route for the 10.1.10 network for testing the WebVPN setup.
 - ➔ **You can also test from the test PC.**
- m) You should be able to telnet into R1 thru the WebVPN connection.
 - ➔ **Verify that you can telnet from R1. Open a command window and telnet from the test PC.**

8 – IOS Firewall (4 Points)

8.1 – Cisco IOS Firewall on R4 (4 Points)

- a) Inspect all tcp, udp and icmp traffic from the Ethernet segment going towards the Frame networks.
- b) Only allow relevant traffic coming in.

- c) ACL should be set to inbound on the Serial interface.

```

R4(config)#ip inspect name IPFW tcp
R4(config)#ip inspect name IPFW udp
R4(config)#ip inspect name IPFW icmp

R4(config)#access-list 181 permit tcp host 2.2.2.2 host 4.4.4.4
eq bgp
R4(config)#access-list 181 permit tcp host 2.2.2.2 eq bgp host
4.4.4.4 est
R4(config)#access-list 181 permit ospf host 192.1.24.2 host
224.0.0.5
R4(config)#access-list 181 permit tcp any host 4.4.4.4 eq 22
R4(config)#access-list 181 permit tcp any host 192.1.24.4 eq 22
R4(config)#access-list 181 permit tcp any host 192.1.49.4 eq 22
R4(config)#access-list 181 permit udp host 192.1.24.2 host
192.1.49.4 eq 67

R4(config)#int ser0/0/0
R4(config-if)#ip access-group 181 in
R4(config-if)#ip inspect IPFW out

```

- **Note:** for the DHCP traffic look at the output of debug ip packet and send a DHCP request.

```

*Dec 20 20:47:13.886: IP: s=0.0.0.0 (FastEthernet0/0), d=255.255.255.255,
len 604, rcvd 2
*Dec 20 20:47:13.886:      UDP src=68, dst=67
*Dec 20 20:47:13.886: IP: tableid=0, s=192.1.49.4 (local), d=192.1.24.2
(Serial0/0/0), routed via FIB
*Dec 20 20:47:13.886:      IP:      s=192.1.49.4 (local),      d=192.1.24.2
(Serial0/0/0), len 604, sending
*Dec 20 20:47:13.886:      UDP src=67, dst=67
*Dec 20 20:47:14.010: IP: tableid=0, s=192.1.24.2 (Serial0/0/0),
d=192.1.49.4 (FastEthernet0/0), routed via RIB
*Dec 20 20:47:14.014: IP: s=192.1.24.2 (Serial0/0/0), d=192.1.49.4, len
328, rcvd 4
*Dec 20 20:47:14.014:      UDP src=67, dst=67
*Dec 20 20:47:14.014: IP: s=192.1.49.4 (local), d=255.255.255.255
(FastEthernet0/0), len 328, sending broad/multicast
*Dec 20 20:47:14.014:      UDP src=67, dst=68

```

9 – Advanced Security and Attacks (14 Points)

9.1 – IP TCP Intercept (4 Points)

- The 192.1.6.0 network is experiencing SYN attacks from the Frame cloud to your web servers.
- R6 should watch the traffic and if it does not complete the TCP handshake in 20 seconds, it should drop the packets.
- Limit IP TCP intercept to only watch packets coming from 192.1.26.0, 192.1.24.0 or the 192.1.25.0 networks for Web traffic towards R6.

- d) Configure IP TCP intercept such that the router drops embryonic connections if they reach 1050. It should stop dropping the embryonic connections once the number reaches 850.

→ Start with an access list to match the traffic.

```
R6(config)#access-list 191 permit tcp 192.1.24.0 0.0.2.255
192.1.6.0 0.0.0.255 eq 80
R6(config)#access-list 191 permit tcp 192.1.24.0 0.0.2.255
192.1.6.0 0.0.0.255 eq 443
R6(config)#access-list 191 permit tcp 192.1.25.0 0.0.0.255
192.1.6.0 0.0.0.255 eq 80
R6(config)#access-list 191 permit tcp 192.1.25.0 0.0.0.255
192.1.6.0 0.0.0.255 eq 443
```

→ Configure the TCP intercept parameters

```
R6(config)#ip tcp int mode watch
R6(config)#ip tcp int watch-timeout 20
R6(config)#ip tcp int max-inc high 1049
R6(config)#ip tcp int max-inc low 851
R6(config)#ip tcp int list 191
```

→ Test by telnetting from R2 to Cat1, and looking at the output of show tcp intercept statistics.

```
R2>telnet 192.1.6.20 80
Trying 192.1.6.20, 80 ... Open

R6#show tcp int stat
Watching new connections using access-list 191
0 incomplete, 0 established connections (total 0)
1 connection requests per minute
R6#
```

9.2 – ICMP (2 points)

- a) On R5, rate-limit ICMP echo inbound from BB2 to 64kb/sec.

```
R5(config)#access-list 192 permit icmp an any echo
R5(config)#int fa0/0
R5(config-if)#rate-limit access-group 192 64000 12000 24000
conform transmit exceed drop
```

→ If you perform a large ping with repeat, you can see the packets limited.

```
BB2#ping 10.5.5.5 size 1000 repeat 1000

Type escape sequence to abort.
Sending 1000, 1000-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

- b) Configure R4 such that it will send a maximum of one ICMP unreachable every 3 seconds.

→ By default, a router will only send out one unreachable every 500 milliseconds.

```
R4(config)#ip icmp rate-limit unreachable 3000
```


9.3 – Fragments (2 points)

- a) Configure R6's FastEthernet interface to block inbound non-initial fragments with a destination of R2's FastEthernet interface. Other traffic should not be affected.

→ **The fragments keyword on an access list will affect how non-initial fragments are treated.**

```
R6(config)#access-list 193 deny ip any host 192.1.12.2 frag
R6(config)#access-list 193 permit ip any any
R6(config)#int fa0/0
R6(config-if)#ip access-group 193 in
```

9.4 – Spoofing (2 points)

- a) On R4, prevent address spoofing for traffic coming from R9. Only legitimate sources from R9 should be allowed. Traffic to 192.168.5.0/24 should be permitted, but any other traffic with a destination address in the range of 192.168.0.0/16 should be silently dropped by R4.

→ **Permit the traffic from legitimate sources, and block other traffic.**

```
R4(config)#access-list 194 permit ip host 9.9.9.9 192.168.5.0
0.0.0.255
R4(config)#access-list 194 permit ip host 199.99.99.99
192.168.5.0 0.0.0.255
R4(config)#access-list 194 permit ip host 192.1.49.9 192.168.5.0
0.0.0.255
R4(config)#access-list 194 deny ip any 192.168.0.0 0.0.0.255
R4(config)#access-list 194 permit ip host 9.9.9.9 any
R4(config)#access-list 194 permit ip host 199.99.99.99 any
R4(config)#access-list 194 permit ip host 192.1.49.9 any
R4(config)#int fa0/0
R4(config-if)#ip access-group 194 in
R4(config-if)#no ip unreachable
```

9.5 – Spoofing (4 Points)

- a) R5 is seeing a lot of spoofed packets from the BB2.
- b) You want to make sure that RFC 1918 addresses are not received from the backbone. Create an ACL to block all RFC 1918 addresses coming in as source packets. Allow 10.5.5.0/24 to come in.
- c) You also would like to make sure that the internal networks that R5 has a route for are not seen as source packets on the E 0/0 interface of R5. Don't use an ACL for this step.

→ **Configure an access list to match the RFC1918 address space. Permit 10.5.5.0/24 first.**

```
R5(config)#access-list 95 permit 10.5.5.0 0.0.0.255
R5(config)#access-list 95 deny 10.0.0.0 0.255.255.255
R5(config)#access-list 95 deny 172.16.0.0 0.15.255.255
R5(config)#access-list 95 deny 192.168.0.0 0.0.255.255
R5(config)#access-list 95 permit any
```


- **URPF checks will prevent traffic with a source network inside our topology from entering via the interface.**

```
R5(config)#int fa0/0
R5(config-if)#ip verify unicast reverse-path
R5(config-if)#ip access-group 95 in
```

10 – IDS (16 Points)

10.1 – Basic Configuration of IDS through IDS, IDM and IEV (3 Points)

- Configure the IDS Sensor's Command and Control Interface through the CLI to allow access to the Sensor from the IDM PC based on the Network Diagram.
- Add the Sensor to the IEV Console.

- **Run setup to configure basic parameters from the CLI.**

```
Enter host name[sensor]: IDS
Enter IP interface[10.1.9.201/24,10.1.9.1]: 10.1.1.15/24,10.1.1.1
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 10.1.1.0/24
```

- **You can add the sensor to the IEV console, or just use the monitoring tab of IDM.**
- **From the GUI interface, enable the interface and assign to the virtual sensor under analysis engine – virtual sensor.**

10.2 – Switch Configuration (2 Points)

- You would like to monitor all traffic received in the outside VLAN of the ASA.
 - Configure the Switch to copy all relevant traffic to the monitoring port.
- **A specific port isn't given, so you could send it to any of the IDS sniffing ports.**

```
Cat1(config)#vlan 900
Cat1(config-vlan)#remote-span

Cat3(config)#monitor session 1 source vlan 12 rx
Cat3(config)#monitor session 1 dest remote vlan 900

Cat1(config)#monitor session 1 source vlan 12 , 900 rx
Cat1(config)#monitor session 1 dest int fa0/7
```


10.3 –Custom Signature (4 Points)

- a) Create a custom string signature that detects the word “cmd.exe” anywhere in a HTTP url.
- b) Set the Alarm Severity to High.

- Create the signature using the wizard. Use service HTTP as the engine. Specify the Request Regex as cmd.exe, and a source port of 80.
- Verify by telnetting from R1 and triggering the signature. Make sure the signature shows up in the Event Viewer.

```
R1>telnet 10.2.2.2 80
Trying 10.2.2.2, 80 ... Open
get /cmd.exe

[Connection to 10.2.2.2 closed by foreign host]
R1>
```

10.4 – Signature tuning (3 points)

- a) When R2 does a broadcast DNS lookup, signature 4620 fires on the IDS sensor. Configure R2 to not send DNS broadcasts. Also, disable signature 4620 on the IDS sensor.

```
R2 (config) #no ip domain-lookup
```

- Under signature configuration on the IDM, disable signature 4620.

10.5 – PIX IDS (4 Points)

- a) Configure a Syslog Server at 10.1.1.100. Configure the ASA1 to send message to the Syslog server.

```
ASA1 (config) #logging host inside 10.1.1.100
```

- b) Configure Console Logging to level 4. Configure Trap logging level to debugging.

```
ASA1 (config) #logging con 4
ASA1 (config) #logging trap debug
```

- c) Configure the ASA1 IDS with the following parameters:

- Send an alarm for Info signatures
- Send an alarm and drop packets for Attack signatures

```
ASA1 (config) #ip audit name INFO info action alarm
ASA1 (config) #ip audit name ATTACK attack action alarm drop
```


- d) Enable the IDS sensing on the outside interface of the ASA

```
ASA1 (config) #ip audit interface outside INFO  
ASA1 (config) #ip audit interface outside ATTACK
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

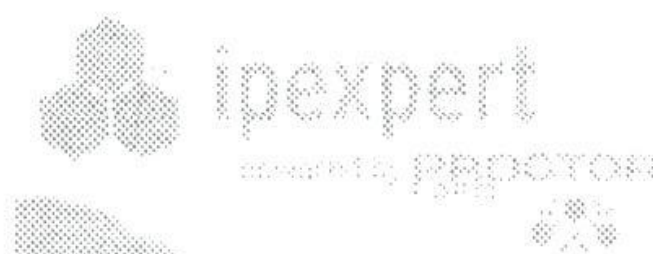
This page left intentionally blank.

Section 17: Multiprotocol Challenge F One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 17 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs* → Section 17 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your *www.IPexpert.com Member's Area*.

1 – Bridging and Switching (4 points)

1.1 – 2 points

- a) Configure SSH only access on CAT1. Make sure no other method is allowed.
- b) Only allow directed connected networks and VLAN 10 network to connect to the switch.
- c) Use local database for authentication.

→ **First ssh needs to be enabled:**

```
CAT1(config)#ip domain-name ipexpert.net
CAT1(config)#crypto key generate rsa g m 512
The name for the keys will be: CAT1.ipexpert.net
```

```
% The key modulus size is 512 bits
% Generating 512 bit RSA keys ... [OK]
02:53:38: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

→ **Configure a username to be used for the SSH sessions and an Access-List to limit who can SSH to the switch :**

```
CAT1(config)#username cisco password cisco
CAT1(config)#access-list 1 per 172.16.111.0 0.0.0.255
CAT1(config)#access-list 1 per 172.16.10.0 0.0.0.255
```

→ **There are two ways to limit management to SSH only, using ACL and using the transport input command.**

→ **Configure vty line to use ACL 1, set authentication to local and limit connection to SSH only:**

```
CAT1(config-if)#line vty 0 15
CAT1(config-line)#access-class 1 in
CAT1(config-line)#tran input ssh
CAT1(config-line)#login local
```

1.2 – 2 points

- a) Enable DHCP snooping on VLAN 111 at CAT2.

- b) Make sure the DHCP snooping data won't be erased when the switch reloads.

→ **Configure vlan snooping and configure a database to keep the bindings after the switch reboot:**

```
CAT2 (config)#ip dhcp snooping vlan 111
CAT2 (config)#ip dhcp snooping database flash:sn dhsnooping.tx
03:19:36: %DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running;
reloaded binding lease expiration times are incorrect.
03:19:36: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP
snooping database Write succeeded.
```

2 – PIX basic (9 points)

2.1 – 2 points

- a) Configure host name to "PIX".
- b) Configure PIX interfaces according to the IP addressing table.
- c) Configure domain name to "ipexpert.net".

→ **Configure hostname, domain name, nameif and IP addresses:**

```
hostname PIX
domain-name ipexpert.net
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 200.13.112.11 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.111.11 255.255.255.0
```

2.2 – 2 points

- a) Configure PIX to serve DHCP requests on VLAN 111.
- b) Set the following parameters:
- Network 172.16.111.0/24
 - Default gateway 172.16.111.11
 - Domain name ipexpert.net
- **Configure DHCPD on the PIX. There is no need to configure the default gateway on the PIX, the PIX always uses its own IP address:**

```
dhcpd address 172.16.111.20-172.16.111.254 inside
dhcpd domain ipexpert.net
dhcpd enable inside
```


- But this is not enough, DHCP snooping is enabled on VLAN 111 so the PIX's port on CAT2 needs to be trusted:

CAT2

```
interface FastEthernet0/3
 ip dhcp snooping trust
```

2.3 - 3 points

- a) Hosts on the inside should use NAT pool of 200.13.122.1-49.
- b) You are allowed one static route on R2.
- c) Allow hosts to connect to the network even if the NAT pool is overloaded.
- d) The switch should appear as 200.13.122.12. The pix should not change any TCP headers other then the checksum header.
- e) Hosts on VLAN 6 should be able to SSH the switch. Do not configure CAT1 to allow this.

- **Configure NAT and GLOBAL on the PIX. To allow hosts to connect to the outside network even if the pool is overloaded, the last IP address 200.13.122.49 will be used for PAT, and the PIX will use it only when the pool is overloaded.**

- **CAT1 won't accept SSH connections from VLAN6, so outside NAT will be used to map VLAN6 addresses to a pool on VLAN111:**

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 200.13.122.1-200.13.122.48
global (outside) 1 200.13.122.49
nat (outside) 2 200.13.6.0 255.255.255.0 outside
global (inside) 2 172.16.111.6
```

- **By default the PIX will randomize the TCP sequence, to disable this the keyword norandomseq is used:**

```
static (inside,outside) 200.13.122.12 172.16.111.12 netmask
255.255.255.255 norandomseq
```

2.4 – 2 points

- a) Configure the PIX not to allow devices to ping its interfaces.
 - b) Allow ICMP to the inside network. You are allowed only one ACL entry.
- **Configuration of ICMP traffic to the PIX is controlled by the icmp command, and the ICMP packets are evaluated in the order of the “icmp” statements:**

```
icmp deny any echo outside
icmp permit any echo-reply outside
icmp deny any echo inside
icmp permit any echo-reply inside
```



```
access-list OUT extended permit icmp any any echo
access-group OUT in interface outside
```

3 – ASA basic (9 points)

3.1 – 1 point

- Set ASA host name to "ASA".
- Configure ASA interfaces according to the IP addressing table.
- Configure the DMZ interface with security level of 50.
- Configure domain name to "ipexpert.net".

→ Configure hostname, domain name, nameif and IP addresses:

```
hostname ASA
domain-name ipexpert.net
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 200.13.24.9 255.255.255.0 standby 200.13.24.19
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.10.9 255.255.255.0 standby 172.16.10.19
!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 172.16.7.9 255.255.255.0 standby 172.16.7.19
!
```

3.2 – 2 points

- Configure failover. Use VLAN 222 on a free interface for failover link. Configure the switch to reflect the changes.
- When failover takes place, make sure that current TCP sessions do not need to be restarted.

→ Configure failover using LAN based failover. First configure the switches for VLAN222 and then assign the VLAN to e0/3 ports. To configure VLAN222, configure it on CAT1, as CAT1 is the VTP server:

CAT1

```
vlan 222
```


CAT3

```
interface FastEthernet0/13
 switchport access vlan 222
 switchport mode dynamic desirable
```

CAT4

```
interface FastEthernet0/13
 switchport access vlan 222
 switchport mode dynamic desirable
```

- Fail over configuration is the same for both ASAs except for the failover lan unit which should be primary for ASA1 and secondary for ASA2:

```
failover lan unit primary/secondary
failover lan interface ASA_FAIL Ethernet0/3
failover interface ip ASA_FAIL 172.16.222.9 255.255.255.0 standby
_ 172.16.222.19
failover
```

- Configure failover link so the active ASA will send updates to the conn and xlate table to the standby ASA, so when the primary will fail the secondary will have all the needed information to handle established sessions:

```
failover link ASA_FAIL Ethernet0/3
```

- From now on, there is no need to configure ASA2, the configuration will be synced:

3.3 - 3 points

- Hosts on the DMZ interface should use NAT pool of 200.13.24.101-119.
- Hosts on the inside networks should use NAT pool of 200.13.24.120-139.
- Allow hosts to connect to the network even if the NAT pool is overloaded.
- When R1 tries to telnet to R2 it should appear as 200.13.24.20.
- When R1 tries to telnet to R4 it should appear as 200.13.24.21.
- ACS server should appear as 200.13.24.100.

- **Configure NAT and GLOBAL on the PIX. To allow hosts to connect to the outside network even if the pool is overloaded, the last IP address 200.13.24.139 and 200.13.24.119 will be used for PAT, and the PIX will use it only when the pool is overloaded:**

```
nat (inside) 2 0.0.0.0 0.0.0.0
nat (DMZ) 1 0.0.0.0 0.0.0.0
global (outside) 1 200.13.24.120-200.13.24.138
global (outside) 2 200.13.24.101-200.13.24.118
global (outside) 1 200.13.24.139
global (outside) 2 200.13.24.119
```


- Use policy based NAT to control what global IP address R1 will use when connecting to the outside world:

```
access-list NAT1 extended permit tcp host 172.16.10.1 host 200.13.24.2 eq telnet
access-list NAT2 extended permit tcp host 172.16.10.1 host 200.13.24.4 eq telnet
nat (inside) 3 access-list NAT1
nat (inside) 4 access-list NAT2
global (outside) 3 200.13.24.20
global (outside) 4 200.13.24.21
```

- Configure static NAT for the ACS server:

```
static (inside,outside) 200.13.24.100 172.16.11.100 netmask 255.255.255.255
```

3.4 – 2 points

- a) Configure the ASA not to allow devices from the outside and from the DMZ to ping its interfaces.
- b) Allow ICMP pings pass through the ASA. You are allowed only two ACL entries.

- Configuration of ICMP traffic to the PIX is controlled by the icmp command, and the ICMP packets are evaluated in the order of the “icmp” statements:

```
icmp deny any echo outside
icmp permit any echo-reply outside
```

- Configure access-list and access-group to allow ICMP echo requests

```
access-list OUT extended permit icmp any any echo
access-group OUT in interface outside
access-list DMZ extended permit icmp any any echo
access-group DMZ in interface DMZ
```

- ICMP inspection is needed to allow return traffic of echo-reply. Configure class-map to match all traffic for inspection, then configure global policy map to inspect ICMP:

```
class-map cmALL
match default-inspection-traffic
policy-map pmGlobal
class cmALL
inspect icmp
service-policy pmGlobal global
```


3.5 – 1 point

- a) Allow all routers' loopback addresses to access ACS server using syslog, TACACS and RADIUS.

→ The easiest way is to use objects:

```
object-group network netL00
 network-object host 2.2.2.2
 network-object host 4.4.4.4
 network-object host 5.5.5.5
 network-object host 6.6.6.6
access-list OUT extended permit tcp object-group netL00 host 200.13.24.100 eq tacacs
access-list OUT extended permit udp object-group netL00 host 200.13.24.100 eq radius
access-list OUT extended permit udp object-group netL00 host 200.13.24.100 eq syslog
```

4 – PIX/ASA advanced (12 points)**4.1 – 2 Points**

- a) On both ASA and PIX, configure OSPF on the inside interface.
- b) The OSPF area should be area 0. Use the most secure authentication with key cisco
- c) Make sure inside devices will be able to route packets to all the network.
- d) Configure default route on the PIX/ASA to R2.
- e) R7 is running OSPF. Configure ASA to run OSPF on dmz interface using area 0. All OSPF routes on R7 should appear as external.

→ Configure OSPF process and send default route to internal devices so they will know the way out:

```
router ospf 1
 network 172.16.10.0 255.255.255.0 area 0
 default-information originate always
```

→ Configure authentication on the inside interfaces:

```
interface Ethernet0/1
 nameif inside
 ospf message-digest-key 1 md5 cisco
 ospf authentication message-digest
```

→ Configure the default route using the route command:

ASA

```
route outside 0.0.0.0 0.0.0.0 200.13.24.2 1
```


PIX

```
route outside 0.0.0.0 0.0.0.0 200.13.112.2 1
```

- To make routes appear as external routes on R7 configure additional routing process on the ASA and redistribute between the processes:

```
router ospf 1
 redistribute ospf 2 subnets
!
router ospf 2
 network 172.16.7.0 255.255.255.0 area 0
 log-adj-changes
 redistribute ospf 1 subnets
 default-information originate always
```

4.2 – 3 points

- a) Traffic from the ASAs' inside networks to VLAN 6 should be limited to 64K.
 - b) Traffic from the ASAs' inside networks to VLAN5 should be limited to 128K.
- Configure access-list to match traffic, configure class-map to classify traffic, configure policy-map to control the bandwidth, then enable the policy on the outside interface:

```
access-list to6 extended permit ip any 200.13.6.0 255.255.255.0
access-list to5 extended permit ip any 200.13.5.0 255.255.255.0
class-map cm25
 match access-list to5
class-map cm26
 match access-list to6
policy-map pmOUT
 class cm25
  police 128000
 class cm26
  police 64000
service-policy pmOUT interface outside
```

4.3 – 3 point

- a) There are 2 FTP servers on the DMZ: 172.16.7.104 and 172.16.7.105.
- b) They should be seen to the outside world as 200.13.24.104 and 200.13.24.105.
- c) The FTP servers on the DMZ are using port 2121. Make sure outside networks can FTP to servers in the DMZ.

- d) Do not allow active FTP traffic from the inside networks to FTP server 200.13.6.100 (do not forget the DMZ).

→ **Configure static NAT for the FTP servers:**

```
static (DMZ,outside) 200.13.24.104 172.16.7.104 netmask 255.255.255.255
static (DMZ,outside) 200.13.24.105 172.16.7.105 netmask 255.255.255.255
```

→ **Configure OUT access-list to allow FTP on port 2121:**

```
access-list OUT extended permit tcp any host 200.13.24.104 eq 2121
access-list OUT extended permit tcp any host 200.13.24.105 eq 2121
```

→ **Configure FTP inspection for port 2121:**

```
class-map cm_ftp
match port tcp eq 2121
policy-map pmGlobal
class cm_ftp
inspect ftp
```

- To disable active FTP to the server, configure the ASA to disable FTP inspection for that server. Without FTP inspection the ASA won't let the DATA channel to open from the outside to the inside:

```
access-list FTP6 extended permit tcp 172.16.10.0 255.255.255.0 host 200.13.6.100 eq ftp
class-map cmFTP6
match access-list FTP6
policy-map pmGlobal
class cmFTP6
```

4.4 – 2 points

- a) A group of servers on the DMZ are running web services on ports 80, 81, 82, 83, 84, 86, 87, 88.
 b) The IP addresses are 172.16.7.111, 172.16.7.112, 172.16.7.113.
 c) They should be seen to the outside world as 200.13.24.111, 200.13.24.112, 200.13.24.113.
 d) You are allowed only one ACE entry in the ACL.

→ **Configure static NAT for the servers:**

```
static (DMZ,outside) 200.13.24.111 172.16.7.111 netmask 255.255.255.255
static (DMZ,outside) 200.13.24.112 172.16.7.112 netmask 255.255.255.255
static (DMZ,outside) 200.13.24.113 172.16.7.113 netmask 255.255.255.255
```


- To use only one ACL entry for multiple servers/ports configure objects and apply them in one ACL entry:

```
object-group service WEBTCP tcp
port-object range www 80 80
port-object range 80 80
object-group network WEBSRV
network-object host 200.13.24.111
network-object host 200.13.24.112
network-object host 200.13.24.113
access-list OUT extended permit tcp any object-group WEBSRV
object-group WEBTCP
```

4.5 – 2 point

- a) Due to MTU problems on the Internet, users going through the PIX are suffering from fragmentation problems. Make sure that TCP segments are not larger than 1200 bytes.

- MSS stands for Maximum Segment Size, which sets to largest packet size for the session. The ASA can control this size when sessions are established through it:

```
sysctl connection tcpmss 1200
```

5 – IOS Features (10 points)

5.1 – 4 points

- a) Configure R6 for SSH only management.
- b) Login, and command authorization should be using TACACS.
- c) Configure on the ACS username cisco with password cisco. Allow that user to use any commands or configurations.
- d) Configure on the ACS username oper with password oper. Allow that user the following commands:
- show ver
 - show proc cpu
- e) Allow username cisco to work even if there is no response from the TACACS server.
- f) Do not configure the ASA to accomplish the task.

- First ssh needs to be enabled:

```
R6(config)#ip domain-name ipexpert.net
R6(config)#crypto key generate rsa g m 512
The name for the keys will be: CAT1.ipexpert.net

% The key modulus size is 512 bits
% Generating 512 bit RSA keys ... [OK]
02:53:38: %SSH-5-ENABLED: SSH 1.99 has been enabled
```


- Configure a username to be used as a backup with priv 15:

```
R6 (config) #username cisco priv 15password cisco
```

- Configure AAA for authentication and authorization. The local database will be used as a backup:

```
aaa new-model
aaa authentication login A3 group tacacs+ local
aaa authorization exec A3 group tacacs+ local
aaa authorization commands 0 A3 group tacacs+ local
aaa authorization commands 1 A3 group tacacs+ local
aaa authorization commands 15 A3 group tacacs+ local
```

- Configure TACAS server. The ASA was configured to accept TACAS only from 6.6.6.6, so set the source interface for TACAS request to Lo0:

```
ip tacacs source-interface Loopback0
tacacs-server host 200.13.24.100 key cisco
```

- Apply AAA configuration to the vty lines and enforce SSH only authentication:

```
line vty 0 15
authorization commands 0 A3
authorization commands 1 A3
authorization commands 15 A3
authorization exec A3
login authentication A3
transport input ssh
```


→ Add R6 to the ACS server:

The screenshot shows the Cisco Systems Network Configuration web interface. On the left is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration (which is highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname:
- AAA Client IP Address: with up/down arrow buttons on the right.
- Key:
- Authenticate Using: with a dropdown arrow on the right.
- Four unchecked checkboxes with labels:
 - ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
 - ☐ Log Update/Watchdog Packets from this AAA Client
 - ☐ Log RADIUS Tunneling Packets from this AAA Client
 - ☐ Replace RADIUS Port info with Username from this AAA Client

- Configure a group for cisco user with shell access and set the priv level to 15 and allow to run any command:

CISCO SYSTEMS

Group Setup

Jump To: **Enable Options**

Note: PPP LCP will be automatically enabled if this service is enabled

- ☒ **Shell (exec)**
- ☐ Access control list
- ☐ Auto command
- ☐ Callback line
- ☐ Callback rotary
- ☐ Idle time
- ☐ No callback verify
- ☐ No escape
- ☐ No hangup
- ☒ Privilege level: **15**
- ☐ Timeout

Navigation buttons: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, Online Documentation.

CISCO SYSTEMS

Group Setup

Jump To: **Enable Options**

- ☐ None
- ☐ Assign a Shell Command Authorization Set for any network device: **R6_Oper**
- ☒ Per Group Command Authorization
 - Unmatched Cisco IOS commands
 - ☒ Permit
 - ☐ Deny

Command:

Arguments:

Buttons: Submit, Submit + Restart, Cancel

Footer: Applet dialup_filter started

→ In the “Share Profile Component” create “Command authorization Set”:

The screenshot shows the Cisco Systems Shared Profile Components web interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components (selected), Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Shared Profile Components" and "Shell Command Authorization Set". It contains the following fields and controls:

- Name:** A text box containing "R6_Oper".
- Description:** An empty text box.
- Unmatched Commands:** Two radio buttons: "Permit" (unselected) and "Deny" (selected).
- exit** and **show** command lists: Two text boxes. The first contains "exit" and "show". The second contains "permit version" and "permit processes cpu".
- Permit Unmatched Args:** A checkbox that is unchecked.
- Add Command** and **Remove Command** buttons: Two buttons at the bottom of the command lists.

The browser address bar at the bottom shows the URL: http://127.0.0.1:2230/spc/dcs/SH_exec.htm#AddEdit

→ Assign the Authorization Set to the oper's group:

CISCO SYSTEMS

Group Setup

Jump To: Access Restrictions

Shell Command Authorization Set

☐ None

☒ Assign a Shell Command Authorization Set for any network device

R6_Oper

☐ Per Group Command Authorization

Unmatched Cisco IOS commands

☐ Permit

☒ Deny

☐ Command:

Arguments:

Submit Submit + Restart Cancel

5.2 – 2 points

- R4 should send its logs to the ACS server.
- The messages should be stamped using milliseconds resolution.
- All logs should be sent.
- Due to constrained storage on the ACS server, limit the info messages to 5/sec.
- Do not configure the ASA to accomplish the task.

→ **Configure logging on R4. To time-stamp the logs use service timestamps. Remember that the ASA expects syslog to come from the IP address of Lo0. Also configure rate limiting using the logging command to limit the number of syslog packets per second:**

```
service timestamps debug datetime msec
service timestamps log datetime msec
logging rate-limit 5
logging trap debugging
logging source-interface Loopback0
logging 200.13.24.100
```


5.3 – 2 points

- a) R4 should remove any DF bits when packets are smaller than 512 bytes.

→ **Configure PBR on all interfaces to remove the DF bits. Match on packet size:**

```
route-map NODF permit 10
  match length 64 512
  set ip df 0
!
interface FastEthernet0/0
  ip policy route-map NODF
interface FastEthernet0/1
  ip policy route-map NODF
```

5.4 – 2 points

- a) Due to some high traffic load, using telnet to R4 is very slow, optimize R4 to make telnet more responsive. Don't you QOS.

→ **Configure Nagel algorithm so the router will not send a packet for each telnet character being sent to the telnet user, but will try to group several characters in a single packet:**

```
service nagle
```

6 – VPN Basic (10 points)**6.1 – 3 points**

- a) Configure new loopback interfaces on R2 and R4:

- R2 Lo24: 10.22.22.22/32
- R4 Lo24: 10.44.44.44/32

- b) Configure GRE tunnel between R2 and R4. Use Lo 0 interface as source.

- c) Configure OSPF to on the tunnel. Advertise Lo24 interfaces over the tunnel. Make sure they are not visible on the network.

- d) Protect the tunnel using ESP and preshared ISAKMP key.

→ **Configure loopbacks and the GRE tunnels:**

R4

```
interface Loopback24
  ip address 10.44.44.44 255.255.255.255
interface Tunnel24
  ip address 172.16.24.4 255.255.255.0
  tunnel source Loopback0
  tunnel destination 2.2.2.2
```


R2

```

interface Loopback24
 ip address 10.22.22.22 255.255.255.255
interface Tunnel24
 ip address 172.16.24.2 255.255.255.0
 tunnel source Loopback0
 tunnel destination 4.4.4.4

```

- The hidden issue here is to avoid recursive routing, because enabling OSPF on the tunnel interfaces will cause the routes to Lo0 be learned via the tunnel, and the tunnel will fail.
- To avoid this configure another OSPF process to run on the tunnel interfaces:

R2

```

router ospf 2
 log-adjacency-changes
 network 10.22.22.0 0.0.0.255 area 24
 network 172.16.24.0 0.0.0.255 area 0

```

R4

```

router ospf 2
 log-adjacency-changes
 network 10.44.44.0 0.0.0.255 area 24
 network 172.16.24.0 0.0.0.255 area 0

```

- But that is not enough because R2 is using “redistribute connected”, so Lo24 will be advertised on V24 also. To avoid this limit the routes redistributed to R2:

```

route-map C20 permit 10
 match interface Loopback0
router ospf 1
 redistribute connected subnets route-map C20

```

- Now protect the tunnel using IPSEC:

R4

```

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco address 200.13.24.2
crypto ipsec transform-set ts24 esp-des esp-md5-hmac
crypto map CM24 10 ipsec-isakmp
 set peer 200.13.24.2
 set transform-set ts24
 match address actUN24
interface FastEthernet0/0
 crypto map CM24
ip access-list extended actUN24
 permit gre host 4.4.4.4 host 2.2.2.2

```


6. 2 – 4 points

- a) Configure VPN3000 with initial IP addresses.
- b) Configure OSPF on the private interface and configure R2 as the default gateway.
- c) Allow management via the public interface.

➔ **Initial and OSPF configuration must be manually because there is no route to the ACS server where the VPN is usually configured from. Here is a transcript of a VPN CLI configuration session:**

```

Login: admin
Password:
Quick -> [ 10/13/2006 ]
> Time Zone
Quick -> [ -6 ]
1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support
Quick -> [ 1 ]
> Enter IP Address
Quick Ethernet 1 -> [ 0.0.0.0 ] 172.16.10.13
Waiting for Network Initialization...
> Enter Subnet Mask
Quick Ethernet 1 -> [ 255.255.0.0 ] 255.255.255.0
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 1 -> [ 3 ]
1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex
Quick Ethernet 1 -> [ 1 ]
> MTU (68 - 1500)
Quick Ethernet 1 -> [ 1500 ]
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit
Quick -> 5
Login: admin
Password:
1) Configuration
...
6) Exit
Main -> 1
1) Interface Configuration
....
Config -> 1
1) Configure Ethernet #1 (Private)
...
Interfaces -> 1
...
7) Set Port Routing Config
...
Ethernet Interface 1 -> 7

```



```
...
3) Enable/Disable OSPF
...
Ethernet Interface 1 -> 3
1) Enable OSPF
2) Disable OSPF
Ethernet Interface 1 -> [ 2 ] 1
...
4) Set OSPF parameters
...
Ethernet Interface 1 -> 4
1) Set OSPF Area ID
Ethernet Interface 1 -> 1
> OSPF Area ID
Ethernet Interface 1 -> [ 0.0.0.0 ]
...
8) Set OSPF Authentication
Ethernet Interface 1 -> 8
1) No Authentication
2) Password Authentication
3) MD5 Authentication
Ethernet Interface 1 -> [ 1 ] 3
1) Set OSPF Password
2) Set OSPF MD5 Authentication Key ID
3) Back
Ethernet Interface 1 -> 2
> OSPF MD5 Authentication Key ID
Ethernet Interface 1 -> [ 1 ]
1) Set OSPF Password
2) Set OSPF MD5 Authentication Key ID
3) Back
Ethernet Interface 1 -> 1
> OSPF Password
Ethernet Interface 1 -> cisco
...
3) Back
Ethernet Interface 1 -> 3
...
9) Back
Ethernet Interface 1 -> 9
...
5) Back
Ethernet Interface 1 -> 5
...
11) Back
Ethernet Interface 1 -> 11
...
4) Back
Interfaces -> 4
...
2) System Management
...
Config -> 2
...
3) IP Routing (static routes, OSPF, etc.)
...
```



```
System -> 3
1) Enable/Disable OSPF
2) Set Router ID
...
OSPF -> 2
> Router ID
OSPF -> [ 0.0.0.0 ] 172.16.10.13
1) Enable/Disable OSPF
...
OSPF -> 1
1) Enable OSPF
2) Disable OSPF
OSPF -> [ 2 ] 1
...
4) Back
OSPF -> 4
...
9) Back
Routing -> 9
...
9) Back
System -> 9
1) Interface Configuration
Config -> 1
...
2) Configure Ethernet #2 (Public)
...
Interfaces -> 2
1) Interface Setting (Disable, DHCP or Static IP)
...
Ethernet Interface 2 -> 1
1) Disable
2) Enable using DHCP Client
3) Enable using Static IP Addressing
Ethernet Interface 2 -> [ 3 ] 3
...
> Enter IP Address
Ethernet Interface 2 -> [ 0.0.0.0 ] 200.13.24.13
...
> Enter Subnet Mask
Ethernet Interface 2 -> [ 255.255.255.0 ]
...
10) Set Interface WebVPN Parameters
11) Back
Ethernet Interface 2 -> 10
1) Enable/Disable HTTP and HTTPS Management
...
Ethernet Interface 2 -> 1
1) Enable HTTP and HTTPS Management
2) Disable HTTP and HTTPS Management
Ethernet Interface 2 -> [ 2 ] 1
...
7) Back
Ethernet Interface 2 -> 7
...
11) Back
Ethernet Interface 2 -> exit
```


6.3 – 3 points

- a) Configure IPSEC tunnel between R4 VLAN 4 and VPN3000 VLAN11.
- b) Use preshared key, DH1, ESP-DES, ESP-SHA-HMAC.
- c) You are allowed one static route on R4.

→ Configure R4 IPSEC parameters. A static route is needed because the IPSEC will be used only if packets are going through an interface with crypto map configured:

```
crypto isakmp policy 20
  encr 3des
  hash md5
  authentication pre-share
crypto isakmp key cisco address 200.13.24.13
crypto ipsec transform-set tsVPN esp-des esp-sha-hmac
crypto map CM24 20 ipsec-isakmp
  set peer 200.13.24.13
  set transform-set tsVPN
  match address acVPN
ip route 172.16.11.0 255.255.255.0 FastEthernet0/0
ip access-list extended acVPN
  permit ip 200.13.4.0 0.0.0.255 172.16.11.0 0.0.0.255
```

→ On the VPN configure IPSEC LAN2LAN tunnel. The hidden issue here is how R1 will know that packets to 200.13.4.0/24 should go via the VPN? the answer is “reverse-route”. Its not enough to enable reverse route on the VPN, also configure the VPN as ASBR, as these routers are external routes to OSPF:

Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

CISCO SYSTEMS

Add a new IPsec LAN-to-LAN connection.

Enable ☒


Name

Interface

Connection Type

Peers

-



Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

Preshared Key


Authentication

Encryption

IKE Proposal

Filter

IPSec NAT-T ☐



Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

Routing

Local Network: If a LAN-to-LAN NAT rule is used, this is address.

Network List

IP Address

Wildcard Mask

Configuration

Interfaces

System

User Management

Policy Management

Tunneling and Security

PPTP

L2TP

IPSec

LAN-to-LAN

IKE Proposals

NAT Transparency

Alerts

SSH

SSL

WebVPN

Administration

Monitoring

CISCO SYSTEMS

Routing

Reverse Route Injection

Local Network: If a LAN-to-LAN NAT rule is used, this is address.

Network List


Use IP Address/Wildcard-mask below

IP Address

172.16.11.0

Wildcard Mask

0.0.0.255



Configuration

- Interfaces
- System
- User Management
- Policy Management
- Tunneling and Security
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - Alerts
 - SSH
 - SSL
 - WebVPN
- Administration
- Monitoring

Wildcard Mask

Remote Network: If a LAN-to-LAN NAT rule is used, this address.

Network List

IP Address

Wildcard Mask

7 – VPN Advanced (10 points)

7.1 – 4 points

- Configure the following loopbacks on R2,R5 and R6:
 - R2 – Lo256 : 10.2.56.2/32
 - R5 – Lo256 : 10.2.56.5/32
 - R6 – Lo256 : 10.2.56.6/32
- Configure DMVPN R2 as the hub and R5,R6 as the spokes. Use interface tun256.
- Configure EIGRP on tun256 and advertise Lo256 addresses.
- Use tunnel key = 256.
- Use Network ID = 256.

- f) Ensure that spoke to spoke traffic go directly from spoke to spoke without the hub router decrypting/encrypting the packets.

→ Configure Lo256 addresses on R2, R5 and R6:

R2

```
interface Loopback256
 ip address 10.2.56.2 255.255.255.255
```

R5

```
interface Loopback256
 ip address 10.2.56.5 255.255.255.255
```

R6

```
interface Loopback256
 ip address 10.2.56.6 255.255.255.255
```

- Configure the crypto parameters; ISAKMP policy, transform sets, ISAKMP keys and IPsec profiles.
- IPsec profiles are place holders for the IPsec parameters. Crypto maps cannot be used because in DMVPN the peer IP address is unknown and so are the "SA proxies" (the crypto ACL)
- Transport mode is chosen because it produces less overhead of encapsulation GRE inside a new IP header, as it would be if the IPsec was using "tunnel mode":

```
crypto isakmp policy 30
 encr 3des
 hash md5
 authentication pre-share
crypto isakmp key cisco address 2.2.2.2
crypto isakmp key cisco address 5.5.5.5
crypto isakmp key cisco address 6.6.6.6
crypto ipsec transform-set tsDMVPN esp-des esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN
 set transform-set tsDMVPN
```

- Hub tunnel configuration is different from its spokes. The hub acts as the NHS for the spokes to register with.

```
interface Tunnel256
 ip address 172.16.56.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 256
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 256
 tunnel protection ipsec profile DMVPN
```


- The spoke configuration are the same for both R5 and R6 excluding the interface's IP address:

```
interface Tunnel256
 ip address 172.16.56.5 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map 172.16.56.2 2.2.2.2
 ip nhrp map multicast 2.2.2.2
 ip nhrp network-id 256
 ip nhrp nhs 172.16.56.2
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 256
 tunnel protection ipsec profile DMVPN
```

- Configure EIGRP on R2, R5 and R6 to run only on 172.16.56.0/24 network and also advertise Lo256:

```
router eigrp 1
 network 10.2.56.0 0.0.0.255
 network 172.16.56.0 0.0.0.255
 no auto-summary
```

- The hub needs special EIGRP configurations: Disabling split horizon so routes from R5 will be advertised to R6 via R2. Doing that will cause R2 to advertise routes from R5 with next hop = 172.16.25.2. So traffic from R6 to R5 will flow to R2, be decrypted and encrypted again and sent to R5. To correct this the command `no ip next-hop-self eigrp` needs to be configured on R2. On 12.2T IOS use `no ip route-cache` on the interfaces:

R2

```
interface Tunnel256
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
```

7.2 – 4 Points

- Configure R2 as EasyVPN server for users coming from the Internet.
 - Use local user authentication authentication.
 - Use pool named EZ_Pool using address range 10.22.33.1-10.22.33.254.
 - Use group name "EZGroup" with password "ccie".
 - Make sure remote-access users will be able to ping R4's loopback0.
 - <http://tinyurl.com/yhhopc>.
- The hidden issue here is coexistence between DMVPN and EasyVPN server on the same interface. Refer to <http://tinyurl.com/yhhopc> . Configure the EasyVPN server using ISAKMP profiles.

- Configure AAA for user authentication and configuration for EZVPN, IP pool and group configuration:

```
aaa authentication login easyVPN local
aaa authorization network easyVPN local
username cisco password cisco
ip local pool EZ_Pool 10.22.33.1 10.22.33.254
crypto isakmp client configuration group EZGroup
key ccie
pool EZ_Pool
```

- Configure ISAKMP profile. The profile will match the EZGroup and set its configuration and user authentication:

```
crypto isakmp profile EZGroup
match identity group EZGroup
client authentication list easyVPN
isakmp authorization list easyVPN
client configuration address respond
```

- Configure dynamic crypto map which will bind the ISAKMP profile and the IPsec parameters such as the transform-set. Configure also reverse route so other routers will know how to reach the connected remote users:

```
crypto dynamic-map DYN 10
set transform-set ts24
set isakmp-profile EZGroup
reverse-route
```

- Configure crypto-map to bind the dynamic map to a static map and apply the map to then interface facing the Internet s0/1/0.26. Also configure the local address for the crypto-map to Lo0 so it will match the DMVPN ISAKMP addresses:

```
crypto map CMEZ local-address Loopback0
crypto map CMEZ 999 ipsec-isakmp dynamic DYN
interface Serial0/1/0.26 multipoint
crypto map CMEZ
```

7.3 – 2 Points

- Configure VPN from R4 to ASA to protect traffic from R4 Lo0 to R1 Lo0.
 - Limit traffic from the R1's Lo0 to R4's Lo0 to 128kb per flow. Do not configure QoS on R4 or R1.
 - You are allowed one static route on R4.
- Configure the IPsec tunnel on R4. A static route is needed to force traffic destined to R1 Lo0 going through the crypto map on f0/0:

```
crypto isakmp policy 30
encr 3des
hash md5
authentication pre-share
group 2
```



```
crypto isakmp key cisco address 200.13.24.9
ip access-list extended acVPN1
  permit ip host 4.4.4.4 host 1.1.1.1
crypto map CM24 30 ipsec-isakmp
  set peer 200.13.24.9
  set transform-set tsVPN
  match address acVPN1
ip route 1.1.1.1 255.255.255.255 FastEthernet0/0
```

- Configure the IPsec tunnel on the ASA. As the current NAT rules, the traffic from 1.1.1.1 will be NATed, to avoid this configure NAT exemption so the ASA won't NAT 1.1.1.1 traffic when the destination is 4.4.4.4:

```
access-list acVPN4 extended permit ip host 1.1.1.1 host 4.4.4.4
nat (inside) 0 access-list acVPN4
crypto ipsec transform-set tsR4 esp-des esp-sha-hmac
crypto map CM 10 match address acVPN4
crypto map CM 10 set peer 200.13.24.4
crypto map CM 10 set transform-set tsR4
crypto map CM interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp nat-traversal 20
tunnel-group 200.13.24.4 type ipsec-l2l
tunnel-group 200.13.24.4 ipsec-attributes
  pre-shared-key cisco
```

- Configuring QoS matching "esp host 200.13.24.9 host 200.13.24.4" will not allow to do QoS per flow. Configure class-map to match the tunnel group and to match "pre-flow" then limit the traffic using the policy-map:

```
class-map VPN_R4
  match flow ip destination-address
  match tunnel-group 200.13.24.4
policy-map pmOUT
  class VPN_R4
    police 128000
```

8 – IOS Firewall and NAT (8 points)

8.1 – 4 points

- Configure R2 to protect VLAN24 and VLAN 112 from internet traffic using CBAC.
- Allow only the minimum from the Internet.
- Log all sessions to the ACS server.
- During port scan attacks, the router is very busy sending logs to the ACS. Configure the router not to send these logs.

- e) Allow any TCP/UDP/ICMP sessions initiated from VLAN24 and VLAN112.
- f) Allow any ICMP traffic.
- g) Do not allow Java applications. Some web servers on the Internet use port 8080.
- h) Drop TCP sessions after one hour of inactivity time.
- i) Start deleting half open sessions when there are 1000 half open sessions. Stop deleting when there are 500 half open sessions.

→ **Configure ACL to allow the only the required traffic from R6. At the end of the ACL log all denied traffic so it will be easier to debug the ACL during the lab:**

```
ip access-list extended CBAC
 permit esp any host 2.2.2.2
 permit udp any host 2.2.2.2 eq isakmp
 permit udp any host 2.2.2.2 eq non500-isakmp
 permit ospf host 200.13.26.6 host 224.0.0.5
 permit ospf host 200.13.26.6 host 224.0.0.6
 permit ospf host 200.13.26.6 host 200.13.26.2
 permit icmp any any
 permit tcp host 200.13.26.6 host 200.13.26.2 eq bgp
 permit tcp host 200.13.26.6 eq bgp host 200.13.26.2
 permit tcp host 6.6.6.6 host 200.13.24.100 eq tacacs
 deny ip any any log
 interface Serial0/1/0.26 multipoint
 ip access-group CBAC in
```

→ **Configure the R2 to inspect TCP/UDP/ICMP traffic. It is possible to choose the direction and location of the inspection, using the "out" direction of the interface facing the internet will cause any traffic going through R2 to the internet to be inspected:**

```
ip inspect name FWOUT tcp
ip inspect name FWOUT udp
ip inspect name FWOUT icmp
interface Serial0/1/0.26 multipoint
ip inspect FWOUT out
```

→ **CBAC produces two types of logs: Audit trails and alerts. Audit trails log every session passing through the firewall and alerts log protocol security problems and some basic attacks. Configure CBAC to turn off the alerts. Also configure CBAC to log all sessions:**

```
ip inspect alert-off
ip inspect audit-trail
```

→ **Configure CBAC to block java, and configure R2 watch for http also on port 8080:**

```
ip port-map http port tcp 8080
ip inspect name FWOUT http java-list 99
```


→ Tune CBAC timers:

```
ip inspect max-incomplete low 500
ip inspect max-incomplete high 1000
```

→ Configure logging to the ACS. Remember that the ASA will accept syslog packets only from the router's Lo0:

```
logging source-interface Loopback0
logging 200.13.24.100
```

8.2 – 2 points

- a) Configure R4 to authenticate users browsing BB1.
- b) Configure R4 to download ACL from ACS. Use username R4 and password cisco. Configure ACS to allow any IP traffic.

→ Configure AAA on R4 to authenticate and authorize auth-proxy sessions. The http server will use the authentication configuration of its vty lines. On some IOS there is a bug, the auth-proxy will use the console authentication methods. Remember that the ASA will allow TACACS traffic only from router's Lo0 interface:

```
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
tacacs-server host 200.13.24.100 key cisco
tacacs-server directed-request
ip tacacs source-interface Loopback0
```


→ Configure the http server on R4:

```
ip http server
ip http authentication aaa
```

→ Configure the auth-proxy and apply it to f0/0:

```
ip auth-proxy name AUTHPROXY http
interface FastEthernet0/0
ip auth-proxy AUTHPROXY
```


→ Configure ACS with a new service type under the interface configuration:



Interface Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

☐ PPP VPDN
☐ PPP LCP
☐ ARAP
☒ Shell (exec)
☐ PDX Shell (pixshell)
☐ SLIP

New Services

Service	Protocol
<input checked="" type="checkbox"/> auth-proxy	
<input type="checkbox"/>	

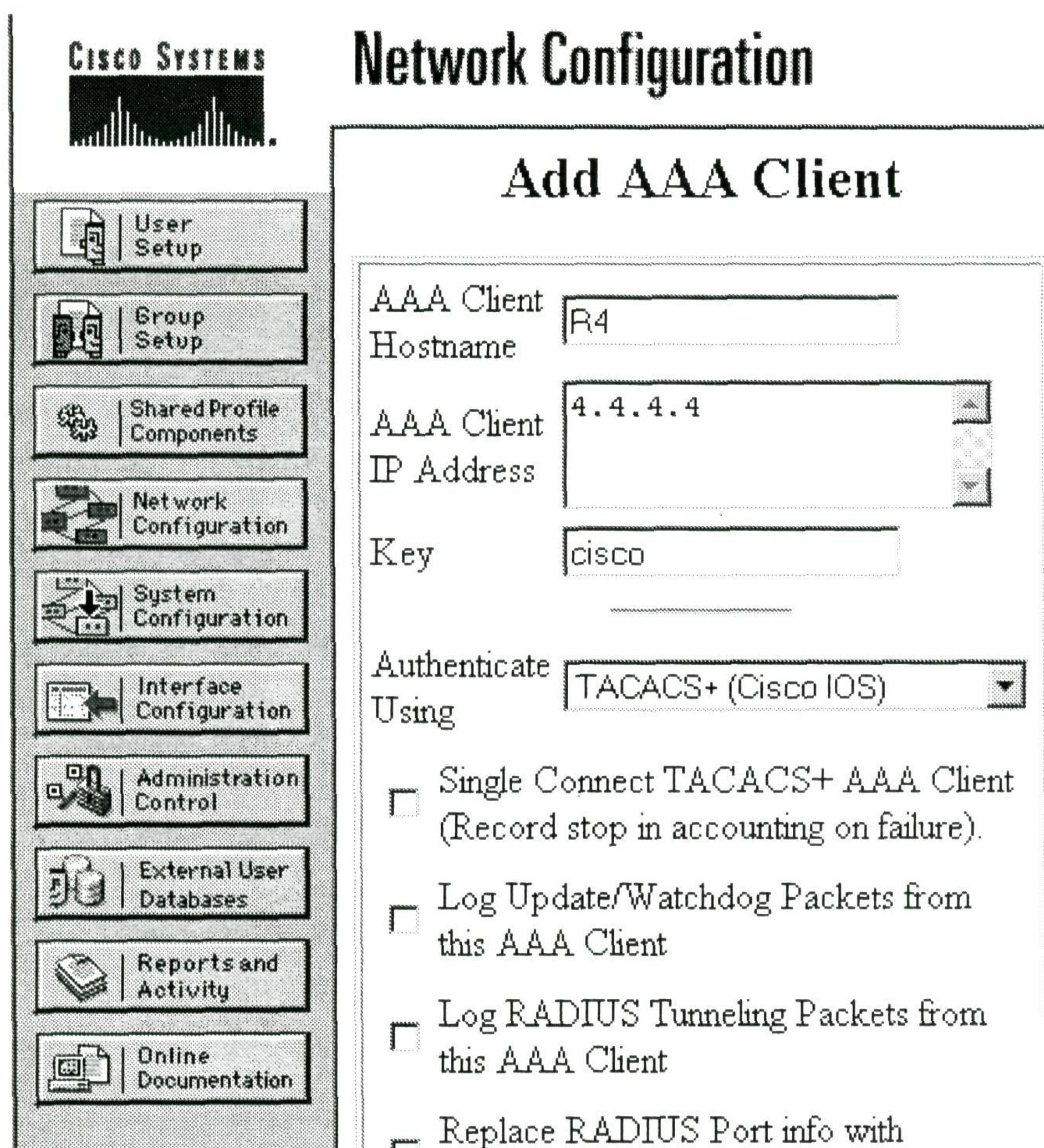
Advanced Configuration Options ?

☒ Advanced TACACS+ Features
☐ Display a Time-of-Day access grid for every TACACS+ service where you can

Submit

Cancel

→ Configure R4 in the ACS client configuration:



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration (which is highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure): ☐
- Log Update/Watchdog Packets from this AAA Client: ☐
- Log RADIUS Tunneling Packets from this AAA Client: ☐
- Replace RADIUS Port info with: ☐

- Configure the group with auth-proxy service and av-pairs which will allow any IP traffic one a client authenticated to R4:

CISCO SYSTEMS

Group Setup

Jump To: **RADIUS (IETF)**

Unlisted arguments

☐ Permit

☒ Deny

☒ auth-proxy

☒ Custom attributes

priv-lvl=15
proxyacl#1=permit ip any any

Submit Submit + Restart Cancel

8.3 – 2 Point

- a) Configure lo66 on R6:

→ Lo66 : 10.66.66.66/24

- b) R6's loopback66 should be seen as 200.13.26.26 to the frame-relay cloud.

→ Configure Lo66 and NAT on R6:

```
interface Loopback66
 ip address 10.66.66.66 255.255.255.0
 ip nat inside
interface Serial0/1/0.26 multipoint
 ip nat outside
access-list 11 permit 10.66.66.0 0.0.0.255
ip nat pool P66 200.13.26.26 200.13.26.26 prefix-length 30
ip nat inside source list 11 pool P66 overload
```


- There is a hidden issue here .There is no mapping for 200.13.26.26 address on R2 frame-relay interface. Configure frame-relay mapping on R2:

```
interface Serial0/1/0.26 multipoint
frame-relay map ip 200.13.26.26 206
```

9 – Security and Attacks (6 points)

9.1 – 2 points

- a) Using NBAR, block Code Red on R6 coming from the Internet.

- Configure class map to match http urls used by NBAR. Then configure policy-map to match the CodeRed class and drop the packets. Apply the policy map to f0/0 interface:

```
class-map match-all CodeRed
match protocol http url "*default.ida*"
match protocol http url "*CMD.exe*"
match protocol http url "*root.exec*"
!
!
policy-map pmCodeRed
class CodeRed
drop
interface FastEthernet0/0
service-policy input pmCodeRed
```

9.2 – 2 points

- a) You notice that BB1 is generating too much broadcasts on VLAN4, restrict broadcasts from BB1 to 20%.

- Configure the switch to control the amount of broadcasts on the interface facing BB1 using the storm-control command:

```
interface FastEthernet0/11
storm-control broadcast level 20.00
```

9.3 – 2 points

- a) There is a web server on VLAN6. Its IP address is 200.13.6.80.
- b) Protect the server from Denial of service by enabling the TCP intercept for that server.
- c) Watch the connection and drop connections if they don't complete in 10 seconds.
- Configure ip tcp intercept to protect the web server. Use watch mode protection and tune the idle timeout parameter:

```
ip tcp intercept list 166
ip tcp intercept watch-timeout 10
```



```
ip tcp intercept mode watch
access-list 166 permit tcp any host 200.13.6.80
```

10 – Security and Attacks – Advanced (8 points)

10.1 – 6 points

- a) Discard traffic from a list of networks on R2, R5 and R6 that might be coming from the F/R network. Do not use ACL, MCQ or PBR.
- b) You are allowed one static route on R5 and R6 routers. You are allowed 4 static routes on R2.
- c) This is the list of networks to discard traffic from:

- 199.100.222.0/24
- 199.100.224.0/24
- 199.100.226.0/24
- 199.100.228.0/24

- One way to discard traffic is by using ip verify unicast reverse-path. Any packet coming from an interface that will fail the reverse-path check will be dropped. Reverse-path searches each packet's source IP addresses in the router's routing table and finds a matching interface. If the packet does not come from that interface, the packet is dropped. By setting the next-hop interface of 199.100.222.0/24 route to a null interface will cause all reverse-path checks to fail for packets with source IP of 199.100.222.0/24 range.
- Since only R2 is allowed 4 static routes, and R5 and R6 are allowed only one static route, R2 will send the list of routes to R5 and R6 via BGP, while setting the next hop to 99.99.99.99.
- Configure R5 and R6 to statically route 99.99.99.99 to Null0 interface and configure reverse path router on the FR interfaces of R2, R5 and R6. When R5 and R6 will get a list of routes from R2 with next-hop set to 99.99.99.99 the effective next-hop of this routes will be Null0.
- Configure R2 with static routes to the list of networks, route-map to set the next-hop to 99.99.99.99, advertise these routes in BGP and use the route-map to change their next-hop when they are advertised to R5 and R6:

```
ip route 199.100.222.0 255.255.255.0 Null0
ip route 199.100.224.0 255.255.255.0 Null0
ip route 199.100.226.0 255.255.255.0 Null0
ip route 199.100.228.0 255.255.255.0 Null0
route-map rmBGP permit 10
  set ip next-hop 99.99.99.99
router bgp 65001
  network 199.100.222.0
  network 199.100.224.0
  network 199.100.226.0
  network 199.100.228.0
```

```
neighbor 200.13.25.5 route-map rmBGP out
neighbor 200.13.26.6 route-map rmBGP out
```


- **Configure static route for 99.99.99.99 on R5 and R6:**

```
ip route 99.99.99.99 255.255.255.255 Null0
```

- **Configure reverse-path checking on all FR interfaces:**

```
interface Serial0/1/0.2[56] multipoint
ip verify unicast reverse-path
```

10.2 – 2 points

- a) Some old PC's on VLAN11 are vulnerable to some AppleTalk attacks. Prevent IPX running on VLAN11.

- **Configure VLAN filter, to filter AppleTalk. Configure the same filters on all switches with active VLAN11 ports on them:**

```
mac access-list extended NOAPPLE
 permit any any appletalk
vlan access-map VNOAPPLE 10
 action drop
 match mac address NOAPPLE
vlan access-map VNOAPPLE 20
 action forward
vlan filter VNOAPPLE vlan-list 11
!
```

11 – IDS Basic (4 points)

11.1 – 2 points

- a) Configure IDS's C&C interface using CLI.
- b) Add IDS to IEV Console.
- c) Configure the switches to copy all traffic from VLAN 10 to the IDS's sensor interface.

- **Configure initial configuration using the IDS CLI:**

```
IDS#setup
...
Continue with configuration dialog?[yes]:
Enter host name[IDS]:

Enter IP interface[10.1.1.15/24,10.1.1.1]: _
172.16.10.14/24,127.16.10.1
Enter telnet-server status[disabled]:

Enter web-server port[443]:

Modify current access list?[no]: yes
Current access list entries:

[1] 10.1.1.0/24
```


Delete: 3

Delete:

Permit: 172.16.11.0/24

Permit:

Modify system clock settings? [no] :

Modify virtual sensor "vs0" configuration? [no] :

...

[2] Save this configuration and exit setup.

Enter your selection [2] :

Configuration Saved.

→ Add IDS to the IEV console:

The screenshot shows a 'Device Properties' window with the following sections:

- New Sensor Information**
 - Sensor IP Address: 172.16.10.14
 - Sensor Name: IDS
 - User Name: cisco
 - Password: *****
 - Web Server Port: 443
- Choose the communication protocol**
 - ☒ Use encrypted connection (https)
 - ☐ Use non-encrypted connection (http)
- Event Start Time (UTC)**
 - ☒ Latest Alerts
 - Start Date (Y/Y/Y MM/DD): [] : [] : []
 - Start Time (HH/MM/SS): [] : [] : []
- Exclude alerts of the following severity level(s)**
 - ☐ Informational
 - ☐ Low
 - ☐ Medium
 - ☐ High

- Configure the switches with RSPAN session to pass traffic to the IDS sensor interface:

CAT1

```
Vlan 99
  remote-span
exit
monitor session 1 source vlan 10 rx
monitor session 1 destination remote vlan 99 reflector-port
Fa0/20
monitor session 2 destination interface Fa0/7
monitor session 2 source remote vlan 99
```

CAT2/3/4

```
monitor session 1 source vlan 10 rx
monitor session 1 destination remote vlan 99 reflector-port
Fa0/20
```

11.2 – 2 point

- a) Enable the ICMP echo and ICMP echo-reply alarms.
- b) The Alarm severity should be High.
- c) Test the alarm.

→ Set the alarm priority on the IDS for signatures 2000 and 2004

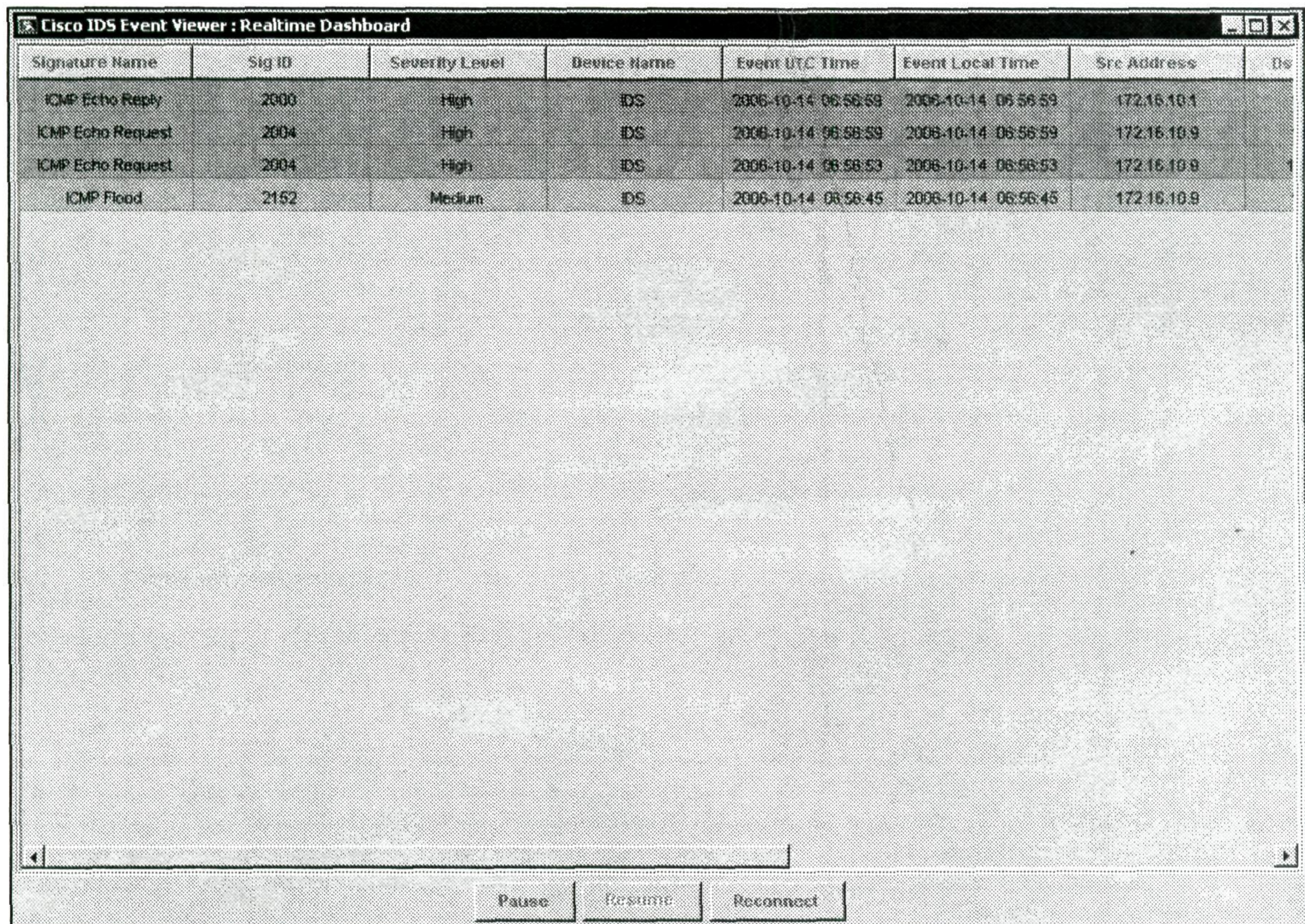
Signature Configuration

Select By: L2/L3/L4 Protocol Select Protocol: General ICMP

Sig ID	SubSig ID	Name	Enabled	Action
2000	0	ICMP Echo Reply	Yes	Produce Alert
2001	0	ICMP Host Unreachable	No	Produce Alert
2002	0	ICMP Source Quench	No	Produce Alert
2003	0	ICMP Redirect	No	Produce Alert
2004	0	ICMP Echo Request	Yes	Produce Alert
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert
2006	0	ICMP Parameter Problem on ...	No	Produce Alert
2007	0	ICMP Timestamp Request	No	Produce Alert
2008	0	ICMP Timestamp Reply	No	Produce Alert
2009	0	ICMP Information Request	No	Produce Alert
2010	0	ICMP Information Reply	No	Produce Alert
2011	0	ICMP Address Mask Request	No	Produce Alert
2012	0	ICMP Address Mask Reply	No	Produce Alert
2153	0	ICMP Smurf Attack	No	Produce Alert
2154	0	Ping of Death Attack	No	Produce Alert
2155	0	Modem DoS	No	Produce Alert

Buttons: Select All, NSDB Link, Add, Clone, Edit, Enable, Disable, Actions, Restore Defaults, Delete, Activate, Retire, Apply, Reset

→ Generate ICMP traffic on VLAN10 and check the IEV:



Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst
ICMP Echo Reply	2000	High	IDS	2006-10-14 06:58:59	2006-10-14 06:58:59	172.16.10.1	
ICMP Echo Request	2004	High	IDS	2006-10-14 06:58:59	2006-10-14 06:58:59	172.16.10.9	
ICMP Echo Request	2004	High	IDS	2006-10-14 06:58:53	2006-10-14 06:58:53	172.16.10.9	
ICMP Flood	2152	Medium	IDS	2006-10-14 06:58:45	2006-10-14 06:58:45	172.16.10.9	

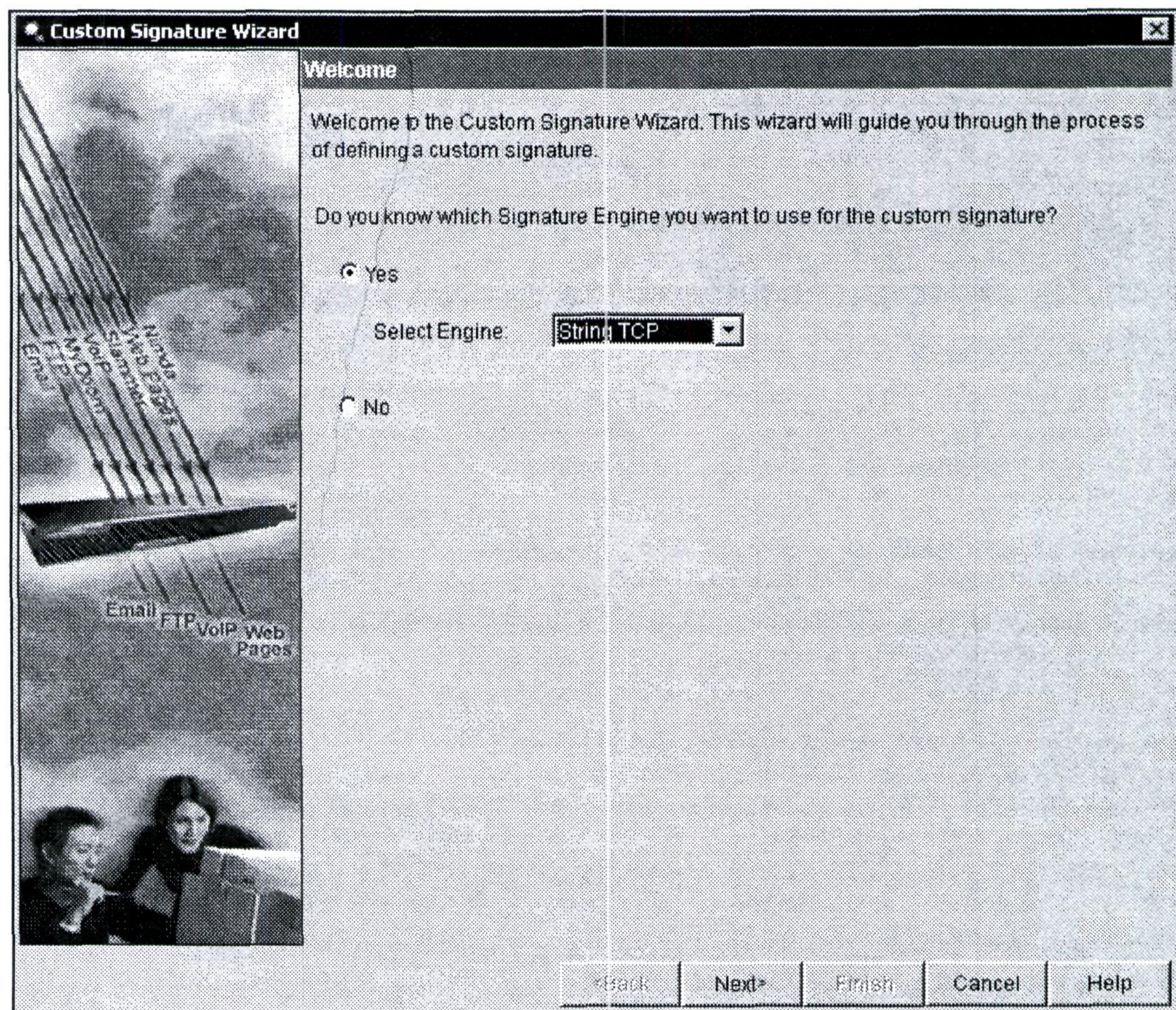
Below the table is a large, empty, light-gray rectangular area, likely a placeholder for a map or detailed event information. At the bottom of the window are three buttons: 'Pause', 'Resume', and 'Reconnect'.

12 – IDS Advanced (10 points)

12.1 – 4 points

- Define custom signature which will trigger when the following keywords are seen in a telnet session:
 - Cisco
 - clsco
 - ciSco
- The alarm severity should be medium.
- When the alarm fires, use the ASA to block traffic. The sensor should not telnet to the ASA.
- Do not fire events for traffic originated from ASA.

- Start the custom signature wizard and choose "Stream TCP" engine and press next:



- Choose Produce Alert and Request Block Host in the Event action. The regex sting is "(Cisco)|(clsco)|(ciSco)" which will match any "|" of the stings encapsulated in "()". Configure the port to watch to 23 – Telnet and press next:

Custom Signature Wizard

Engine Specific Parameters

Engine-specific parameters determine what the signature looks for and what causes the signature to fire. You can set the following String TCP engine parameters used for this signature.

☒ Event Action: **Produce Alert**

☒ Strip Telnet Options: No

Specify Min Match Length: No

Regex String: (Cisco)|(clsco)|(ciSco)

Service Ports: 23

☒ Direction: To Service

☒ Specify Exact Match Offset: No

Specify Max Match Offset: No

Specify Min Match Offset: No

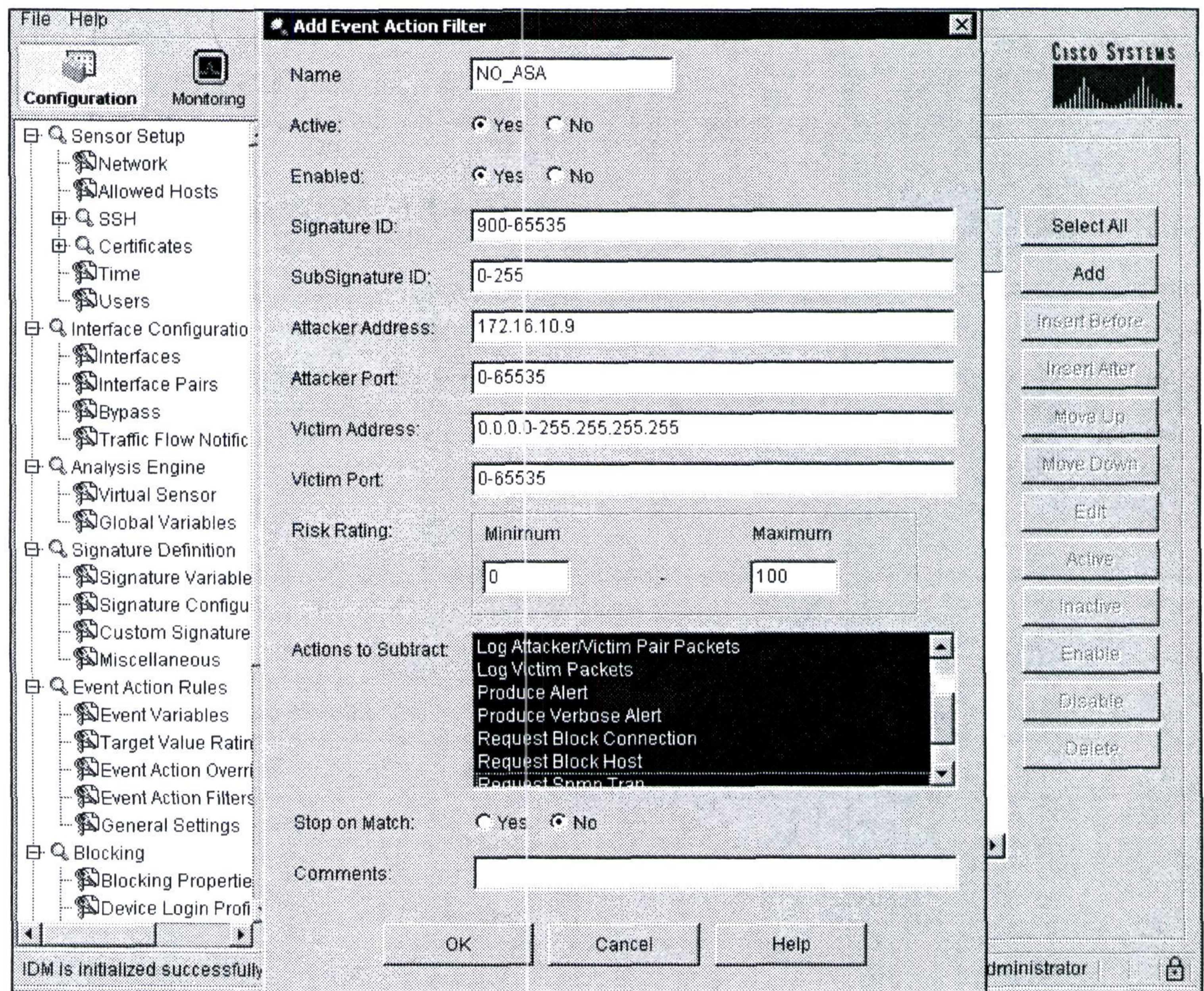
☒ Parameter uses the Default Value. Click the icon to edit the value.

☒ Parameter uses a User-Defined Value. Click the icon to restore the default value.

<Back Next> Finish Cancel Help

- Press next next next... finally press finish and apply.

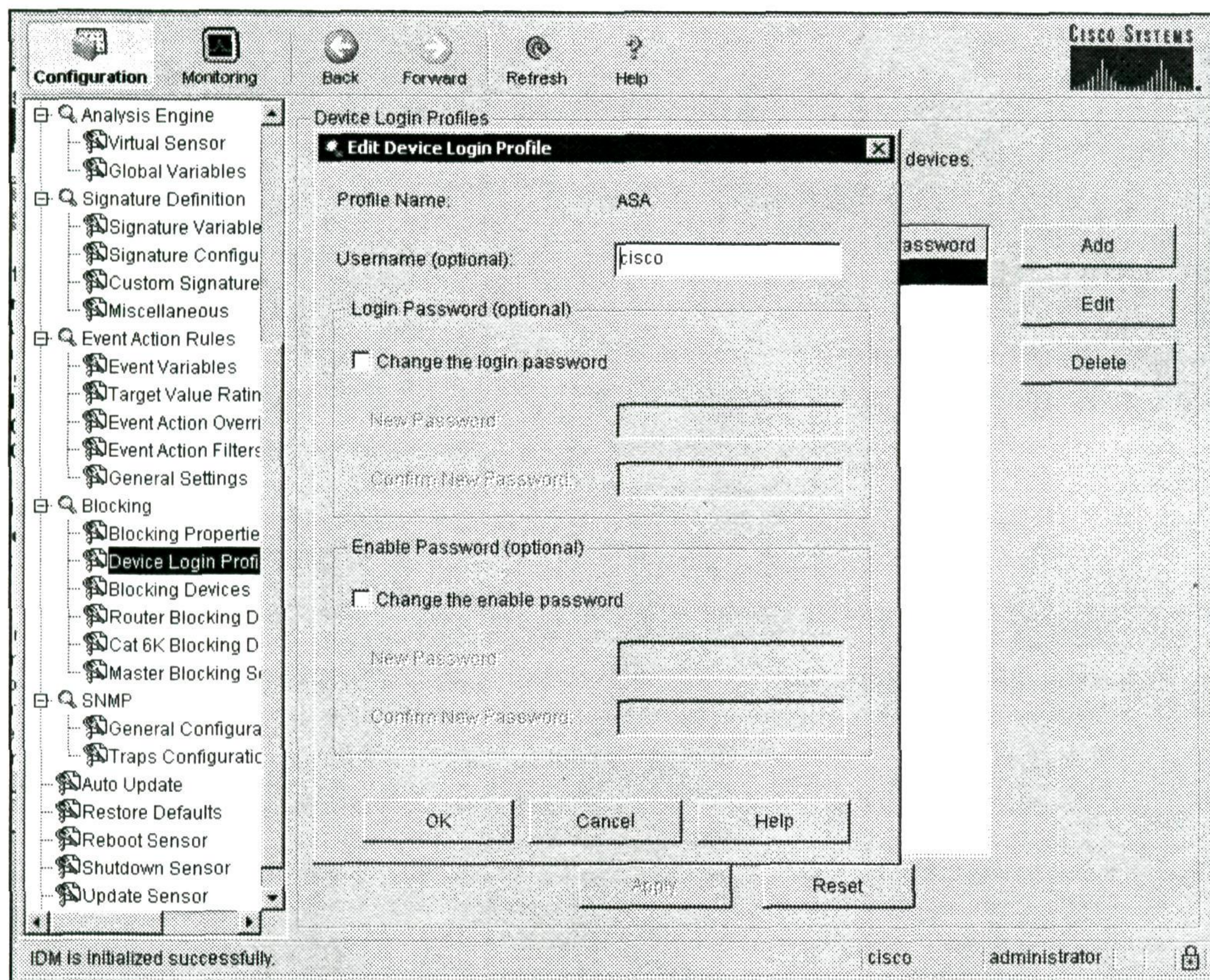
→ Configure event filter to filter events coming from the ASA:



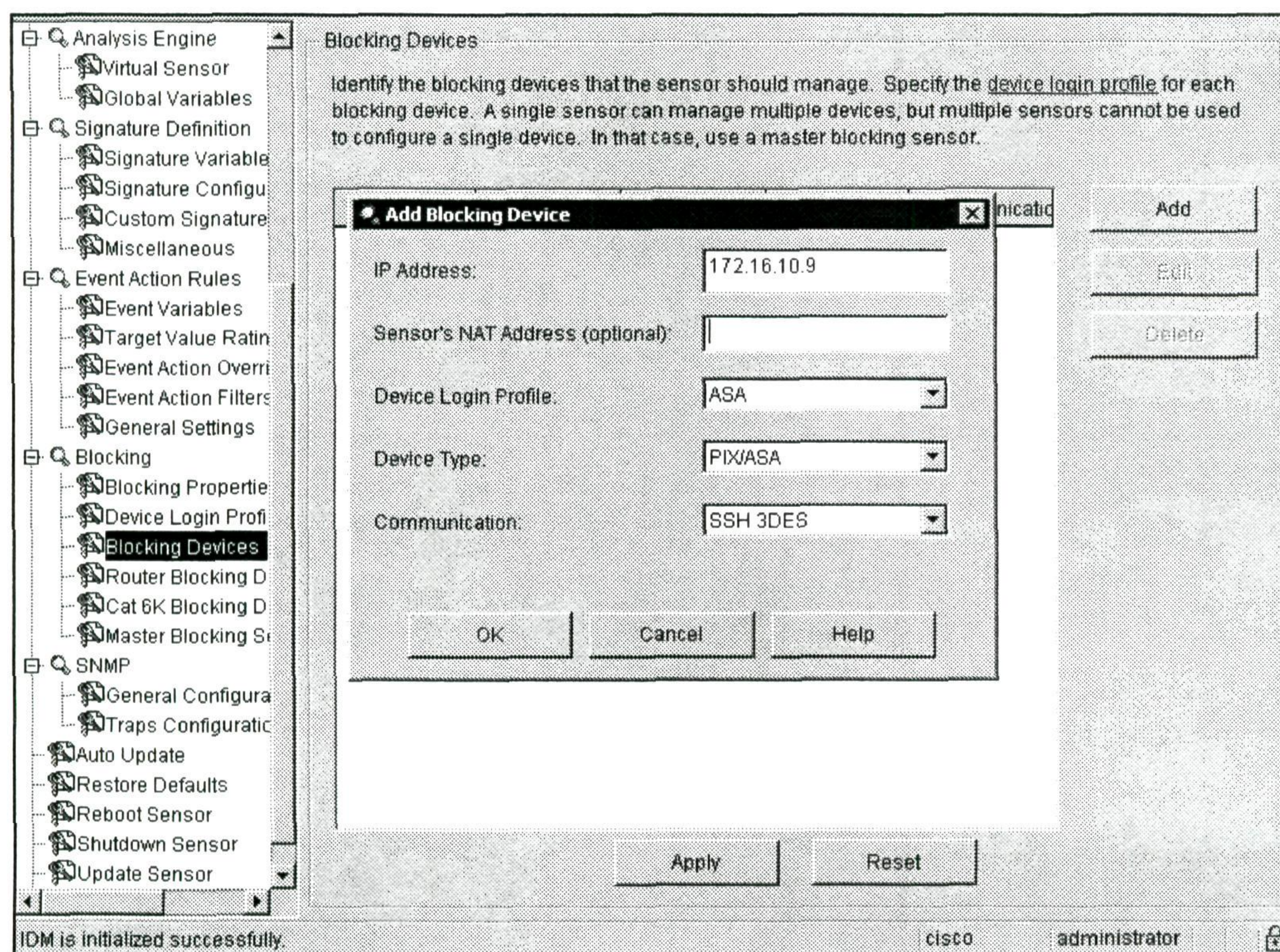
→ Configure the ASA for SSH login from the IDS. Configure local authentication for SSH. Generate RSA key and configure SSH access ASA:

```
username cisco password cisco
aaa authentication ssh console LOCAL
ssh 172.16.10.14 255.255.255.255 inside
```


→ **Configure device login profile for the ASA:**



→ **Add the ASA as device for blocking:**



- The IDS needs to know what the public key of the ASA is, use "Add Known Host Key" screen and press the "Retrieve Host Key":

Add Known Host Key

IP Address: 172.16.10.9 Retrieve Host Key

Modulus Length: 512

Public Exponent: 65537

Public Modulus: 1001545754210123571581164560655864197951877343810968892273
9424158785163423235438634917749941993172434899058950859982
410034663721311504303650621382488326449

OK Cancel Help

→ Check the new signature by generating alarm and watch for alarm:

```

R1
R1#telnet 172.16.10.13
Trying 172.16.10.13 ... Open
Login: admin
Password:

Welcome to
Cisco Systems
VPN 3000 Concentrator Series
Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.

1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main -> Cisco

```

Cisco IDS Event Viewer : Realtime Dashboard							
Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Us
My Sig	60000	Medium	IDS	2006-10-14 15:50:00	2006-10-14 15:50:00	172.16.10.1	1
ICMP Echo Request	2004	High	IDS	2006-10-14 06:57:24	2006-10-14 06:57:24	172.16.10.9	1
ICMP Echo Reply	2003	High	IDS	2006-10-14 06:56:59	2006-10-14 06:56:59	172.16.10.1	
ICMP Echo Request	2004	High	IDS	2006-10-14 06:56:58	2006-10-14 06:56:58	172.16.10.8	
ICMP Echo Request	2004	High	IDS	2006-10-14 06:56:53	2006-10-14 06:56:53	172.16.10.9	1
ICMP Flood	2152	Medium	IDS	2006-10-14 06:56:45	2006-10-14 06:56:45	172.16.10.9	

12.2 – 2 points

- Enable IPS on the PIX outside interface.
- The pix should send alarms to the syslogd server.
- The pix should drop attacks.
- Disable ICMP echo, and ICMP echo-reply signatures.

e) Do not configure ACL on any device.

- Configure the IPS on the PIX to send alarm when info signatures are triggered and drop packets when attack signatures are triggered:

```
ip audit name A2 info action alarm
ip audit name A1 attack action drop
ip audit interface outside A2
ip audit interface outside A1
```

- Configure the PIX to send syslog to the ACS. The hidden issue here is that the ASA is not configured to allow the PIX sending syslog. Add the PIX address to the group of hosts allowed sending syslog to the ACS.

PIX

```
logging host outside 200.13.24.100
```

ASA

```
object-group network netL00
network-object host 200.13.112.11
```

- Disable echo and echo-reply signatures. To find the number of the signature use the show audit count command:

```
ip audit signature 2000 disable
ip audit signature 2004 disable
```

Technical Verification and Support

To verify your router configurations please ensure that you have downloaded the latest configurations at www.IPexpert.com. Please visit the following web site for instructions: <http://www.ipexpert.com/configs>

Support is also available in the following ways:

- Email: support@ipexpert.com
- Telephone (US and Canada): +1.866.225.8064
- Telephone (Outside U.S. & Canada): +1.810.326.1444
- Support Ticket System (Elite Members): <http://www.ipexpert.com>
- Mailing List: <http://www.OnlineStudyList.com>
- Online Forum: <http://www.CertificationTalk.com>

Section 18: Multiprotocol Challenge G One Day Lab Experience)

Estimated Time to Complete: 8 Hours

NOTE:

Please reference your Security Workbook for all diagrams and tables.



Section 18 Pre-Lab Setup

Pre-load the Initial Configurations for all the devices. You will find these configurations in the "Initial Configurations" subfolder within each section (i.e. *IPexpert CCIE Security 4.0 WB Configs* → Section 18 → Initial Configurations → Router X.txt.). To ensure you are using the most up-to-date and accurate configurations, please be sure to check the "MY CONFIGS" area of your www.IPexpert.com Member's Area.

1 – Bridging and Switching (4 points)

1.1 – 2 points

- a) Configure SSH only access on CAT1. Make sure no other method is allowed.
- b) Only allow direct connected networks to connect to the switch.
- c) Use local database for authentication.
- d) After authentication the switch should send a greeting to the user.

→ To enable SSH first configure the domain name and generate the RSA keys:

```
ip domain-name ipexpert.net
crypto key generate rsa general-keys modulus 1024
```

→ Configure ACL to define which SSH clients are allowed to initiate a session:

```
access-list 1 permit 192.168.12.0 0.0.0.255
```

→ Configure a user and a password to be used for SSH authentication:

```
username cisco password cisco
```

→ Configure VTY lines to accept only SSH, apply the ACL to the incoming session requests and use the local authentication database:

```
line vty 0 15
 access-class 1 in
 login local
 transport input ssh
```

→ Configure an exec banner to show a message to users after a successful login.

```
banner exec X
welcome !!!
X
```

1.2 – 2 points

- a) Configure a macro to set a port with the following security parameters:
- b) Turn on DTP.

- c) Set mode to access.
 - d) The switch should shutdown the interface if BPDUs are received.
 - e) Protect the port from mac-address-table flood. Allow only 1 MAC entry for each port.
 - f) Apply the macro to all ports connected to the ASAs and to the PIX.
- **Configure a macro to be used as a template for interface configuration. Apply the macro on all switches with PIX/ASA ports:**

```
macro name SECURE
! setting the port mode to access - needed to turnoff DTP
switchport mode access
! turn off DTP
switchport nonegotiate
! bpduguard will shut the interface when receiving BPDUs
spanning-tree bpduguard enable
! enable port security and limit the MACs allowed per port to one
switchport port-security
switchport port-security maximum 1
```

- **Apply the macro to all switches with PIX/ASA ports:**

```
interface range f0/10 - 13
macro apply SECURE
```

2 – PIX basic (5 points)

2.1 – 2 points

- a) Configure host name to "PIX".
 - b) Configure PIX interfaces according to the IP addressing table.
 - c) Configure domain name to "ipexpert.net".
- **Configure the basic PIX setup, including nameif, security-level and the IP address:**

```
hostname PIX
domain-name ipexpert.net
interface Ethernet0
 nameif outside
 security-level 0
 ip address 9.12.112.10 255.255.255.0
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.12.10 255.255.255.0
```


2.2 – 2 points

- a) Hosts on the inside should use NAT pool of 9.12.112.30-50.
- b) Allow hosts to connect to the network even if the NAT pool is overloaded.
- c) The switch should appear as 9.12.112.11. The pix should not change any TCP header's field other than the checksum field.
- d) The switch is not configured with a default gateway. Configure the PIX to allow routers to connect to CAT1 using SSH.

→ **Configure NAT pool and leave the last address to be used for PAT in case the pool is exhausted:**

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 9.12.112.30-9.12.112.49
global (outside) 1 9.12.112.50
```

→ **Configure static NAT translation for the switch global address. Configure the PIX not to randomize the TCP sequence number, so the only TCP header field that will be changed is the checksum, due to the changing IP addresses:**

```
static (inside,outside) 9.12.112.11 192.168.12.11 netmask \
255.255.255.255 norandomseq
```

→ **To allow SSH connections to CAT1, first create ACL and then apply it to the outside interface:**

```
access-list OUT extended permit tcp any host 9.12.112.11 eq ssh
access-group OUT in interface outside
```

→ **CAT1 allows only the 192.168.12.0/24 network to connect using SSH. Configure outside NAT so SSH sessions coming to CAT1 will be translated to appear as if they are coming locally from VLAN12:**

```
access-list NAT_OUT extended permit tcp any host 9.12.112.11 eq
ssh
nat (outside) 2 access-list NAT_OUT outside
global (inside) 2 192.168.12.99
```

→ **Note that since the connection will come from VLAN12, CAT1 won't need a default gateway to communicate with it's SSH clients as they are on the same directly connected network.**

2.3 – 1 point

- a) Allow only the inside network to ping the PIX. Allow to PIX to ping everywhere.
- **Configure the PIX to deny any echo requests from the outside interface and allow all other ICMP packets. The order of the icmp statements is important:**

```
icmp deny any echo outside
icmp permit any outside
icmp permit any inside
```


3 – ASA basic (15 points)

3.1 – 4 points

- a) Configure ASA1 with two security contexts.
- b) Name the first Vasa1a and the second Vasa1b.
- c) Allocate and name the interfaces according to the IP addressing table.
- d) Configure IP addresses according to the IP addressing table.
- e) Configure Vasa1 to be the “admin” context.

→ First set the mode of ASA1 to multiple contexts:

```
mode multiple
```

→ After the ASA reboots configure the sub interfaces so it will be possible to allocate them to the virtual contexts:

```
interface Ethernet0/2.10
vlan 10
interface Ethernet0/2.11
vlan 11
```

→ Create the contexts and allocate the interfaces:

```
context Vasala
allocate-interface Ethernet0/0
allocate-interface Ethernet0/1
config-url disk0:/Vasala
context Vasalb
allocate-interface Ethernet0/2
allocate-interface Ethernet0/2.10-Ethernet0/2.11
allocate-interface Ethernet0/3
config-url disk0:/Vasalb
```

→ Set the Vasa1a context to be the admin context:

```
admin-context Vasala
```

→ Configure CAT3 port, which is connected to e0/2 of ASA1 to be a trunk, and remove port security, because there will be more than one mac address for that port:

```
int f0/12
no switchport port-security
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,11
```


- Configure Vasa1a context with nameif, security-level and IP addresses:

```
hostname Vasala
interface Ethernet0/0
  nameif inside
  security-level 100
  ip address 192.168.10.9 255.255.255.0
interface Ethernet0/1
  nameif outside
  security-level 0
  ip address 9.12.112.9 255.255.255.0
```

- Configure Vasa1b context with nameif, security-level and IP addresses:

```
hostname Vasalb
interface Ethernet0/2.10
  nameif inside
  security-level 100
  ip address 192.168.10.19 255.255.255.0
interface Ethernet0/2.11
  nameif DMZ
  security-level 50
  ip address 192.168.11.19 255.255.255.0
```

3.2 – 3 points

- Configure ASA2 as transparent firewall.
- Configure the interfaces according to the diagram.
- Make sure traffic between BB1 and R1 pass through the ASA.

- Set ASA2 mode to transparent mode and set the host name:

```
firewall transparent
host ASA2
```

- Set the inside interface and the outside interface, no need for IP addresses:

```
int e0/0
  nameif inside
  no shut
int e0/1
  nameif outside
  no shut
```

- Even if this lab does not use the management interface, it still needed to be configured for correct operation of the ASA. Without it the transparent configuration won't be complete and the behavior will be "undefined" :

```
ip address 13.13.13.13 255.255.255.0
int management 0/0
  no shut
```


- Now we need to force traffic between BB1 and R1 to pass through ASA2, to do that split VLAN101 to two VLANS. VLAN101 as the inside VLAN and VLAN102 as the outside VLAN:
- On CAT1 add VLAN102 to the VLAN database and configure BB1's interface to VLAN102:

```
vlan 102
int f0/11
switchport access vlan 102
```

- On CAT4 configure ASA's outside interface to VLAN102, inside interface to VLAN101 and turn off port security:

```
int f0/10
switchport access vlan 101
no switchport port-security
int f0/11
switchport access vlan 102
no switchport port-security
```

3.33 - 3 points

a) On Vasa1a:

- Hosts on the inside should use NAT pool of 9.12.112.230-250.
- Allow hosts to connect to the network even if the NAT pool is overloaded.
- The ACS should appear as 9.12.112.100.
- Allow routes loopbacks to access the ACS using the following protocols:
 - syslogd
 - radius (old RFC)
 - tacacs+
 - http
- Don't use more than two ACL lines.
- Configure static route to R2.

b) On Vasa1b:

- The VPN3000 should appear as 9.12.112.112 on the outside.
- The VPN3000 should appear as 192.168.10.12 on the inside network.
- Configure static route to R2.

Vasa1a

- Configure NAT for all traffic coming from the inside interface. Leave one address for PAT to be used when the pool is exhausted:

```
nat (inside) 1 0 0
global (outside) 1 9.12.112.230-9.12.112.249
global (outside) 1 9.12.112.250
```


- Configure static NAT for the ACS server:

```
static (i,o) 9.12.112.100 192.168.10.100
```

- Configure ACL to allow traffic to the ACS server. Configure the ACL using objects to decrease the amount of ACL entries:

```
object-group network R_LOOP
network-object host 1.1.1.1
network-object host 2.2.2.2
network-object host 5.5.5.5
network-object host 6.6.6.6
object-group service ACS_TCP tcp
port-object eq tacacs
port-object eq http
object-group service ACS_UDP udp
port-object eq syslog
port-object eq 1645
port-object eq 1646
access-list OUT extended permit tcp object-group R_LOOP host \
9.12.112.100 object-group ACS_TCP
access-list OUT extended permit udp object-group R_LOOP host \
9.12.112.100 object-group ACS_UDP
access-group OUT in in outside
```

- Configure default gateway:

```
route outside 0 0 9.12.112.2
```

Vasa1b

- Configure static NAT entries to map VPN3000 on both inside and outside interfaces:

```
static (DMZ,outside) 9.12.112.112 192.168.11.12
static (DMZ,inside) 192.168.10.12 192.168.11.12
```

- Configure default gateway:

```
route outside 0 0 9.12.112.2
```

3.4 – 2 points

- Enable SSH on both virtual ASAs.
- Allow only the inside network to connect to the ASAs.
- Use local authentication.

Vasa1 and Vasa2

- To enable SSH, first configure a domain name and generate RSA keys:

```
domain ipexpert.net
crypto key generate rsa modulus 1024
```


- Configure users, authentication method and enable ssh on the inside interface:

```
ssh 192.168.10.0 255.255.255.0 inside
username cisco password cisco
aaa authentication ssh console LOCAL
```

3.5 – 2 point

- a) Deny FTP site commands for FTP sessions going through Vasa1a.

- Create FTP map to deny site commands and allow all other:

```
policy-map type inspect ftp FTP_MAP
parameters
match request-command site
reset
```

- Apply the map to the default global policy:

```
policy-map global_policy
class inspection_default
inspect ftp strict FTP_MAP
```

4 – PIX/ASA advanced (12 points)

4.1 – 2 points

- a) R1 is peering with BB1 using BGP. Allow BB1 to peer with R1.
b) The BGP session is protected using MD5.
c) Make sure that only BB1 is allowed to initiate the BGP session.

- TCP MD5 is using TCP option 19, which is denied by default. Configure TCP map on ASA2 to allow it. Create class-map to classify BGP traffic:

```
tcp-map ALLOW_BGP
tcp-options range 19 19 allow
access-list BGP per tcp any any eq bgp
class-map cmBGP
match access-list BGP
```

- Configure the default global policy-map to match the class-map and to apply the tcp-map:

```
policy-map global_policy
class cmBGP
set connection advanced-options ALLOW_BGP
set connection random-sequence-number disable
```


- To make sure that BB1 is the BGP session initiator, block R1 from initiating BGP session to BB1 and allow BB1 to initiate BGP session to R1 via the outside interface:

```
access-list OUT permit tcp host 9.12.101.100 host 9.12.101.1 eq  
bgp  
access-list IN deny tcp host 9.12.101.1 host 9.12.101.100 eq bgp  
access-list IN permit ip any any  
access-group IN in in inside
```

4.2 – 2 points

- a) FTP sessions flowing through Vasa1a from inside network takes long time to get established.
- b) You find the problem to be IDENT being blocked.
- c) Configure Vasa1a to fix the problem.
- d) Don't use "service" commands.

- Configure the established command to allow a return IDENT session when a FTP session was initiated. The established command will monitor outgoing sessions matching port 21, and will allow a session coming back from the FTP server to the client using port 113. The established will also setup an xlate entry for the incoming session:

```
established tcp 0 21 permitto tcp 113 permitfrom tcp 0
```

4.3 – 2 point

- a) Users on VLAN 12 are using a telnet application. Sometimes they leave the sessions open for 2 hours, and when they return they are forced to reestablish the session. Configure the PIX to keep the sessions alive for more than 2 hours.

- A TCP session can remain idle for ever without the session parties exchanging a single segment. The PIX monitors these idle session both to prevent overloading its own session table and to limit the number of open sessions in the network, which might be hijacked. Configure the PIX to timeout a session after more than two hours:

```
timeout conn 2:00:01
```

4.4 – 2 points

- a) Configure OSPF on the PIX.
- b) Both interfaces should be on area 0.
- c) Configure the most secure authentication using "cciesec" as password.

- d) BB3 should get the default route only while maintaining full reachability to 9.12.0.0/16 network.

- As seen in the IGP diagram, OSPF is using only area 0. We need somehow to filter routes to BB3 and to generate a default route. In OSPF the only way to filter is to filter between areas or to filter when redistributing.
- As there is only one area it's not possible to filter routes to BB3. The solution is to split OSPF on PIX into two processes:

```
router ospf 1
 network 9.12.112.0 255.255.255.0 area 0
 log-adj-changes
 redistribute ospf 2 subnets
router ospf 2
 network 192.168.12.0 255.255.255.0 area 0
 log-adj-changes
 default-information originate always
```

- Configure the MD5 authentication on both interfaces:

```
interface Ethernet0
 ospf message-digest-key 1 md5 cciesec
 ospf authentication message-digest
interface Ethernet1
 ospf message-digest-key 1 md5 cciesec
 ospf authentication message-digest
```

4.5 – 2 points

- a) On all firewall devices, allow Inside networks to ping outside networks.
- b) Do not configure any ACLs to achieve that.
- As inside networks can access outside networks without needing any ACL to permit it (unless ACL on the inside interface is not allowing such traffic). The problem is the returning ICMP packets. For simple TCP and UDP traffic the PIX/ASA takes care for the returning traffic, but for all the other protocols, such as FTP/RPC/SIP, inspection needs to be configured. By default ICMP inspection is turned off. Turn on ICMP inspection on all PIX/ASAs:

```
policy-map global_policy
 class inspection_default
 inspect icmp
```

4.6 – 2 points

- a) Don't allow fragments on the outside interface of Vasa1a.
- Use fragment chain command to limit the number of fragments per IP packet. Any fragmented IP packet needs two or more fragments. Setting the limit to one will not allow any fragments:

```
fragment chain 1 outside
```


5 – IOS Features (10 points)

5.1 – 4 Points

- a) Configure R6 for AAA using TACACS for SSH access.
- b) Don't permit Telnet connections. Don't use ACL.
- c) The TACACAS server is the ACS server.
- d) Configure authentication and command authorization.
- e) Configure the ACS server with username "cisco", which should be able to issue all commands.
- f) Configure the ACS server with username "oper", which should be able to issue all show commands except "show memory" commands.
- g) Use TACACS to authorize each a every commands.
- h) Configure a backup solution so "cisco" can login to the router when the ACS is not available.

→ **Configure AAA for authentication and authorization. Use TACACS use local as the backup method if the TACACS server is not available. By default commands are mapped to 3 privilege levels: 0, 1 and 15. To authorize all the commands, configure authorization for the 3 privilege levels. Don't configure aaa using the default method list because you are not allowed to change the console behavior:**

```
aaa new-model
aaa authentication login TAC group tacacs+ local
aaa authorization exec TAC group tacacs+ local
aaa authorization commands 0 TAC group tacacs+ local
aaa authorization commands 1 TAC group tacacs+ local
aaa authorization commands 15 TAC group tacacs+ local
```

→ **By default, AAA won't authorize configuration commands. Enable authorization for the configuration commands:**

```
aaa authorization config-commands
```

→ **Configure the TACAS server. Because Vasa1a accepts TACACS connection only from loopback interfaces, configure R6 to send TACACS requests with source interface of Lo0:**

```
tacacs-server host 9.12.112.100 key cisco
ip tacacs source-interface loopback 0
```

→ **Apply the authentication and authorization lists to the VTY lines. Allow only SSH as input protocol:**

```
line vty 0 4
authorization commands 0 TAC
authorization commands 1 TAC
```



```
authorization commands 15 TAC
authorization exec TAC
login authentication TAC
transport input ssh
```

- Configure the domain name and generate RSA keys to enable SSH:

```
ip domain-name ipexpert.net
cry key gen rsa gen modulus 1024
```

- Configure a user for backup:

```
username cisco privilege 15 password cisco
```

- Configure the ACS server:

- Add R6's loopback to the network clients:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="R6"/>
AAA Client IP Address	<input type="text" value="6.6.6.6"/>
Key	<input type="text" value="cisco"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	

- Configure Interface configuration to allow per user TACACS/RADIUS attributes, and allow advanced TACAS configuration:

Interface Configuration

Edit

Advanced Options ?

Note: Only the selected options will appear in the user interface.

- ☒ Per-user TACACS+/RADIUS Attributes
- ☐ User-Level Shared Network Access Restrictions
- ☒ User-Level Network Access Restrictions
- ☐ User-Level Downloadable ACLs
- ☒ Default Time-of-Day / Day-of-Week Specification
- ☐ Group-Level Shared Network Access Restrictions
- ☒ Group-Level Network Access Restrictions

Submit Cancel

Interface Configuration

- ☐ ☐ ARAP
- ☒ ☒ Shell (exec)
- ☐ ☐ PIX Shell (pixshell)
- ☐ ☐ SLIP

New Services

	Service	Protocol
<input type="checkbox"/> <input type="checkbox"/>		
<input type="checkbox"/> <input type="checkbox"/>		

Advanced Configuration Options ?

- ☒ Advanced TACACS+ Features
- ☐ Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day

Submit Cancel

- Configure commands authorization set to allow administrators issue all the commands:

Shared Profile Components

Edit

Shell Command Authorization Set

Name: ALL

Description:

Unmatched Commands: ☒ Permit ☐ Deny

☐ Permit Unmatched Args

- Configure commands authorization set to allow ops to issue show commands except show memory commands:

Shared Profile Components

Edit

Shell Command Authorization Set

Name: SHOW

Description:

Unmatched Commands: ☐ Permit ☒ Deny

☒ Permit Unmatched Args

show

deny memory

- Create users, and for both of them enable the Shell (exec) attribute:

The 'User Setup' dialog box has a title bar with 'User Setup'. Below the title bar is a section titled 'TACACS+ Settings' with a help icon (?). The settings are as follows:

- ☒ Shell (exec)
- ☐ Access control list
- ☐ Auto command
- ☐ Callback line
- ☐ Callback rotary
- ☐ Idle time
- ☐ No callback verify ☐ Enabled
- ☐ No escape ☐ Enabled
- ☐ No hangup ☐ Enabled
- ☐ Privilege level
- ☐ Timeout

At the bottom are 'Submit' and 'Cancel' buttons.

- For the administrator user configure privilege level of 15 and a commands authorization set to allow all commands:

The 'User Setup' dialog box shows the following settings:

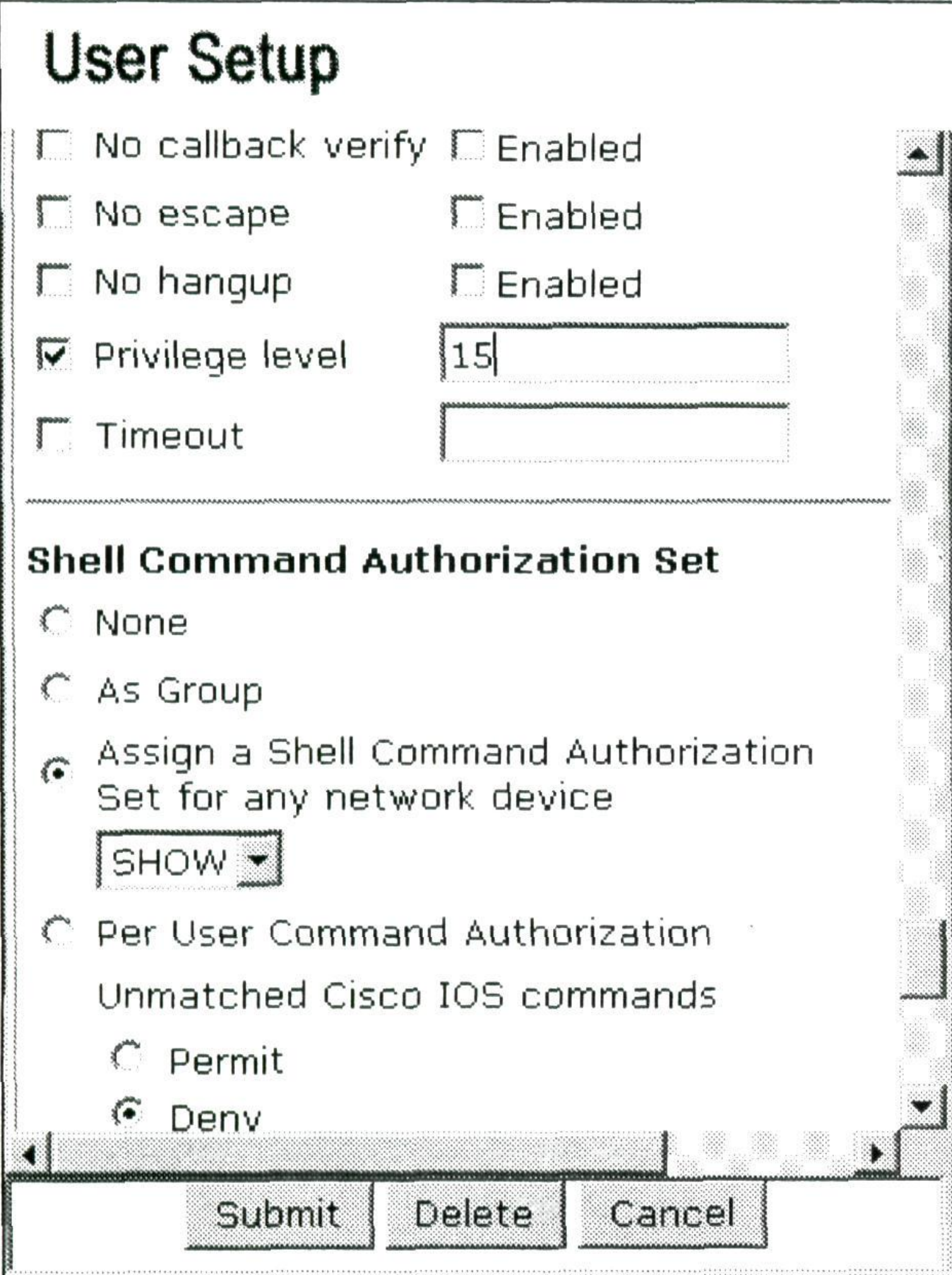
- ☐ No callback verify ☐ Enabled
- ☐ No escape ☐ Enabled
- ☐ No hangup ☐ Enabled
- ☒ Privilege level
- ☐ Timeout

Below these is the 'Shell Command Authorization Set' section:

- ☐ None
- ☐ As Group
- ☒ Assign a Shell Command Authorization Set for any network device
 -
- ☐ Per User Command Authorization
 - Unmatched Cisco IOS commands
 - ☐ Permit
 - ☒ Deny

At the bottom are 'Submit', 'Delete', and 'Cancel' buttons.

- For the oper user configure privilege level of 15 and a commands authorization set to allow show commands only commands. Privilege level 15 is needed to put the user directly to enabled mode:



The image shows a 'User Setup' configuration window. It has two main sections. The first section contains several options with checkboxes: 'No callback verify' (unchecked), 'No escape' (unchecked), 'No hangup' (unchecked), 'Privilege level' (checked with a value of 15 entered in a text box), and 'Timeout' (unchecked). Each of the first three options also has an 'Enabled' checkbox to its right, which is unchecked. The second section is titled 'Shell Command Authorization Set' and contains three radio button options: 'None', 'As Group', and 'Assign a Shell Command Authorization Set for any network device' (which is selected). Below the selected option is a dropdown menu showing 'SHOW'. There are also two more radio button options: 'Per User Command Authorization' (unchecked) and 'Unmatched Cisco IOS commands' (unchecked). Below these are two more radio button options: 'Permit' (unchecked) and 'Deny' (checked). At the bottom of the window are three buttons: 'Submit', 'Delete', and 'Cancel'.

5.2 – 2 points

- a) R6 is experiencing high traffic. During this high traffic, OSPF connections are dropped.
- b) Configure R6 to allocate 2.5% of CPU time for OSPF and other processing.
- The router needs to balance the CPU time between forwarding packets and running all other processes such as: OSPF, ARP, VTY. Forwarding packets is done when the router serves interrupts coming from the network interfaces. The scheduler allocate command controls the CPU allocation between interrupts processing and any other processing:

```
scheduler allocate 39000 1000
```

5.3 – 2 points

- a) Configure R5 for remote telnet sessions.
- b) Use local authentication.

- c) Configure a user named "oper", which will be restricted to the following commands:
- show process cpu
 - show logging
 - show running-config
- d) Make sure user "oper" is not able to issue any other commands. Don't use the "privilege" commands to accomplish the task.

- An easy way to limit the scope of commands for a user is to use a menu. Configure a menu to enable the oper user to issue commands:

```
menu MMM text 1 show process cpu
menu MMM command 1 show proc cpu
menu MMM text 2 show logging
menu MMM command 2 show logging
menu MMM text 3 show running-config
menu MMM command 3 show running-config
menu MMM text 4 exit
menu MMM command 4 exit
```

- Configure the oper user. To enable the oper user issue these commands, configure it with privilege level of 15. When oper logs in it will be able to issue any command. Configure R5 to force oper to run the menu command when it logs in:

```
username oper privilege 15 password 0 oper
username oper autocommand menu MMM
```

- Configure the virtual terminal lines to authenticate using the local user database:

```
line vty 0 4
login local
```

5.4 – 2 point

- a) Configure R5 and R6 to send logs to the ACS.
- b) Configure only R5 and R6 to accomplish the task.
- Vasa1a accepts syslog only from the router's loopback interfaces, configure logging and set the source interface of the syslog messages to be Lo0:

```
logging source-interface Loopback0
logging 9.12.112.100
```

6 – VPN Basic (10 points)

6.1 – 2 points

- a) Configure VPN3000 according to the IP address table.
- b) The default gateway should be Vasa1b.
- c) Don't allow management on port 80.

d) Make sure the ACS can manage the VPN3000.

➔ **First configure the IP address of the Public interface:**

1) Configuration

...

6) Exit

Main -> **1**

1) Interface Configuration

...

6) Back

Config -> **1**

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	Not Configured	0.0.0.0/0.0.0.0	00.90.A4.08.09.08
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured

DNS Domain Name:

Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)

...

4) Back

Interfaces -> **2**

1) Interface Setting (Disable, DHCP or Static IP)

...

12) Back

Ethernet Interface 2 -> **1**

1) Disable

2) Enable using DHCP Client

3) Enable using Static IP Addressing

Ethernet Interface 2 -> [3] **3**

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	Not Configured	0.0.0.0/0.0.0.0	00.90.A4.08.09.08
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured

DNS Domain Name:

Default Gateway: Default Gateway Not Configured

> Enter IP Address

Ethernet Interface 2 -> [0.0.0.0] **192.168.11.12**

Waiting for Network Initialization...

14 12/22/2006 13:00:21.080 SEV=3 IP/1 RPT=3

IP Interface 2 status changed to Link Up.

> Enter Subnet Mask

Ethernet Interface 2 -> [255.255.255.0] [enter]

→ **Configure the Public interface to allow management and to redirect HTTP sessions to HTTPS. At the end, exit the interface configuration mode:**

1) Interface Setting (Disable, DHCP or Static IP)

...

11) Set Interface WebVPN Parameters

12) Back

Ethernet Interface 2 -> **11**

1) Enable/Disable HTTP and HTTPS Management

...

7) Back

Ethernet Interface 2 -> **1**

1) Enable HTTP and HTTPS Management

2) Disable HTTP and HTTPS Management

Ethernet Interface 2 -> [2] **1**

1) Enable/Disable HTTP and HTTPS Management

2) Enable/Disable HTTPS WebVPN

...

6) Enable/Disable HTTP Redirect

7) Back

Ethernet Interface 2 -> **6**

1) Enable Redirect HTTP to HTTPS

2) Disable Redirect HTTP to HTTPS

Ethernet Interface 2 -> [1] [enter]

1) Enable/Disable HTTP and HTTPS Management

...

7) Back

Ethernet Interface 2 -> **7**

1) Interface Setting (Disable, DHCP or Static IP)

...

12) Back

Ethernet Interface 2 -> **12**

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	Not Configured	0.0.0.0/0.0.0.0	00.90.A4.08.09.08
Ether2-Pub	UP	192.168.11.12/255.255.255.0	00.90.A4.08.09.09

DNS Server(s): DNS Server Not Configured

DNS Domain Name:

Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)

...

4) Back

Interfaces -> **4**

Configure default gateway and exit the system configuration:

- 1) Interface Configuration
- 2) System Management

...

- 6) Back

Config -> **B**

- 1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)

- 2) Address Management

- 3) IP Routing (static routes, OSPF, etc.)

...

- 9) Back

System -> **3**

- 1) Static Routes

- 2) Default Gateways

...

- 9) Back

Routing -> **2**

- 1) Set Default Gateway

...

- 5) Back

Routing -> **1**

> Default Gateway

Routing -> **192.168.11.19**

- 1) Set Default Gateway

...

- 5) Back

Routing -> **5**

- 1) Static Routes

...

- 9) Back

Routing -> **9**

- 1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)

..

- 9) Back

System -> **9**

➔ **Allow HTTPS and HTTP to the Public interface Filter:**

- 1) Interface Configuration

...

- 4) Policy Management

- 5) Tunneling and Security

- 6) Back

Config -> **4**

- 1) Access Hours
- 2) Traffic Management

..

- 5) Back

Policy -> 2

.

- 1) Network Lists
- 2) Rules
- 3) Security Associations (SAs)
- 4) Filters
- 5) Network Address Translation (NAT) Rules
- 6) Bandwidth Policies
- 7) Back

Traffic -> 4

Current Active Filters

1. Private (Default)	2. Public (Default)	
3. External (Default)	4. Firewall Filter for VPN Client (De	

- 1) Add a Filter

...

- 4) Assign Rules to a Filter
- 5) Copy a Filter
- 6) Back

Filters -> 4

> Which Filter to assign Rules to

Filters -> 2

The Current Rules for this Filter

1. GRE In	IN FORWARD
2. IPSEC-ESP In	IN FORWARD
3. IKE In	IN FORWARD
4. PPTP In	IN FORWARD
5. L2TP In	IN FORWARD
6. ICMP In	IN FORWARD
7. VRRP In	IN FORWARD
8. NAT-T In	IN FORWARD
9. GRE Out	OUT FORWARD
10. IKE Out	OUT FORWARD
11. PPTP Out	OUT FORWARD
12. L2TP Out	OUT FORWARD
13. ICMP Out	OUT FORWARD
14. VRRP Out	OUT FORWARD
15. NAT-T Out	OUT FORWARD

1) Add a Rule to this Filter

...

6) Back

Filters -> **1**

Current Filter Rules

1. GRE In	2. GRE Out
3. IPSEC-ESP In	4. IKE I
5. IKE Out	6. PPTP In
7. PPTP Out	8. L2TP In
9. L2TP Out	10. ICMP In
11. ICMP Out	12. RIP In
13. RIP Out	14. OSPF In
15. OSPF Out	16. Incoming HTTP In
17. Incoming HTTP Out	18. VRRP In
19. VRRP Out	20. Any In
21. Any Out	22. Incoming HTTPS In
23. Incoming HTTPS Out	24. LDAP In
25. LDAP Out	26. TelnetSSL In
27. Telnet/SSL Out	28. Outgoing HTTP In
29. Outgoing HTTP Out	30. Outgoing HTTPS In
31. Outgoing HTTPS Out	32. CRL over LDAP In
33. CRL over LDAP Out	34. SSH In
35. SSH Out	36. VCA In
37. VCA Out	38. NAT-T In
39. NAT-T Out	40. DHCP In
41. DHCP Out	

> Which Rule to add

Filters -> **22**

The Current Rules for this Filter

1. GRE In	IN FORWARD
2. IPSEC-ESP In	IN FORWARD
3. IKE In	IN FORWARD
4. PPTP In	IN FORWARD
5. L2TP In	IN FORWARD
6. ICMP In	IN FORWARD
7. VRRP In	IN FORWARD
8. NAT-T In	IN FORWARD
9. GRE Out	OUT FORWARD
10. IKE Out	OUT FORWARD
11. PPTP Out	OUT FORWARD
12. L2TP Out	OUT FORWARD
13. ICMP Out	OUT FORWARD
14. VRRP Out	OUT FORWARD
15. NAT-T Out	OUT FORWARD
16. Incoming HTTPS In	IN FORWARD

1) Add a Rule to this Filter

...

6) Back

Filters -> **1**

Current Filter Rules

1. GRE In	2. GRE Out
3. IPSEC-ESP In	4. IKE In
5. IKE Out	6. PPTP In
7. PPTP Out	8. L2TP In
9. L2TP Out	10. ICMP In
11. ICMP Out	12. RIP In
13. RIP Out	14. OSPF In
15. OSPF Out	16. Incoming HTTP In
17. Incoming HTTP Out	18. VRRP In
19. VRRP Out	20. Any In
21. Any Out	22. Incoming HTTPS In
23. Incoming HTTPS Out	24. LDAP In
25. LDAP Out	26. Telnet/SSL In
27. Telnet/SSL Out	28. Outgoing HTTP In
29. Outgoing HTTP Out	30. Outgoing HTTPS In
31. Outgoing HTTPS Out	32. CRL over LDAP In
33. CRL over LDAP Out	34. SSH In
35. SSH Out	36. VCA In
37. VCA Out	38. NAT-T In
39. NAT-T Out	40. DHCP In
41. DHCP Out	

> Which Rule to add

Filters -> **23**

The Current Rules for this Filter

1. GRE In	IN FORWARD
2. IPSEC-ESP In	IN FORWARD
3. IKE In	IN FORWARD
4. PPTP In	IN FORWARD
5. L2TP In	IN FORWARD
6. ICMP In	IN FORWARD
7. VRRP In	IN FORWARD
8. NAT-T In	IN FORWARD
9. GRE Out	OUT FORWARD
10. IKE Out	OUT FORWARD
11. PPTP Out	OUT FORWARD
12. L2TP Out	OUT FORWARD
13. ICMP Out	OUT FORWARD
14. VRRP Out	OUT FORWARD
15. NAT-T Out	OUT FORWARD
16. Incoming HTTPS In	IN FORWARD
17. Incoming HTTPS Out	OUT FORWARD

1) Add a Rule to this Filter

...

6) Back

Filters -> 6

Current Active Filters

1. Private (Default)	2. Public (Default)
3. External (Default)	4. Firewall Filter for VPN Client (De

1) Add a Filter

2) Modify a Filter

3) Delete a Filter

4) Assign Rules to a Filter

5) Copy a Filter

6) Back

Filters -> 6

→ Now you should be able to configure the VPN3000 using the ACS.

6.2 – 3 points

a) Configure VPN3000 with remote-access group with the following parameters:

- Group name: grp1
- Pool : 192.168.100.0/24
- Authentication: Local database, Make sure the VPN clients can ping BB2

→ Enable the VPN3000 to allocate IP addresses using the local pool:

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address ☐

Use Address from Authentication Server ☒

Use DHCP ☐

Use Address Pools ☒

Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Check to use an IP address retrieved from an authentication server for the client.

Check to use DHCP to obtain an IP address for the client.

Check to use internal address pool configuration to obtain an IP address for the client.

IP Reuse Delay

Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply

Cancel

Copyright IPexpert, Inc. (<http://www.ipexpert.com>) 2007. All Rights Reserved.

463

→ Add a group named grp1:

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	grp1	Enter a unique name for the group.
Password	••••	Enter the password for the group.
Verify	••••	Verify the group's password.
Type	Internal ▾	<i>External</i> groups are configured on an external authentication (e.g. RADIUS). <i>Internal</i> groups are configured on the VP Concentrator's Internal Database.

Add Cancel

→ Configure a pool for the group:


Configuration User Management Groups Address Pools Add		
Add an address pool.		
Range Start	192.168.100.1	Enter the start of the IP pool address range.
Range End	192.168.100.255	Enter the end of the IP pool address range.
Subnet Mask	255.255.255.0	Enter the subnet mask of the IP pool address range. Enter 0.0.0.0 to use default behavior.

Add Cancel

→ To allow VPN connections set the Public interface with the default Public filter:

Configuration Administration Monitor		
MAC Address	00.90.A4.08.09.09	The MAC address for this interface.
Interface Name	<input type="text"/>	Enter the textual name of the interface.
Filter	2. Public (Default) ▼	Select the filter for this interface.
Speed	10/100 auto ▼	Select the speed for this interface.
Duplex	Auto ▼	Select the duplex mode for this interface.
MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
Public Interface	<input checked="" type="radio"/> Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission	
IPSec Fragmentation Policy	<input type="radio"/> Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)	
	<input type="radio"/> Fragment prior to IPSec encapsulation without Path MTU	

→ Enable NAT-T:

Configuration Administration Monitoring	
Configuration Tunneling and Security IPSec NAT Transparency	
Save Needed 	
This section lets you configure system-wide IPSec NAT Transparency.	
IPSec over TCP <input type="checkbox"/>	Check to enable IPSec over TCP.
TCP Port(s) <input type="text" value="10000"/>	Enter up to 10 comma-separated TCP ports (1 - 65535).
IPSec over NAT-T <input checked="" type="checkbox"/>	Check to enable IPSec over NAT-T, which detects the need for UDP encapsulation in NAT/PAT environments, using UDP port 4500.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Add a user which belongs to group grp1:

Configuration Administration Monitor		
This section lets you add a user. Uncheck the Inherit? box and enter a new value to override group values.		
<div> <div>Identity</div> <div>General</div> <div>IPSec</div> <div>PPTP/L2TP</div> </div>		
Identity Parameters		
Attribute	Value	Description
Username	u_grp1	Enter a unique username.
Password	••••••	Enter the user's password. The password must satisfy the group password requirements.
Verify	••••••	Verify the user's password.
Group	grp1	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.
<div> <div>Add</div> <div>Cancel</div> </div>		

- Configure Vasa1b to route traffic destined to the pool to VPN3000:

```
route DMZ 192.168.100.0 255.255.255.0 192.168.11.12
```

- Configure ACL on Vasa1b to allow ISAKMP and IPSEC to VPN3000:

```
access-list OUT extended permit udp any host 9.12.112.112 eq isakmp
access-list OUT extended permit udp any host 9.12.112.112 eq 4500
access-list OUT extended permit esp any host 9.12.112.112
access-group OUT in interface outside
```

- Although users will be able to connect to the VPN3000, pinging to BB2 will fail because BB2 is located on a higher privileged interface. Configure Vasa1b to allow any traffic from the DMZ:

```
access-list DMZ per ip any any
access-group DMZ in in DMZ
```

- Because BB2's default gateway is Vasa1a, returning packets to the VPN clients will go through Vasa1a. Configure a route to the VPN clients pool on Vasa1a via Vasa1b inside IP address:

```
route DMZ 192.168.100.0 255.255.255.0 192.168.11.12
```

- By default Vasa1a won't allow traffic coming to an interface to be routed out of the same interface. Configure Vasa1a to allow this:

```
same-security-traffic permit intra-interface
```


- When returning traffic to the VPN client will come to Vasa1a's inside interface, it will be NATed because of "nat (inside) 1 0 0" configuration. Configure NAT exemption to bypass NAT for traffic destined to the VPN clients pool:

```
access-list NAT0 extended permit ip 192.168.0.0 255.255.0.0 \
192.168.0.0 255.255.0.0
nat (inside) 0 access-list NAT0
```

- That's not enough!!! Now when Vasa1a will receive echo reply packets, it will try to inspect them, while doing so, it will discover that there is no matching echo request to the echo reply and will drop the echo reply. Configure Vasa1a not to inspect packets going to the VPN clients pool:

```
access-list ICMP extended deny icmp 192.168.0.0 255.255.0.0 \
192.168.0.0 255.255.0.0
access-list ICMP extended permit icmp any any
class-map cmICMP
match access-list ICMP
policy-map global_policy
class cmICMP
inspect icmp
```

- Finally VPN clients should be able to ping BB2.

6.3 – 2 points

- a) Configure the VPN3000 to reserve 128Kb per client, and max of 1000Kb for all clients.

→ **Add bandwidth policy:**

Configuration Administration Monitoring	
Configuration Policy Management Traffic Management Bandwidth Policies Add	
Configure bandwidth policy parameters. To create a bandwidth policy, you must enable at least one of the checkboxes.	
Policy Name	<input type="text" value="QOS_PUB"/> Enter a unique name for this policy.
<hr/>	
<input checked="" type="checkbox"/> Bandwidth Reservation	Check to reserve a minimum bandwidth per session.
Minimum Bandwidth	<input type="text" value="128"/> <input type="text" value="kbps"/> Enter the minimum bandwidth.
<hr/>	
Traffic policing allows you to control a policing rate or size of traffic transmitted or received on an interface. Traffic that exceeds the policing rate or burst size is dropped.	
<input checked="" type="checkbox"/> Policing	Check to enable Policing.
Policing Rate	<input type="text" value="1000"/> <input type="text" value="kbps"/> Enter the policing rate. Traffic below this rate will be transmitted; traffic above this rate will be dropped.

→ Apply the policy to Public interface:

Configuration Administration Monitor		
Bandwidth Management Parameters		
Attribute	Value	Description
Bandwidth Management	<input checked="" type="checkbox"/>	Check to enable bandwidth management.
Link Rate	1544 kbps	Set the link rate that will be applied to all tunneled traffic. The defined link rate must be based on available Internet bandwidth and not the physical LAN connection rate.
Bandwidth Policy	QOS_PUB	This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are configured at Configuration Policy

6.4 – 3 points

- Configure R1 as EasyVPN server for remote access from the Internet.
- Configure a group with the following parameters:
 - Group name: EZG
 - Group password: ezpassword
 - IP pool: 9.12.201.0/24
- Remote users should use the VPN for protected networks only.
- BB2 should be able to ping remote users.

- e) Use TACACS to authenticate users.

→ Add R1 to the ACS server:

Add AAA Client

AAA Client Hostname	<input type="text" value="R1"/>
AAA Client IP Address	<input type="text" value="1.1.1.1"/>
Key	<input type="text" value="cisco"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Rec accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this	

- Configure AAA to use TACACS for client authentication and the local database for EZVPN group parameters:

```
aaa new-model
aaa authentication login EZT group tacacs+
aaa authorization network EZ local
```

- Configure the TACACS server. Remember that Vasa1a accept TACACS connection only from loopback interfaces:

```
tacacs-server host 9.12.112.100 key cisco
ip tacacs source-interface Loopback0
```

- Configure a pool for the VPN client and ACL for the split tunnel, which will make sure the tunnel is used to reach the internal networks only:

```
ip local pool EZ 9.12.201.1 9.12.201.255
ip access-list extended acEZ
 permit ip 192.168.0.0 0.0.255.255 any
 permit ip 9.12.0.0 0.0.255.255 any
```


- Configure ISKAMP policy which will allow preshared authentication and DH group 2:

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
```

- Configure the actual EZVPN group:

```
crypto isakmp client configuration group EZG
  key ezpassword
  pool EZ
  acl acEZ
```

- Configure IPSEC transform set, and apply to a dynamic crypto-map. Under the dynamic crypto-map configure reverse-route so R1 will be able to inject client's pool address to OSPF so the network will be able to send traffic to the VPN clients:

```
crypto ipsec transform-set TSEZ esp-3des esp-sha-hmac
crypto dynamic-map DYN 10
  set transform-set TSEZ
  reverse-route
```

- Configure a crypto map and set the EZVPN parameters, namely the authentication and authorization methods to be used:

```
crypto map CMINT client authentication list EZT
crypto map CMINT isakmp authorization list EZ
crypto map CMINT client configuration address initiate
crypto map CMINT client configuration address respond
```

- Configure the crypto map to use the dynamic crypto map and apply it to the interface facing the Internet:

```
crypto map CMINT 999 ipsec-isakmp dynamic DYN
interface FastEthernet0/1
  crypto map CMINT
```

- Configure the OSPF process to redistribute the reverse routes:

```
router ospf 1
  redistribute static subnets
```

- The default gateway of Vasa1a is R2. When a packet coming through Vasa1a to the VPN client it will be sent to R2. R2 will send ICMP redirect to Vasa1a so Vasa1a will learn that that address is better routed by R1. As Vasa1a does not support such ICMP messages, configure R2 G0/0 interface not to send ICMP redirects:

```
interface GigabitEthernet0/0
  no ip redirects
```


- Configure ASA2 to allow ISAKMP and IPSEC to R1:

```
access-list OUT extended permit udp any host 9.12.101.1 eq isakmp
access-list OUT extended permit udp any host 9.12.101.1 eq 4500
access-list OUT extended permit esp any host 9.12.101.1
```

7 – VPN Advanced (10 points)

7.1 – 2 points

- Configure IPSEC tunnel between V5 and V6 Loopback0 interfaces.
- Use default ISAKMP policy only.

- Create RSA keys on R5:

```
ip domain-name ipsecpert.net
cry key gen rsa general-keys modulus 1024
```

On both routers

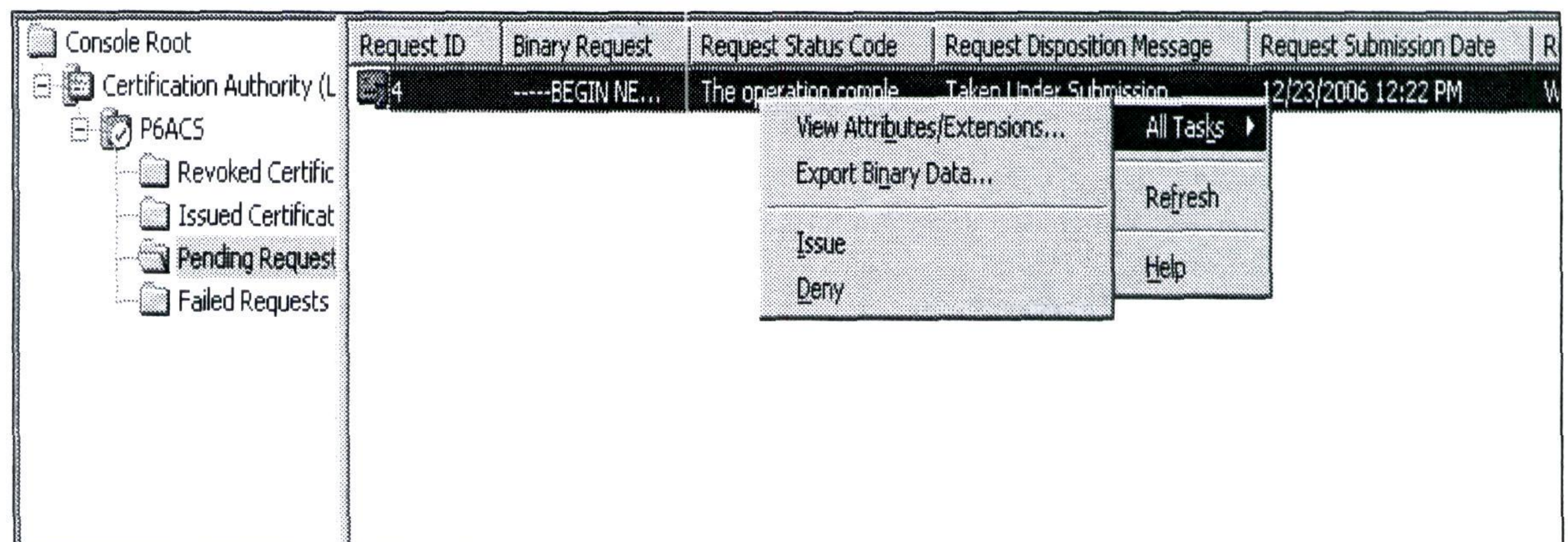
- Configure the ca/pki trust point. As Vasa1a accepts HTTP connections from the loopback interfaces, configure the routers to use Lo0 as a source interface for all the PKI communication:

```
crypto ca trustpoint MYCA
enrollment mode ra
enrollment url http://9.12.112.100:80/certsrv/mscep/mscep.dll
revocation-check none
source interface Loopback0
```

- For older IOS use : `crl optional` instead of `revocation-check none`
- Authenticate the CA and enroll the router's certificate to the CA:

```
cry ca authen MYCA
cry ca enroll MYCA
```

- On the CA issue the certificate:



R6

- Configure ACL to select the traffic to encrypt/decrypt:

```
ip access-list extended acR6R5
 permit ip host 6.6.6.6 host 5.5.5.5
```

- Configure the transform set and crypto map. Apply the crypto map to the Serial interface:

```
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
crypto map CMINT 10 ipsec-isakmp
 set peer 9.12.56.5
 set trans TS1
 match address acR6R5
int s0/1/0
 crypto map CMINT
```

R5

- Configure ACL to select the traffic to encrypt/decrypt:

```
ip access-list extended acR5R6
 permit ip host 5.5.5.5 host 6.6.6.6
```

- Configure the transform set and crypto map. Apply the crypto map to the Serial interface:

```
crypto ipsec transform-set TS1 esp-3des esp-sha-hmac
crypto map CMINT 10 ipsec-isakmp
 set peer 9.12.56.6
 set trans TS1
 match address acR5R6
int s0/1/0
 crypto map CMINT
```

Note

MAKE SURE THE TIME IS SYNCED BETWEEN: CA, R5 and R6

7.2 – 3 points

- a) Configure the following loopback interfaces on R1 and R2:

- R1 Lo12: 192.168.12.1/24
- R2 Lo12: 192.168.12.2/24

- b) Configure IPSec VPN tunnel between the loopbacks.

- c) One static route is allowed on each router.

- d) Make sure that R2 is able to ping R1's Lo12 interface.
- e) Use the following networks: 192.168.1.0 and 192.168.2.0.
- To enable overlapping address configure NAT and remember that NAT is done before encryption, and decryption is done before NAT.

R1:

- Configure Lo1 and ACL to be used in the crypto map configuration. Note that the source address in the ACL is after NAT and the destination is before NAT:

```
int lo 12
ip addr 192.168.12.1 255.255.255.0
access-list 112 per ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
```

- Configure ISAKMP policy, ISKAMP keys and transform set:

```
crypto isakmp policy 20
authentication pre-share
cry isakmp key 0 cisco address 9.12.112.2
cry ipsec transform-set TS12 esp-3des esp-sha-hmac
```

- Configure crypto map:

```
crypto map CMLAN 10 ipsec-isakmp
set peer 9.12.112.2
set transform-set TS12
match address 112
```

- Configure NAT and apply NAT and crypto map to the interfaces. The ip nat inside interface is Lo12 interface:

```
ip nat inside source static network 192.168.12.0 192.168.1.0 /24
in lo 0
ip nat inside
int f0/0
ip nat outside
crypto map CMLAN
```

- 192.168.2.0/24 is not in the routing table. Configure static route so the router will route packets to 192.168.2.0/24 to F0/0. Without it, both NAT and the crypto map won't kick-in:

```
ip route 192.168.2.0 255.255.255.0 f0/0
```

R2:

- Configure Lo1 and ACL to be used in the crypto map configuration. Note that the source address in the ACL is after NAT and the destination is before NAT:

```
int lo 12
ip addr 192.168.12.2 255.255.255.0
access-list 112 per ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
```


- Configure ISAKMP policy, ISKAMP keys and transform set:

```
crypto isakmp policy 20
  authentication pre-share
cry isakmp key 0 cisco address 9.12.112.1
cry ipsec transform-set TS12 esp-3des esp-sha-hmac
```

- Configure crypto map:

```
crypto map CMLAN 10 ipsec-isakmp
  set peer 9.12.112.1
  set transform-set TS12
  match address 112
```

- Configure NAT and apply NAT and crypto map to the interfaces. The ip nat inside interface is Lo12 interface:

```
ip nat inside source static network 192.168.12.0 192.168.2.0 /24
in lo 0
  ip nat inside
int f0/0
  ip nat outside
  crypto map CMLAN
```

- 192.168.1.0/24 is not in the routing table. Configure static route so the router will route packets to 192.168.1.0/24 to F0/0. Without it, both NAT and the crypto map won't kick-in:

```
ip route 192.168.1.0 255.255.255.0 f0/0
```

7.3 – 3 points

- a) Configure IPSec VPN to protect traffic between VLAN 112 and VLAN 5.
- b) Do not configure static crypto-maps on R2.
- c) Make sure that R2 accept encrypted traffic from VLAN5 to VLAN112 only.
- d) Use pre-shared keys for ISAKMP.
- e) Use the most bandwidth efficient way for the VPN tunnel.

R2

- Use dynamic crypto map to accept incoming ISAKMP/IPSEC connections from R5.
- Configure ISAKMP key. There is no need to configure ISKAMP policy to allow preshared keys because it was configured in the previous task:

```
crypto isakmp key 0 cisco address 9.12.56.5
```


- Configure transform set and ACL. The ACL will be used to check that the negotiated IPSEC SA proxies are covered by the ACL so IPSEC will be used between VLAN5 and VLAN112 only. The transform set will use LZS compression to conserve bandwidth on the FR links :

```
crypto ipsec transform-set TS25 esp-3des esp-sha-hmac comp-lzs
access-list 125 per ip 9.12.112.0 0.0.0.255 9.12.5.0 0.0.0.255
```

- Configure a dynamic crypto map and use a match address to use the ACL to check the negotiated IPSEC SA proxies. Configure crypto map to use the dynamic crypto map and apply it to the serial interface:

```
crypto dynamic-map DYN 10
  set tran TS25
  match address 125
crypto map CMSR 999 ipsec-isakmp dynamic DYN
int s0/1/0
  crypto map CMSR
```

R5

- Configure ISKAMP policy for preshared authentication. Configure transform set, ACL, crypto map and apply it to the serial interface:

```
crypto isakmp policy 10
  authentication pre-share
cry isa key 0 cisco address 9.12.56.2
crypto ipsec transform-set TS25 esp-3des esp-sha-hmac comp-lzs
access-list 125 per ip 9.12.5.0 0.0.0.255 9.12.112.0 0.0.0.255
crypto map CMINT 20 ipsec-isakmp
  set peer 9.12.56.2
  set trans TS25
  match address 125
int s0/1/0
  crypto map CMINT
```

7.4 – 2 points

- a) Configure the following loopback interfaces on R5 and R6:
 - R5 Lo56: 192.168.5.5/24
 - R6 Lo56: 192.168.6.6/24
 - b) Configure IPSEC tunnel protection for traffic between these loopback interfaces
 - c) You are allowed one static route for each router.
 - d) The solution should support multicast traffic.
- IPSEC tunnels doesn't support multicast traffic. But encrypted GRE tunnels do support multicast.

R6**→ Configure Loopback interface:**

```
int lo 56
ip addr 192.168.6.6 255.255.255.0
```

→ Configure ISAKMP and IPSEC. The ACL should match the GRE packets, as encryption is done after GRE encapsulation and decryption is done before GRE decapsulation:

```
! configure isakmp policy and key
crypto isakmp policy 56
  authentication pre-share
crypto isakmp key 0 cisco address 9.12.56.5
! configure transform-set with transport mode
crypto ipsec transform-set TSGRE esp-3des esp-sha-hmac
  mode transport
! configure acl which will match gre end points
access-list 156 permit gre host 9.12.56.6 host 9.12.56.5
! configure crypto map
cry map CMINT 56 ipsec-isakmp
  set peer 9.12.56.5
  set trans TSGRE
  match address 156
int s0/1/0
  crypto map CMINT
```

→ Configure the GRE interface and add a static route to R5's loopback via the GRE interface:

```
interface Tunnel56
ip address 192.168.56.6 255.255.255.0
tunnel source Serial0/1/0
tunnel destination 9.12.56.5
ip route 192.168.5.0 255.255.255.0 tunnel 56
```

R5**→ Configure Loopback interface:**

```
int lo 56
ip addr 192.168.5.5 255.255.255.0
```

→ Configure ISKAMP and IPSEC:

```
crypto isakmp policy 56
  authentication pre-share
crypto isakmp key 0 cisco address 9.12.56.6
! configure transform-set with transport mode
crypto ipsec transform-set TSGRE esp-3des esp-sha-hmac
  mode transport
! configure acl which will match gre end points
access-list 156 permit gre host 9.12.56.5 host 9.12.56.6
! configure crypto map
cry map CMINT 56 ipsec-isakmp
```



```

set peer 9.12.56.6
set trans TSGRE
match address 156

```

- Configure the GRE interface and add a static route to R6's loopback via the GRE interface:

```

interface Tunnel56
ip address 192.168.56.5 255.255.255.0
tunnel source Serial0/1/0
tunnel destination 9.12.56.6
ip route 192.168.6.0 255.255.255.0 tunnel 56

```

8 – IOS Firewall and NAT (8 points)

8.1 – 2 points

- When R2 tries to ping 5.5.5.5 from Lo0 it should use the following address: 9.12.56.25.
- When R2 tries to ping 6.6.6.6 from Lo0 it should use the following address: 9.12.56.26.

R2

- Configure NAT ACLs to match packets which will be NATed:

```

ip access-list exten acNAT5
permit icmp host 2.2.2.2 host 5.5.5.5
ip access-list exten acNAT6
permit icmp host 2.2.2.2 host 6.6.6.6

```

- For any policy base NAT route-maps are needed so extended NAT entries in the translation table will be created:

```

route-map RM5
match ip address acNAT5
route-map RM6
match ip address acNAT6

```

- Configure NAT pools with only one address in each one, configure the NAT statements and set the interfaces NAT roles:

```

ip nat pool PL5 9.12.56.25 9.12.56.25 net 255.255.255.252
ip nat pool PL6 9.12.56.26 9.12.56.26 net 255.255.255.252
ip nat inside source route-map RM5 pool PL5
ip nat inside source route-map RM6 pool PL6
int s0/1/0
ip nat outside
int lo0
ip nat inside

```

- The FR network is using static address mapping. When R5 will try to send packet destined to 9.12.56.25, the router won't know the DLCI to put in the frame header. Same problem exists with R6.

R5

- **Configure FR mapping for 9.12.56.25:**

```
int s0/1/0
frame-relay map ip 9.12.56.25 502
```

R6

- **Configure FR mapping for 9.12.56.25:**

```
int s0/1/0
frame-relay map ip 9.12.56.26 602
```

8.2 – 2 points

- a) Translate source IP address of traffic going to the Internet with address 9.12.101.13.
- b) There is a web server on the Internet which uses port 5060 to serve HTTP traffic, but users coming from the network can't use it. Configure R1 to fix the problem.

- **Configure ACL that will ensure that only traffic to the Internet will be NATed:**

```
ip access-list extended acNAT_INT
deny ip any 9.12.201.0 0.0.0.255
deny tcp host 9.12.101.1 host 9.12.101.100 eq bgp
deny ip host 9.12.112.1 any
deny ip host 9.12.101.1 any
permit ip 9.12.0.0 0.0.255.255 any
```

- **Configure NAT pool, NAT statements and set the interfaces NAT roles:**

```
ip nat pool PLINT 9.12.101.11 9.12.101.13 prefix-length 30
ip nat inside source list acNAT_INT pool PLINT overload
int f0/1
ip nat outside
```

- Port 5060 is reserved for SIP, and the router will do deep inspection for the protocol so it will be able to set the right NAT entries in the NAT translation table for RTP sessions. Running non SIP protocol on port 5060 will cause the router to fail the deep packet inspection and will drop the NAT entries for that session.

- **Configure R1 to disable NAT inspection for SIP:**

```
no ip nat service sip tcp port 5060
```

- As NAT was previously configured on R1 for one of VPN tasks, some adjustment will be needed.

- **First F0/0 needs to be the inside interface:**

```
int f0/0
ip nat inside
```


- This will break the NAT for the VPN tunnel between R1 and R2, to fix this, delete the old NAT definitions and configure outside static nat:

```
no ip nat inside source static network 192.168.12.0 192.168.1.0 /24
ip nat outside source static network 192.168.12.0 192.168.1.0 /24
```

- This R2 will be able to ping R1 Lo12 but R1 won't be able to ping to R2 Lo12. The VPN task required that R2 will be able to ping R1 so the configuration is safe. This is a very good example of a question to ask the proctor.

8.3 – 4 points

- Configure R1 to protect the network from the Internet.
- Configure input access-list on F0/1. Use the most specific ACEs possible.
- Many concurrent sessions are expected. Optimize the sessions table for faster lookups.
- Set the HTTP timeout timer to two minutes.
- Don't allow any Java applets, except from IBM network (9.0.0.0/8).
- Some web sites use port 8000 for HTTP.
- Log all HTTP sessions to the syslogd server running on the ACS server.
- Time stamp the logs.
- Allow all TCP, UDP sessions to access the Internet.
- Also allow users to ping to the Internet. Don't configure ACL to achieve the task.
- There is a server on the Internet. Allow users to connect to a program number 666 using RPC.

- Copy ASA2 ACL to R1, with some little modifications. Add deny ip any any log so it will be easier to debug the ACL if we missed something. In the remaining lab time watch for ACL logs:

```
access-list 111 permit udp any host 9.12.101.1 eq isakmp
access-list 111 permit udp any host 9.12.101.1 eq 4500
access-list 111 permit esp any host 9.12.101.1
access-list 111 permit tcp host 9.12.101.100 host 9.12.101.1 eq 179
access-list 111 deny ip any any log
```

- Configure the IOS firewall to inspect all UDP and TCP connections. This will not enable inspections of Layer7 protocols:

```
ip inspect name FWOUT tcp
ip inspect name FWOUT udp
```


- To allow users to ping hosts on the Internet, configure the IOS firewall to inspect ICMP packets so the IOS firewall will let the replies in:

```
ip inspect name FWOUT icmp
```

- Configure HTTP inspection to filter out Java and to set the timeout to two minutes. Configure ACL to allow Java from IBM network, which is 9.0.0.0/8:

```
access-list 9 permit 9.0.0.0 0.255.255.255
ip inspect name FWOUT http java-list 9 audit-trail on timeout 120
```

- Configure logging. Remember that Vasa1a will allow syslog only from loopback addresses. Enable the timestamp service to time stamp the syslog packets sent to the syslog server:

```
logging host 9.12.112.100
logging source-interface loopback 0
service timestamps log datetime
```

- To enable HTTP inspection for TCP sessions using non standard ports, configure the IOS firewall to look for HTTP in sessions using port 8000. Without it, it will be possible to get Java applets from these sites without the IOS firewall blocking them:

```
ip port-map http port tcp 8000
```

- RPC is using dynamic ports, like FTP does. Configure the IOS firewall to inspect RPC sessions using program number 666 so it will allow the returning connections:

```
ip inspect name FWOUT rpc program-number 666
```

- Configure the IOS firewall with enlarged hash table, which will cause less collisions, hence increase performance:

```
ip inspect hashtable-size 8192
```

- Apply the ACL and the IOS firewall to the interface facing the internet:

```
int f0/1
ip inspect FWOUT out
ip access-group 111 in
```

9 – Security and Attacks (6 points)

9.1 – 2 points

- A hub is going to be connected to VLAN 10 via CAT1 port f0/6.
- On that hub there is a host with MAC address 4200.8118.0000 which should not be accessed outside the hub. Configure the port to be part of VLAN 10.

- c) Don't configure any ACL.

→ First configure the port to belong to VLAN10:

```
int f0/6
sw ac vlan 10
```

- Configure the CAM table to drop packets with destination address of 4200.8118.0000. Configuring that will be effective only on the switch and not on the hub:

```
mac address-table static 4200.8118.0000 vlan 10 drop
```

9.2 – 2 points

- a) Prevent users from using embedded commands in FTP when connecting to FTP servers on the Internet.

→ To block embedded FTP commands, configure strict FTP inspection:

```
policy-map global_policy
class inspection_default
inspect ftp strict
```

9.3 – 2 points

- a) To enable future investigation of attacks coming from the Internet, enable accounting.

- b) The accounting reports should include protocol details.

→ NBAR is usually used for QoS classification, but it can also be used as accounting tool:

→ int f0/1

```
ip nbar protocol-discovery
```

10 – Security and Attacks – Advanced (9 points)

10.1 – 3 points

- a) A web server on VLAN112 is under attack. Its IP address is 9.12.112.222.
- b) Using a sniffer you notice the following line: "GET /scripts../winnt/system32/cmd.exe?".
- c) It looks like users on VLAN6 are infected with a Trojan.
- d) The web server is using the following ports: 80, 8080 and 21.

- e) Configure R6's FR interface to prevent such attacks.
- f) Limit all other HTTP traffic to 64Kb/sec.
- **Configure class-maps to differentiate between legitimate HTTP traffic and an attack. The attack will match HTTP sessions that includes "cmd.exe" in their URL:**

```
access-list 101 permit ip any host 9.12.112.222
class-map match-all cmHTTP
match protocol http
class-map match-all cmAttack
match access-group 101
match protocol http url "*cmd.exe"
```

- **Configure a policy-map, which will drop attacks and limit the bandwidth for the legitimate HTTP traffic. Apply the policy-map to the Serial interface:**

```
policy-map pmFR
class cmAttack
drop
class cmHTTP
shape average 64000
int s0/1/0
service-policy output pmFR
```

- **Because FTP is using port 21, it will not be possible to configure NBAR to look for HTTP on port 21. Configure NBAR to look for FTP on port 9999 then configure NBAR to look for HTTP traffic on ports 80, 8080 and 21:**

```
ip nbar port-map ftp tcp 9999
ip nbar port-map http tcp 80 8080 21
```

10.2 – 2 points

- a) A server on VLAN6, which address is 9.12.6.66, is experiencing SYN flood attack.
- b) The server can support 2000 sessions at most.
- c) Configure R6 to prevent such attacks.
- d) Make sure that the server is not accessed directly.

- **The requirement implies that the router should use TCP interception mode and not the watch mode.**
- **Interception mode is on by default. Configure ACL and enable TCP intercept:**

```
access-list 102 permit tcp any host 9.12.6.66
ip tcp intercept list 102
```

- **Configure the max-incomplete threshold so the router will start dropping uncompleted TCP sessions when they count 200:**

```
ip tcp intercept max-incomplete high 2000
```


10.3 – 2 points

- a) Configure R1 to prevent telnet application passing through it.
- b) Don't use access-group or policy-map.

→ Another way to filter packets is using policy base routing, by sending matched packets to the Null interface. Configure ACL to match TELNET traffic. Configure route-map to send matching packets to Null interface:

```
access-list 150 permit tcp any any eq telnet
access-list 150 permit tcp any eq telnet any
route-map rmNO_TELNET
  match ip address 150
  set interface Null0
```

→ Policy base routing is performed on incoming packets only. Configure policy based routing on both interfaces:

```
int f0/0
  ip policy route-map rmNO_TELNET
int f0/1
  ip policy route-map rmNO_TELNET
```

10.4 – 2 point

- a) A new security policy mandates that R6 router should be managed only on weekdays from 9am to 8pm.
- b) Apply this policy on R6.
- c) Log policy violations.

→ Time ranges can be applied to any ACL, no matter for what the ACL is used for.

→ Configure time range to match the requested time frames:

```
time-range TR
  periodic weekdays 9:00 to 20:00
```

→ Configure ACL which allows SSH connections only on the valid time range. Configure the ACL to log all denied connections:

```
access-list 103 permit tcp any any eq 22 time-range TR
access-list 103 deny ip any any log
```

→ Apply the ACL to the VTY lines:

```
line vty 0 4
  access-class 103 in
```


11 – IDS Basic (5 points)

11.1 – 3 points

- Configure IPS to be inline with outside interface of Vasa1a.
- Set the IPS name to IPEXPERT_IPS.
- Set the ip address of the management interface to 192.168.10.13.
- Set the alarm severity of “Echo reply” to medium. Trigger the alarm and make sure it appears at the IEV console.

→ **Configure basic sensor configuration. Set the hostname, IP address and add 192.168.10.0/24 to the allowed networks, so the ACS would be able to configure the IDS:**

```

sensor#setup
...
Continue with configuration dialog?[yes]: [enter]
Enter host name[sensor]: IPEXPERT_IPS
Enter IP interface[10.1.9.201/24,10.1.9.1]: \
192.168.10.13/24,192.168.10.9
Enter telnet-server status[disabled]: [enter]
Enter web-server port[443]: [enter]
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 192.168.10.0/24
Permit: [enter]
Modify system clock settings?[no]: [enter]
Modify virtual sensor "vs0" configuration?[no]: [enter]
...
exit
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]: [enter]
...
Modify system date and time?[no]: [enter]
sensor#reset

```

→ **Configure CAT1 to place C&C interface on VLAN10:**

```

Int f0/8
Switchport access vlan 10

```

→ **To place the IDS between Vasa1a and VLAN112, split VLAN112 into two VLANS: VLAN112 and VLAN 113. Place Vasa1a outside interface and IDS F1/0 interface on VLAN113, and place F1/1 on VLAN112.**

- On CAT1 add VLAN113 to the VLAN database and place IDS F1/0 in VLAN 113 and F1/1 in VLAN112:

```
vlan 113
interface FastEthernet0/17
switchport access vlan 113
interface FastEthernet0/17
switchport access vlan 112
```

- Set CAT3 F0/11 interface, which belongs to Vasa1a outside interface to VLAN113

```
int f0/11
switchport access vlan 113
```

- IDS configuration using GUI:

- On the interfaces screen, enable both F1/0 and F1/1 and apply:

Cisco IDM 5.1 - 192.168.10.13

File Help

Configuration Monitoring Back Forward Refresh Help

Sensor Setup

- Network
- Allowed Hosts
- SSH
- Certificates
- Time
- Users

Interface Configuration

- Summary
- Interfaces**
- Interface Pairs
- VLAN Pairs
- Bypass
- Traffic Flow Notific

Analysis Engine

- Virtual Sensor
- Global Variables

Signature Definition

- Signature Variable
- Signature Configu
- Custom Signature
- Miscellaneous

Event Action Rules

- Event Variables
- Target Value Ratin
- Event Action Overri
- Event Action Filters
- General Settings

Blocking

Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed
FastEthernet0/1	No	TX (copper)	Auto	Auto
FastEthernet1/0	Yes	TX (copper)	Auto	Auto
FastEthernet1/1	Yes	TX (copper)	Auto	Auto
FastEthernet1/2	No	TX (copper)	Auto	Auto
FastEthernet1/3	No	TX (copper)	Auto	Auto

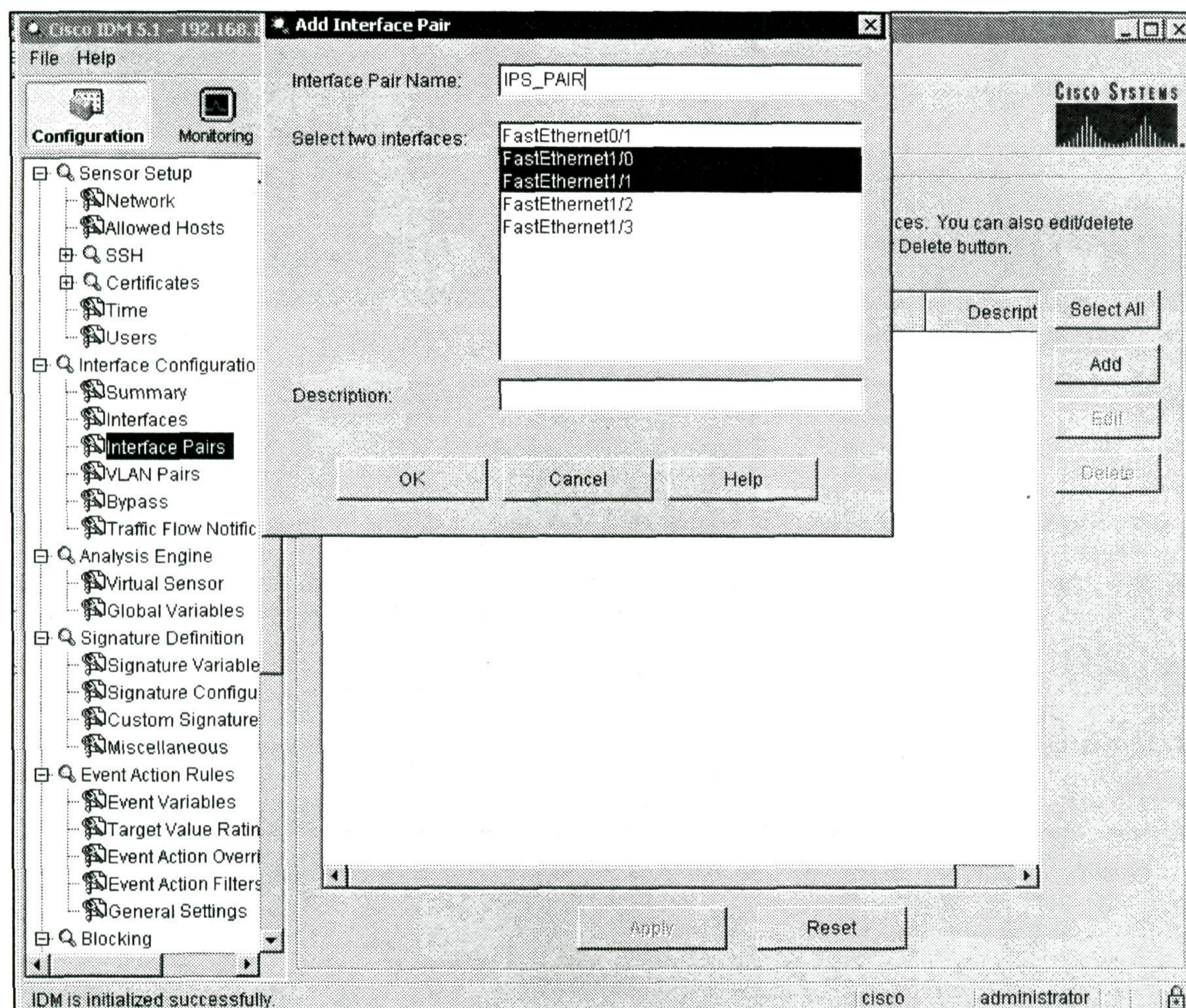
Select All Edit Enable Disable

Apply Reset

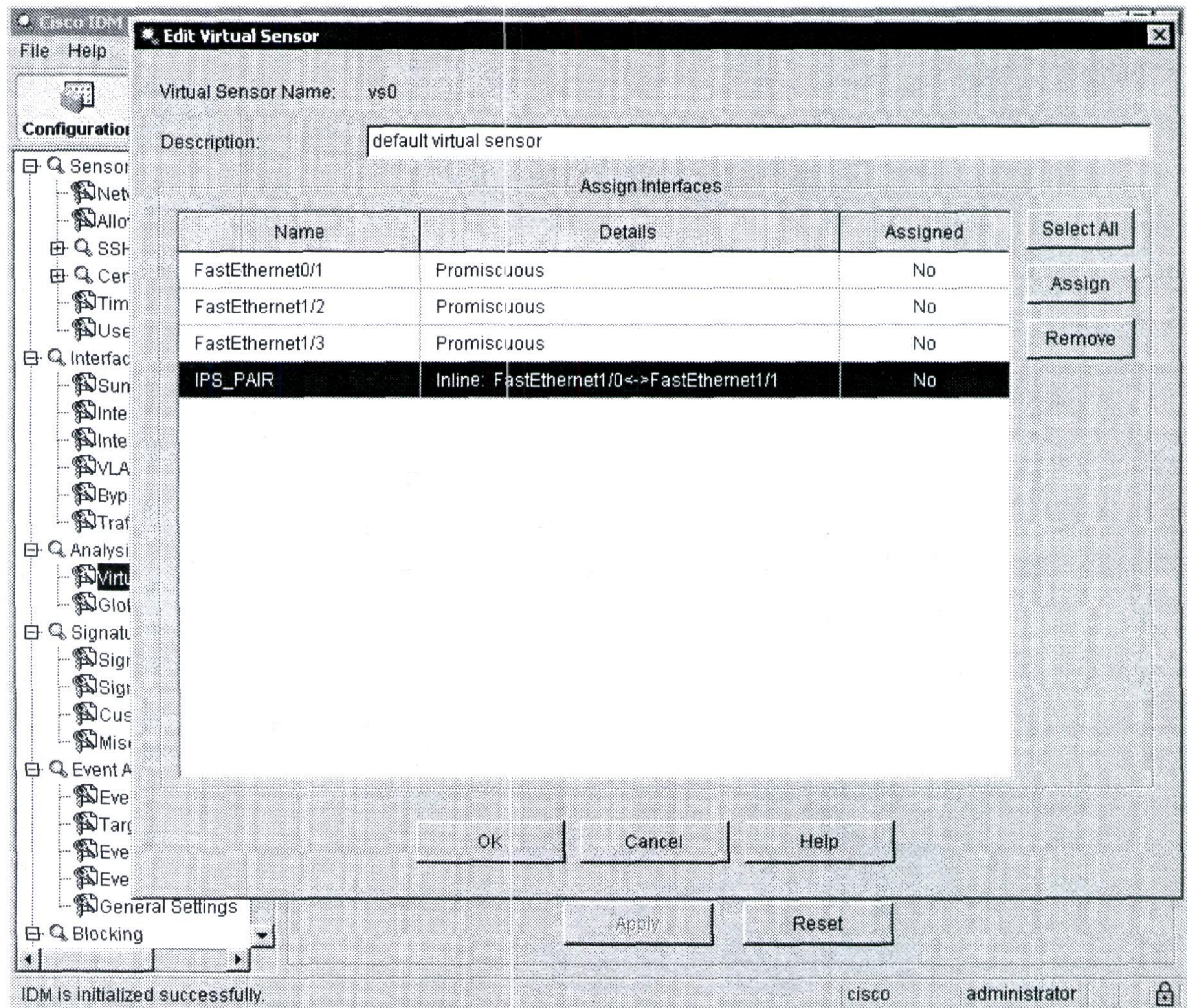
IDM is initialized successfully

cisco administrator

→ On the Interface pairs screen, add a new pair made of F1/0 and F1/1:



→ On the Virtual sensor screen, assign IPS_Pair to vs0:



- On the Signature configuration screen, locate "Echo reply" signature 2000, enable it and set the alarm to medium. Apply the changes:

Edit Signature

Name	Value
Signature ID:	2000
SubSignature ID:	0
Alert Severity:	Medium
Sig Fidelity Rating:	100
Promiscuous Delta:	0

Sig Description:

Signature Name:	ICMP Echo Reply
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	S1

Engine: Atomic IP

Event Action:

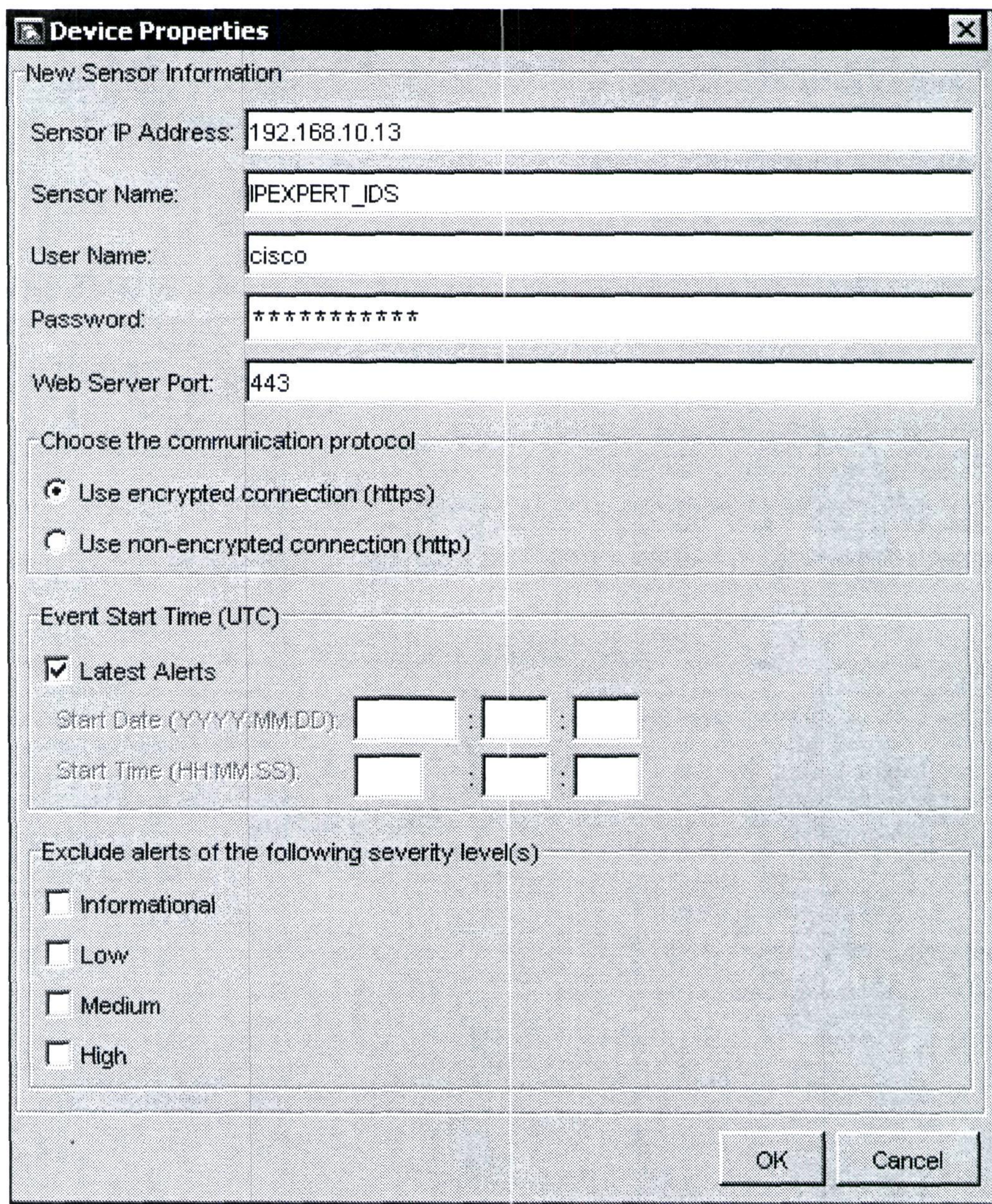
- Produce Alert
- Produce Verbose Alert
- Request Block Connection
- Request Block Host
- Request SNMP Trap

Fragment Status: Any

Parameter uses the Default Value. Click the icon to edit the value.
Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

→ Add the sensor to IEV desktop application:



The image shows a 'Device Properties' dialog box with a title bar containing a minimize button, a maximize button, and a close button. The dialog is divided into several sections. The first section, 'New Sensor Information', contains five text input fields: 'Sensor IP Address' (192.168.10.13), 'Sensor Name' (IPEXPERT_IDS), 'User Name' (cisco), 'Password' (masked with asterisks), and 'Web Server Port' (443). The second section, 'Choose the communication protocol', has two radio buttons: 'Use encrypted connection (https)' (selected) and 'Use non-encrypted connection (http)'. The third section, 'Event Start Time (UTC)', has a checked checkbox for 'Latest Alerts' and two sets of three input fields for 'Start Date (YYYY-MM-DD)' and 'Start Time (HH:MM:SS)'. The fourth section, 'Exclude alerts of the following severity level(s)', has four unchecked checkboxes: 'Informational', 'Low', 'Medium', and 'High'. At the bottom right are 'OK' and 'Cancel' buttons.

Device Properties

New Sensor Information

Sensor IP Address: 192.168.10.13

Sensor Name: IPEXPERT_IDS

User Name: cisco

Password: *****

Web Server Port: 443

Choose the communication protocol

☒ Use encrypted connection (https)

☐ Use non-encrypted connection (http)

Event Start Time (UTC)

☒ Latest Alerts

Start Date (YYYY-MM-DD): [] : [] : []

Start Time (HH:MM:SS): [] : [] : []

Exclude alerts of the following severity level(s)

☐ Informational

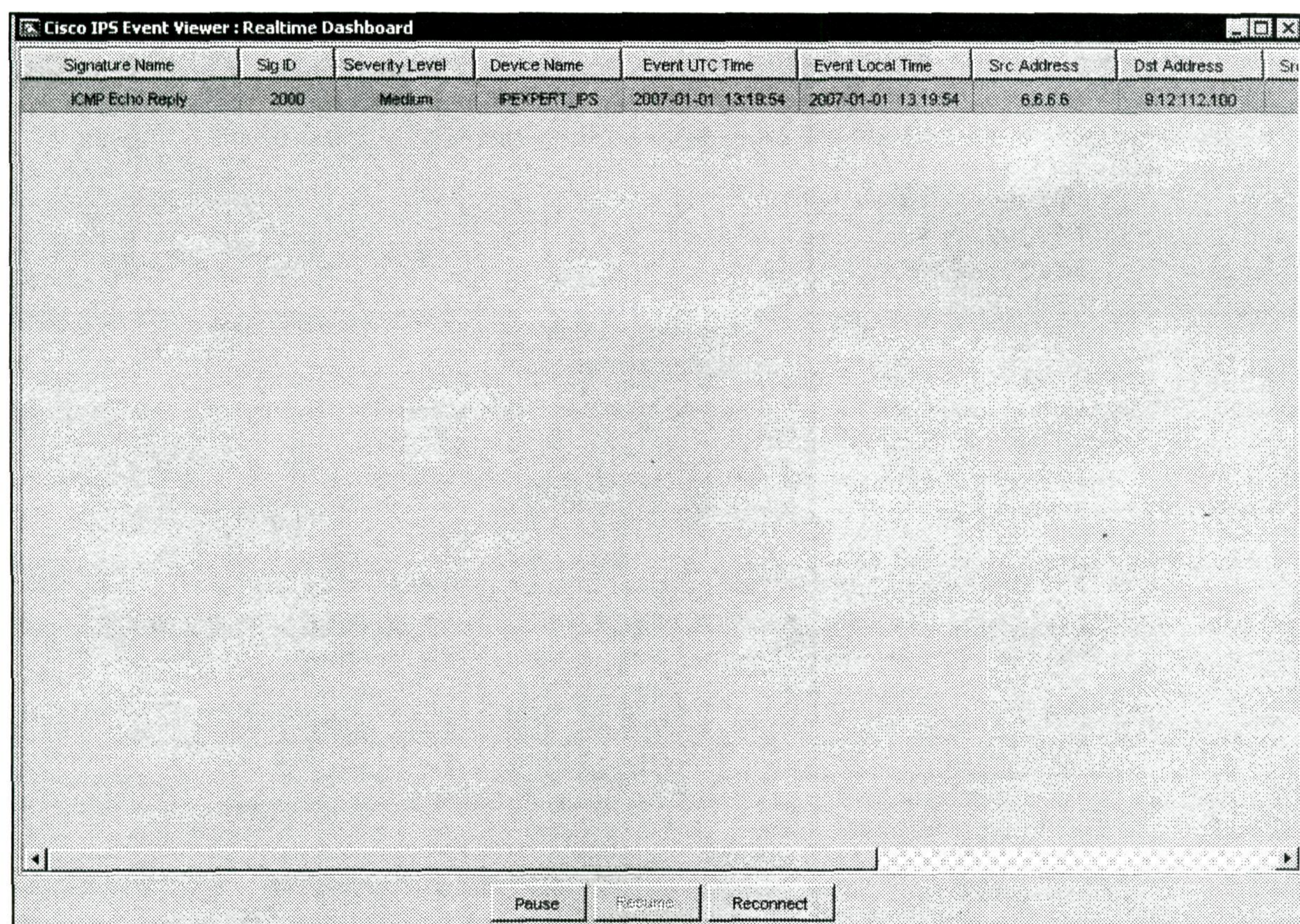
☐ Low

☐ Medium

☐ High

OK Cancel

→ Trigger a ping from the ACS to 6.6.6.6 and watch for the event:



11.2 – 2 points

- Configure the PIX to protect VLAN12 using signatures.
- Enable IPS on the outside interface.
- Log all events to the ACS server.
- There are many tear drops attacks on VLAN12. The ACS server is very busy and can accept no more than 10 messages per second. Make sure not to overwhelm the ACS server.
- You notice a lot of false positive alarms of "Bomb attack". Prevent such alarms from showing up in the logs.
- Informational signatures should be logged.
- Attack signatures should be logged and the session should drop.

→ Configure Vasa1a to allow syslog from the PIX:

```
access-list OUT extended permit udp host 9.12.112.10 host \
9.12.112.100 eq syslog
```


- Configure logging and limit the number of syslog sent to the ACS. Look at the PIX messages on “univercd” to look for the right message ID:

```
logging enable
logging host outside 9.12.112.100
logging rate-limit 10 1 message 106020
```

- Configure IPS parameters and disable the “Bomb attack” signature. To find out what is the signature number use the following command after enabling IPS on one of the interfaces sh ip audit count global:

```
ip audit name A2 attack action alarm drop
ip audit name A1 info action alarm
ip audit interface outside A1
ip audit interface outside A2
ip audit signature 4050 disable
```

12 – IDS Advanced (6 points)

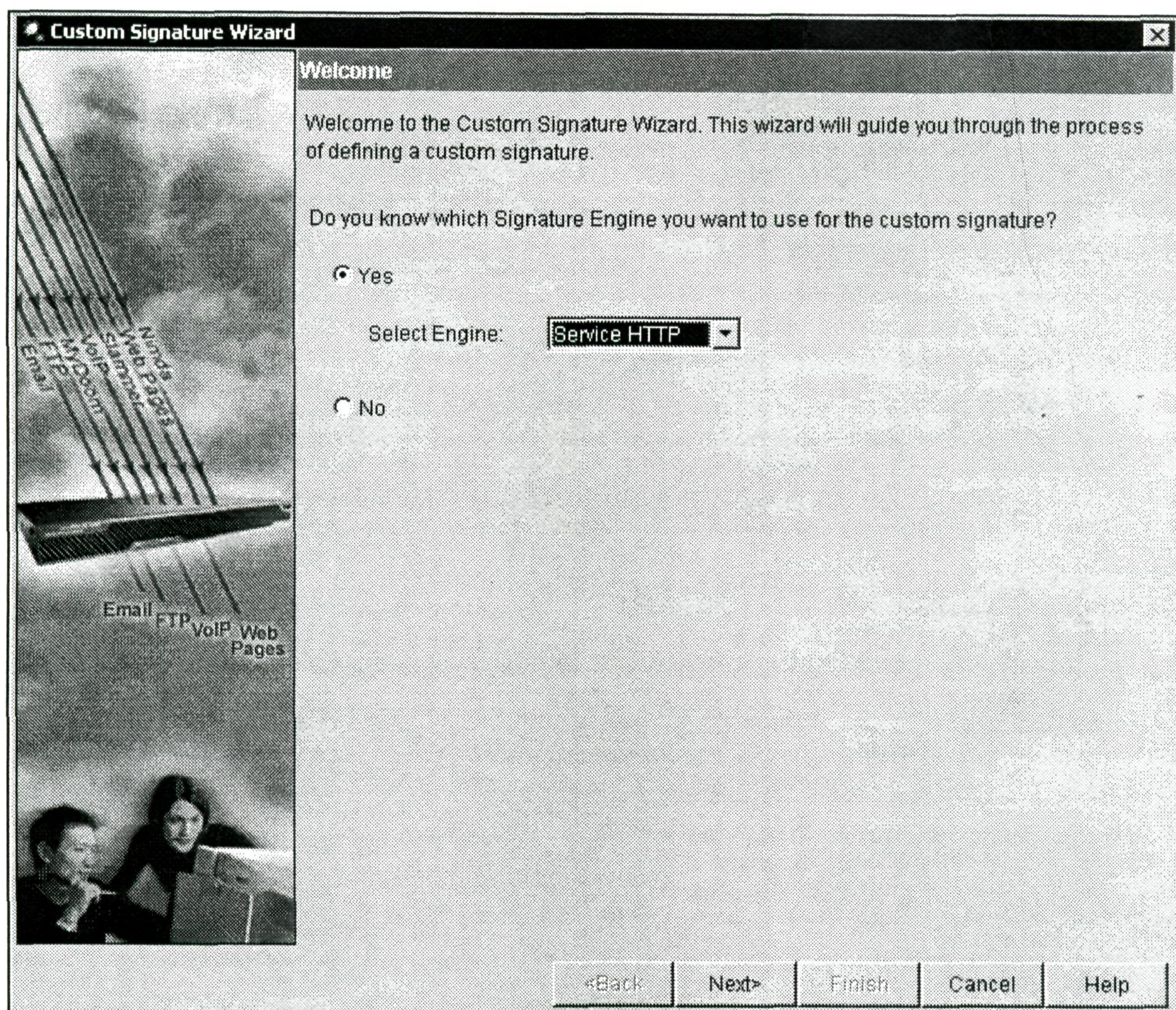
12.1 – 3 points

- a) Configure the IPS to drop any HTTP sessions using the following URLs:

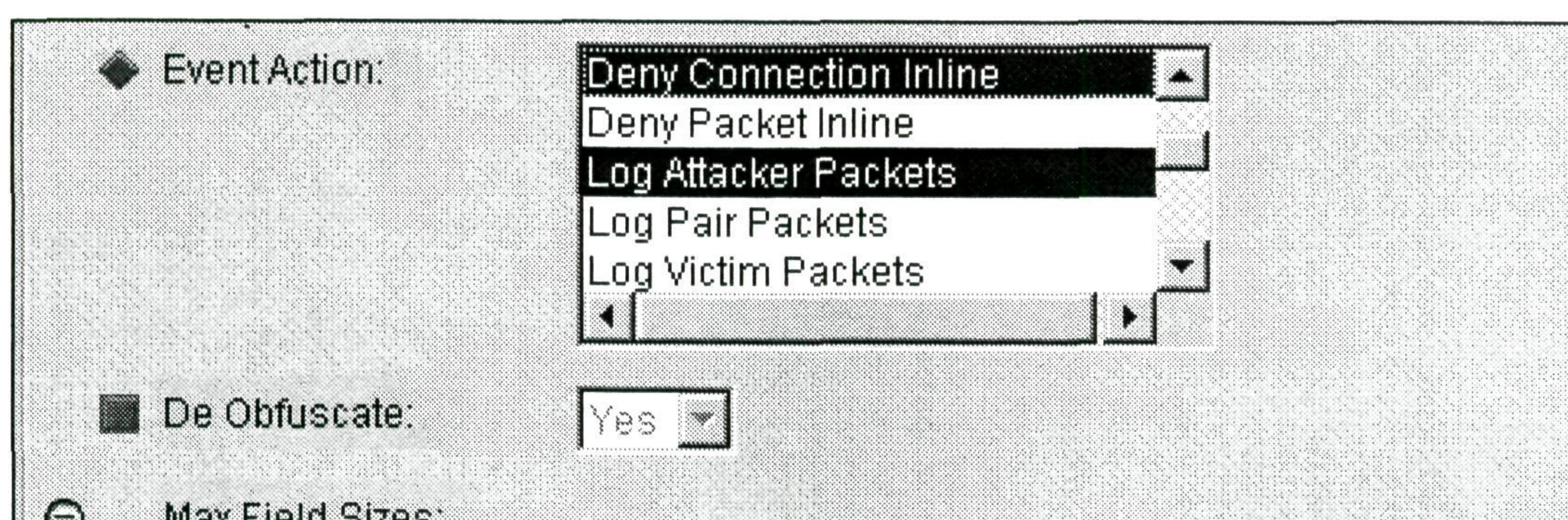
- "CMD.exe"
- "Cmd.exe"
- "cMd.ExE"

b) Log these sessions and keep packet trace.

→ Use the Signature wizard on Custom signature screen to create a new signature base on HTTP service:



→ Select Deny connection inline, Produce alert and Log attacker packets in the Event action:



- Specify URI regex, which is "(CMD.exe)|(Cmd.exe)|(cMD.ExE)", set the service port to 80 :

Regex:

Specify URI Regex: Yes

URI Regex: (CMD.exe)|(Cmd.exe)|(cMD.ExE)

Specify Arg Name Regex: No

Specify Header Regex: No

Specify Request Regex: No

Service Ports: 80

Swap Attacker Victim: No

- Click next, next , next ... and so on...

- Trigger the signature by browsing to <http://2.2.2.2/CMD.exe> from the CAS server:

Address <http://2.2.2.2/CMD.exe> Go Link

Cisco IPS Event Viewer : Realtime Dashboard

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst Address	Src Port	Dst Port
My Sig	60000	Medium	IPEXPERT_IPS	2007-01-01 13:48:50	2007-01-01 13:48:50	9.12.112.100	2.2.2.2		
ICMP Echo Reply	2000	Medium	IPEXPERT_IPS	2007-01-01 13:20:24	2007-01-01 13:20:24	6.6.6.6	9.12.112.100		
ICMP Echo Reply	2000	Medium	IPEXPERT_IPS	2007-01-01 13:19:54	2007-01-01 13:19:54	6.6.6.6	9.12.112.100		

Access

Show

More

Show

Exte

QoS