Copyright Information

Copyright © 2003 - 2007 Internetwork Expert, Inc. All rights reserved.

The following publication, *CCIE Security Lab Workbook Volume I*, was developed by Internetwork Expert, Inc. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means without the prior written permission of Internetwork Expert, Inc.

Cisco®, Cisco® Systems, CCIE, and Cisco Certified Internetwork Expert, are registered trademarks of Cisco® Systems, Inc. and/or its affiliates in the U.S. and certain countries. All other products and company names are the trademarks, registered trademarks, and service marks of the respective owners. Throughout this manual, Internetwork Expert, Inc. has used its best efforts to distinguish proprietary trademarks from descriptive names by following the capitalization styles used by the manufacturer.

Disclaimer

The following publication, *CCIE Security Lab Workbook Volume I*, is designed to assist candidates in the preparation for Cisco Systems' CCIE Routing & Switching Lab exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE[™] lab material is completely coincidental.

Table of Contents

VPN	1
COMMON CONFIGURATIONS	1
IOS Router and the PIX/ASA	1
IOS Router and VPN3k	6
GRE and DMVPN	24
VPN3k Easy VPN/WebVPN	27
IOS Easy VPN	42
PIX/ASA Easy VPN/WebVPN	46
IPSEC LAN-TO-LAN	50
IOS and the PIX/ASA with PSK	50
IOS and the PIX/ASA with PSK and NAT on the Firewall	55
IOS and the PIX/ASA with Digital Certificates	57
IOS and the PIX/ASA: Matching Name in Certificate	65
IOS and IOS with PSK Across the PIX/ASA	68
IOS and IOS with PSK Across the PIX/ASA and NAT	74
IOS and IOS with PSK Across the PIX/ASA with Overlapping Subnets	80
IOS and IOS with PSK Across the PIX/ASA and NAT with IKE AM	87
IOS and IOS with Digital Certificates Across the PIX/ASA	96
IOS and VPN3K With PSK	.103
IOS and VPN3K WITH PSK using CLI only	.113
IOS and VPN3k with DSK: Tuning IPcop Parameters	1/0
IOS and VPNSK with PSK. Turning IPSec Parameters	140
	169
GRE Tunnels over IPsec with Static Crypto Mans	168
GRE Tunnels over IPsec with Crypto Profiles	175
DMVPN with PSK	182
FASY VPN	.189
VPN3k and Cisco VPN Client	.189
VPN3k and Cisco VPN Client with Split-Tunneling	.201
VPN3k and Cisco VPN Client with Hold-Down Route	.206
VPN3k and Cisco VPN Client with RRI	.212
VPN3k and Cisco VPN Client with DHCP Server	.219
VPN3k and Cisco VPN Client with RADIUS Authentication	.224
VPN3k and Cisco VPN Client with External Group	.244
VPN3k and Cisco VPN Client with Digital Certificates	.256
VPN3k and IOS ezVPN Remote Client Mode with Split-Tunneling	.284
VPN3k and IOS ezVPN Remote NW Extension Mode with RRI	.298
IOS and IOS ezVPN Remote Client Mode with Xauth/RRI	.308
IOS and IOS ezVPN Remote NW Extension Mode with Xuath/RRI	.315
PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI	.318
PIX/ASA and Cisco VPN Client with External Policy	.324

PIX/ASA and Cisco VPN Client with RADIUS	339
PIX/ASA and Cisco VPN Client with Digital Certificates	345
The PIX/ASA and IOS ezVPN Remote NW Extension Mode	362
WEBVPN AND SSL VPN	367
ASA and WebVPN Client	367
ASA and WebVPN Port Forwarding	374
ASA and SSL VPN Client	380
VPN3k and WebVPN Client	383
VPN3k and WebVPN Port Forwarding	397
VPN QoS	407
IOS and the PIX/ASA: Policing the L2L IPsec tunnel	407
IOS and VPN3k: QoS for L2L Tunnel	410
PIX/ASA and Cisco VPN Client: Per-Flow Policing	417
QoS Pre-Classify for IPsec Tunnel	421
ADVANCED VPN TOPICS	425
Decoding IPsec Debugging Output on VPN3k	425
IPsec and Fragmentation Issues	440
ISAKMP Pre-Shared Keys via AAA	443
IPsec NAT-T: L2L Tunnel with VPN3k and IOS Box	459
IKE Tunnel Endpoint Discovery (TED)	466
IPsec VPN High-Availability with HSRP	470
IPsec High Availability with NAT and HSRP	479
IPsec Pass-Through Inspection on the PIX/ASA	483
L2TP over IPsec between the ASA and Windows 2000 PC	485
VPN3k and PPTP Client	494
Using ISAKMP Profiles	506
IOS FIREWALL	518
Common Configuration	518
Basic Access-Lists	521
Reflexive Access-Lists	527
Dynamic Access-Lists	531
Stateful Inspection with CBAC	534
CBAC Port-to-Application Mapping	537
Preventing DoS Attacks with CBAC	539
CBAC Performance Tuning	542
Authentication Proxy with RADIUS	544
Content Filtering with IOS Firewall	556

<u>VPN</u>

Common Configurations

IOS Router and the PIX/ASA

Objective: Configure common L2/L3 settings for IOS & the PIX/ASA VPN scenarios.



Directions

- Create VLANs, configure trunk and access-ports to reflect the diagram topology.
- Configure IP addressing as per the diagram.
- Configure RIP on the ASA Firewall and R3. Advertise all the connected interfaces.
- Configure static default route on R1 and R2 to point at ASA/R3 respectively.
- Permit outside access to AAA/CA server via HTTP/NTP, as well as ICMP traffic from outside.

Final Configuration

```
ASA1:

!

! IP addressing

!

interface Ethernet0/0

no shut

nameif outside
```

Copyright © 2007 Internetwork Expert

```
security-level 0
ip address 136.1.123.12 255.255.255.0
1
interface Ethernet0/1
no shut
nameif inside
security-level 100
ip address 136.1.121.12 255.255.255.0
T
interface Ethernet0/2
no shut
nameif dmz
security-level 50
ip address 10.0.0.12 255.255.255.0
!
! RIP configuration
!
router rip
version 2
no auto-summary
network 10.0.0.0
network 136.1.0.0
!
! Access-Control: permit HTTP/NTP and ICMP
!
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit icmp any any
!
access-group OUTSIDE_IN in interface outside
SW1 & SW2:
!
! create VLANs and configure trunk links
1
vlan 23,120,121,123
!
interface range Fa 0/21 - 23
switchport trunk encapsulation dotlq
switchport mode trunk
no shut
SW1:
!
 Configure switchports
!
1
interface Fa 0/1
switchport host
switchport access vlan 121
!
interface Fa 0/2
switchport host
switchport access vlan 23
!
interface Fa 0/3
switchport host
switchport access vlan 123
!
interface Fa 0/13
switchport host
switchport access vlan 121
!
interface Fa 0/20
```

```
switchport host
 switchport access vlan 120
SW2:
1
! Configure switchports
1
interface Fa 0/3
 switchport host
switchport access vlan 23
!
interface Fa 0/12
switchport host
switchport access vlan 123
R1:
interface E 0/0
no shut
ip add 136.1.121.1 255.255.255.0
T
ip route 0.0.0.0 0.0.0.0 136.1.121.12
R2:
interface E 0/0
no shut
ip add 136.1.23.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.23.3
R3:
interface E 0/0
no shut
ip add 136.1.123.3 255.255.255.0
interface E 0/1
no shut
ip add 136.1.23.3 255.255.255.0
!
router rip
version 2
no auto-summary
network 136.1.0.0
```

Verification

```
ASA1(config)# 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
       El - 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
     136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:06, outside
R
     136.1.121.0 \tt 255.255.255.0 is directly connected, inside
С
     136.1.123.0 255.255.255.0 is directly connected, outside
С
С
     10.0.0.0 255.255.255.0 is directly connected, \mbox{dmz}
```

Copyright © 2007 Internetwork Expert

```
R3#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, 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
     136.1.0.0/24 is subnetted, 3 subnets
С
        136.1.23.0 is directly connected, Ethernet0/1
        136.1.121.0 [120/1] via 136.1.123.12, 00:00:17, Ethernet0/0
R
        136.1.123.0 is directly connected, Ethernet0/0 \,
С
     10.0.0/24 is subnetted, 1 subnets
        10.0.0.0 [120/1] via 136.1.123.12, 00:00:17, Ethernet0/0
R
ASA1(config)# ping 10.0.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.100, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R2#ping 136.1.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.23.3, timeout is 2 seconds:
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/5 ms
R1#ping 136.1.121.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.12, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#telnet 136.1.23.2
Trying 136.1.23.2 ... Open
User Access Verification
Password:
R2>
R3#ping 10.0.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.100, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R3#telnet 10.0.100 80
Trying 10.0.0.100, 80 ... Open
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 12 Jan 2007 09:54:11 GMT
```

Content-Type: text/html Content-Length: 87 <html><head><title>Error</title></head><body>The parameter is incorrect. </body></html> [Connection to 10.0.0.100 closed by foreign host]

IOS Router and VPN3k

Objective: Configure common L2/L3 settings for IOS & VPN3k scenarios.



Directions

- Create VLANs, configure trunk and access-ports to reflect the diagram topology.
- Configure IP addressing as per the diagram.
- Configure RIP on the ASA Firewall, VPN3k and R2. Advertise all the connected interfaces.
- Configure static route for 150.X.1.0/24 on VPN3k.
- Configure static default route on R1 to point at VPN3k.
- Permit outside access to AAA/CA server via HTTP/NTP, as well as ICMP traffic from outside.
- Permit acess from DMZ to VPN3k via HTTPs.

Final Configuration

```
ASA1:

! IP addressing

!

interface Ethernet0/0

no shut

nameif outside

security-level 0

ip address 136.1.122.12 255.255.255.0

!

interface Ethernet0/1

no shut

nameif inside

security-level 100

ip address 136.1.121.12 255.255.255.0

!

interface Ethernet0/2

no shut
```

Copyright © 2007 Internetwork Expert

```
nameif dmz
security-level 50
ip address 10.0.0.12 255.255.255.0
!
! RIP configuration
!
router rip
version 2
no auto-summary
network 10.0.0.0
network 136.1.0.0
!
! Access-Control: permit HTTP/NTP and ICMP
1
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit icmp any any
1
access-group OUTSIDE_IN in interface outside
!
! HTTPs to VPN3k
1
access-list DMZ_IN extended permit tcp any any eq https
access-group DMZ_IN in interface dmz
SW1 & SW2:
!
! create VLANs and configure trunk links
!
vlan 111,120,121,122
I
interface range Fa 0/21 - 23
switchport trunk encapsulation dotlq
switchport mode trunk
no shut
SW1:
!
! Configure switchports
interface Fa 0/1
switchport host
switchport access vlan 111
1
interface Fa 0/2
switchport host
switchport access vlan 122
1
interface Fa 0/11
switchport host
switchport access vlan 111
T
interface Fa 0/13
switchport host
switchport access vlan 121
1
interface Fa 0/20
switchport host
switchport access vlan 120
SW2:
!
!
  Configure switchports
```

```
1
interface Fa 0/11
 switchport host
 switchport access vlan 121
!
interface Fa 0/12
switchport host
switchport access vlan 122
R1:
interface E 0/0
no shut
ip add 136.1.111.1 255.255.255.0
T
interface Loopback0
ip add 150.1.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 136.1.111.11
R2:
interface E 0/0
no shut
ip add 136.1.122.2 255.255.255.0
T
router rip
 version 2
no auto
network 136.1.0.0
network 150.1.0.0
interface Loopback 0
ip address 150.1.2.2 255.255.255.0
VPN3k:
Reboot with clean config:
                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
VPN3k: Main -> 2
1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Traceroute
7) Access Rights
8) File Management
9) Certificate Management
```

```
10) Back
VPN3k: Admin -> 3
1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back
VPN3k: Admin -> 2
1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back
VPN3k: Admin -> 3
1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
6) Back
VPN3k: Admin -> 2
41 01/15/2007 19:47:44.160 SEV=1 REBOOT/1 RPT=1
Reboot scheduled immediately.
Done
Perform initial setup:
                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
         Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.
 -- : Set the time on your device. The correct time is very important,
 -- : so that logging and accounting entries are accurate.
 -- : Enter the system time in the following format:
           HH:MM:SS. Example 21:30:00 for 9:30 PM
 -- :
> Time
Quick -> [ 19:52:27 ]
 -- : Enter the date in the following format.
-- : MM/DD/YYYY Example 06/12/1999 for June 12th 1999.
> Date
Quick -> [ 01/15/2007 ]
 -- : Set the time zone on your device. The correct time zone is very
```

-- : important so that logging and accounting entries are accurate. -- : Enter the time zone using the hour offset from GMT: ---: -12 : Kwajalein -11 : Samoa -10 : Hawaii -9 : Alaska ---: -8 : PST -7 : MST -6 : CST -5 : EST -6 · CS1 -7 · MS1 -6 · CS1 -5 · ES1 -4 : Atlantic -3 : Brasilia -3.5 : Newfoundland -1 : Mid--- : Atlantic --: -1: Azores 0: GMT +1: Paris +2: Cairo --: +3: Kuwait +3.5: Tehran +4: Abu Dhabi +4.5: Kabul -- : +5 : Karachi+5.5 : Calcutta +5.75 : Kathmandu+6 : Almaty-- : +6.5 : Rangoon+7 : Bangkok+8 : Singapore+9 : Tokyo-- : +9.5 : Adelaide+10 : Sydney+11 : Solomon Is.+12 : Marshall Is. > Time Zone Quick -> [-8] 1) Enable Daylight Savings Time Support 2) Disable Daylight Savings Time Support Quick -> [1] This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address _____
 Etherl-Pri | Not Configured |
 0.0.0.0/0.0.0.0
 |

 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 ** An address is required for the private interface. ** > Enter IP Address Quick Ethernet 1 -> [0.0.0.0] 136.1.111.11 Waiting for Network Initialization... > Enter Subnet Mask Quick Ethernet 1 -> [255.255.0.0] 255.255.255.0 > Enter Interface Name Quick Ethernet 1 -> Private 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)

Copyright © 2007 Internetwork Expert

```
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 -> 2
This table shows current IP addresses.
                                                              MAC Address
 Tntf
                            IP Address/Subnet Mask
               Status
     ------
                                         _____

      Ether1-Pri
      UP
      136.1.111.11/255.255.255.0
      00.03.A0.88.BD.29

      Ether2-Pub
      Not Configured
      0.0.0.0/0.0.00
      0

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured
> Enter IP Address
Quick Ethernet 2 -> [ 0.0.0.0 ] 136.1.121.11
> Enter Subnet Mask
Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.2
> Enter Interface Name
Quick Ethernet 2 -> Public
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 2 -> [ 3 ]
1) Enter Duplex - Half/Full/Auto

    2) Enter Duplex - Full Duplex
    3) Enter Duplex - Half Duplex

Quick Ethernet 2 -> [ 1 ]
> MTU (68 - 1500)
Quick Ethernet 2 -> [ 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
Ouick -> 4
 -- : Assign a System Name (hostname) to this device.
 -- : This may be required for DHCP.
> System Name
```

```
Quick -> VPN3K
 -- : Specify a local DNS server, which lets you enter hostnames
 -- : rather than IP addresses while configuring.
> DNS Server
VPN3K: Quick -> [ 0.0.0.0 ]
-- : Enter your Internet domain name; e.g., yourcompany.com
> Domain
VPN3K: Quick ->
> Default Gateway
VPN3K: Quick ->
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings
        PPTP
                    L2TP
                                           ......
| Enabled | Enabled |
| No Encryption Req | No Encryption Req |
1) Enable PPTP
2) Disable PPTP
VPN3K: Quick -> [ 1 ]
1) PPTP Encryption Required
2) No Encryption Required
VPN3K: Quick -> [ 2 ]
1) Enable L2TP
2) Disable L2TP
VPN3K: Quick -> [ 1 ]
1) L2TP Encryption Required
2) No Encryption Required
VPN3K: Quick -> [ 2 ]
1) Enable IPSec
2) Disable IPSec
VPN3K: Quick -> [ 1 ]
1) Enable WebVPN
2) Disable WebVPN
VPN3K: Quick -> [ 1 ] 2
-- : Configure address assignment for PPTP, L2TP and IPSec.
1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment
```

```
Copyright © 2007 Internetwork Expert
```

```
VPN3K: Quick -> [ 2 ]
1) Enable Per User Address Assignment
2) Disable Per User Address Assignment
VPN3K: Quick -> [ 2 ]
1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment
VPN3K: Quick -> [ 2 ]
1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment
VPN3K: Quick -> [ 2 ]
-- : Specify how to authenticate users
1) Internal
2) RADIUS
3) NT Domain
4) SDI
5) Kerberos/Active Directory
6) Continue
VPN3K: Quick -> [ 1 ]
                              Current Users
-----
                                _____
                                             _____
                               No Users
_____
1) Add a User
2) Delete a User
3) Continue
VPN3K: Ouick -> 3
> IPSec Group Name
VPN3K: Quick ->
-- : We strongly recommend that you change the password for user admin.
> Reset Admin Password
VPN3K: Quick -> [ ***** ]
Verify ->
1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit
VPN3K: Quick -> 2
1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit
VPN3K: Quick -> 1
```

1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3K: Config ->h Now configure RIP routing: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3K: Config -> 1 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address _____ Etherl-Pri UP | 136.1.111.11/255.255.255.0 | 00.03.A0.88.BD.29 UP Ether2-Pub 136.1.121.11/255.255.255.0 | 00.03.A0.88.BD.2A _____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Power Supplies 4) Back VPN3K: Interfaces -> 2 1) Interface Setting (Disable, DHCP or Static IP) 2) Set Public Interface 3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters 12) Back VPN3K: Ethernet Interface 2 -> 8

Copyright © 2007 Internetwork Expert

```
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3K: Ethernet Interface 2 -> 1
1) Disable Inbound RIP
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound
VPN3K: Ethernet Interface 2 -> [ 1 ] 3
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3K: Ethernet Interface 2 -> 2
1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound
VPN3K: Ethernet Interface 2 -> [ 1 ] 3
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3K: Ethernet Interface 2 ->
Permit RIP through the Public Filter:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3K: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3K: Config -> 4
1) Access Hours
2) Traffic Management
```

3) Group Matching 4) Network Admission Control 5) Back VPN3K: Policy -> 2 1) Network Lists 2) Rules 3) Security Associations (SAs) 4) Filters 5) Network Address Translation (NAT) Rules 6) Bandwidth Policies 7) Back VPN3K: Traffic -> 4 Current Active Filters _____ | 1. Private (Default) | 3. External (Default) 2. Public (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 VPN3K: Filters -> 4 > Which Filter to assign Rules to VPN3K: 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 | IN FORWARD 5. L2TP In 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 OUT FORWARD | 15. NAT-T Out _____ _____ 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3K: Filters -> 1

Copyright © 2007 Internetwork Expert

Current Fi	lter Rules
<pre>1. GRE In 3. IPSEC-ESP In 5. IKE Out 7. PPTP Out 9. L2TP Out 11. ICMP Out 13. RIP Out 15. OSPF Out 17. Incoming HTTP Out 19. VRRP Out 21. Any Out 23. Incoming HTTPS Out 25. LDAP Out 27. Telnet/SSL Out 29. Outgoing HTTP Out 31. Outgoing HTTPS Out 33. CRL over LDAP Out 35. SSH Out 37. VCA Out 39. NAT-T Out 41. DHCP Out</pre>	<pre>2. GRE Out 4. IKE In 6. PPTP In 8. L2TP In 10. ICMP In 12. RIP In 14. OSPF In 16. Incoming HTTP In 18. VRRP In 20. Any In 22. Incoming HTTPS In 24. LDAP In 26. Telnet/SSL In 28. Outgoing HTTP In 30. Outgoing HTTPS In 32. CRL over LDAP In 34. SSH In 36. VCA In 38. NAT-T In 40. DHCP In</pre>
> Which Rule to add VPN3K: Filters -> 12 The Current Rules	s for this Filter
<pre>1. GRE In 2. IPSEC-ESP In 3. IKE In 4. PPTP In 5. L2TP In 6. ICMP In 7. VRRP In 8. NAT-T In 9. GRE Out 10. IKE Out 11. PPTP Out 12. L2TP Out 13. ICMP Out 14. VRRP Out 15. NAT-T Out 16. RIP In</pre>	IN FORWARD IN FORWARD IN FORWARD IN FORWARD IN FORWARD IN FORWARD IN FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD IN FORWARD IN FORWARD
 Add a Rule to this Filter Remove a Rule from this Filter Move the Rule Up Move the Rule Down Assign Security Assoc. to Rule Back VPN3K: Filters -> 1 	
Current Fi	lter Rules
1. GRE In 3. IPSEC-ESP In 5. IKE Out	2. GRE Out 4. IKE In 6. PPTP In

8. L2TP In 7. PPTP Out 10. ICMP In 9. L2TP Out 11. ICMP Out 12. RIP In 13. RIP Out 14. OSPF In | 16. Incoming HTTP In 15. OSPF Out 18. VRRP In 17. Incoming HTTP Out 19. VRRP Out 20. Any In 22. Incoming HTTPS In 24. LDAP In 21. Any Out 24. LDAF ____ 26. Telnet/SSL In 28. Outgoing HTTP In 30. Outgoing HTTPS In 32. CRL over LDAP In 34. SSH In 23. Incoming HTTPS Out 25. LDAP Out 27. Telnet/SSL Out 29. Outgoing HTTP Out 31. Outgoing HTTPS Out 33. CRL over LDAP Out 35. SSH Out 37. VCA Out | 38. NAT-T In 39. NAT-T Out 40. DHCP In 41. DHCP Out _____ > Which Rule to add VPN3K: Filters -> 13 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 OUT FORWARD 9. GRE Out OUT FORWARD 10. IKE Out 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 | IN FORWARD 16. RIP In 17. RIP Out OUT FORWARD _____ 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3K: Filters -> Configure static route to 150.1.0.0/24: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

6) Exit VPN3K: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3K: Config -> 2 1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.) 2) Address Management 3) IP Routing (static routes, OSPF, etc.) 4) Management Protocols (Telnet, TFTP, FTP, etc.) 5) Event Configuration 6) General Config (system name, time, etc.) 7) Client Update 8) Load Balancing Configuration 9) Back VPN3K: System -> 3 1) Static Routes 2) Default Gateways 3) OSPF 4) OSPF Areas 5) DHCP Parameters 6) Redundancy 7) Reverse Route Injection 8) DHCP Relay 9) Back VPN3K: Routing -> 1 Static Routes _____ Destination Mask Metric Destination _____ _____ No Static Routes Configured 1) Add Static Route 2) Modify Static Route 3) Delete Static Route 4) Back VPN3K: Routing -> 1 > Net Address VPN3K: Routing -> 150.1.1.0 > Subnet Mask VPN3K: Routing -> 255.255.255.0 1) Destination is Router 2) Destination is Interface VPN3K: Routing -> 1

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

> Router Address VPN3K: Routing -> 136.1.111.1 > Route Metric (1 - 16) VPN3K: Routing -> [1] Static Routes _____ Destination Mask Metric Destination 150.1.1.0 255.255.255.0 1 136.1.111.1 1) Add Static Route 2) Modify Static Route 3) Delete Static Route 4) Back VPN3K: Routing -> Permit management from outside via HTTPs: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3K: Config -> 1 This table shows current IP addresses. MAC Address Status IP Address/Subnet Mask Tntf _ _ _ _ _ _____ _____ Ether1-PriUP|136.1.111.11/255.255.255.0|00.03.A0.88.BD.29Ether2-PubUP|136.1.121.11/255.255.255.0|00.03.A0.88.BD.2A -----_____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Power Supplies 4) Back VPN3K: Interfaces -> 2 1) Interface Setting (Disable, DHCP or Static IP) 2) Set Public Interface

Copyright © 2007 Internetwork Expert

3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters 12) Back VPN3K: Ethernet Interface 2 -> 11 1) Enable/Disable HTTP and HTTPS Management 2) Enable/Disable HTTPS WebVPN 3) Enable/Disable POP3S 4) Enable/Disable IMAP4S 5) Enable/Disable SMTPS 6) Enable/Disable HTTP Redirect 7) Back VPN3K: Ethernet Interface 2 -> 1 1) Enable HTTP and HTTPS Management 2) Disable HTTP and HTTPS Management VPN3K: Ethernet Interface 2 -> [2] 1 You may save current config for further reference: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 2 1) Administer Sessions 2) Software Update 3) System Reboot 4) Reboot Status 5) Ping 6) Traceroute 7) Access Rights 8) File Management 9) Certificate Management 10) Back VPN3K: Admin -> 8 List of Files _ _ _ _ _ _ _ _ _ _ _ _ _ SAVELOG.TXT CONFIG CONFIG.SAV CRSHDUMP.TXT CONFIG.BAK 1) Delete File 2) Copy File 3) View File 4) Put File via TFTP 5) Get File via TFTP

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

6) Swap Config Files 7) Export XML File 8) Import XML File 9) Reformat Filesystem 10) Back VPN3K: File -> 2 > Which File to copy VPN3K: File -> CONFIG > File name to copy to VPN3K: File -> CONFIG.SAV List of Files _____ SAVELOG.TXT CONFIG CONFIG.SAV CRSHDUMP.TXT CONFIG.BAK 1) Delete File 2) Copy File 3) View File 4) Put File via TFTP 5) Get File via TFTP 6) Swap Config Files 7) Export XML File 8) Import XML File 9) Reformat Filesystem 10) Back

Verification

VPN3k: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 3 1) Routing Table 2) Event Log 3) System Status 4) Sessions 5) General Statistics 6) Dynamic Filters 7) Back VPN3K: Monitor -> 1 Routing Table _____ Number of Routes: 5 IP Address Mask Next Hop Intf Protocol Age Metric _____ 10.0.0.0 255.255.255.0 136.1.121.12 2 RIP 28 2

```
Copyright © 2007 Internetwork Expert
```

255.255.255.0 0.0.0.0 136.1.111.0 1 Local 0 1 136.1.121.0 255.255.255.0 0.0.0.0 2 Local 0 1 2 RIP 136.1.122.0 255.255.255.0 136.1.121.12 28 2 150.1.1.0 255.255.255.0 136.1.111.1 1 Static 0 1 1) Refresh Routing Table 2) Clear Routing Table 3) Back VPN3K: Routing -> ASA1(config)# 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 $\rm N1$ - OSPF NSSA external type 1, $\rm N2$ - OSPF NSSA external type 2 El - 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 136.1.111.0 255.255.255.0 [120/1] via 136.1.121.11, 0:00:19, inside R 136.1.121.0 255.255.255.0 is directly connected, inside С С 136.1.122.0 255.255.255.0 is directly connected, outside 10.0.0.0 255.255.255.0 is directly connected, dmz С R 150.1.1.0 255.255.255.0 [120/1] via 136.1.121.11, 0:00:19, inside R2#show ip route rip 136.1.0.0/24 is subnetted, 3 subnets 136.1.111.0 [120/2] via 136.1.122.12, 00:00:27, Ethernet0/0 R R 136.1.121.0 [120/1] via 136.1.122.12, 00:00:27, Ethernet0/0 10.0.0/24 is subnetted, 1 subnets 10.0.0.0 [120/1] via 136.1.122.12, 00:00:27, Ethernet0/0 R 150.1.0.0/24 is subnetted, 1 subnets R 150.1.1.0 [120/2] via 136.1.122.12, 00:00:27, Ethernet0/0 R1#ping 136.1.111.11 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 136.1.111.11, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms R1#ping 150.1.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds: . ! ! ! ! Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

GRE and DMVPN

Objective: Configure common L2/L3 settings for DMVPN and GRE scenarios.



Directions

- Configure Loopback interfaces as per the diagram.
- Configure Frame-Relay interfaces. Use physical interfaces and static mappings on every router.
- R2 should be able to reach R3 via R1. Provide static mappings to make this possible.
- Configure RIP as routing protocol on FR cloud.
- Advertise Loopback0 interfaces into RIP.

Final Configuration

```
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
```

Copyright © 2007 Internetwork Expert

```
interface Loopback1
ip address 192.168.1.1 255.255.255.0
T
interface Serial 0/0
  encaps frame
 no frame inverse
 no shut
  frame map ip 136.1.0.2 102 broad
  frame map ip 136.1.0.3 103 broad
  ip add 136.1.0.1 255.255.255.0
!
router rip
 ver 2
 no auto
 net 136.1.0.0
 net 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
interface Loopback1
ip address 192.168.2.2 255.255.255.0
T
interface Serial 0/0
 encaps frame
 no frame inverse
 no shut
 frame map ip 136.1.0.1 201 broad
  frame map ip 136.1.0.3 201
  ip add 136.1.0.2 255.255.255.0
!
router rip
  ver 2
  no auto
 net 136.1.0.0
 net 150.1.0.0
R3:
interface Loopback0
ip address 150.1.3.3 255.255.255.0
1
interface Loopback1
ip address 192.168.3.3 255.255.255.0
!
interface Serial 1/0
 encaps frame
 no frame inverse
 no shut
 frame map ip 136.1.0.1 301 broad
  frame map ip 136.1.0.2 301
  ip add 136.1.0.3 255.255.255.0
!
router rip
 ver 2
  no auto
 net 136.1.0.0
  net 150.1.0.0
```

Verification

```
R1#ping 136.1.0.2
```

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 136.1.0.2, timeout is 2 seconds: IIIII Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms R1#ping 136.1.0.3

Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 136.1.0.3, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms R1#show ip route rip 150.1.0.0/24 is subnetted, 3 subnets R 150.1.3.0 [120/1] via 136.1.0.3, 00:00:13, Serial0/0 R 150.1.2.0 [120/1] via 136.1.0.2, 00:00:06, Serial0/0 R3#show ip route rip 150.1.0.0/24 is subnetted, 3 subnets 150.1.2.0 [120/2] via 136.1.0.2, 00:00:28, Serial1/0 R R 150.1.1.0 [120/1] via 136.1.0.1, 00:00:28, Serial1/0 R3#ping 150.1.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms

VPN3k Easy VPN/WebVPN

Objective: Configure common L2/L3 settings for VPN3k Easy VPN/WebVPN scenarios.



Directions

- Create VLANs 100,111,113, 200 on SW1 and SW2.
- Configure the switchports into respective VLANs.
- Configure HDLC link between R2 and R3.
- Configure IP addressing on routers and VPN3k as per the diagram.
- Configure IP addressing on Test PC.
- Confiture RIP routing on VPN3k. Permit RIP to pass through the Public filter.
- Configure a static default route on R1 and Test PC to point at VPN3k and R3 respectively.
- Configure RIP routing on R2 and R3.

Final Configuration

```
SW1 & SW2:
!
!
! create VLANs and configure trunk links
!
vlan 100,111,113,200
```

Copyright © 2007 Internetwork Expert

```
interface range Fa 0/21 - 23
switchport trunk encapsulation dotlq
 switchport mode trunk
no shut
SW1:
!
!
  Configure switchports
!
interface Fa 0/1
switchport host
switchport access vlan 111
T
interface Fa 0/2
switchport host
switchport access vlan 200
1
interface Fa 0/3
switchport host
switchport access vlan 113
T
interface Fa 0/11
switchport host
switchport access vlan 111
!
interface Fa 0/20
switchport host
switchport access vlan 200
SW2:
!
! Configure switchports
!
interface Fa 0/3
switchport host
switchport access vlan 100
!
interface Fa 0/11
switchport host
switchport access vlan 113
1
interface Fa 0/20
switchport host
switchport access vlan 100
R1:
interface E 0/0
no shut
ip add 136.1.111.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 136.1.111.11
R2:
interface E 0/0
no shut
ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
no shut
ip address 136.1.23.2 255.255.255.0
!
router rip
```

network 10.0.	0.0		
	0.0		
R3:			
interface E 0/	0		
ip add 136.1.	113.3 255.255.255.0		
!	11010 1001100110010		
interface E 0/	1		
no shut	100 3 255 255 255 0		
!	100.5 255.255.255.0		
interface Ser	1/3		
no shut	1000		
ip address 13	36.1.23.3 255.255.255.0		
!			
router rip			
ver 2 no auto			
network 136.1			
Test PC:			
		portios 2 X	
-	iternet Protocol (TCP/1P) Pro	percies i A	
	General		
	You can get IP settings assigned	automatically if your network supports	
	the appropriate IP settings.	ed to ask your network administrator for	
	Obtain an IP address autor	matically	
		ss:	
	IP address:	136. 1.100.200	
	S <u>u</u> bnet mask:	255.255.255.0	
	Defendence		
	Default gateway:	136.1.100.3	
	C Obtain DNS server address	s automatically	
	C Obtain DNS server address	s automatically ver addresses:	
	Optain DNS server address Optain DNS server Optain DNS server	ver addresses:	
	C Optain DNS server address • Use the following DNS server: Preferred DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3	
	© Optain DNS server address © Use the following DNS serv Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3	
	© Optain DNS server address © Use the following DNS serv Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3	
	C Optain DNS server address ■ Use the following DNS server: Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3 	
	C Optain DNS server address ■ Use the following DNS server: Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3 Ad <u>v</u> anced	
	© Optain DNS server address © Use the following DNS serv Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3 Advanced	
	C Optain DNS server address ■ Use the following DNS server: Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3 Advanced	
	C Optain DNS server address ■ Use the following DNS server: Preferred DNS server: Alternate DNS server:	s automatically ver addresses: 136 . 1 . 100 . 3 Advanced OK. Cancel	

```
Erase present configuration:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3K: Main -> 2
1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Traceroute
7) Access Rights
8) File Management
9) Certificate Management
10) Back
VPN3K: Admin -> 3
1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back
VPN3K: Admin -> 2
1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back
VPN3K: Admin -> 3
1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
6) Back
VPN3K: Admin -> 2
VPN3k Initial configuration:
                Welcome to
               Cisco Systems
       VPN 3000 Concentrator Series
         Command Line Interface
Copyright (C) 1998-2005 Cisco Systems, Inc.
 -- : Set the time on your device. The correct time is very important,
 -- : so that logging and accounting entries are accurate.
 -- : Enter the system time in the following format:
```

HH:MM:SS. Example 21:30:00 for 9:30 PM -- : > Time Quick -> [23:53:38] -- : Enter the date in the following format. -- : MM/DD/YYYY Example 06/12/1999 for June 12th 1999. > Date Quick -> [01/17/2007] -- : Set the time zone on your device. The correct time zone is very -- : important so that logging and accounting entries are accurate. -- : Enter the time zone using the hour offset from GMT:

 -- : -12 : Kwajalein
 -11 : Samoa
 -10 : Hawaii
 -9 : Alaska

 -- : -8 : PST
 -7 : MST
 -6 : CST
 -5 : EST

 -- : -8 : PST -7 : MST -6 : CST -5 : EST -- : -4 : Atlantic -3 : Brasilia -3.5 : Newfoundland -1 : Mid-Atlantic 0 : GMT +1 : Paris +2 : Cairo +3.5 : Tehran +4 : Abu Dhabi +4.5 : Kabul -- : -1 : Azores -- : +3 : Kuwait -- : +3 : Kuwalt+3.5 : Tehran+4 : Abu Dhabi+1.5 : Kabu I-- : +5 : Karachi+5.5 : Calcutta +5.75 : Kathmandu+6 : Almaty-- : +6.5 : Rangoon+7 : Bangkok+8 : Singapore+9 : Tokyo-- : +9.5 : Adelaide+10 : Sydney+11 : Solomon Is.+12 : Marshall Is. > Time Zone Quick -> [-8] 1) Enable Daylight Savings Time Support 2) Disable Daylight Savings Time Support Quick -> [1] This table shows current IP addresses. Status IP Address/Subnet Mask MAC Address Intf _____
 Ether1-Pri |Not Configured
 0.0.0.0/0.0.0

 Ether2-Pub |Not Configured
 0.0.0.0/0.0.0
 _____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured ** An address is required for the private interface. ** > Enter IP Address Quick Ethernet 1 -> [0.0.0.0] 136.1.111.11 Waiting for Network Initialization ... > Enter Subnet Mask Quick Ethernet 1 -> [255.255.0.0] 255.255.255.0 > Enter Interface Name Quick Ethernet 1 -> Private

- 31 -

Copyright © 2007 Internetwork Expert

```
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 1 -> [ 3 ]

    Enter Duplex - Half/Full/Auto
    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 -> 2
This table shows current IP addresses.
               Status
                             IP Address/Subnet Mask
                                                                MAC Address
 Intf
_____

      Ether1-Pri
      UP
      136.1.111.11/255.255.255.0
      00.03.A0.88.BD.29

      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
Quick Ethernet 2 -> [ 0.0.0.0 ] 136.1.113.11
> Enter Subnet Mask
Quick Ethernet 2 -> [ 255.255.0.0 ] 255.255.255.0
> Enter Interface Name
Quick Ethernet 2 -> Public
1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect
Quick Ethernet 2 -> [ 3 ]

    Enter Duplex - Half/Full/Auto
    Enter Duplex - Full Duplex
    Enter Duplex - Half Duplex

Quick Ethernet 2 -> [ 1 ]
> MTU (68 - 1500)
Quick Ethernet 2 -> [ 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 -> 4
-- : Assign a System Name (hostname) to this device.
-- : This may be required for DHCP.
> System Name
Ouick -> VPN3k
 -- : Specify a local DNS server, which lets you enter hostnames
-- : rather than IP addresses while configuring.
> DNS Server
VPN3k: Quick -> [ 0.0.0.0 ]
-- : Enter your Internet domain name; e.g., yourcompany.com
> Domain
VPN3k: Quick ->
> Default Gateway
VPN3k: Quick ->
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings
                 PPTP
                            L2TP
                                          _____

    Enabled
    Enabled

    No Encryption Req
    No Encryption Req

_____
1) Enable PPTP
2) Disable PPTP
VPN3k: Quick -> [ 1 ]
1) PPTP Encryption Required
2) No Encryption Required
VPN3k: Quick -> [ 2 ]
1) Enable L2TP
2) Disable L2TP
VPN3k: Quick -> [ 1 ]
1) L2TP Encryption Required
2) No Encryption Required
VPN3k: Quick -> [ 2 ]
1) Enable IPSec
```

```
2) Disable IPSec
VPN3k: Quick -> [ 1 ]
1) Enable WebVPN
2) Disable WebVPN
VPN3k: Quick -> [ 1 ] 2
-- : Configure address assignment for PPTP, L2TP and IPSec.
1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment
VPN3k: Quick -> [ 2 ]
1) Enable Per User Address Assignment
2) Disable Per User Address Assignment
VPN3k: Quick -> [ 2 ]
1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment
VPN3k: Quick -> [ 2 ]
1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment
VPN3k: Quick -> [ 2 ]
-- : Specify how to authenticate users
1) Internal
2) RADIUS
3) NT Domain
4) SDI
5) Kerberos/Active Directory
6) Continue
VPN3k: Quick -> [ 1 ]
                              Current Users
_____
                               No Users
_____
1) Add a User
2) Delete a User
3) Continue
VPN3k: Quick -> 3
> IPSec Group Name
VPN3k: Quick ->
-- : We strongly recommend that you change the password for user admin.
> Reset Admin Password
VPN3k: Quick -> [ ***** ]
```

```
Verify ->
1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit
VPN3k: Quick -> 1
Permit RIP to pass through Public traffic filter:
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 4
1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back
VPN3k: Policy -> 2
1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back
VPN3k: Traffic -> 4
                        Current Active Filters
_____
1. Private (Default)2. Public (Default)3. External (Default)4. Firewall Filter f
                                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
VPN3k: Filters -> 4
> Which Filter to assign Rules to
VPN3k: Filters -> 2
                   The Current Rules for this Filter
 _____
1. GRE In
                                 IN FORWARD
                                   IN FORWARD
 2. IPSEC-ESP In
                                  IN FORWARD
 3. IKE In
                                 | IN FORWARD
 4. PPTP In
 5. L2TP In
                                 | IN FORWARD
```

```
Copyright © 2007 Internetwork Expert
```

| 6. ICMP In I IN FORWARD 7. VRRP In IN FORWARD 8. NAT-T In IN FORWARD 9. GRE Out OUT FORWARD OUT FORWARD 10. IKE Out OUT FORWARD 11. PPTP Out 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 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3k: Filters -> 1 Current Filter Rules _____ | 1. GRE In 2. GRE Out 3. IPSEC-ESP In 5. IKE Out 4. IKE In 6. PPTP In 7. PPTP Out 8. L2TP In 9. L2TP Out | 10. ICMP In 12. RIP In 14. OSPF In 11. ICMP Out 13. RIP Out 15. OSPF Out | 16. Incoming HTTP In 17. Incoming HTTP Out 18. VRRP In 19. VRRP Out | 20. Any In 22. Incoming HTTPS In 24. LDAP In 21. Any Out 23. Incoming HTTPS Out 26. Telnet/SSL In 28. Outgoing HTTP In 25. LDAP Out 27. Telnet/SSL Out 30. Outgoing HTTPS In 32. CRL over LDAP In 29. Outgoing HTTP Out 31. Outgoing HTTPS Out 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 VPN3k: Filters -> 12 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 IN FORWARD 7. VRRP In 8. NAT-T In IN FORWARD OUT FORWARD 9. GRE Out 10. IKE Out | OUT FORWARD | OUT FORWARD 11. PPTP Out

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

CCIE Security Lab Workbook Volume I Version 3.0

| 12. L2TP Out | OUT FORWARD | 13. ICMP Out | OUT FORWARD 14. VRRP Out | OUT FORWARD 15. NAT-T Out | OUT FORWARD | 16. RIP In IN FORWARD 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3k: 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 | 14. OSPF In 13. RIP Out | 16. Incoming HTTP In 15. OSPF Out 18. VRRP In 17. Incoming HTTP Out 19. VRRP Out 20. Any In 22. Incoming HTTPS In 24. LDAP In 21. Any Out 23. Incoming HTTPS Out | 26. Telnet/SSL In 25. LDAP Out 28. Outgoing HTTP In 27. Telnet/SSL Out 30. Outgoing HTTPS In 32. CRL over LDAP In 29. Outgoing HTTP Out 31. Outgoing HTTPS Out 34. SSH In 33. CRL over LDAP Out 36. VCA In 35. SSH Out 37. VCA Out | 38. NAT-T In 39. NAT-T Out | 40. DHCP In 41. DHCP Out _____ > Which Rule to add VPN3k: Filters -> 13 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. RIP In IN FORWARD

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

| 17. RIP Out OUT FORWARD _____ ------1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3k: Filters -> h Configure RIP on Public interface: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3k: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3k: Config -> 1 This table shows current IP addresses. Status IP Address/Subnet Mask Intf MAC Address _____ Ether1-PriUP|136.1.111.11/255.255.255.0|00.03.A0.88.BD.29Ether2-PubUP|136.1.113.11/255.255.255.0|00.03.A0.88.BD.2A _____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Power Supplies 4) Back VPN3k: Interfaces -> 2 1) Interface Setting (Disable, DHCP or Static IP) 2) Set Public Interface 3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters

Copyright © 2007 Internetwork Expert

```
12) Back
VPN3k: Ethernet Interface 2 -> 8
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 2 -> 1
1) Disable Inbound RIP
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound
VPN3k: Ethernet Interface 2 -> [ 1 ] 3
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 2 -> 2
1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound
VPN3k: Ethernet Interface 2 -> [ 1 ] 3
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 2 ->
Enable management on Public interface:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 1
This table shows current IP addresses.
```

CCIE Security Lab Workbook Volume I Version 3.0

Intf Status IP Address/Subnet Mask MAC Address _____ _____ -----Ether1-PriUP136.1.111.11/255.255.255.000.03.A0.88.BD.29Ether2-PubUP136.1.113.11/255.255.255.000.03.A0.88.BD.2A . _____ _____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Power Supplies 4) Back VPN3k: Interfaces -> 2 1) Interface Setting (Disable, DHCP or Static IP) 2) Set Public Interface 3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters 12) Back VPN3k: Ethernet Interface 2 -> 11 1) Enable/Disable HTTP and HTTPS Management 2) Enable/Disable HTTPS WebVPN 3) Enable/Disable POP3S 4) Enable/Disable IMAP4S 5) Enable/Disable SMTPS 6) Enable/Disable HTTP Redirect 7) Back VPN3k: Ethernet Interface 2 -> 1 1) Enable HTTP and HTTPS Management 2) Disable HTTP and HTTPS Management VPN3k: Ethernet Interface 2 -> [2] 1 1) Enable/Disable HTTP and HTTPS Management 2) Enable/Disable HTTPS WebVPN 3) Enable/Disable POP3S 4) Enable/Disable IMAP4S 5) Enable/Disable SMTPS 6) Enable/Disable HTTP Redirect 7) Back VPN3k: Ethernet Interface 2 ->

```
R3#ping 136.1.113.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.113.11, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
        136.1.0.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
R
        136.1.111.0 [120/1] via 136.1.113.11, 00:00:05, Ethernet0/0
R
     10.0.0.0/24 is subnetted, 1 subnets
R
        10.0.0.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
     150.1.0.0/24 is subnetted, 1 subnets
R
        150.1.2.0 [120/1] via 136.1.23.2, 00:00:00, Serial1/3
VPN3k CLI:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 3
1) Routing Table
2) Event Log
3) System Status
4) Sessions
5) General Statistics
6) Dynamic Filters
7) Back
VPN3k: Monitor -> 1
Routing Table
_____
Number of Routes: 7
  IP Address
                      Mask
                                     Next Hop
                                                  Intf Protocol Age Metric
                 -----
  _____
10.0.0.0
            255.255.255.0 136.1.113.3 2 RIP
                                                                 13
                                                                          3
10.0.0.0255.255.255.0136.1.113.3136.1.0.0255.255.255.0136.1.113.3136.1.23.0255.255.255.0136.1.113.3136.1.100.0255.255.255.0136.1.113.3136.1.111.0255.255.255.00.0.0.0136.1.113.0255.255.255.00.0.0.0150.1.2.0255.255.255.0136.1.113.3
                                                    2 RIP
2 RIP
2 RIP
2 RIP
                                                                  13
                                                                            3
                                                                   13
                                                                            2
                                                                  13
                                                                            2
                                                                 0
                                                     1 Local
                                                                            1
                                                                   0
                                                      2 Local
                                                                            1
                                                      2 RIP
                                                                   13
                                                                            3
1) Refresh Routing Table
2) Clear Routing Table
3) Back
VPN3k: Routing ->
```

IOS Easy VPN

Objective: Configure common L2/L3 setting for IOS Easy VPN scenarios.



Directions

- Create VLANs 100,200,121,123 on SW1 & SW2.
- Configure the switchports into respective VLANs.
- Configure serial HDLC link between R2 and R3.
- Configure IP addressing as per the diagram.
- Configure RIP as routing protocol on R1, R2, R3, and ASA1.
- Configure the ASA to permit inbound IKE/ESP.

Final Configuration

```
SW1 & SW2:
    !
    create VLANs and configure trunk links
!
vlan 100,121,123,200
!
interface range Fa 0/21 - 23
    switchport trunk encapsulation dot1q
    switchport mode trunk
    no shut

SW1:
    !
    Configure switchports
!
interface Fa 0/1
```

Copyright © 2007 Internetwork Expert

```
switchport host
switchport access vlan 121
1
interface Fa 0/2
 switchport host
switchport access vlan 200
T
interface Fa 0/3
switchport host
switchport access vlan 123
!
interface Fa 0/12
switchport host
switchport access vlan 121
!
interface Fa 0/20
switchport host
switchport access vlan 200
SW2:
!
! Configure switchports
1
interface Fa 0/3
switchport host
switchport access vlan 100
!
interface Fa 0/12
switchport host
switchport access vlan 123
!
interface Fa 0/20
switchport host
switchport access vlan 100
R1:
interface E 0/0
no shut
ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
ip add 150.1.1.1 255.255.255.0
!
router rip
version 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E 0/0
no shut
ip add 10.0.0.2 255.255.255.0
1
interface Ser 0/1
no shut
ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
no auto
network 136.1.0.0
network 10.0.0.0
```

```
R3:
interface E 0/0
no shut
ip add 136.1.123.3 255.255.255.0
!
interface E 0/1
no shut
ip add 136.1.100.3 255.255.255.0
!
interface Ser 1/3
no shut
 clock rate 64000
ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
no auto
network 136.1.0.0
ASA1:
!
! IP addressing
I
interface Ethernet0/0
no shut
nameif outside
security-level 0
ip address 136.1.123.12 255.255.255.0
!
interface Ethernet0/1
no shut
nameif inside
security-level 100
ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
version 2
no auto-summary
network 136.1.0.0
!
! Permit Inbound IKE/ESP
!
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside
```

Copyright © 2007 Internetwork Expert

```
- 44 -
```

```
R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
R
        136.1.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
        136.1.121.0 [120/1] via 136.1.123.12, 00:00:23, Ethernet0/0
R
     10.0.0/24 is subnetted, 1 subnets
       10.0.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
R
     150.1.0.0/24 is subnetted, 1 subnets
        150.1.1.0 [120/2] via 136.1.123.12, 00:00:23, Ethernet0/0
R
R2#show ip route rip
    136.1.0.0/24 is subnetted, 5 subnets
        136.1.100.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
R
        136.1.121.0 [120/2] via 136.1.23.3, 00:00:21, Serial0/1
R
        136.1.123.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
R
     150.1.0.0/24 is subnetted, 2 subnets
R
        150.1.1.0 [120/3] via 136.1.23.3, 00:00:04, Serial0/1
```

PIX/ASA Easy VPN/WebVPN

Objective: Configure common L2/L3 setting for the PIX/ASA Easy VPN/WebVPN scenarios.



Directions

- Create VLANs 100,200,121,123 on SW1 & SW2.
- Configure the switchports into respective VLANs.
- Configure serial HDLC link between R2 and R3.
- Configure IP addressing as per the diagram.
- Configure RIP as routing protocol on R1, R2, R3, and ASA1.

Final Configuration

```
SW1 & SW2:

!
create VLANs and configure trunk links
!
vlan 100,121,123,200
!
interface range Fa 0/21 - 23
switchport trunk encapsulation dot1q
switchport mode trunk
no shut

SW1:
!
Configure switchports
!
interface Fa 0/1
```

Copyright © 2007 Internetwork Expert

```
switchport host
switchport access vlan 121
1
interface Fa 0/2
 switchport host
switchport access vlan 200
T
interface Fa 0/3
switchport host
switchport access vlan 123
!
interface Fa 0/12
switchport host
switchport access vlan 121
!
interface Fa 0/20
switchport host
switchport access vlan 200
SW2:
!
! Configure switchports
1
interface Fa 0/3
switchport host
switchport access vlan 100
!
interface Fa 0/12
switchport host
switchport access vlan 123
!
interface Fa 0/20
switchport host
switchport access vlan 100
R1:
interface E 0/0
no shut
ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
ip add 150.1.1.1 255.255.255.0
!
router rip
version 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E 0/0
no shut
ip add 10.0.0.2 255.255.255.0
1
interface Ser 0/1
no shut
ip address 136.1.23.2 255.255.255.0
!
router rip
 ver 2
no auto
network 136.1.0.0
network 10.0.0.0
```

```
R3:
interface E 0/0
no shut
ip add 136.1.123.3 255.255.255.0
!
interface E 0/1
no shut
ip add 136.1.100.3 255.255.255.0
!
interface Ser 1/3
no shut
 clock rate 64000
ip address 136.1.23.3 255.255.255.0
!
router rip
 ver 2
no auto
network 136.1.0.0
ASA1:
1
! IP addressing
I
interface Ethernet0/0
no shut
nameif outside
security-level 0
ip address 136.1.123.12 255.255.255.0
interface Ethernet0/1
no shut
nameif inside
 security-level 100
ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
version 2
no auto-summary
```

network 136.1.0.0

```
R1#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
        136.1.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0
R
        136.1.23.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R
R
        136.1.100.0 [120/2] via 136.1.121.12, 00:00:21, Ethernet0/0
R
        136.1.123.0 [120/1] via 136.1.121.12, 00:00:21, Ethernet0/0
     10.0.0/24 is subnetted, 1 subnets
       10.0.0.0 [120/3] via 136.1.121.12, 00:00:21, Ethernet0/0
R
R3#show ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
        136.1.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
R
        136.1.121.0 [120/1] via 136.1.123.12, 00:00:23, Ethernet0/0
R
     10.0.0/24 is subnetted, 1 subnets
R
        10.0.0.0 [120/1] via 136.1.23.2, 00:00:11, Serial1/3
     150.1.0.0/24 is subnetted, 1 subnets
```

```
Copyright © 2007 Internetwork Expert
```

CCIE Security Lab Workbook Volume I Version 3.0

R 150.1.1.0 [120/2] via 136.1.123.12, 00:00:23, Ethernet0/0
R2#show ip route rip
136.1.0.0/24 is subnetted, 5 subnets
R 136.1.100.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
R 136.1.123.0 [120/1] via 136.1.23.3, 00:00:21, Serial0/1
I50.1.0.0/24 is subnetted, 2 subnets
R 150.1.1.0 [120/3] via 136.1.23.3, 00:00:04, Serial0/1

IPsec LAN-to-LAN

IOS and the PIX/ASA with PSK

Objective: Configure IPsec L2L tunnel between the ASA firewall and IOS router using pre-shared key for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"IOS Router and the PIX/ASA"</u>.
- Configure L2L VPN on the ASA Firewall.
 - Create ISAKMP policy with priority 10 as follows:
 - Use 3DES encryption.
 - Use MD5 hash.
 - Use DH Group2.
 - Use Pre-Shared keys authentication.
 - Enable ISAKMP policy on the outside interface.
 - Create L2L tunnel-group with name "136.1.123.3" and configure pre-shared key "CISCO".
 - Create access-list VLAN121_TO_VLAN23 to match traffic from VLAN23 to VLAN121.
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES cipher

- Use MD5 hash
- Create crypto map VPN of type IPsec-ISAKMP as follows:
 - Match access-list VLAN121_TO_VLAN23.
 - Set peer ip 136.1.123.3.
 - Set transform-set 3DES_MD5.
- Apply crypto map VPN to outside interface.
- Enable VPN traffic to bypass ACL check.
- Configure L2L VPN on R3 as follows:
 - o Create ISAKMP policy with priority 10 as follows.
 - Use 3DES encryption.
 - Use MD5 hash.
 - Use DH Group2.
 - Use Pre-Shared keys authentication.
 - Configure pre-shared ISAKMP key "CISCO" for IP 136.1.123.3.
 - Create access-list VLAN23_TO_VLAN121 to match traffic from VLAN23 to VLAN121
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES cipher
 - Use MD5 hash
 - Create crypto map VPN of type IPsec-ISAKMP as follows:
 - Match access-list VLAN23_TO_VLAN121
 - Set peer ip 136.1.123.12
 - Set transform-set 3DES_MD5
 - Apply crypto map VPN to interface Eth 0/0.

Final Configuration

```
ASA1:

!

! Configure & Enable ISAKMP policy

!

crypto isakmp policy 10

authentication pre-share

encryption 3des

hash md5

!

crypto isakmp enable outside
```

Copyright © 2007 Internetwork Expert

```
1
! Configure tunnel group for L2L tunnel
1
tunnel-group 136.1.123.3 type ipsec-121
tunnel-group 136.1.123.3 ipsec-attributes
pre-shared-key CISCO
T
! Configure transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-list to classify traffic for encryption
access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0 136.1.23.0
255.255.255.0
!
! Configure crypto-map
!
crypto map VPN 10 match address VLAN121_TO_VLAN23
crypto map VPN 10 set peer 136.1.123.3
crypto map VPN 10 set transform-set 3DES_MD5
! Apply crypto-map and enable VPN traffic to bypass ACLs
1
crypto map VPN interface outside
sysopt connection permit-vpn
R3:
!
! Configure ISAKMP policy
crypto isakmp policy 10
encryption 3des
 auth pre-share
hash md5
group 2
!
crypto isakmp key CISCO address 136.1.123.12
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
! Create access-list to classify traffic for encryption
ip access-list extended VLAN23_TO_VLAN121
permit ip 136.1.23.0 0.0.0.255 136.1.121.0 0.0.0.255
!
! Create & apply crypto map
!
crypto map VPN 10 ipsec-isakmp
match address VLAN23_TO_VLAN121
set transform 3DES_MD5
set peer 136.1.123.12
1
interface E 0/0
 crypto map VPN
```

```
R2#ping 136.1.121.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 100/166/189 ms
R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                                      I-VRF
                                                Encr Hash Auth DH Lifetime Cap.
                      Remote
      136.1.123.3 136.1.123.12
                                                3des md5 psk 2 23:54:52
2
R3#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.123.3
   protected vrf:
   local ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     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 21, #recv errors 0
     local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
     path mtu 1500, media mtu 1500
     current outbound spi: 482D0576
     inbound esp sas:
      spi: 0xB0A78AA3(2963770019)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4455492/3285)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x482D0576(1210910070)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4455492/3285)
        IV size: 8 bytes
        replay detection support: Y
```

Copyright © 2007 Internetwork Expert

outbound ah sas: outbound pcp sas: ASA1(config) # show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 IKE Peer: 136.1.123.3 1 : L2L Role : responder Type : no : MM_ACTIVE Rekey State ASA1(config)# show cry ipsec sa interface: outside Crypto map tag: VPN, seq num: 10, local addr: 136.1.123.12 access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0 136.1.23.0 255.255.255.0 local ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0) current_peer: 136.1.123.3 #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: 4, #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.: 136.1.123.12, remote crypto endpt.: 136.1.123.3 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: B0A78AA3 inbound esp sas: spi: 0x482D0576 (1210910070) transform: esp-3des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 1, crypto-map: VPN sa timing: remaining key lifetime (kB/sec): (4274999/3132) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xB0A78AA3 (2963770019) transform: esp-3des esp-md5-hmac none in use settings ={L2L, Tunnel, } slot: 0, conn_id: 1, crypto-map: VPN sa timing: remaining key lifetime (kB/sec): (4274999/3132) IV size: 8 bytes replay detection support: Y

Further Reading

Configuring LAN-to-LAN IPSec VPNs

Copyright © 2007 Internetwork Expert

IOS and the PIX/ASA with PSK and NAT on the Firewall

Objective: Configure IPsec L2L tunnel between the ASA firewall and IOS router using pre-shared key for authentication. Consider NAT configured for users behind the ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and the PIX/ASA with PSK"</u>.
- Enable NAT control on the firewall.
- Configure NAT for inside users, use outside IP for PAT.
- When using NAT with VPN configuration, remember to exempt VPN traffic from NAT.
- Configure NAT exemption for IPsec VPN traffic.
- Use access-list EXEMPT to match traffic from VLAN121 to VLAN23.

Final Configuration

```
ASA1:

nat-control

NAT for inside users

nat (inside) 1 0 0

global (outside) 1 interface

Exemption access-list

access-list EXEMPT permit ip 136.1.121.0 255.255.255.0 136.1.23.0 255.255.255.0

nat (inside) 0 access-list EXEMPT
```

```
R1#telnet 136.1.123.3
Trying 136.1.123.3 ... Open
User Access Verification
Password:
R3>
Rack1AS>12
[Resuming connection 12 to asa1 ... ]
ASA1(config) # show x
1 in use, 10 most used
PAT Global 136.1.123.12(1024) Local 136.1.121.1(11072)
R1#ping 136.1.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.23.2, timeout is 2 seconds:
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 96/165/189 ms
R1#telnet 136.1.23.2
Trying 136.1.23.2 ... Open
User Access Verification
Password:
R2>
ASA1(config) # show x
0 in use, 10 most used
ASA1(config)# show conn
5 in use, 43 most used
TCP out 136.1.23.2:23 in 136.1.121.1:11073 idle 0:00:52 bytes 111 flags UIO
```

Further Reading

Configuring LAN-to-LAN IPSec VPNs

IOS and the PIX/ASA with Digital Certificates

Objective: Configure L2L VPN tunnel between R3 and the ASA. Use digital certificates for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"IOS Router and the PIX/ASA"</u>.
- Configure CA Truspoint with name IE1 on the ASA as follows:
 - Use enrollment URL: <u>http://10.0.0.100:80/certsrv/mscep/mscep.dll</u>
 - CRL is optional.
- Enroll the ASA with CA as follows:
 - Configure NTP server to 10.0.0.100.
 - Authenticate the CA.
 - o Configure domain-name and create RSA key-pair.
 - Enroll with CA finally.
- Configure L2L VPN on the ASA Firewall as follows.
 - Create ISAKMP policy with priority 10 as follows:
 - Use 3DES encryption.
 - Use MD5 hash.
 - Use DH Group2.
 - Use RSA-SIG authentication.

- Enable ISAKMP policy on the outside interface.
- Create L2L tunnel-group with name "136.1.123.3" and configure trustpoint "IE1".
- Create access-list VLAN121_TO_VLAN23 to match traffic from VLAN23 to VLAN121.
- Create transform-set 3DES_MD5 as follows:
 - Use 3DES cipher.
 - Use MD5 hash.
- Create crypto map VPN of type IPsec-ISAKMP as follows:
 - Match access-list VLAN121_TO_VLAN23.
 - Set peer ip 136.1.123.3.
 - Set transform-set 3DES_MD5.
- Apply crypto map VPN to outside interface.
- Enable VPN traffic to bypass ACL check.
- Configure CA Truspoint with name IE1 on R3 as follows:
 - Use enrollment URL: <u>http://10.0.0.100:80/certsrv/mscep/mscep.dll</u>
 - CRL is optional.
- Enroll R3 with CA as follows:
 - Configure NTP server to 10.0.0.100.
 - Authenticate the CA.
 - Configure domain-name and create RSA key-pair.
 - Enroll with CA finally.
- Configure L2L VPN on R3 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use 3DES encryption.
 - Use MD5 hash.
 - Use DH Group2.
 - Use RSA-Sig authentication.
 - Create access-list VLAN23_TO_VLAN121 to match traffic from VLAN23 to VLAN121
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES cipher.

- Use MD5 hash.
- Create crypto map VPN of type IPsec-ISAKMP as follows:
 - Match access-list VLAN23_TO_VLAN121.
 - Set peer ip 136.1.123.12.
 - Set transform-set 3DES_MD5.
- Apply crypto map VPN to interface Eth 0/0.

Final Configuration

```
ASA1:
1
! Trustpoint configuration
1
crypto ca trustpoint IE1
enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
crl optional
!
ntp server 10.0.100
!
crypto ca auth IE1
domain-name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
crypto ca enroll IE1
1
! L2L VPN. ISAKMP Configuration
!
crypto isakmp policy 10
 authentication rsa-sig
encryption 3des
hash md5
1
crypto isakmp enable outside
1
! Configure tunnel group for L2L tunnel
1
tunnel-group 136.1.123.3 type ipsec-121
tunnel-group 136.1.123.3 ipsec-attributes
  trust-point IE1
!
! Configure transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-list to classify traffic for encryption
access-list VLAN121_TO_VLAN23 permit ip 136.1.121.0 255.255.255.0 136.1.23.0
255.255.255.0
!
! Configure crypto-map
!
crypto map VPN 10 match address VLAN121_TO_VLAN23
crypto map VPN 10 set peer 136.1.123.3
crypto map VPN 10 set transform-set 3DES_MD5
```

```
Copyright © 2007 Internetwork Expert
```

```
! Apply crypto-map and enable VPN traffic to bypass ACLs
!
crypto map VPN interface outside
sysopt connection permit-vpn
R3:
!
! Configure trustpoint
!
crypto ca trustpoint IE1
enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
crl optional
!
! Generate keypair and enroll
ip domain name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
ntp server 10.0.0.100
crypto ca authenticate IE1
crypto ca enroll IE1
1
! L2L VPN:
! Configure ISAKMP policy
1
crypto isakmp policy 10
 encryption 3des
 auth rsa-sig
hash md5
group 2
!
crypto isakmp key CISCO address 136.1.123.12
!
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Create access-list to classify traffic for encryption
ip access-list extended VLAN23_TO_VLAN121
permit ip 136.1.23.0 0.0.0.255 136.1.121.0 0.0.0.255
!
! Create & apply crypto map
!
crypto map VPN 10 ipsec-isakmp
match address VLAN23_TO_VLAN121
set transform 3DES_MD5
set peer 136.1.123.12
1
interface Eth 0/0
 crypto map VPN
```

```
Enroll the ASA with CA:

ASA1(config)# crypto ca authenticate IE1

INFO: Certificate has the following attributes:

Fingerprint: 74f95e93 4f8c8af3 5fd15364 8efbb479

Do you accept this certificate? [yes/no]: yes
```

Copyright © 2007 Internetwork Expert

```
Trustpoint CA certificate accepted.
ASA1(config)# crypto key generate rsa general-keys modulus 512
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 ...
ASA1(config)# crypto ca enroll IE1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
Password: cisco
Re-enter password: cisco
% The fully-qualified domain name in the certificate will be:
ASA1.internetworkexpert.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ASA1(config) # The certificate has been granted by CA!
ASA1(config) # show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 2358cad200010000026
  Certificate Usage: General Purpose
  Public Key Type: RSA (512 bits)
  Issuer Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
  Subject Name:
    hostname=ASA1.internetworkexpert.com
  CRL Distribution Points:
    [1] http://ieserver1/CertEnroll/IESERVER1(1).crl
    [2] file://\\IESERVER1\CertEnroll\IESERVER1(1).crl
  Validity Date:
    start date: 10:07:47 UTC Jan 12 2007
    end date: 10:17:47 UTC Jan 12 2008
  Associated Trustpoints: IE1
CA Certificate
  Status: Available
  Certificate Serial Number: 6a8b964c37f91bb245b01de2a6363745
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
```

```
Copyright © 2007 Internetwork Expert
```

```
Subject Name:
    cn=IESERVER1
    o=Internetwork Expert
    l=Reno
    st=NV
    c=US
    ea=bmcgahan@internetworkexpert.com
  CRL Distribution Points:
    [1] http://ieserver1/CertEnroll/IESERVER1(1).crl
    [2] file://\\IESERVER1\CertEnroll\IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1
Enroll R3 with CA:
R3(config)#crypto ca authenticate IE1
Certificate has the following attributes:
Fingerprint: 74F95E93 4F8C8AF3 5FD15364 8EFBB479
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
R3(config)#crypto ca enroll IE1
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco
% The fully-qualified domain name in the certificate will be:
R3.internetworkexpert.com
% The subject name in the certificate will be: R3.internetworkexpert.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
R3(config)#
               Fingerprint: 4913AF72 E8D4DEC9 01526382 C936CF4D
Jan 12 11:07:54.762: %CRYPTO-6-CERTRET: Certificate received from Certificate
Authority
R3#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 23869E24000100000027
  Certificate Usage: General Purpose
  Issuer:
    CN = IESERVER1
    0 = Internetwork Expert
    L = Reno
     ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R3.internetworkexpert.com
```

```
OID.1.2.840.113549.1.9.2 = R3.internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 10:57:52 UTC Jan 12 2007
    end date: 11:07:52 UTC Jan 12 2008
   renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1
CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
     0 = Internetwork Expert
     L = Reno
    ST = NV
     C = US
     EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
     0 = Internetwork Expert
    L = Reno
     ST = NV
     C = US
    EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
   http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1
R2#ping 136.1.121.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 12/30/48 ms
R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                                      I-VRF Encr Hash Auth DH Lifetime Cap.
                      Remote
     136.1.123.3
                     136.1.123.12
                                               3des md5 rsig 2 23:58:57
1
R3#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.123.3
   protected vrf:
   local ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
```

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 2, #recv errors 0
local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
path mtu 1500, media mtu 1500
current outbound spi: 4A807DEA
 inbound esp sas:
 spi: 0xED9B3EDE(3986374366)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4403363/3534)
   IV size: 8 bytes
   replay detection support: Y
 inbound ah sas:
 inbound pcp sas:
outbound esp sas:
 spi: 0x4A807DEA(1249934826)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4403363/3534)
   IV size: 8 bytes
   replay detection support: Y
 outbound ah sas:
 outbound pcp sas:
```

Further Reading

Configuring LAN-to-LAN IPSec VPNs Configuring Certificates

IOS and the PIX/ASA: Matching Name in Certificate

Objective: Match remote L2L endpoint by hostname in certificate on the PIX/ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and the PIX/ASA with Digital Certificates"</u>
- Clear existing tunnel group "136.1.123.3".
- Create new tunnel-group as follows:
 - o Base group-name on FQDN: "R3.internetworkexpert.com".
 - Use trustpoint IE1 for this group.
- Configure ASA1 and R3 to use hostname as identity.

Final Configuration

```
ASA1:

crypto isakmp identity hostname

clear configure tunnel-group

!

tunnel-group R3.internetworkexpert.com type ipsec-121

tunnel-group R3.internetworkexpert.com ipsec-attributes

trust-point IE1

R3:

crypto isakmp identity hostname
```

```
Snip from ASA debug output:
ASA1# debug crypto isakmp 9
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing ID payload
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing cert payload
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing RSA signature
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, Computing hash for ISAKMP
Jan 12 13:09:17 [IKEv1 DEBUG]: IP = 136.1.123.3, processing notify payload
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Trying to find group via OU...
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, No Group found by matching OU(s)
from ID pavload:
                  Unknown
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Trying to find group via IKE ID...
Jan 12 13:09:17 [IKEv1]: IP = 136.1.123.3, Connection landed on tunnel_group
R3.internetworkexpert.com
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, peer ID type 2 received (FQDN)
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing ID payload
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing cert payload
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, constructing RSA signature
Jan 12 13:09:17 [IKEv1 DEBUG]: Group = R3.internetworkexpert.com, IP =
136.1.123.3, Computing hash for ISAKMP
R3#ping 136.1.121.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.121.1, timeout is 2 seconds:
Packet sent with a source address of 136.1.23.3
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                      Remote
                                    I-VRF Encr Hash Auth DH Lifetime Cap.
      136.1.123.3
                     136.1.123.12
                                               3des md5 rsig 2 23:52:24
R3#show crypto ipsec sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.123.3
   protected vrf:
   local ident (addr/mask/prot/port): (136.1.23.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 12, #recv errors 0
```

```
Copyright © 2007 Internetwork Expert
```

```
local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
path mtu 1500, media mtu 1500
current outbound spi: A45F614E
inbound esp sas:
 spi: 0xF77C2C21(4152110113)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4546831/3141)
   IV size: 8 bytes
   replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
 spi: 0xA45F614E(2757714254)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4546831/3141)
   IV size: 8 bytes
   replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

Configuring LAN-to-LAN IPSec VPNs Configuring Certificates

IOS and IOS with PSK Across the PIX/ASA

Objective: Configure IPsec tunnel across the PIX/ASA firewall between two IOS routers with PSK authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "<u>Common Configuration</u>".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure access-control on the ASA.
- Create and apply to the outside interface access-list OUTSIDE_IN as follows:
 - Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create ISAKMP key CISCO for address 136.X.122.2 (R2).
 - Create transform-set 3DES_MD5 as follows:
- Use 3DES for cipher.
- Use MD5 for hash.
- Create access-list LO1_TO_LO2 as follows:
 - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
- o Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2.
 - Set transform-set 3DES_MD5.
- Apply crypto-map VPN to interface E0/0.
- Configure R2 to mirror R1's configuration.

Final Configuration

```
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
1
router rip
network 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
router rip
network 150.1.0.0
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
1
access-group OUTSIDE_IN in interface outside
R1:
!
! Configure ISAKMP policy & PSK
crypto isakmp policy 10
authentication pre-share
hash md5
encryption 3des
crypto isakmp key CISCO address 136.1.122.2
!
! Create transform set
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
! Access-List to classify VPN traffic
```

Copyright © 2007 Internetwork Expert

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
ip access-list extended LO1_TO_LO2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
Т
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
match address LO1_TO_LO2
set transform 3DES_MD5
set peer 136.1.122.2
!
interface E 0/0
crypto map VPN
R2:
crypto isakmp policy 10
authentication pre-share
hash md5
encryption 3des
!
crypto isakmp key CISCO address 136.1.121.1
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
ip access-list extended LO2_TO_LO1
 permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
match address LO2_TO_LO1
set transform 3DES_MD5
set peer 136.1.121.1
!
interface E 0/0
crypto map VPN
```

Verification

```
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
. . . ! !
Success rate is 40 percent (2/5), round-trip min/avg/max = 8/10/12 ms
R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                                    I-VRF
                                               Encr Hash Auth DH Lifetime Cap.
                     Remote
     136.1.122.2
                                               3des md5 psk 1 23:59:27
1
                    136.1.121.1
R2#show crypto ipsec sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
  local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 13, #recv errors 0
     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
    current outbound spi: 566119F8
     inbound esp sas:
      spi: 0xE069002C(3764977708)
       transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4517902/3508)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x566119F8(1449204216)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4517902/3508)
        IV size: 8 bytes
```

Copyright © 2007 Internetwork Expert

```
replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
      K - Keepalives, N - NAT-traversal
      X - IKE Extended Authentication
      psk - Preshared key, rsig - RSA signature
      renc - RSA encryption
                                   I-VRF Encr Hash Auth DH Lifetime Cap.
C-id Local
                     Remote
                    136.1.122.2
     136.1.121.1
                                               3des md5 psk 1 23:57:54
1
R1#show cry ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.121.1
  protected vrf:
  local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2
    #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.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: E069002C
     inbound esp sas:
      spi: 0x566119F8(1449204216)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4402011/3469)
       IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xE069002C(3764977708)
       transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4402011/3469)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
```

Copyright © 2007 Internetwork Expert

Further Reading

Configuring IPSec Network Security Configuring Internet Key Exchange Security Protocol

IOS and IOS with PSK Across the PIX/ASA and NAT

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall with NAT setup.Use PSK for authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "<u>Common Configuration</u>".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure NAT on the PIX/ASA firewall as follows:
 - Translate inside networks as they go outside using the outside interface IP address.
 - Enable NAT-Control on the firewall.
- Configure access-control on the ASA as follows:
 - Create and apply to the outside interface access-list OUTSIDE_IN:
 - Permit ISAKMP traffic from outside.
 - Permit NAT-T traffic from outside (UDP 4500).
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.

- Use MD5 for hash.
- Create ISAKMP key CISCO for address 136.X.122.2 (R2).
- Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
- Create access-list LO1_TO_LO2 as follows:
 - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2.
 - Set transform-set 3DES_MD5.
- Configure IPsec L2L tunnel on R2 as follows:
 - Configure ISAKMP just like you did on R1.
 - However, configure wildcard pre-shared ISAKMP key "CISCO" for address 0.0.0.0 0.0.0.0.
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create dynamic crypto-map DYNAMIC entry 10 as follows:
 - Set transform-set 3DES_MD5.
 - Create crypto-map VPN entry 10 of type IPsec-ISAKMP and attach dynamic crypt-map DYNAMIC to it.
 - Apply crypto-map VPN to interface Ethernet 0/0.

Final Configuration

```
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
network 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
```

Copyright © 2007 Internetwork Expert

```
router rip
network 150.1.0.0
ASA1:
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit udp any any eq 4500
!
access-group OUTSIDE_IN in interface outside
! NAT Configuration
!
nat-control
nat (inside) 1 0 0
global (outside) 1 interface
R1:
!
! Configure ISAKMP policy & PSK
1
crypto isakmp policy 10
authentication pre-share
hash md5
encryption 3des
T
crypto isakmp key CISCO address 136.1.122.2
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
1
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
match address LO1_TO_LO2
set transform 3DES_MD5
set peer 136.1.122.2
1
interface E 0/0
crypto map VPN
R2:
crypto isakmp policy 10
authentication pre-share
hash md5
encryption 3des
!
! Wildcard pre-shared key
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
! Dynamic map
1
crypto dynamic-map DYNAMIC 10
set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
```

Copyright © 2007 Internetwork Expert

interface E 0/0 crypto map VPN

Verification

```
R1#ping 150.1.2.2 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms
R1#show cry isa sa
                                               conn-id slot
dst
                                state
                src
                136.1.121.1
136.1.122.2
                                QM_IDLE
                                                     1
                                                           Ω
R1#show cry ips sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.121.1
   protected vrf:
   local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.122.2:4500
     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 6, #recv errors 0
     local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2
     path mtu 1500, media mtu 1500
     current outbound spi: 652A3F6F
     inbound esp sas:
      spi: 0xE6BFA8E(241957518)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4585150/3572)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x652A3F6F(1697267567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4585150/3572)
        IV size: 8 bytes
```

Copyright © 2007 Internetwork Expert

```
replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R2#sho cry isa sa
dst.
                                state
                                             conn-id slot
                src
                                QM_IDLE
               136.1.122.12
                                                 1 0
136.1.122.2
R2#show cry ips sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
   local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.122.12:1027
     PERMIT, flags={}
    #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 0, #recv errors 0
     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.122.12
     path mtu 1500, media mtu 1500
     current outbound spi: E6BFA8E
     inbound esp sas:
     spi: 0x652A3F6F(1697267567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4520954/3533)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xE6BFA8E(241957518)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
       slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4520954/3533)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
ASA1(config)# show x
2 in use, 10 most used
PAT Global 136.1.122.12(1027) Local 136.1.121.1(4500)
PAT Global 136.1.122.12(1) Local 136.1.121.1(500)
ASA1(config)# show conn
```

Copyright © 2007 Internetwork Expert

7 in use, 209 most used UDP out 136.1.122.2:4500 in 136.1.121.1:4500 idle 0:00:58 flags -UDP out 136.1.122.2:500 in 136.1.121.1:500 idle 0:01:14 flags -

Further Reading

Configuring IPSec Network Security Configuring Internet Key Exchange Security Protocol

IOS and IOS with PSK Across the PIX/ASA with Overlapping Subnets

Objective: Configure IPsec tunnel across the PIX/ASA firewall between two IOS routers with PSK authentication. Handle the overlapping subnets issue.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, however do not advertise them into RIP.
- To handle the overlapping subnets issue a NAT configuration should be implemented.
- Configure access-control on the ASA.
- Create and apply to the outside interface access-list OUTSIDE_IN as follows:
 - o Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
- Configure NAT on R1 as follows:
 - Configure Lo1 as inside and E0/0 as outside interface.
 - Configure static network NAT for 12.12.12.0/24 to 10.10.10.0/24.
- Configure NAT on R2 as follows:
 - Configure Lo1 as inside and E0/0 as outside interface.

CCIE Security Lab Workbook Volume I Version 3.0

- Configure static network NAT for 12.12.12.0/24 to 20.20.20.0/24.
- Configure static routes on R1 and R2 for 20.20.20.0/24 and 10.10.10.0/24 respectively to point at the ASA.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create ISAKMP key CISCO for address 136.X.122.2 (R2).
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create access-list LO1_TO_LO2 as follows:
 - Permit IP traffic from 10.10.10.0/24 to 20.20.20.0/24.
 - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2.
 - Set transform-set 3DES_MD5.
- Configure R2 to mirror R1's configuration.

Final Configuration

```
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside
R1:
!
! NAT Configuration
!
interface Loopback1
ip address 12.12.12.1 255.255.255.0
ip nat inside
!
interface E 0/0
ip nat outside
!
ip nat inside source static network 12.12.12.0 10.10.10.0 /24
```

! Static route to peer's post-NAT network ip route 20.20.20.0 255.255.255.0 136.1.121.12 1 ! Configure ISAKMP policy & PSK ! crypto isakmp policy 10 authentication pre-share hash md5 encryption 3des ! crypto isakmp key CISCO address 136.1.122.2 ! Create transform set ! crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac ! ! Access-List to classify VPN traffic ! ip access-list extended LO1_TO_LO2 permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255 1 ! Create and apply crypto-map 1 crypto map VPN 10 ipsec-isakmp match address LO1_TO_LO2 set transform 3DES MD5 set peer 136.1.122.2 ! interface E 0/0 crypto map VPN R2: 1 ! NAT Configuration 1 interface Loopback1 ip address 12.12.12.2 255.255.255.0 ip nat inside 1 interface E 0/0 ip nat outside ip nat inside source static network 12.12.12.0 20.20.20.0 /24 ! ! Static route to peer's post-NAT network ip route 10.10.10.0 255.255.255.0 136.1.122.12 ! crypto isakmp policy 10 authentication pre-share hash md5 encryption 3des ! crypto isakmp key CISCO address 136.1.121.1 crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac ip access-list extended LO2_TO_LO1 permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255 1 crypto map VPN 10 ipsec-isakmp match address LO2_TO_LO1

Copyright © 2007 Internetwork Expert

set transform 3DES_MD5
set peer 136.1.121.1
!
interface E 0/0
crypto map VPN

Verification

```
R2#ping 10.10.10.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 12.12.12.2
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms
R2#show crypto isakmp sa
dst
                                state
                                              conn-id slot
                src
136.1.121.1
                136.1.122.2
                                QM_IDLE
                                                  1
                                                          0
R2#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
   local ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer: 136.1.121.1:500
    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.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: FE66CA03
     inbound esp sas:
      spi: 0x6BD89D6B(1809358187)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4554053/3567)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     spi: 0xFE66CA03(4268149251)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4554053/3567)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
```

Copyright © 2007 Internetwork Expert

R2#**show ip nat tra** Pro Inside global Inside local Outside local Outside global --- 20.20.20.2 12.12.12.2 _ _ _ _ _ _ Subnet translation: Inside global Inside local Outside local Outside global /prefix /24 20.20.20.0 12.12.12.0 ---_ _ _ _ R1#**sh ip nat tra** Pro Inside global Inside local Outside local Outside global --- 10.10.10.1 12.12.12.1 ____ ___ Subnet translation: Inside global Inside local Outside local Outside global /prefix 10.10.10.0 12.12.12.0 _ _ _ _ _ _ _ /24 R1#show cry ips sa interface: Ethernet0/0 Crypto map tag: VPN, local addr. 136.1.121.1 protected vrf: local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0) current_peer: 136.1.122.2:500 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 0, #recv errors 0 local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2 path mtu 1500, media mtu 1500 current outbound spi: 6BD89D6B inbound esp sas: spi: 0xFE66CA03(4268149251) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4466441/3540) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x6BD89D6B(1809358187) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4466441/3540) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

Copyright © 2007 Internetwork Expert

Gamma Further Reading

Configuring IPSec Network Security Configuring Internet Key Exchange Security Protocol Cisco - NAT Order of Operation Configuring Network Address Translation: Getting Started

IOS and IOS with PSK Across the PIX/ASA and NAT with IKE AM

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall with NAT setup.Use PSK for authentication and hostname for IKE identity.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- The main advantage of IKE Agressive Mode (IKE AM) with PSK is that identity is present at IKE initiation phase, allowing for flexible policy lookup.
- In this lab the hostname will be used as router's identity, to avoid configuring the wildcard pre-shared key on the "hub" site (R2).
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure domain-name "internetworkexpert.com" on R1 and R2, as well as hostnames R1 and R2.
- Configure NAT on the PIX/ASA firewall as follows:
 - Translate inside networks as they go outside using the outside interface IP address.
 - Enable NAT-Control on the firewall.
- Configure access-control on the ASA as follows:
 - Create and apply to the outside interface access-list OUTSIDE_IN:

- Permit ISAKMP traffic from outside.
- Permit NAT-T traffic from outside (UDP 4500).
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
 - Configure ISAKMP profile AGGRESSIVE as follows:
 - Initiate IKE aggressive mode.
 - Use FQDN as self-identity.
 - Use global keyring.
 - Configure host entry for host "R2.internetworkexpert.com" to IP 136.1.122.2. This way you attach a "peer IP" in crypto map to it's hostname for key lookup.
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create ISAKMP key CISCO for host "R2.internetworkexpert.com".
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create access-list LO1_TO_LO2 as follows:
 - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
 - Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2
 - Set transform-set 3DES_MD5.
- Configure IPsec L2L tunnel on R2 as follows:
 - Configure ISAKMP just like you did on R1.
 - o Configure ISAKMP identity "hostname".
 - However, configure pre-shared ISAKMP key "CISCO" for hostname "R1.internetworkexpert.com".
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.

- Use MD5 for hash.
- Create dynamic crypto-map DYNAMIC enry 10 as follows:
 - Set transform-set 3DES_MD5.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP and attach dynamic crypto-map DYNAMIC to it.
- Apply crypto-map VPN to interface Ethernet 0/0.

Final Configuration

```
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
network 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.255.0
1
router rip
network 150.1.0.0
ASA1 .
access-list OUTSIDE_IN permit udp any any eq 500
access-list OUTSIDE_IN permit udp any any eq 4500
!
access-group OUTSIDE_IN in interface outside
!
! NAT Configuration
!
nat-control
nat (inside) 1 0 0
global (outside) 1 interface
R1:
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
 authentication pre-share
hash md5
encryption 3des
!
! ISAKMP profile
1
crypto isakmp profile AGGRESSIVE
initiate mode aggressive
 self-identity fqdn
keyring default
!
! Domain-name & host mapping
!
hostname R1
ip domain-name internetworkexpert.com
```

```
ip host R2.internetworkexpert.com 136.1.122.2
!
! Hostname pre-shared key
!
crypto isakmp key CISCO host R2.internetworkexpert.com
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Access-List to classify VPN traffic
1
ip access-list extended LO1_TO_LO2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create and apply crypto-map
! Apply ISAKMP profile to crypto map
!
crypto map VPN isakmp-profile AGGRESSIVE
crypto map VPN 10 ipsec-isakmp
match address LO1_TO_LO2
set transform 3DES_MD5
set peer 136.1.122.2
1
interface E 0/0
crypto map VPN
R2:
crypto isakmp policy 10
authentication pre-share
hash md5
encryption 3des
!
crypto isakmp identity hostname
1
! Host pre-shared key
!
hostname R2
ip domain-name internetworkexpert.com
crypto isakmp key CISCO host R1.internetworkexpert.com
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Dynamic map
1
crypto dynamic-map DYNAMIC 10
set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
interface E 0/0
crypto map VPN
```

Verification

```
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#ping 150.1.2.2 source 100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
R1#
ISAKMP: received ke message (1/1)
ISAKMP (0:0): SA request profile is AGGRESSIVE
ISAKMP: local port 500, remote port 500
<code>ISAKMP: set new node 0 to QM_IDLE</code>
ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 8256C708
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3): constructed NAT-T vendor-03 ID
ISAKMP (0:3): constructed NAT-T vendor-02 ID
ISAKMP (0:3): SA is doing pre-shared key authentication using id type ID_FQDN
ISAKMP (3): ID payload
        next-payload : 13
        type
                     : 2
        FQDN name : R1.internetworkexpert.com
        protocol : 17
        port
                     : 0
                     : 29
        length
ISAKMP (3): Total payload length: 33
ISAKMP (0:3): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM
ISAKMP (0:3): Old State = IKE_READY New State = IKE_I_AM1
ISAKMP (0:3): beginning Aggressive Mode exchange
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 500 peer_port 500 (I)
AG_INIT_EXCH
ISAKMP (0:3): received packet from 136.1.122.2 dport 500 sport 500 Global (I)
AG_INIT_EXCH
ISAKMP (0:3): processing SA payload. message ID = 0
ISAKMP (0:3): processing ID payload. message ID = 0
ISAKMP (3): Process ID payload
                     : 2
        type
        FQDN name : R2.internetworkexpert.com
                   : 17
        protocol
                     : 0
        port
        length
                     : 25
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): vendor ID is Unity
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): vendor ID is DPD
ISAKMP (0:3): processing vendor id payload
ISAKMP (0:3): speaking to another IOS box!
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3) local preshared key found
ISAKMP : Scanning profiles for xauth ... AGGRESSIVE
ISAKMP (0:3): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:
             encryption 3DES-CBC
ISAKMP:
             hash MD5
ISAKMP:
             default group 1
ISAKMP:
             auth pre-share
ISAKMP:
             life type in seconds
```

```
Copyright © 2007 Internetwork Expert
```

```
life duration (VPI) of 0x0 0x1 0x51 0x80
TSAKMP:
ISAKMP (0:3): atts are acceptable. Next payload is 0
ISAKMP (0:3): vendor ID is NAT-T v3
ISAKMP (0:3): processing KE payload. message ID = 0
ISAKMP (0:3): processing NONCE payload. message ID = 0
ISAKMP (0:3): Found HOST key in keyring default
ISAKMP (0:3): SKEYID state generated
ISAKMP (0:3): processing HASH payload. message ID = 0
ISAKMP: received payload type 17
ISAKMP (0:3): Detected NAT-D payload
ISAKMP (0:3): NAT does not match MINE hash
hash received: 76 26 A8 59 D9 6E F6 8 20 A7 A9 25 2E 60 5A 89
my nat hash \phantom{.} : E C6 37 A2 9A BB 13 5D F1 C5 96 3 31 E6 12 B4
ISAKMP: received payload type 17
ISAKMP (0:3): Detected NAT-D payload
\tt ISAKMP (0:3): <code>NAT</code> match <code>HIS</code> hash
ISAKMP (0:3): SA has been authenticated with 136.1.122.2
ISAKMP: Locking peer struct 0x82E737F0, IKE refcount 2 for from
crypto_ikmp_udp_enc_ike_init
ISAKMP (0:3): Setting UDP ENC peer struct 0x82E73A58 sa= 0x8256C708
ISAKMP (0:3): Send initial contact
ISAKMP (0:3): constructed HIS NAT-D
ISAKMP (0:3): recalc his hash for NAT-D
ISAKMP (0:3): constructed MINE NAT-D
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I)
AG_INIT_EXCH
ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
ISAKMP (0:3): Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE
ISAKMP: sending nat keepalive packet to 136.1.122.2(4500)
ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -785375327
ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I)
OM IDLE
ISAKMP (0:3): Node -785375327, Input = IKE_MESG_INTERNAL, IKE_INIT_QM
ISAKMP (0:3): Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP (0:3): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
ISAKMP (0:3): received packet from 136.1.122.2 dport 4500 sport 4500 Global (I)
QM_IDLE
ISAKMP (0:3): processing HASH payload. message ID = -785375327
ISAKMP (0:3): processing SA payload. message ID = -785375327
ISAKMP (0:3): Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
           encaps is 61443
TSAKMP:
ISAKMP:
             SA life type in seconds
            SA life duration (basic) of 3600
ISAKMP:
ISAKMP:
           SA life type in kilobytes
ISAKMP:
           SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:
            authenticator is HMAC-MD5
ISAKMP (0:3): atts are acceptable.
ISAKMP (0:3): processing NONCE payload. message ID = -785375327
ISAKMP (0:3): processing ID payload. message ID = -785375327
ISAKMP (0:3): processing ID payload. message ID = -785375327
ISAKMP: Locking peer struct 0x82E737F0, IPSEC refcount 1 for for stuff_ke
ISAKMP (0:3): Creating IPSec SAs
        inbound SA from 136.1.122.2 to 136.1.121.1 (f/i) 0/ 0
        (proxy 150.1.2.0 to 150.1.1.0)
        has spi 0x2127CD37 and conn_id 2000 and flags 400
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        has client flags 0x10
```

```
Copyright © 2007 Internetwork Expert
```

outbound SA from 136.1.121.1 (f/i) 0/ 0 (proxy to 136.1.122.2 150.1.1.0 to 150.1.2.0) has spi -847945563 and conn_id 2001 and flags 408lifetime of 3600 seconds lifetime of 4608000 kilobytes has client flags 0x10 ISAKMP (0:3): sending packet to 136.1.122.2 my_port 4500 peer_port 4500 (I) QM_IDLE ISAKMP (0:3): deleting node -785375327 error FALSE reason "" ISAKMP (0:3): Node -785375327, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH ISAKMP (0:3): Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE R1#show crypto isakmp sa detail Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption C-id Local Remote I-VRF Encr Hash Auth DH Lifetime Cap. 136.1.121.1 136.1.122.2 3des md5 psk 1 23:57:42 N R1#show cry ipsec sa interface: Ethernet0/0 Crypto map tag: VPN, local addr. 136.1.121.1 protected vrf: local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0) current_peer: 136.1.122.2:4500 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.: 136.1.121.1, remote crypto endpt.: 136.1.122.2 path mtu 1500, media mtu 1500 current outbound spi: CD7560A5 inbound esp sas: spi: 0x2127CD37(556256567) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4458262/3456) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xCD7560A5(3447021733) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4458262/3456) IV size: 8 bytes

Copyright © 2007 Internetwork Expert

```
replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R2#show crypto isakmp sa
dst
                                             conn-id slot
                src
                                state
                               QM_IDLE
136.1.122.2
                136.1.122.12
                                                   3
                                                         0
R2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                                    I-VRF
                                               Encr Hash Auth DH Lifetime Cap.
                     Remote
     136.1.122.2
                    136.1.122.12
                                               3des md5 psk 1 23:56:43 N
3
R2#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
  local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.122.12:1027
     PERMIT, flags={}
    #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 0, #recv errors 0
     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.122.12
     path mtu 1500, media mtu 1500
    current outbound spi: 2127CD37
     inbound esp sas:
      spi: 0xCD7560A5(3447021733)
       transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4449442/3395)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x2127CD37(556256567)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4449442/3395)
        IV size: 8 bytes
        replay detection support: Y
```

```
Copyright © 2007 Internetwork Expert
```

outbound ah sas:

outbound pcp sas:

Further Reading

<u>Configuring IPSec Network Security</u> <u>Configuring Internet Key Exchange Security Protocol</u>

IOS and IOS with Digital Certificates Across the PIX/ASA

Objective: Configure IPsec tunnel between two IOS routers across the PIX/ASA firewall, with digital certificates based authentication.



Directions

- Configure devices as per the scenario "PIX/ASA Firewall/Access Control" "Common Configuration".
- Create two additional loopback interfaces on R1 and R2 as per the diagram, advertise them into RIP.
- Configure access-control on the ASA.
- Create access-list OUTSIDE IN as follows:
 - Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
 - Permit HTTP to 10.0.0.100.
 - Permit NTP to 10.0.0.100.
- Apply this access-group to the outside interface
- Configure R1, R2 and the ASA to synchronize time with the AAA/CA server via NTP.
- Configure IPsec LAN-to-LAN tunnel on R1 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use RSA-sig authentication.
 - Use 3DES for cipher.

- Use MD5 for hash.
- Enroll R1 with CA:
 - Configure domain-name "internetworkexpert.com"
 - Generate RSA key-pair.
 - Configure CA Trustpoint IE1 as follows:
 - Use enrollment URL: <u>http://10.0.0.100/certsrv/mscep/mscep.dll</u>
 - Use RA mode.
 - Set CRL as optional.
 - Authenticate the CA and Enroll.
- Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
- Create access-list LO1_TO_LO2 as follows:
 - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2.
 - Set transform-set 3DES_MD5.
- Configure R2 to mirror R1's configuration.

Final Configuration

```
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
network 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.0
!
router rip
network 150.1.0.0
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit tcp any host 10.0.0.100 eq 80
```

```
Copyright © 2007 Internetwork Expert
```

```
access-list OUTSIDE_IN permit udp any host 10.0.0.100 eq 123
access-list OUTSIDE_IN permit esp any any
!
access-group OUTSIDE_IN in interface outside
1
ntp server 10.0.0.100
R1:
ntp server 10.0.0.100
1
! Configure ISAKMP policy & PSK
1
crypto isakmp policy 10
authentication rsa-sig
hash md5
encryption 3des
!
crypto ca trustpoint IE1
enrollment url http://10.0.0.100/certsrv/mscep/mscep.dll
crl optional
enrollment mode ra
exit
1
! Generate RSA key, authenticate CA and enroll
1
ip domain-name internetworkexpert.com
hostname R1
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
!
! Create transform set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Access-List to classify VPN traffic
!
ip access-list extended LO1_TO_LO2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create and apply crypto-map
!
crypto map VPN 10 ipsec-isakmp
match address LO1_TO_LO2
set transform 3DES_MD5
set peer 136.1.122.2
1
interface E 0/0
crypto map VPN
R2:
ntp server 10.0.0.100
!
! Configure ISAKMP policy & PSK
crypto isakmp policy 10
authentication rsa-sig
hash md5
encryption 3des
!
crypto ca trustpoint IE1
enrollment url <a href="http://lo.0.0.100/certsrv/mscep/mscep.dll">http://lo.0.0.100/certsrv/mscep/mscep.dll</a>
```

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

```
crl optional
enrollment mode ra
exit
!
! Generate RSA key, authenticate CA and enroll
!
ip domain-name internetworkexpert.com
hostname R2
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
1
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
ip access-list extended LO2_TO_LO1
 permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
match address LO2_TO_LO1
set transform 3DES_MD5
set peer 136.1.121.1
1
interface E 0/0
 crypto map VPN
```

Verification

```
Enroll R1 and R2 with CA, check certificates:
R2(config)#do sho cry ca cert
Certificate
  Status: Available
  Certificate Serial Number: 32D2CA1D0001000002A
  Certificate Usage: General Purpose
  Issuer:
   CN = IESERVER1
    0 = Internetwork Expert
    L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R2.internetworkexpert.com
   OID.1.2.840.113549.1.9.2 = R2.internetworkexpert.com
  CRL Distribution Point:
   http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
   start date: 10:16:14 UTC Jan 15 2007
    end date: 10:26:14 UTC Jan 15 2008
   renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1
CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
    0 = Internetwork Expert
```

Copyright © 2007 Internetwork Expert

```
L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
    0 = Internetwork Expert
    L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
    http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
    start date: 09:01:58 UTC Jul 21 2006
    end date: 09:09:34 UTC Jul 21 2008
  Associated Trustpoints: IE1
R1(config)#do sh cry ca cert
Certificate
  Status: Available
  Certificate Serial Number: 32CEEFC600010000028
  Certificate Usage: General Purpose
  Issuer:
   CN = IESERVER1
     0 = Internetwork Expert
    L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  Subject:
    Name: R1.internetworkexpert.com
    OID.1.2.840.113549.1.9.2 = R1.internetworkexpert.com
  CRL Distribution Point:
   http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
   start date: 10:12:01 UTC Jan 15 2007
    end date: 10:22:01 UTC Jan 15 2008
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: IE1
CA Certificate
  Status: Available
  Certificate Serial Number: 6A8B964C37F91BB245B01DE2A6363745
  Certificate Usage: Signature
  Issuer:
    CN = IESERVER1
    0 = Internetwork Expert
    L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  Subject:
    CN = IESERVER1
    0 = Internetwork Expert
     L = Reno
    ST = NV
    C = US
    EA = bmcgahan@internetworkexpert.com
  CRL Distribution Point:
   http://ieserver1/CertEnroll/IESERVER1(1).crl
  Validity Date:
   start date: 09:01:58 UTC Jul 21 2006
```

```
Copyright © 2007 Internetwork Expert
```

date: 09:09:34 UTC Jul 21 2008 end Associated Trustpoints: IE1 R2#ping 150.1.1.1 source loopback 0 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds: Packet sent with a source address of 150.1.2.2 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms R2#**show cry isa sa det** Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption I-VRF Encr Hash Auth DH Lifetime Cap. C-id Local Remote 1 136.1.122.2 136.1.121.1 3des md5 rsig 1 23:59:29 R2#show cry ips sa interface: Ethernet0/0 Crypto map tag: VPN, local addr. 136.1.122.2 protected vrf: local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0) current_peer: 136.1.121.1:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7 #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7 #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 3, #recv errors 0 local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.1 path mtu 1500, media mtu 1500 current outbound spi: 24ADFE7A inbound esp sas: spi: 0x8ADF82D(145618989) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4480341/3568) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x24ADFE7A(615382650) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4480341/3568) IV size: 8 bytes replay detection support: Y

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 101 -

outbound ah sas:

outbound pcp sas:

Further Reading

<u>Configuring IPSec Network Security</u> <u>Configuring Internet Key Exchange Security Protocol</u> <u>Configuring Certification Authority Interoperability</u>

IOS and VPN3k with PSK

Objective: Configure L2L IPsec tunnel between IOS router and VPN3k across the PIX/ASA Firewall. Use pre-shared keys for authentication.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"IOS Router and VPN3k"</u>.
- Configure access-control on the ASA. Add rules to the access-list OUTSIDE_IN as follows:
 - Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R2 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Use DH Group 2.
 - Create ISAKMP key CISCO for address 136.X.121.11 (VPN3k).
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Create access-list LO2_TO_LO1 as follows:

- Permit IP traffic from 150.X.2.0/24 to 150.X.1.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO2_TO_LO1.
 - Set peer 136.X.121.11.
 - Set transform-set 3DES_MD5.
- Apply crypto-map VPN to interface E0/0.
- Configure IPsec LAN-to-LAN tunnel on VPN3k as follows:
 - o Use L2L tunnel wizard to complete to configuration steps.

Final Configuration

```
R2:
crypto isakmp policy 10
authentication pre-share
hash md5
group 2
 encryption 3des
!
crypto isakmp key CISCO address 136.1.121.11
1
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
ip access-list extended LO2_TO_LO1
 permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
crypto map VPN 10 ipsec-isakmp
match address LO2_TO_LO1
 set transform 3DES_MD5
set peer 136.1.121.11
interface E 0/0
 crypto map VPN
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
```

VPN3k:

Add new L2L Tunnel: Add peer IP address.
🖉 Cisco Systems, Inc. VPN 3000 Co	oncentrator	[VPN3K] - Microsoft I	Internet Exp	lorer		_ 🗆 ×
<u>File Edit View Favorites Tool</u>	s <u>H</u> elp	⇔Back • ⇒ • 💌) 🕑 🛛 Ag	dress 🦉 h	ttps://136.1.121.11/access.html	-
VPN.	3000				Main Help St	ipport 💽 Logout
Conce	entrator	Series Mana	ger		L	ogged in: admin
				-	Configuration Administra	tion Monitoring
- Configuration	0.0		10			
	Configu	ration Lunneling :	and Secur	ty IPSec	LAN-to-LAN	In Needed
					29/	re needed
Delicy Management	This sect	tion lets you configu	re IPSec I	AN-to-L	AN connections LAN-to-LA	N
E-Tunneling and Security pro	connecti	ons are established	with other	VPN 300	0 Concentrators, PIX firewalls	s, 7100/4000
L2TP	series ro	uters and other IPS	ec-complia	nt security	y gateways. To configure a VP	'N 3002 or
	other rer	note access connec	tion, go to	User Man	<u>agement</u> and configure a Grou	ıp and User.
LAN-to-LAN	To config	gure NAT over LAI	N-to-LAN	, go to \underline{LA}	<u>AN-to-LAN NAT Rules.</u>	
NAT Transparency	200 1 4			T 43T		
Alorta	Click the	e Add button to add	1 a LAN-to	-LAN cot	nnection, or select a connectio	n and click
	INTOMIY	of Delete.				
	(D) indic	ates a disabled LAI	N-to-LAN	connectic	on.	
- <u> - H</u> <u> Administration</u>						
H±H <u>Monitoring</u>			LAN-te	-LAN		
			Conne	ction	Actions	
		F	Empt	у		
					Add	
		I				
2012/2012/11					Modify	
Cisco Systems					Delete	
and how all how a						
I IPSec LAN-to-LAN		I			A linte	ernet



Set pre-shared key:



Designate protected networks:



VPN 3000 Main Help Support L Concentrator Series Manager Logged in: Configuration Administration Mon Positions to match. For example, Distribution Mon Wildcard Mask 0.0.0.255 example, Distribution Mon Mon Post Main Help Support Iteration Wildcard Mask 0.0.0.255 example, Distribution Main addresses Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address list or the IP address Material Network List Use IP Address/Wildcard-mask below Note: Enter a wildcard mask for this LAN-to-LAN connection. Monitoring IP Address [150.1.2.0 Note: Enter a wildcard mask, A wildcard mask has Is in bit positions to ignore, 0 in bit positions to ignore, 0 in bit positions to ignore, 0 in bit positions to match. For example, 10.10.1.000.0.0.255 = all 10.	Elisco Systems, Inc. VPN 5000 Co File Edit View Favorites Tool:	$\frac{\text{Help}}{\text{Help}} \Leftrightarrow \text{Back} \star \Rightarrow \star \bigotimes \bigotimes$	Address Address Address	21.11/access.html	
Concentrator Series Manager Logged in: Configuration Administration Mont POStatem positions to match. For example, 10.10.1.000.0.255 example, PUSer Management 10.10.1.000.0.255 example, 10.10.1.000.0.255 = all PUSer Management 10.10.1.000.0.255 example, 10.10.1.000.0.255 = all PUSer Management 10.10.1.000.0.255 example, 10.10.1.000.0.255 = all PUSer Management Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address. Specify the remote network Wildcard Mask Use IP Address/Wildcard-mask below Specify the remote network Add State Specify the remote network BAdministration IP Address 150.1.2.0 Note: Enter a wildcard mask, which is the reverse of a subnet mask. A Wildcard Mask 0.00.255 example, 10.10.1.00.0.0.255 = all 10.10.1.00.0.0.255 = all 10.10.1.00.0.0.255 = all 10.10.1.0.00.0.0.255 = all 10.10.1.0.00.0.	VPN ?	3000		Main Help Support	Logout
Configuration Administration Monit Interfaces positions to match. For example, positions to match. For example, Interfaces 10.10.1.0/0.0.0.255 = all Interfaces Specify the remote Network Interfaces Specify the remote network address Isto Specify	Nonce	ntrator Series Manager		Logged in	n: admir
Configuration positions to match. For example, Description 10.10.1.0/0.0.0.255 Best Management 10.10.1.0/0.0.0.255 = all Defice Management Specify the remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address. Specify the remote network address. Network List Use IP Address/Wildcard-mask below address list or the IP address address 150.1.2.0 Note: Enter a wildcard mask. A Wildcard Mask 0.0.0.255 os in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.0.0/0.0.0.255 = all 10.10.1.0.0/0.0.0.255 = all 10.10.1.0.0/0.0.0.255 = all 10.10.			Configura	ation Administration Mo	nitoring
Cisco Systems Add Cisco Systems Add Add Cancel Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address is to the IP address address list or the IP address and wildcard mask below Specify the remote network address is to the IP address and wildcard mask below Specify the remote network address is to the IP address and wildcard mask for this LAN-to-LAN connection. 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 10.10.1.0.1.0.1.0.1.0.1.0.1.0.1.0.1.0.1	Configuration Interfaces System System User Management Holicy Management	Wildcard Mask 0.0.0.255		positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	
LAN-to-LAN LAN-to-LAN Specify the remote network address list or the IP addres and wildcard mask for this LAN-to-LAN connection. SSH SSH SSH Network List Use IP Address/Wildcard-mask below IP address and wildcard mask for this LAN-to-LAN connection. B-Administration IP Address 150.1.2.0 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 ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.0/0.0.0.255 = all 10.10.1.0/0.0.0.0.255 = all 10.10.1.0/0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.		Remote Network : If a LAN-to- address.	LAN NAT rule is used, thi	is is the Remote Network	_
CISCO SYSTERS Add Cancel	LAN-to-LAN KE Proposals NAT Transparency Alorts SSH	Network List Use IP Addres	s/Wildcard-mask below 💌	Specify the remote networ address list or the IP addr and wildcard mask for this LAN-to-LAN connection	rk ress s 1.
CISCO SYSTEMS Add Cancel Cancel 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.		IP Address 150.1.2.0		Note: Enter a <i>wildcard</i> mask, which is the reve of a subnet mask. A wildcard mask has 1s in b	rse >it
CISCO SYSTEMS Add Cancel		Wildcard Mask 0.0.0.255		positions to ignore, 0s in b positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	vit [
antilita antilita -	CISCO SYSTEMS	Add Cancel			-



Verification

```
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/8 ms
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
C-id Local
                                    I-VRF
                                               Encr Hash Auth DH Lifetime Cap.
                     Remote
     136.1.122.2
                    136.1.121.11
                                               3des md5 psk 2 23:59:32
1
R2#show cry ipsec sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
  local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.11:500
     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 26, #recv errors 0
     local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
     path mtu 1500, media mtu 1500
    current outbound spi: 3EE679DF
     inbound esp sas:
      spi: 0xFE812159(4269875545)
       transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4474125/3567)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x3EE679DF(1055291871)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4474125/3567)
        IV size: 8 bytes
```

Copyright © 2007 Internetwork Expert

replay detection support: Y outbound ah sas: outbound pcp sas:

VPN3k:

Administration > Administer Session:

Cisco Systems, Inc. VPN 3000 Cond File Edit View Eavorites Tools	tentrator [VPN3K]	- Microsoft Int	ernet Explorer	i	6 1 121 11/	accase biml		
VPN 30	000 Dirator Serie	es Manag		121 https://13	M	ain Help	Suppo	rt Logout
Concern	drator serv	es manage	-1	Conf	iguration	Administi	ation	Monitoring
<u>Administration</u>	LAN-to-LA	N Sessions	[<u>Re</u> r	mote Access	Sessions	Managem	ent Sess	sions]
System Reboot Reboot Status	Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
	VPN TO R2	136.1.122.2 []]	PSec/LAN- to-LAN	3DES-168	Jan 15 21:25:30	0:01:50	416	416 [
	Remote Ac	cess Session	15 [<u>L</u> 2	AN-to-LAN	<u>Sessions</u>	<u>Managem</u>	ent Sess	sions]
	Username As Pu A	isigned IP ddress ublic IP ddress	Protocol Encryption	Login Time <u>Duration</u>	<u>Client</u> <u>Type</u> Version	Bytes N. Tx Re Bytes Pos Rx To	AC sult ture ken	ctions
			No Remote	Access Sess	sions			
	Manageme	nt Sessions	[<u>LAN</u>	I-to-LAN Se	<u>ssions Re</u>	emote Acci	ess Sess	sions]
CISCO SYSTEMS	Administrate	or IP Address	s Protocol	Encryption	Login Ti	me Durat	ion Ac	tions 🗸
Administer Sessions						🔒 🔮 In	ternet	

Further Reading

Tunneling and Security: IPsec LAN-to-LAN

IOS and VPN3k with PSK using CLI only

Objective: Configure L2L IPsec tunnel between IOS router and VPN3k across the PIX/ASA Firewall. Use pre-shared keys for authentication. Use CLI to configure VPN3k.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"IOS Router and VPN3k"</u>.
- Configure access-control on the ASA. Add rules to the access-list OUTSIDE_IN as follows:
 - Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
- Configure IPsec LAN-to-LAN tunnel on R2 as follows:
 - Create ISAKMP policy with priority 10 as follows:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Use DH Group 2.
 - Create ISAKMP key CISCO for address 136.X.121.11 (VPN3k).
 - Create transform-set 3DES_MD5 as follows:
 - Use 3DES for cipher.
 - Use MD5 for hash.

- Create access-list LO2_TO_LO1 as follows:
 - Permit IP traffic from 150.X.2.0/24 to 150.X.1.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address LO2_TO_LO1.
 - Set peer 136.X.121.11.
 - Set transform-set 3DES_MD5.
- Apply crypto-map VPN to interface E0/0.
- Configure IPsec LAN-to-LAN tunnel on VPN3k using CLI as follows:
 - Create new IPsec SA: "L2L:VPN_TO_R2" as follows:
 - Use 3DES as cipher.
 - Use MD5 as hash.
 - Use IKE-3DES-MD5 IKE proposal.
 - Create access-list rule "L2L:VPN_TO_R2 In" as follows:
 - Match traffic from 150.1.2.0/24 to 150.1.1.0/24.
 - Configure "apply IPsec" as rule action.
 - Create access-list rule "L2L:VPN_TO_R2 Out" as follows:
 - Match traffic from 150.1.1.0/24 to 150.1.2.0/24.
 - Configure "apply IPsec" as rule action.
 - Assign rules "L2L:VPN_TO_R2 Out" and "L2L:VPN_TO_R2 In" to Public filter.
 - Apply IPsec SA "L2L:VPN_TO_R2" to this rules.
 - Create new group as follows:
 - Name "136.1.122.2"
 - Password "CISCO"
 - IPsec Parameters:
 - IPsec SA: "L2L:VPN_TO_R2".
 - Tunnel Type: LAN-to-LAN.

Final Configuration

```
R2:
crypto isakmp policy 10
authentication pre-share
hash md5
group 2
encryption 3des
!
crypto isakmp key CISCO address 136.1.121.11
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
ip access-list extended LO2_TO_LO1
 permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
T
crypto map VPN 10 ipsec-isakmp
match address LO2_TO_LO1
set transform 3DES_MD5
set peer 136.1.121.11
1
interface E 0/0
crypto map VPN
ASA1:
access-list OUTSIDE_IN permit udp any any eq isakmp
access-list OUTSIDE_IN permit esp any any
VPN3k:
Create IPsec SA, based on existing "stock" SA:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3K: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3K: Config -> 4
1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back
VPN3K: Policy -> 2
1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
```

5) Network Address Translation (NAT) Rules 6) Bandwidth Policies 7) Back VPN3K: Traffic -> 3 Current Security Associations -----------2. ESP-3DES-MD5 1. ESP-DES-MD5 3. ESP/IKE-3DES-MD5 4. ESP-3DES-NONE 5. ESP-L2TP-TRANSPORT 6. ESP-3DES-MD5-DH7 7. ESP-3DES-MD5-DH5 8. ESP-AES128-SHA 1) Add Security Associations 2) Modify Security Association 3) Delete Security Association 4) Copy Security Association 5) Back VPN3K: Security Associations -> 4 > Copy which SA VPN3K: Security Associations -> 2 > SA Name VPN3K: Security Associations -> L2L:VPN_TO_R2 1) Modify SA Name 2) Modify the SA's Inheritance 3) Modify the IPSec Parameters 4) Modify the IKE Parameters 5) Back VPN3K: Security Associations -> 4 1) Modify IKE Peer 2) Modify Negotiation Mode 3) Modify Authentication Method 4) Modify IKE Proposal 5) Back VPN3K: Security Associations (IKE) -> 1 > IKE Peer VPN3K: Security Associations (IKE) -> [0.0.0.0] 136.1.122.2 1) Modify IKE Peer 2) Modify Negotiation Mode 3) Modify Authentication Method 4) Modify IKE Proposal 5) Back VPN3K: Security Associations (IKE) -> Create rule to match outgoing traffic: 1) Configuration 2) Administration 3) Monitoring

Copyright © 2007 Internetwork Expert

4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3K: Config -> 4 1) Access Hours 2) Traffic Management 3) Group Matching 4) Network Admission Control 5) Back VPN3K: Policy -> 2 1) Network Lists 2) Rules 3) Security Associations (SAs) 4) Filters 5) Network Address Translation (NAT) Rules 6) Bandwidth Policies 7) Back VPN3K: Traffic -> 2 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 | 12. RIP In 11. ICMP Out 13. RIP Out | 14. OSPF In | 16. Incoming HTTP In 15. OSPF Out | 18. VRRP In 17. Incoming HTTP Out 19. VRRP Out 20. Any In 22. Incoming HTTPS In 24. LDAP In 26. Telnet/SSL In 28. Outgoing HTTP In 30. Outgoing HTTPS In 32. CRL over LDAP T 21. Any Out 23. Incoming HTTPS Out 25. LDAP Out 27. Telnet/SSL Out 29. Outgoing HTTP Out 31. Outgoing HTTPS Out | 32. CRL over LDAP In | 34. SSH In 33. CRL over LDAP Out 35. SSH Out | 36. VCA In 37. VCA Out 38. NAT-T In 39. NAT-T Out 40. DHCP In | 41. DHCP Out _____ 1) Add Filter Rule 2) Modify Filter Rule 3) Delete Filter Rule 4) Copy Filter Rule 5) Back

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

```
VPN3K: Filter Rules -> 1
> Rule Name
VPN3K: Filter Rules -> L2L:VPN_TO_R2 Out
1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back
VPN3K: Filter Rules -> 3
1) Use Single Address/Wildcard
2) Use Network List
3) Back
VPN3K: Filter Rules (Source) -> 1
> Source IP Address for this rule
VPN3K: Filter Rules (Source) -> [ 0.0.0.0 ] 150.1.1.0
> Wildcard Mask for this rule
VPN3K: Filter Rules (Source) -> [ 255.255.255.255 ] 0.0.0.255
1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back
VPN3K: Filter Rules -> 4
1) Use Single Address/Wildcard
2) Use Network List
3) Back
VPN3K: Filter Rules (Destination) -> 1
> Destination IP Address for this rule
VPN3K: Filter Rules (Destination) -> [ 0.0.0.0 ] 150.1.2.0
> Wildcard Mask for this rule
VPN3K: Filter Rules (Destination) -> [ 255.255.255.255 ] 0.0.0.255
1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
```

```
Copyright © 2007 Internetwork Expert
```

```
7) Modify ICMP Packet type
8) Back
VPN3K: Filter Rules -> 2
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
VPN3K: Filter Rules -> 1
1) Apply Rule to inbound data
2) Apply Rule to outbound data
VPN3K: Filter Rules -> [ 1 ] 2
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
VPN3K: Filter Rules -> 2
1) Drop
2) Forward
3) Drop and log
4) Forward and log
5) Apply IPSec
6) Apply IPSec and log
7) Override Tunnel Default Gateway
8) Override Tunnel Default Gateway and log
VPN3K: Filter Rules -> [ 1 ] 5
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
Create rule for inbound traffic (for policy matching):
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3K: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3K: Config -> 4
1) Access Hours
2) Traffic Management
```

Copyright © 2007 Internetwork Expert

3) Group Matching 4) Network Admission Control 5) Back VPN3K: Policy -> 2 1) Network Lists 2) Rules 3) Security Associations (SAs) 4) Filters 5) Network Address Translation (NAT) Rules 6) Bandwidth Policies 7) Back VPN3K: Traffic -> 2 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 | 14. OSPF In | 16. Incoming HTTP In 13. RIP Out 15. OSPF Out 18. VRRP In 17. Incoming HTTP Out 19. VRRP Out 20. Any In 21. Any Out 22. Incoming HTTPS In 24. LDAP In 23. Incoming HTTPS Out | 26. Telnet/SSL In 25. LDAP Out 26. Termet, Ser 1 28. Outgoing HTTP In 27. Telnet/SSL Out 30. Outgoing HTTPS In 32. CRL over LDAP In 34. SSH In 29. Outgoing HTTP Out 31. Outgoing HTTPS Out 33. CRL over LDAP Out 36. VCA In 35. SSH Out 37. VCA Out | 38. NAT-T In 39. NAT-T Out 40. DHCP In 42. L2L:VPN_TO_R2 Out 41. DHCP Out 'q' to Quit, '<SPACE>' to Continue -> _____ 1) Add Filter Rule 2) Modify Filter Rule 3) Delete Filter Rule 4) Copy Filter Rule 5) Back VPN3K: Filter Rules -> 1 > Rule Name VPN3K: Filter Rules -> L2L:VPN TO R2 In 1) Modify Rule Name 2) Modify Rule parameters 3) Modify Source Address 4) Modify Destination Address 5) Modify TCP/UDP Source Port 6) Modify TCP/UDP Destination Port 7) Modify ICMP Packet type 8) Back

Copyright © 2007 Internetwork Expert

```
VPN3K: Filter Rules -> 3
1) Use Single Address/Wildcard
2) Use Network List
3) Back
VPN3K: Filter Rules (Source) -> 1
> Source IP Address for this rule
VPN3K: Filter Rules (Source) -> [ 0.0.0.0 ] 150.1.2.0
> Wildcard Mask for this rule
VPN3K: Filter Rules (Source) -> [ 255.255.255 ] 0.0.0.255
1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back
VPN3K: Filter Rules -> 4
1) Use Single Address/Wildcard
2) Use Network List
3) Back
VPN3K: Filter Rules (Destination) -> 1
> Destination IP Address for this rule
VPN3K: Filter Rules (Destination) -> [ 0.0.0.0 ] 150.1.1.0
> Wildcard Mask for this rule
VPN3K: Filter Rules (Destination) -> [ 255.255.255.255 ] 0.0.0.255
1) Modify Rule Name
2) Modify Rule parameters
3) Modify Source Address
4) Modify Destination Address
5) Modify TCP/UDP Source Port
6) Modify TCP/UDP Destination Port
7) Modify ICMP Packet type
8) Back
VPN3K: Filter Rules -> 2
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
VPN3K: Filter Rules -> 1
1) Apply Rule to inbound data
2) Apply Rule to outbound data
VPN3K: Filter Rules -> [ 1 ] 1
```

Copyright © 2007 Internetwork Expert

```
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
VPN3K: Filter Rules -> 2
1) Drop
2) Forward
3) Drop and log
4) Forward and log
5) Apply IPSec
6) Apply IPSec and log
7) Override Tunnel Default Gateway
8) Override Tunnel Default Gateway and log
VPN3K: Filter Rules -> [ 1 ] 5
1) Choose data direction
2) Select action for the rule
3) Rule applies to which protocol
4) Back
VPN3K: Filter Rules -> 4
Assign rules to the Public traffic filer:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3K: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3K: Config -> 4
1) Access Hours
2) Traffic Management
3) Group Matching
4) Network Admission Control
5) Back
VPN3K: Policy -> 2
1) Network Lists
2) Rules
3) Security Associations (SAs)
4) Filters
5) Network Address Translation (NAT) Rules
6) Bandwidth Policies
7) Back
VPN3K: Traffic -> 4
```

Copyright © 2007 Internetwork Expert

Current Active Filters _____ 1. Private (Default)2. Public (Default)3. External (Default)4. Firewall Filter for 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 VPN3K: Filters -> 4 > Which Filter to assign Rules to VPN3K: 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 OUT FORWARD 13. ICMP Out 14. VRRP Out OUT FORWARD | OUT FORWARD | 15. NAT-T Out 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3K: 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 | 18. VRRP In 17. Incoming HTTP Out 19. VRRP Out 20. Any In 21. Any Out 22. Incoming HTTPS In 23. Incoming HTTPS Out | 24. LDAP In 26. Telnet/SSL In 25. LDAP Out

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

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 36. VCA In 35. SSH Out 37. VCA Out 38. NAT-T In 39. NAT-T Out 40. DHCP In 41. DHCP Out 42. L2L:VPN_TO_R2 Out 'q' to Quit, '<SPACE>' to Continue -> 43. L2L:VPN_TO_R2 In _____ _____ > Which Rule to add VPN3K: Filters -> 42 The Current Rules for this Filter _____ 1. L2L:VPN_TO_R2 Out OUT IPSEC 2. GRE In | IN FORWARD 3. IPSEC-ESP In IN FORWARD 4. IKE In | IN FORWARD 5. PPTP In | IN FORWARD 6. L2TP In | IN FORWARD 7. ICMP In | IN FORWARD 8. VRRP In | IN FORWARD 9. NAT-T In IN FORWARD 10. GRE Out | OUT FORWARD 11. IKE Out OUT FORWARD 12. PPTP Out OUT FORWARD 13. L2TP Out | OUT FORWARD 14. ICMP Out | OUT FORWARD 15. VRRP Out OUT FORWARD | 16. NAT-T Out | OUT FORWARD _____ _____ 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back VPN3K: 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 | 10. ICMP In 9. L2TP Out 11. ICMP Out | 12. RIP In 13. RIP Out | 14. OSPF In 15. OSPF Out | 16. Incoming HTTP In | 18. VRRP In 17. Incoming HTTP Out 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 28. Outgoing HTTP In 27. Telnet/SSL Out 30. Outgoing HTTPS In 32. CRL over LDAP In 29. Outgoing HTTP Out 31. Outgoing HTTPS Out

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

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 42. L2L:VPN_TO_R2 Out 'q' to Quit, ' <space>' to Continue -> 43. L2L:VPN_TO_R2 In </space>						
The Current Rules	s for this Filter					
1. L2L:VPN_TO_R2 In	IN IPSEC					
2. L2L:VPN_TO_R2 Out	OUT IPSEC					
3. GRE In	IN FORWARD					
4. IPSEC-ESP IN	IN FORWARD					
6 PPTP In	IN FORWARD					
7. L2TP In	IN FORWARD					
8. ICMP In	IN FORWARD					
9. VRRP In	IN FORWARD					
10. NAT-T In	IN FORWARD					
11. GRE Out	OUT FORWARD					
12. IKE Out	OUT FORWARD					
13. PPTP OUC						
14. LZIP OUC	OUT FORWARD					
16. VRRP Out	OUT FORWARD					
17. NAT-T Out	OUT FORWARD					
	·					
 Add a Rule to this Filter Remove a Rule from this Filter Move the Rule Up Move the Rule Down Assign Security Assoc. to Rule Back VPN3K: Filters -> 5 						
> Enter the Rule						
VPN3K: Filters -> 1						
Current Security Associations						
1. ESP-DES-MD5	2. ESP-3DES-MD5					
3. ESP/IKE-3DES-MD5	4. ESP-3DES-NONE					
5. ESP-L2TP-TRANSPORT	6. ESP-3DES-MD5-DH7					
7. ESP-3DES-MD5-DH5	8. ESP-AES128-SHA					
9. L2L:VPN_TO_R2						
> Enter the Security Association						
VPN3K: Filters -> 9						
The Current Rules	for this Filter					
1. L2L:VPN TO R2 In	IN IPSEC L2L:VPN TO R2					

Copyright © 2007 Internetwork Expert

2. L2L:VPN_TO_R2 Out 3. GRE In 4. IPSEC-ESP In 5. IKE In 6. PPTP In 7. L2TP In 8. ICMP In 9. VRRP In 10. NAT-T In 11. GRE Out 12. IKE Out 13. PPTP Out 14. L2TP Out 15. ICMP Out 16. VRRP Out 17. NAT-T Out	OUT IPSEC IN FORWARD IN FORWARD IN FORWARD IN FORWARD IN FORWARD IN FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD OUT FORWARD
 Add a Rule to this Filter Remove a Rule from this Filter Move the Rule Up Move the Rule Down Assign Security Assoc. to Rule Back 	
VPN3K: Filters -> 5	
> Enter the Rule	
VPN3K: Filters -> 2	
Current Securit	y Associations
1. ESP-DES-MD5 3. ESP/IKE-3DES-MD5 5. ESP-L2TP-TRANSPORT 7. ESP-3DES-MD5-DH5 9. L2L:VPN_TO_R2	2. ESP-3DES-MD5 4. ESP-3DES-NONE 6. ESP-3DES-MD5-DH7 8. ESP-AES128-SHA
> Enter the Security Association	
VDN3K: Filters -> 9	
VENSK. FILCEIS > >	
The Current Rules	for this Filter
1. L2L:VPN_TO_R2 In	IN IPSEC L2L:VPN_TO_R2
2. L2L:VPN_TO_R2 Out	OUT IPSEC L2L:VPN_TO_R2
3. GRE IN 4 IDSEC_ESD In	IN FORWARD
5. IKE In	IN FORWARD
6. PPTP In	IN FORWARD
7. L2TP In	IN FORWARD
8. ICMP In	IN FORWARD
9. VRRP In	IN FORWARD
10. NAT-T In	IN FORWARD
12 TKE OUT	OUT FORWARD
13. PPTP Out	OUT FORWARD
14. L2TP Out	OUT FORWARD
15. ICMP Out	OUT FORWARD
16. VRRP Out	OUT FORWARD
17. NAT-T Out	OUT FORWARD

Copyright © 2007 Internetwork Expert

_____ 1) Add a Rule to this Filter 2) Remove a Rule from this Filter 3) Move the Rule Up 4) Move the Rule Down 5) Assign Security Assoc. to Rule 6) Back Create Tunnel Group: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 1 1) Interface Configuration 2) System Management 3) User Management Policy Management
 Tunneling and Security 6) Back VPN3K: Config -> 3 1) Base Group 2) Groups 3) Users 4) Back VPN3K: User Management -> 2 Current User Groups _____ No User Groups _____ 1) Add a Group 2) Modify a Group 3) Delete a Group 4) Back VPN3K: Groups -> 1 > Group Name VPN3K: Groups -> 136.1.122.2 > Password VPN3K: Groups -> CISCO Verify -> CISCO 1) Group Type - Internal 2) Group Type - External VPN3K: Groups -> 1

Copyright © 2007 Internetwork Expert

1) Identification 2) General Parameters 3) Servers 4) IPSec Parameters 5) VPN Client Firewall Parameters 6) Hardware Client Parameters 7) PPTP/L2TP Parameters 8) Address Pools 9) Client Update 10) Assign Bandwidth Policies 11) WebVPN Parameters 12) NAC Parameters 13) Back VPN3K: Groups -> 4 1) Select IPSec SA 2) Select IKE Peer Validation 3) Enable/Disable IKE Keepalives 4) Set Confidence Interval 5) Set Tunnel Type 6) Back VPN3K: Groups -> 1 Current Security Associations _____ 0. Use '0' for no selection 1. ESP-DES-MD5 4. ESP-3DES-NONE 3. ESP/IKE-3DES-MD5 5. ESP-L2TP-TRANSPORT 6. ESP-3DES-MD5-DH7 7. ESP-3DES-MD5-DH5 8. ESP-AES128-SHA 9. L2L:VPN_TO_R2 > IPSec SA VPN3K: Groups -> [(inherited) ESP-3DES-MD5] 9 1) Select IPSec SA 2) Select IKE Peer Validation 3) Enable/Disable IKE Keepalives 4) Set Confidence Interval 5) Set Tunnel Type 6) Back VPN3K: Groups -> 5 1) LAN-to-LAN 2) Remote Access VPN3K: Groups -> [(inherited) 2] 1 1) Select IPSec SA 2) Select IKE Peer Validation 3) Enable/Disable IKE Keepalives 4) Set Confidence Interval 5) Set Tunnel Type 6) Back VPN3K: Groups ->

Verification

```
R2#ping 150.1.1.1 so lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
R2#sho crypto isakmp sa
dst.
                src
                                state
                                               conn-id slot
               136.1.122.2
136.1.121.11
                                QM_IDLE
                                                 1 0
R2#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.122.2
  protected vrf:
   local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.121.11:500
     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 1, #recv errors 0
    local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
     path mtu 1500, media mtu 1500
     current outbound spi: 49A180DF
     inbound esp sas:
      spi: 0x380D5231(940397105)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4433672/3564)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x49A180DF(1235321055)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4433672/3564)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
```

Copyright © 2007 Internetwork Expert

Monitor session at VPN3k: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 3 1) Routing Table 2) Event Log 3) System Status 4) Sessions 5) General Statistics 6) Dynamic Filters 7) Back VPN3K: Monitor -> 4 1) View Session Statistics 2) View Top Ten Lists 3) View Session Protocols 4) View Session Encryption 5) Filter Sessions on Group 6) Back VPN3K: Sessions -> 1 Active Sessions _____ Active LAN-to-LAN Sessions: 1 Active Remote Access Sessions: 0 Active Management Sessions: 1 Total Active Sessions: 2 Weighted Active Load: Percent Session Load: 1 Total Active Sessions: Peak Concurrent 1.00% 2 2 Total Cumulative Sessions: 8 Num Username IP Address Protocol Encrypt Duration Data Tx Data Rx _____ Console None 0:10:44 N/A 1 admin Local N/A 2 Auth'ing 136.1.122.2 IPSecL2L 3DES168 0:02:45 936 936 1) Refresh Session Statistics 2) Reset Session Statistics 3) Restore Session Statistics 4) Session Details 5) Back VPN3K: Sessions ->

Further Reading

Tunneling and Security: IPsec LAN-to-LAN

Copyright © 2007 Internetwork Expert

IOS and VPN3k with Digital Certificates

Objective: Configure L2L IPsec tunnel between IOS and VPN3k using authentication based on Digital Certificates.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK"</u>.
- Enroll VPN3k with CA:
 - Set up clock synchronization via NTP with CA server.
 - Configure Public traffic filter to permit Outgoing NTP as follows:
 - Configure two rules: inbound and outbound.
 - Assign them to Public traffic filter.
 - Retrieve CA Certificate via SCEP:
 - Configure Public traffic filter to permit:
 - Ougoing HTTP traffic In and Out.
 - Use the pre-configured rules for this task.
 - Use enrollment URL http://10.0.0.100/certsrv/mscep/mscep.dll
 - o Generate Certificate Request.
- Enroll R2 with CA:
 - Configure domain-name and generate key-pair.

- Synchronize clock via NTP with CA Server.
- Configure CA Trustpoint as follows:
 - Use enrollment URL: <u>http://10.0.0.100/certsrv/mscep/mscep.dll</u>
 - Configure CRL as optional.
 - Use RA mode.
- Modify L2L Tunnel settings on VPN3k as follows:
 - o Use IKE Proposal with "RSA" keyword (RSA-Sig authentication).
 - o Chose certificate you have requested to be used for authentication.
- Modify ISAKMP policy at R2 to use RSA-sig authentication.

Final Configuration

```
R2:
crypto isakmp policy 10
authentication rsa-sig
T
crypto ca trustpoint IE1
 enrollment url http://10.0.0.100/certsrv/mscep/mscep.dll
 crl optional
 enrollment mode ra
exit
!
! Configure NTP server
1
ntp server 10.0.0.100
!
! Generate RSA key, authenticate CA and enroll
1
ip domain-name internetworkexpert.com
hostname R2
crypto key generate rsa general modulus 512
crypto ca authenticate IE1
crypto ca enroll IE1
```

VPN3k:

Create rule for Outgoing NTP Out:

🖉 Cisco Systems, Inc. VPN 3000 C	oncentrator [¥PN3K] - Microsoft Interne	t Explorer
<u>File Edit View Favorites Too</u>	ls Help (⇔Back + ⇒ → 🛛 🚱	Address 🙆 https://136.1.121.11/access.html
VPN	3000	Main Help Support Logout
Conc	entrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
	Configuration Policy Managem	ent Traffic Management Rules Modify
	Modify a filter rule.	
Access Hours	Rule Name Outgoing NTP C	Name of this filter rule. The name must be unique.
	Direction Outbound 💌	Select the data direction to
BW Policies 	Action Forward	Specify the action to take when this filter rule applies.
⊕ <u>Network Admission Control</u> ⊕ <u>Tunneling and Security</u> @}Administration @ Monitoring	Protocol UDP	Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
	TCP Don't Care	Select whether this rule should apply to an established TCP connection.
CISCO SYSTEMS	Source Address	Specify the source
🖉 Filter Rules		🛛 🔒 🔮 Internet

Cisco Systems, Inc. VPN 3000 C	oncentrator [VPN3K] - Microsoft Internet Explorer	
File Edit View Favorites 100	s Help (⇔Back • ⇒) • 💟 😰 Agdress 4 3000	Main Help Support Logout
Conc	entrator Series Manager	Logged in: admin
	0	Configuration Administration Monitoring
Configuration Interfaces System		10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Arcess Hours Access Hours Access Hours Access Hours Access Hours	TCP/UDP Source Port	For TCP/UDP, specify the source port ranges that this rule checks. For a single
Network Lists Rules SAs Filters BNAT BWAT BWAT BWAT BWR Admission Control BUNetwork Admission Control BTunneling and Security BAdministration BMonitoring	or Range 0 to 65535	port number, use the same number for the start and end.
	TCP/UDP Destination Port Port Range	For TCP/UDP, specify the destination port ranges that this rule checks. For a
	or Range 123 to 123	single port number, use the same number for the start and end.
	ICMP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
CISCO SYSTEMS	Add Cancel	orone
🔊 Filter Rules		📄 🙆 🍘 Internet

Create	rule	for	Outaoina	NTP	in:
create	rure	TOT	outgoing	TATE	T 11•

🚰 Cisco Systems, Inc. ¥PN 3000 Co	ncentrator [¥PN3K] - Microsoft Internet	Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	: <u>H</u> elp	Address 🖉 https://136.1.121.11/access.html
VPN 3	3000	Main Help Support Logout
Nonce	ntrator Series Manager	Logged in: admir
		Configuration Administration Monitoring
Hiterfaces HERSystem	Configuration Policy Manageme	nt Traffic Management Rules Add
E-User Management Policy Management Access Hours	Configure and add a new filter rule.	
Access nours Traffic Management Network Lists	Rule Name Outgoing NTP In	Name of this filter rule. The name must be unique.
	Direction Inbound	Select the data direction to which this rule applies.
	Action Forward	Specify the action to take when this filter rule applies.
⊕ <u>Network Admission Control</u> ⊕ <u>Tunneling and Security</u> ⊕ <u>Administration</u> ⊕ <u>Monitoring</u>	Protocol UDP	Select the protocol to which this rule applies. For Other protocols, enter the protocol sumpler.
	TCP Don't Care 🗾	Select whether this rule should apply to an established TCP connection.
Cisco Systems tillitutillitu	Source Address	Specify the source
🖉 Filter Rules		🔚 🍘 Internet

Cisco Systems, Inc. VPN 3000 C File Edit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	oncentrator [VPN3K] - Microsoft Internet Is Help (⇔Back → ⇒) → (∞) (‡)	Explorer 2 3 Address Thtps://136.1.121.11/access.html
VPN Conc	3000 entrator Series Manager	Main Help Support Logou
	8	Configuration Administration Monitoring
Configuration	Wildcard-mask 255.255.255.255	to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
	TCP/UDP Source Port Port Range	For TCP/UDP, specify the source port ranges that this rule checks. For a single
	or Range 123 to 123	number, use the same number for the start and end.
Boroup Matching Byletwork Admission Control Byletwork Admission Control Byletwork Admission Byletwork Admission	TCP/UDP Destination Port Port Range	For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the
	or Range 0 to 6553	5 same number for the start and end.
	ICMP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
CISCO SYSTEMS	Add Cancel	
🖞 Filter Rules		📔 🔒 🞯 Internet



Add rules to Public filter, permitting outgoing NTP:

🚰 Cisco Systems, Inc. VPN 3000 C	oncentrator [VPN3K] - Microsoft Interne	t Explorer		_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ool	s <u>H</u> elp	Address 🛃 https://136.1.12	1.11/access.html	
VPN	3000		Main Help Sup	oport Logout
Conce	entrator Series Manager		Log	ged in: admin
		Configura	tion Administration	n Monitoring
	Filter Name: Public (Default) Select an Available Rule and clic Select a Current Rule in Filter a SA to Rule as appropriate. Select an Available Rule, then se to add the available rule above the	k Add to apply it to this filt nd click Remove, Move U elect a C urrent Rule in Filt current rule.	er. J p, Move Down, or ter, and click Insert	r Assign : Above
Ellers -ENAT BW Policics -ENGroup Metching	Current Rules in Filte	er	Actions	
Detwork Admission Control	Outgoing NTP In (forward/in)		<< Add	OSPF
□ <u>□ <u>Tunneling</u> and Security</u>	L2L: VPN_TO_R2 Out (IPSec/L2L)	VPN_TO_R2/out)	<< Insert Above	OSPF
-# <u>Monitoring</u>	IKE Out (forward/out) PPTP Out (forward/out)		Remove >>	Incom Any In
	L2TP Out (forward/out)		Move Up	Any O
	VRRP Out (forward/out) NAT-T Out (forward/out)		Move Down	
	RIP Out (forward/out)		Assign SA to Rule	LDAP
Cisco Systems	Outgoing HTTP Out (forward/out) Outgoing NTP Out (forward/out)	•	Done	Telner
antillina a				Þ
🕙 User/Group Management	99. 		📋 🔒 🎯 Internet	1

Configure NTP Server:

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer	_ 🗆 ×
<u>File Edit V</u> iew F <u>a</u> vorites <u>T</u> ools	: <u>H</u> elp (⇒ Back → ⇒) → 区 😰	Address 🖉 https://136.1.121.11/access.html	-
VPN 3	3000	Main Help	Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuration Administ	ration Monitoring
Interfaces	Configuration System Servers	NTP Hosts Add	
	Add a new NTTD hast		
	Add a new 141F nost.		
Authorization	NTP Host 10.0.0.100	Enter the hostname or IP address of the	NTP server.
	Add Cancel		
	200 - 202 C-		
Parameters			
Hosts			
Address Management			
	l .		
Load Balancing			
<u>EPolicy Management</u>			
<u>-</u> <u></u>	4		
	1		
Cesco Sestens			
E NTP Servers		Ir 🍏 🗎	ternet //

Add rules to Public filter, permitting Outgoing HTTP In/Out (for SCEP):

🖉 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer 📃 🛛 🔀			
<u>Eile Edit View Favorites Tools</u>	Help (= Back + => - 💽 😭	Address 🕘 https://136.1.121.11/access.html	-
Main Help Support Logout			
Conce	ntrator Series Manager		Logged in: admin
Configuration Administration Monitoring			
Configuration Interfaces System Duser Management Access Hours Diraffic Management Network Lists Rules	Filter Name: Public (Default) Select an Available Rule and click Add to apply it to this filter. Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate. Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.		
Filters - The NAT -	Current Rules in Filto	er Actions	
Hetwork Admission Control Honeling and Security Administration Monitoring	Outgoing HTTP In (forward/in) L2L: VPN_TO_R2 Out (IPSec/L2L: VPN_TO_R2/out) GRE Out (forward/out) IKE Out (forward/out) PPTP Out (forward/out) L2TP Out (forward/out) ICMP Out (forward/out) VRRP Out (forward/out) VRRP Out (forward/out) VRP Out (forward/out) Outgoing HTTP IP Out (forward/out) Outgoing HTTP IP Out (forward/out)	VPN_TO_R2/out)	ve Incom
			Any In Any O Incom
		Assign SA to F	LDAP Rule LDAP Teine Teine
Filter Policies			ternet
Install CA Certificate:



🗿 Fisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3K] - Microsoft Interne	t Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🔹 🖘 🛪 🙆 🕼	Address Address Address Address Attps://136.1.121.11/access.html	•
VPN 3	3000	Main Help	Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuration Administr	ation Monitoring
Configuration Administration Administer Sessions	Administration Certificate Mana	ngement Install CA Certificate SCEP	
<u>System Reboot</u> <u>Reboot Status</u> <u>Ping</u>	Enter the information needed to re operation to complete.	trieve the CA certificate via SCEP. Please	wait for the
<u>Initia</u> <u>Traceroute</u> <u>Monitoring Refresh</u> <u>Monitoring Refresh</u>	URL 10.0.0.100/certsrv CA lice1	//mscep/mscep.dll Required for some PKI	
Grie Management Gretificate Management Enrollment Installation	Descriptor ^E Retrieve Cancel	configurations.	
- IIIstaliation - III Monitoring			
CISCO SYSTEMS			
🙋 Certificate Management		📔 🕒 🔤 In	ternet //.

Enroll with certification authority:



🚰 Cisco Systems, Inc. VPN 300	0 Concentrator [¥PN3K] - Microsoft Interne	t Explorer
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	Iools Help 🗘 🖙 Back 🔹 🖘 🛪 🔇 🚱	Address 🖉 https://136.1.121.11/access.html
VPI	N 3000	Main Help Support Logout
Cor	icentrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
Configuration Administration Administer Sessions	Administration Certificate Mana	agement Enroll Identity Certificate SCEP
B-Software Update System Reboot Reboot Status Dica	Enter the information to be include operation to finish.	d in the certificate request. Please wait for the
Tinceroute <u>Monitoring Refresh</u> <u>DAccess Rights</u> <u>DEFie Management</u>	Common Name (CN) VPN3k	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
	Organizational Unit (OU)	Enter the department.
Installation Imponitoring	Organization (O)	Enter the Organization or company.
	Locality (L)	Enter the city or town.
	State/Province (SP)	Enter the State or Province
	Country (C)	Enter the two-letter country abbreviation (e.g. United States = US).
CISCO SYSTEMS	Subject AlternativeName VPN3k (FQDN)	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
View All CRL Caches		



Modify L2L tunnel settings:

🏂 Cisco Systems, Inc. VPN 3000	Concentrator [VPN3K] - Microsoft Int	ernet Explorer
<u>File Edit View Favorites To</u>	pols Help (⇔ Back + ⇒) - 💟	Address @ https://136.1.121.11/access.html
VPN	3000	Main Help Support Logout
Con	centrator Series Manag	er Logged in: admin
		Configuration Administration Monitoring
Configuration Interfaces System User Management Deloicy Management De	Peers	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.
LAN-to-LAN 	Digital Certificate VPN3k Certificate C Entire o Transmission © Identity	Select the digital certificate to use. Certificate chain v certificate only certificate only certificate only
Generation Gener	Preshared Key CISCO	Enter the preshared key for this LAN-to-LAN connection.
	Authentication ESP/MD5/	/HMAC-128 /HMAC-128
0	Encryption 3DES-168	Specify the encryption mechanism to use.
utilitionalition.	IKE Proposal IKE-3DES	MD5-RSA 🔽 Select the IKE Proposal to use for this LAN-to-LAN
F IPSec LAN-to-LAN		🔒 🔮 Internet

Verification

```
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 8/9/12 ms
R2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
      K - Keepalives, N - NAT-traversal
      X - IKE Extended Authentication
      psk - Preshared key, rsig - RSA signature
      renc - RSA encryption
C-id Local
                                   I-VRF Encr Hash Auth DH Lifetime Cap.
                    Remote
     136.1.122.2 136.1.121.11
1
                                              3des md5 rsig 2 23:59:18
```

Copyright © 2007 Internetwork Expert

Check Authentication mode for IPsec session on VPN3k:

Cisco Systems, Inc. VPN 3000 Cor Eile Edit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	ncentrator [¥PN3K] - Micros Help (⇔ Back → ⇒)	• Oft Internet Explorer • O • O • Address	🔊 https://136.1.121.11/acce	ess.html
VPN 3 Conce	000 ntrator Series Ma	anager	Main	i Help Support Logout Logged in: admii
Configuration Interfaces User Management Delicy Management Turneling and Security	IKE Sessions: 1 IPSec Sessions: 1		Configuration Ad	Iministration Monitoring
		IKE ?	Session	
Administer Sessions 	Session ID	1	Encryption Algorithm	3DES-168
Reboot Status —Ping —Traceroute	Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
Monitoring Refresh	Authentication Mode	RSA Certificate	IKE Negotiation Mode	Main
-⊕ <u>Monitoring</u>	Rekey Time Interval	86400 seconds		
		IPSec	Session	
	Session ID	2	Remote Address	150.1.2.0/0.0.0.255
	Local Address	150.1.1.0/0.0.0.255	Encryption Algorithm	3DES-168
CISCO SYSTEMS	Hashing Algorithm	MD5	Encapsulation Mode	Tunnel
	Rekey Time	3600 seconds	Rekey Data	
Administer Sessions				👌 🥥 Internet

Further Reading

VPN3k: Certificate Management

IOS and VPN3k with PSK: Tuning IPsec Parameters

Objective: Fine-Tune IPsec parameters for L2L tunnel between IOS and VPN3k.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK"</u>.
- Re-Configure IPsec L2L on R2 as follows:
 - Re-Configure ISAKMP policy to use DH Group 1 for authentication.
 - Create IPsec transform-set 3DES_SHA on R2 as follows:
 - Use 3DES cipher.
 - Use SHA hash.
 - Re-configure crypto-map VPN as follows:
 - Use transform-set 3DES_SHA.
 - Use PFS DH Group 2.
- Re-Configure IPsec L2L on VPN3k as follows:
 - Create new IKE Proposal named "IKE_3DES_MD5_DH1" as follows:
 - Use DH Group 1.
 - Use 3DES as cipher.
 - Use MD5 as hash.
 - Modify L2L tunnel to use new IKE Proposal.

- Modify exististing IPsec SA for the L2L Tunnel:
 - Use SHA hash
 - Use PFS Group 2

Final Configuration

```
R2:
crypto isakmp policy 10
group 1
!
crypto ipsec transform-set 3DES_SHA esp-3des esp-sha-hmac
!
crypto map VPN 10
set transform-set 3DES_SHA
set pfs group2
```

VPN3k:

Add new IKE proposal:



🚈 Cisco Systems, Inc. ¥PN 3000 Co	ncentrator [VPN3K] - Microsoft Interne	t Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🖙 Back 🔹 🖘 🔹 😰	Address 🛃 https://136.1.121	11/access.html
VPN 3	3000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configurat	ion Administration Monitoring
-=- <u>Configuration</u>	Configuration Tunnoling and S		
Interfaces	Configuration Tunneting and Se	ecurity IPSec INE Propos	als Add
- <u>⊞-User Management</u>	Configure and add a new IKE Pre	posal.	
Policy Management FTuppeling and Security		▲2.5.5.5.999	
	Proposal Name IKE_3DES_M	D5_DH1	Specify the name of this IKE Proposal
	x .A		Select the
KE Proposals	Made Preshared Keys		🔄 authentication mode
NAT Transparency	TATORE		to use.
<u>LAlerts</u> SSH	Authentication		Select the packet
	Algorithm MD5/HMAC-128	28 💌	authentication
	Enguration		algorithm to use.
	Algorithm 3DES-168		algorithm to use.
			Select the Diffie
	Diffie-Hellman Group 1 (768-	bits) 🔽 💌	Hellman Group to
	Group -		use.
	I if otime		Select the lifetime
	Measurement Time		measurement of the
CISCO SYSTEMS			IKE keys.
ally ally a	D-4- T : fatima 10000		Specify the data
ART THE Dropocals	Data Literine 1.0000		

Activate this proposal:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Internel	t Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🔹 🖘 👻 🚯	Address 🖉 https://136.1.12	1.11/access.html
VPN 3 Conce	000 ntrator Series Manager		Main Help Support Logout Logged in: admin
		Configura	tion Administration Monitoring
Configuration Interfaces DSystem DUser Management DPolicy Management DTunneling and Security DTUNNELING and Security DTUNNELING AND SECURITY DTUNELING AND SECURITY DTUNELING AND SECURITY	Select an Inactive Proposal and c or Delete as appropriate. Select an Active Proposal and clic or Move Down to change its prior Click Add or Copy to add a new I <u>Associations</u> to specify IKE param	click Activate to make it A ck Deactivate to make it I rity. Inactive Proposal. IKE P leters.	Active, or click Modify, Copy
LAN-to-LAN	Active Proposals	Actions	Inactive Proposals
-D-Administration -D-Monitoring	CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5-DH7 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA IKE-AES128-SHA-DH2 CRACK-3DES-SHA-DH2 CRACK-3DES-SHA-DH2 HYBRID_AES256_SHA_RSA_DH HYBRID_AES192_SHA_RSA_DH HYBRID_AES192_SHA_RSA_DH HYBRID_3DES_SHA_RSA_DH5		IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-R: CiscoVPNClient-3DES-MD5-R: CiscoVPNClient-3DES-SHA-D: CiscoVPNClient-3DES-SHA-D: CiscoVPNClient-AES256-SHA IKE-AES256-SHA IKE-AES256-SHA IKE-MD5_DH1 HYBRID_AES128_SHA_RSA_ HYBRID_3DES_MD5_RSA_DI HYBRID_3DES_MD5_RSA_DI CRACK-AES256-SHA-DH5 CRACK-3DES-SHA1-DH5
IPSec NAT Transparency			Internet

🗿 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer		
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 🔹 🖘 🗸 💽 🔂	Address 🙋 https://136.1.121.11/ac	cess.html	
VPN 3	000	Ma	in Help Support Logout	
Conce	ntrator Series Manager		Logged in: admin	
		Configuration /	Administration Monitoring	
	Configuration Tunneling and S	ecurity IPSec LAN-to-LAN	A	
	This section late you confirm TDS	oo TAN to TAN compositions T		
E-Tunneling and Security	connections are established with o	ther VPN 3000 Concentrators. P	IX firewalls, 7100/4000	
	series routers and other IPSec-cor	mpliant security gateways. To con	figure a VPN 3002 or	
-EH <u>PSec</u> <u>LAN-to-LAN</u> <u>IKE Proposals</u>	CHPSec other remote access connection, go to User Management and configure a Group and User. LAN-to-LAN To configure NAT over LAN-to-LAN, go to LAN-to-LAN NAT Rules.			
NAT Transparency Alerts SSH	Click the Add button to add a LA Modify or Delete .	N-to-LAN connection, or select :	a connection and click	
	(D) indicates a disabled LAN-to-I	LAN connection.		
+±+ <u>Administration</u> -#+Monitoring				
	LA	N-to-LAN		
	C	onnection	Actions	
	VPN TO R2 (136 1 122	2) on Ethernet 2 (Public)		
			Add	
200320103			Modify	
Cisco Systems			Delete	
and how and how -				
IPSec LAN-to-LAN			🔒 🔮 Internet 🏼 🎢	

Modify L2L tunnel settings:

Cisco Systems, Inc. VPN 3000 Co	oncentrator [VPN3K] - M	licrosoft Interne	t Explorer		
	3000 entrator Series	Manager		/136.1.121.11/access.htm Main Help Sup Log	oport Logout uged in: admin
			C	onfiguration Administratio	n Monitoring
Configuration Interfaces ElSystem Filese Management	Digital	None (Use Pre	shared Keys) 🔽	Select the digital cer	rtificate to
Decentrations Decentration Decentration	Certificate Transmission	 C Entire certif ● Identity cer 	icate chain tificate only	Choose how to send digital certificate to t peer.	d the the IKE
LAN-to-LAN HE Proposals	Preshared Key	CISCO		Enter the preshared this LAN-to-LAN connection.	key for
Alerts 	Authentication	ESP/MD5/HM/	4C-128 💌	Specify the packet authentication mech use.	anism to 🛛 –
⊕ <u>Administration</u> ⊕A <u>dministration</u> ⊕A <u>Monitoring</u>	Encryption	3DES-168 💌		Specify the encrypti mechanism to use.	ion
	IKE Proposal	IKE-3DES-MD!	5	Select the IKE Prop use for this LAN-to connection.	oosal to -LAN
CISCO SYSTEMS	Filter	IKE-3DES-MD5 IKE-DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5 IKE-AES128-SI	-DH1 ;-DH7 ;-RSA HA	Choose the filter to the traffic that is turn through this LAN-to connection.	apply to neled o-LAN
		IKE_3DES_MD	5_DIFI	Check to let NAT-	Г
IPSec LAN-to-LAN				🔒 🎯 Internet	t

Gissa Sustants Tas, UNN 2000 Co	Nicyosoft Tatow	at Euplayor		
Eile Edit View Favorites Tools	; Help (⇔ Back → ⇒) → 🔕 👔	Address 🙆 https://	/136.1.121.11/access.html	
VPN 3	3000		Main Help Support	Logout
Conce	entrator Series Manager		Logged	in: admin
		Ca	onfiguration Administration M	onitoring
	Configuration Policy Manager This section lets you add, configu Security Associations use <u>IKE Pr</u> Click Add to add an SA, or sele	nent Traffic Manag re, modify, and delet roposals to negotiate ct an SA and click IM	ement Security Associations Save Need te IPSec Security Associations (S IKE parameters. fodify or Delete.	ed 🔒
BAS Filters	ESP-3D ESP-3D ESP-3D ESP-3D ESP-AE ESP-DE ESP-DE ESP-LE ESP-LE ESP/KE	ESec SAs ES-MD5-DH5 ES-MD5-DH7 ES-NONE S128-SHA S-MD5 TP-TRANSPORT -3DES-MD5 -3DES-MD5 -10_R2	Actions Add Modify Delete	
CISCO SYSTEMS			🔒 👩 Internet	

Modify L2L tunnel's IPsec SA:

Change authentication:

Cisco Systems, Inc. VPN 3000 Col	ncentrator [VPN3K] - Microsoft Interne	t Explorer
<u>File Edit Yiew Favorites Tools</u>	Help ← Back + ⇒ + 💽 🕼	Address 🔊 https://136.1.121.11/access.html
VPN 3	3000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admir
		Configuration Administration Monitoring
<u>——Interfaces</u> —⊞ <u>Sγstem</u>	Configuration Policy Managemo Modify	ent Traffic Management Security Associations
	Modify a configured Security Asso	ociation.
	SA Name L2L: VPN_TO_	R2 Specify the name of this Security Association (SA).
<u>SAs</u> <u>Filters</u>	Inheritance From Rule 💌	Select the granularity of this SA.
	IPSec Parameters	
	Authentication ESP/SHA/HM	AC-160 Select the packet authentication algorithm to use.
⊕Administration ⊕Monitoring	Encryption 3DES-168	Select the ESP encryption algorithm to use.
	Encapsulation Mode	Select the Encapsulation Mode for this SA.
	Perfect Forward Secrecy	Select the use of Perfect Forward Secrecy.
Cisco Systems	Lifetime Measurement	Select the lifetime measurement of the IPSec keys.
	Data Lifetime 10000	Specify the data lifetime in kilobytes (KB)
Cesco Systems Cesco Systems Desc Security Associations Desc Security Associations	Inheritance From Rule IPSec Parameters Authentication Algorithm Encryption Algorithm Encapsulation Mode Perfect Forward Secrecy Lifetime Measurement Data Lifetime 10000	Select the granularity of this SA. Select the packet authentication algorithm to use. Select the ESP encryption algorithm to use. Select the Encapsulation Mode for this SA. Select the use of Perfect Forward Secrecy. Select the lifetime measurement of the IPSec keys. Specify the data lifetime in kilobytes (KB)

Change PFS group:

File Edit View	nc. VPN 3000 Cor Favorites Tools	Help (Back + => +	It Internet	Address Abtro://136.1.121.11/access.btml	
	VPN 3	000		Main Help Supp	ort Logout
X # 1/2	Conce	ntrator Series Mar	nager	Logg	ed in: admiı
Capfiguration	_			Configuration Administration	Monitoring
<u>Interfaces</u> — <u>Interfaces</u> — <u>⊡System</u>	-*	Configuration Policy M Modify	anageme	nt Traffic Management Security Association	s
	<u>ent</u> 'S	Modify a configured Secu	urity Asso	ciation.	
Network L	<u>lists</u>	SA Name L2L:\	/PN_TO_F	R2 Specify the name of this Security Association (S.	A).
<u>—SAs</u> <u>—Filters</u>		Inheritance From	Rule 💌	Select the granularity of	this SA.
	<u>53</u>	IPSec Parameters			
<u> ⊕⊕Group Match</u> <u>⊕Network Adn</u> ⊕Tunneling and S	<u>ing</u> <u>nission Control</u> ecurity	Authentication ESP/	/SHA/HM/	AC-160 Select the packet auther algorithm to use.	ntication –
⊕ <u>Administration</u> ⊕ <u>Monitoring</u>		Encryption 3DES	S-168 💌	Select the ESP encrypti algorithm to use.	on
		Encapsulation Mode	el 💌	Select the Encapsulation for this SA.	n Mode
		Perfect Forward Secrecy Grou	p 2 (1024-l	Select the use of Perfect Forward Secrecy.	t
Cisco Sys	TENS	Lifetime Measurement	•	Select the lifetime measu of the IPSec keys.	ırement
Մ	din	Data Lifetime 10000)	Specify the data lifetime kilobytes (KB)	in .
IPSec Security Asso	ociations			🔒 🥑 Internet	

Verification

R2# pi	ng 150.1.1.1 sou	rce loopback 0					
Type Sendi Packe .!!!! Succe	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds: Packet sent with a source address of 150.1.2.2 Success rate is 80 percent (4/5), round-trip min/avg/max = 8/9/12 ms						
R2# sh Codes	<pre>R2#show crypto isakmp sa det Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption</pre>						
C-id 1	Local 136.1.122.2	Remote 136.1.121.11	I-VRF	Encr Ha 3des mo	lash Auth d5 psk	DH Lifetime 1 23:59:24	Cap.
R2# sh	ow crypto ipsec	sa					
inter	face: Ethernet0/	0					

Copyright © 2007 Internetwork Expert

```
Crypto map tag: VPN, local addr. 136.1.122.2
protected vrf:
local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
current_peer: 136.1.121.11:500
  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 6, #recv errors 0
  local crypto endpt.: 136.1.122.2, remote crypto endpt.: 136.1.121.11
  path mtu 1500, media mtu 1500
  current outbound spi: 4BBCC626
  inbound esp sas:
   spi: 0x5553683(89470595)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4401657/3547)
     IV size: 8 bytes
     replay detection support: Y
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x4BBCC626(1270662694)
     transform: esp-3des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4401657/3547)
     IV size: 8 bytes
     replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
```

VPN3k:

Administration > Administer Sessions > VPN_TO_R2:

Cisco Systems, Inc. VP	N 3000 Con	centrator [¥PN3K]	- Micros	oft Inte	ernet Explorer					_ 🗆
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorit	es <u>T</u> ools	Help 🗘 Back	、 + ≓> ·	• 🕑 [Address	🙆 https://136	6.1.121.11/ac	cess.html		-
	VPN 30	000					Ma	in Help	Suppo	rt Logou
	Concen	trator Serie	es Ma	nage	21				Logge	l in: adm
						Confi	iguration	Administr	ation	Monitorin
Configuration									0007.0	
Administration		Administration	Admin	ister S	lessions Det	tail	Monday, 1	5 January Dece	/ 2007 2	2:31:18
- El-Software Update								Rese	Ker	esnev
		Back to Sessior	15							
<u>—Reboot Status</u> —Ping										
<u>Traceroute</u>		Connection	царана со со со со со со со со со со со со со		Durteral		Login	n	Bytes	Bytes
Monitoring Refresh		Name	IP Aŭŭ	ress	Protocol	Encryption	Time	Duration	Tx	Rx
- <u>⊞File Management</u>		TENT TO DO	126.1.1		PSec/LAN-	2010 160	Jan 15	0.00.01	416	416
<u> Certificate Management</u>	Ĺ	VPN_IO_KZ	130.1.1	22.2 t	:o-LAN	3DE2-100	22:28:56	0:02:21	410	410
Monitoring										
		TVE Samian	- A.							
		IKE Sessions	5: 1 ns: 1							
					пит	C !				
	IKE Session			_						
Session ID 1 Encryption 3DES				n 3DES-	-168					
							Algorith	n		
CISCO SYSTEMS		Hashing Alg	orithm	MD5		Diff	ie-Hellma	n Group	1 (768-	bit)
							Grou	P	- 2	
	1	•								
Administer Sessions								📋 🎯 Ini	ternet	

Further Reading

VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.7

IOS and VPN3k: Filtering Tunneled Traffic

Objective: Configure VPN3k to filter tunneled traffic.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK"</u>.
- The goal is to deny ICMP echo and echo-replay message to flow in the tunnel.
- Configure VPN3k as follows:
 - Create Fitler Rule DENY_ECHO to deny ICMP Echo Outbound.
 - Create Filter Rule DENY_ECHO_REPLY to deny ICMP Echo-Reply Inbound.
 - Create Filter VPN_TO_R2_FILTER as follows:
 - Permit traffic by default with this filter.
 - Assign rules "DENY_ECHO" and "DENY_ECHO_REPLY" to this filter.
 - Assign Filter VPN_TO_R2_FILTER to L2L Tunnel VPN_TO_R2.

Final Configuration

VPN3k:

Create "DENY_ECHO" Rule:

Cisco Systems, Inc. VPN 3000 C	oncentrator [¥PN3K] - Microsoft Interne	Explorer	l ×
<u>File Edit View Favorites Tool</u>	ls Help (⇔ Back → ⇒ → 🙆 🚺	Address 🖉 https://136.1.121.11/access.html	-
VPN	3000	Main Help Support Log	out
Conce	entrator Series Manager	Logged in: ad	mi
		Configuration Administration Monitor	ring
			_
<u>Interfaces</u>	Configuration Policy Manageme	ent Traffic Management Rules Add	
Horsen Management Policy Management	Configure and add a new filter rule		
Access Hours Access	Rule Name DENY_ECHO	Name of this filter rule. The name must be unique.	
	Direction Outbound	Select the data direction to which this rule applies.	
BW Policies 	Action Drop	Specify the action to take when this filter rule applies.	
<u>Administration</u> <u>Administration</u>	Protocol ICMP -	Select the protocol to which this rule applies. For Other protocols, enter the protocol number.	
	TCP Don't Care	Select whether this rule should apply to an established TCP connection.	
CISCO SYSTEMS	Source Address	Specify the source	
Filter Rules		📑 🔮 Internet	-

jle <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	: Help 🗘 Back 🔹 🖘 🗸 🔕 🚯 🛛 Address 🙋 htt	cps://136.1.121.11/access.html 🗾 🔢
VPN 3	3000	Main Help Support Logou
Conce	ntrator Series Manager	Logged in: admi
		Configuration Administration Monitoring
Configuration Interfaces BSystem RUser Management	Wildcard-mask (255.255.255.255	to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
	TCP/UDP Source Port	For TCP/UDP, specify the source port ranges that this
-Rules -SAs -Filters -GNAT	Port Range or Range 0 to 65535	port number, use the same number for the start and end.
<u>Over Policies</u> <u>Over Policies</u> <u>Over Admission Control</u> <u>Over Work Admission Control</u> <u>Over Tunneling and Security</u>	TCP/UDP Destination Port	For TCP/UDP, specify the destination port ranges that this rule checks. For a
j <u>Administration</u> }Monitoring	or Range 0 to 65535	single port number, use the same number for the start and end.
	ICMP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
CISCO SYSTEMS	Add Cancel	N

Create "	DENY_	ЕСНО	REP"	rule:
----------	-------	------	------	-------

🚰 Cisco Systems, Inc. VPN 3000 C	oncentrator [¥PN3K] - Microsoft Interne	et Explorer 📃 📃
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	ls Help ⇔Back • ⇒ • 🔇 🚱	Address 🛃 https://136.1.121.11/access.html
VPN	3000	Main Help Support Logo
Conc	entrator Series Manager	Logged in: adm
		Configuration Administration Monitori
Configuration Interfaces Insurtain	Configuration Policy Manageme	ent Traffic Management Rules Add
	Configure and add a new filter rule	3
Access Hours	Rule Name DENY_ECHO_F	REP Name of this filter rule. The name must be unique.
Rules SAS Filters	Direction Inbound	Select the data direction to which this rule applies.
BW Policies 	Action Drop	Specify the action to take when this filter rule applies.
Hetwork Admission Control Durneling and Security Administration Monitoring		Select the protocol to which this rule applies. For Other protocols, enter the
	or Other	protocol number. Select whether this rule
	TCP Don't Care Connection	should apply to an established TCP connection.
CISCO SYSTEMS	Source Address	Specify the source
Filter Rules		

Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Internet Explore	er 📃 🗆 🗙
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 🕶 🚽 💽 🛃 Addre	ss 🛃 https://136.1.121.11/access.html 📃 🔳
VPN 3	3000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
- <u>L-Configuration</u> Interfaces <u>E-System</u>		10.10.1.0/0.0.255 = all 10.10.1.nnn addresses.
	TCP/UDP Source Port	For TCP/UDP, specify the source port ranges that this
	Port Range or Range 0 to 65535	rule checks. For a single port number, use the same number for the start and end.
	TCP/UDP Destination Port Port Range	For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the
	or Range 0 to 65535	same number for the start and end.
	ICMP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
Cisco Systems	Add Cancel	· · · · · · · · · · · · · · · · · · ·
街 Filter Rules		📄 🙆 🙋 Internet

Add new traffic filter named "VPN_TO_R2_FILTER":



Assign previously created rules to filter:

🚰 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer 📃 🔲 🗙					
<u>File Edit View Favorites T</u> ools	<u>H</u> elp ⇔ Back • ⇒ - 🛛 🚱	Address 🖉 https://136.1.121	.11/access.html		
VPN 3	3000		Main Help Support Logout		
Conce	ntrator Series Manager		Logged in: admin		
		Configurat	ion Administration Monitoring		
-[]- <u>Configuration</u>	Add, remove, prioritize, and confi	gure rules that apply to a filte	er. 🔺		
Interfaces 	Filter Name: VPN_TO_R2_FILTER Select an Available Rule and click Add to apply it to this filter. Select a Current Rule in Filter and click Remove, Move Up, Move Down, or Assign SA to Rule as appropriate. Select an Available Rule, then select a Current Rule in Filter, and click Insert Above to add the available rule above the current rule.				
Evy Policies Evy Policies	Current Dulas in Filter	Actions	Avoilable Pulse		
Hetwork Admission Control		Actions			
Tunneling and Security	DENY_ECHO_REP (drop/in)	<< Add	GRE In (forward/in)		
-⊞ <u>Administration</u> -⊞ <u>Monitoring</u>		<< Insert Above	IPSEC-ESP In (forward/in)		
		Nemove >>	IKE In (forward/in)		
		Move Up	PPTP In (forward/in) PPTP Out (forward/out)		
		Move Down	L2TP In (forward/in) L2TP Out (forward/out)		
		Assign SA to Rule	ICMP In (forward/in)		
CISCO SYSTEMS		Done	RIP In (forward/in)		
Filter Policies			🔒 🥔 Internet 🏼 🍂		

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer . 🗆 🗙 Edit Favorites Tools Help (= Back - => - 💌 🚱 Address 🙋 https://136.1.121.11/access.html File View **VPN 3000** Main | Help | Support | Logout **Concentrator Series Manager** Logged in: admin Configuration | Administration | Monitoring Specify the packet -Configuration * Authentication ESP/SHA/HMAC-160 authentication mechanism to -Interfaces -⊞-<u>System</u> use. -⊞-<u>User Management</u> Specify the encryption - Policy Management Encryption 3DES-168 mechanism to use. Tunneling and Security PPTP Select the IKE Proposal to -L2TP IKE Proposal IKE_3DES_MD5_DH1 use for this LAN-to-LAN EHPSec connection. -LAN-to-LAN **-IKE Proposals** Choose the filter to apply to -NAT Transparency the traffic that is tunneled Filter VPN_TO_R2_FILTER Alerts through this LAN-to-LAN -SSH connection. -IFI-SSL -⊞-<u>WebVPN</u> Check to let NAT-T - Administration compatible IPSec peers • Monitoring establish this LAN-to-LAN IPSec NAT-T connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency. Choose the bandwidth policy Bandwidth Policy to apply to this LAN-to-CISCO SYSTEMS LAN connection. Choose the routing 🔒 🤣 Internet IPSec LAN-to-LAN

Assign filter to L2L tunnel:

Verification

R1#telnet 150.1.2.2 /source-interface loopback 0 Trying 150.1.2.2 ... Open

Password required, but none set

[Connection to 150.1.2.2 closed by foreign host]

```
R1#ping 150.1.2.2 so lo 0
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
.....
Success rate is 0 percent (0/5)
```

Further Reading

VPN3k: Policy Management

GRE and DMVPN

GRE Tunnels over IPsec with Static Crypto Maps

Objective: Configure GRE tunnels and encrypt them using static crypto maps.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"DMVPN"</u>.
- Configure GRE tunnels between R2 and R1, R1 and R3 as follows:
 - Use Loopback0 interface as tunnel sources.
 - Use IP addresses from subnet 12.12.12.0/24 for R1/R2.
 - $\circ~$ Use IP addresses from subnet 13.13.13.0/24 for R1/R3.
- Configure R1 for encryption of Tunnel0 as follows:

- Create ISAKMP policy with priority 10 as follows:
 - Use 3DES/MD5 as cipher/hash.
 - Use pre-shared keys authentication.
- Create ISAKMP key CISCO for host 136.1.0.2
- Create IPsec transform-set 3DES_MD5_TRANS as follows:
 - Use 3DES cipher.
 - Use MD5 hash.
 - Use transport mode for minimum overhead.
- Create access-list R1_TO_R2 as follows:
 - Match GRE traffic from 150.1.1.1 to 150.1.2.2
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP as follows:
 - Match address R1_TO_R2.
 - Set transform-set 3DES_MD5_TRANS.
 - Set peer 136.X.0.2.
- Configure encryption of Tunnel1 (R1-R3) on R1 the same way:
 - Create ISAKMP key CISCO for address 136.X.0.3
 - Create crypto-map VPN entry 20 of type IPsec-ISAKMP:
 - Match address R1_TO_R2.
 - Set transform-set 3DES_MD5_TRANS
 - Set peer 136.X.0.2
- Apply crypto-map VPN to interface Serial 0/0.
- Configure R2 and R3 to mirror R1's configuration.
- Configure VPN routing as follows:
 - Enable EIGRP process 100 on R1, R2, R3:
 - Include networks 12.12.12.0/24 and 13.13.13.0/24 into EIGRP
 - Include Loopback1 interfaces into EIGRP

Final Configuration

```
Tunnels & IPsec:
R1:
!
! Tunnel to R2
!
interface Tunnel0
tunnel source Loopback0
 tunnel destination 150.1.2.2
ip address 12.12.12.1 255.255.255.0
!
! Tunnel to R3
1
interface Tunnel1
tunnel source Loopback0
tunnel destination 150.1.3.3
 ip address 13.13.13.1 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
 auth pre-share
encr 3des
hash md5
1
! Pre-shared keys
!
crypto isakmp key CISCO address 136.1.0.2
crypto isakmp key CISCO address 136.1.0.3
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
1
! Access-list to match tunnels' traffic
1
ip access-list extended R1 TO R2
permit gre host 150.1.1.1 host 150.1.2.2
!
ip access-list extended R1_T0_R3
permit gre host 150.1.1.1 host 150.1.3.3
!
! Crypto map to encrypto traffic to R2
!
crypto map VPN 10 ipsec-isakmp
set peer 136.1.0.2
set transform-set 3DES_MD5_TRANS
match address R1_TO_R2
1
! Crypto map to encrypto traffic to R3
!
crypto map VPN 20 ipsec-isakmp
set peer 136.1.0.3
set transform-set 3DES_MD5_TRANS
match address R1_TO_R3
interface Se 0/0
crypto map VPN
R2:
!
! Tunnel to R1
```

Copyright © 2007 Internetwork Expert

1

```
interface Tunnel0
 tunnel source Loopback0
 tunnel destination 150.1.1.1
ip address 12.12.12.2 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
auth pre-share
encr 3des
hash md5
I
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
mode transport
1
ip access-list extended R2_T0_R1
permit gre host 150.1.2.2 host 150.1.1.1
!
! Crypto map to encrypto traffic to R1
!
crypto map VPN 10 ipsec-isakmp
set peer 136.1.0.1
set transform-set 3DES_MD5_TRANS
match address R2_TO_R1
!
interface Serial0/0
crypto map VPN
R3:
!
! Tunnel to R1
interface Tunnel0
tunnel source Loopback0
tunnel destination 150.1.1.1
 ip address 13.13.13.3 255.255.255.0
1
! ISAKMP policy
1
crypto isakmp policy 10
auth pre-share
 encr 3des
hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Access-list to match tunnel traffic
!
ip access-list extended R3_TO_R1
```

Copyright © 2007 Internetwork Expert

permit gre host 150.1.3.3 host 150.1.1.1 ! ! Crypto map to encrypt traffic to R1 1 crypto map VPN 10 ipsec-isakmp set peer 136.1.0.1 set transform-set 3DES_MD5_TRANS match address R3_TO_R1 I interface Serial 1/0 crypto map VPN VPN Routing: R1: router eigrp 100 no auto-summary network 12.12.12.0 0.0.0.255 network 13.13.13.0 0.0.0.255 network 192.168.1.0 0.0.0.255 R2: router eigrp 100 no auto-summary network 12.12.12.0 0.0.0.255 network 192.168.2.0 0.0.0.255 R3: router eigrp 100 no auto-summary network 13.13.13.0 0.0.0.255 network 192.168.3.0 0.0.0.255

Verification

R1#**show ip eigrp neighbors** IP-EIGRP neighbors for process 100 Interface Hold Uptime SRTT RTO Q Seq H Address Type (ms) Cnt Num 2:17 92 5000 0 13 (sec) Cnt Num 10 00:12:17 92 5000 0 13 11 00:16:21 113 5000 0 11 12.12.12.2 Tu0 1 0 13.13.13.3 Tul R1#**show crypto isakmp sa**
 src
 state

 136.1.0.1
 QM_IDLE

 136.1.0.1
 QM_IDLE
 conn-id slot dst src 136.1.0.2 45 0 136.1.0.3 44 0 R3#ping 192.168.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 76/76/80 ms R1#show crypto ipsec sa interface: Serial0/0 Crypto map tag: VPN, local addr. 136.1.0.1

Copyright © 2007 Internetwork Expert

```
protected vrf:
local ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
current_peer: 136.1.0.2:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 121, #pkts encrypt: 121, #pkts digest 121
 #pkts decaps: 120, #pkts decrypt: 120, #pkts verify 120
 #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.: 136.1.0.1, remote crypto endpt.: 136.1.0.2
  path mtu 1500, media mtu 1500
  current outbound spi: 15AF12C4
  inbound esp sas:
   spi: 0x2A1EEF14(706670356)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2002, flow_id: 3, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4382403/3058)
     IV size: 8 bytes
     replay detection support: Y
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x15AF12C4(363795140)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2003, flow_id: 4, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4382403/3058)
     IV size: 8 bytes
     replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
protected vrf:
local ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
current_peer: 136.1.0.3:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 118, #pkts encrypt: 118, #pkts digest 118
 #pkts decaps: 117, #pkts decrypt: 117, #pkts verify 117
 #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.: 136.1.0.1, remote crypto endpt.: 136.1.0.3
  path mtu 1500, media mtu 1500
  current outbound spi: C50B2425
  inbound esp sas:
   spi: 0x6DB01774(1840256884)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
```

```
Copyright © 2007 Internetwork Expert
```

```
sa timing: remaining key lifetime (k/sec): (4399740/3055)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xC50B2425(3305841701)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
sa timing: remaining key lifetime (k/sec): (4399740/3052)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

GRE over IPSec with EIGRP to Route Through a Hub and Multiple Remote Sites

GRE Tunnels over IPsec with Crypto Profiles

Objective: Configure GRE tunnels and encrypt them using crypto profiles.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"DMVPN"</u>.
- Configure GRE tunnels between R2 and R1, R1 and R3 as follows:
 - Use Loopback0 interface as tunnel sources.
 - Use IP addresses from subnet 12.12.12.0/24 for R1/R2.
 - Use IP addresses from subnet 13.13.13.0/24 for R1/R3.
- The difference with profiles is that IPsec is initiated from Loopbacks, hence you need to configure ISAKMP keys for Loopback addresses.
- Configure R1 for encryption of Tunnel0 as follows:

- Create ISAKMP policy with priority 10 as follows:
 - Use 3DES/MD5 as cipher/hash.
 - Use pre-shared keys authentication.
- Create ISAKMP key CISCO for host 150.X.2.2.
- Create IPsec transform-set 3DES_MD5_TRANS as follows:
 - Use 3DES cipher.
 - Use MD5 hash.
 - Use transport mode for minimum overhead.
- Create crypto profile VPN as follows:
 - Apply transform set 3DES_MD5_TRANS.
- Apply crypto profile VPN to Tunnel0.
- Configure encryption of Tunnel1 (R1-R3) on R1 the same way:
 - Create ISAKMP key CISCO for host 150.X.2.2.
 - Apply crypto profile VPN to Tunnel1.
- Configure R2 and R3 to mirror R1's configuration.
- Configure VPN routing as follows:
 - Enable EIGRP process 100 on R1, R2, R3:
 - Include networks 12.12.12.0/24 and 13.13.13.0/24 into EIGRP.
 - Include Loopback1 interfaces into EIGRP.

Final Configuration

```
Tunnels & IPsec:
R1:
!
!
Tunnel to R2
!
interface Tunnel0
tunnel source Loopback0
tunnel destination 150.1.2.2
ip address 12.12.12.1 255.255.255.0
!
! Tunnel to R3
!
interface Tunnel1
tunnel source Loopback0
```

Copyright © 2007 Internetwork Expert
```
tunnel destination 150.1.3.3
 ip address 13.13.13.1 255.255.255.0
T
! ISAKMP policy
1
crypto isakmp policy 10
auth pre-share
 encr 3des
hash md5
!
! Pre-shared keys
!
crypto isakmp key CISCO address 150.1.3.3
crypto isakmp key CISCO address 150.1.2.2
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Create IPsec profile
1
crypto ipsec profile VPN
  set transform-set 3DES_MD5_TRANS
!
! Apply crypto profile to tunnels
!
interface Tunnel0
tunnel protection ipsec profile VPN
!
interface Tunnel1
tunnel protection ipsec profile VPN
R2:
1
! Tunnel to R1
!
interface Tunnel0
 tunnel source Loopback0
tunnel destination 150.1.1.1
ip address 12.12.12.2 255.255.255.0
!
! ISAKMP policy
1
crypto isakmp policy 10
auth pre-share
 encr 3des
hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
1
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
1
! Create IPsec profile
!
crypto ipsec profile VPN
  set transform-set 3DES_MD5_TRANS
```

Copyright © 2007 Internetwork Expert

```
! Apply crypto profile to tunnels
!
interface Tunnel0
tunnel protection ipsec profile VPN
R3:
!
! Tunnel to R1
I
interface Tunnel0
tunnel source Loopback0
tunnel destination 150.1.1.1
ip address 13.13.13.3 255.255.255.0
!
! ISAKMP policy
!
crypto isakmp policy 10
auth pre-share
encr 3des
hash md5
!
! Pre-shared key
!
crypto isakmp key CISCO address 150.1.1.1
!
! Transform-set
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5-hmac
 mode transport
!
! Create IPsec profile
!
crypto ipsec profile VPN
 set transform-set 3DES_MD5_TRANS
1
! Apply crypto profile to tunnels
!
interface Tunnel0
tunnel protection ipsec profile VPN
VPN Routing:
R1:
router eigrp 100
no auto-summary
network 12.12.12.0 0.0.0.255
network 13.13.13.0 0.0.0.255
network 192.168.1.0 0.0.0.255
R2:
router eigrp 100
no auto-summary
network 12.12.12.0 0.0.0.255
network 192.168.2.0 0.0.0.255
R3:
router eigrp 100
no auto-summary
network 13.13.13.0 0.0.0.255
network 192.168.3.0 0.0.0.255
```

Verification

R1#**show ip eigrp neighbors** IP-EIGRP neighbors for process 100 H Address Interface Hold Uptime SRTT RTO Q Seq Type (sec) (ms) Cnt Num 1 13.13.13.3 Tu1 12 00:01:34 261 5000 0 5 73 5000 0 13 00:01:47 7 0 12.12.12.2 Tu0 R1#show ip ro ei 192.168.2.0/24 [90/297372416] via 12.12.12.2, 00:01:52, Tunnel0 192.168.3.0/24 [90/297372416] via 13.13.13.3, 00:01:38, Tunnel1 D D R1#**sho crypto isakmp sa** conn-id slot dst state src QM_IDLE 150.1.1.1 150.1.3.3 4 0 150.1.2.2 150.1.1.1 3 0 QM_IDLE R3#ping 192.168.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 68/69/72 ms R1#show crypto ipsec sa interface: Tunnel0 Crypto map tag: Tunnel0-head-0, local addr. 150.1.1.1 protected vrf: local ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0) current_peer: 150.1.2.2:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 32, #pkts encrypt: 32, #pkts digest 32 #pkts decaps: 33, #pkts decrypt: 33, #pkts verify 33 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 225, #recv errors 0 local crypto endpt.: 150.1.1.1, remote crypto endpt.: 150.1.2.2 path mtu 1500, media mtu 1500 current outbound spi: 60AAA69E inbound esp sas: spi: 0xFD7661D(265774621) transform: esp-3des esp-md5-hmac , in use settings ={Transport, } slot: 0, conn id: 2000, flow_id: 1, crypto map: Tunnel0-head-0 sa timing: remaining key lifetime (k/sec): (4532966/3472) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas:

Copyright © 2007 Internetwork Expert

```
spi: 0x60AAA69E(1621796510)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Transport, }
       slot: 0, conn id: 2001, flow_id: 2, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4532966/3472)
       IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
interface: Tunnell
   Crypto map tag: Tunnel1-head-0, local addr. 150.1.1.1
  protected vrf:
  local ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
   current_peer: 150.1.3.3:500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 31, #pkts encrypt: 31, #pkts digest 31
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify 30
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 225, #recv errors 0
    local crypto endpt.: 150.1.1.1, remote crypto endpt.: 150.1.3.3
    path mtu 1500, media mtu 1500
    current outbound spi: A1C5A428
    inbound esp sas:
     spi: 0xD0532A43(3495111235)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Transport, }
       slot: 0, conn id: 2002, flow_id: 3, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4402696/3481)
       IV size: 8 bytes
       replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     spi: 0xA1C5A428(2714084392)
       transform: esp-3des esp-md5-hmac ,
       in use settings ={Transport, }
       slot: 0, conn id: 2003, flow_id: 4, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4402696/3481)
        IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
```

Further Reading

GRE over IPSec with EIGRP to Route Through a Hub and Multiple Remote Sites

DMVPN with PSK

Objective: Configure Dynamic Multopoint VPN with EIGRP routing.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"DMVPN"</u>.
- The key idea behind DMVPN is to use NHRP for dynamic next-hop resolution, and establish direct spoke-to-spoke tunnels on demand, as opposed to "static" Hub-And-Spoke model.
- NHRP uses client-server model, where server (usually the hub router) responds to NHRP next-hop queries, providing spokes with "best" next-hop available.
- NHRP is used in combination with multipoint GRE encapsulation, thereby allowing a tunnel to be connected to multiple remote endpoints simultaneously.
- Multipoint GRE is combined with IPsec profiles to allow for dynamic IPsec session establishment. Altogether mGRE+NHRP+IPsec provides the three building blocks of DMVPN technology.

- Create Tunnel0 interfaces at R1, R2, R3 as follows:
 - Use multipoint GRE encapsulation.
 - Use tunnel source Loopback0.
 - o Use tunnel key 123.
 - Use addresses 123.123.123.Y/24 where Y is router number.
 - Configure bandwidth of 1024Kbps (to override defaults).
 - Configure delay value of 100.
- Configure common NHRP settings on R1, R2, R3 as follows:
 - o Use network-id 123.
 - Use authentication-key "CISCO".
 - Use Hold-Time of 60 seconds.
- Configure IPsec at Hub & Spokes router as follows:
 - Create ISAKMP policy.
 - o Configure wildcard pre-shared key "CISCO".
 - Create IPsec transform-set 3DES_MD5_TRANS as follows:
 - Encryption 3DES.
 - Hash MD5.
 - Mode Transport.
 - Create IPsec Profile DMVPN as follows:
 - Apply transform-set 3DES_MD5_TRANS.
 - Apply IPsec Profile DMVPN to Tunnel0 interfaces.
- Configure NHRP specific settings for R1 (Hub) as follows:
 - Map multicast traffic to dynamic NHRP entries.
- Configure NHRP specific settings for R2, R3 (Spokes) as follows:
 - Map 123.123.123.1 to 150.X.1.1
 - Map multicast to 150.X.1.1.
 - Use 123.123.123.1 as NHS server.
- Configure EIGRP 100 for VPN routing on R1, R2, R3 as follows:
 - o Include network 123.123.123.0/24.
 - o Include networks 192.168.Y.0/24 on R2, and R3.
 - Disable EIGRP split horizon on interface Tunnel0 of R1.

Final Configuration

```
R1:
crypto isakmp policy 10
auth pre-share
encr 3des
hash md5
! Wildcard pre-shared key to authenticate any valid peer
1
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
! Transport mode transform-set
1
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
 mode tunnel
!
! IPsec profile
!
crypto ipsec profile DMVPN
 set transform 3DES_MD5_TRANS
1
! DMVPN Hub
I
interface Tunnel0
 ip address 123.123.123.1 255.255.255.0
tunnel source Loopback0
tunnel mode gre multi
tunnel key 123
 ip nhrp network-id 123
ip nhrp authentication CISCO
 ip nhrp hold 30
ip nhrp map multicast dynamic
 1
 ! Override default bw/delay for tunnel
 1
bandwidth 1024
 delay 100
 !
! Apply IPsec
 !
tunnel protection ipsec profile DMVPN
R2:
crypto isakmp policy 10
auth pre-share
encr 3des
hash md5
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
 mode tunnel
1
crypto ipsec profile DMVPN
  set transform 3DES_MD5_TRANS
1
! DMVPN Spoke
1
interface Tunnel0
ip address 123.123.123.2 255.255.255.0
```

Copyright © 2007 Internetwork Expert

```
tunnel source Loopback0
 tunnel mode gre multi
 tunnel key 123
 ip nhrp network-id 123
 ip nhrp authentication CISCO
 ip nhrp hold 30
 ip nhrp map 123.123.123.1 150.1.1.1
 ip nhrp map multicast 150.1.1.1
 ip nhrp nhs 123.123.123.1
 1
 ! Override default bw/delay for tunnel
 bandwidth 1024
 delay 100
 !
 tunnel protection ipsec profile DMVPN
R3:
crypto isakmp policy 10
auth pre-share
 encr 3des
hash md5
!
crypto isakmp key CISCO address 0.0.0.0 0.0.0.0
1
crypto ipsec transform-set 3DES_MD5_TRANS esp-3des esp-md5
 mode tunnel
!
crypto ipsec profile DMVPN
  set transform 3DES_MD5_TRANS
I
! DMVPN Spoke
interface Tunnel0
 ip address 123.123.123.3 255.255.255.0
 tunnel source Loopback0
 tunnel mode gre multi
 tunnel key 123
 ip nhrp network-id 123
 ip nhrp authentication CISCO
 ip nhrp hold 30
 ip nhrp map 123.123.123.1 150.1.1.1
 ip nhrp map multicast 150.1.1.1
 ip nhrp nhs 123.123.123.1
 ! Override default bw/delay for tunnel
 bandwidth 1024
 delay 100
 1
 tunnel protection ipsec profile DMVPN
VPN Routing:
R1:
router eigrp 100
no auto-summarv
network 123.123.123.0 0.0.0.255
network 192.168.1.0 0.0.0.255
interface Tunnel0
no ip split-horizon eigrp 100
```

```
R2:
router eigrp 100
no auto-summary
network 123.123.123.0 0.0.0.255
network 192.168.2.0 0.0.0.255
```

no auto-summary network 123.123.123.0 0.0.0.255 network 192.168.3.0 0.0.0.255

Verification

R1#**show ip eigrp neighbors** IP-EIGRP neighbors for process 100 H Address Interface Hold Uptime SRTT RTO Q Seq Type (sec) (ms) Cnt Num 1 123.123.123.3 Tu0 12 00:01:22 56 336 0 2 17 123.123.123.2 200 0 3 12 00:01:33 0 Tu0 R1#show ip nhrp 123.123.123.2/32 via 123.123.123.2, Tunnel0 created 00:35:30, expire 00:00:12 Type: dynamic, Flags: authoritative unique registered NBMA address: 150.1.2.2 123.123.123.3/32 via 123.123.123.3, Tunnel0 created 00:35:10, expire 00:00:13 Type: dynamic, <u>Flags: authoritative unique registered used</u> NBMA address: 150.1.3.3 R2#show ip eigrp neighbors IP-EIGRP neighbors for process 100 Address Interface Hold Uptime SRTT Н RTO O Seq Type (sec) (ms) Cnt Num 123.123.123.1 10 00:01:44 20 200 0 4 0 T110 R2#show ip route eigrp 192.168.1.0/24 [90/2653440] via 123.123.123.1, 00:01:49, Tunnel0 D D 192.168.3.0/24 [90/2679040] via 123.123.123.1, 00:01:41, Tunnel0 R2#ping 192.168.1.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 16/17/20 ms R2#ping 192.168.3.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds: ..!!! Success rate is 60 percent (3/5), round-trip min/avg/max = 76/77/80 ms R2#show ip nhrp 123.123.123.1/32 via 123.123.1, Tunnel0 created 00:35:05, never expire Type: static, Flags: authoritative used NBMA address: 150.1.1.1 192.168.3.0/24 via 192.168.3.3, Tunnel0 created 00:00:00, expire 00:00:29

Copyright © 2007 Internetwork Expert

Type: dynamic, Flags: router unique NBMA address: 150.1.3.3 R2#show crypto isakmp sa conn-id slot dst state src 150.1.2.2 150.1.3.3 QM_IDLE 2 0 1 150.1.1.1 150.1.2.2 QM_IDLE 0 R2#ping 192.168.3.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 68/72/80 ms R2#show cry ips sa interface: Tunnel0 Crypto map tag: Tunnel0-head-0, local addr. 150.1.2.2 protected vrf: local ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (150.1.1.1/255.255.255.255/47/0) current_peer: 150.1.1.1:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11 #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7 #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.: 150.1.2.2, remote crypto endpt.: 150.1.1.1 path mtu 1500, media mtu 1500 current outbound spi: 52678822 inbound esp sas: spi: 0xC26D47B9(3261941689) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2004, flow_id: 5, crypto map: Tunnel0-head-0 sa timing: remaining key lifetime (k/sec): (4564366/3567) IV size: 8 bytes replay detection support: Y spi: 0x9A04BA4D(2584001101) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2006, flow_id: 7, crypto map: Tunnel0-head-0 sa timing: remaining key lifetime (k/sec): (4579606/3567) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xD33C8295(3543958165) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2005, flow_id: 6, crypto map: Tunnel0-head-0 sa timing: remaining key lifetime (k/sec): (4564366/3567) IV size: 8 bytes

Copyright © 2007 Internetwork Expert

```
replay detection support: Y
   spi: 0x52678822(1382516770)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2007, flow_id: 8, crypto map: Tunnel0-head-0
     sa timing: remaining key lifetime (k/sec): (4579606/3565)
     IV size: 8 bytes
     replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
protected vrf:
local ident (addr/mask/prot/port): (150.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (150.1.3.3/255.255.255.255/47/0)
current_peer: 150.1.3.3:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
 #pkts decaps: 8, #pkts decrypt: 8, #pkts verify 8
 #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.: 150.1.2.2, remote crypto endpt.: 150.1.3.3
  path mtu 1500, media mtu 1500
  current outbound spi: 138EA870
  inbound esp sas:
   spi: 0x50C4E27E(1355080318)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2008, flow_id: 9, crypto map: Tunnel0-head-0
     sa timing: remaining key lifetime (k/sec): (4592139/3581)
     IV size: 8 bytes
     replay detection support: Y
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x138EA870(328116336)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2009, flow_id: 10, crypto map: Tunnel0-head-0
     sa timing: remaining key lifetime (k/sec): (4592140/3579)
     IV size: 8 bytes
     replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
```

Further Reading

Dynamic Multipoint VPN (DMVPN)

Copyright © 2007 Internetwork Expert

Easy VPN

VPN3k and Cisco VPN Client

Objective: Configure VPN3k to accept remote VPN Client connections.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"VPN3k ezVPN"</u>.
- Create new Group on VPN 3000 Concentrator as follows:
 - Name EZVPN password CISCO.
 - o Configure IPsec as the only tunneling protocol.
 - Configure IPsec Remote Access Tunnel Type.
 - o Configure IPsec Xauth.
- Assign Address Pool "20.0.0.1-20.0.0.254" to group EZVPN.
- Create new User on VPN 3000:
 - Name CISCO password CISCO1234

- o Group EZVPN
- Permit address allocation from Address Pools.
- Configure Cisco VPN Client to connect to VPN3000.

Final Configuration

VPN3k:

Create new group:

🤌 Cisco S	iystems, l	Inc. ¥PN 30	000 Conce	ntrator [Vi	PN3k] - Microsoft Interr	net Explorer		_ 🗆 ×	
<u>Eile E</u> dit	t <u>V</u> iew	F <u>a</u> vorites	<u>I</u> ools <u>H</u>	<u>t</u> elp 🛟	= Back 🔹 🖘 🔹 🚺	Address	🕘 https://136.1.113.11/access.html	-	
	211/	VI	PN 300	00			Main Help	Support Logout	
	F	Co	oncent	rator S	eries Manager			Logged in: admin	
					Ű		Configuration Administ	tration Monitoring	
	<u>uration</u>								
	faces em			Contigurat	tion User Managemo	ent Groups	s Add		
	<u>r Managem</u>	ent .	Т	his section	n lets vou add a groun	Check the	• Inherit? box to set a field that	you want to	
	lase Group	-95 8)	đ	lefault to the	he base group value. T	Jncheck the	e Inherit? box and enter a new v	value to	
	Jse <u>rs</u>		0	verride ba	ase group values.				
- Delic	y Manager	<u>nent</u>							
-⊞- <u>Hunn</u>	<u>teling and S</u> istration	<u>Security</u>		ldentity 📗	General IPSec Cli	ent Config	Client FW HW Client PPTP	/L2TP WebVPN	
- Monito	ring		-			Iden	ntity Parameters		
				Attribute	Value	Description			
				Grou Nam	P EZVPN	Enter a uni	ique name for the group.		
				Passwor	d www	Enter the password for the group.			
				Verif	y	Verify the group's password.			
				Тур	e Internal 💌	<i>External g</i> (e.g. RAD Concentra	groups are configured on an exte IUS). <i>Internal g</i> roups are config tor's Internal Database.	rnal authentication se gured on the VPN 3	
			[Add	Cancel				
	Cisco Sy	STEMS	<u>.</u>						
🤌 Group F	Parameters						🔒 🔮 Iı	nternet //	

CCIE Security Lab Workbook Volume I Version 3.0

<u>Fi</u> le <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	s <u>H</u> elp (⇔ Back → ==	> - 😢 🔂	Address 🙆 https://136.1.113.11	/access.html
VPN	3000			Main Help Support Logou
Conc	entrator series w	lanager	Configuration	Logged in: admi
	1 × P			primary DNS server.
<u> </u>	Secondary DNS			Enter the IP address of the secondary DNS server.
Base Group <u>Groups</u>	Primary WINS			Enter the IP address of the primary WINS server.
Users <u>Users</u> <u>Users</u> <u>Users</u> <u>Users</u> <u>Users</u>	Secondary WINS		N	Enter the IP address of the secondary WINS server.
<u>-urrunneung and Security</u> B <u>Administration</u> B <u>Monitoring</u>	Tunneling Protocols	PPTP L2TP IPSec L2TP over IP WebVPN	Sec	Select the tunneling proto group can connect with.
	Strip Realm 🗖		<u>ज</u>	Check to remove the rea qualifier of the username authentication.
	DHCP Network Scope		ন	Enter the IP sub-network which users within this gr- be assigned when using th concentrator as a DHCP
CISCO SYSTEMS	Add Can	cel		

Permit IPsec as the only tunneling protocol in General Tab:

CCIE Security Lab Workbook Volume I Version 3.0

Make sure you group have "Remote Access" IPSec "Tunnel type":

Lisco Systems, Inc. VPN 3000 Lo	ncentrator [¥PN3k] - Mi	icrosoft Interne	t Explorer		_ 0
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🔹	=> • 💌 🛃	Address 🙋 https://136	5.1.113.11/access.ht	ml 🗾 🦉
🐔 🗐 VPN 3	3000			Main H	elp Support Logou
Conce	ntrator Series I	Manager			Logged in: adm
			Confi	guration Admii	nistration Monitorin
<u>Configuration</u> <u>Interfaces</u>	override base group	values.			
	Identity General	IPSec Clier	nt Config Client FW	HW Client PP	TP/L2TP WebVPN
Base Group Croups			IPSec Parar	neters	
Users	Attribute		Value	Inherit?	Descripti
Helicy Management Helicy Management Helicy Management Helicy Management	IPSec SA	ESP-3DES-M	D5 🗾		Select the group's II Security Association
<u>-Administration</u> B <u>Monitoring</u>	IKE Peer Identity Validation	If supported by	y certificate 💌	N	Select whether or no validate the identity using the peer's cert
	IKE Keepalives	N			Check to enable the keepalives for memł group.
	Confidence Interval	300		ম	(seconds) Enter hov peer is permitted to the VPN Concentra to see if it is still con
CISCO SYSTEMS	Tunnel Type	Remote Acce	ss 💌	ম	Select the type of tu group. Update the F Access parameters needed.

<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🕶 ==	> - 🕑 🚺 🔺	dress 🖉 https://136.1.11	3.11/access.htm	n 🔽 🎬
VPN 3	000			Main He	lp Support Logoı
🧏 🕂 💋 Conce	ntrator Series N	lanager			Logged in: adm
			Configura	tion Admin	istration Monitorin
Configuration					parameters below_ needed.
— <u>⊞-System</u> —⊟User Manaαement		R	emote Access Param	eters	
Base Group	Group Lock				Lock users into thi
Groups Users Delicy Management Dunneling and Security Administration Monitoring	Authentication	Internal	×	N	Select the authenti method for membe this group. This pa does not apply to Individual User Authentication.
	Authorization Type	None		ঘ	If members of this need authorization addition to authent select an authoriza method. If you cor this field, you must configure an Autho Server.
	Authorization Required			ঘ	Check to require successful authoriz
Cisco Systems					For certificate-bas users select the su

And that you have authentication (Xauth) enabled in IPsec Tab:

🗿 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer	
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 🔹 🖘 🚽 🔕 🚯	Address 🛃 https://136.1.113	3.11/access.html
VPN 3	000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configura	tion Administration Monitoring
- <u>Configuration</u>	Configuration User Managemer	nt Groups Address Pools	
<u></u> -⊕- <u>Sγstem</u>		and the second second	Save Needed 🗖
Huser Management Base Group Groups Users	This section lets you configure $\mathrm{I\!P}$.	Address Pools.	
	Click the Add button to add a poor Move . Click Done to finish.	ol entry, or select a range an	d click Modify, Delete or
- III Monitoring	А	ddress Pool for EZVPN	
	IP	Pool Entry Actions	
		Empty — Add	
		Modify	
		Delete	
		Delete	
		Move Up	
		Move Down	
		Done	
Cisco Systems			
Filters and Access Policies			📄 🤮 Internet 🏼 🎢

Modify address pools for a Group:

CCIE Security Lab Workbook Volume I Version 3.0

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer				
<u>File Edit Yiew Favorites T</u> ools	Help 🗘 Back 🔹 🖘 👻 😰	Address 🖉 https://136.1.113.11/access.html				
VPN 3	3000	Main Help Support Log				
Conce	ntrator Series Manager	Logged in: adm				
		Configuration Administration Monitorin				
<u>Configuration</u>	Configuration User Managemen	t Groups Address Pools Add				
	Add an address pool.					
	Range Start 20.0.0.1	Enter the start of the IP pool address range.				
<u>⊡Policy Management</u> <u>⊡</u> Tunneling and Security	Range End 20.0.0.254	Enter the end of the IP pool address range.				
-⊞Administration -⊞Monitoring	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.				
Cisco Systems	Add Cancel					
Filters and Access Policies		📄 📄 🔮 Internet				

CCIE Security Lab Workbook Volume I Version 3.0

Add new user "CISCO/CISCO1234" to the group "EZVPN":

🗿 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer 📃 🔀									
<u>File Edit View Favorites Tools</u>	Help 🗘 🖙 Ba	ick 🔹 🔿 🔹 🚺	Address 🔊 https://136.1.113.11/access.html	-					
VPN 3	000		Main Help S	Support Logout					
Concer	trator Ser	ies Manager	L	ogged in: admin					
Configuration Administration Monitoring									
- Configuration	C C	111 M							
Interfaces	Configuration	i User Manageme	nt Users Add						
	This section le	ts vou add a user. T	Jncheck the Inherit? box and enter a new va	due to					
Base Group	override group	values.							
Users									
Policy Management	Identity Ge	neral IPSec PP1	(P/L2TP						
	1	1	dentity Parameters						
-# <u>Monitoring</u>	Attribute	Value	Description						
	Username	CISCO	Enter a unique username.						
	Password	Jelekolakakak	Enter the user's password. The password m the group password requirements.	ust satisfy					
	Verify	kolololololok	Verify the user's password.						
	Group	EZVPN 🔽	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.						
	Add	Cancel							
Cisco Systems	10 U								
🕗 User Parameters			📄 🚺 🚺 Inter	rnet //					

Allow IP address Assignment from Address Pools:



Verification
Configure Cisco VPN Client on Test PC, use key "CISCO":
👌 ¥PN Client Create New ¥PN Connection Entry
Connection Entry: EZVPN
Host: 136.1.113.11
Authentication Transport Backup Servers Dial-Up
Name: EZVPN
Password:
C <u>o</u> nfirm Password: *****
C Certificate Authentication
Name:
Send CA Certificate Chain
Erase User Password Save Cancel
Connect the VPN Client and enter CISCO/CISCO1234 when prompted for Xauth.

🖉 Cisco Systems, Inc. VPN 3000 Conce	entrator [¥PN3	3k] - Microsoft In	ternet Exp	olorer				_ [X
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 B	ack 🔹 🖘 💌 💌	A	ddress 🙋 http	s://136.1.11	3.11/access.htm	ป	-	9
VPN 30	00					Main He	lp Supp	oort Log	out
Concent	trator Sei	ries Manag	ger				Logg	ed in: ad	min
	.			- 1	Configurat -	tion Admin	istration	Monitor	ing
<u>Configuration</u> <u>Interfaces</u> 	Active Tota	al Active Total	Active 7	Fotal Active	e Total	Active Tot	al Activ	e Total	
			U	0 0	U		1	1	
Base Group Groups									
	LAN-to-I	AN Session	s	[<u>Remote Ac</u>	cess Sessi	ons <u>Manag</u> e	ement Se	ssions]	
Tunneling and Security	Connectio Name	on IP Address	Protocol	Encryption	Login Time	Duration]	Bytes Tx	Bytes Rx	
<u>Monitoring</u> <u>Routing Table</u>	No LAN-to-LAN Sessions								
<u>Dynamic Filters</u> <u>Filterable Event Log</u>								50	
	Remote A	ccess Sessio	ns	[LAN-to-I	AN Sessi	ons Manage	ement Se	ssions]	
	<u>Username</u>	Assigned IP Address Public IP Address	<u>Group</u>	<u>Protocol</u> Encryption	Login Time <u>Duration</u>	<u>Client</u> <u>Type</u> <u>Version</u>	<u>Bytes</u> <u>Tx</u> <u>Bytes</u> <u>Rx</u>	<u>NAC</u> <u>Result</u> <u>Posture</u> <u>Token</u>	
	<u>CISCO</u>	20.0.0.1 136.1.100.200	EZVPN	IPSec 3DES-168	Jan 18 1:14:37 0:02:21	WinNT 4.8.01.0300	2880 6232	N/A	
CISCO SYSTEMS								J	- -
Essions							Internet		1.

Verify connected Remote Sessions at VPN3k:

CCIE Security Lab Workbook Volume I Version 3.0

<u>-</u> <u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help ⇔ Back • ⇒	🔹 🕑 🛛 🖂 Address 🖉 htt	ps://136.1.113.11/access.ht	ml 🔄			
VPN 3 Concer	000 ntrator Series M	anager	Main H	elp Support Logo Logged in: adm			
			Configuration Admir	nistration Monitorir			
Configuration Interfaces		IKE Sessi	on				
- EP- <u>System</u> 	Session ID	1	Encryption Algorithm	3DES-168			
Groups Users GPolicy Management	Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024- bit)			
<u>Terrent and Security</u>	Authentication Mode	Pre-Shared Keys (XAUTH)	IKE Negotiation Mode	Aggressive			
- <u>Monitoring</u> <u>Routing Table</u> <u>Dynamic Filters</u>	Rekey Time Interval	86400 seconds					
—⊞ <u>Filterable Event Loq</u> —⊞Svstem Status	IPSec Session						
	Session ID	2	Remote Address	20.0.0.1			
	Local Address	0.0.0.0/255.255.255.255	Encryption Algorithm	3DES-168			
—⊕ <u>Statistics</u>	Hashing Algorithm	MD5	Idle Time	0:00:17			
	Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds			
CISCO SYSTEMS	Bytes Received	7664	Bytes Transmitted	3648			
	<u></u>						

Further Reading

IPsec with VPN Client to VPN 3000 Concentrator Configuration Example

VPN3k and Cisco VPN Client with Split-Tunneling

Objective: Configure VPN3k and Cisco VPN Client for split-tunneling.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco VPN Client".</u>
- The goal to encrypt only traffic from client to network 136.1.111.0/24.
- First, create network list to distinguish network 136.1.111.0/24, name it SPLIT_TUNNEL.
- Next, modify group EZVPN, changing split-tunneling settings under "Client Config" Tab.

Final Configuration

VPN3k:

Create Network List for split-tunneling:

🖉 Cisco Systems, Inc. ¥PN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer 📃 🗆 🗙
<u>File Edit View Favorites Tools</u>	; Help 🗘 🖙 Back 🔹 🖘 👻 🛃	Address 🕘 https://136.1.113.11/access.html
VPN :	3000	Main Help Support Logout
Conce	intrator series Manager	Logged in: admin
		Configuration Administration Monitoring
	Configuration Doligy Manageme	ent Troffie Monagement Notwork jets Medify
	Configuration Policy Manageme	ent Trainc Management Network Lists Mouny
	Modify a configured Network List list based on routing entries on the	. Click on Generate Local List to generate a network Private interface.
	List Name SPLIT_TUNNEL	Name of the Network List you are adding. The name must be unique.
		 Enter the Networks and Wildcard masks using the following format:
		n.n.n.n/n.n.n.n (e.g.
- <u> - H</u> <u> Administration</u>		10.10.0.0/0.0.255.255).
		• Note: Enter a
Casaa Suorrus	136.1.111.0/0.	.0.0.255
CISCO OTSIEMS	INetwork List	match. For example,
		10.10.1.0/0.0.255 =
Network Lists		🔒 🔮 Internet

Modify group "EZVPN", "Client Config" Tab. Chose "Only tunnel networks in the list":

🚰 Cisco Systems, Inc. VPN 3000	Concentrator [VPN3	k] - Microsoft Internet Explorer		
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ols <u>H</u> elp 🗘 B	ack 🔹 🖘 👻 🚱 🛛 🗚 Address 🖉 https://1	36.1.113.11/	access.html 🔄 🌆
VPN	3000		M	lain Help Support Logout
Conc	centrator Ser	ries Manager		Logged in: admin
		Cun	figuration	Administration Monitoring
- <u>Configuration</u> - <u>Interfaces</u>			-	
Duser Management Duser Management Duser Management Duser Management Dusers Dusers	Split Tunneling Policy	 Tunnel everything Allow the networks in list to bypass the tunnel Only tunnel networks in the list 		Select the method and net to be used for Split Tunnel Tunnel Everything: Sen- traffic through the tunnel. Allow the networks in th bypass the tunnel: The V Client may choose to send to addresses in this list to t client's LAN. Send all oth
	Split Tunneling Network List	-None- -None- VPN Client Local LAN (Default) SPLIT_TUNNEL	R	through the tunnel. NOTE setting only applies to the VPN Client. Tunnel networks in the Send traffic to addresses i through the tunnel. Send a traffic to the client's LAN.
CISCO SYSTEMS	Default Domain Name			Enter the default domain n given to users of this group
autilitus autilitus.				Enter the set of domains,
🛃 Group Parameters				🔒 🔮 Internet 🥢

ct Cisco VPN Client	t on Test PC	? :	
👌 VPN Client	User Auther	ntication for "EZ¥PN"	X
Enter Usernam	e and Password.		
CISCO SYSTE	NS <u>U</u> sername:		
		ОК	Cancel
VPN Client Statist	tics:		
A VPN Client	Statistics		X
State of the second			
Tunnel Details	Route Details	Firewall	
Tunnel Details Address Info	Route Details	Firewall Connection Informat	ion
Tunnel Details Address Info Client Server	Route Details	Firewall Connection Informati Entry: Time:	ion EZVPN 0.dau(s).00:00.41
Tunnel Details Address Info Client: Server: Bytes	Route Details rmation 20.0.0.1 136.1.113.11	Firewall Connection Informat Entry: Time: Crypto	ion EZVPN 0 day(s), 00:00.41
Tunnel Details Address Info Client: Server: Bytes Received: Sent:	Route Details mation 20.0.0.1 136.1.113.11 0 0	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication:	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5
Tunnel Details Address Info Client: Server: Bytes Received: Sent: Packets	Route Details 700.0.0.1 136.1.113.11 0 0	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transport	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5
Tunnel Details Address Info Client Server: Bytes Received: Sent: Packets Encrypted Decrypted	Route Details	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transport Transparent Tunneli Local LAN:	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5 ng:Inactive Disabled
Tunnel Details Address Info Client: Server: Bytes Received: Sent: Packets Encrypted Decrypted Discarded: Bypassed:	Route Details 20.0.0.1 136.1.113.11 0 0 0 0 :0 :0 :4 332	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transport Transparent Tunneli Local LAN: Compression:	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5 ng:Inactive Disabled None
Tunnel Details Address Info Client: Server: Bytes Received: Sent: Packets Encrypted Discarded: Bypassed:	Route Details 20.0.0.1 136.1.113.11 0 0 0 :0 :0 :4 332	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transport Transparent Tunneli Local LAN: Compression:	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5 ng:Inactive Disabled None Reset
Tunnel Details Address Info Client: Server: Bytes Received: Sent: Packets Encrypted Discarded: Bypassed:	Route Details mation 20.0.0.1 136.1.113.11 0 0 0 :0 :4 332	Firewall Connection Informat Entry: Time: Crypto Encryption: Authentication: Transparent Tunneli Local LAN: Compression:	ion EZVPN 0 day(s), 00:00.41 168-bit 3-DES HMAC-MD5 ng:Inactive Disabled None Reset

	👌 VPN Client	Statistics		×		
	Tunnel Details Route Details Firewall					
	Local LAN Routes		Secured Routes			
	Network	Subnet Mask	Network	Subnet Mask		
			136.1.111.0	255.255.255.0		
				Close		
Test connec	ctivity:					
C:\WINNT\s	ystem32\cmd.ex	(e			_ 🗆 ×	
C:\Document Pinging 130 Reply from Reply from Reply from Ping statis Packets Approximato Minimuu C:\Document	ts and Setti 6.1.111.1 wi 136.1.111.1 136.1.111.1 136.1.111.1 stics for 13 s: Sent = 4, e round trip m = Øms, Max ts and Setti	ngs\IEAdmin>ping 1 th 32 bytes of dat : bytes=32 time<14 : bytes=32 time<14 : bytes=32 time<14 : bytes=32 time<14 6.1.111.1: Received = 4, Los times in milli-se imum = Øms, Avera ngs\IEAdmin>_	136.1.111.1 ta: Oms TTL=253 Oms TTL=253 Oms TTL=253 Oms TTL=253 et = 0 (0% loss econds: age = Oms	s),		
-						

VPN3k and Cisco VPN Client with Hold-Down Route

Objective: Configure VPN3k to advertise Hold-Down route via RIP.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco VPN Client with Split Tunneling"</u>.
- The idea of hold-down route is to advertise the network corresponding to the locally configure address pool.
- Remove static default route on R1, and configure RIP routing.
- Note that inbound RIP is enabled by default on VPN3k Private Interface.
- Configure outbound RIPv2 on Private Interface of VPN3k.
- Create Hold-Down routes on VPN3k by generating them based on preconfigured Address-Pools.

Final Configuration

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
router rip
ver 2
no auto
network 136.1.0.0
```

```
VPN3k CLI:
```

Copyright © 2007 Internetwork Expert

Enable RIP outbound on Private Interface: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3k: Main -> 1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5) Tunneling and Security 6) Back VPN3k: Config -> 1 This table shows current IP addresses. Tntf Status IP Address/Subnet Mask MAC Address _____ _____ Ether1-PriUP|136.1.111.11/255.255.255.0|00.03.A0.88.BD.29Ether2-PubUP|136.1.113.11/255.255.255.0|00.03.A0.88.BD.2A _____ DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Power Supplies 4) Back VPN3k: Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static IP) 2) Set Public Interface 3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters 12) Back VPN3k: Ethernet Interface 1 -> 8 1) Set Inbound RIP Options 2) Set Outbound RIP Options 3) Enable/Disable OSPF 4) Set OSPF parameters 5) Back VPN3k: Ethernet Interface 1 -> 1 1) Disable Inbound RIP

Copyright © 2007 Internetwork Expert

```
2) Enable RIP V1 Inbound
3) Enable RIP V2 Inbound
4) Enable RIP V2/V1 Inbound
VPN3k: Ethernet Interface 1 -> [ 4 ]
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 1 -> 2
1) Disable Outbound RIP
2) Enable RIP V1 Outbound
3) Enable RIP V2 Outbound
4) Enable RIP V2/V1 Outbound
VPN3k: Ethernet Interface 1 -> [ 1 ] 4
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 1 ->
```

VPN3k GUI:

Configure Hold-Down Route on VPN3k: Choose "Generate Hold Down Routes":

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Internet	Explorer	_ 🗆 ×					
<u>File Edit View Favorites T</u> ools	Help 🗘 Back 🔹 🖘 👻 😰	Address 🖉 https://136.1.113.11/access.html	-					
VPN 3	3000	Main Help	Support Logout					
Conce	ntrator Series Manager		Logged in: admin					
	<u> </u>	Configuration Administ	ration Monitoring					
			A					
Interfaces	Configuration System IP Routin	g Reverse Route Injection						
U <u>⊕Servers</u>	Configure system-wide <i>Reverse Route Injection</i> parameters. This feature adds specific							
	The Address Management routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path							
Static Routes	discovery. Click on Generate Hol	d Down Routes to generate hold down r	routes based on					
Default Gateways	configured address pools.							
DHCP Parameters			Check to a					
DHCP Relay	Client Reverse Route Injection		interface) c					
Redundancy			table.					
Reverse Route Injection	N. 1 F		Check to a					
Management Protocols	Network Extension		extension c					
	Reverse Route Injection		table.					
□ □ □ □ □ Client Update			• Add					
Load Balancing		20.0.0.0/255.255.255.0	and and					
			follo					
			n.n.1					
- E-Administration	A J J		192.					
- 	Address Pool		Ente					
	Hold Down Routes		subn					
CISCO SYSTEMS			• If yo					
and the south the s		l	mast 🕶					
Reverse Route Injection Configuratio	n	j 🗎 🧶 Ir	nternet //.					

Verification

VPN3k: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3k: Main -> 3 1) Routing Table 2) Event Log 3) System Status 4) Sessions 5) General Statistics 6) Dynamic Filters 7) Back VPN3k: Monitor -> 1 Routing Table _____ Number of Routes: 7 Mask IP Address Next Hop Intf Protocol Age Metric _____ 255.255.255.0 136.1.113.3 2 RIP 17 10.0.0.0 3 20.0.0.0 255.255.255.0 136.1.113.11 2 Static 0 1
 136.1.0.0
 255.255.255.0
 136.1.113.3
 2 RIP

 136.1.23.0
 255.255.255.0
 136.1.113.3
 2 RIP

 136.1.100.0
 255.255.255.0
 136.1.113.3
 2 RIP

 136.1.110.0
 255.255.255.0
 136.1.113.3
 2 RIP

 136.1.110.0
 255.255.255.0
 136.1.113.3
 2 RIP

 136.1.111.0
 255.255.255.0
 0.0.0.0
 1 Local

 136.1.113.0
 255.255.255.0
 0.0.0.0
 2 Local
 17 3 17 2 17 2 1 Local 0 0 1 2 Local 1 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, 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 136.1.0.0/24 is subnetted, 5 subnets 136.1.0.0 [120/3] via 136.1.111.11, 00:00:22, Ethernet0/0 R 136.1.23.0 [120/2] via 136.1.111.11, 00:00:22, Ethernet0/0 R 136.1.111.0 is directly connected, Ethernet0/0 С R 136.1.100.0 [120/2] via 136.1.111.11, 00:00:22, Ethernet0/0 136.1.113.0 [120/1] via 136.1.111.11, 00:00:22, Ethernet0/0 R R 20.0.0.0/8 [120/1] via 136.1.111.11, 00:00:22, Ethernet0/0 10.0.0.0/8 [120/3] via 136.1.111.11, 00:00:22, Ethernet0/0 R R3#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

```
Copyright © 2007 Internetwork Expert
```

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 136.1.0.0/24 is subnetted, 5 subnets R 136.1.0.0 [120/1] via 136.1.23.2, 00:00:24, Serial1/3 С 136.1.23.0 is directly connected, Serial1/3 136.1.111.0 [120/1] via 136.1.113.11, 00:00:10, Ethernet0/0 R С 136.1.100.0 is directly connected, Ethernet0/1 136.1.113.0 is directly connected, Ethernet0/0 20.0.0.0/24 is subnetted, 1 subnets С R 20.0.0.0 [120/1] via 136.1.113.11, 00:00:10, Ethernet0/0 10.0.0/24 is subnetted, 1 subnets 10.0.0.0 [120/1] via 136.1.23.2, 00:00:26, Serial1/3 R Connect VPN Client and ping R1 from Test PC: _ 🗆 × C:\WINNT\system32\cmd.exe * C:\Documents and Settings\IEAdmin>ping 136.1.111.1 Pinging 136.1.111.1 with 32 bytes of data: Reply from 136.1.111.1: bytes=32 time=10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Ping statistics for 136.1.111.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 2ms C:\Documents and Settings\IEAdmin>_

Further Reading

How to Populate Dynamic Routes Using Reverse Route Injection

VPN3k and Cisco VPN Client with RRI

Objective: Configure VPN3k for RRI with OSPF routing.



Directions

- Configure devices as per the scenario " VPN/Easy VPN" <u>"VPN3k and Cisco VPN Client with Split Tunneling"</u>.
- The key point with RRI into OSPF is to configure ASBR feature on the VPN3k, so that it starts advertising external routes into OSPF.
- Remove static default route on R1 and configure OSPF routing as per the diagram.
- Enable OSPF process on VPN3k as follows:
 - Use router-id 150.X.11.11.
 - Permit ASBR feature.
- Enable OSPF on the Private interface of the VPN3k. Use Area 0.

Final Configuration

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
!
router ospf 1
network 136.1.111.0 0.0.0.255 area 0
```

Copyright © 2007 Internetwork Expert
```
VPN3k CLI:
Configure OSPF on the Private Interface:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 2
1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back
VPN3k: System -> 3
1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back
VPN3k: Routing -> 3
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> 2
> Router ID
VPN3k: OSPF -> [ 0.0.0.0 ] 150.1.11.11
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
```

```
VPN3k: OSPF -> 1
1) Enable OSPF
2) Disable OSPF
VPN3k: OSPF -> [ 2 ] 1
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> 3
1) Enable Autonomous System
2) Disable Autonomous System
VPN3k: OSPF -> [ 2 ] 1
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> h
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 1
This table shows current IP addresses.
         Status IP Address/Subnet Mask
 Intf
                                                      MAC Address
 _____
Ether1-PriUP|136.1.111.11/255.255.255.0|00.03.A0.88.BD.29Ether2-PubUP|136.1.113.11/255.255.255.0|00.03.A0.88.BD.2A
         ·
------
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured
1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back
VPN3k: Interfaces -> 1
1) Interface Setting (Disable, DHCP or Static IP)
```

Copyright © 2007 Internetwork Expert

2) Set Public Interface 3) Set Interface Name 4) Select IP Filter 5) Select Ethernet Speed 6) Select Duplex 7) Set MTU 8) Set Port Routing Config 9) Set Bandwidth Management 10) Set Public Interface IPSec Fragmentation Policy 11) Set Interface WebVPN Parameters 12) Back VPN3k: Ethernet Interface 1 -> 8 1) Set Inbound RIP Options 2) Set Outbound RIP Options 3) Enable/Disable OSPF 4) Set OSPF parameters 5) Back VPN3k: Ethernet Interface 1 -> 3 1) Enable OSPF 2) Disable OSPF VPN3k: Ethernet Interface 1 -> [2] 1 1) Set Inbound RIP Options 2) Set Outbound RIP Options 3) Enable/Disable OSPF 4) Set OSPF parameters 5) Back VPN3k: Ethernet Interface 1 -> 4 1) Set OSPF Area ID 2) Set OSPF Priority 3) Set OSPF Metric 4) Set OSPF Retransmit Interval 5) Set OSPF Hello Interval 6) Set OSPF Dead Interval 7) Set OSPF Transit Delay 8) Set OSPF Authentication 9) Back VPN3k: Ethernet Interface 1 -> 1 > OSPF Area ID VPN3k: Ethernet Interface 1 -> [0.0.0.0] 0.0.0.0 1) Set OSPF Area ID 2) Set OSPF Priority 3) Set OSPF Metric 4) Set OSPF Retransmit Interval 5) Set OSPF Hello Interval 6) Set OSPF Dead Interval 7) Set OSPF Transit Delay 8) Set OSPF Authentication 9) Back VPN3k: Ethernet Interface 1 ->

Copyright © 2007 Internetwork Expert

VPN3k GUI:

Configure Client Reverse Route Injection:



Verification

```
Connect Cisco VPN Client from Test PC to the VPN3k:
R1#show ip route ospf
     136.1.0.0/24 is subnetted, 4 subnets
O E2
        136.1.0.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
O E2
        136.1.23.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
O E2
        136.1.100.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
     20.0.0.0/32 is subnetted, 1 subnets
        20.0.0.1 [110/20] via 136.1.111.11, 00:00:32, Ethernet0/0
O E2
     10.0.0/24 is subnetted, 1 subnets
        10.0.0.0 [110/20] via 136.1.111.11, 00:08:09, Ethernet0/0
O E2
R3#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, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
```

Copyright © 2007 Internetwork Expert

P - periodic downloaded static route Gateway of last resort is not set 136.1.0.0/24 is subnetted, 5 subnets 136.1.0.0 [120/1] via 136.1.23.2, 00:00:01, Serial1/3 R 136.1.23.0 is directly connected, Serial1/3 С R 136.1.111.0 [120/1] via 136.1.113.11, 00:00:07, Ethernet0/0 С 136.1.100.0 is directly connected, Ethernet0/1 $\,$ С 136.1.113.0 is directly connected, Ethernet0/0 10.0.0/24 is subnetted, 1 subnets R 10.0.0.0 [120/1] via 136.1.23.2, 00:00:01, Serial1/3 C:\WINNT\system32\cmd.exe _ 🗆 × * C:\Documents and Settings\IEAdmin>ping 136.1.111.1 Pinging 136.1.111.1 with 32 bytes of data: Reply from 136.1.111.1: bytes=32 time=10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Reply from 136.1.111.1: bytes=32 time<10ms TTL=253 Ping statistics for 136.1.111.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 2ms C:\Documents and Settings\IEAdmin>_

VPN3k GUI:

Monitor connected sessions:

🖉 Cisco Systems, Inc. VPN 3000 Con	centrator [¥PN3k] -	Microsoft Inte	rnet Exp	olorer				_ 🗆 ×		
<u>Fi</u> le <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back	• => • 🕑 🛛	Ag	ddress 🙋 http:	s://136.1.113	8.11/access.htm	l.	•		
VPN 3	000					Main Hel	p Supj	oort Logout		
Concer	Concentrator Series Manager Logged in: admir									
Configuration Administration Monitorin										
- E <u>Administration</u>	Connection Name	IP Address P	rotocol	Encryption	Login Time	Duration ¹	Bytes Tx	Bytes A		
Routing Table			No LA	N-to-LAN	Sessions					
Dynamic Filters D	Remote Acc	ess Session	S	[<u>LAN-to-I</u>	AN Sessi	ons <u>Manag</u> e	ment Se	ssions]		
Protocols Encryption Grop Ten Lists GrStatistics	Username Ass P A	signed IP ddress ublic IP ddress	<u> Froup</u>	<u>Protocol</u> Encryption	Login Time <u>Duration</u>	<u>Client</u> <u>Type</u> <u>Version</u>	Bytes Tx Bytes Rx	<u>NAC</u> <u>Result</u> <u>Posture</u> <u>Token</u>		
	CISCO 2 136.	0.0.0.1 1.100.200 E	ZVPN	IPSec 3DES-168	Jan 18 3:55:20 0:00:55	WinNT 4.8.01.0300	0	N/A		
Management Sessions [LAN-to-LAN Sessions Remo					Remote A	ne Di	ssions]			
	admin	Local	Conso	le None	, <u>r</u>	Jan 18 03:4	7:08 0:0	9:07		
CISCO SYSTEMS	admin	10 0 0 100	HTTP	3DES-16	58 SSL#3	Jan 18 03:4	9.59 0.0)6·16		
	•	0		.0.				¥		
街 Sessions							Internet	1		

Further Reading

How to Populate Dynamic Routes Using Reverse Route Injection

VPN3k and Cisco VPN Client with DHCP Server

Objective: Configure VPN3k to allocate addresses from DHCP server.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco</u> <u>VPN Client with RRI</u>".
- VPN3k could allocate client IPs using external DHCP server, acting as DHCP client itself (proxing).
- Do not confuse this with DHCP Relay feature, where VPN3k transparenty passes the DHCP requests from Public interface.
- Configure DHCP pool EZVPN on R1 as follows:
 - Use address pool 20.0.0/24
 - o Configure static route for 20.0.0/24 to 136.1.111.11
 - The latter route is required since VPN3k proxies the DHCP request, sending it from IP address in network 20.0.0.
- Configure VPN3k to permit address allocation via DHCP
- Configure VPN3k to disable adderss allocation via Address Pools.
- Configure DHCP server 136.1.111.1 on the VPN3k.
- Configure DHCP network scope 20.0.0.0 under group EZVPN "General" Tab.

Final Configuration

```
R1:
ip dhcp pool EZVPN
    network 20.0.0.0 /24
!
ip route 20.0.0.0 255.255.255.0 136.1.11.11
```

VPN3k GUI:

Configure DHCP Server:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Internet	Explorer
<u>File Edit View Favorites Tools</u>	: <u>H</u> elp (⇒ Back → ⇒) → 💌 😰	Address 🕘 https://136.1.113.11/access.html
VPN 3	3000	Main Help Support Logo
Conce	ntrator Series Manager	Logged in: adm
		Configuration Administration Monitorir
-=		
	Configuration System Servers	DHCP Add
Authentication	Configure and add a DHCP server	
Authorization Accounting	DHCP Server 136.1.111.1	Enter IP address or hostname.
	Server Port 67	
Firewall	Add Cancel	
H H H H H H H H H H H H H H H H H H H		
- EHP Routing		
Hanagement Protocols		
□ □ □ <u>□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ </u>		
—⊞ <u>User Management</u>		
Policy Management		
E dministration		
CISCO SYSTEMS		
DHCP Servers		📔 🎒 😰 Internet

Configure Address Allocation via DHCP:



The Table (Read Table 7)	Carlo Hala d a d		100000000000000000000000000000000000000	
<u>File Edit View Favorites I</u>	ools Help 🗘 🛱 Back 🔻 🖂	Address 🦉 htt	ps://136.1.113.11/a	ccess.html
VPN VPN	N 3000		M	ain Help Support Logou
Con	centrator Series M	lanager		Logged in: admi
			Configuration	Administration Monitorin
				primary DNS server.
<u>— Interfaces</u> — <u>⊕System</u> ——User Management	Secondary DNS		N	Enter the IP address of the secondary DNS server.
	Primary WINS		ঘ	Enter the IP address of th primary WINS server.
	Secondary WINS		ঘ	Enter the IP address of the secondary WINS server.
∄Administration ∄Monitoring	Tunneling Protocols	PPTP L2TP IPSec L2TP over IPSec WebVPN		Select the tunneling proto group can connect with.
	Strip Realm 🗖		ঘ	Check to remove the rea- qualifier of the username authentication.
	DHCP Network Scope	0.0.0		Enter the IP sub-network which users within this gr- be assigned when using th concentrator as a DHCP
CISCO SYSTEMS	Apply Canc	cel		

Modify group "EZVPN" settings to use DHCP Network Scope:

Verification

```
Connect the VPN Client to VPN3k:
R1#debug ip dhcp server events
R1#debug ip dhcp server packet
R1#
*Mar 1 05:18:51.793: DHCPD: assigned IP address 20.0.0.2 to client
0000.03a0.88bd.2900.004b.9447.ad08.df00.
*Mar 1 05:18:51.793: DHCPD: Sending DHCPOFFER to client 0000.03a0.88bd.2900.004b.9447.ad08.df00 (20.0.0.2).
*Mar 1 05:18:51.793: DHCPD: unicasting BOOTREPLY for client 0003.a088.bd29 to
relay 20.0.0.0.
*Mar 1 05:18:51.801: DHCPD: DHCPREQUEST received from client
0000.03a0.88bd.2900.004b.9447.ad08.df00.
*Mar 1 05:18:51.801: DHCPD: Sending DHCPACK to client
0000.03a0.88bd.2900.004b.9447.ad08.df00 (20.0.0.2).
*Mar 1 05:18:51.801: DHCPD: unicasting BOOTREPLY for client 0003.a088.bd29 to
relay 20.0.0.0.
Check VPN Client statistics:
```

Copyright © 2007 Internetwork Expert



Further Reading

VPN3k: Configuring DHCP Server

Copyright © 2007 Internetwork Expert

VPN3k and Cisco VPN Client with RADIUS Authentication

Objective: Configure VPN3k for authentication and address allocation via RADIUS.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco</u> <u>VPN Client with RRI</u>".
- The goal is to authenticate users and allocate addresses using RADIUS server.
- Configure VPN3k to communicate with RADIUS server as follows:
 - First, create two filter rules, to permit outgoing RADIUS traffic IN and OUT.
 - Name these rules "Outgoing RADIUS In" and "Outgoing RADIUS Out".
 - Permit UDP packets from/to port 1645 of host 10.0.0.100.
 - Configure VPN3k to use RADIUS Authentication Server with IP 10.0.0.100.
 - $\circ~$ Use key "CISCO" to secure communications.
- Configure ACS server:
 - Add network client for VPN3k as follows:

- Use IP 136.1.113.11.
- Use key CISCO.
- Use RADIUS server type specific for VPN3000.
- o Add user "CISCO" with password "CISCO1234"
 - Configure this user's profile to allocate static IP "20.0.0.1"
- Configure VPN3k as follows:
 - Modify group EZVPN as follows:
 - With IPsec Tab set authentication to "RADIUS".
 - Modify address allocation policy, permitting address allocation by Authentication Server.

Final Configuration

VPN3k GUI:

Configure RADIUS Authentication Server:

Lisco Systems, Inc. VPN 3000 C	oncentrator [YPN3k] - Microsoft Interne	t Explorer
<u>File Edit View Favorites T</u> ool	ls Help (⇔ Back + ⇒ + 💽 🔮	Address 🖉 https://136.1.113.11/access.html
VPN	3000	Main Help Support Logo
Conce	entrator Series Manager	Logged in: adr
		Configuration Administration Monitori
Configuration Interfaces	Configuration System Servers	Authentication Add
	Configure and add a user authentic	ation server.
Authorization Accounting DNS DHCP Firewall NBNS BHNTP	Server Type RADIUS	Selecting <i>Internal Server</i> will let you add users to the internal user database. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server
	Authentication 10.0.0.100	Enter IP address or hostname.
—⊕ <u>Events</u> —⊕ <u>General</u> —⊕Client Update	Used For User Authentice	tion Select the operation(s) for which this RADIUS server will be used.
	Server Port 0	Enter 0 for default port (1645).
- <u>Houser Management</u> - <u>EP-Olicy Management</u> - <u>EP-Tunneling and Security</u>	Timeout 4	Enter the timeout for this server (seconds).
Administration Monitoring	Retries 2	Enter the number of retries for this server.
CISCO SYSTEMS	Server Secret	Enter the RADIUS server secret.
adly addr.	Verify	Re-enter the secret

Configure Rule for Outgoing RADIUS traffic Out:

🕗 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer				
<u>File Edit View Favorites Tools</u>	Help (⇔ Back + ⇒ + 🐼 🖸	Address 🖉 https://136.1.113.	11/access.html			
VPN 3	000		Main Help Support Logout			
Conce	ntrator Series Manager		Logged in: admin			
		Configurati	on Administration Monitoring			
Configuration Interfaces Surface	Configuration Policy Managem	ent Traffic Management R	tules Add			
	Configure and add a new filter rule	L.				
Access Hours <u>Access Hours</u> <u>Access</u>	ic Management Rule Name Outgoing RADIUS Out					
Electronic SAS	Direction Outbound 💌		Select the data direction to which this rule applies.			
	Action Forward	<u>•</u>	Specify the action to take when this filter rule applies.			
Deriver Admission Control Durneling and Security Administration Monitoring	Protocol UDP 💌		Select the protocol to which this rule applies. For Other protocols, enter the			
	TCP Connection		protocol number. Select whether this rule should apply to an established TCP connection.			
Cisco Systems	Source Address		Specify the source			
🐔 Filter Rules			📑 🔮 Internet 🍡			

🚰 Cisco Systems, Inc. VPN 3000 Co	oncentrator [¥PN3k] - Microsoft Internet Exp	lorer _	
File Edit View Favorites Looi	s Help (⇔ Back • ⇒) • ເ (≥) Ag 3000 entrator Series Manager	Idress 🖉 https://136.1.113.11/access.html 🗾 Main Help Support Lo Logged in: a	gout admin
- <u>Configuration</u> Interfaces - D System		Configuration Administration Monit 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.	uring
	TCP/UDP Source Port Port Range or Range 0 to 65535	For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end.	- B S
By Policies By Policies By Admission Control Difference Difference	TCP/UDP Destination Port Port Range or Range 1645 to 1645	For TCP/UDP, specify the destination port ranges tha this rule checks. For a single port number, use the same number for the start and end.	e
Cisco Systems	ICMP Packet Type 0 to 255 Add Cancel	For ICMP, specify the range of ICMP packet types that this rule checks.	-
/ @ Filter Rules		📔 🎒 💓 Internet	

Configure Rule for Outgoing RADIUS traffic In:

🚈 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer	_ [] ×
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 🔹 🖘 👻 😰	Address 🙋 https://136.1.113.:	11/access.html
VPN 3	000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuratio	on Administration Monitoring
Configuration Interfaces	Configuration Policy Manageme	ent Traffic Management R	ules Add
	Configure and add a new filter rule		
Access Hours	Rule Name Outgoing RADIU	IS In	Name of this filter rule. The name must be unique.
Fules SAs Filters	Direction Inbound		Select the data direction to which this rule applies.
BW Policies Group Matching	Action Forward	•	Specify the action to take when this filter rule applies.
Hetwork Admission Control Honoring and Security Administration Administration Monitoring	Protocol UDP 💌		Select the protocol to which this rule applies. For Other protocols, enter the
	TCP Connection		protocol number. Select whether this rule should apply to an established TCP connection.
CISCO SYSTEMS	Source Address		Specify the source
🖉 Filter Rules			📔 🤮 Internet 🛛 🏸

ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	ils Help (⇒ Back + ⇒ - 💌 🕼 Address 🖉 htt	tps://136.1.113.11/access.html
VPN Conc	3000 entrator Series Manager	Main Help Support Logout Logged in: admir Configuration Administration Monitoring
Configuration —Interfaces —⊡System —⊡Iser Management		10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
HUser Management Policy Management Access Hours Piraffic Management Network Lists Rules SAs Filters DNAT	TCP/UDP Source Port	For TCP/UDP, specify the source port ranges that this rule checks. For a single
	or Range 1645 to 1645	port number, use the same number for the start and end.
BW Policies BY Policies By Group Matching By Retwork Admission Control By Retwork Admission	TCP/UDP Destination Port	For TCP/UDP, specify the destination port ranges that this rule checks. For a
<u>Administration</u> Monitoring	or Range 0 to 65535	single port number, use the same number for the start and end.
	ICMP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
CISCO SYSTEMS	Add Cancel	

Assign both rules to the Public filter:



🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	<u>H</u> elp ⇔ Back → ⇒ → 🙆 🔮	Address 🛃 https://136.1.113	.11/access.html
VPN 3	3000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configurati	ion Administration Monitoring
-Enterfaces -Enterfaces -Enterfaces	Filter Name: Public (Default)		<u> </u>
	Select an Available Rule and clic	k Add to apply it to this filte	r.
Access Hours	Select a Current Rule in Filter a	nd click Remove , Move U	p, Move Down, or Assign
- E-Traffic Management	SA to Rule as appropriate.		
Network Lists	Select an Available Rule, then se	elect a Current Rule in Filt	er, and click Insert Above
	to add the available rule above the	current rule.	
	Current		
BVV Policies	Rules in Filter	Actions	Available R
Group Matching Group Matching Group Matching Group Matching	NAT-T In (forward/in)	Add <<	OSPF In (forward/in)
<u> </u>	RIP In (forward/in) Outgoing RADIUS In (forward/in)	Insert Above</td <td>OSPF Out (forward/out) Incoming HTTP In (forv</td>	OSPF Out (forward/out) Incoming HTTP In (forv
- Monitoring	GRE Out (forward/out) IKE Out (forward/out)	Remove >>	Incoming HTTP Out (fo
	PPTP Out (forward/out) L2TP Out (forward/out)	Move Up	Any Out (forward/out)
	ICMP Out (forward/out)	Move Down	Incoming HTTPS Out (
	NAT-T Out (forward/out)	Assign SA to Rul	e LDAP Out (forward/out)
CISCO SYSTEMS	Outgoing RADIUS Out (forward/out)	ut) 🔽 Done	Telnet/SSL Out (forward)
			_
🙆 Filter Policies			📄 🔮 Internet 🏼 🎢

e <u>E</u> dit y	view F <u>a</u> vorit	es <u>T</u> ools	Help	🗘 Back 🔻	=> - 💌 🛃	Address	http://127.0.0.1;	2318/	
Cisco Sys	TEMS	Netwo	k Cont	igurati	ion				
ամիրուտ	lluEd	irt							-
User User									
Group Setup					Add /	AAA C	lient		
Shared Compon	Profile lents	AAA Clie	ent Hostn	ame	VPN3k				
System	uration uration	AAA Clie	ent IP Ado	lress	136.1.11	3.11	*		
⊨ Interfa Config	ace uration	Кеу			CISCO				
Admini: Contro	stration I	Authent	icate Usi	ıg	RADIUS (Cisco VPN 3	3000/ASA/PIX 7	.x+)	
Extern Databa	al User ses	🗖 Sing	gle Conne	et TACA	CS+ AAA Clie	nt (Record	stop in accoun [.]	ting on failure)	í.
Posturi Valida Network Profiles	e tion « Access	Log	Update/\ RADIUS ⁻ lace RADI	Vatchdog Tunneling US Port	g Packets fro Packets fro info with Use	m this AAA m this AAA rname from	Client Client this AAA Client		
Activit	ts and ty entation			Su	ıbmit Sı	ıbmit + App	ily Cancel		

Configure ACS Server - Add VPN3k as network client:

🖉 CiscoSecure AC	S - Microsoft Internet Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew	Favorites Tools Help ← Back → → → 🔇 🕼 Address 🖗 http://127.0.0.1:2318/	
CISCO SYSTEMS	User Setup	×
IllinIllin.	Edit	- F
User Setup	User: CISCO	
Shared Profile	Account Disabled	
Network Configuration	Supplementary User Info	
System Configuration	Real Name Description	
Administratio	n	
Databases	User Setup	
Posture Validation	Password Authentication:	
Profiles Reports and	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	
Online Documentation	Password	
, Ø Applet nas_filter s	itarted	

Create user CISCO with password CISCO1234 and configure address allocation:

CiscoSecure ACS - M	icrosoft Internet Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> ve	prites Tools Help (-> Back + => + 🔇 🔁 Address 🗳 http://127.0.0.1:2318/	<u> </u>
CISCO SYSTEMS	User Setup	×
User	Caliback	
- g Setup	 Use group setting 	
Group Setup	C No callback allowed	
Shared Profile	O Callback using this number	
Sur Components	O Dialup client specifies callback number	
Network Configuration	C Use Windows Database callback settings	
System Configuration	Client IP Address Assignment	
Configuration	C Use group settings	
Administration Control	C No IP address assignment	
- External User	O Assigned by dialup client	
Databases	Assign static IP address 20.0.0.1	
Posture Validation	C Assigned by AAA client pool	
Network Access Profiles		
Reports and Activity	· · · · · · · · · · · · · · · · · · ·	
Documentation	Submit Delete Cancel	
Applet dialup_filter star	ted	net //

Test AAA server on VPN3k:

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	et Explorer	_ 🗆 ×
<u>File Edit View Favorites Tools</u>	<u>H</u> elp (⇒ Back • ⇒) • 🔕 🚱	Address 🛃 https://136.1.113.11/access.html	-
VPN 3	000	Main Help	Support Logout
Conce	ntrator Series Manager		Logged in: admin
	U	Configuration Adminis	tration Monitoring
-⊕- <u>Configuration</u>			
Interfaces	Configuration System Servers	Authentication Test	
- D System			
Authentication <u>Authentication</u> <u>Authorization</u>	Enter a username and password w complete or timeout.	with which to test. Please wait for the ope	ration to
Accounting DNS	Use	ername CISCO	
	Pa	s crant woodood	
	OK Cancel		
<u>Address Management</u>			
- EHP Routing			
Hereite Management Protocols			
Client Update			
Load Balancing			
<u> </u>			
□ <u>□ ⊡ Tunneling and Security</u>			
TET MONICOLING			
CISCO SYSTEMS			
illiuilliu			
 Authentication Servers 			nternet //

🖉 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer _ 🗆 × <u>File Edit View Favorites Tools Help</u> (== Back • => • 💌 🚱 Address 🛃 https://136.1.113.11/access.html • -**VPN 3000** Main | Help | Support | Logout **Concentrator Series Manager** Logged in: admin Configuration | Administration | Monitoring -Interfaces Authentication Successful $(\mathbf{i}$ -Authentication -Authorization Continue -Accounting -DNS -DHCP -Firewall -NBNS L____NTP -⊞-<u>Address Management</u> - HP Routing - Hanagement Protocols - Events -⊞-<u>General</u> -<u>⊞-Client Update</u> -Load Balancing -⊕Policy Management - Administration - Honitoring CISCO SYSTEMS մին ովիս 🔒 🎯 Internet Authentication Servers

Configure Address allocation by Authentication Server:



Elle Edit Yiew Favorites Loois Help ← Back → → ◆ ● ● Address ● https://136. VPN 3000 Concentrator Series Manager Configuration Configuration Configuration Interval 300	1.113.11/access.ht Main Ho uration Admir	ml 💽 📆 elp Support Logout Logged in: admin nistration Monitoring	
VPN 3000 Concentrator Series Manager Configuration Interval 300 Configuration Interval 300	Main He uration Admir R	elp Support Logout Logged in: admin histration Monitoring	
Concentrator Series Manager Config C	uration Admir	Logged in: admin nistration Monitoring	
Configuration Configuration Interval 300	uration Admir I	nistration Monitoring	
Configuration Interval System Her Management	v		
		before the VPN Concentrator chec see if it is still conn	
Base Group Groups Users Delicy Management Tunneling and Security Delicy Management Delicy Management	ঘ	Select the type of for this group. Up Remote Access parameters below needed.	
Honitoring Remote Access Par	ameters		
Group Lock	V	Lock users into thi	
Authentication RADIUS		Select the authenti method for membe this group. This pa does not apply to Individual User Authentication.	
Cisco Systems Type	<u>य</u>	If members of this need authorization addition to authent select an authoriza method. If you cor this field, you must	

Configure group EZVPN to authenticate users via RADIUS:

Verification

Enable logging of passed authentications under System Configuration on ACS:



/a) Ci	scoSec	cure AC	5 - M	licr	osoft Inter	net Ex	plorer								1 ×
Eile	Edit	⊻iew	F <u>a</u> v	orite	es <u>T</u> ools	Help	🗘 Ba	ack • ≕> • (× 🖄	Addres:	s 🛃 http://127.0.0	.1:2318/		-	-
C	ISCO S	YSTEMS	s		Report	s ar	nd Act	ivity							×
					Select	4.uth	onticat	ions active	- CEU			and 1			
	Setu)p			Peoular	Exnre	encou		.634	E Kene	Start Date & 7	<u>Jau</u> Cime	End	Date & Ti	ime
	Grou	up up				<u>-vhic</u>	551011				mm/dd/yyyy,ł	h:mm	:ss mm	/dd/yyyy,	hh:r
4	Share Comp	ed Profik ponents	•		Apply	Filter	r C	lear Filter			<u>.</u>				
	Netw Conf	vork Tiguratio	n		Filtering	is no	t applied	d.						Network	c
	Syste Confi	em iguratio	2n		Date		<u>Time</u>	<u>Message-</u> <u>Type</u>	<u>User-</u> Name	<u>Group-</u> <u>Name</u>	Caller-ID	NAS- Port	NAS-IP- Address	Access Profile Name	<u>Sh</u> <u>R</u>
	Conf	rface 'iguratic ninistrati	on		01/18/20	107 0!	5:50:39	Authen OK	CISCO	Default Group	136.1.100.200	1015	136.1.113.11	(Default)	i ar
	Conti Exte	rol arnal Use abases	ər	-											
000	Post Valio	ture dation													
3	Netwo	ork Acce les	255												
	≩ Repo ≱ Activ	orts and vity	1												
) Onlir Docu	ne imentatic	on	H	•										•
🎒 Ap	pplet sta	artStop	starte	ed									🔹 🔮 Internet		11.

Connect Cisco VPN Client and check Passed Authentications on ACS:

```
Check Client Statistics:
```

Address Information	Connection Informa	tion		
Client: 20.0.0.1	Entry:	EZVPN		
Server: 136.1.113.11	Time:	0 day(s), 00:02.15		
Bytes	Crypto			
Received: 0	Encryption:	168-bit 3-DES		
Sent: 0	Authentication:	HMAC-MD5		
Packets	Transport			
Encrypted: 0	Transparent Tunneling:Inactive			
Decrypted:0	Local LAN:	Disabled		
Discarded: 7	Compression:	None		
Bypassed: 301				
		Reset		

```
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, 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
     136.1.0.0/24 is subnetted, 4 subnets
O E2
        136.1.0.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
O E2
        136.1.23.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
        136.1.111.0 is directly connected, Ethernet0/0
С
O E2
        136.1.100.0 [110/20] via 136.1.111.11, 02:06:12, Ethernet0/0
     20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
        20.0.0/24 [1/0] via 136.1.111.11
S
O E2
       20.0.0.1/32 [110/20] via 136.1.111.11, 00:03:20, Ethernet0/0
     10.0.0/24 is subnetted, 1 subnets
       10.0.0.0 [110/20] via 136.1.111.11, 02:06:13, Ethernet0/0
O E2
R1#ping 20.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/32 ms
```

Further Reading

Using Cisco Secure ACS for Windows with the VPN 3000 Concentrator - IPSec

VPN3k and Cisco VPN Client with External Group

Objective: Configure VPN3k to authenticate and apply attributes received for external group via RADIUS.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco VPN Client with RADIUS Authentication"</u>.
- VPN3000 has capability of downloading all group attributes from RADIUS server.
- When you configure a group on VPN3000, you specify it as a "external" one, and configue a group password. This password will be used to authenticate against the RADIUS server.
- Take the previously configured group "EZVPN" and configure it as external.
- On the RADIUS server you need first to enable certain RADIUS attributes, used for group configuration. At least, these should be attributes to specify user's authentication.
- Configure ACS Interface, and activate these RADIUS attributes.
- Create group EZVPN and configure the following VPN3000 attributes:
 - Tunneling-Protocols = "IPsec".
 - IPsec-Authentication = "RADIUS".

- Split-Tunneling-Policy = "Only Tunnel networks in the List".
- Split-Tunneling-List = "SPLIT_TUNNEL".
- On the RADIUS server you need to create a user with a name matching the group name. Create user named EZVPN with password "CISCO".
- Assign this use to group EZVPN.
- On the VPN3000 you should have RADIUS server already configured for authentication. It will be used to download group attributes as well.

Final Configuration

ACS:

Enable VPN3000 RADIUS attributes under Interface Configuration:







Create group EZVPN:

🖉 CiscoSecure ACS ·	- Microsoft Internet Explorer			_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F	F <u>a</u> vorites Iools Help 🗘 🖙 Back ▾ ≔)	· · 🕑 😰	Address 🛃 http://127.0.0.1:3190/	
CISCO SYSTEMS	Group Setup			×
	Select		Help	10
User Setup	Renaming Group: (Group 1	<u>Rename Group</u>	
Setup Shared Profile Components Configuration System Configuration Configur	Group EZVPN Submit Cance		Rename Group Type a new group name and dick Submit to assign a more descriptive name to the group profile. This is useful if different groups have been configured to allow specific authorization privileges, such as PPP or Telnet-only capability. Click Cancel to return to the Group Setup window without saving a new group name. [Back to Top]	
🙋 Applet nas_filter sta	rted		📔 📄 🚺 💓 Internet	
CISCO SYSTEMS User Setup User Setup User Setup				
--	---			
Jump To Access Restrictions User Access Restrictions IP Address Assignment				
User Access Restrictions IP Address Assignment				
GFO RADIUS (Cisco IOS/PIX 6.0) RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) RADIUS (IETE)	-			
Shared Profile				
Network Configuration Access Restrictions				
System				
Configuration Group Disabled	2			
Administration Control				
Default Time-of-Day Access Settings	?			
00:00 06:00 12:00 18:00 24:00				
Mon True				
Network Access Profiles Wed				
Network Access Wed Thu				
Network Access Wed Thu Reports and Activity				

Set values for VPN3000 RADIUS attributes:

CiscoSecure ACS - M	licrosoft Internet Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	rorites Iools Help 🗘 Back + => - 🔕 🗊 Address 🙋 http://127.0.0.1:3190/	-
CISCO SYSTEMS	Group Setup	×
illin	Jump To RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) 💌	
User Setup	Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes	
Shared Profile Components		
Network Configuration	IPSec ■ IPSec ■ IPSec ■	
System Configuration	RADIUS ▼ [3076\027] IPSec-Split-Tunnel-List	
Interface Configuration	SPLIT_TUNNEL	
Control	Only tunnel networks in the list	
Posture Validation	s	
Network Access Profiles	IETF RADIUS Attributes	
Activity	🗖 [006] Service-Type	•
Documentation	Submit Submit + Restart Cancel	
Applet dialup_filter star	I 👘 👔 👔 Internet	

CiscoSecure ACS -	Microsoft Internet Expl	orer		
<u>Elie Edit View F</u>	User Setup	🗘 🔁 Back 🔹 🖘 🖈 💟 👔	Address 2 http://127.0.0.1:3190/	<u> </u>
	Edit			
User Setup		User: EZV	PN (New User)	
Group Setup		AC	count Disabled	
Components	L			
Configuration	Real Name	Supplemen	itary User Info	<u> </u>

User Setup

Submit

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

Cancel

Create user EZVPN with password, matching the group's password configured on VPN3000 ("CISCO"):

Description

Password Authentication:

Password

Interface Configuration

Administration

Di External User Databases

Dood Posture Validation

Network Access Profiles

Documentation

Reports and Activity

Applet dialup_filter started

?

-

🥝 Internet

ACS Internal Database

Assign it to group EZVPN:

jie <u>E</u> di	it <u>V</u> iew	Favorites	Tools	Help	⇔Back 👻	=> - 😢 🛃	A <u>d</u> dress	🛃 http://127.0.0.1:3190/	-
Cisco	SYSTEMS	Us	ser Se	etup					×
	տում	•	E] Separa	te (CHAP	/MS-CHAP/4	(RAP)		-
	ser etup			I	assword				
6 6 61	roup			Confirm I	assword				
	etup	4	W	hen a to	en serve	er is used for	authenti	cation, supplying a separate	
Sh Co	iared Profile imponents		es Ch	HAP pass specially	wora for useful wh	a token caro ien token ca	ching is e	enabled.	
	etwork	7	-	a 10.			1270		
	onfiguration	<u> </u>				Group to whi	ch the us	er is assigned:	-
	ystem onfiguration	1			Defa	ault Group		<u> </u>	
	terface	-	-		Defa EZV	ult Group PN			
EP Co	onfiguratio				Grou	ip 2			
	dministratio ontrol	n.	0	Use 🤉	Grou Grou	ир 3 ир 4			
Q. LE	vtorna) lleon	-	(No c	allba Grou	ip 5			
	atabases		(Callb	ack (Grou	ւթ6 107			
	osture alidation			D Dialu	o clie	ip 8			
	4) Use V	Grou Vind Grou	ю9 10		-	
Pr	ofiles	**	_			- Per anor			
	eports and					Client IP	Address A	Assignment	
								2000-000-000-000-000-000-000-000-000-00	
	niine ocumentatio	n				Su	ubmit (Cancel	
1 Applet	dialup, filto	r started							

Configure group EZVPN on VPN3k as External:

🚰 Cisco Systems, Inc. VPN 3000 Concentrato	r [¥PN3k] - Microsoft Inter	net Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	🖙 Back 🔹 🖘 🔹 🚱	Address 🙋 https://136.1.113.11/access.html	-
VPN 3000		Main Help 1	Support Logout
Concentrato	r Series Manager	•	ogged in: admin
	Ű	Configuration Administra	tion Monitoring
Interfaces Config	uration User Managem	ent Groups Modify EZVPN	
	the Inherit? how to set a	field that you want to default to the base grout	n value
Base Group Unched	k the Inherit? box and e	enter a new value to override base group value.	s.
Users			
Denti Identi	ty [™] General [™] IPSec [™] Cli	ient Config Client FW HW Client PPTP/L	2TP WebVPN
		Identity Parameters	
- Monitoring Attrib	oute Value	Description	
G	roup Tame	Enter a unique name for the group.	
Pass	word	Enter the password for the group.	
V	erify .	Verify the group's password.	
	Гуре <mark>Extemal ▼</mark>	<i>External</i> groups are configured on an extern (e.g. RADIUS). <i>Internal</i> groups are configur Concentrator's Internal Database.	al authentication se red on the VPN 31
Ар	ply Cancel		
Piero Svercue			
L L			
 Tunneling and Security 		📄 🚺 🎯 Inte	rnet //

Verification

Connect Cisco VPN Client and check session status at VPN3000:

🖉 Cisco Systems, Inc. VPN 3000 Conc	entrator	VPN3k] - Micro	soft In	ternet Ex	plorer							X
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	🗘 Bac	k • ≓>	- 💌	A	dress	🕘 http:	s://136.1.113	8.11/access.	.html		-	1
VPN 30	000								Main	Help	Supp	ort Log	out
Concen	trator	Seri	es Ma	anag	ger					I	Logge	d in: ad	min
								Configurat	tion Adn	ninistra	ntion	Monitor	ing
- E-Configuration	Active	Total	Active	Total	Active	Total	Active	e Total	Active 7	Fotal A	Active	Total	
-==+Monitoring	0	0	0	0	0	0	0	0	0	0	1	16	
Routing Table													
<u> </u>				-									
	LAN-1	to-LA	AN Ses	sion	S	[<u>Ren</u>	note Ac	cess Sessi	ons Man	lagemei	nt Ses	sions]	
Protocols	Conn	ection	I	P	Protoco	l Enc	ryption	Login	Duration	Byte	es I	3ytes	
Encryption	Na	me	Add	ress				Time		Tx		Rx	
					No L	AN-to	-LAN :	Sessions					
	Remo	te Ac	ress S	essio	ns	ET.A	N-to-T	AN Sessi	ons I Man	agemer	nt Ses	sions 1	
	ICCIIIO			1 70	113				<u> </u>	m		MAG	1
		A	Addre	<u>a 11</u>		Pro	tocol	Login	Clien	$\underline{t} = \frac{B}{2}$	ytes Tx	Result	
	Userna	me	Public	IP	Group	Encr	yption	Time	Type	В	ytes	Posture	
			Addre	<u>s s</u>				Duration	versio	<u>m</u>]]	Rx	<u>Token</u>	
	-		20.0.0	1		TP	Sec	Jan 19	WinN	т	٥		
	CISCO	13	6.1.100	0.200	EZVPN	3DE	S-168	1:08:15	4.8.01.0	300	õ	N/A	
	1	-						0:00:06					
CISCO SYSTEMS													Ţ
addinaaddina.	1												
🔊 Sessions										🤣 Inte	ernet		1.

coSecure	e ALS	- Mic	rosoft Internet	Explorer							
Fair A	iew	Favori	tes <u>L</u> oois <u>H</u> ei	p (= B	ack ▼ ≕> * l	S 🛛	Address	s 🙋 http://127.0.0.	1:3190/		
SCO SYST	TEMS		Reports a	and Act	ivitv						
اسال	h., .										
			Select								
User Setup			Passed Aut	thenticat	ions active	.csv	Refre	esh 🗗 Downlo	iad		
		4	Regular Exp	ression				Start Date & T	ime	End D	ate & T
Group Setup								mm/dd/yyyy,h	h:mm:s	is mm/c	ld/yyyy,
L Shared Pi	rofile	i	Annly Fil	ter C	lear Filter	i i					
Compone	ents					C .					
Network	<	1	Filtering is r	not applie	<u>.</u>						
Contigur	ration										Netwo
System Configur	ration		Date 🖊	Time	Message-	User-	Group-	Caller-ID	NAS-	Address	Acces
1.1.4.4.4.6.4.4		1	and the second		TYPE	<u>Nume</u>	wante		TOIL	Hudress	Name
Configur	ration		01/19/2007	01:08:21	Authen OK	EZVPN	EZVPN	<u>α</u>	EZVPN	136.1.113.11	(Defaul
Administ	tratior	1	01/19/2007	01:08:20	Authen OK	EZVPN	EZVPN		EZVPN	136.1.113.11	(Defau
Control Externa	1 User		01/19/2007	01:08:20	Authen OK	CISCO	Default Group	136.1.100.200	1025	136.1.113.11	(Defaul
Databas	es	J۲	01/19/2007	01:08:15	Authen OK	EZVPN	EZVPN	136.1.100.200	0	136.1.113.11	(Defau
Posture	ion		01/19/2007	01:00:23	Authen OK	EZVPN	EZVPN	302	EZVPN	136.1.113.11	(Defaul
l o anada			01/19/2007	01:00:23	Authen OK	EZVPN	EZVPN		EZVPN	136.1.113.11	(Defaul
Network Profiles	Acces	s	01/19/2007	01:00:23	Authen OK	cisco	Default Group	136.1.100.200	1024	136.1.113.11	(Defaul
Reports	s a.nd		01/19/2007	01:00:18	Authen OK	EZVPN	EZVPN	136.1.100.200	0	136.1.113.11	(Defaul
L On Kin			01/19/2007	00:52:11	Authen OK	EZVPN	EZVPN		EZVPN	136.1.113.11	(Defaul
Documer	ntation	┛┝	01/19/2007	00.52.11	∆uthen ∩K	EZVPN	FZVPN		FZVPN	136 1 113 11	(Defaul

Check the passed authentications on ACS server:

Further Reading

<u>Cisco VPN Client User and Group Attribute Processing on the VPN 3000</u> <u>Concentrator</u>

VPN3k and Cisco VPN Client with Digital Certificates

Objective: Configure VPN3k and Cisco VPN client for group authentication using digital certificates.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and Cisco</u> <u>VPN Client with RRI</u>".
- Start by configuring VPN Client:
 - First, enroll VPN client with CA via SCEP.
 - Use enrollment URL
 <u>http://10.0.0.100/certsrv/mscep/mscep.dll</u>
 - Specify "OU=EZVPN" to be used for group matching on VPN3k.
 - Next, use Internet Explorer to retreive and install CA Root Certificate into Windows trusted certificates store.
 - After that, download CA certificate and import it into VPN client Store.
 - Modify VPN connection setting, and choose authentication based on certificates.
- Enroll VPN3k with CA:
 - Set up clock synchronization via NTP with CA server.
 - Configure Public traffic filter to permit Outgoing NTP.

- Configure two rules: inbound and outbound.
- Assign them to Public traffic filter.
- Retrieve CA Certificate via SCEP:
 - Configure Public traffic filter to permit:
 - Ougoing HTTP traffic In and Out.
 - Use the pre-configured rules for this task.
 - Use enrollment URL
 - http://10.0.0.100/certsrv/mscep/mscep.dll
- o Generate Certificate Request.
- Configure VPN3k for Group authentication with certificates.
 - Activate "CiscoVPN" IKE proposal that uses RSA-Sig authentication.
 - o Make it top priority.
- Modify the default IPsec SA "ESP-3DES-MD5"
 - Configure it to use digital certificates for authentication.
 - Chose certificate you have obtained from CA for identity.
- Check group "EZVPN" to make sure you have assigned IPsec SA "ESP-3DES-MD5" in "IPsec" Tab.

Final Configuration

Test PC/VPN Client:

<i>Choose Certificates/Enroll:</i>	loose	tificates/Enroll:
------------------------------------	-------	-------------------

👌 VPN Client Cert	ificate Enrollment
Choose a certificate er	rollment type: "*" denotes a required field:
<u>○</u> nline	
Certificate Authority:	<new></new>
ca <u>u</u> rl*:	http://10.0.0.100/certsrv/mscep/mscep.dll
CA <u>D</u> omain:	IE1
Challenge P <u>a</u> ssword:	XXXXX
C <u>F</u> ile	
File encoding:	Binary 💌
File <u>n</u> ame*:	
New <u>P</u> assword:	
	<u>N</u> ext Cancel

🍐 VPN Client	Certificate Enrollment
Enter certificate	fields, "*" denotes a required field:
<u>N</u> ame [CN]*:	Cisco
Department [OU	J]: EZVPN
<u>C</u> ompany (0):	
<u>S</u> tate [ST]:	
Country (C):	
E <u>m</u> ail (E):	
IP Address:	
Dom <u>a</u> in:	
	Back Enroll Cancel

View your certificate:

VPN Client Certi	ficate Properties for "CISCO"
Common Name	CISCO
Department	EZVPN
Company	
State	
Country	
Email	
MD5 Thumbprint	13A36EFFDF8B5564E7F8BE1FE1C7C6B9
SHA1 Thumbprint	01E9886EAD466BDE24750290272F06A5FD0A7B0F
Key Size	2048
Subject	cn=CISCO,ou=EZVPN
Issuer	cn=IESERVER1,o=Internetwork Expert,I=Reno,st=NV,c=US,e=bmcgahan@internetworkexpert.com
Serial Number	431B460800010000002E
Not valid before	Thu Jan 18 06:10:15 2007
Not valid after	Fri Jan 18 06:20:15 2008

Retreive CA certificate and install it into Trusted Roots store:

Microsoft Certificate Services - Microsoft Internet Explorer	
j Eile Edit View Favorites Iools Help ← Back → ↔ ♥ 🔇 🗊 Address 🖉 http://10.0.0	0.100/certsrv/ 🗾 🌃
	×
Microsoft Certificate Services IESERVER1	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or o program. Once you acquire a certificate, you will be able to securely identify yourself over the web, sign your e-mail messages, encrypt your e-mail messages, and more type of certificate you request.	ther secure to other people depending upon the
Select a task:	
C Request a certificate	
C Check on a pending certificate	
9.	Next>
	~
Done Done	🛛 🥝 Internet 👘 🏼

Choose "Install this CA certification path":

Microsoft	Certificate Services - Microsoft Internet Explorer
<u>E</u> ile <u>E</u> dit	View Favorites Iools Help 🛛 ⇔ Back • ↔ - 🔇 🐉 🔤 Address 🙋 /10.0.0.100/certsrv/certcarc.asp 💌 🌆
Minungh	
Wherosom	
Retrieve	The CA Certificate Or Certificate Revocation List
Install this authority.	S CA certification path to allow your computer to trust certificates issued from this certification
lt is not n this certif	ecessary to manually install the CA certification path if you request and install a certificate from ication authority, because the CA certification path will be installed for you automatically.
Choose	file to download:
CA Certi	ficate: Current [IESERVER1(1)] Previous [IESERVER1]
	Download CA certificate
	Download CA certification path
	Download latest certificate revocation list
Done	🖉 Internet

Root Cert	ificate Store 🛛 🕅
1	Do you want to ADD the following certificate to the Root Store? Subject : IESERVER1, Internetwork Expert, Reno, NV, US, bmcgahan@internetworkexpert.com Issuer : Self Issued Time Validity : Friday, July 21, 2006 through Monday, July 21, 2008 Serial Number : 6A8B964C 37F91BB2 45B01DE2 A6363745 Thumbprint (sha1) : 4BFF916B 2D7A58C4 9DB6A69C E39C770D 94A8EAB7 Thumbprint (md5) : 74F95E93 4F8C8AF3 5FD15364 8EFBB479 <u>Y</u> es <u>Y</u> es <u>Y</u> es
🖉 Microsoft C	Certificate Services - Microsoft Internet Explorer
<u> </u>	View Favorites Iools Help 🛛 🗇 Back 🔹 🖘 🖉 🕼 🗍 Address 🖉 10.0.0.100/certsrv/certrmpn.asp 💌
Microsoft (Certificate Services IESERVER1 Home
CA Cartif	
CACEI	
The CA ce	ertificate has been successfully installed.
A Dono	

Download CA certificate for installation into Cisco VPN Client certificate store:

🖉 Mici	rosoft	Certific	ate Servio	es - Mi	crosoft	Intern	et Expl	orer				19.						-	
j <u>F</u> ile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	Tools	<u>H</u> elp] ∉	= Back	- ₽	• 🗵) 🕼		∫ A <u>d</u> dress	🛃 http	://10.0	.0.100	/certsrv	1	-	-
Міс	rosoft	Certifi	cate Servi	ces	IESER	VER1												Home	*
Wel	com	e																	-
You prog over type Sele	use t gram. the v of ce ect a Ret C Rec	his we Once web, s ertifica task: tieve quest eck or	eb site to e you acc sign your ate you re the CA o a certific n a pend	o requ quire a e-ma eques certific cate ing ce	est a c a certif il mes t. ate or ertifical	certific icate, sage: certif	cate f , you v s, enc ficate	or yoi will be rrypt y revo	ur we e able your e catio	eb bro e to s e-mai n list	owse ecui I me	er, e-ma rely ide essage:	ail clier ntify yc s, and	nt, or o oursel more	other f to c dep	secu other p endir	ire beopling upo	e on the	
Don	e) Inter	net		*

Choose "Download CA Certificate":

Microsoft Certificate Services - Microsoft Internet Explorer _ 🗆 X 🗇 Back 🔹 🖘 💌 🚱 Address 🙋 /10.0.0.100/certsrv/certcarc.asp 🔻 <u>File Edit View Favorites Tools Help</u> Microsoft Certificate Services -- IESERVER1 Home **Retrieve The CA Certificate Or Certificate Revocation List** Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [IESERVER1(1)] Previous [IESERVER1] • DER encoded or • Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list 🙋 Done 🧑 Internet

Save As						? ×
Save jn:	My Documer	nts	•	+ 🖻 🗂	• 🏢 -	
History Desktop	My Pictures Security CA-CRT.cer Certnew.cer IDSUSER-CRT	.cer				
My Documents						
My Computer						
De Net Charge	File <u>n</u> ame:	certnew.cer]	<u>S</u> ave
Do Not Chang	Save as <u>t</u> ype:	Security Certificate		•]	Cancel

Next choose "Import" in Certificate Menu of Cisco VPN Client, and browse to downloaded file:

👌 VPN Client In	nport Certificate	×
• Import from File		
Luci Dali		- I
Import <u>P</u> ath:	Ind Settings/IEAdmin/My Documents/certnew.cer	Browse
Import P <u>a</u> ssword:		
C Import from <u>Micro</u> Import C <u>e</u> rtificate: Entering a new pa identity certificate:	osoft Certificate store	word protect
<u>N</u> ew Password	:	
<u>C</u> onfirm Password	:]	
	Import	Cancel

You should now have identity ceritificate and CA certificate into Cisco VPN Client Store:

👌 status: Connect	ed VPN Client -	Version 4.8.01	.0300			
Connection Entries	<u>5</u> tatus C <u>e</u> rtificate:	s <u>L</u> og <u>O</u> ptions	Help			
View Imp	ort Export	Enroll	Verify	X Delete		CISCO SYSTEMS
Connection Entries	Certificates L	og				
Number	Certificate		Store	4	Key Size	Validity
0 1	IESERVER1 CISCO		CA Cisco		1024 2048	until Jul 21, 2008 until Jan 18, 2008
Connected to "EZVPN	ľ.			Conn	ected Time: 0 day	y(s), 00:06.16 💌

onnection Entry: E	ZVPN		
Host: 1	36.1.113.11		
Authentication	Transport Backup Servers	Dial-Up	
C Group Authen	tication	C Mutual Group	Authentication
<u>N</u> ame:	EZVPN		
Password:	ххххх		
Confirm Passwo	ord: S****		
 Certificate Aut 	hentication		
Name: 3 - CIS	CO (Cisco)		
Send CA Co	ertificate Chain		
		-	

Modify connection Settings to use Certificates for authentication:

VPN3k:

Create rule for Outgoing NTP Out:

🖉 Cisco Systems, Inc. ¥PN 3000 (Concentrator [¥PN3K] - Microsoft Intern	et Explorer 📃 🗌 🗙
<u>File Edit View Favorites Too</u>	ols Help (⇔ Back → ⇒ → 🙆 🔂	Address 🖉 https://136.1.121.11/access.html
VPN	3000	Main Help Support Logout
Conc	entrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
		· · · · · · · · · · · · · · · · · · ·
Interfaces	Configuration Policy Manager	nent Traffic Management Rules Modify
	Modify a filter rule.	
Access Hours	Rule Name Outgoing NTP	Out Name of this filter rule. The name must be unique.
	Direction Outbound	Select the data direction to
BW Policies	Action Forward	Specify the action to take when this filter rule applies.
	Protocol UDP 💌	Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
	TCP Don't Care	Select whether this rule should apply to an established TCP connection.
CISCO SYSTEMS	Source Address	Specify the source
🛃 Filter Rules		📄 📔 🕐 Internet

Configuration Interfaces DSystem Configuration User Management Configuration) ator Series Manager	Main Help Support Logout Logged in: admin Configuration Administration Monitoring 10.10.1.0/0.0.255 = all 10.10.1.nnn addresses. For TCP/UDP, specify the
Configuration Interfaces DSystem DUser Management Policy Management Access Hours TC Access Hours TC Network Lists Rules	CP/UDP Source Port	10.10.1.0/0.0.255 = all 10.10.1.nnn addresses. For TCP/UDP, specify the
Orgen international internatinternatinational international international international interna	CP/UDP Source Port	For TCP/UDP, specify the
Rules	Port Range	rule checks. For a single
	or Range 0 to 65535	port number, use the same number for the start and end.
Byv Policies Byv Policies Byv Policies Byv Policies Trophysical Control Byvetwork Admission Control Administration	CP/UDP Destination Port	For TCP/UDP, specify the destination port ranges that this rule checks. For a
Monitoring	or Range 123 to 123	single port number, use the same number for the start and end.
IC	MP Packet Type	For ICMP, specify the range of ICMP packet types that this rule checks.
CISCO SYSTEMS	Add Cancel	

e <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🔹 🖘 👻 🕼	Address 🙋 https://136.1.121.11/access.h	ntml 🔽 🦉
VPN 3	000	Main	lelp Support Logo
Concer	itrator Series Manager		Logged in: adm
		Configuration Adm	inistration Monitorin
Configuration —Interfaces ElSustem	Configuration Policy Manageme	nt Traffic Management Rules Ad	ld
⊕ <u>System</u> ⊕User Management ⊖Policy Management	Configure and add a new filter rule		
Access Hours	Rule Name Outgoing NTP In	Name o name m	of this filter rule. The just be unique.
Rules SAs Filters	Direction Inbound	Select ti which th	he data direction to his rule applies.
BW Policics Group Matching	Action Forward	Specify when th	the action to take is filter rule applies.
☐ <u>⊕Network Admission Control</u> <u>⊕Tunneling and Security</u> <u>Idministration</u> <u>Idministration</u>	Protocol UDP 💌	Select ti which th Other p	he protocol to his rule applies. For rotocols, enter the
	TCP Connection	Select w should a establish connect	whether this rule apply to an ned TCP ion.
CISCO SYSTEMS	Source Address	Specify	the source

Create rule for Outgoing NTP inbound:

Cisco Systems, Inc. VPN 3000 Co	oncentrator [¥PN3K] - Microsoft Internel	Explorer	
		Address Address Address https://136.1.121.11/access.html	
VPN.	3000	Main Help Sup	port Logout
Conce	entrator Series Manager	Logg	jed in: admin
		Configuration Administration	Monitoring
Configuration Interfaces System Gyser Management	Wildcard-mask 255.255.255.255	to match. For exar 10.10.1.0/0.0.0.2: 10.10.1.nnn addre	nple, 55 = all sses.
	TCP/UDP Source Port Port Range	For TCP/UDP, sp source port ranges rule checks. For a port number, use t	ecify the that this single he same
SAS Filters - CHAI - EW Policies	or Range 123 to 123	number for the star end.	rt and
Develop Matching Develop Matching	TCP/UDP Destination Port Port Range	For TCP/UDP, sp destination port ra this rule checks. F single port number	ecify the nges that or a -, use the
	or Range 0 to 6553	same number for t and end.	he start
CISCO SYSTEMS	ICMP Packet Type	For ICMP, specify range of ICMP pa types that this rule	y the icket checks.
adhaadha.	Add Cancel		Ţ
Filter Rules		📄 📄 💕 Internet	1

Add rules to Public filter, permitting outgoing NTP:

Cisco Systems, Inc. VPN 3000 Col	ncentrator [¥PN3K] - Microsoft Interne	t Explorer		_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	<u>H</u> elp	Address 🙋 https://136.1.12	1.11/access.html	-
VPN 3	000		Main Help Supp	oort Logout
Conce	ntrator Series Manager		Logg	ed in: admin
		Configura	tion Administration	Monitoring
<u>Configuration</u>				
Interfaces	Configuration Policy Managem	ent Traffic Management	Assign Rules to Filte	r 🔤
<u>+⊕System</u>			Save No	eeded
Access Hours	Add, remove, prioritize, and config	gure rules that apply to a filt	er.	
Traffic Management	Elter New Poltin Column			
Network Lists	Filter Name: Public (Default)			
	Colort on Ameilable Dula on dolla	le Add the secolarity to this filt	22	
Filters	Select an Available Rule and the	ed alials Damana Maria I	n Merre Derre or	Assim
	SA to Pulo as appropriate	na chek Keniove, iviove (p, wrove rown, or	Assign
	Select on Available Rule, then se	lect a Current Rule in Fil	tor and click Incort	Abovo
	to add the available rule above the	current rule	ter, and elect motif.	10070
	to add ale attainable fale about ale	CONTEND TONC.		
	Current			
- Et Monitoring	Bulos in Filt		Actions	
	itues in ritu		Actions	
	L2L: VPN_TO_R2 In (IPSec/L2L: \	/PN_TO_R2/in) 🔺 🔜	<< Add	OSPF
	GRE In (forward/in)		<< Insert Above	USPF
	IKE In (forward/in)			
	PPTP In (forward/in)		Remove >>	Any In
	L2TP In (forward/in)		Move Up	Any O
CISCO SYSTEMS	ICMP In (forward/in)			
and house the second	<pre>veer in (iorward/in)</pre>		Move Down	↓ Inicom
) User/Group Management			🔚 🙆 Internet	

🚈 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer		_ 🗆 ×
<u>File Edit View Favorites T</u> ools	<u>H</u> elp	Address 🙋 https://136.1.121	1.11/access.html	-
VPN 3	3000		Main Help Supp	ort Logout
Conce	ntrator Series Manager		Loggi	ed in: admin
	v	Configurat	tion Administration	Monitoring
	Filter Name: Public (Default) Select an Available Rule and clic Select a Current Rule in Filter a SA to Rule as appropriate. Select an Available Rule, then se to add the available rule above the	k Add to apply it to this filt nd click Remove, Move U lect a C urrent Rule in Filt current rule.	er. J p, Move Down , or . t er, and click Insert 2	Assign Above
	Current Rules in Filte	er	Actions	
Group Matching Group Matching Group Matching Group Matching	Outgoing NTP In (forward/in)		<< Add	OSPF
□ <u>□ • <u>Tunneling</u> and <u>Security</u></u>	L2L: VPN_TO_R2 Out (IPSec/L2L:	VPN_TO_R2/out)	<< Insert Above	OSPF
- <u>B-Monitoring</u>	IKE Out (forward/out) PPTP Out (forward/out)		Remove >>	Incom Any In
	L2TP Out (forward/out)		Move Up	Any O
	VRRP Out (forward/out) NAT-T Out (forward/out)		Move Down	
	RIP Out (forward/out)		Assign SA to Rule	LDAP
CLEED SVETENS	Outgoing NTP Out (forward/out)	T	Done	Telne
	<u>ر</u>			
e User/Group Management			📋 🥝 Internet	11.

Configure NTP Server:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Internel	t Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help ⇔Back + ⇒ - 🕲 😰	Address 🖉 https://136.1.121.11/access.html	-
VPN 3	3000	Main Help	Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuration Administ	ration Monitoring
Interfaces	Configuration System Servers	NTP Hosts Add	
- □ <u>System</u>	11 KAN 1000		
Authentication	Add a new NTP host.		
Authorization	16		
Accounting	NTP Host 10.0.0.100	Enter the hostname or IP address of the	NTP server.
		_	
	Add Cancel		
Parameters			
Hosts			
Address Management			
<u></u> <u></u> <u>Client Update</u>			
Load Balancing			
-t+User Management			
	1		
CISCO SYSTEMS			
NTP Servers		🔒 🚳 Ir	ternet //

Add rules to Public filter, permitting Outgoing HTTP In/Out (for SCEP):

🏄 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer		_ 🗆 ×
<u>File Edit View Favorites T</u> ools	Help (⇔ Back • ⇒ • 🔇 🛃	Address 🙋 https://136.1.121	1.11/access.html	-
VPN 3	3000		Main Help Supp	ort Logout
Conce	ntrator Series Manager		Logge	ed in: admin
	0	Configurat	tion Administration	Monitoring
- Configuration Interfaces - System	Filter Name: Public (Default)			•
	Select an Available Rule and cho Select a Current Rule in Filter a SA to Rule as appropriate. Select an Available Rule, then se to add the available rule above the	k Add to apply it to this filte nd click Remove, Move U dect a Current Rule in Filt current rule.	er. J p, Move Down , or A c er , and click Insert A	Assign Above
	Rules in Filte	er	Actions	
Group Matching Matching Matching Metwork Admission Control	RIP In (forward/in)		<< Add	
	L2L: VPN_TO_R2 Out (IPSec/L2L:	VPN_TO_R2/out)	<< Insert Above	Incom
- <u>mMonitoring</u>	GRE Out (forward/out) IKE Out (forward/out)		Remove >>	Incom Any In
	I 2TP Out (forward/out)		Move Up	Any O Incom
	ICMP Out (forward/out) VRRP Out (forward/out)		Mo∨e Down	
	NAT-T Out (forward/out)		Assign SA to Rule	LDAP
Curra Curran	Cutgoing HTTP Out (forward/out)	-	Done	Telne
	<u> </u>			▼ ►
e Hiter Policies			📋 🥶 Internet	11

Install CA Certificate:



Cisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3K] - Microsoft Interne	t Explorer	_ 🗆 ×
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 🔹 🖘 👻 🔯	Address 🛃 https://136.1.121.11/access.html	• 1
VPN 3	000	Main Help	Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuration Administ	ration Monitoring
Configuration Administration Administer Sessions Doctore locate	Administration Certificate Mana	gement Install CA Certificate SCEP	
<u>System Reboot</u> <u>Reboot Status</u>	Enter the information needed to re operation to complete.	trieve the CA certificate via SCEP. Please	• wait for the
Monitoring Refresh	URL 10.0.0.100/certsr√ CA l⊫1	/mscep/mscep.dll Required for some PK	I
Certificate Management	Descriptor Retrieve Cancel	configurations.	
- Monitoring			
Cisco Systems			
🝘 Certificate Management		II 🔷 🖨 🚺	nternet //

Enroll with certification authority:



Cisco Systems, Inc. VPN 3000	Concentrator [VPN3K] - Microsoft Interne	t Explorer	>
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> o	ols Help ← Back + => + 😢 🔂	Address 🛃 https://136.1.121.11/access.html	_
VPN	3000	Main Help Supp	port Logou
Conc	entrator Series Manager	Logg	ed in: admi
		Configuration Administration	Monitoring
Configuration Administration Administer Sessions	Administration Certificate Mana	gement Enroll Identity Certificate SCEP	
Software Update System Reboot Reboot Status	Enter the information to be include operation to finish.	d in the certificate request. Please wait for the	
<u>Ping</u> <u>Traceroute</u> <u>Monitoring Refresh</u> <u>DrAccess Rights</u> <u></u>	Common Name (CN) VPN3k	Enter the common na the VPN 3000 Conc to be used in this PK	ame for centrator II.
Enrollment	Organizational Unit (OU)	Enter the department	t.
Monitoring	Organization (O)	Enter the Organizatio	n or
	Locality (L)	Enter the city or town	n.
	State/Province (SP)	Enter the State or Pr	ovince.
	Country (C)	Enter the two-letter of abbreviation (e.g. Un States = US).	ountry nited
Cisco Systems	Subject AlternativeName VPN3k (FQDN)	Enter the Fully Qualif Domain Name for th 3000 Concentrator t used in this PKI	fied .e VPN :o be
Miew All CRI Caches		used in this FAL	



Activate IKE Proposal that uses RSA-Sig authentication:

🚰 Cisco Systems, Inc. VPN 3000 C	oncentrator [¥PN3k] - Microsoft	Internet Explorer		
<u>File Edit View Favorites Too</u>	Is Help \Leftrightarrow Back $\star \Rightarrow \star$ (🔊 😰 🛛 A <u>d</u> dress 🙋	https://136.1.113.11/access.html	-
VPN Conc	3000 entrator Series Man	agar	Main Help Support L	ogout
Conc	entrator series Man	agei	Logged III: Configuration Administration Mani	aumin
			Configuration Auministration Mon	lunng
	on Tunneling and Securit	v IPSec IKE Propo	sals	-
	3		Save Needed	
<u>Depolicy Management</u> <u>Tunneling and Security</u>	, prioritize, and configure IK	E Proposals.		
	active Proposal and click A	Activate to make it A	Active, or click Modify, Copy	
	is appropriate.			
LAN-to-LAN	ctive Proposal and click D	eactivate to make it	Inactive, or click Move Up	
NAT Transparency	own to change its priority.	· p ·		
Alerts	or Copy to add a new Inact	ive Proposal. IKE P	roposals are used by <u>Security</u>	
	Activo		Inactivo	
- E- <u>Administration</u>	Pronosals	Actions	Pronosals	
- Honitoring	Client 2DES MDE	11040115		-
	MD5	<< Activate	IKE-3DES-MD5-BSA-DH1	
	MD5-DH1	Deactivate >>	IKE-DES-MD5-DH7	
	1D5		CiscoVPNClient-3DES-MD5-RSA	
	MD5-DH7	Move Up	CiscoVPNClient-3DES-SHA-DSA	
	Client-3DES-MD5-DH5	Move Down	CiscoVPNClient-3DES-SHA-DSA-DH5	
CISCO SYSTEMS	Client-AES128-SHA	A 1.1	CiscoVPNClient-AES256-SHA	
allo allo	:8-SHA	Add	I IKE-AES256-SHA	
	1			
🥙 IKE Proposals			📔 📋 📋 💕 Internet	11.

Make it top priority:

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer	
<u>File Edit View Favorites T</u> ools	: <u>H</u> elp \⇔ Back → ⇒ → 🙆 🛃	Address 🛃 https://136.1.11	3.11/access.html
VPN :	3000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configura	tion Administration Monitoring
			A
Interfaces	Configuration Tunneling and So	ecurity IPSec IKE Propos	sals
			Save Needed
		<u></u>	
Tunneling and Security	Add, delete, prioritize, and configu	ure IKE Proposals.	
PPTP			
	Select an Inactive Proposal and	click Activate to make it A	ctive, or click Modify, Copy
	or Delete as appropriate.		
	Select an Active Proposal and ch	ick Deactivate to make it I	nactive, or click Move Up
NAT Transparency	or Move Down to change its prio	nty.	1 11 0 5
<u>Alerts</u>	Click Add or Copy to add a new	Inactive Proposal. IKE Pr	roposals are used by <u>Security</u>
<u>SSH</u>	Associations to specify IKE paran	neters.	
	17.45/3.		
	Active	25 A	Inactive
	Proposals	Actions	Proposals
	CiscoVPNClient-3DES-MD5-RSA		IKE-3DES-SHA-DSA
	IKE-3DES-MD5-DH1	· Activate	IKE-3DES-MD5-RSA-DH1
		Deactivate >>	IKE-DES-MD5-DH7
	IKE-3DES-MD5-BSA	Movellin	CiscoVPNClient-3DES-MD5-B:
	CiscoVPNClient-3DES-MD5-DH5	- Move Op	CiscoVPNClient-3DES-SHA-D:
	CiscoVPNClient-AES128-SHA	Move Down	CiscoVPNClient-AES256-SHA
CISCO SYSTEMS	IKE-AES128-SHA	Add	IKE-AES256-SHA
	CHACK-JUES-SHA-DHZ		HYDRID_AES128_SHA_RSA_
	<u></u>		
E IKE Proposals			📋 🔯 Internet 🥢

Modify the default IPsec SA "ESP-3DES-MD5":



Choose	the	digital	certificate	you	have	obtained	for	authentication:
--------	-----	---------	-------------	-----	------	----------	-----	-----------------

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3k] - Microsoft Internet Explorer	
<u>File Edit View Favorites Tools</u>	Help (= Back + => - 🙆 🚯 Address 🛃 http:	s://136.1.113.11/access.html
VPN 3	000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
- <u> Configuration</u> <u> Interfaces</u>	Measurement	keys.
	Data Lifetime 10000	Specify the data lifetime in kilobytes (KB).
Access Hours Orraffic Management Orraffic Management Network Lists	Time Lifetime 28800	Specify the time lifetime in seconds.
Rules SAs	IKE Parameters	
EW Policies	IKE Peer 0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Tetroroup Watching Tetroroup Watching Tetroroup Matching Tetroroup Matchin	Negotiation Mode Main	Select the IKE Negotiation mode to use.
-⊞ <u>Administration</u> -⊞ <u>Monitoring</u>	Digital Certificate VPN3k	Select the Digital Certificate to use.
	Certificate C Entire certificate chain Transmission • Identity certificate only	Choose how to send the digital certificate to the IKE peer.
	IKE Proposal IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.
Cisco Systems	Apply Cancel	-
IPSec Security Associations		📄 🔒 🔮 Internet 🏼 🏸

Make sure this SA is assigned to group EZVPN:

🕗 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Mic	rosoft Internet	Explorer		_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Back 🔹 🚍	- 🖉 🔄	Address 🛃 https://136.1	1.113.11/access.html	-
VPN 3	000			Main Hel	p Support Logout
Conce	ntrator Series N	lanager			Logged in: admin
		Ŭ	Config	uration Admini	stration Monitoring
	Can Succetion Hoos	M	Comuna Mardife E70	DN	
I <u>Interraces</u> I IIII-Sy <u>stem</u>	Configuration User	Managemen	Groups Mouny EZV	PN	
	Check the Inherit? t	oox to set a fie	ld that you want to defa	ault to the base g	roup value.
Base Group Groups	Uncheck the Inherit	? box and ente	er a new value to overri	de base group va	dues.
		IDC as Clian	A Comfort Closed FMC		DVLATID MARANON
<u> <u> </u></u>	Identity General	IPSec Chen		HW Client PPT	P/LZTP WebVPN
- <u>Administration</u>	Attributo		Volue	Tubovit?	Deceriptie
- <u>Monitoring</u>	Attribute		Value	Innerit :	Descriptio
	IPSec SA	ESP-3DES-N	4D5	N	Select the group's Security Associati
	IKE Peer Identity Validation	If supported I	oy certificate 💌	ঘ	Select whether or validate the identit peer using the pee: certificate.
	IKE Keepalives	J		ঘ	Check to enable tl IKE keepalives fo members of this gr
Cisco Systems	Confidence Interval	300		ম	(seconds) Enter ha a peer is permitted before the VPN Concentrator chec
Group Parameters					Internet

Verification

Connect Cisco VPN Client and monitor session on VPN3k:

🖉 Cisco Systems, Inc. VPN 3000 Con	centrator [¥PN3k] - Micro	soft Internet Explorer		_ 🗆 ×
<u>File Edit View Favorites Tools</u>	Help (⇒ Back → ⇒)	🗸 🔇 🕼 🛛 Address 🙋 http	os://136.1.113.11/access.ht	ml 🔄 🏢
VPN 3	000		Main He	elp Support Logout
Concer	ntrator Series Ma	anager		Logged in: admin
			Configuration Admir	ristration Monitoring
	IKE Sessions: 1			<u></u>
	IPSec Sessions: 1			
<u>Routing Table</u> <u>Dynamic Filters</u>		IKE Sessi	on	
	Session ID	1	Encryption Algorithm	3DES-168
Protocols Encryption 	Hashing Algorithm	MD5	Diffie-Hellman Group	Group 2 (1024-bit)
En <u>rop set and</u> En <u>Statistics</u>	Authentication Mode	RSA Certificate (XAUTH)	IKE Negotiation Mode	Main
	Rekey Time Interval	86400 seconds		
		IPSec Sess	ion	
	Session ID	2	Remote Address	20.0.0.1
	Local Address	0.0.0.0/255.255.255.255	Encryption Algorithm	3DES-168
	Hashing Algorithm	MD5	Idle Time	0:25:28
CISCO SYSTEMS	Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
	Rutas Rasaivad	n	Rutae Transmittad	
E Sessions	199 4 .			Internet

Further Reading

<u>Cisco - Configuring the VPN 3000 Concentrator to Communicate with the VPN</u> <u>Client Using Certificates</u>

VPN3k and IOS ezVPN Remote Client Mode with Split-Tunneling

Objective: Configure VPN3k to support IOS ezVPN Remote feature in Client mode.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"VPN3k ezVPN"</u>.
- In this task, R3 will be configured as ezVPN Remote device in Client mode. That is, it will simulate VPN Client behavior, requesting new IP address from VPN3k server.
- Create ezVPN client group on R3:
 - Use group name EZVPN with key CISCO.
 - Use peer 136.1.113.11.
 - Specify connect mode manual.
 - Specify client mode.
 - Configure E0/0 as outside interface.
 - Configure E0/1 as inside interface.
- Create network list to distinguish network 136.1.111.0/24, name it SPLIT_TUNNEL.
- Create new Group on VPN 3000 Concentrator:
 - Name EZVPN password CISCO.
- Configure IPsec as the only tunneling protocol.
- o Configure IPsec Remote Access Tunnel Type.
- o Configure IPsec Xauth.
- Modify group EZVPN, changing split-tunneling settings under "Client Config" Tab:
 - Tunnel only to networks in list.
 - Use network list SPLIT_TUNNEL.
- Assign Address Pool "20.0.0.1-20.0.0.254" to group EZVPN.
- Create new User on VPN 3000:
 - Name CISCO password CISCO1234
 - Group EZVPN
- Permit address allocation from Address Pools.

Final Configuration

```
R3:

crypto ipsec client ezvpn EZVPN

connect manual

group EZVPN key CISCO

mode client

peer 136.1.113.11

!

interface Ethernet0/0

crypto ipsec client ezvpn EZVPN

!

interface Ethernet0/1

crypto ipsec client ezvpn EZVPN inside
```

VPN3k:

Create new group:

🚰 Cisco Systems, Inc. VPN 3000 Con	centrator [VPI	N3k] - Microsoft Interne	t Explorer	_ 🗆 ×
<u>File Edit View Favorites Tools</u>	Help 🗇	Back 🔹 🖘 💌 🚺	Address 🙋 https://136.1.113.11/access.html	-
VPN 30	000		Main Help	Support Logout
Concen	trator Se	eries Manager		Logged in: admin
		0	Configuration Administra	ation Monitoring
- [] Configuration				
Interfaces	Configurati	on User Managemer	nt Groups Add	
	me .		CH 1 4 T 1 101	
Base Group	This section	lets you add a group.	Check the Inherit? box to set a field that y	ou want to
Groups	override has	e base group value. Or se group values	icheck the inner t? Box and enter a new va	ane to
	00000000	e group mades.		
	Identity 0	eneral TIPSec Clie	nt Config Client FW HW Client PPTP/I	2TP WebVPN
- Administration			Identity Parameters	
	Attribute	Value	Description	
	Group	EZVPN J	Enter a unique name for the group.	
	Password		Enter the password for the group.	
	Verify		Verify the group's password.	
	Туре	Internal 🔽	<i>External</i> groups are configured on an extern (e.g. RADIUS). <i>Internal</i> groups are configu Concentrator's Internal Database.	nal authentication se ared on the VPN 31
	Add	Cancel		
Cisco Systems	•	- 92 		
🙆 Group Parameters			📃 🔒 😻 Int	ernet //

Cisco Systems, Inc. VPN 3000 File Edit View Eavorites To	Concentrator [VPN3k] -	Microsoft Interne	Address Abtroci//126-1-1	12 11/2	cross html
VPN Cond	3000 centrator Series	Manager	Hourses Princips. (130-11)	13.11)a M:	ain Help Support Logout Logged in: admin
		0	Configui	ation	Administration Monitoring
		۳ <mark>.</mark>			primary DNS server. 🔺
Interfaces 	Secondary DNS			N	Enter the IP address of th secondary DNS server.
Base Group Groups	Primary WINS			N	Enter the IP address of th primary WINS server.
Users Users Declicy Management Declicy Management	Secondary WINS			ব	Enter the IP address of th secondary WINS server.
	Tunneling Protocols	□ PPTP □ L2TP ☞ IPSec □ L2TP over I □ WebVPN	PSec	Γ	Select the tunneling proto group can connect with.
	Strip Realm	–		ঘ	Check to remove the rea qualifier of the username authentication.
	DHCP Network Scope			ব	Enter the IP sub-network which users within this gr- be assigned when using th concentrator as a DHCP
CISCO SYSTEMS	Add C	Cancel	· · ·		>
街 Group Parameters					📋 🥶 Internet

Permit IPsec as the only tunneling protocol in General Tab:

<u>File Edit V</u> iew F <u>a</u> vorites <u>T</u> ool:	s <u>H</u> elp (⇔ Back →	🖙 🖌 💽 🚺 🛛 Add	lress 🙋 https://136.1.11	.3.11/access.ht	:ml 🔽 📲
VPN:	3000			Main H	elp Support Logo
Conce	entrator Series	Manager			Logged in: adm
			Configura	ition Admi	nistration Monitorii
H <u>Configuration</u> ——I <u>nterfaces</u>	override base group	values.			
–⊕- <u>System</u> –⊖- Iser Management	Identity General	IPSec Client Co	nfig Client FW HW	/ Client PF	TP/L2TP WebVPN
Base Group			IPSec Paramet	ers	
Users	Attribute	V	alue	Inherit?	Descripti
HPolicy Management Honitoring	IPSec SA	ESP-3DES-MD5		N	Select the group's I Security Association
	IKE Peer Identity Validation	If supported by certi	ificate 💌	ঘ	Select whether or no validate the identity using the peer's cert
	IKE Keepaliv <mark>e</mark> s	ম		ঘ	Check to enable the keepalives for mem group.
	Confidence Interval	300		ঘ	(seconds) Enter how peer is permitted to the VPN Concentra to see if it is still cor
Cisco Systems	Tunnel Type	Remote Access 💌		ঘ	Select the type of tu group. Update the l Access parameters

Make sure yoru group has Remote Access IPSec tunnel type:

And that you have authentication (Xauth) enabled in IPsec Tab:

<u>File Edit View Favorites T</u> ool	s <u>H</u> elp (⇒ Back → ≖	÷ - 🛛 🔁	Address 🖉 https://136.1.1	13.11/access.htm	ı 💽 🏢
VPN	3000			Main He	lp Support Logou
Conce	entrator Series N	Aanager			Logged in: admi
			Configui	ation Admini	istration Monitoring
Configuration					parameters below <u>-</u> needed.
— <u>⊞User Management</u>			Remote Access Parar	neters	
Base Group	Group Lock			N	Lock users into thi
Groups Users Users Groups Users Groups Groups	Authentication	Internal	×	ঘ	Select the authenti method for membe this group. This pa does not apply to Individual User Authentication.
	Authorization Type	None 💌		ঘ	If members of this need authorization addition to authent select an authoriza method. If you cor this field, you must configure an Autho Server.
	Authorization Required			N	Check to require successful authoriz
CISCO SYSTEMS					For certificate-bas



Create Network List for split-tunneling:

Modify group "EZVPN", "Client Config" Tab. Chose "Only tunnel networks in the list":

🖉 Cisco Systems, Inc. VPN 3000 C	Concentrator [VPN:	Bk] - Microsoft Internet Explorer		
<u>Eile Edit View Favorites Too</u>	ols <u>H</u> elp 🗘 B	ack 🔹 🖘 👻 👔 🛛 Address 🛃 https://13	6.1.113.11/	access.html
VPN Conc	3000	rias Managar	M	1ain Help Support Logout
Conc	entrator ser	Cunf	inuration	Logged in: admin
-[]Configuration Interfaces				
Base Group Groups Gr	Split Tunneling Policy	 Tunnel everything Allow the networks in list to bypass the tunnel Only tunnel networks in the list 		Select the method and net to be used for Split Tunnel Tunnel Everything: Sen- traffic through the tunnel. Allow the networks in th bypass the tunnel: The V Client may choose to send to addresses in this list to t client's LAN. Send all oth
	Split Tunneling Network List	-None- -None- VPN Client Local LAN (Default) SPLIT_TUNNEL	ঘ	through the tunnel. NOTE setting only applies to the VPN Client. Tunnel networks in the Send traffic to addresses i through the tunnel. Send a traffic to the client's LAN.
Ciero Svetche	Default Domain Name		N	Enter the default domain n given to users of this group
	1			Enter the set of domains,
Ø Group Parameters				🔒 🍘 Internet

Modify address pools for a Group:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	et Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help ← Back → ⇒ → 🔇 🗗	Address 🖉 https://136.1.11	3.11/access.html
VPN 3	3000		Main Help Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configura	tion Administration Monitoring
	C- C- M-	ALC	
<u>Interfaces</u> —⊕ <u>System</u>	Configuration User Manageme	nt Groups Address Pools	Save Needed
- EH <u>User Management</u>			
Groups	This section lets you configure ${\rm I\!P}$	Address Pools.	
	Click the Add button to add a po	ol entry or select a range an	d click Modify Delete or
<u>-⊕-Tunneling and Security</u>	Move. Click Done to finish.	or charge, or beleet a range an	a choic initiality, is choice of
-⊞ <u>Administration</u>			
	A	ddress Pool for EZVPN	
	Ш	Pool Entry Actions	
	F	Empty Add	
		Modify	
		Delete	
		Mayalla	
		O	
		Move Down	
		Done	
Cisco Systems			
Filters and Access Policies			📋 🎒 🔮 Internet 🍡 🍂

🚰 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Interne	t Explorer	_ 🗆 ×		
Eile Edit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	; Help 🗘 🖙 Back 🔹 🖘 🗸 🚺	Address 🛃 https://136.1.113.11/access.html	-		
VPN 3	3000	Main Help St	upport Logout		
Conce	entrator Series Manager	Lo	gged in: admin		
		Configuration Administration	un Munituring		
-E- <u>Configuration</u> <u>Interfaces</u> 	Configuration User Managemen	t Groups Address Pools Add			
	Add an address pool.				
Users	Range Start 20.0.0.1	Enter the start of the IP pool address range.			
<u> </u>	Range End 20.0.0.254	Enter the end of the IP pool address range.			
-@- <u>Administration</u> -@ <u>Monitoring</u>	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				
CISCO SYSTEMS					
Filters and Access Policies		📔 📔 👔 Intern	et //		

Add new user "CISCO/CISCO1234" to group "EZVPN":

🖉 Cisco Systems, Inc. VPN 3000 Conce	entrator [VPN3	k] - Microsoft Interne	t Explorer	
<u>File Edit View Favorites Tools</u>	Help 🗘 🗇 Ba	ck 🔹 🔿 🔺 🚺	Address Addres	
VPN 30	00		Main Help Support Lo	gout
Concent	trator Ser	ies Manager	Logged in: a	Idmin
			Configuration Administration Monit	uriny
Configuration	Configuration	User Managemer	ıt Users Add	
	This section le override group Identity Ge	ts you add a user. U 9 values. neral IPSec PPT	ncheck the Inherit? box and enter a new value to	
<u> </u>		I	lentity Parameters	
-⊞ <u>Administration</u> -⊞ <u>Monitoring</u>	Attribute	Value	Description	
	Username	CISCO	Enter a unique username.	
	Password	yaalaalaalaa	Enter the user's password. The password must satisfy the group password requirements.	
	Verify	Jololololololol	Verify the user's password.	
	Group	EZVPN 🔽	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.	
CISCO SYSTEMS	Add	Cancel		
thin				
🕙 User Parameters			📄 🎽 💣 Internet	1.

Allow IP address Assignment from Address Pools:



Verification

```
R3#crypto ipsec client ezvpn connect
R3#
*Mar
     2 02:30:23.220: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
*Mar 2 02:30:23.220: EZVPN: crypto ipsec client ezvpn xauth
R3#crypto ipsec client ezvpn xauth
Enter Username and Password.: CISCO
Password: : CISCO1234
R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC ACTIVE
Last Event: SOCKET_UP
Address: 20.0.0.1
Mask: 255.255.255.255
Split Tunnel List: 1
```

```
Copyright © 2007 Internetwork Expert
```

```
Address
                  : 136.1.111.0
       Mask : 255.255.255.0
       Protocol
                : 0x0
       Source Port: 0
       Dest Port : 0
R3#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list internet-list interface Ethernet0/0 refcount 0
[Id: 1] access-list enterprise-list pool EZVPN refcount 0
pool EZVPN: netmask 255.255.255.0
        start 20.0.0.1 end 20.0.0.1
        type generic, total addresses 1, allocated 0 (0%), misses 0
R3#ping 136.1.111.1 source ethernet 0/1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.111.1, timeout is 2 seconds:
Packet sent with a source address of 136.1.100.3
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms
R3# show ip nat translations
Pro Inside global
                     Inside local
                                         Outside local
                                                              Outside global
                      136.1.100.3:8471 136.1.111.1:8471 136.1.111.1:8471
icmp 20.0.0.1:8471
                                          136.1.111.1:8472
136.1.111.1:8473
icmp 20.0.0.1:8472
                       136.1.100.3:8472
                                                              136.1.111.1:8472
                      136.1.100.3:8473
icmp 20.0.0.1:8473
                                                              136.1.111.1:8473
icmp 20.0.0.1:8474 136.1.100.3:8474 136.1.111.1:8474 136.1.111.1:8474
icmp 20.0.0.1:8475
                      136.1.100.3:8475 136.1.111.1:8475 136.1.111.1:8475
R3#sh cry isakmp sa
                                               conn-id slot
dst
               src
                                state
136.1.113.11
               136.1.113.3
                                QM_IDLE
                                                     1
                                                           Ω
R3#show cry ipsec sa
interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.113.3
   protected vrf:
   local ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (136.1.111.0/255.255.255.0/0/0)
   current_peer: 136.1.113.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #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.: 136.1.113.3, remote crypto endpt.: 136.1.113.11
     path mtu 1500, media mtu 1500
     current outbound spi: 31B8C3A
```

```
Copyright © 2007 Internetwork Expert
```

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
inbound esp sas:
spi: 0xC5A8C13C(3316171068)
   transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4539243/27495)
  IV size: 8 bytes
   replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x31B8C3A(52137018)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
  sa timing: remaining key lifetime (k/sec): (4539243/27495)
   IV size: 8 bytes
   replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

ezVPN Remote Phase I

VPN3k and IOS ezVPN Remote NW Extension Mode with RRI

Objective: Configure VPN3k for ezVPN Remote in network extension mode with RRI into OSPF.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"VPN3k and IOS ezVPN Remote Client Mode with Split Tunneling"</u>.
- Re-configure R3, and change ezVPN mode to "network-extension".
- Network Extension mode does not need an additional IP address from VPN 3000, and router does not enable NAT automatiacally.
- Therefore, you may disable IP address allocation in global Configuration.
- Additionally, you need to permit network extension mode, under "HW Client" Tab of group "EZVPN".
- The key point with RRI into OSPF is to configure ASBR feature on the VPN3k, so that it starts advertising external routes into OSPF.
- Also, you have to enable Network Extension RRI under IP Routing Configuration.
- Configure R1:
 - Remove static default route on R1 and configure OSPF routing as per the diagram.
- Enable OSPF process on VPN3k
 - Use router-id 150.X.11.11.

- o Permit ASBR feature
- Enable OSPF on the Private interface of the VPN3k. Use Area 0.

```
Final Configuration
```

```
R1:
no ip route 0.0.0.0 0.0.0.0 136.1.111.11
1
router ospf 1
network 136.1.111.0 0.0.0.255 area 0
VPN3k CLI:
Configure OSPF on the Private Interface:
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 2
1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back
VPN3k: System -> 3
1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back
VPN3k: Routing -> 3
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
```

```
Copyright © 2007 Internetwork Expert
```

```
VPN3k: OSPF -> 2
> Router ID
VPN3k: OSPF -> [ 0.0.0.0 ] 150.1.11.11
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> 1
1) Enable OSPF
2) Disable OSPF
VPN3k: OSPF -> [ 2 ] 1
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> 3
1) Enable Autonomous System
2) Disable Autonomous System
VPN3k: OSPF -> [ 2 ] 1
1) Enable/Disable OSPF
2) Set Router ID
3) Enable/Disable Autonomous System
4) Back
VPN3k: OSPF -> h
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
VPN3k: Main -> 1
1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back
VPN3k: Config -> 1
This table shows current IP addresses.
                       IP Address/Subnet Mask
            Status
                                                     MAC Address
 Intf
 _____
Ether1-PriUP|136.1.111.11/255.255.255.0|00.03.A0.88.BD.29Ether2-PubUP|136.1.113.11/255.255.255.0|00.03.A0.88.BD.2A
_____
```

```
Copyright © 2007 Internetwork Expert www.InternetworkExpert.com
```

```
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured
1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back
VPN3k: Interfaces -> 1
1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Set Interface Name
4) Select IP Filter
5) Select Ethernet Speed
6) Select Duplex
7) Set MTU
8) Set Port Routing Config
9) Set Bandwidth Management
10) Set Public Interface IPSec Fragmentation Policy
11) Set Interface WebVPN Parameters
12) Back
VPN3k: Ethernet Interface 1 -> 8
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 1 -> 3
1) Enable OSPF
2) Disable OSPF
VPN3k: Ethernet Interface 1 -> [ 2 ] 1
1) Set Inbound RIP Options
2) Set Outbound RIP Options
3) Enable/Disable OSPF
4) Set OSPF parameters
5) Back
VPN3k: Ethernet Interface 1 -> 4
1) Set OSPF Area ID
2) Set OSPF Priority
3) Set OSPF Metric
4) Set OSPF Retransmit Interval
5) Set OSPF Hello Interval
6) Set OSPF Dead Interval
7) Set OSPF Transit Delay
8) Set OSPF Authentication
9) Back
VPN3k: Ethernet Interface 1 -> 1
> OSPF Area ID
VPN3k: Ethernet Interface 1 -> [ 0.0.0.0 ] 0.0.0.0
```

Set OSPF Area ID
 Set OSPF Priority
 Set OSPF Metric
 Set OSPF Retransmit Interval
 Set OSPF Hello Interval
 Set OSPF Dead Interval
 Set OSPF Transit Delay
 Set OSPF Authentication
 Back

VPN3k GUI:

Disable address assignment:





Enable RRI for Network Extension Prefixes:

Allow Network Extensiion mode for the group "EZVPN":

🚈 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Int	ernet Explorer		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 🖙 Help	🚯 🛛 A <u>d</u> dress 餐 H	ttps://136.1	.113.11/access.html
VPN 3	000			Main Help Support Logout
Conce	ntrator Series Manag	er		Logged in: admin
			Configu	nation Administration Monitoring
- <u> Configuration</u> <u> Interfaces</u>	Configuration User Manage	ement Groups Me	odify EZVF	PN A
	Check the Inherit? box to se Uncheck the Inherit? box an	t a field that you wa d enter a new value	ant to defa to overric	ult to the base group value. le base group values.
<u> <u> </u></u>	Identity General IF Sec	Hardware C	lient Pa	
- Administration	Attribute	Value	Inherit?	Description
	Require Interactive Hardware Client Authentication		ঘ	Check to require the hardware cli- interactively authenticated at each connection attempt.
	Require Individual User Authentication		ম	Check to require users behind a h client to be authenticated.
	User Idle Timeout	30	N	Enter the session idle timeout in m Use 0 for no timeout.
	Cisco IP Phone Bypass		ঘ	Check to allow Cisco IP Phones t bypass Individual User Authentica behind a hardware client.
CISCO SYSTEMS	LEAP Bypass		ঘ	Check to allow LEAP packets fro wireless access points to bypass I User Authentication.
Click to expand nested items				Internet

🚰 Cisco Systems, Inc. VPN 3000 C	Concentrator [VPN3k] - Microsoft Int	ernet Explorer		_ O ×
<u>File Edit View Favorites Too</u>	ols Help (> Back + => + (>)	🕼 Address 🩋	https://136.1	.113.11/access.html
VPN	3000			Main Help Support Logout
Conc	entrator Series Manag	er		Logged in: admin
			Configu	nation Administration Monitoring
<u>Configuration</u>	Identity General IPSec	Client Config (Client FW H	IW Client PPTP/L2TP WebVPN
<u>—⊞System</u>		Hardware	Client Pa	rameters
	Attribute	Value	Inherit?	Description
Groups Users 	Require Interactive Hardware Client Authentication		ঘ	Check to require the hardware cli- interactively authenticated at each connection attempt.
	Require Individual User Authentication		N	Check to require users behind a h client to be authenticated.
	User Idle Timeout	30		Enter the session idle timeout in m Use 0 for no timeout.
	Cisco IP Phone Bypass		অ	Check to allow Cisco IP Phones t bypass Individual User Authentica behind a hardware client.
	LEAP Bypass		অ	Check to allow LEAP packets fro wireless access points to bypass I User Authentication.
	Allow Network Extension Mode	N		Check to allow hardware clients u Network Extension Mode to conr
CISCO SYSTEMS	Apply Cancel			
Tunneling and Security				📔 🔮 Internet

Verification

```
R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Split Tunnel List: 1
       Address : 136.1.111.0
Mask : 255.255.255.0
Protocol : 0x0
       Source Port: 0
       Dest Port : 0
R3#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
 Ethernet0/1
Hits: 10 Misses: 10
Expired translations: 10
Dynamic mappings:
```

Copyright © 2007 Internetwork Expert

```
-- Inside Source
[Id: 3] access-list internet-list interface Ethernet0/0 refcount 0
Check for RRI-injected route:
R1#show ip route ospf
    136.1.0.0/24 is subnetted, 4 subnets
O E2
        136.1.0.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0
O E2
        136.1.23.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0
0 E2 136.1.100.0 [110/20] via 136.1.111.11, 00:00:27, Ethernet0/0
    10.0.0/24 is subnetted, 1 subnets
      10.0.0.0 [110/20] via 136.1.111.11, 23:54:52, Ethernet0/0
O E2
R1#ping 136.1.100.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
R1#
R3#show crypto isakmp sa
dst
                src
                               state
                                              conn-id slot
136.1.113.11 136.1.113.3
                               QM_IDLE
                                                      1
                                                           Ω
R3#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.113.3
   protected vrf:
   local ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.111.0/255.255.255.0/0/0)
   current_peer: 136.1.113.11:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #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.: 136.1.113.3, remote crypto endpt.: 136.1.113.11
     path mtu 1500, media mtu 1500
     current outbound spi: 1D1B61D3
     inbound esp sas:
      spi: 0xCA9D083A(3399288890)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4434055/28659)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x1D1B61D3(488333779)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
```

```
Copyright © 2007 Internetwork Expert
```

slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
sa timing: remaining key lifetime (k/sec): (4434055/28659)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:

outbound pcp sas:

Further Reading

Configuring the Cisco EzVPN Client on Cisco IOS with the VPN 3000 Concentrator

IOS and IOS ezVPN Remote Client Mode with Xauth/RRI

Objective: Configure IOS router to support ezVPN Remote connections and redistribute connected host routes.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"IOS ezVPN".</u>
- Configure R3 as ezVPN Server:
 - Enable AAA and make sure console is unaffected.
 - Configure ISAKMP Policy.
 - Use DH Group 2.
 - Use 3DES cipher.
 - Use MD5 hash.
 - Use Pre-Shared authentication.
 - Configure IP addressing for remote clients.
 - Create local IP address pool EZVPN: 20.0.0.1-20.0.0.254.
 - Configure ISAKMP to use this pool.
 - Configure split-tunneling ACL, name it "SPLIT_TUNNEL":
 - Permit network 136.X.100.0/24 to be tunneled.
 - o Configure ISAKMP Authorization parameters.
 - Configure network AAA authorization list named EZVPN, user local database.
 - Create ISAKMP configuration group "EZVPN":
 - Specify key "CISCO".

- Use local pool "EZVPN".
- Use split-tunnel list "SPLIT_TUNNEL".
- Configure crypto-map VPN to use ISAKMP authorization list "EZVPN".
- Configure crypto-map VPN to respond to IKE configuration requests.
- Configure client authentication:
 - Configure AAA authentication list for login named "EZVPN", use local database.
 - Create local username CISCO with password CISCO1234.
 - Configure crypto-map VPN to use client authentication AAA list EZVPN. This will activate Xauth.
- Configure crypto:
 - Create crypto transform-set 3DES_MD5:
 - Use 3DES cipher.
 - Use MD5 hash.
 - Create dynamic crypto-map DYNAMIC:
 - Apply 3DES_MD5 transform-set.
 - Enable reverse-route injection
 - Configure crypto-map VPN entry 10:
 - Use type IPsec-ISAKMP.
 - Use dynamic crypt-map DYNAMIC.
 - Apply crypto-map to interface Eth0/0.
- Redistribute static routes into RIP. This way you make remote router visible in the routing domain.
- Configure R1 as ezVPN Remote in client mode:
 - Create ezVPN group named "EZVPN":
 - Use group name "EZVPN" and key CISCO.
 - Specify manual connect mode.
 - Specify peer 136.X.123.3
 - Configure interface Ethernet 0/0 as ezVPN outside
 - Configure interface Loopback0 as ezVPN inside.

Final Configuration

```
R3:
aaa new-model
aaa authentication login CONSOLE none
!
! ezVPN Authorization & Authentication
!
aaa authorization network EZVPN local
aaa authentication login EZVPN local
!
! Local username for Xauth
!
username CISCO pass CISCO1234
!
line con 0
```

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 309 -

```
login authentication CONSOLE
!
! Configure ISAKMP policy
! Note the pre-shared key and group 2
! DH Group 2 should be used for ezVPN Remote
crypto isakmp policy 10
authentication pre-share
 encr 3des
hash md5
group 2
1
! Configure local address pool
! Configure ISAKMP to use this address pool
ip local pool EZVPN 20.0.0.1 20.0.0.254
crypto isakmp client configuration address-pool local EZVPN
1
! Split-tunnel ACL
1
ip access-list extended SPLIT_TUNNEL
permit ip 136.1.100.0 0.0.0.255 any
!
! Configure ISAKMP Group
T
crypto isakmp client configuration group EZVPN
 kev CISCO
 pool EZVPN
 acl SPLIT_TUNNEL
! Configure IPsec transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Dynamic crypto map
!
crypto dynamic-map DYNAMIC 10
 set transform-set 3DES MD5
  reverse-route
!
! RRI into RIP
!
router rip
redistribute static
!
! Configure crypto-map for authorization & authentication
!
crypto map VPN isakmp authorization list EZVPN
!
! Activating client authentication enables Xauth
!
crypto map VPN client authentication list EZVPN
crypto map VPN client configuration address respond
1
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
! Attach crypto-map to an interface
interface E 0/0
crypto map VPN
R1:
crypto ipsec client ezvpn EZVPN
```

Copyright © 2007 Internetwork Expert

```
group EZVPN key CISCO
connect manual
peer 136.1.123.3
!
interface E 0/0
crypto ipsec client ezvpn EZVPN
!
interface Loopback0
crypto ipsec client ezvpn EZVPN inside
```

Verification

```
R1#crypto ipsec client ezvpn connect
*Mar 1 00:09:10.577: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
*Mar 1 00:09:10.577: EZVPN: crypto ipsec client ezvpn xauth
R1#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234
Rl#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : EZVPN
Inside interface list: Loopback0,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 20.0.0.2
Mask: 255.255.255.255
Split Tunnel List: 1
       Address : 136.1.100.0
       Mask : 255.255.255.0
       Protocol : 0x0
       Source Port: 0
       Dest Port
                 : 0
R1#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
 Ethernet0/0
Inside interfaces:
 Loopback0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list internet-list interface Ethernet0/0 refcount 0
[Id: 1] access-list enterprise-list pool EZVPN refcount 0
pool EZVPN: netmask 255.255.255.0
        start 20.0.0.2 end 20.0.0.2
        type generic, total addresses 1, allocated 0 (0%), misses 0
R1#ping 136.1.100.3 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
```

```
Copyright © 2007 Internetwork Expert
```

11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/12 ms R1#show ip nat translations Inside local Outside local Pro Inside global Outside global 136.1.100.3:3391 136.1.100.3:3391 icmp 20.0.0.2:3391 150.1.1.1:3391 icmp 20.0.0.2:3392 150.1.1.1:3392 136.1.100.3:3392 136.1.100.3:3392 136.1.100.3:3393136.1.100.3:3393136.1.100.3:3394136.1.100.3:3394 icmp 20.0.0.2:3393 150.1.1.1:3393 icmp 20.0.0.2:3394 150.1.1.1:3394 136.1.100.3:3395 136.1.100.3:3395 icmp 20.0.0.2:3395 150.1.1.1:3395 R1#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.121.1 protected vrf: local ident (addr/mask/prot/port): (20.0.0.2/255.255.255.255/0/0) remote ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0) current_peer: 136.1.123.3:500 PERMIT, flags={origin_is_acl,} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5 #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.: 136.1.121.1, remote crypto endpt.: 136.1.123.3 path mtu 1500, media mtu 1500 current outbound spi: 953B01EC inbound esp sas: spi: 0x734BD2AE(1934348974) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0 sa timing: remaining key lifetime (k/sec): (4588571/3570) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x953B01EC(2503672300) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0 sa timing: remaining key lifetime (k/sec): (4588571/3570) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: R3#show ip route static 20.0.0/32 is subnetted, 1 subnets 20.0.0.2 [1/0] via 136.1.121.1 S R2#show ip route rip Accessed by swami, vikas@gmail.com from 202.177.171.138 at 02:14:45 Mar 17,2008

Copyright © 2007 Internetwork Expert

```
136.1.0.0/24 is subnetted, 5 subnets
       136.1.100.0 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
R
        136.1.121.0 [120/2] via 136.1.23.3, 00:00:18, Serial0/1
R
R
        136.1.123.0 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
     20.0.0/32 is subnetted, 1 subnets
        20.0.0.2 [120/1] via 136.1.23.3, 00:00:18, Serial0/1
R
     150.1.0.0/24 is subnetted, 2 subnets
        150.1.1.0 [120/3] via 136.1.23.3, 00:00:18, Serial0/1
R
R3#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
      psk - Preshared key, rsig - RSA signature
      renc - RSA encryption
C-id Local
                      Remote
                                    I-VRF
                                               Encr Hash Auth DH Lifetime Cap.
                     136.1.121.1
                                               3des md5 2 23:55:49 CX
     136.1.123.3
1
R3#show crypto ipsec sa
interface: Ethernet0/0
  Crypto map tag: VPN, local addr. 136.1.123.3
  protected vrf:
   local ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (20.0.0.2/255.255.255.255/0/0)
   current_peer: 136.1.121.1:500
    PERMIT, flags={}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #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.: 136.1.123.3, remote crypto endpt.: 136.1.121.1
     path mtu 1500, media mtu 1500
     current outbound spi: 734BD2AE
     inbound esp sas:
     spi: 0x953B01EC(2503672300)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4384197/3348)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x734BD2AE(1934348974)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4384197/3348)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
```

Copyright © 2007 Internetwork Expert

outbound pcp sas:

Further Reading

Cisco Easy VPN Remote Feature Easy VPN Server

IOS and IOS ezVPN Remote NW Extension Mode with Xuath/RRI

Objective: Configure ezVPN server to accept ezVPN Remote in networkextension mode.



Directions

- Configure devices as per the scenario "VPN/ezVPN" <u>"IOS and IOS ezVPN Remote Client Mode with Xauth/RRI"</u>.
- In network extension mode, remote client does not need new IP address to be allocated.
- Hence, you may remove the following from R3's configuration:
 - Reference to local address pool EZVPN from group EZVPN.
 - ISAKMP reference to address-pool EZVPN.
 - o Local IP pool EZVPN.
 - "client configuration address respond" statement from crypto-map VPN.
- Configure ezVPN client on R1 to use network-extension mode.

Final Configuration

```
R3:

crypto isakmp client config group EZVPN

no pool EZVPN

!

no crypto isakmp client configuration address-pool local EZVPN

no crypto map VPN client configuration address respond

no ip local pool EZVPN
```

Copyright © 2007 Internetwork Expert

R1: crypto ipsec client ezvpn EZVPN mode network-extension

Verification

```
R1#crypto ipsec client ezvpn connect
R1#
.Jan 19 17:54:52.206: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
.Jan 19 17:54:52.206: EZVPN: crypto ipsec client ezvpn xauth
R1#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234
R1#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : EZVPN
Inside interface list: Loopback0,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Split Tunnel List: 1
       Address : 136.1.100.0
       Mask : 255.255.255.0
Protocol : 0x0
       Source Port: 0
       Dest Port : 0
R1#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
 Loopback0
Hits: 5 Misses: 5
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 5] access-list internet-list interface Ethernet0/0 refcount 0
R1#ping 136.1.100.3 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/13 ms
R1#show crypto isakmp sa
dst
                                state
                                               conn-id slot
                src
                136.1.121.1
                                QM_IDLE
136.1.123.3
                                                   122
                                                           0
R1#show crypto ipsec sa
interface: Ethernet0/0
    Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.121.1
```

Copyright © 2007 Internetwork Expert

```
protected vrf:
  local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
current_peer: 136.1.123.3:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #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.: 136.1.121.1, remote crypto endpt.: 136.1.123.3
     path mtu 1500, media mtu 1500
     current outbound spi: CA5E3CB
     inbound esp sas:
      spi: 0x2FBDC4BD(800965821)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4457618/3396)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xCA5E3CB(212198347)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
        sa timing: remaining key lifetime (k/sec): (4457618/3396)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R3#show ip route static
    150.1.0.0/24 is subnetted, 1 subnets
        150.1.1.0 [1/0] via 136.1.121.1
```

Further Reading

S

Cisco Easy VPN Remote Feature Easy VPN Server

PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI

Objective: Configure the PIX/ASA firewall to support Cisco VPN Clients.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"The PIX/ASA Easy VPN/WebVPN"</u>.
- The PIX/ASA VPN configuration borrowed many concepts from IOS and VPN 3000. You configure crypto maps and ISAKMP policy just like you do on IOS (and older PIX).
- However you define tunnel group, group policy and attributes similar to VPN3000.
- Like with VPN3000 group attributes inherit their default values from default system groups. Take this in consideration, while configuring VPN.
- If you'd like to see the defaults, simply issue the following:

"show run all tunnel-group" "show run all group-policy".

• Configure ISAKMP as follows:

0

- Enable ISAKMP on the outside interface.
 - Configure ISAKMP policy with priority 10:
 - Use Pre-Shared authentication.
 - Use 3DES cipher.
 - Use MD5 hash.

- Use DH group 2.
- Configure VPN addressing:
 - Enable address allocation from local pools.
 - Create local-pool EZVPN with address range:
 - 20.0.0.1-20.0.0.254
- Create access-list SPLIT_TUNNEL:
 - Permit network 136.X.121.0/24.
- Add a local user for Xauth:
 - Create local user "CISCO" with password "CISCO1234".
- Define group-policy named EZVPN as internal:
 - Configure IPsec as the tunneling protocol.
 - Configure DNS server 10.0.0.100.
 - o Specify split-tunneling policy "only tunnel networks in the list".
 - Assign split-tunnel network-list SPLIT_TUNNEL
- Define tunnel group:
 - Create tunnel group "EZVPN" of type Remote-Access.
 - o Group General Attributes:
 - Set authentication-server group to "LOCAL" (it's the default value, inherited from default group).
 - Specify address pool "EZVPN".
 - Assign group-policy "EZVPN".
 - Group IPSec Attributes:
 - Specify pre-shared key "CISCO".
- Configure crypto:
 - Create transform-set 3DES_MD5:
 - Cipher 3DES.
 - Hash MD5.
 - Create dynamic crypto-map DYNAMIC entry 10:
 - Set transform-set 3DES_MD5
 - Set reverse-route
 - Create crypto-map VPN entry 10 to use dynamic crypto-map DYNAMIC.
 - o Attach crypto-map VPN to interface outside.
 - Explicitly permit VPN traffic to pass through acess-lists.
- Redistribute static routes into RIP (this will redistribute RRI routes).

Final Configuration

```
ASA1:

!

! ISAKMP configuration

!

crypto isakmp enable outside

crypto isakmp policy 10

auth pre-share

encr 3des

hash md5
```

```
group 2
!
! Enable VPN address allocation from local pools
! Note that it's enabled by default with the PIX/ASA
!
vpn-addr-assign local
1
! Local address pool
ip local pool EZVPN 20.0.0.1-20.0.0.254
! Split-tunneling ACL
access-list SPLIT_TUNNEL permit ip 136.1.121.0 255.255.255.0 any
!
! Local username for Xauth
!
username CISCO password CISCO1234
!
! Tunnel-group policy
!
group-policy EZVPN internal
group-policy EZVPN attributes
vpn-tunnel-protocol IPSec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value SPLIT_TUNNEL
dns-server value 10.0.0.100
!
! Tunnel-group definition
! Note that "authentication-server-group"
! is LOCAL by default
tunnel-group EZVPN type ipsec-ra
tunnel-group EZVPN general-attributes
 authentication-server-group LOCAL
 address-pool EZVPN
 default-group-policy EZVPN
tunnel-group EZVPN ipsec-attributes
 pre-shared-key CISCO
! IPsec transform-set
1
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Dynamic crypto-map
crypto dynamic-map DYNAMIC 10 set transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 10 set reverse-route
!
! Define crypto-map
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
1
! Attach crypto map to the interface
crypto map VPN interface outside
! Permit VPN traffic to bypass ACLs
1
sysop connection permit-vpn
! Redistribute static routes into RIP
```

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 320 -
```
router rip
redistribute static
```

```
Verification
Configure Cisco VPN client to connect to the ASA:
   • Use group name EZVPN and password "CISCO".
   • Use username/password CISCO/CISCO1234 when prompted for Xauth.
Check connected sessions:
ASA1(config)# show vpn-sessiondb remote
Session Type: Remote
             : CISCO
Username
Index
             : 1
Assigned IP : 20.0.0.1
                                       Public IP : 136.1.100.200
             : IPSec
Protocol
                                       Encryption
                                                    : 3DES
            : MD5
Hashing
Bytes Tx : 978500
Client Type : WinNT
                                                    : 978500
                                       Bvtes Rx
                                       Client Ver : 4.8.01.0300
Group Policy : EZVPN
Tunnel Group : EZVPN
Login Time : 07:10:40 UTC Mon Jan 22 2007
Duration
             : 0h:09m:50s
Filter Name
NAC Result : N/A
   Posture Token:
Check the ASA's routing table after connection has been established:
ASA1(config) # show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       \ensuremath{\texttt{D}} - EIGRP, EX - EIGRP external, \ensuremath{\texttt{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
     136.1.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:22, outside
R
     136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:22, outside
R
     136.1.100.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:22, outside
R
С
     136.1.121.0 255.255.255.0 is directly connected, inside
     136.1.123.0 255.255.255.0 is directly connected, outside
C
S 20.0.0.1 255.255.255.255 [1/0] via 136.1.123.3, outside
R
     10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:22, outside
R
     150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:23, inside
R1#sho ip route rip
     136.1.0.0/24 is subnetted, 5 subnets
R
        136.1.0.0 [120/3] via 136.1.121.12, 00:00:12, Ethernet0/0
R
        136.1.23.0 [120/2] via 136.1.121.12, 00:00:12, Ethernet0/0
        136.1.100.0 [120/2] via 136.1.121.12, 00:00:12, Ethernet0/0
R
R
        136.1.123.0 [120/1] via 136.1.121.12, 00:00:12, Ethernet0/0
     20.0.0/32 is subnetted, 1 subnets
```

20.0.0.1 [120/1] via 136.1.121.12, 00:00:12, Ethernet0/0 R 10.0.0/24 is subnetted, 1 subnets R 10.0.0.0 [120/3] via 136.1.121.12, 00:00:12, Ethernet0/0 R1#ping 20.0.0.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/10/36 ms ASA1(config-router)# show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 IKE Peer: 136.1.100.200 1 Type : user Role : responder Rekey : no State : AM_ACTIVE ASA1(config-router)# show crypto ipsec sa interface: outside Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0) current_peer: 136.1.100.200, username: CISCO dynamic allocated peer ip: 20.0.0.1 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5 #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.: 136.1.123.12, remote crypto endpt.: 136.1.100.200 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 010C3FDC inbound esp sas: spi: 0xA17A46D4 (2709145300) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 6, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 28402 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x010C3FDC (17579996) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 6, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 28402 IV size: 8 bytes replay detection support: Y Check VPN Client Statistics:

	1 Houte Details		
Address Inf Client: Server:	ormation 20.0.0.1 136.1.123.12	Connection Inform Entry: Time:	ation EZVPN 0 day(s), 00:06.02
Bytes Received Sent:	t: 500 500	Crypto Encryption: Authentication:	168-bit 3-DES HMAC-MD5
Packets Encrypte Decrypte Discarde Bypassed	±5 ±5 ±5 ±1414	Transport Transparent Tunr Local LAN: Compression:	neling:Inactive Disabled None Beset
VPN Client	Statistics		<u>C</u> lose
VPN Client	Statistics Route Details	Firewall	<u>C</u> lose
VPN Client Tunnel Details Local LAN Ro Network	Statistics	Firewall Secured Rou	
VPN Client	Statistics Boute Details Utes Subnet Mask	Firewall Secured Rou k Network 136.1.121.0	<u>Close</u> Ites Subnet Mask 255.255.255.0

Further Reading Configuring Remote Access VPNs

PIX/ASA and Cisco VPN Client with External Policy

Objective: Configure the PIX/ASA to apply external group policy from RADIUS server to remote-access VPN connections.



Directions

- Configure devices as per the scenario "VPN/ezVPN"
 <u>"The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI"</u>.
- The concept of group policy is decoupled from group definition with the PIX/ASA configuration. This makes it easy to change policy, retaining the group attributes.
- Note that with VPN3000 group policy is bound to a group itself, and VPN3000 uses the group password when retreiving group attributes.
- What we want, is to authenticate user locally on the firewall, yet download policy from RADIUS server.
- First, define a RADIUS server on the firewall:
 - Define server protocol to be RADIUS.
 - Define server to reside on the "outside":
 - Use CISCO as communication key.
 - Use CISCO as key for authorization transactions.
- Delete previously configured internal group-policy EZVPN.
- Configure external group-policy EZVPN to use server-group RADIUS and password CISCO.
- ACS Configuration:
 - o Configure ACS server to support new RADIUS client.
 - Configure ACS Interface and permit ASA RADIUS attributes.

- Create group EZVPN and set values for ASA RADIUS attributes:
 - Tunneling-Protocols = "IPsec".
 - IPsec-Authentication = "Internal".
 - Split-Tunneling-Policy = "Only Tunnel networks in the List".
- Split-Tunneling-List = "SPLIT_TUNNEL".
 Create user with name "EZVPN" and password matching the password you specified for group policy.
- Assign user "EZVPN" to group "EZVPN".

Final Configuration

```
ASA1:

aaa-server RADIUS protocol radius

aaa-server RADIUS (outside) host 10.0.0.100

key CISCO

radius-common-pw CISCO

!

clear configure group-policy EZVPN

group-policy EZVPN external server-group RADIUS password CISCO
```

ACS:

Add new AAA client:

🖉 CiscoSecure ACS - I	Microsoft Internet Explo	er		
<u>File E</u> dit <u>V</u> iew F <u>a</u>	vorites <u>T</u> ools <u>H</u> elp	⇔Back • ⇒ • 🔕 🖗 Address 🖉 http:	://127.0.0.1:3277/	-
CISCO SYSTEMS	Network Cor	figuration		×
վիսվիս	Ldet			
A I User				▝▔▎▙▖
Setup				1
Group Setup		Add AAA Clie	nt	4
Shared Profile Components	<u> </u>			C F
Network	AAA Client Host	name ASA1		
Configuration	AAA Client IP A	dress		Ē
Configuration		×	1	
Interface Configuration	Кеу	CISCO		
Administration Control	Authenticate U	ng RADIUS (Cisco VPN 3000/A	ASA/PIX 7.x+)	
External User Databases	🗖 🗖 Single Conr	ect TACACS+ AAA Client (Record stop i	n accounting on failure).	
paga Posture	📕 🗖 Log Update	Watchdog Packets from this AAA Client	ť,	
Network Access	Log RADIUS	Tunneling Packets from this AAA Client		
Profiles	🗖 🗖 Replace RA	IUS Port info with Username from this 4	AAA Client	
Reports and Activity				
Online Documentation		Submit Submit + Apply	Cancel	•111
I Applet encryptor starl	ted		Internet	

Configure ACS Interface to enable some of VPN3k/ASA RADIUS attribute	<i>Configure I</i>	ACS Interface	to	enable	some	of	VPN3k/ASA	RADIUS	attributes
--	--------------------	---------------	----	--------	------	----	-----------	--------	------------

🖉 Cis	scoSec	ure AC	5 - Microso	oft Inter	net Exp	orer				_ 🗆 ×
Eile	Edit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	(== Back 🔹 => 🔹 😰	A <u>d</u> dress	🕙 http://127.0.0.1:3277)	-
C	ISCO S	YSTEMS	In	terfa	e C	onfiguration				×
	սՈրու	ա		Cina		Jinguration				
			Edit							1007
	User Setu	Р								
	Grou Setu	ip P			R	ADIUS (Cisco VPN	1 300	0/ASA/PIX 7	/.x+)	
(Rea	Share	ed Profile	1			•		5 (65)	1	
803	Comp	onents								
3	Conf	ork iguration		G	roup					
	Syste Conf	em iguratior	,	Г	[02	5/3076/001] Access-Hours				
	Inter	face		Γ	[02	5/3076/002] Simultaneous-	Logins			
	P Conf	iguratio		F	[02	5/3076/005] Primary-DNS				
-	Adm Cont	inistratio rol	'n	Г	[02	5/3076/006] Secondary-DN	IS			
-0	L Exte	rnalliser	7	Г	[02	5/3076/007] Primary-WINS				
봐	Data	bases		E	[02	5/3076/008] Secondary-WI	INS			
000	Post Valio	ure Lation		E	[02	5/3076/009] SEP-Card-Assi	ignment			
				F	· [02	5/3076/011] Tunneling-Prot	tocols			
	Profil	es es	55	Г	[02	5/3076/012] IPSec-Sec-As	sociatio	n		
	Repo	ortsand	1	F	· [02	5/3076/013] IPSec-Authen	tication			
	Activ	vity		Г	[02	5/3076/015] IPSec-Banner:	1	32		-
	Docu	ne mentatio				Subr	nit C	ancel		ŀ
🥭 🖌	oplet sta	artStop s	started						👔 👔 Internet	





Create ne	ew grou	o named	"EZVPN":
-----------	---------	---------	----------

🗧 CiscoSecu	re ACS	- Microso	ft Inter	net Exp	olorer							_	. 🗆 ×
<u>File Edit</u>	<u>∕</u> iew	F <u>a</u> vorites	<u>T</u> ools	Help	🗘 Bac	< → ⇒ →	8	Address	🖉 http://	127.0.0.1:3190	1	•	-
Cisco Svs	TEMS	G	roup	Setu	q								×
االس	dlu	Î			Jun	p To AC	cess Res	strictions	;		-		
User Setup]			~	Acc IP /	cess Res Address	trictions Assignm	ent				_
Group Group]			G		DIUS (Ci DIUS (IE	sco VPN TF)	3000/AS	A/PIX 7.x+)			
Shared Compor	Profile ients						_						
Networ Config	k uration					A	ccess	Rest	riction	S			
System Config	uration						Grour) Disable	ed			2	
Config	ace uration		🗌 Mer	nbers (of this gr	oup will b	e denie	d access	to the n	etwork.			
Contro	stration)efault T	ime-of-	Day Acc	cess Set	tings		?	
Del Databa	ses					00;00	0 06:00	12:00	18:00	24:00			
Valida	tion					Mon Tue							
Profiles	Acces					Wed Thu							
Activi	ts and ty					Fri					1		<u> </u>
Docum Docum	entation					Submit	Su	bmit + R	estart	Cancel			
Applet dialu	p_filter	started									🔹 🚺 🕜 Inter	net	

CiscoSecure ACS - Mi	icrosoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vor	orites Tools Help 🗘 🖙 Back 🔹 🤿 🖉 👔 🛛 Address 🙋 http://127.0.0.1:3277/	-
CISCO SYSTEMS	Group Setup	×
tilliutilliu	Jump To RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) 💌	
User Setup	Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes	<u></u> ?
Setup Shared Profile Components	[3076\005] Primary-DNS [3076\005]	
Network Configuration	[10.0.0.1] [10.0.0.1]	
System Configuration	IPSec ☑ [3076\013] IPSec-Authentication	
Administration Control	Internal ☐ [3076\027] IPSec-Split-Tunnel-List	
Call External User Databases	SPLIT_TUNNEL	
Validation	Only tunnel networks in the list	
Profiles		
Online Documentation	Submit Submit + Restart Cancel	<u> </u>
Applet dialup_filter start	ted	Internet

Create user EZVPN with password, matching the common RADIUS authorization password on the ASA ("CISCO"):

🖉 CiscoSecure ACS - M	icrosoft Internet Explorer	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	orites Iools Help 🗘 Back + => + 🔕 😰 Address 🛃 http://127.0.0.1:3190/	
CISCO SYSTEMS	User Setup	×
	Edit	
User Setup	User: EZVPN (New User)	
Shared Profile Components	Account Disabled	
Network Configuration	Supplementary User Info	2
System Configuration	Real Name Description	
Administration Control		
Databases	User Setup	2
Validation Validation	Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate	
Reports and Activity	Password *****	-
Documentation	Submit Cancel	-
Applet dialup_filter star	ted 🛛 🔰 🚺 💓 Internet	1

Assign this user to group EZVPN:

CiscoSecure AC	5 - Microsof	t Internet	Explorer					_ 🗆 >
<u>File E</u> dit <u>V</u> iew	F <u>a</u> vorites	<u>T</u> ools <u>H</u> el	p 🗘 Ba	ick 🔹 🖘 👻 🛃	Address 🖉 H	http://127.0.0.1:3190/		-
CISCO SYSTEMS	Us	er Seti	up					×
User Setup Setur S		Co Co Whe CHAR espe	Geparate (Pass nfirm Pass n a token password cially usef Use grou	CHAP/MS-CHAP/. word server is used fo d for a token car ful when token car Group to wh Default Group Default Group Ezypn Group 2 Group 3 Group 4	ARAP)	on, supplying a separ CHAP authentication ed. assigned:	rate . This is	
External User Databases Posture Validation Validation Profiles Reports and Activity		0 0 0 0 	No callba Callback Dialup cli Use Winc	Group 5 Group 6 Group 7 Group 8 Group 9 Group 10 Client IP	Address Assign	nment		
Doline Documentation		ž		S	ubmit Cance	el		<u> </u>
) Applet dialup_filte	r started						o Internet	

Verification

Enable debugging on the ASA, and connect Cisco VPN Client to the ASA: (use group password "CISCO" and "CISCO/CISCO1234" for Xauth): ASA1(config)# debug radius ASA1(config)# debug aaa authentication debug aaa authentication enabled at level 1 ASA1(config)# debug aaa authorization debug aaa authorization enabled at level 1 radius mkreq: 0xe alloc_rip 0x41ed900 new request 0xe --> 3 (0x41ed900) got user '' got password add_req 0x41ed900 session 0xe id 3 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request)

Copyright © 2007 Internetwork Expert

```
_____
Raw packet data (length = 155)....
                                                 | ....>...J..1...
m.3...EZVPN...h.
01 03 00 9b f9 3e 9f ec b5 4a bb d8 31 16 97 84
6d a2 33 f0 01 07 45 5a 56 50 4e 02 12 18 68 ef
c0 3b 69 3b a5 75 28 66 7a f4 d5 a0 e5 05 06 00
                                                 | .;i;.u(fz.....
00 00 09 06 06 00 00 00 02 07 06 00 00 00 01 1e
                                                 .136.1.123.12..1
36.1.100.200=...
0e 31 33 36 2e 31 2e 31 32 33 2e 31 32 1f 0f 31
33 36 2e 31 2e 31 30 30 2e 32 30 30 3d 06 00 00
00 05 42 0f 31 33 36 2e 31 2e 31 30 30 2e 32 30
                                                   ..B.136.1.100.20
                                                 | 0....{...i
30 04 06 88 01 7b 0c 1a 24 00 00 00 09 01 1e 69
                                                 p:source-ip=136.
1.100.200..
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 33 36 2e
31 2e 31 30 30 2e 32 30 30 d9 1e
Parsed packet data....
Radius: Code = 1 (0x01)
Radius: Identifier = 3 (0x03)
Radius: Length = 155 (0x009B)
Radius: Vector: F93E9FECB54ABBD8311697846DA233F0
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) =
45 5a 56 50 4e
                                               EZVPN
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
18 68 ef c0 3b 69 3b a5 75 28 66 7a f4 d5 a0 e5 | .h..;i;.u(fz....
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x9
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 14 (0x0E)
Radius: Value (String) =
Radius: Length = 15 (0-07)
Radius: Length = 15 (0x0F)
Radius: Value (String) =
31 33 36 2e 31 2e 31 30 30 2e 32 30 30
                                          136.1.100.200
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 15 (0x0F)
Radius: Value (String) =
31 33 36 2e 31 2e 31 30 30 2e 32 30 30 | 136.1.100.200
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 136.1.123.12 (0x88017B0C)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 36 (0x24)
Radius: Vendor ID = 9 (0x0000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 30 (0x1E)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 33 36
                                                 ip:source-ip=136
2e 31 2e 31 30 30 2e 32 30 30 d9 1e
                                                 .1.100.200..
send pkt 10.0.0.100/1645
```

Copyright © 2007 Internetwork Expert

```
rip 0x41ed900 state 7 id 3
rad_vrfy() : response message verified
rip 0x41f02c8
 : chall_state ''
: state 0x7
: timer 0x0
 : reqauth:
    f9 3e 9f ec b5 4a bb d8 31 16 97 84 6d a2 33 f0
 : info 0xe
    session_id 0xe
    request_id 0x3
    user 'EZVPN'
     response '***'
     app 0
     reason 0
     skey 'CISCO'
     sip 10.0.0.100
     type 1
RADIUS packet decode (response)
Raw packet data (length = 118).....
02 03 00 76 2b 96 dd 0f 10 d9 50 76 a2 38 04 78
                                                    | ...v+....Pv.8.x
87 60 fc 89 1a 0c 00 00 0c 04 05 06 0a 00 00 64
                                                    | .`....d
1a Oc 00 00 Oc 04 0b 06 00 00 00 04 1a Oc 00 00
                                                       . . . . . . . . . . . . . . . .
0c 04 0d 06 00 00 00 05 1a 14 00 00 0c 04 1b 0e
                                                       . . . . . . . . . . . . . . . .
53 50 4c 49 54 5f 54 55 4e 4e 45 4c 1a 0c 00 00
                                                    ____IONNEL....
| ..7....
| CACS:0/57
                                                    | SPLIT_TUNNEL....
Oc 04 37 06 00 00 00 01 08 06 ff ff ff ff 19 18
43 41 43 53 3a 30 2f 35 31 65 61 2f 38 38 30 31
                                                      7b0c/9
37 62 30 63 2f 39
Parsed packet data....
Radius: Code = 2 (0x02)
Radius: Identifier = 3 (0x03)
Radius: Length = 118 (0x0076)
Radius: Vector: 2B96DD0F10D95076A23804788760FC89
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 5 (0x05) Primary-DNS
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.0.0.100 (0x0A000064)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 11 (0x0B) Tunnelling-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 4 (0x0004)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 13 (0x0D) IPSec-Authentication
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 5 (0x0005)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 20 (0x14)
Radius: Vendor ID = 3076 (0x0000C04)
Radius: Type = 27 (0x1B) Split-Tunnel-Inclusion-List
Radius: Length = 14 (0x0E)
Radius: Value (String) =
53 50 4c 49 54 5f 54 55 4e 4e 45 4c
                                                   SPLIT_TUNNEL
Radius: Type = 26 (0x1A) Vendor-Specific
```

```
Copyright © 2007 Internetwork Expert
```





👌 VPN Client \mid Statistics × Route Details Firewall Tunnel Details Local LAN Routes Secured Routes Subnet Mask Network Network Subnet Mask 136.1.121.0 255,255,255,0 Close ASA1(config) # show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 IKE Peer: 136.1.100.200 1 Role : responder Type : user Rekey : no State : AM_ACTIVE R1#ping 20.0.0.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/24 ms R1# ASA1(config)# show crypto ipsec sa interface: outside Crypto map tag: DYNAMIC, seg num: 10, local addr: 136.1.123.12 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0) current_peer: 136.1.100.200, username: CISCO dynamic allocated peer ip: 20.0.0.1 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5 #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.: 136.1.123.12, remote crypto endpt.: 136.1.100.200

Copyright © 2007 Internetwork Expert

path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: E7392AD9 inbound esp sas: spi: 0xD7D854C0 (3621278912) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 9, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 27808 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xE7392AD9 (3879283417) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 9, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 27808 IV size: 8 bytes replay detection support: Y

Further Reading

Migrating to ASA 7.2 for VPN 3000 Concentrator Administrators

PIX/ASA and Cisco VPN Client with RADIUS

Objective: Configure the to authenticate remote user and download group policy from RADIUS server. Additionally, specify a group ACL on RADIUS server to be applied to user's session.



Directions

- Configure devices as per the scenario "VPN/Easy VPN" <u>"The PIX/ASA and Cisco VPN Client with External Policy"</u>
- We want to force group "EZVPN" member to be authenticated against the RADIUS server, not the local database.
- To make that possible, configure group EZVPN" general-attributes to use RADIUS server group for authentication.
- Note that user's authentication is performed before the external policy is retreived from RADIUS server. This allows you to specify different policy name in user's profile.
- Create user "CISCO" with password "CISCO1234" on ACS. This entry will be used to authenticate remote client via Xauth.
- Additionally, we want all group members to have simple ACL applied. The ACL should permit only ICMP traffic to group members.
- Configure group EZVPN on ACS server, and add Cisco AV-Pair:
 - "ip:inacl#1="permit icmp any any"

Final Configuration

ASA1:

```
tunnel-group EZVPN general-attributes authentication-server-group RADIUS
```

ACS:

Create user "CISCO" with password "CISCO1234":

🖉 CiscoSe	ecure AC	5 - Microso	oft Inter	net Explo	rer									_ 🗆 ×]
<u>Eile E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	<u>H</u> elp	🗢 Back	•=	- 🗵 🔮	Ad	dress 🥻	🖞 http://127	7.0.0.1:2318	3/		•	
Cisco	SYSTEMS	U	ser S	etup										×	Ī
			5.7.5 (T)												
		Edi	t]
Us Se	er tup						He	or	CISC	-0					
	oup tup	1					03	CI.	010						
an, Sha	red Profile						□ A	ccour	nt Disa	abled					
Cor	nponents													_	
Cor	work figuratio	'n				S	upplem	entar	y Usei	r Info			?		
Sus Cor	stem nfiguratio		Real N	lame		Γ									
	erface		Descri	ption		E									
Con	nfiguratio					000									
Ad Cor	ministratio ntrol	n.											_		
	ternal Use tabases	-					U	er Se	tup				?		
DODD PO	sture lidation		P	assword	d Auther	nticati	on:			85-					
	work Acce	-								ACS In	ternal Da	atabase	•		
Pro	files			Cisco	Secure	PAP (Also used	l for C	HAP/N	/IS-CHAP/	ARAP, if	the Sep	arate ked.)		
Re Ac	ports and tivity				Passw	ord			****	*****					
	line						Submit	De		Cancel	r		_	<u> </u>	.1
	sumentatio					_	Submit		siete	Cancer				ľ	-
🥙 Applet r	has_filter :	started											Internet	1	11

Add group attribute "Cisco AV-Pair" to specify downloadble ACL:

CiscoSecure ACS - M	licrosoft Inter	net Expl	orer		_ 0
<u>File E</u> dit ⊻jew F <u>a</u> v	orites <u>T</u> ools	Help	🖙 Back 🔹 🖘 👻 🛃	Address Address Address Address	277]
CISCO SYSTEMS	Group	Setu	p		[
	10-10-00 E 10-000 ■ 200		Jumn To RADIUS (0	Cisco IOS/PIX 6.0)	-
User			Access Re	strictions	
			GroiRADIUS (isco IOS/PIX 6.0)	
Setup			RADIUS (C	isco VPN 3000/ASA/PIX 7.x FTF)	+)
Shared Profile Components					
Network			-		
			Acces	s Restrictions	
Configuration			Cro	m Dicabled	9
Interface Configuration	5-04		Grut	ip Disableu	<u>.</u>
Administration	☐ Men	nbers o	f this group will be denie	ed access to the network.	
Control			Default Time-of	-Day Access Settings	?
Databases	2		00;00 06;0	0 12;00 18;00 24;00	
Posture Validation			Mon		
Natwork Becass			Tue		
Profiles			Wed		
Reports and			Thu		
Mativity			Fri		•
0nline Documentation			Submit S	ubmit + Restart Cance	2
and I see all straight	3				
Applet dialup_filter sta	rted				S Internet

CiscoSecure ACS - Mic	osoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vori	es Iools Help 🗘 🖙 Back 🔹 🖘 🗸 🔇 🖓 🛛 Address 🖉 H	http://127.0.0.1:3277/
CISCO SYSTEMS	Group Setup	X
	Jump To RADIUS (Cisco IOS/PIX	6.0)
User Setup	Cisco IOS/PIX 6.x RADIUS A	ttributes
Shared Profile Components	[009\001] cisco-av-pair ip:inacl#1=permit icmp ic	any any
Network Configuration		
Configuration	 □ [009\101] cisco-h323-credit-amount	
Administration Control	□ [009\102] cisco-h323-credit-time	
Databases	☐ [009\103] cisco-h323-return-code	
Network Access Profiles	□ [009\104] cisco-h323-prompt-id	
Reports and Activity	[009\105] cisco-h323-day-and-time	
Documentation	Submit Submit + Restar	rt Cancel
Applet dialup_filter starte		Internet

Verification

Connect Cisco VPN Client, and check "Passed Authentication" on ACS:

🥙 Cis	scoSec	ure AC	5 - Mic	rosoft Inter	net Explorer							_ 0	×
Eile	Edit	⊻iew	Favor	rites <u>T</u> ools	Help 🗘 E	iack $\star \Rightarrow$	8	Address	s 🙋 http://127.0.0	1:3277/		-	Ē
C	ISCO SI	ISTEMS	. A	Report	s and Ac	tivity							×
	User Setu Grou Setu	p p p		Passed . Regular	Authenticat Expression	ions active	e.csv	Refre	esh 🗗 <u>Downlo</u> Start Date & T mm/dd/yyyy,h	i <u>ad</u> ime ih:mm	End :ss mm/	Date & Tir ′dd/yyyy,ł	me h:r
	Share Compo Netwo Confi Syste	d Profile onents ork guratior m		Apply Filtering	Filter (is not applie Time	Clear Filter d. <u>Message-</u>	User-	Group-	Caller-ID	NAS-	NAS-IP-	Network Access	<u>Sh</u>
	Inter Confi	face iguratio		01/20/20	107 04:08:03	Iype Authen OK	EZVPN	EZVPN	136.1.100.200	12	136.1.123.12	Name (Default)	
-72	Admi Contr	nistratio ^{rol}	'n	01/20/20	107 04:08:03	Authen OK	CISCO	Default Group	136.1.100.200	12	136.1.123.12	(Default)	
R	Exter Datab	rnal User bases		01/20/20	107 04:04:36 107 03:38:36	Authen OK Authen OK	EZVPN EZVPN	EZVPN EZVPN	136.1.100.200 136.1.100.200	11 10	136.1.123.12 136.1.123.12	(Default) (Default)	
	Postu Valid	ure lation		01/20/20	107 03:07:45	Authen OK	EZVPN	EZVPN	136.1.100.200	9	136.1.123.12	(Default)	
	Netwo Profile Repo Activ	ork Acce es orts and /ity ie mentation	SS N										
Ar	nlet sta	rtStop s	started								M Internet		
Can we		a cocop s									ancornoc		111

Note that user was authenticated first, before the policy retreival.

Check access-list at the ASA:

R1#ping 20.0.0.1

Copyright © 2007 Internetwork Expert

```
R1#telnet 20.0.0.1 139
Trying 20.0.0.1, 139 ...
% Connection refused by remote host
ASA1(config) # show crypto ipsec sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0)
      current_peer: 136.1.100.200, username: CISCO
      dynamic allocated peer ip: 20.0.0.1
      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#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.: 136.1.123.12, remote crypto endpt.: 136.1.100.200
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: ACE45F0C
    inbound esp sas:
      spi: 0xDDC0489C (3720366236)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 12, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28278
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xACE45F0C (2900647692)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 12, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (sec): 28278
         IV size: 8 bytes
         replay detection support: Y
```

Further Reading

<u>Cisco VPN Client User and Group Attribute Processing on the VPN 3000</u> <u>Concentrator</u>

PIX/ASA and Cisco VPN Client with Digital Certificates

Objective: Configure the ASA to authenticate remote VPN Client connections using digital certificates.



Directions

- Configure devices as per the scenario "VPN/Easy VPN" <u>"The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI"</u>.
- Start by configuring VPN Client as follows:
 - First, enroll VPN client with CA via SCEP.
 - Use enrollment URL
 <u>http://10.0.0.100/certsrv/mscep/mscep.dll</u>
 - Specify "OU=EZVPN" to be used for group matching on the ASA.
 - Next, use Internet Explorer to retreive and install CA Root Certificate into Windows trusted certificates store.
 - After that, download CA certificate and import it into VPN client Store.
 - Modify VPN connection setting and choose authentication based on certificates.
- Enroll the ASA with CA:
 - Configure NTP server to 10.0.0.100.
 - Configure CA trustpoint IE1:
 - Use enrollment URL: <u>http://10.0.0.100/certsrv/mscep/mscep.dll</u>

- Set revocation-check to none.
- o Authenticate the CA trustpoint.
- Configure domain-name and create RSA key-pair.
- Enroll with CA finally.
- Change ISAKMP policy entry 10 on the ASA
 - Specify RSA-Sig authentication.
- Change tunnel-group EZVPN ipsec-attributes settings on the ASA:
 Use trustpoint IE1

Final Configuration

ASA1:

```
1
! Sync time, set domain-name, generate key
!
ntp server 10.0.0.100
domain-name internetworkexpert.com
crypto key generate rsa general-keys modulus 512
!
! Trustpoint config
1
crypto ca trustpoint IE1
enrollment url http://10.0.0.100:80/certsrv/mscep/mscep.dll
crl configure
!
! Authenticate and enroll
1
crypto ca authenticate IE1
crypto ca enroll IE1
!
! Change ISAKMP policy to use RSA-Sig Auth
!
crypto isakmp policy 10
authentication rsa-sig
!
! Configure IE1 as trustpoint for group EZVPN
!
tunnel-group EZVPN ipsec-attr
  trust-point IE1
```

Test PC/VPN Client:

```
Choose Certificates/Enroll:
```

🖲 <u>O</u> nline	
Certificate Authority:	<new></new>
CA <u>U</u> RL*:	http://10.0.0.100/certsrv/mscep/mscep.dll
CA <u>D</u> omain:	IE1
Challenge P <u>a</u> ssword:	NHXHN
C Eile	
File encoding:	Binary 💌
File <u>n</u> ame*:	
New Password:	

👌 VPN Client	Certificate I	Inrollment			×
Enter certificate fi	ields, ''*'' deno	tes a required fiel	±:		
<u>N</u> ame [CN]*:	CISCO				
Department [OU]:	EZVPN				
Company [0]:					
<u>S</u> tate [ST]:	<u></u>				
Country (C):	<u></u>				
E <u>m</u> ail (E):	[
IP Address:					
Dom <u>a</u> in:					
		<u>B</u> ack		<u>E</u> nroll	Cancel

Review your certificate:

Common Name	- CISCO
Denartment	FZVPN
Comnany	
State	
Country	
Email	
MD5 Thumbprint	13A36EFFDF8B5564E7F8BE1FE1C7C6B9
SHA1 Thumbprint	01E98B6EAD466BDE24750290272F06A5FD0A7B0F
Key Size	2048
Subject	cn=CISCO,ou=EZVPN
ssuer	cn=IESERVER1,o=Internetwork Expert,I=Reno,st=NV,c=US,e=bmcgahan@internetworkexpert.com
Serial Number	431B460800010000002E
Not valid before	Thu Jan 18 06:10:15 2007
Not valid after	Fri Jan 18 06:20:15 2008

Retreive CA certificate and install it into trusted store:

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	_ 🗆 ×
j Eile Edit View Favorites Iools Help ⇔Back → ↔ 🛇 🕼 Address 🙆 http://10.0.0.100/certsrv/	-
Microsoft Certificate Services IESERVER1	ome
Welcome	
Welcome	_
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon type of certificate you request.	ı the
Select a task:	
Retrieve the CA certificate or certificate revocation list	
C Request a certificate	
C Check on a pending certificate	
Next>	Γ
	-
🙋 Done	

Choose "Install this CA certification path":



Root Cer	tificate Store 🔀
A	Do you want to ADD the following certificate to the Root Store?
	Subject : IESERVER1, Internetwork Expert, Reno, NV, US, bmcgahan@internetworkexpert.com Issuer : Self Issued Time Validity : Friday, July 21, 2006 through Monday, July 21, 2008 Serial Number : 6A8B964C 37F91BB2 45B01DE2 A6363745 Thumbprint (sha1) : 4BFF916B 2D7A58C4 9DB6A69C E39C770D 94A8EAB7 Thumbprint (md5) : 74F95E93 4F8C8AF3 5FD15364 8EFBB479 <u>Y</u> es <u>No</u>

Microsoft Certificate Services - Microsoft Internet Explorer	
j Eile Edit View Favorites Iools Help ⇔Back + ↔ + 🚳 🔂 🛛 Address 🖉 10.0	D.O.100/certsrv/certrmpn.asp 🗾 🏾 🌆
	*
Microsoft Certificate Services IESERVER1	<u>Home</u>
CA Certificate Installed	
The CA certificate has been successfully installed.	
	<u>_</u>
e Done	I I I I I I I I I I I I I I I I I I I

Download CA certificate for installation into Cisco VPN client store:

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
j Eile Edit View Favorites Iools Help ⇔ Back - ↔ - 🕲 😰 Address 🖉 http://10.	.0.0.100/certsrv/
<i>Microsoft</i> Certificate Services IESERVER1	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or program. Once you acquire a certificate, you will be able to securely identify yourse over the web, sign your e-mail messages, encrypt your e-mail messages, and more type of certificate you request. Select a task: Retrieve the CA certificate or certificate revocation list C Request a certificate C Check on a pending certificate	∙other secure ୬lf to other people e depending upon the
	Next >
	v
Done	📄 🔮 Internet 🌱

Choose "Download CA Certificate":

Microsoft Certificate Services - Microsoft Internet Explorer _ 🗆 × File Edit View Favorites Tools Help 🖙 Back 🔹 🖘 💌 🚱 Address 🙋 /10.0.0.100/certsrv/certcarc.asp 🔻 1 Microsoft Certificate Services -- IESERVER1 Home **Retrieve The CA Certificate Or Certificate Revocation List** Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [IESERVER1(1)] Previous [IESERVER1] ● DER encoded or ● Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list 🌍 Internet 🥭 Done Save As ? X

Save jn:	My Documen	its 💆] ← E d	*
History	My Pictures			
Desktop	Ecertnew.cer EIDSUSER-CRT.	.cer		
My Documents				
My Computer				
Do Not Chang	File <u>n</u> ame:	certnew.cer		<u>S</u> ave
	Save as type:	Security Certificate	-	Cancel

👌 YPN Client Im	port Certificate	×
Import from <u>File</u>		
Import <u>P</u> ath:	d Settings\IEAdmin\My Documents\certnew.cer	Browse
Import P <u>a</u> ssword: [
C Import from <u>M</u> icro Import C <u>e</u> rtificate:	soft Certificate store	¥
Entering a new pas identity certificates.	sword may be required. It is recommended to pass	word protect
<u>N</u> ew Password:		
Confirm Password:		
		Cancel

Next choose "Import" in Certificate Menu of Cisco VPN Client:

You should have identity ceritificate and CA certificate into Cisco VPN Client Store:

👌 status: Connect	ed VPN Clien	t - Version 4.8.0	1.0300			
<u>⊂</u> onnection Entries	<u>5</u> tatus C <u>e</u> rtifica	ates Log Options	: <u>H</u> elp			
			4	X		CISCO SYSTEMS
View Imp	ort Expor	t Enroll	Verify	Delete		
Connection Entries	Certificates	Log				
Number	Certificate		Store	6	Key Size	Validity
0	IESERVER1 CISCO		CA Cisco		1024 2048	until Jul 21, 2008 until Jan 18, 2008
Connected to "EZVPN	ľ ⁿ .			Conn	ected Time: 0 day	/(s), 00:06.16 💌 //

Modify connection Settings to use Certificates for authentication:

Copyright © 2007 Internetwork Expert

Connection Entry: EZVPN		
Host: 136.1.113.11		K
Authentication Transport Backup S	ervers Dial-Up	
C Group Authentication	C Mutual Group	Authentication
Name: EZVPN		
Password:		
Confirm Password:		
Certificate Authentication		
Name: 3 - CISCO (Cisco)	•	
🦵 Send CA Certificate Chain		
	C	Consul

Verification

<pre>ASAl(config)# crypto ca enroll IE1 % % Start certificate enrollment % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: cisco Re-enter password: cisco</pre>
% The fully-qualified domain name in the certificate will be: ASA1.internetworkexpert.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority ASA1(config)# The certificate has been granted by CA!
VPN Client:
Change connection settings to use Digital Certificate:

```
4 VPN Client | Properties for "EZVPN"
                                                                       ×
           Connection Entry: EZVPN
               Description:
                    Host: 136.1.123.12
            Authentication Transport Backup Servers Dial-Up
            C Group Authentication
                                                Mutual Group Authentication
              Name:
                           EZVPN
              Confirm Password: *

    Certificate Authentication

              Name: 1 - CISCO (Cisco)
                                             -
              Send CA Certificate Chain
                                                                Cancel
                                                     Save
Enable debugging at the ASA and connect VPN Client:
ASA1(config)# debug crypto isakmp 9
ASA1(config)#
Jan 20 13:45:40 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 1144
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing SA payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Oakley proposal is
acceptable
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received xauth V6 VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received DPD VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Fragmentation VID
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, IKE Peer included IKE
fragmentation capability flags: Main Mode:
                                                     True Aggressive Mode:
False
With certificates connection occurs in IKE Main Mode
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received NAT-Traversal ver
02 VTD
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Cisco Unity client
VTD
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, processing IKE SA payload
Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, IKE SA Proposal # 1,
Transform # 22 acceptable Matches global IKE entry # 1
```

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 355 -

ISAKMP Policy match found

Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing ISAKMP SA pavload Jan 20 13:45:40 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing Fragmentation VID + extended capabilities payload Jan 20 13:45:40 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 108 Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 224 Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ke payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ISA_KE payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing nonce payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Processing IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing VID payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Received Cisco Unity client VID Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing ke payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing nonce payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing certreq payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing Cisco Unity VID pavload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing xauth V6 VID payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Send IOS VID Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, constructing VID payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Send Altiga/Cisco VPN3000/Cisco ASA GW VID Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Generating keys for Responder.. Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 403 Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Rcv'd fragment from a new fragmentation set. Deleting any old fragments. Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Successfully assembled an encrypted pkt from rcv'd fragments! Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + CERT_REQ (7) + SIG (9) + NOTIFY (11) + NONE (0) total length : 1714 Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing ID payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing cert payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing cert request payload Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing RSA signature Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, Computing hash for ISAKMP Jan 20 13:45:41 [IKEv1 DEBUG]: IP = 136.1.100.200, processing notify payload Group name is taken from the OU field in the certificate: Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, Trying to find group via OU... Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, Connection landed on tunnel_group EZVPN Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, peer ID type 9 received (DER_ASN1_DN) Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing

Copyright © 2007 Internetwork Expert
ID payload Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing cert payload Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing RSA signature Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, Computing hash for ISAKMP Jan 20 13:45:41 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing dpd vid payload Jan 20 13:45:41 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0) total length : 1244 Jan 20 13:45:42 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing blank hash pavload Jan 20 13:45:42 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, constructing qm hash payload Jan 20 13:45:42 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=ed5985ad) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68 Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=ed5985ad) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 82 Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, process_attr(): Enter! Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, IP = 136.1.100.200, Processing MODE_CFG Reply attributes. Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: primary DNS = 10.0.0.100 Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: secondary DNS = cleared Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: primary WINS = cleared Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: secondary WINS = cleared Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, TP = 136.1.100.200, IKEGetUserAttributes: split tunneling list = SPLIT_TUNNEL Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: IP Compression = disabled Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: Split Tunneling Policy = Split Network Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKEGetUserAttributes: Browser Proxy Setting = no-modify Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP : 136.1.100.200, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Jan 20 13:45:47 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, User (CISCO) authenticated. Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, constructing blank hash payload Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, constructing qm hash payload Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=e2adfc00) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Jan 20 13:45:47 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=e2adfc00) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, process_attr(): Enter! Jan 20 13:45:47 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Processing cfg ACK attributes Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=f10a41b4) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 188

Copyright © 2007 Internetwork Expert

```
- 357 -
```

Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, process_attr(): Enter! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Processing cfg Request attributes Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for IPV4 address! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for IPV4 net mask! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for DNS server address! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for WINS server address! Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Received unsupported transaction mode attribute: 5 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Banner! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Save PW setting! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Default Domain Name! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Split Tunnel List! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Split DNS! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for PFS setting! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Client Browser Proxy Setting! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for backup ip-sec peer list! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for Application Version! Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Client Type: WinNT Client Application Version: 4.8.01.0300 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for FWTYPE! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for DHCP hostname for DDNS is: ieserver3! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, MODE_CFG: Received request for UDP Port! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Obtained IP addr (20.0.0.1) prior to initiating Mode Cfg (XAuth enabled) Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Assigned private IP address 20.0.0.1 to remote user Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, constructing blank hash payload Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Send Client Browser Proxy Attributes! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Browser Proxy set to No-Modify. Browser Proxy data will NOT be included in the mode-cfg reply Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, constructing qm hash payload Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=f10a41b4) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 184 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,

Copyright © 2007 Internetwork Expert

```
PHASE 1 COMPLETED
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, Keep-alive type for this
connection: DPD
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Starting P1 rekey timer: 82080 seconds.
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, sending notify message
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing qm hash payload
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message
(msgid=926c5df3) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total
length : 88
Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message
(msgid=be168033) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
+ ID (5) + NONE (0) total length : 1022
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing SA payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing nonce payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing ID payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Received remote Proxy Host data in ID Payload: Address 20.0.0.1, Protocol 0,
Port 0
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing ID payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask
0.0.0.0, Protocol 0, Port 0
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
QM IsRekeyed old sa not found by addr
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
IKE Remote Peer configured for crypto map: DYNAMIC
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, processing IPSec SA payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IPSec SA Proposal # 11, Transform # 1 acceptable Matches global
IPSec SA entry # 10
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
IKE: requesting SPI!
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, IKE got SPI from key engine: SPI = 0xd9191a19
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, oakley constucting quick mode
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing blank hash payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing IPSec SA payload
Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200,
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing IPSec nonce payload
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, constructing proxy ID
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
136.1.100.200, Transmitting Proxy Id:
  Remote host: 20.0.0.1 Protocol 0 Port 0
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0
Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP =
```

```
Copyright © 2007 Internetwork Expert
```

136.1.100.200, Sending RESPONDER LIFETIME notification to Initiator Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, constructing qm hash payload Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE SENDING Message (msgid=be168033) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176 Jan 20 13:45:48 [IKEv1]: IP = 136.1.100.200, IKE_DECODE RECEIVED Message (msgid=be168033) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, processing hash payload Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, loading all IPSEC SAs Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Generating Quick Mode Key! Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Generating Quick Mode Key! Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Security negotiation complete for User (CISCO) Responder, Inbound SPI = 0xd9191a19, Outbound SPI = 0x70ec9942Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, IKE got a KEY_ADD msg for SA: SPI = 0x70ec9942 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Pitcher: received KEY_UPDATE, spi 0xd9191a19 Jan 20 13:45:48 [IKEv1 DEBUG]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Starting P2 rekey timer: 27360 seconds. Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, Adding static route for client address: 20.0.0.1 Jan 20 13:45:48 [IKEv1]: Group = EZVPN, Username = CISCO, IP = 136.1.100.200, PHASE 2 COMPLETED (msgid=be168033) R1#ping 20.0.0.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/40 ms ASA1(config) # show crypto ipsec sa interface: outside Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0) current_peer: 136.1.100.200, username: CISCO dynamic allocated peer ip: 20.0.0.1 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5 #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.: 136.1.123.12, remote crypto endpt.: 136.1.100.200 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 70EC9942 inbound esp sas: spi: 0xD9191A19 (3642300953) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, }

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
slot: 0, conn_id: 14, crypto-map: DYNAMIC
sa timing: remaining key lifetime (sec): 28540
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x70EC9942 (1894553922)
transform: esp-3des esp-md5-hmac none
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 14, crypto-map: DYNAMIC
sa timing: remaining key lifetime (sec): 28540
IV size: 8 bytes
replay detection support: Y
```

Gamma Further Reading

Configuring the VPN Client 3.x to Get a Digital Certificate

The PIX/ASA and IOS ezVPN Remote NW Extension Mode

Objective: Configure the PIX/ASA to support IOS hardware clients in network extension mode.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"The PIX/ASA ezVPN"</u>.
- Configure ISAKMP:
 - Enable ISAKMP on the outside interface.
 - Configure ISAKMP policy with priority 10:
 - Use Pre-Shared authentication.
 - Use 3DES cipher.
 - Use MD5 hash.
 - Use DH group 2.
- With Network-Extension mode you do not need to configure any VPN addressing, since remote router does not need it.
- Create access-list SPLIT_TUNNEL:
 - Permit network 136.X.121.0/24.
- Add a local user for Xauth:
 - Create local user "CISCO" with password "CISCO1234".
- Define group-policy named EZVPN as internal:
 - Configure IPsec as the tunneling protocol.
 - Configure DNS server 10.0.0.100.
 - Specify split-tunneling policy "only tunnel networks in the list".
 - Assign split-tunnel network-list SPLIT_TUNNEL.

- Allow network-extension mode (NEM).
- Define tunnel group:
 - Create tunnel group "EZVPN" of type Remote-Access.
 - o Group General Attributes:
 - Set authentication-server group to "LOCAL" (it's the default value, inherited from default group).
 - Assign group-policy "EZVPN".
 - Group IPSec Attributes:
 - Specify pre-shared key "CISCO".
- Configure crypto:
 - Create transform-set 3DES_MD5:
 - Cipher 3DES.
 - Hash MD5.
 - Create dynamic crypto-map DYNAMIC entry 10:
 - Set transform-set 3DES_MD5
 - Set reverse-route
 - Create crypto-map VPN entry 10 to use dynamic crypto-map DYNAMIC.
 - o Attach crypto-map VPN to interface outside.
 - o Explicitly permit VPN traffic to pass through acess-lists.
- Redistribute static routes into RIP (this will redistribute RRI routes).

Final Configuration

```
ASA1:
1
! ISAKMP configuration
1
crypto isakmp enable outside
crypto isakmp policy 10
auth pre-share
 encr 3des
hash md5
group 2
!
! Split-tunneling ACL
!
access-list SPLIT_TUNNEL permit ip 136.1.121.0 255.255.255.0 any
1
! Local username for Xauth
1
username CISCO password CISCO1234
!
! Tunnel-group policy
!
group-policy EZVPN internal
group-policy EZVPN attributes
vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value SPLIT_TUNNEL
 dns-server value 10.0.0.100
 nem enable
I
! Tunnel-group definition
```

Copyright © 2007 Internetwork Expert

```
! Note that "authentication-server-group"
! is LOCAL by default
1
tunnel-group EZVPN type ipsec-ra
tunnel-group EZVPN general-attributes
 authentication-server-group LOCAL
  default-group-policy EZVPN
tunnel-group EZVPN ipsec-attributes
 pre-shared-key CISCO
1
! IPsec transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
! Dynamic crypto-map
crypto dynamic-map DYNAMIC 10 set transform-set 3DES_MD5
crypto dynamic-map DYNAMIC 10 set reverse-route
!
! Define crypto-map
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
! Attach crypto map to the interface
1
crypto map VPN interface outside
1
! Permit VPN traffic to bypass ACLs
!
sysop connection permit-vpn
1
! Redistribute static routes into RIP
1
router rip
redistribute static
R3:
crypto ipsec client ezvpn EZVPN
 connect manual
group EZVPN key CISCO
mode network-extension
peer 136.1.123.12
interface E0/0
crypto ipsec client ezvpn EZVPN
1
interface E0/1
 crypto ipsec client ezvpn EZVPN inside
```

Verification

Connect R3 to the ASA:

```
R3#crypto ipsec client ezvpn connect
R3#crypto ipsec client ezvpn
Jan 20 16:36:01.429: EZVPN(EZVPN): Pending XAuth Request, Please enter the
following command:
Jan 20 16:36:01.429: EZVPN: crypto ipsec client ezvpn xauth
```

Copyright © 2007 Internetwork Expert

```
- 364 -
```

```
R3#crypto ipsec client ezvpn xauth
Username: : CISCO
Password: : CISCO1234
R3#show crypto ipsec client ezvpn
Easy VPN Remote Phase: 2
Tunnel name : EZVPN
Inside interface list: Ethernet0/1,
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 10.0.0.100
Split Tunnel List: 1
       Address : 136.1.121.0
                : 255.255.255.0
: 0x0
       Mask
       Protocol
       Source Port: 0
       Dest Port : 0
Verify RRI:
ASA1(config) # 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
     136.1.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:20, outside
R
     136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:20, outside
R
S
     136.1.100.0 255.255.255.0 [1/0] via 136.1.123.3, outside
С
     136.1.121.0 255.255.255.0 is directly connected, inside
     136.1.123.0 255.255.255.0 is directly connected, outside
С
     10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:20, outside
R
R
     150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:09, inside
R1#ping 136.1.100.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 136.1.100.3, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
R3#show crypto ipsec sa
interface: Ethernet0/0
   Crypto map tag: Ethernet0/0-head-0, local addr. 136.1.123.3
   protected vrf:
   local ident (addr/mask/prot/port): (136.1.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (136.1.121.0/255.255.255.0/0/0)
   current_peer: 136.1.123.12:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
Copyright © 2007 Internetwork Expert
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
local crypto endpt.: 136.1.123.3, remote crypto endpt.: 136.1.123.12
path mtu 1500, media mtu 1500
current outbound spi: BA77E350
inbound esp sas:
 spi: 0x6FD779C7(1876392391)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2000, flow_id: 1, crypto map: Ethernet0/0-head-0
   sa timing: remaining key lifetime (k/sec): (4501355/28260)
   IV size: 8 bytes
   replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
 spi: 0xBA77E350(3128419152)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   slot: 0, conn id: 2001, flow_id: 2, crypto map: Ethernet0/0-head-0
   sa timing: remaining key lifetime (k/sec): (4501355/28260)
   IV size: 8 bytes
   replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

PIX/ASA 7.x Easy VPN with an ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example

WebVPN and SSL VPN

ASA and WebVPN Client

Objective: Configure the PIX/ASA to accept WebVPN connections and authenticate users internally.



Directions

- Configure devices as per the scenario "VPN/Common Configuration" <u>"PIX/ASA Easy VPN/WebVPN"</u>.
- We would like to set up basic WebVPN functionality, permitting WebVPN users from outside to access the inside servers.
- At the same time, we would like to permit selected outside users to access ASDM from the outside interace.
- Configure WebVPN globally:
 - Configure WebVPN to run on port 444 instead of default 443.
 - Enable WebVPN on the outside interface.
 - Permit user to choose among the WebVPN tunnel groups.
 - Create URL-List named "LIST":
 - Add entry "R1" with value <u>http://136.1.121.1</u>
 - Configure WebVPN Policy:
 - Create access-list "WEBACCESS" of type "webtype":
 - Permit http connections on ports 80 and 443.

- Create group-policy WEBVPN:
 - Specify WebVPN attributes:
 - Permit URL entry and WebFilter functions.
 - Apply WEBACCESS filter.
 - Specify URL List "LIST".
- Create local user "CISCO" with password "CISCO1234"
- Configure WebVPN tunnel-group named "WEBVPN":
 - General Attributes:
 - Specify LOCAL authentication.
 - Apply WEBVPN group-policy.
 - WebVPN Attributes:
 - Authenticate via AAA.
 - Specify group-alias "WEBVPN" so that users may choose group upon signon.
- Lock use "CISCO" in group "WEBVPN".
- Enable ASDM on the outside interface.
 - Permit HTTPS connections from any host

Final Configuration

```
ASA1:
webvpn
port 444
 enable outside
url-list LIST "R1" http://136.1.121.1
 tunnel-group-list enable
!
! Web-type access-list to permit only ports 80/443
1
access-list WEBACCESS webtype permit tcp any eq www
access-list WEBACCESS webtype permit tcp any eq https
!
! Group-policy to apply web-type access-list
!
group-policy WEBVPN internal
group-policy WEBVPN attributes
 webvpn
  functions url-entry filter
  filter value WEBACCESS
  url-list value LIST
1
! Local username to authenticate remote users
!
username CISCO password CISCO1234
!
! Lock this user into WEBVPN group only
!
username CISCO attributes
group-lock value WEBVPN
1
! Tunnel-group definition
1
tunnel-group WEBVPN type webvpn
tunnel-group WEBVPN general-attributes
 default-group-policy WEBVPN
```

- 368 -

```
.
tunnel-group WEBVPN webvpn-attributes
group-alias WEBVPN enable
authentication aaa
!
! Enable ASDM on the outside
!
asdm image disk0:/asdm-522.bin
http server enable
http 0 0 outside
```

Verification

Initiate connection to the ASA, default port 443:



1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	in the second		-	10000					
Edi	t <u>V</u> iew	Favorites	Tools	Help	C Back	. • ≓>	- × (×)	Address 🖉 https://136.1.123.12:444/+webvpn+/index.htr
ISCO	SYSTEMS	1							
որիր	սուլլ լլու	• WebV	/PN S	Servic	е				
					-				
			1				L	ogin	
				Please	enter y	our us	sernar	me an	id password.
				USE	RNAM	=. [Active and		
				DAG				_	
				PAS	SWORL				
					GROUP	*: WE	EBVPN	4	_
							_ogin		Clear

Connect to port 444 and login to WebVPN:

WebVPN	Service	e - Microso	ft Inter	net Exp	lorer							
ile <u>E</u> dit	⊻iew	Favorites	Tools	Help	(Back	< • ⇒	- 🗵 💆	Address 🥙 https	://136.1.123.12	:444/+wet	vpn+/index.ht	
Cisco S	YSTEMS											
ավիրու		WebV	'PN S	ervic	e							
			r			_	Login					
				Please	e enter y	our use	rname a	nd password.				
				USE		E: Cisc	:0					
				PAS	SWOR	D: 📖	lololok					
					GROUP	> : WEB	BVPN	-				
						L	ogin	Clear	1			
Done											Internet	

VebVPN	Servic	e - Microsol	ft Inter	net Exp	lorer				_				_ [
Edit	⊻iew	Favorites	Tools	Help	(= Back	· • ⇒ • (•	9 2	A <u>d</u> dress 🧔] https://136	5.1.123.12:	144/+webvp	n+/portal.h	it 🗾 🔡
usco S	YSTEMS												
alla	III.			-									
		WebV	PN S	ervie	e						20.004		
											[2 🖌 🙆	
WEB	APPL		vs		Web Bo	ookmarks							
Enter V	Veb Ad	Idress (URI	L)		<u>R1</u>								
				Go									
Web B	lookma	rks	-										
			_										
one											🔒 🥥 1	internet	

Click the bookmark URL "R1":



Further Reading

ASA with WebVPN and Single Sign-on using ASDM and NTLMv1 Configuration Example

ASA and WebVPN Port Forwarding

Objective: Configure the PIX/ASA to accept WebVPN connections and forward local connections on specific port to the remote host.



Directions

- Configure devices as per the scenario "VPN/WebVPN and SSL VPN" <u>"ASA and WebVPN Clients"</u>.
- As the added function, we will permit users to use application port forwarding.
- The way it works is that user's browser dowloads Java applet, which listens on specified port, and forward connections to remote host via SSL connection.
- Change group-policy WEBVPN:
 - Permit port-forward.
 - Enable applet auto-download.
- Change webtype access-list WEBACCESS:
 - Permit access via telnet.
- Configure WebVPN forward rule named TELNET_R3:
 o Forward port 20023 to host R1 port 23.
- Assign this rule to group-policy WEBVPN.

Final Configuration

Copyright © 2007 Internetwork Expert

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
ASA1:
group-policy WEBVPN attributes
webvpn
 functions url-entry port-forward filter auto-download
 port-forward value TELNET_R3
 port-forward-name value Port Forwarding
 exit
exit
!
! Permit telnet access in WebACL
!
access-list WEBACCESS webtype permit tcp any eq 23
!
! Port-forwarding config is global
!
webvpn
 port-forward TELNET_R3 20023 136.1.121.1 telnet
```

Verification

Connect to port 444 and login to WebVPN services:

WebVPN	Servic	e - Microso	ft Inter	net Expl	orer							
e <u>E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	<u>H</u> elp	🗘 Back	•⇒ • (8	Address 🛃 https	://136.1.123	.12:444/+	webvpn+/index	.htr 💌 📲
C	******											
uli.	TSTEMS											
nillillin.	ailiilina.	WebV	'PN S	ervic	e							
				-	-		ogin	_				
				Please	enter yo	our usern	ame an	id password.				
				USE	RNAME	: cisco	-					
				PAS	SWORD): ********						
					GROUP	: WEBVI	PN	•				
						Logi	in	Clear				
Done											🔮 Internet	

EDVPN	Service	- Microso	it Inter	net Expl	orer		
Edit	⊻iew	Favorites	Tools	Help	(== Back • => • 💽 🔮	Address 2 https://136.1.123.12:444/+webvpn+,	Links "
ISCO at	STEM 5						
ullium		WebV	PN S	ervic	e		
						? 🖌	
WEB	APPL	ICATIO	NS		Web Bookmarks		
Enter V	Veb Ad	dress (UR	L		R1		
		<i></i>	r	Go			
Web B	cokma	rko	-				
WCD D	UOKIIIGI	K3					
PORT	FOR	WARDI	<u>NG</u>				
Start A	pplicati	on Client	l	Go			

Application forwarding is started automatically:

Close this wind Please wait for If you shut dow later have prob	ow when you fir the table to be n your compute lems running th	nish using Appli displayed befor r without closin le applications l	ication Acc re starting ng this wind listed below	ess. applicatio low, you 1 w. <u>Click h</u>	ons. might <u>ere for</u>
Name TELNET_R3	Local 127.0.0.1:20023	Remote 136.1.121.1:23	Bytes Out 0	Bytes In 0	Sockets 0
	<u>R</u> e	eset Byte Counter:	s	Tabaun ab	



Please wait fo If you shut do ater have pro <u>letails.</u>	r the table to be wn your compute blems running th	displayed befor r without closin e applications li	e starting g this wind isted below	applicatio low, you 1 w. <u>Click h</u>	ons. night <u>ere for</u>
Name TELNET_R3	Local 127.0.0.1:20023	Remote 136.1.121.1:23	Bytes Out 49	Bytes In 1721	Sockets 0

Further Reading
Thin-Client SSL VPN (WebVPN) on ASA with ASDM Configuration Example

ASA and SSL VPN Client

Objective: Configure the ASA to support remote SSL VPN Client connections.



Directions

- Configure devices as per the scenario "VPN/Common Configuration" <u>"PIX/ASA Easy VPN/WebVPN"</u>.
- by
- step
- directions
- on
- how
- to
- complete
- objective

Final Configuration

```
ASA1:
webvpn
port 444
webvpn enable outside
svc image disk0:/sslclient-win-1.1.3.173.pkg 1
svc enable
!
ip local pool SSLVPN 20.0.0.1-20.0.0.254
username CISCO password CISCO1234
!
```

Copyright © 2007 Internetwork Expert

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
!
group-policy SSLVPN internal
group-policy SSLVPN attributes
vpn-tunnel-protocol webvpn
webvpn
 svc required
 svc keep-installer installed
!
!
!
tunnel-group SSLVPN type webvpn
tunnel-group SSLVPN general-attributes
address-pool SSLVPN
default-group-policy SSLVPN
!
!
!
username CISCO attributes
vpn-group-policy SSLVPN
```

Verification	
🚰 Installation - Microsoft Internet Explorer	
Elle Edit View Favorites Iools Help 🗘 Back 🕶 🛩 🔇 🔮	Address 🛃 https://136.1.123.12:444/CACHE/stc/1/index.F
Cisco Systems SSL VPN CLIENT for WEBVPN	
Security Warning The installer is trying to launch ActiveX, which is digitally signed by Cisco Systems. In order to properly download and install the plug-in, be sure to click "Yes" on the security pop-up. Yes No	
	1.
	×
Opening page https://136.1.123.12:444/CACHE/stc/1/binaries/ocx.htm	📕 🖉 🚰 🔯 Internet

Further Reading

Release Notes for Cisco SSL VPN Client, Release 1.1.0 SSL VPN Client (SVC) on ASA with ASDM Configuration Example

VPN3k and WebVPN Client

Objective: Configure VPN3k concentrator to accept WebVPN client sessions.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"VPN3k Easy VPN/WebVPN"</u>.
- Enable WebVPN services on the Public interface.
- Configure WebVPN settings:
 - o Create URL entry "R1" to "http://136.1.111.1"
- Create group WebVPN:
 - Specify password "CISCO".
 - Permit WebVPN as the only tunneling protocol.
 - Configure WebVPN Attribute:
 - Disable URL entry.
 - Apply WebACL.
 - Configure WebACL to permit only access to URL "<u>http://136.1.111.1</u>"
- Create user "CISCO" with password "CISCO1234" and assign it to group "WEBVPN".

Final Configuration

VPN3k CLI:

Enable WebVPN on Public Interface:

🗿 Cisco Sy	stems, I	nc. VPN 30)00 Con	centrato	r [VPN3k] - Mic	rosoft In	terne	t Explorer		_ 🗆 >
<u>Eile E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	⇔ Back 🔹 ≖	⇒ - 💌	¢	Address 🛃 https://136.1.3	113.11/access.html	-
	+1/	VF	PN 30	000					Main Help	Support Logou
	天	Co	oncer	itrato	r Series N	Aanag	er			Logged in: admi
								Configu	ration Administ	ration Monitoring
Configur	ation ces			Config	uration Inte	rfaces E	ther	net 2		i i i i i i i i i i i i i i i i i i i
⊕ <u>Policy</u> ⊕ <u>Tunne</u> ⊕Adminis ⊕Monitori	<u>Managem</u> ling and <u>S</u> tration ng	<u>ent</u> ecurity		Confi Gener	ny changes, y guring Eth al RIP OSI	rou will b nernet I PF Ban	nter nter dwid	the connection and you w face 2 (Public). th WebVPN	rill have to restart	from the login
					ttrihute	Value		Doser	rintion	
				Allow HT	Managemer TPS sessior		Che on ti thro	ck to enable management nis interface. Disabling wil ugh a web browser on this	HTTP and HTT. prevent managir s interface.	PS sessions ng the device
				Al HT	low WebVP TPS sessior		Che inter	ck to enable WebVPN H face.	ITTPS sessions o	n this
c	isco Svs	TENS		Redi	rect HTTP (HTTP	^{to} S	Che redii Une this :	ck to force any connection rected to HTTPS. This pr ncrypted HTTP sessions r interface.	ns coming in as H ovides additional will no longer be	ITTP to be security. allowed on
	ավիստո	dlu.			Allow POP3 sessior	S D	Che usin	ck to enable POP3S e-m g an e-mail program.	ail sessions on thi	s interface
Accession of the second s	* * C	-							A 🙆 In	ternet

Create static URL entry for R1:



Tisco Systems Tor, VPN 3000 Co	ncentrator [VPN3k] - Microsoft Interne	at Evolorer		
<u>File Edit View Favorites Tools</u>	Help (= Back - =) - 🔊 🕅	Address	//136.1.113.11/access.html	
VPN 3	3000		Main Help Su	ipport Logout
Conce	ntrator Series Manager		Lo	aaed in: admin
Conte	in and series manager	C	onfiguration Administratio	on Monitoring
Configuration				
Interfaces	Configuration Tunneling and S	ecurity WebVPN	Servers and URLs	2000
<u> ⊕⊕System</u>			Save	Needed
	This section lets you configure ser	vers and URLs that	are accessible over WebV	PN
PPTP	connections. These include file ser	vers (CIFS), web s	servers (HTTP and HTTPS)), URLs,
	and e-mail proxy servers. You mu	ist also enable File <i>i</i>	Access on the Base Group/	Groups
	pages.			
	OP.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1			234525-0
	Click the Add button to add a ser	ver, or select a serv	er and click Modify, Dele	te or
HTTP/HTTPS Proxy	VIOVE			
Home Page		1 1 1 1 1		
E-mail Proxy	Serve	ers and URLs	Actions	
Servers and URLs	R1 (http	://136.1.111.1)		
Port Forwarding			17	
Cisco SSL VPN Client			Add	
-#- <u>Secure Desktop</u>		1	Modify	
- Honitoring		-	woully	
			Delete	
FICTA SVOTENC				
CISCO OTSIEMS				
autilium at the second second				
🕗 Web Servers and URLs	·		📄 📄 🤷 Interne	et //.

-						
	sco Systen	is, Inc. VPN 3	1000 Cond	centrator [VP	N3k] - Microsoft Intern	net Explorer
Eile	<u>E</u> dit ⊻ie	w F <u>a</u> vorites	<u>T</u> ools	Help 🔁	Back 🔹 🖘 💉 💽 🔂	Address 🕖 https://136.1.113.11/access.html
1		V	PN 3(000		Main Help Support Logou
	天	C	oncen	trator Se	eries Manager	r Logged in: admi
					Ű	Configuration Administration Monitoring
-Ģ-Co	nfiguration	L				
	<u>Interfaces</u>			Configuration	on User Manageme	ient Groups Add
	- <u>System</u> - <u>User Manac</u> <u>Base Gr</u> <u>Groups</u> <u>Users</u> - <u>Policy Mana</u>	<u>ement</u> oup gement		This section default to the override bas	lets you add a group e base group value. T se group values.	p. Check the Inherit? box to set a field that you want to Uncheck the Inherit? box and enter a new value to
L⊕	- <u>Tunnelinq a</u>	nd Security		Identity G	Seneral TIPSec Cli	lient Config Client FW HW Client PPTP/L2TP WebVPN
- E-Ad	ministratio	<u>in</u>			70 NG	Identity Parameters
10100	A new mag					
				Attribute	Value	Description
				Attribute Group Name	Value WEBVPN	Description Enter a unique name for the group.
				Attribute Group Name Password	Value WEBVPN	Description Enter a unique name for the group. Enter the password for the group.
				Attribute Group Name Password Verify	Value WEBVPN Image: second	Description Enter a unique name for the group. Enter the password for the group. Verify the group's password.
				Attribute Group Name Password Verify Type	Value WEBVPN	Description Enter a unique name for the group. Enter the password for the group. Verify the group's password. External groups are configured on an external authentication (e.g. RADIUS). Internal groups are configured on the VPN Concentrator's Internal Database.
				Attribute Group Name Password Verify Type	Value WEBVPN	Description Enter a unique name for the group. Enter the password for the group. Verify the group's password. External groups are configured on an external authentication (e.g. RADIUS). Internal groups are configured on the VPN Concentrator's Internal Database.
	Cisco	Systems		Attribute Group Name Password Verify Type Add	Value WEBVPN	Description Enter a unique name for the group. Enter the password for the group. Verify the group's password. External groups are configured on an external authentication (e.g. RADIUS). Internal groups are configured on the VPN Concentrator's Internal Database.

Create group "WEBVPN" with password "CISCO":

🚰 Cisco Systems, Inc. VPN 3000 C	oncentrator [VPN3k] - I	Microsoft Interne	t Explorer		
<u>File Edit View Favorites Tool</u>	ls Help 🗘 Back 🔹	• => • 🙆 🚱	Address 🛃 https://13	6.1.113.11/a	ccess.html
VPN	3000			Ma	ain Help Support Logout
Conce	entrator Series	Manager			Logged in: admin
			Conf	iguration	Administration Monitoring
		-			primary DNS server.
	Secondary DNS			N	Enter the IP address of the secondary DNS server.
	Primary WINS	I		N	Enter the IP address of the primary WINS server.
Users DPolicy Management DTunneling and Security	Secondary WINS			V	Enter the IP address of the secondary WINS server.
Administration Administration Routing Table Dynamic Filters Dynam	Tunneling Protocols	□ PPTP □ L2TP □ IPSec □ L2TP over I ☑ WebVPN	PSec		Select the tunneling proto group can connect with.
	Strip Realm	–		ସ	Check to remove the rea qualifier of the username authentication.
	DHCP Network Scope			ঘ	Enter the IP sub-network which users within this gr be assigned when using th concentrator as a DHCP
CISCO SYSTEMS	Apply C	Cancel			
街 Group Parameters					🔒 🔮 Internet 🥢

Enable WebVPN as the tunneling protocol:

Disable client URL entry:

🚰 Cisco Systems, Inc. YPN 3000 Concentrator [YPN3k] - Microsoft Internet Explorer 📃 🗌 🗙						
<u>File Edit View Favorites T</u> ool	ls <u>H</u> elp (⇔ Back → ⇒ → 💽	🖒 🛛 Address 🙋	https://136.1.	113.11/access.html	-	
VPN	3000			Main Help	Support Logout	
Conce	entrator Series Manage	er			Logged in: admin	
	0		Configu	ration Administra	tion Monitoring	
-[]- <u>Configuration</u>						
Interfaces	Configuration User Manage	ment Groups <i>I</i>	Add			
	This section lets you add a gro default to the base group value override base group values.	up. Check the Ir e. Uncheck the Ir	herit? box t herit? box :	to set a field that yo and enter a new va	yu want to lue to	
E	Identity General IPSec	Client Config ⊺ C	lient FW 🛛 H	W Client PPTP/L	2TP WebVPN	
- Administration	WebVPN Parameters					
H Monitoring	Attribute	Value	Inherit?	De	scription	
	Enable URL Entry			Check to place th the home page.	e URL entry bo	
	Enable File Access			Check to enable through HTTPS. Access, a NetBIC to be configured u Servers .	Windows file ac When enabling I DS Name Serve Inder System	
	Enable File Server Entry			Check to place th onto the home pay enabled.	e file server enti ge. File Access	
CISCO SYSTEMS	Enable File Server			Check to enable b network for doma	rowsing the Wi iins/workgroups ◄	
街 Group Parameters				📄 🤷 Inte	ernet //	

Permit WebACL Application:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Int	ernet Explorer		
<u>File Edit View Favorites Tools</u>	; <u>H</u> elp (⇔ Back → ⇒) → 💽	🚯 🛛 Address 🦉 http	os://136.1.113.11/acc	ess.html 💌 🗐
VPN :	3000		Mai	n Help Support Logout
Conce	entrator Series Manage	er		Logged in: admin
			Configuration A	dministration Monitoring
Configuration Interfaces ElSystem ElSystem Base Group	Enable File Access		through Access, to be co Servers	HTTPS. When enabling I a NetBIOS Name Serve nfigured under System 5.
Groups Users Delicy Management Dunneling and Security Administration Monitoring	Enable File Server Entry		Check t onto the enabled	o place the file server entr home page. File Access
	Enable File Server Browsing		Check t network and shar	o enable browsing the Wi for domains/workgroups es. File Access must be e
	Enable Port Forwarding		Check t	o enable port forwarding.
	Enable Outlook/Exchange Proxy		Check t proxy.	o enable the Outlook/Exc
	Apply ACL		Check t defined	o apply the WebVPN AC for the users of this group
	Enable Auto Applet Download		Check t login.	o enable auto applet dow
	Enable Citrix MetaFrame	itrix MetaFrame 🗖		o allow access using Citri ame terminal services.
Cisco Systems	Enable Cisco SSL VPN Client	Enable Cisco SSL VPN Client		o enable use of the Cisco ient.
Group Parameters				🔒 🔮 Internet

Configure WebACL:

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3k] - Microsoft Intern	et Explorer		
<u>File Edit View Favorites Tools</u>	Help ⇔Back → ⇒ → 😒 🚱	Address 🙋 https://136.1	1.113.11/access.html	
VPN 3	000		Main Help Support Logout	
Conce	ntrator Series Manager		Logged in: admin	
		Config	uration Administration Monitoring	
			cookies to track visitors.	
	WebVPN ACLs			
	permit url http://136.1.		 The WebVPN Access Control L apply to user sessions. If you do not define any filters, connections are permitted. If you configure a permit filter, default action is to deny connectic than what the filter defines. A WebVPN ACL can have a 255 characters. Source and destination IDs are addresses and wildcard masks or hostnames. WebVPN ACLs are not applie SSL VPN Client connections. Or ACLs are applied to the SSL VP Client. 	
Cisco Systems	Syntax for protocol filters: [permit deny] [ip smtp im Example: permit ip any host Example: permit ip any 192 (ap4 pop3 cifs http t 10.86.9.22 .168.1.0 0.0.0.255	https]Src-ID Dst-ID	
🕗 Group Parameters			📄 🔮 Internet 🥢	

Create user <code>"CISCO"</code> with <code>password</code> <code>"CISCO1234"</code> and add it to group <code>"WEBVPN"</code>:

🚰 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer 📃 🗖 🛛						
<u>Eile Edit View Favorites Tools</u>	Help 🗘 🗘 Ba	ck 🔹 🔿 🔹 🚺	Address 🙋 https://136.1.113.11/access.html	-		
VPN 30	00		Main Help S	Support Logout		
Concentrator Series Manager Logged in: admin						
Configuration Administration Monitoring						
Interfaces	Configuration User Management Users Add					
	This section lets you add a user. Uncheck the Inhavit? how and enter a new value to					
Base Group	override group values					
Users						
	Identity Ge	neralŤIPSecŤPPT	P/L2TP			
<u>-</u> <u></u>)	I	dentity Parameters			
-#Monitoring	Attribute Value Description					
	Username	CISCO	Enter a unique username.			
	Password	*****	Enter the user's password. The password m	ust satisfy		
	Verify	kololololololok	Verify the user's password			
	Groun		Enter the group to which this user belongs			
	TT & Januar		Enter the ID eddares estimed to the this see			
	IF Autress		Enter the LP address assigned to this user.			
	Subnet Maale		Enter the subnet mask assigned to this user.			
	IVIASK					
	Add	Cancel				
CISCO SYSTEMS						
User Parameters			📔 🔮 Inte	rnet //		
Verification

Connect to the public interface of VPN3k:

ðw	eb¥PN	Servic	es - Micros	oft Inte	rnet Ex	plorer						
File	Edit	⊻iew	F <u>a</u> vorites	Tools	Help	Back	* =>	- 💌 😰	Address 🛃 https://136.1.1	.13.11/webvpn.html	-	1
C	sco S1	STEMS	WebV	'PN S	ervio	es						
				F	Please Userr Passi Log	enter yo name Cis word F	our use SCO 	Login ername and	d password.			
E D	one									🔒 🎯 Interne	ət	

¢°¶₩	eb¥PN	Servic	es - Micros	oft Inte	rnet Exp	olorer							_ 🗆 🛛
Eile	<u>E</u> dit	⊻iew	Favorites	Tools	Help	🗘 Back	•=	- 🗵 🖸	A	ddress 🙋 https://136	5.1.113.11/web	vpn/index.html	-
CI	sco Sy	STEMS	WebV	PN S	ervic	es						?	
				<u>lf t</u>	ne Floa	ating Too	lbar c	loes not	oper	i <u>, click here to op</u>	en it.		
-							1	Websit	es				
<u>R</u> ′													
													*
🥑 D	ownload	ling from	n site: about:	blank								j 💋 Internet	11



Check statistics on the VPN3k:

<u>E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>T</u> ools <u>H</u> elp 🗲	Back 🔹	- => - 💌 🛛) /	A <u>d</u> dres:	s 🙋 htt	tps://136.1.1	13.11/access.htm	nl	•
VP	N 3000							Main He	lp Sup	oport Log
Co	ncentrator S	eries	Manage	r					Log	ged in: ad
				19(0) 1	HINE	0-1-9-13	Configura	ation Admin	istratio	n Monito
onfiguration dministration				110 12		o mi	1 0 0 0 0 1 0 1 0			
onitoring										
— <u>Routing Table</u> — <u>Dγnamic Filters</u>	Remote	Acce	ess Session:	S	[<u>L</u>	AN-to-	LAN Sess	ions Manag	ement S	essions]
BFilterable Event Log BSystem Status Sessions Protocols Encryption Brop Ten Lists	Username	Assi Add Pub Add	igned P hress Gro hc P hress	up	Prot Encr	tocol yption	Login Time <u>Duration</u>	<u>Client</u> <u>Type</u> <u>Version</u>	Bytes Tx Bytes <u>Rx</u>	<u>NAC</u> <u>Result</u> <u>Posture</u> <u>Token</u>
<u>⊦Statistics</u>	CISCO	N 10.0	I/A 0.100 WEB	VPN	Web 3DE: SS	VPN S-168 Lv3	Jan 21 23:26:15 0:06:21	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) N/A	64323 13897	Unknown
	Manage Administ	ment rator	Sessions IP Address	[Prote	LAN col	I-to-L./ Enc	AN Sessior ryption	ns Remote A Login Ti	.ccess S me D	essions] Puration
Cisco Systems	admin		10.0.0.100	HITI	P :	3DES-	168 SSLv3	Jan 21 23:3	32:21 0	:00:15

Further Reading

Configuring the VPN Concentrator for WebVPN

VPN3k and WebVPN Port Forwarding

Objective: Configure VPN3k to provide port-forwarding service to WebVPN clients.



Directions

- Configure devices as per the scenario "VPN/WebVPN and SSL VPN" <u>"VPN3k and WebVPN Client"</u>.
- We would like to tunnel local connection to port 20023 to remote router R1 port 23.
- Configure group WEBVPN
 - Set up port-forwarding:
 - Use name TELNET_R1.
 - Specify local port 20023
 - Specify remote server 136.1.111.1
 - Specify remote port 23
 - Enable port-forwarding under group's WebVPN attributes.
 - Modify WebACL to permit any type of access to host 136.1.111.1

Final Configuration

VPN3k GUI:

Configure port-forwarding settings for group "WEBVPN":

🖉 Cisco Systems, Inc. VPN 3000 C	oncentrator [¥PN3k] - Microsoft Intern	net Explorer 📃 🗆 🗙					
<u>File Edit View Favorites Tool</u>	s Help 🗘 Back 🔹 🖘 🔹 🛃	Address 🙋 https://136.1.113.11/access.html					
VPN	3000	Main Help Support Logout					
Conce	entrator Series Manager	Logged in: admir					
	0	Configuration Administration Monitoring					
Configuration Interfaces System	Configuration User Manageme	ent Groups WebVPN Port Forwarding Save Needed 🔒					
	This section lets you configure TC must enable TCP Port forwarding below, then the global list of forw	CP port forwarding for WebVPN users in this group. You ng on the Base Group/Group pages. If no ports are defined warded ports is used.					
	Click the Add button to add a forwarded port, or select a forwarded port and click Modify or Delete. Click Done to finish.						
	Port	rt Forwarding for WEBVPN					
	For	rwarded Ports Actions					
		- Empty —					
		Add					
		Modify					
		Delete					
		Deve					
		Dohe					
CISCO SYSTEMS							
🛃 Group Parameters		📔 📔 💕 Internet 💋					

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3k] - Microsoft Interne	t Explorer
<u>File Edit View Favorites T</u> ools	: <u>H</u> elp 🗢 Back → ⇒ → 🙆 🔂	Address 🖉 https://136.1.113.11/access.html
VPN 3	3000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
		Configuration Administration Monitoring
-E <mark>) Configuration</mark> 	Configuration User Managemen	t Groups WebVPN Port Forwarding Add
Base Group Groups	Configure a forwarded TCP port.	
Users	Name TELNET_R1	Enter a name or short description for the user to see.
	Local 20023 TCP Port	This is the TCP port that the user connects to on their local workstation. Setting the TCP port in the range from 1024 to 65535 is recommended to avoid conflicts with existing services that may be on the user's workstation.
	Remote 136.1.111.1	Enter name or IP address of the remote server. Connections to the local port are forwarded to this remote server.
	Remote Z3	Enter the TCP port on the remote server that connections to the local port will be forwarded to.
Cisco Systems	Add Cancel	
🙆 Group Parameters		📄 🎽 💕 Internet 🏼 🎢

Enable port forwarding under WebVPN tab and permit it with WebACL:

🖉 Cisco Systems, Inc. VPN 3000 Con	centrator [VPN3k] - Microsoft Int	ernet Explorer		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help (⇔ Back → ⇒ → 😒	🚯 Address 🦉	https://136.1.1	113.11/access.html
VPN 3 Concer	000 ntrator Series Manag	er		Main Help Support Logout Logged in: admin
			Configur	ation Administration Monitoring
- <u>Configuration</u>		WebVP	'N Parame	eters 🔺
Interfaces III-System	Attribute	Value	Inherit?	Description
Base Group	Enable URL Entry			Check to place the URL entry bo the home page.
Users Users <u>DPolicy Management</u>	Enable File Access			Check to enable Windows file ac through HTTPS. When enabling I Access, a NetBIOS Name Serve to be configured under System Servers.
	Enable File Server Entry			Check to place the file server entr onto the home page. File Access enabled.
	Enable File Server Browsing			Check to enable browsing the Wi network for domains/workgroups and shares. File Access must be e
	Enable Port Forwarding	V		Check to enable port forwarding.
	Enable Outlook/Exchange Proxy			Check to enable the Outlook/Exc proxy.
CISCO SYSTEMS	Apply ACL	অ		Check to apply the WebVPN A(defined for the users of this group
authnaathna	Enable Auto Applet	-		Check to enable auto applet dow
🕗 Group Parameters				📑 🔮 👔 Internet 🥢



Verification

Connect to VPN3k & start application access:

e v	eb¥PN	Servic	es - Micros	oft Inte	rnet Exp	lorer								_ 🗆 ×
Eile	Edit	⊻iew	Favorites	<u>T</u> ools	Help	🗘 Back	•=> *	8	A <u>d</u> dress	s 🙋 https://136.	1.113.11/w	ebvpn/inde:	<.html	-
	sco Sy	STEMS	WebV	PN S	ervic	es						?		
				<u>lf t</u>	ne Floa	ating Too	olbar do	es not o	<u>pen, clic</u>	<u>k here to ope</u>	<u>en it.</u>			
						<u>S</u>	tart Ap	plicatior	Acces	S				
							1	Nehsite						
R1								irebalte.						
												0		*
2											J	📄 😻 Ir	nternet	1

Close Please wai	this window when it for the table to	n you finish usir be displayed be	ng Applicat efore starti	ion Acces ng applic	ss. ations.
'you shut dov	wn your computer	without closing th	is window,	you might	later hav
problem	is running the appli	cations listed belo	ow. <u>Click he</u>	ere for det	atis.
Name	Local	Remote	Bytes Out	Bytes In	Sockets
ELNET R1	127.0.0.1:20023	136.1.111.1:23	0	0	0

Verify local port 20023:

C:\WINNT\system32\cmd.exe			_ 🗆 🗙
C:\>netstat -an ¦ findstr 023 TCP 127.0.0.1:20023 TCP 127.0.0.1:20023 TCP 127.0.0.1:20023	0.0.0.0:0 127.0.0.1:1378 127.0.0.1:1462	LISTENING TIME_WAIT TIME_WAIT	
C:\>telnet 127.0.0.1 20023_			
			-

 C.\WINNT\system32\cmd.exe - telnet 127.0.0.1 20023
 R1>show ver Cisco Internetwork Operating System Software (Gisco Internetwork Operating System Software (Fc1)
 Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc. Compiled Fri 12-Aug-05 15:49 by kehsiao Image text-base: 0x80008098, data-base: 0x81942FEC
 ROM: System Bootstrap, Version 11.3(2)XA3, PLATFORM SPECIFIC RELEASE SOFTWARE (f c1)
 ROM: C26600 Software (C2600-IK90383-M), Version 12.2(15)I17, RELEASE SOFTWARE (f c1)
 ROM: C26600 Software (C2600-IK90383-M), Version 12.2(15)I17, RELEASE SOFTWARE (f c1)
 R1 uptime is 2 hours, 40 minutes System returned to ROM by reload System image file is "flash:c2600-ik903s3-mz.122-15.T17.bin"
 This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
 A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wu/export/crypto/tool/stgrg.html
 If you require further assistance please contact us by sending email to export@cisco.com.
 cisco 2610 (MPC860) processor (revision 0x202) with 59392K/6144K bytes of memory . Frocessor board ID JAB03040BW9 (1247782719) M860 processor: part number 0, mask 49 Eridging software.

Check session statistics on VPN3k:

- Microsoft Inl	ternet Explorer			_ 🗆 >
window whe r the table to our computer nning the appl	n you finish usin be displayed be without closing th ications listed bel	n g Applicat efore starti nis window, ow. <u>Click h</u>	ion Acces ing applic you might ere for det	ss. ations. later have <u>ails.</u>
Local	Remote	Bytes Out	Bytes In	Sockets
27.0.0.1:20023	136.1.111.1:23	85	1718	1
R	eset Byte Counter	s		r
	R	<u>R</u> eset Byte Counter	<u>R</u> eset Byte Counters	<u>R</u> eset Byte Counters

Copyright © 2007 Internetwork Expert

Further Reading

Configuring the VPN Concentrator for WebVPN

<u>VPN QoS</u>

IOS and the PIX/ASA: Policing the L2L IPsec tunnel

Objective: Configure policing for L2L IPsec tunnel on the ASA firewall.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and the PIX/ASA with PSK"</u>.
- Create class-map L2L_TO_R3_DATA and match tunnel group "136.1.123.3". Match flow based on destination IP.
- Create class-map L2L_TO_R3_VOICE and match tunnel group "136.1.123.3". Match DSCP EF.
- Create policy-map OUTSIDE:
 - Match class L2L_TO_R3_DATA. Police up to 128Kbps with default burst.
 - Match class L2L_TO_R3_VOICE. Provide LLQ service for this class.
 - o For class-default police to 2000000 bps
- Apply policy-map OUTSIDE to outside interface.

Final Configuration

```
ASA1:

class-map L2L_TO_R3_DATA

match tunnel-group 136.1.123.3

match flow ip destination

!

class-map L2L_TO_R3_VOICE

match tunnel-group 136.1.123.3

match dscp ef
```

Copyright © 2007 Internetwork Expert

```
policy-map OUTSIDE
    class L2L_TO_R3_DATA
    police out 128000
    class L2L_TO_R3_VOICE
    priority
    class class-default
    police out 2000000
!
service-policy OUTSIDE interface outside
```

Verification

```
R1#ping 136.1.23.2 repeat 1000 size 1000
Type escape sequence to abort.
Sending 1000, 1000-byte ICMP Echos to 136.1.23.2, timeout is 2 seconds:
Success rate is 96 percent (967/1000), round-trip min/avg/max = 28/34/621 ms
ASA1(config)# show service-policy interface outside
Interface outside:
Service-policy: OUTSIDE
 Class-map: L2L_TO_R3_VOICE
  Priority:
   Interface outside: aggregate drop 0, aggregate transmit 0
 Class-map: L2L_T0_R3_DATA
  Output police Interface outside:
   cir 128000 bps, bc 4000 bytes
   conformed 967 packets, 1034690 bytes; actions: transmit
   exceeded 33 packets, 35310 bytes; actions: drop
   conformed 0 bps, exceed 0 bps
 Class-map: class-default
  Output police Interface outside:
   cir 2000000 bps, bc 62500 bytes
   conformed 367 packets, 59649 bytes; actions: transmit
   exceeded 0 packets, 0 bytes; actions: drop
   conformed 0 bps, exceed 0 bps
```

Further Reading

Applying QoS Policies

IOS and VPN3k: QoS for L2L Tunnel

Objective: Configure VPN3k to provide minimum bandwidth and maximum allowed rate for a tunnel.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK"</u>.
- Create Bandwidth Policy named DEFAULT:
 - Reserve 56Kbps
 - Policy to 56Kbps
- Create Bandwidth Policy named "VPN_TO_R2":
 - Use bandwidth of 128Kbps
 - Police up to 256Kbps
- Consider the minimum bandwidth along the path to VPN3k to be 2Mbps. Configure Public interface bandwidth accordingly.
- Assign "DEFAULT" policy as default Public interface bandwidth policy.
- Configure L2L Tunnel "VPN_TO_R2" to use bandwidth policy "VPN_TO_R2".

Final Configuration

VPN3k:

Create default bandwidth policy:

😤 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Internet Explorer	
<u>File Edit View Favorites T</u> ools	Help ⇐ Back • ⇒ • 🛞 🚯 Address 🙆 https://136.	1.121.11/access.html
VPN 3	3000	Main Help Support Logout
Conce	ntrator Series Manager	Logged in: admin
	Config	uration Administration Monitoring
	Configuration Policy Management Traffic Manageme Configure bandwidth policy parameters. To create a band	nt Bandwidth Policies Modify width policy, you must enable at
Access Hours	Policy Name DEFAULT	Enter a unique name for this policy.
Filters 	 Bandwidth Reservation Minimum Bandwidth 56 	Check to reserve a minimum bandwidth per session. Enter the minimum bandwidth.
	Traffic policing allows you to control a policing rate or size on an interface. Traffic that exceeds the policing rate or bu Policing	e of traffic transmitted or received arst size is dropped. Check to enable Policing.
Alerts	Policing Rate 56 kbps 💌	Enter the policing rate. Traffic below this rate will be transmitted; traffic above this rate will be dropped.
	Normal Burst Size 10500 bytes	Enter the amount of data allowed in a burst before excess packets will be

<u>File Edit View Favorites Tool:</u>	s Help 🗘 🖙 Back 🕶 🚽 💌 🔯 🛛 Address	🛿 🖉 https://136.1.121.11/access.html 🛛 🗾 🔳
VPN :	3000	Main Help Support Logout
Conce	entrator Series Manager	Logged in: admir
		Configuration Administration Monitoring
Configuration Interfaces	Configuration Policy Management Traf	fic Management Bandwidth Policies Add
	Configure bandwidth policy parameters. To least one of the checkboxes.	o create a bandwidth policy, you must enable at
	Policy Name VPN_TO_R2	Enter a unique name for this policy.
EVV Policies	🛛 Bandwidth Reservation	Check to reserve a minimum bandwidth per session.
	Minimum Bandwidth 128	kbps 💌 Enter the minimum bandwidth.
	Traffic policing allows you to control a polio on an interface. Traffic that exceeds the pol	cing rate or size of traffic transmitted or received licing rate or burst size is dropped.
LAN-to-LAN	🔽 Policing	Check to enable Policing.
NAT Transparency Alerts 	Policing Rate 256	Enter the policing rate. Traffic below this rate will be transmitted; traffic above this rate will be dropped.
CISCO SYSTEMS	Normal Princt Size 10500	Enter the amount of data

Create bandwidth policy for L2L tunnel:

Configure Public interface:

🚰 Cisco Systems, Inc. VPN 3000 Con	centrator [¥PN3K] - Microsoft I	nternet Explorer] X		
<u>File Edit View Favorites Tools</u>	Help 🗘 🖙 Back 🔹 🖘 👻) 🙆 Address 🖉 https://136.1.121	.11/access.html			
VPN 3	000		Main Help Support Log	out		
Concer	itrator Series Mana	ger	Logged in: ad	min		
		Configurati	ion Administration Monitor	ing		
- <u>Interfaces</u>	General RIP OSPF Ba	ndwidth WebVPN		1		
	Bandwidth Management Parameters					
	Attribute	Value	Description			
PTunneling and Security PPTP L2TP	Bandwidth Management		Check to enable bandwidth management.			
-EHPSec LAN-to-LAN HE Proposals 	Link Rate	2 Mbps 💌	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.			
Cisco Systems	Bandwidth Policy		This policy is applied to all VPN tunnels that do not have a group based Bandwidth Management policy. Policies are configured at Configuration Policy Management Traffic Management Bandwidth			

🚰 Cisco Systems, Inc. ¥PN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer	
<u>File Edit View Favorites T</u> ools	Help 🗘 🖙 Back 👻 🖈 🖉 🛐	Address 🖉 https://136.1.121.11/access.ht	tml 🔄 🗐
VPN 3	3000	Main H	elp Support Logout
Conce	ntrator Series Manager		Logged in: admin
		Configuration Admi	nistration Monitoring
- <u> - Configuration</u>			<u> </u>
	Configuration Tunneling and S	ecurity IPSec LAN-to-LAN	
			Save Needed
Delicy Management	This section lets you configure TDS	er TANT to TANT connections, TANT t	~ T AN
Tunneling and Security	connections are established with o	ther VPN 3000 Concentrators PTX fir	ewalls 7100/4000
	series routers and other PSec-co	mpliant security gateways. To configure	a VPN 3002 or
	other remote access connection, g	o to User Management and configure a	Group and User.
LAN-to-LAN	To configure NAT over LAN-to-	LAN, go to LAN-to-LAN NAT Rules	
KE Proposals			
	Click the Add button to add a LA	N-to-LAN connection, or select a com	nection and click
	Modify or Delete.		
—⊕ <u>ssl</u>		2 (A) (2) (3)	
	(D) indicates a disabled LAN-to-1	LAN connection.	
	LA	N-to-LAN	(
	С	onnection	Actions
	VPN TO R2 (136.1.122.	2) on Ethernet 2 (Public)	
			Add
			Modify
		5	wouny
CISCO SYSTEMS			Delete
authtrassathtras.			•
IKE Proposals			Dinternet

Apply bandwidth policy to L2L Tunnel:

🖉 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer View Favorites Tools Help (= Back + => - 🙁 👩 Address 🙋 https://136.1.121.11/access.html File Edit 1 **VPN 3000** Main | Help | Support | Logout **Concentrator Series Manager** Logged in: admin Configuration | Administration | Monitoring * Configuration * IPSec NAT-T □ connection through a NAT -Interfaces device. You must also enable -⊞-<u>System</u> IPSec over NAT-T under -<u>⊞-User Management</u> NAT Transparency. Policy Management -Access Hours Choose the bandwidth policy Bandwidth Policy VPN_TO_R2 to apply to this LAN-to--Network Lists LAN connection. -Rules SAS Choose the routing -Filters mechanism to - MAT Routing None use. Parameters below are -BW Policies ignored if Network - Group Matching Autodiscovery is chosen. - Network Admission Control -Tunneling and Security PPTP Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network L2TP address. EHPSec Specify the local network -LAN-to-LAN HKE Proposals address list or the IP address Network List Use IP Address/Wildcard-mask below 💌 -NAT Transparency and wildcard mask for this Alerts LAN-to-LAN connection. -<u>SSH</u> - SSL -Note: Enter a wildcard CISCO SYSTEMS IP Address 150.1.1.0 mask, which is the reverse allu սՈՒ of a subnet mask. A IPSec LAN-to-LAN 🔒 🎯 Internet

CCIE Security Lab Workbook Volume I Version 3.0

Verification

VPN3k:

Administration > Administer Session > Detail

e Edit View Favorites Loois	Help 🗘 Back	、 + ≓	- 🛛	Addres	s 🙋 https://	136.1.121.11	access.html				
VPN 3	000						Aain Help	Support	Logo		
Concer	ntrator Serie	es N	lanag	er				Logged in	n: adn		
				9 - 1999 - 90 - 90 - 90 - 90 - 90 - 90 -	Co	nfiguration	Administr	ation Mo	nitori		
<u>∓-User Management</u> ▲	0 durinistration	1.0.1	luistar (Canalana I Da	4.1	Maudau	45 1	. 2007 22.2	1.00		
<u> Policy Management</u>	Auministration	Aan	iinister :	Sessions De	tall	monuay,	To January Recot	2007 23:2			
							ncoci	Nelles	an Cov		
Network Lists	Back to Session	15									
Rules		_									
	Connection			management	.	Login	.	Bytes	By		
	Name	IPA	ddress	Protocol	Encryptic	in Time	Duration	Tx	R		
<u>BW Policies</u>	TENT DO DO	100.	1 100 0	IPSec/LAN-	J- 00000 1 400	Jan 15	0.01.00	1000550	1005		
	VPN_IO_RZ	130.1	1.122.2	to-LAN	SDES-10	⁵ 23:22:35	0:01:30	1008260	100.		
Tunneling and Security											
	Bandwidth St	atisti	cs								
	Troffic Vo					Volumo					
LAN-to-LAN	User Name		Interface	erface	Traffic Rate (kbps)		(bytes)				
						C	onformed	Throttled	Conformed	l Throttl	ed
NAT Transparency											
Alerts		.	Etherne	et 2	المعد		40001	21	0		
Alerts	VPN_TO_R2	? (In)	Etherne (Public	et 2)	105	0	105954	-			
Alerts 	VPN_TO_R2	? (In)	Etherne (Public Etherne	et 2) et 2	105	0	105954				
NAT Transparency Alerts SSH GPSSL GWebVPN dministration - Administration	VPN_TO_R2 VPN_TO_R2 (Out)	? (In) ?	Etherne (Public) Etherne (Public)	et 2) et 2)	105 105	0	105954:	2	0		
Alerts SSH SSH SSH SSH SSH Alerts SSH Alerts SSH SSH SSH Alerts SSH SSH Alerts SSH Alerts SSH SSH Alerts Alerts Al	VPN_TO_R2 VPN_TO_R2 (Out)	? (In) ?	Etherne (Public Etherne (Public	et 2) et 2)	105	0	105954	2	0		
Alerts Alerts SSH SSL WebVPN dministration Administer Sessions	VPN_TO_R2 VPN_TO_R2 (Out)	? (In) ?	Etherne (Public Etherne (Public	et 2) et 2)	105	0	105954	2	0		
NAT Transparency Alerts SSH B-SSL D-WebVPN dministration -Administer Sessions Cisco Systems antillingual linguage	VPN_TO_R2 VPN_TO_R2 (Out)	? (In) ?	Etherne (Public Etherne (Public	et 2) et 2)	105	0	105954	2	0		

Further Reading

VPN3k: Policy Management

PIX/ASA and Cisco VPN Client: Per-Flow Policing

Objective: Configure the firewall to limit maximum permitted per-flow rate for remote-access VPN group users.



Directions

- Configure devices as per the scenario "VPN/ezVPN"
 <u>"The PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI"</u>.
- Create class-map VPN_DATA and match tunnel group "EZVPN". Match flow based on destination IP.
- Create class-map L2L_TO_R3_VOICE and match tunnel group "EZVPN". Match DSCP EF.
- Create policy-map OUTSIDE:
 - Match class VPN_DATA. Police up to 256Kbps with default burst.
 - Match class VPN_VOICE. Provide LLQ service for this class.
 - For class-default police to 2000000 bps
- Apply policy-map OUTSIDE to outside interface.

Final Configuration

```
ASA1:

!

! Tunneled voice traffic, marked by DSCP EF

!

class-map VPN_VOICE

match dscp ef

match tunnel-group EZVPN
```

Copyright © 2007 Internetwork Expert

```
! Tunneled data flows
!
class-map VPN DATA
match flow ip destination-address
match tunnel-group EZVPN
!
! Outside interface policy
!
policy-map OUTSIDE
class VPN_VOICE
 priority
class VPN_DATA
 police output 256000
class class-default
 police output 2000000
T
service-policy OUTSIDE interface outside
```

Verification

Connect Cisco VPN Client to the ASA: ASA1(config)# show vpn-sessiondb remote Session Type: Remote Username : CISCO Index : 1 Assigned IP : 20.0.0.1 : 136.1.100.200 Public IP Encryption : 3DES Protocol : IPSec Hashing : MD5 : 978500 : 978500 Bytes Tx Bytes Rx Client Type : WinNT Client Ver : 4.8.01.0300 Group Policy : EZVPN Tunnel Group : EZVPN Login Time : 07:10:40 UTC Mon Jan 22 2007 Duration : 0h:09m:50s Filter Name : NAC Result : N/A Posture Token: R1#ping 20.0.0.1 repeat 1000 size 1000 Type escape sequence to abort. Sending 1000, 1000-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds: 1111111111111111111111

Copyright © 2007 Internetwork Expert

Success rate is 97 percent (978/1000), round-trip min/avg/max = 8/9/24 ms R1# ASA1(config)# show ipsec sa interface: outside Crypto map tag: DYNAMIC, seg num: 10, local addr: 136.1.123.12 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (20.0.0.1/255.255.255.255/0/0) current_peer: 136.1.100.200, username: CISCO dynamic allocated peer ip: 20.0.0.1 #pkts encaps: 983, #pkts encrypt: 983, #pkts digest: 983 #pkts decaps: 983, #pkts decrypt: 983, #pkts verify: 983 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 983, #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.: 136.1.123.12, remote crypto endpt.: 136.1.100.200 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 457752CA inbound esp sas: spi: 0x3A8E8CC1 (982420673) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 2, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 28691 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x457752CA (1165447882) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 2, crypto-map: DYNAMIC sa timing: remaining key lifetime (sec): 28691 IV size: 8 bytes replay detection support: Y ASA1(config)# show service-policy interface outside Interface outside: Service-policy: OUTSIDE Class-map: VPN_VOICE Prioritv: Interface outside: aggregate drop 0, aggregate transmit 0 Class-map: VPN_DATA Output police Interface outside: cir 256000 bps, bc 8000 bytes conformed 983 packets, 1041412 bytes; actions: transmit exceeded 22 packets, 23408 bytes; actions: drop conformed 14408 bps, exceed 320 bps Class-map: class-default Output police Interface outside: cir 2000000 bps, bc 62500 bytes conformed 983 packets, 1047290 bytes; actions: transmit exceeded 0 packets, 0 bytes; actions: drop conformed 14488 bps, exceed 0 bps

Further Reading

Applying QoS Policies

QoS Pre-Classify for IPsec Tunnel

Objective: Configure IOS router for QoS pre-classify feature with IPsec tunnel.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario <u>"IOS and IOS with PSK Across the PIX/ASA".</u>
- QoS pre-classify feature permits classification on an interface to occur before the actual data encryption. In turn, this feature is useful to apply QoS policies to tunnel-encapsualted traffic.
- Configure class-map VPN_VOICE:
 - Match traffic with DSCP value EF.
 - Match access-list LO1_TO_LO2.
- Configure class-map VPN_DATA:
 - Match access-list LO1_TO_LO2.
 - Match traffic with DSCP value any besides EF.
- Configure policy-map VPN_QOS:
 - For class VPN_VOICE provide prioriy queue with 64Kbps
 - For class VPN_DATA police traffic up to 256Kbps
- Create policy-map INTERFACE_QOS:
 - Shape class-default up to 384Kbps
 - Apply policy-map VPN_QOS inside class-default.
- Configure crypto-map VPN:
 - Enable QoS pre-classify.

Final Configuration

```
R1:
1
! VPN voice traffic
1
class-map VPN_VOICE
 match access-group name LO1_TO_LO2
  match dscp ef
!
! VPN regular data
!
class-map VPN_DATA
match access-group name LO1_TO_LO2
match not dscp ef
1
! Configure VPN QoS Policy
!
policy-map VPN_QOS
 class VPN_VOICE
   priority 64
  class VPN_DATA
   police 256000
!
policy-map INTERFACE_QOS
  class class-default
   shape average 384000
    service-policy VPN_QOS
!
! Apply service policy to an interface
1
interface E0/0
  service-policy output INTERFACE_QOS
!
! Enable QoS pre-classify under crypto map
!
crypto map VPN 10
 qos pre-classify
```

Verification

Copyright © 2007 Internetwork Expert

5 minute offered rate 8000 bps, drop rate 0 bps Match: any Traffic Shaping Target/Average Byte Sustain Excess Interval Increment Limit bits/int bits/int (ms) (bytes) Rate 384000/384000 2400 9600 9600 25 1200 Packets Bytes Packets Bytes Shaping Adapt Oueue Active Depth Delayed Delayed Active 0 203 214186 0 0 no Service-policy : VPN_QOS Class-map: VPN_DATA (match-all) 200 packets, 214000 bytes 5 minute offered rate 8000 bps, drop rate 0 bps Match: access-group name LO1_TO_LO2 Match: not dscp ef police: cir 256000 bps, bc 8000 bytes conformed 200 packets, 214000 bytes; actions: transmit exceeded 0 packets, 0 bytes; actions: drop conformed 8000 bps, exceed 0 bps Class-map: VPN_VOICE (match-all) 0 packets, 0 bytes 5 minute offered rate 0 bps, drop rate 0 bps Match: dscp ef Match: access-group name LO1_TO_LO2 Queueing Strict Priority Output Queue: Conversation 40 Bandwidth 64 (kbps) Burst 1600 (Bytes) (pkts matched/bytes matched) 0/0 (total drops/bytes drops) 0/0 Class-map: class-default (match-any) 3 packets, 186 bytes 5 minute offered rate 0 bps, drop rate 0 bps Match: any Send traffic with DSCP EF value; note that EF corresponds to DSCP value 46 and ToS byte 46*4=184: R1#ping Protocol [ip]: Target IP address: 150.1.2.2 Repeat count [5]: 100 Datagram size [100]: Timeout in seconds [2]: 1 Extended commands [n]: y Source address or interface: 150.1.1.1 Type of service [0]: 184 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 100, 100-byte ICMP Echos to 150.1.2.2, timeout is 1 seconds: Packet sent with a source address of 150.1.1.1

Copyright © 2007 Internetwork Expert

```
..........
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/11/13 ms
R1#show policy-map interface ethernet 0/0
Ethernet0/0
  Service-policy output: INTERFACE_QOS
   Class-map: class-default (match-any)
     825 packets, 301562 bytes
     5 minute offered rate 2000 bps, drop rate 0 bps
     Match: any
     Traffic Shaping
          Target/Average Byte Sustain Excess
                                                  Interval Increment
                        Limit bits/int bits/int (ms)
                                                           (bytes)
           Rate
          384000/384000
                         2400
                                9600
                                         9600
                                                   25
                                                            1200
                      Packets Bytes
                                        Packets Bytes
       Adapt Queue
                                                            Shaping
       Active Depth
                                         Delayed Delayed
                                                            Active
                                301562
             0
                       825
                                         0
                                                  0
                                                            no
     Service-policy : VPN_QOS
       Class-map: VPN_DATA (match-all)
         500 packets, 263800 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match: access-group name LO1_TO_LO2
         Match: not dscp ef
         police:
            cir 256000 bps, bc 8000 bytes
           conformed 500 packets, 263800 bytes; actions:
            transmit
           exceeded 0 packets, 0 bytes; actions:
            drop
           conformed 0 bps, exceed 0 bps
       Class-map: VPN VOICE (match-all)
         100 packets, 16600 bytes
         5 minute offered rate 2000 bps, drop rate 0 bps
         Match: dscp ef
         Match: access-group name LO1_TO_LO2
         Queueing
           Strict Priority
           Output Queue: Conversation 40
           Bandwidth 64 (kbps) Burst 1600 (Bytes)
           (pkts matched/bytes matched) 0/0
           (total drops/bytes drops) 0/0
       Class-map: class-default (match-any)
         225 packets, 21162 bytes
         5 minute offered rate 0 bps, drop rate 0 bps
         Match: any
```

Further Reading

Reference Guide to Implementing Crypto and QoS Quality of Service Options on GRE Tunnel Interfaces

Copyright © 2007 Internetwork Expert

Advanced VPN Topics

Decoding IPsec Debugging Output on VPN3k

Objective: Configure VPN3k debugging for IPsec/IKE events.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK using CLI"</u>.
- Activate logging for the following systems Events:
 - IKE, IKEDBG, IKEDECODE.
 - IPSEC, IPSECDBG, IPSEDECODE.
 - Log events with severity up to 9.
- Configure Monitor Log to display up to 100 events per page.
- Filter only events for group 136.1.122.2

Final Configuration

ASA1:

```
1) Configuration
```

```
    Administration
    Monitoring
```

- 4) Save changes to Config file
- 5) Help Information
 6) Exit

VPN3K: Main -> 1

```
1) Interface Configuration
```

2) System Management

```
3) User Management
```

Copyright © 2007 Internetwork Expert

```
4) Policy Management
5) Tunneling and Security
6) Back
VPN3K: Config -> 2
1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back
VPN3K: System -> 5
1) General
2) FTP Backup
3) Classes
4) Trap Destinations
5) Syslog Servers
6) SMTP Servers
7) E-mail Recipients
8) Back
VPN3K: Event -> 3
                                        The Active Event Classes
_____
1. MIB2TRAP
                                             _____
1) Add an Event Class
2) Modify an Event Class
3) Delete an Event Class
4) Back
VPN3K: Event Class -> 1
                                            The Event Classes
11. MIB2TRAP2. PSOS3. SYSTEM4. QUEUE5. EVENT6. EVENTDBG7. SMTP8. RM9. DM10. IP11. TCP12. PPP13. L2TP14. HTTP15. AUTH16. AUTHDBG17. AUTHDECODE18. PPTP19. PPTPDBG20. PPTPDECODE21. GRE22. GREDBG23. GREDECODE24. PSH25. CONFIG26. L2TPDBG27. L2TPDECODE28. TELNET29. TELNETDBG30. TELNETDECODE31. FTPD32. DNS33. DNSDBG34. IPSEC35. IPSECDBG36. IPSECDECODE37. IKE38. IKEDBG39. IKEDECODE40. HARDWAREMON41. IPDBG42. CAPI43. IPDECODE44. PPPDBG45. PPPDECODE46. DNSDECODE47. DHCP48. DHCPDBG49. DHCPDECODE50. FILTER51. FILTERDBG52. EVENTMIB53. REBOOT54. SNMP55. OSPF56. VRRP57. SSL58. CERT59. GENERAL60. TIME64. EXPANSIONCARD67. FSM68. SSH69. LBSSF71. PPPOE72. PPPOEDBG73. PPPOEDECODE74. NETBIOS75. CLIENT76. XML77. FW78. FWDBG79. FWDECODE82. BMGT83. BMGTDBG84. FIPS85. FIPSDIAG86. WEBVPN87. EMAILPROXY88. CIFS
      _____
```

```
Copyright © 2007 Internetwork Expert www.InternetworkExpert.com
```

| 89. CIFSDBG | 90. STC 91. CSTP 92. NAC 'q' to Quit, '<SPACE>' to Continue ->93. EAP94. EAPOUDP > Enter the Event Class to Add VPN3K: Event Class -> 34 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap VPN3K: Event Class -> [0] The Active Event Classes _____ _____ 1. MIB2TRAP 34. IPSEC _____ 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back VPN3K: Event Class -> 1 The Event Classes 1. MIB2TRAP2. PSOS3. SYSTEM4. QUEUE5. EVENT6. EVENTDBG7. SMTP8. RM9. DM10. IP11. TCP12. PPP13. L2TP14. HTTP15. AUTH16. AUTHDBG17. AUTHDECODE18. PPTP19. PPTPDBG20. PPTPDECODE21. GRE22. GREDBG23. GREDECODE24. PSH25. CONFIG26. L2TPDBG27. L2TPDECODE28. TELNET29. TELNETDBG30. TELNETDECODE31. FTPD32. DNS33. DNSDBG34. IPSEC35. IPSECDBC36. IPSECDECODE37. IKE38. IKEDBG39. IKEDECODE40. HARDWAREMON41. IPDBG42. CAPI43. IPDECODE44. PPPDBG45. PPPDECODE46. DNSDECODE47. DHCP48. DHCPDBG49. DHCPDECODE50. FILTER51. FILTERDBG52. EVENTMIB53. REBOOT54. SNMP55. OSPF56. VRRP57. SSL58. CERT59. GENERAL60. TIME _____

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

- 427 -

68. SSH 69. LBSSF 64. EXPANSIONCARD67. FSM68. SSH69. LESSF71. PPPOE72. PPPOEDEG73. PPPOEDECODE74. NETBIOS75. CLIENT76. XML77. FW78. FWDBG79. FWDECODE82. BMGT83. BMGTDBG84. FIPS85. FIPSDIAG86. WEBVPN87. EMAILPROXY88. CIFS89. CIFSDBG90. STC91. CSTP92. NAC 64. EXPANSIONCARD 67. FSM 'q' to Quit, '<SPACE>' to Continue -> 93. EAP 94. EAPOUDP _____ _____ > Enter the Event Class to Add VPN3K: Event Class -> 35 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] 1 > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap VPN3K: Event Class -> [0] The Active Event Classes _____ 1. MIB2TRAP | 34. IPSEC 35. IPSECDBG _____ 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back VPN3K: Event Class -> 1 The Event Classes _____ 1. MIB2TRAP2. PSOS3. SYSTEM4. QUEUE5. EVENT6. EVENTDBG7. SMTP8. RM9. DM10. IP11. TCP12. PPP13. L2TP14. HTTP15. AUTH16. AUTHDBG17. AUTHDECODE18. PPTP19. PPTPDBG20. PPTPDECODE21. GRE22. GREDBG23. GREDECODE24. PSH25. CONFIG26. L2TPDBG27. L2TPDECODE28. TELNET29. TELNETDBG30. TELNETDECODE31. FTPD32. DNS33. DNSDBG34. IPSEC35. IPSECDBG36. IPSECDECODE

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

- 428 -
37. IKE38. IKEDBG39. IKEDECODE40. HARDWAREMON41. IPDBG42. CAPI43. IPDECODE44. PPPDBG45. PPPDECODE46. DNSDECODE47. DHCP48. DHCPDBG49. DHCPDECODE50. FILTER51. FILTERDBG52. EVENTMIB53. REBOOT54. SNMP55. OSPF56. VRP57. SSL58. CERT59. GENERAL60. TIME64. EXPANSIONCARD67. FSM68. SSH69. LBSSF71. PPPOE72. PPPOEDBG73. PPPOEDECODE74. NETBIOS75. CLIENT76. XML77. FW78. FWDBG79. FWDECODE82. BMGT83. BMGTDBG84. FIPS85. FIPSDIAG86. WEBVPN87. EMAILPROXY88. CIFS89. CIFSDBG90. STC91. CSTP92. NAC 'q' to Quit, '<SPACE>' to Continue -> | 93. EAP | 94. EAPOUDP | _____ _____ > Enter the Event Class to Add VPN3K: Event Class -> 36 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] 1 > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap VPN3K: Event Class -> [0] The Active Event Classes _____ | 34. IPSEC 1. MIB2TRAP 35. IPSECDBG 36. IPSECDECODE 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back VPN3K: Event Class -> 1 The Event Classes _____

 1. MIB2TRAP
 2. PSOS
 3. SYSTEM
 4. QUEUE

 5. EVENT
 6. EVENTDBG
 7. SMTP
 8. RM

 9. DM
 10. IP
 11. TCP
 12. PPP

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

13. L2TP14. HTTP15. AUTH16. AUTHDBG17. AUTHDECODE18. PPTP19. PPTPDBG20. PPTPDECODE21. GRE22. GREDBG23. GREDECODE24. PSH25. CONFIG26. L2TPDBG27. L2TPDECODE28. TELNET29. TELNETDBG30. TELNETDECODE31. FTPD32. DNS33. DNSDBG34. IPSEC35. IPSECDBG36. IPSECDECODE37. IKE38. IKEDBG39. IKEDECODE40. HARDWAREMON41. IPDBG42. CAPI43. IPDECODE44. PPPDBG45. PPPDECODE46. DNSDECODE47. DHCP48. DHCPDBG49. DHCPDECODE50. FILTER51. FILTERDBG52. EVENTMIB53. REBOOT54. SNMP55. OSPF56. VRRP57. SSL58. CERT59. GENERAL60. TIME64. EXPANSIONCARD67. FSM68. SSH69. LBSSF71. PPPOE72. PPPOEDBG73. PPPOEDECODE74. NETBIOS75. CLIENT76. XML77. FW78. FWDBG79. FWDECODE82. BMGT83. BMGTDBG84. FIPS85. FIPSDIAG86. WEBVPN87. EMAILPROXY88. CIFS89. CIFSDBG90. STC91. CSTP92. NAC'q' to Quit, '<SPACE>' to Continue ->14. DEDECODE14. DEDECODE 'q' to Quit, '<SPACE>' to Continue -> 93. EAP 94. EAPOUDP _____ _____ _____ > Enter the Event Class to Add VPN3K: Event Class -> 38 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] 1 > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap VPN3K: Event Class -> [0] The Active Event Classes _____ 1. MIB2TRAP 34. IPSEC 36. IPSECDECODE | 35. IPSECDBG 38. IKEDBG 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

VPN3K: Event Class -> 1 The Event Classes The Event Classes1. MIB2TRAP2. PSOS3. SYSTEM4. QUEUE5. EVENT6. EVENTDBG7. SMTP8. RM9. DM10. IP11. TCP12. PPP13. L2TP14. HTTP15. AUTH16. AUTHDBG17. AUTHDECODE18. PPTP19. PPTPDBG20. PPTPDECODE21. GRE22. GREDBG23. GREDECODE24. PSH25. CONFIG26. L2TPDBG27. L2TPDECODE28. TELNET29. TELNETDBG30. TELNETDECODE31. FTPD32. DNS33. DNSDBG34. IPSEC35. IPSECDBG36. IPSECDECODE37. IKE38. IKEDBG39. IKEDECODE40. HARDWAREMON41. IPDBG42. CAPI43. IPDECODE44. PPPDBG45. PPPDECODE46. DNSDECODE47. DHCP48. DHCPDBG49. DHCPDECODE50. FILTER51. FILTERDBG52. EVENTMIB53. REBOOT54. SNMP55. OSFF56. VRRP57. SSL58. CERT59. GENERAL60. TIME64. EXPANSIONCARD67. FSM68. SSH69. LBSSF71. PPPOE72. PPPOEDBG73. PPPOEDECODE74. NETBIOS75. CLIENT76. XML77. FW78. FWDBG79. FWDECODE82. BMGT83. BMGTDBG84. FIPS85. FIPSDIAG86. WEBVPN87. EMAILPROXY88. CLFS89. CIFSDBG90. STC91. CSTP92. NAC'q' to Quit, '<SPACE>' to Continue ->92. FAD94. FADOUDD -----_____ 'q' to Quit, '<SPACE>' to Continue -> 93. EAP 94. EAPOUDP _____ > Enter the Event Class to Add VPN3K: Event Class -> 39 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap VPN3K: Event Class -> [0] The Active Event Classes _____ | 34. IPSEC | 1. MIB2TRAP 35. IPSECDBG | 36. IPSECDECODE 38. IKEDBG | 39. IKEDECODE

Copyright © 2007 Internetwork Expert www.InternetworkExpert.com

- 431 -

_____ 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back VPN3K: Event Class -> 1 The Event Classes

 The Event Classes

 1. MIB2TRAP
 2. PSOS
 3. SYSTEM
 4. QUEUE

 5. EVENT
 6. EVENTDBG
 7. SMTP
 8. RM

 9. DM
 10. IP
 11. TCP
 12. PPP

 13. L2TP
 14. HTTP
 15. AUTH
 16. AUTHDBG

 17. AUTHDECODE
 18. PPTP
 19. PPTPDBG
 20. PPTPDECODE

 21. GRE
 22. GREDBG
 23. GREDECODE
 24. PSH

 25. CONFIG
 26. L2TPDBG
 27. L2TPDECODE
 28. TELNET

 29. TELNETDBG
 30. TELNETDECODE
 31. FTPD
 32. DNS

 33. DNSDBG
 34. IPSEC
 35. IPSECDBG
 36. IPSECDCODE

 37. IKE
 38. IKEDBG
 39. IKEDECODE
 40. HARDWAREMON

 41. IPDBG
 42. CAPI
 43. IPDECODE
 44. PPPDBG

 45. PPPDECODE
 46. DNSDECODE
 47. DHCP
 48. DHCPDBG

 49. DHCPDECODE
 50. FILTER
 51. FILTERDBG
 52. EVENTMIB

 53. REBOOT
 54. SNMP
 55. OSFF
 56. VRRP

 57. SSL
 58. CERT
 59. GENERAL
 60. TIME

 64. EXPANSIONCARD
 67. FSM
 68. SSH
 69. LBSSF

 71. P _____ -----_____ 'q' to Quit, '<SPACE>' to Continue -> 93. EAP 94. EAPOUDP _____ > Enter the Event Class to Add VPN3K: Event Class -> 37 1) Enable this Class 2) Disable this Class VPN3K: Event Class -> [1] > Events to Log VPN3K: Event Class -> [5] 9 > Events to Console VPN3K: Event Class -> [3] > Events to Syslog VPN3K: Event Class -> [0] > Events to E-mail VPN3K: Event Class -> [0] > Events to SNMP Trap

VPN3K: Event Class -> [0] The Active Event Classes -----34. IPSEC 1. MIB2TRAP 35. IPSECDBG 36. IPSECDECODE 37. IKE 38. IKEDBG 39. IKEDECODE _____ 1) Add an Event Class 2) Modify an Event Class 3) Delete an Event Class 4) Back VPN3K: Event Class -> Configure events monitor: 1) Configuration 2) Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit VPN3K: Main -> 3 1) Routing Table 2) Event Log 3) System Status 4) Sessions 5) General Statistics 6) Dynamic Filters 7) Back VPN3K: Monitor -> 2 1) Configure Log viewing parameters 2) View Event Log 3) Save Log 4) Clear Log 5) Configure WebVPN Logging 6) Back VPN3K: Log -> 4 1) Configure Log viewing parameters 2) View Event Log 3) Save Log 4) Clear Log 5) Configure WebVPN Logging 6) Back VPN3K: Log -> 1 > Events per page VPN3K: Log -> [5] 100 The Event Classes _____ 3. SYSTEM 4. QUEUE 1. MIB2TRAP 2. PSOS

Copyright © 2007 Internetwork Expert

7. SMTP

 5. EVENT
 6. EVENTDBG
 7. SMTP
 8. RM

 9. DM
 10. IP
 11. TCP
 12. PPP

 13. L2TP
 14. HTTP
 15. AUTH
 16. AUTHDBG

 17. AUTHDECODE
 18. PPTP
 19. PPTPDBG
 20. PPTPDECODE

 21. GRE
 22. GREDBG
 23. GREDECODE
 24. PSH

 25. CONFIG
 26. L2TPDBG
 27. L2TPDECODE
 28. TELNET

 29. TELNETDBG
 30. TELNETDECODE
 31. FTPD
 32. DNS

 33. DNSDBG
 34. IPSEC
 35. IPSECDBG
 36. IPSECDECODE

 37. IKE
 38. IKEDBG
 39. IKEDECODE
 40. HARDWAREMON

 41. IPDBG
 42. CAPI
 43. IPDECODE
 44. PPPDBG

 45. PPPDECODE
 46. DNSDECODE
 47. DHCP
 48. DHCPDBG

 45. REBOOT
 54. SNMP
 55. OSPF
 56. VRRP

 57. SSL
 58. CERT
 59. GENERAL
 60. TIME

 64. EXPANSIONCARD
 67. FSM
 68. SSH
 69. LBSSF

 71. PPPOE
 72. PPPOEDBG
 73. PPPOEDECODE
 74. NETBIOS

 75. CLIENT
 76. XML
 77. FW
 78. FWDBG

 79. FWDECODE
 82. BMGT
 83. BMGTD 6. EVENTDBG 8. RM 5. EVENT q' to Quit, '<SPACE>' to Continue -> 93. EAP 94. EAPOUDP For multiple classes, separate numbers with spaces. > Event classes to view (0 for all Classes) VPN3K: Log -> 0 The following is a description of the Event Severity Levels Severities1 - 3 are Warning :1 - Fault2 - Warning13 - Warning2Severities4 - 6 are Info:4 - Info15 - Info26 - Info3Severities7 - 9 are Debug:7 - Debug18 - Debug29 - Debug3 Severities 10, 11 are Decodes: 10 - Hdecode 11 - Ldecode Severities 12, 13 are Dumps : 12 - HdrDump 13 - PktDump For multiple severities, separate numbers with spaces. > Event severities to view (0 for all Severities) VPN3K: Log -> 0 > Client Address to view (0.0.0.0 for all addresses) VPN3K: Log -> [0.0.0.0] Current User Groups _____ 1. 136.1.122.2 > Group to view (-1 for All Groups, 0 for Base Group) VPN3K: Log -> 1 1) Configure Log viewing parameters 2) View Event Log 3) Save Log 4) Clear Log 5) Configure WebVPN Logging 6) Back

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 434 -

```
VPN3K: Log -> 2
    No more Events
1) First Page
2) Previous Page
3) Next Page
4) Last Page
5) Back
VPN3K: Log ->
```

Verification

```
R2#ping 150.1.1.1 so lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/8/8 ms
1) Configure Log viewing parameters
2) View Event Log
3) Save Log
4) Clear Log
5) Configure WebVPN Logging
6) Back
VPN3K: Log -> 2
IKE Main Mode Exchange begins:
191 01/17/2007 01:14:45.150 SEV=9 IKEDBG/1 RPT=15 136.1.122.2
Group [136.1.122.2]
Processing ID
192 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=46 136.1.122.2
Group [136.1.122.2]
processing hash
193 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=47 136.1.122.2
Group [136.1.122.2]
computing hash
194 01/17/2007 01:14:45.150 SEV=9 IKEDBG/0 RPT=48 136.1.122.2
Group [136.1.122.2]
Processing Notify payload
Looking for a match by peer's IP (it's Main Mode):
201 01/17/2007 01:14:45.150 SEV=9 IKEDBG/23 RPT=2 136.1.122.2
Group [136.1.122.2]
Starting group lookup for peer 136.1.122.2
202 01/17/2007 01:14:45.260 SEV=7 IKEDBG/80 RPT=3 136.1.122.2
Group [136.1.122.2]
Found Phase 1 Group (136.1.122.2)
Group found, extracting authentication attributes:
```

```
Copyright © 2007 Internetwork Expert
```

203 01/17/2007 01:14:45.260 SEV=7 IKEDBG/14 RPT=3 136.1.122.2 Group [136.1.122.2] Authentication configured for Internal 204 01/17/2007 01:14:45.260 SEV=9 IKEDBG/19 RPT=2 136.1.122.2 Group [136.1.122.2] IKEGetUserAttributes: IP Compression = reset 205 01/17/2007 01:14:45.260 SEV=9 IKEDBG/78 RPT=3 136.1.122.2 Group [136.1.122.2] IKEGetUserAttributes: Browser Proxy Setting = 1 206 01/17/2007 01:14:45.260 SEV=9 IKEDBG/78 RPT=4 136.1.122.2 Group [136.1.122.2] IKEGetUserAttributes: Browser Proxy Bypass Local = 0 Respond with IKE message, presenting our ID and authenticationg: 207 01/17/2007 01:14:45.260 SEV=9 IKEDBG/1 RPT=16 136.1.122.2 Group [136.1.122.2] constructing ID 208 01/17/2007 01:14:45.260 SEV=9 IKEDBG/0 RPT=49 Group [136.1.122.2] construct hash payload 209 01/17/2007 01:14:45.260 SEV=9 IKEDBG/0 RPT=50 136.1.122.2 Group [136.1.122.2] computing hash 211 01/17/2007 01:14:45.260 SEV=9 IKEDBG/46 RPT=10 136.1.122.2 Group [136.1.122.2] constructing dpd vid payload 215 01/17/2007 01:14:45.260 SEV=4 IKE/119 RPT=4 136.1.122.2 Group [136.1.122.2] PHASE 1 COMPLETED Phase 1 has been completed, after authentication and attributes negotiation 217 01/17/2007 01:14:45.260 SEV=7 IKEDBG/82 RPT=3 136.1.122.2 Group [136.1.122.2] Starting phase 1 rekey timer: 82080000 (ms) 218 01/17/2007 01:14:45.260 SEV=4 AUTH/22 RPT=4 136.1.122.2 User [136.1.122.2] Group [136.1.122.2] connected, Session Type: IPSec/LAN-to-LAN Phase2 begins: 230 01/17/2007 01:14:45.280 SEV=9 IKEDBG/0 RPT=52 136.1.122.2 Group [136.1.122.2] processing hash 231 01/17/2007 01:14:45.280 SEV=9 IKEDBG/0 RPT=53 136.1.122.2 Group [136.1.122.2] processing SA payload 245 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=17 136.1.122.2 Group [136.1.122.2] processing nonce payload

Copyright © 2007 Internetwork Expert

Received proxy id:

246 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=18 136.1.122.2 Group [136.1.122.2] Processing ID

247 01/17/2007 01:14:45.280 SEV=5 IKE/35 RPT=4 136.1.122.2 Group [136.1.122.2] Received remote IP Proxy Subnet data in ID Payload: Address 150.1.2.0, Mask 255.255.255.0, Protocol 0, Port 0

250 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=19 136.1.122.2 Group [136.1.122.2] Processing ID

251 01/17/2007 01:14:45.280 SEV=5 IKE/34 RPT=4 136.1.122.2 Group [136.1.122.2] Received local IP Proxy Subnet data in ID Payload: Address 150.1.1.0, Mask 255.255.255.0, Protocol 0, Port 0

254 01/17/2007 01:14:45.280 SEV=8 IKEDBG/83 RPT=3 136.1.122.2 Group [136.1.122.2] QM IsRekeyed old sa not found by addr

Applying SA attributes:

255 01/17/2007 01:14:45.280 SEV=5 IKE/66 RPT=4 136.1.122.2 Group [136.1.122.2] IKE Remote Peer configured for SA: L2L:VPN_TO_R2

256 01/17/2007 01:14:45.280 SEV=9 IKEDBG/1 RPT=20 136.1.122.2 Group [136.1.122.2] processing IPSEC SA

Phase2 Proposal match found:

258 01/17/2007 01:14:45.280 SEV=7 IKEDBG/27 RPT=3 136.1.122.2 Group [136.1.122.2] IPSec SA Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 9 Proposal (L2L:VPN_TO_R2)

Generating SPI:

261 01/17/2007 01:14:45.280 SEV=7 IKEDBG/85 RPT=3 136.1.122.2 Group [136.1.122.2] IKE: requesting SPI! (Protocol=ESP)

268 01/17/2007 01:14:45.290 SEV=8 IKEDBG/6 RPT=3 136.1.122.2 Group [136.1.122.2] IKE got SPI from key engine: SPI = 0x55b6504a

269 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=54 136.1.122.2 Group [136.1.122.2] oakley constucting quick mode

270 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=55 136.1.122.2 Group [136.1.122.2] constructing blank hash

271 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=56 136.1.122.2 Group [136.1.122.2] constructing ISA_SA for ipsec

Copyright © 2007 Internetwork Expert

272 01/17/2007 01:14:45.290 SEV=9 IKEDBG/1 RPT=21 136.1.122.2 Group [136.1.122.2] constructing ipsec nonce payload 273 01/17/2007 01:14:45.290 SEV=9 IKEDBG/1 RPT=22 136.1.122.2 Group [136.1.122.2] constructing proxy ID Transmitting our proxies: 274 01/17/2007 01:14:45.290 SEV=7 IKEDBG/91 RPT=3 136.1.122.2 Group [136.1.122.2] Transmitting Proxy Id: Remote subnet: 150.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0 Local subnet: 150.1.1.0 mask 255.255.255.0 Protocol 0 Port 0 278 01/17/2007 01:14:45.290 SEV=9 IKEDBG/0 RPT=57 136.1.122.2 Group [136.1.122.2] constructing qm hash 290 01/17/2007 01:14:45.310 SEV=9 IKEDBG/0 RPT=58 136.1.122.2 Group [136.1.122.2] processing hash 291 01/17/2007 01:14:45.310 SEV=9 IKEDBG/0 RPT=59 136.1.122.2 Group [136.1.122.2] loading all IPSEC SAs Generating QM keying material: 292 01/17/2007 01:14:45.310 SEV=9 IKEDBG/1 RPT=23 136.1.122.2 Group [136.1.122.2] Generating Quick Mode Key! 293 01/17/2007 01:14:45.320 SEV=9 IKEDBG/1 RPT=24 136.1.122.2 Group [136.1.122.2] Generating Quick Mode Key! 294 01/17/2007 01:14:45.320 SEV=7 IKEDBG/93 RPT=3 136.1.122.2 Group [136.1.122.2] Loading subnet: Dst: 150.1.1.0 mask: 255.255.255.0 Src: 150.1.2.0 mask: 255.255.255.0 SAs have been negotiated: 297 01/17/2007 01:14:45.320 SEV=4 IKE/49 RPT=4 136.1.122.2 Group [136.1.122.2] Security negotiation complete for LAN-to-LAN Group (136.1.122.2) Responder, Inbound SPI = 0x55b6504a, Outbound SPI = 0xbf527809 322 01/17/2007 01:14:45.330 SEV=8 IKEDBG/86 RPT=3 136.1.122.2 Group [136.1.122.2] pitcher: rcv KEY_UPDATE, spi 0x55b6504a 323 01/17/2007 01:14:45.330 SEV=4 IKE/120 RPT=4 136.1.122.2 Group [136.1.122.2] PHASE 2 COMPLETED (msgid=022fd181) 326 01/17/2007 01:14:46.270 SEV=8 IKEDBG/87 RPT=3 136.1.122.2 Group [136.1.122.2] pitcher: recv KEY_SA_ACTIVE spi 0x55b6504a

Copyright © 2007 Internetwork Expert

1) First Page

- 2) Previous Page
- 3) Next Page
- 4) Last Page
- 5) Back

VPN3K: Log ->

Further Reading

VPN3k: System Configuration/Events

IPsec and Fragmentation Issues

Objective: Configure IOS router for packet fragmentation prior to encryption.



Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario <u>"IOS and IOS with PSK Across the PIX/ASA".</u>
- IPsec termination router permormace may be severely affected, if encrypted packets are fragmented along the way.
- This is due to the fact the fragments re-assembly takes place at the process level, severely degrading overall performance.
- To avoid this issue, a near-MTU sized packet may be pre-fragmented by sending router before encryption.
- Configure R1 for IPsec pre-fragmentation, and verify how it changes encryption behavior.
- Configure access-list on R2 to match fragmented ESP packets, and see if they apper after the pre-fragmentation is enabled.

Final Configuration

```
R2:
access-list 100 permit esp any any fragments
access-list 100 permit ip any any
!
interface E 0/0
ip access-group 100 in
R1:
interface E0/0
crypto ipsec fragmentation before-encryption
```

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 440 -

Verification

```
R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments
    20 permit ip any any (6 matches)
R1#sh running-config interface ethernet 0/0
Building configuration ...
Current configuration : 141 bytes
interface Ethernet0/0
ip address 136.1.121.1 255.255.255.0
half-duplex
crypto map VPN
 crypto ipsec fragmentation after-encryption
end
R1#ping 150.1.2.2 source loopback 0 size 1500 repeat 10
Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
1111111111
Success rate is 100 percent (10/10), round-trip min/avg/max = 64/65/68 ms
R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments (20 matches)
    20 permit ip any any (44 matches)
R1#sh running-config interface ethernet 0/0
Building configuration...
Current configuration : 142 bytes
interface Ethernet0/0
ip address 136.1.121.1 255.255.255.0
half-duplex
 crypto map VPN
 crypto ipsec fragmentation before-encryption
end
R2#clear access-list counters
R1#ping 150.1.2.2 source loopback 0 size 1500 repeat 10
Type escape sequence to abort.
Sending 10, 1500-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
1111111111
Success rate is 100 percent (10/10), round-trip min/avg/max = 60/61/64 ms
R2#show ip access-lists 100
Extended IP access list 100
    10 permit esp any any fragments
    20 permit ip any any (40 matches)
```

Further Reading

Pre-Fragmentation for IPSec VPNs



ISAKMP Pre-Shared Keys via AAA

Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario <u>"IOS and IOS with PSK Across the PIX/ASA".</u>
- IOS router could retreive ISAKMP attributes from RADIUS server. To make this possible, it sends remote peer ID as login name, along with password "cisco" (hardcoded value). The attributes returned in reply are used to extract pre-shared key for IKE, and to deduce various other attributes.
- Configure the ASA1 to permit inbound RADIUS traffic.
 - Add an entry to access-list OUTSIDE_IN to permit UDP traffic to host 10.0.0.100 port 1645
- Configure ISAKMP peer 136.1.122.2 policy on R1:
 - Set aggressive mode with password "CISCO".
 - Use self-id FQDN "R1".
- Enable AAA on R2 and safeguard console authentication.
- Configure authorization list ISAKMP to use RADIUS server.
- Configure RADIUS server 10.0.0.100 with key CISCO.
- Delete pre-shared key "CISCO" for address 136.1.121.1
- Configure crypto map VPN for ISAKMP authorization with list ISAKMP.
- Configure ACS:
 - Add new RADIUS network client corresponding to R2 with IP 136.1.122.2
 - Create new group ISAKMP.

- Disable IP address assignment.
- Add Cisco AV-Pair "ipsec:key-exchange=IKE".
- Set IETF RADIUS attribute "Service" to value "Outbound".
- Set IETF RADIUS attribute "Tunnel-Type" to value "IP ESP".
- Set IETF RADIUS attribute "Tunnel-Password" to value "CISCO". This is the actual pre-shared key.
- Add new user with name "R1" and password "cisco"
 - Assign this user to group "ISAKMP".

Final Configuration

ASA1:

```
ADAL:
access-list OUTSIDE_IN permit udp any any eq 1645

R2:
aaa-new model
aaa authentication login CONSOLE none
aaa authorization network ISAKMP group radius
!
line console 0
login authentication CONSOLE
!
radius-server host 10.0.0.100 key CISCO
no crypto isakmp key CISCO address 136.1.121.1
crypto map VPN isakmp authorization list ISAKMP

R1:
crypto isakmp peer address 136.1.122.2
set aggressive-mode password CISCO
set aggressive-mode client-endpoint fqdn R1
```

ACS:

Add new AAA client for to R2:

🖉 CiscoSecure ACS	5 - Microsoft Internet Exp	lorer		
<u>File E</u> dit <u>V</u> iew	F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	🖙 Back 🔹 🖘 👻 🚱	Address 🛃 http://127.0.0.1:4413/	
CISCO SYSTEMS	Network Co	onfiguration		×
ավիտավիտ				
Setup				
Group Setup]	Add /	AAA Client	
Shared Profile Components	AAA Client Ho	stname R2		
Network Configuration		136.1.12	2.2	
System Configuration	AAA Client IP	Address	~	
Configuration	Кеу	CISCO		
Administration Control	Authenticate	Jsing RADIUS (Cisco IOS/PIX 6.0)	
Databases	🗌 🗖 Single Cor	inect TACACS+ AAA Clier	nt (Record stop in accounting c	n failure).
Doon Posture	🗌 🗖 Log Updat	e/Watchdog Packets from	m this AAA Client	
Network Acces	Log RADIU	S Tunneling Packets from	m this AAA Client	
Profiles	Replace R	ADIUS Port info with User	rname from this AAA Client	
Reports and Activity				
Online Documentation]	Submit Su	ubmit + Apply Cancel	-1 ⁴
, Ø Applet startStop sl	tarted			Marternet

Create	new	aroup	named	"ISAKMP":
		g-c-p		

🖉 Cie	scoSed	ure AC	5 - Microso	oft Inter	net Exp	lorer									_ 🗆 ×
Eile	Edit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	🗘 Back	•=> •	8	Address	🔊 http:,	//127.0.0.	1:4413)	l –		-
C	ISCO S	YSTEMS	G	roup	Setu	D									×
	ովիստ	ա				F									F
	1.0		Sele	CL											
	Use Seti	r IP													
	Gro	ip ip				(Group :	2: ISA	КМР			•			-
(#b)	Shar	ed Profile				Users ir	n Group	Ed	dit Settings	5	Renar	ne Gr	oup		
	-I Netv	ork													
	Conf	iguratio	n												
	Syst Conf	em iguratio	n												
	Inte Conf	rface iguratio	•					2	Back to Help						
_ 90	Adm	inistratio	on												
	Cont	rol													
jĝ	Exte	rnal Use bases	r												
000	Post Vali	ure dation													
	Netw	ork Acce	ss												
	L Rep	es orte ord													
	Acti	vity													
g) Onli Docu	ne mentatio	n												ŀ
🙆 Ap	oplet st	artStop :	started											🔮 Internet	

CiscoSecure ACS	- Microsoft Internet Explorer	
<u>Eile E</u> dit ⊻iew	Favorites Iools Help (⇒ Back + ⇒ - 🔇 👔 Address 🙋 http://127.0.0.1:4413/	•
CISCO SYSTEMS	Group Setup	×
	Jump To Access Restrictions	
User Setup	Access Restrictions IP Address Assignment	<u> </u>
Group	Grou RADIUS (Cisco IOS/PIX 6.0) RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)	
	RADIUS (IETF)	
Components	KADIOS (ASCENU)	
Network Configuration	Access Restrictions	
System Configuration		
Interface Configuration	Group Disabled	3
90 L Administration	☐ Members of this group will be denied access to the network.	
Control	Default Time-of-Day Access Settings	2
Databases		
nana Posture		
Canada Validation	Tue	
Network Acces	Wed	
I Reports and	Thu	
Activity	Fri Crah	-
Online Documentation	Submit Submit + Restart Cancel	
I	started	Internet

Configure IP address assignment (disable it actually) and Cisco AV-Pair:

CiscoSecure ACS -	Microsoft Internet Explorer	_ 🗆 X
File Edit <u>V</u> iew F	avorites Iools Help 🗘 Back → → → 🔇 😰 Address 🖉 http://127.0.0.1:4413/	-
CISCO SYSTEMS	Group Setup	×
	Jump To IP Address Assignment	
User Setup	IP Assignment	?
Group Setup	No IP address assignment	
Shared Profile Components	Assigned by dialup client Assigned from AAA Client pool	
Network Configuration		
System Configuration		
Interface Configuration	Cisco IOS/PIX 6.x RADIUS Attributes	
Administration	₽ [009\001] cisco-av-pair	
Databases	ipsec:key-exchange=ike	
Posture Validation		
Network Access Profiles	□ □ [009\101] cisco-h323-credit-amount	
Reports and Activity		Ţ
Documentation	Submit Submit + Restart Cancel	
Applet dialup_filter s	tarted	

CiscoSecure ACS - Microsoft Internet E	xplorer .	- 🗆 ×
<u>File E</u> dit <u>View</u> F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	← Back ▼ ⇒ → ③ 🕄 Address 🖗 http://127.0.0.1:4413/	-
CISCO SYSTEMS Group Set	מוו	×
		_
-	Jump To Access Restrictions	
User Setup	Access Restrictions IP Address Assignment	-
	Grou RADIUS (Cisco IOS/PIX 6.0)	
Setup	RADIUS (CISCU VPN SUDD/ASA/PIA 7.84) RADIUS (IETF)	
Shared Profile Components		
Network		
	Access Restrictions	
Configuration		
Interface Configuration	Group Disabled	
Members	of this group will be denied access to the network.	
Control	Dofault Timo-of-Day Accors Sottings	
External User Databases		
Dance Posture	00;00 06;00 12;00 18;00 24;00	
Validation	Mon	
Network Access Profiles	Wed	
Reports and	Thu	
Activity	Pn	•
Documentation	Submit Submit + Restart Cancel	
I Applet dialup_filter started	📘 🛛 🖉 Internet	

ila	Edit	View	Favorite	- Tools	Help	(Park			Addroce	A	27.0.0.1.4412	ü.		1 367
	Eair	Mew	ravonce:		Ūeih		• => +		Agaress	• nttp://1	27.0.0.1:4413	ų.		
CI	sco S	YSTEMS	Ģ	Group	Setu	р								
	միրու		•			Jump	To RAL	DIUS (IE	TF)			•		
ł	Use Setu	r Jp											<u>9</u>	1
L	Grou	up Jp					IE	IF RADI	US Attri	outes				
÷.	Shari Comp	ed Profile conents		0) 🗹	06] Ser	vice-Typ	е							
	Netv Conf	vork 'iguratio		🗖 (o	07] Fra	med-Prot	ocol							
ì	Syst Conf	em iguratio	•	E ro			te tus e els				Xylogic:	s IPX/SLIP	•	
3	Inte Conf	rface Tiguratic	•	ιιυ	nal Fig	meu-IP-N	ietmask				ſ	0.0.0.0		
10	Adm Cont	inistratio rol	n	🗆 (o	10] Fra	med-Rou	ting						(Sara)	
à	Exte	ernal Use abases		[0	11] Filti	er-Id					INone			
	Post Vali	ture dation												
R	Netw Profi	ork Acce les	s s											
2	Rep Acti	orts and vity		🗆 (o	12] Fra	med-MTU	J (6465	535)					Ŧ	
p	Onli Docu	ne imentatio					Submit	Sul	omit + Re	start	Cancel			

<u>-</u> ile	Edit	⊻iew	F <u>a</u> vorite	s <u>T</u> ools	Help	🗘 Back	•=>	- 🗵	¢	A <u>d</u> dress	🖉 http://	(127.0.0.1:44)	13/		-
C	ISCO S	YSTEMS	(Group	Setu	р									×
	սՈրու	ավիրու	• ::			Jumj	p To 🖡	RADIU	S (IE	(F)			•		
	User Setu	r /p			221110	nea obb	io i uik	20110		Г					^
	Grou Setu	ib D		🗖 (o	62] Por	t-Limit									
465)	Shari Comp	ed Profile conents		D (0	63] Log	in-LAT-P	ort						0		
2 7	Netw Conf	vork iguratio em	n	o] 되	54] Tur	nel-Type	e			Ľ					
	j Conf Inter Conf	iguratio rface 'iguratio	n						Tag	1	Value	IP ESP		•	
2	Adm Cont	inistratio rol	n	🗖 (o	65] Tur	inel-Medi	um-Ty	/pe	iagi] value j				
6	E×te Data	rnal Use bases	-							Tag	1	Value		• •	
88	Post Vali	ure dation		I [0	69] <mark>Tur</mark>	inel-Pass	word			ray	-	∎ value [
j	Netw Profil	ork Acce les	55						Та	ag 🚺	🔽 Valu	ie CISCO			
0	Rep Acti	orts and vity		01 🗖	81] Tur	nel-Priva	ate-Gro	oup-II	Ta D	ag 2	💌 Valu	ie 🗌		1	-
1) Onlin Docu	ne imentatio	n 🗌				Submi	t	Sub	mit + R	estart	Cancel			

CiscoSecure ACS - M	licrosoft Internet Explo	prer			
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	orites <u>T</u> ools <u>H</u> elp	🖙 Back 🔹 🖘 👻 😰	Address 🛃 http://127.0.0).1:4413/	▼
CISCO SYSTEMS	User Setup				×
IlliuIlliu	Select				F
User					
Elg Setup					
Setup		User: R1			
Components		Find	Add/Edit		
Network Configuration		List users heain	ning with letter/numbe	ir:	
System Configuration					
		012	3456789		
		Lis	st all users		
Control		Domovs			
Databases		Kemove	Dynamic Osers		
Construction Validation	18				
Network Access Profiles		3	Back to Help		
Reports and Activity					
Online Documentation					
Applet appPing started					🔮 Internet

Add new user with name "R1" and password "cisco":

e <u>E</u>	dit	⊻iew	F <u>a</u> vori	tes]	ools	Help	(= Back	、 → ⇒	- 🗵) 🕼	A <u>d</u> dress	🖉 http:,	/127.0.0.	1:4413/			-
Cisc	o Sv	TEMS	ł	Use	er S	etup											[
الس	Iu	dlu.	• 2	<u> </u>							Jane Di	545,54					
	User Setup			Γ				;	Suppl	ement	ary Us	er Info				?	
	Group Setup		T	F	eal N	lame		Γ									
	Shared Compor	Profile hents			escr	iption		Γ									
	Netwo Config	rk uratior			8	-											1
	Syster Config	n uratior	1					I	Jser S	Setup				?			
}	Interf Config	ace uration	n		Ρ	asswor	d Authe	nticat	ion:								
	Admini Contro	stratio I	n			Cisc	oSecure	PAP	(Also	used fo	r CHAP	ACS MS-CH/	i Intern AP/ARA fiel	al Data P, if th d is no:	ibase e Separi checke	ate	
31	Exterr Databa	ial User ises					Passw	/ord			**	* * *	ner		. checke		
	Postur Valida	e tion	1			Confin	n Passw	ord			**	***					
	letwor	k Acce:	55		ſ	🗌 Sepa	arate (C	HAP/N	1S-CH	AP/ARA	P)						
	rotile:						Passw	ord '									
	Kepor Activi	ts and ty				Confir	n Passw	ord '									
٦1	Online	antation	ЛГ		- 17	U	<u>*-1:</u>			Subr	hit C	ancel	er on in Irain				

🖉 Cis	scoSec	ure AC	5 - Microso	oft Inter	net Explo	orer								_ 🗆 ×
Eile	Edit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	🗘 Bac	k • ≓>	- 🛛 🖸] Ag	<u>i</u> dress 🧔	http://127.	.0.0.1:4413/	-	
C	isco S	YSTEMS	U	ser S	etup									×
	սՈրու	Illiu.	•	F	asswor'	d Authe	enticat	tion:					_	⊥B
	User Setu	r /p /p			Cisc	oSecur	e PAP	(Also use	d for (СНАР/М	ACS Int	ternal Database ARAP, if the Separa field is not checked	rte d.)	
	Setu	/p				Passv	vord			****	*****	***		
4	Shari Comp	ed Profile oonents			Confirr	n Passv	vord			****	*****	***		
2	Netw Conf	vork iguratio	,		🗆 Sepa	rate (Defaul EZVPN ISAKM	t Group I					_	
R.	Syst Conf	em iguratio			Confirr	n Pass	Group Group	3 4						
	Conf	rface 'iguratio inistratic	n		Vhen a CHAP pa Isneciall	token : ssword v usefi	Group Group Group	5 6 7				e separate cation. This i	s	
₽ ∕€ ₩	Cont	rol rnal Use		-	.speeidii	, 4551	Group Group Group	8 9 10				T		
90	Data	ibases					Defau	It Group						
000	Post Vali	ure dation		3.7			2							
	Netw Profil	ork Acce les	ss		1 <u>1</u> 2 - 2015				Call	oack				
	Rep Acti	orts and vity			O Using C No	e group callbad	i settir ok allov	ng wed						-
g) Onlin Docu	ne imentatio						Submi	t D	elete	Cancel			
🖉 Ap	plet dia	alup_filte	r started					0 .					ernet	

Verification

```
R2#debug aaa authentication
AAA Authentication debugging is on
R2#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
R2#deb aaa authorization
AAA Authorization debugging is on
R2#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#ping 150.1.2.2 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
. ! ! ! !
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/10/12 ms
```

Copyright © 2007 Internetwork Expert

R1#

*Mar 1 10:23:30.797: ISAKMP (0:0): received packet from 136.1.121.1 dport 500 sport 500 Global (N) NEW SA *Mar 1 10:23:30.797: ISAKMP: Created a peer struct for 136.1.121.1, peer port 500 *Mar 1 10:23:30.797: ISAKMP: Locking peer struct 0x8291ACFC, IKE refcount 1 for crypto_ikmp_config_initialize_sa *Mar 1 10:23:30.797: ISAKMP (0:0): Setting client config settings 82D89EB0 *Mar 1 10:23:30.797: ISAKMP: local port 500, remote port 500 *Mar 1 10:23:30.801: ISAKMP: insert sa successfully sa = 82BC5CA0 *Mar 1 10:23:30.801: ISAKMP (0:1): processing SA payload. message ID = 0 *Mar 1 10:23:30.801: ISAKMP (0:1): processing ID pavload. message ID = 0 1 10:23:30.801: ISAKMP (0:1): processing ID payload. message ID = 0 *Mar 1 10:23:30.801: ISAKMP (1): Process ID payload : 2 type : R1 FODN name protocol : 17 : 0 port length : 2 *Mar 1 10:23:30.801: ISAKMP (0:1): peer matches *none* of the profiles R2 received aggressive-mode message with FQDN id of R1: *Mar 1 10:23:30.805: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:30.805: ISAKMP (0:1): vendor R2#show de b ID seems Unity/DPD but major 157 mismatch *Mar 1 10:23:30.805: ISAKMP (0:1): vendor ID is NAT-T v3 *Mar 1 10:23:30.805: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:30.805: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch *Mar 1 10:23:30.805: ISAKMP (0:1): vendor ID is NAT-T v2 *Mar 1 10:23:30.805: ISAKMP (0:1): Looking for a matching key for R1 in default *Mar 1 10:23:30.805: ISAKMP: no pre-shared key based on hostname R1! *Mar 1 10:23:30.809: ISAKMP : Scanning profiles for xauth ... *Mar 1 10:23:30.809: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 10 policy *Mar 1 10:23:30.809: ISAKMP: *Mar 1 10:23:30.809: ISAKMP: encryption 3DES-CBC hash MD5 *Mar 1 10:23:30.809: ISAKMP: default group 1 *Mar 1 10:23:30.809: ISAKMP: auth pre-share *Mar 1 10:23:30.809: ISAKMP: *Mar 1 10:23:30.809: ISAKMP: life type in seconds 1 10:23:30.809: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 *Mar 1 10:23:30.813: ISAKMP (0:1): atts are acceptable. Next payload is 0 ISAKMP policy match found: *Mar 1 10:23:30.982: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:30.982: ISAKMP (0:1): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1 10:23:30.986: ISAKMP (0:1): vendor ID is NAT-T v3 *Mar 1 10:23:30.986: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:30.986: ISAKMP (0:1): vendor ID seems Unity/DPD but major 123 mismatch *Mar 1 10:23:30.986: ISAKMP (0:1): vendor ID is NAT-T v2 *Mar 1 10:23:30.986: ISAKMP (0:1): processing KE payload. message ID = 0 *Mar 1 10:23:31.194: ISAKMP (0:1): processing NONCE payload. message ID = 0 *Mar 1 10:23:31.198: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:31.198: ISAKMP (0:1): vendor ID is DPD 1 10:23:31.198: ISAKMP (0:1): processing vendor id payload *Mar *Mar 1 10:23:31.198: ISAKMP (0:1): vendor ID seems Unity/DPD but major 242 mismatch *Mar 1 10:23:31.202: ISAKMP (0:1): vendor ID is XAUTH

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 455 -

*Mar 1 10:23:31.202: ISAKMP (0:1): processing vendor id payload *Mar 1 10:23:31.202: ISAKMP (0:1): vendor ID is Unity *Mar 1 10:23:31.202: AAA: parse name=ISAKMP-ID-AUTH idb type=-1 tty=-1 *Mar 1 10:23:31.202: AAA/MEMORY: create_user (0x82E8C6B8) user='R1' ruser='NULL' ds0=0 port='ISAKMP-ID-AUTH' rem_addr='136.1.121.1' authen_type=NONE service=LOGIN priv=0 initial_task_id='0', vrf= (id=0) *Mar 1 10:23:31.206: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH *Mar 1 10:23:31.206: ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_AM_AAA_AWAIT *Mar 1 10:23:31.206: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): Port='ISAKMP-ID-AUTH' list='ISAKMP' service=NET *Mar 1 10:23:31.206: AAA/AUTHOR/CRYPTO AAA: ISAKMP-ID-AUTH(3753740877) user='R1' *Mar 1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): send AV service=ike *Mar 1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): send AV protocol=ipsec *Mar 1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): found list "ISAKMP" *Mar 1 10:23:31.210: ISAKMP-ID-AUTH AAA/AUTHOR/CRYPTO AAA(3753740877): Method=radius (radius) Next R2 queries RADIUS server to authorize incoming connection and obtain ISAKMP attributes: *Mar 1 10:23:31.210: RADIUS: authenticating to get author data *Mar 1 10:23:31.210: RADIUS: Pick NAS IP for u=0x82E8C6B8 tableid=0 cfg_addr=0.0.0.0 best_addr=136.1.122.2 *Mar 1 10:23:31.210: RADIUS: ustruct sharecount=3 *Mar 1 10:23:31.214: Radius: radius_port_info() success=0 radius_nas_port=1 R2 sends Access-Reques method with FQDN ID of R1 ans password "cisco" (default value, hardcoded): *Mar 1 10:23:31.214: RADIUS(0000000): Send Access-Request to 10.0.0.100:1645 id 21645/5, len 73 *Mar 1 10:23:31.214: RADIUS: authenticator 8D E0 1F 1A A6 0F 06 ED - 7F F5 4F AD 18 04 93 3F *Mar 1 10:23:31.218: RADIUS: NAS-IP-Address [4] 6 136.1.122.2 *Mar 1 10:23:31.218: RADIUS: NAS-Port-Type [61] 6 Async [0] *Mar 1 10:23:31.218: RADIUS: User-Name [1] 4 "R1" *Mar 1 10:23:31.218: RADIUS: Calling-Station-Id [31] 13 "136.1.121.1" *Mar 1 10:23:31.218: RADIUS: User-Password [2] 18 * *Mar 1 10:23:31.218: RADIUS: Service-Type [6] 6 Outbound [5] Access-Accept with a set of attributes received: *Mar 1 10:23:31.286: RADIUS: Received from id 21645/5 10.0.0.100:1645, Access-Accept, len 108 *Mar 1 10:23:31.290: RADIUS: authenticator E2 DC 27 9D C7 FF 16 72 - 71 FE 30 CC 6F 4C A8 42 *Mar 1 10:23:31.290: RADIUS: Vendor, Cisco [26] 30 Kev-exchange protocol: *Mar 1 10:23:31.290: RADIUS: Cisco AVpair [1] 24 "ipsec:keyexchange=ike" *Mar 1 10:23:31.290: RADIUS: Service-Type [6] 6 Outbound [5]

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 456 -

Tunnel-type: *Mar 1 10:23:31.290: RADIUS: Tunnel-Type [64] 6 01:ESP [9] Tunnel-password (pre-shared key actually): *Mar 1 10:23:31.294: RADIUS: Tunnel-Password *Mar 1 10:23:31.294: RADIUS: Class [69] 21 [25] 25 *Mar *Mar 1 10:23:31.294: RADIUS: 43 41 43 53 3A 30 2F 35 63 61 63 2F 38 38 30 31 [CACS:0/5cac/8801] *Mar 1 10:23:31.294: RADIUS: 37 61 30 32 2F 52 31 [7a02/R1] *Mar 1 10:23:31.298: RADIUS: saved authorization data for user 82E8C6B8 at 8291AE94 *Mar 1 10:23:31.298: RADIUS: cisco AVPair "ipsec:key-exchange=ike" *Mar 1 10:23:31.298: RADIUS: Tunnel-Type, [01] 00 00 09 *Mar 1 10:23:31.302: RADIUS: TAS(1) created and engueue 1 10:23:31.302: RADIUS: TAS(1) created and enqueued. *Mar 1 10:23:31.302: RADIUS: Tunnel-Password decrypted, [01] CISCO *Mar 1 10:23:31.302: RADIUS: TAS(1) takes precedence over tagged attributes, tunnel_type=esp *Mar 1 10:23:31.302: RADIUS: free TAS(1) *Mar 1 10:23:31.302: AAA/AUTHOR (3753740877): Post authorization status = PASS_ADD *Mar 1 10:23:31.306: ISAKMP: got callback 1 *Mar 1 10:23:31.306: AAA/AUTHOR/IKE: Processing AV service=ike *Mar 1 10:23:31.306: AAA/AUTHOR/IKE: Processing AV protocol=ipsec *Mar 1 10:23:31.306: AAA/AUTHOR/IKE: Processing AV key-exchange=ike *Mar 1 10:23:31.306: AAA/AUTHOR/IKE: Processing AV tunnel-type*esp *Mar 1 10:23:31.306: AAA/AUTHOR/IKE: Processing AV tunnel-password=CISCO *Mar 1 10:23:31.310: *Mar 1 10:23:31.310: ISAKMP (0:1): SKEYID state generated *Mar 1 10:23:31.314: TSAKMP (0:1): 1 10:23:31.314: ISAKMP (0:1): constructed NAT-T vendor-03 ID *Mar 1 10:23:31.314: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR Sending our ID, in this case - IP address: *Mar 1 10:23:31.314: ISAKMP (1): ID payload next-payload : 10 type : 136.1.122.2 addr protocol : 17 port : 0 length : 8 *Mar 1 10:23:31.314: ISAKMP (1): Total payload length: 12 *Mar 1 10:23:31.318: ISAKMP (0:1): constructed HIS NAT-D *Mar 1 10:23:31.318: ISAKMP (0:1): constructed MINE NAT-D *Mar 1 10:23:31.318: ISAKMP (0:1): sending packet to 136.1.121.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH *Mar 1 10:23:31.318: ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY *Mar 1 10:23:31.322: ISAKMP (0:1): Old State = IKE R AM AAA AWAIT New State = IKE_R_AM2 *Mar 1 10:23:31.322: AAA/MEMORY: free_user (0x82E8C6B8) user='R1' ruser='NULL' port='ISAKMP-ID-AUTH' rem_addr='136.1.121.1' authen_type=NONE service=LOGIN

Copyright © 2007 Internetwork Expert

```
priv=0 vrf= (id=0)
```

```
*Mar 1 10:23:31.538: ISAKMP (0:1): received packet from 136.1.121.1 dport 500
sport 500 Global (R) AG_INIT_EXCH
*Mar 1 10:23:31.542: ISAKMP (0:1): processing HASH payload. message ID = 0
*Mar 1 10:23:31.542: ISAKMP:received payload type 17
*Mar 1 10:23:31.546: ISAKMP (0:1): Detected NAT-D payload
*Mar 1 10:23:31.546: ISAKMP (0:1): recalc my hash for NAT-D
*Mar 1 10:23:31.546: ISAKMP (0:1): NAT match MINE hash
*Mar 1 10:23:31.546: ISAKMP:received payload type 17
*Mar 1 10:23:31.546: ISAKMP (0:1): Detected NAT-D payload
*Mar 1 10:23:31.546: ISAKMP (0:1): recalc his hash for NAT-D
*Mar 1 10:23:31.546: ISAKMP (0:1): NAT match HIS hash
*Mar 1 10:23:31.546: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol
1
        spi 0, message ID = 0, sa = 82BC5CA0
*Mar 1 10:23:31.546: ISAKMP (0:1): Process initial contact,
bring down existing phase 1 and 2 SA's with local 136.1.122.2 remote
136.1.121.1 remote port 500
*Mar 1 10:23:31.550: ISAKMP (0:1): returning IP addr to the address pool
      1 10:23:31.550: ISAKMP (0:1): SA has been authenticated with 136.1.121.1
*Mar
```

General Further Reading

Configuring IKE Shared Secret Using AAA Server IKE: Initiate Aggressive Mode

IPsec NAT-T: L2L Tunnel with VPN3k and IOS Box

Objective: Configure IPsec L2L tunnel between IOS and VPN3k across the NAT.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" <u>"IOS and VPN3k with PSK"</u>.
- The way we are going to change scenario is to make VPN3k to connect to R2 across the PAT configuration on the ASA.
- This way only VPN3k is able to initiate connection to R2.
- Enable NAT-control on the ASA, and translate inside network 136.1.121.0/24 using the outside IP address of the firewall.
- Re-configure IPsec L2L tunnel on R2:
 - Change pre-shared key to match outside IP address of the firewall: 136.1.122.12
 - Create dynamic crypto-map DYNAMIC:
 - Set transform-set 3DES_MD5.
 - Match address LO2_TO_LO1.
 - $\circ~$ Detach crypto-map VPN from interface E0/0 and delete it.
 - Create crypto map VPN and attach dynamic crypt-map DYNAMIC to it.
 - Apply crypto map VPN to interface E0/0.
- VPN3k:
 - Re-configure LAN-to-LAN tunnel "VPN_TO_R2":
 - Set tunnel type to initiate-only
 - Enable NAT-T in tunnel settings
 - o Enable NAT-T globally

Final Configuration

```
ASA1:
nat-control
nat (inside) 1 136.1.121.0 255.255.255.0
global (outside) 1 interface
1
! Static NAT to manage VPN3k
!
static (i,dmz) 136.1.121.11 136.1.121.11
R2:
no crypto isakmp key CISCO address 136.1.121.11
crypto isakmp key CISCO address 136.1.122.12
1
! Delete existing crypto-map
1
interface E 0/0
no crypto map VPN
!
no crypto map VPN
!
! Create dynamic crypto-map
!
crypto dynamic-map DYNAMIC 10
set transform-set 3DES_MD5
match address LO2_TO_LO1
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
!
! Apply new crypto-map
interface E0/0
crypto map VPN
```

VPN3k GUI:

Modify settings for L2L tunnel "VPN_TO_R2":

🚈 Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer 📃 🛛 🗙						
<u>File Edit View Favorites Tool</u>	ls <u>H</u> elp ¢	= Back 🔹 🔿 🔹 🚺	Address 🙋 https://136.1.1	21.11/access.html	Ē.	
VPN 3000 Concentrator Series Manager			Main Help Support Logout Logged in: admin			
			Configur	ation Administration Monitorii	ng	
-D-Contiguration 		Filter -None-	×	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.	-	
	IPSec 1	NAT-T		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.		
- II-SSL - II-SSL - II-Administration - II-Monistration	Ban	dwidth Policy -None- 💌		Choose the bandwidth policy to apply to this LAN-to- LAN connection.		
	F	outing None	•	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen .		
Cisco Systems	Local Net address.	twork: If a LAN-to-LA	N NAT rule is used, this i	s the Translated Network	•	
🛃 IPSec LAN-to-LAN						

🖉 Cisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3K] - Microsoft Interne	t Explorer	_ 🗆 ×		
<u>File Edit Yiew Favorites Tools</u>	; <u>H</u> elp (⇔ Back → ⇒) → 💽 🚺	Address 🗃 https://136.1.121.11/access.html	•		
VPN 3	3000	Main Help S	upport Logout		
Conce	ntrator Series Manager	Logged in: admin			
		Configuration Administrati	ion Monitoring		
	Configuration Tunneling and Security IPSec NAT Transparency				
<u>System</u>	Save Needed				
	This section lets you configure system-wide IPSec NAT Transparency.				
	IPSec over TCP 🗖	Check to enable IPSec over TCP.			
LAN-to-LAN LAN-to-LAN	TCP Port(s) 10000	Enter up to 10 comma-separated TCP ports (1 - 65535).			
-D-NAT Transparency Alerts 	IPSec over NAT-T	Check to enable IPSec over NAT-T, detects the need for UDP encapsulati NAT/PAT environments, using UDP	which on in port 4500.		
CISCO SYSTEMS		Interr	net		

Verification R1#ping 150.1.2.2 so lo 0 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds: Packet sent with a source address of 150.1.1.1 Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms R2#debug crypto isakmp Crypto ISAKMP debugging is on <output omitted> *Mar 1 22:50:31.399: ISAKMP (0:4): processing SA payload. message ID = 0 *Mar 1 22:50:31.399: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:31.399: ISAKMP (0:4): vendor ID seems Unity/DPD but major 123 mismatch *Mar 1 22:50:31.399: ISAKMP (0:4): vendor ID is NAT-T v2 *Mar 1 22:50:31.399: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:31.399: ISAKMP (0:4): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1 22:50:31.399: ISAKMP (0:4): vendor ID is NAT-T v3 *Mar 1 22:50:31.399: ISAKMP (0:4): processing vendor id payload

Copyright © 2007 Internetwork Expert

R2#Mar 1 22:50:31.403: ISAKMP (0:4): vendor ID seems Unity/DPD but major 194 mismatch *Mar 1 22:50:31.403: ISAKMP: Looking for a matching key for 136.1.122.12 in default : success *Mar 1 22:50:31.403: ISAKMP (0:4): found peer pre-shared key matching 136.1.122.12 *Mar 1 22:50:31.403: ISAKMP (0:4) local preshared key found *Mar 1 22:50:31.403: ISAKMP : Scanning profiles for youth 1 22:50:31.403: ISAKMP : Scanning profiles for xauth ... *Mar 1 22:50:31.403: ISAKMP (0:4): Checking ISAKMP transform 1 against priority 10 policy *Mar 1 22:50:31.403: ISAKMP: *Mar 1 22:50:31.407: ISAKMP: encryption 3DES-CBC 1 22:50:31.407: ISAKMP: hash MD5 *Mar 1 22:50:31.407: ISAKMP: default group 2 *Mar 1 22:50:31.407: ISAKMP: auth pre-share *Mar 1 22:50:31.407: ISAKMP: life type in seconds 1 22:50:31.407: ISAKMP: *Mar life duration (VPI) of 0x0 0x1 0x51 0x80 *Mar 1 22:50:31.407: ISAKMP (0:4): atts are acceptable. Next payload is 0 *Mar 1 22:50:31.683: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 123 mismatch *Mar 1 22:50:31.687: ISAKMP (0:4): vendor ID is NAT-T v2 *Mar 1 22:50:31.687: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1 22:50:31.687: ISAKMP (0:4): vendor ID is NAT-T v3 *Mar 1 22:50:31.687: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:31.687: ISAKMP (0:4): vendor ID seems Unity/DPD but major 194 mismatch *Mar 1 22:50:31.691: ISAKMP (0:4): Input = IKE_MESG_INTERNAL, IKE PROCESS MAIN MODE *Mar 1 22:50:31.691: ISAKMP (0:4): Old State = IKE_R_MM1 New State = IKE_R_MM1 *Mar 1 22:50:31.699: ISAKMP (0:4): constructed NAT-T vendor-03 ID *Mar 1 22:50:31.699: ISAKMP (0:4): sending packet to 136.1.122.12 my_port 500 peer_port 2 (R) MM_SA_SETUP *Mar 1 22:50:31.699: ISAKMP (0:4): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE IKE_R_MM2 *Mar 1 22:50:31.811: ISAKMP (0:4): received packet from 136.1.122.12 dport 500 sport 2 Global (R) MM_SA_SETUP *Mar 1 22:50:31.815: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH *Mar 1 22:50:31.815: ISAKMP (0:4): Old State = IKE_R_MM2 New State = IKE_R_MM3 *Mar 1 22:50:31.819: ISAKMP (0:4): processing KE payload. message ID = 0 *Mar 1 22:50:32.156: ISAKMP (0:4): processing NONCE payload. message ID = 0 *Mar 1 22:50:32.168: ISAKMP: Looking for a matching key for 136.1.122.12 in default : success *Mar 1 22:50:32.172: ISAKMP (0:4): found peer pre-shared key matching 136.1.122.12 *Mar 1 22:50:32.172: ISAKMP (0:4): SKEYID state generated *Mar 1 22:50:32.176: ISAKMP (0:4): processing vendor id pa 1 22:50:32.176: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:32.176: ISAKMP (0:4): vendor ID is Unity *Mar 1 22:50:32.176: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:32.176: ISAKMP (0:4): vendor ID seems Unity/DPD but major 39 mismatch *Mar 1 22:50:32.176: ISAKMP (0:4): vendor ID is XAUTH *Mar 1 22:50:32.176: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:32.180: ISAKMP (0:4): speaking to another IOS box!

```
Copyright © 2007 Internetwork Expert
```

www.InternetworkExpert.com

- 463 -

*Mar 1 22:50:32.180: ISAKMP (0:4): processing vendor id payload *Mar 1 22:50:32.180: ISAKMP (0:4): vendor ID seems Unity/DPD but major 4 mismatch *Mar 1 22:50:32.180: ISAKMP:received payload type 17 *Mar 1 22:50:32.180: ISAKMP (0:4): Detected NAT-D payload *Mar 1 22:50:32.180: ISAKMP (0:4): NAT match MINE hash *Mar 1 22:50:32.180: ISAKMP:received payload type 17 1 22:50:32.180: ISAKMP (0:4): Detected NAT-D payload *Mar *Mar 1 22:50:32.184: ISAKMP (0:4): NAT does not match HIS hash *Mar 1 22:50:32.184: hash received: E8 A0 28 25 68 19 1D CB A9 A9 12 CD 33 18 D7 E *Mar 1 22:50:32.184: his nat hash : D 74 46 B9 F4 14 42 22 B5 7F 97 AD 5C 98 C EC *Mar 1 22:50:32.188: ISAKMP (0:4): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE *Mar 1 22:50:32.188: ISAKMP (0:4): Old State = IKE_R_MM3 New State = IKE R MM3 R2#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: VPN, local addr. 136.1.122.2 protected vrf: local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0) current_peer: 136.1.122.12:1025 PERMIT, flags={} #pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5 #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 21 #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.: 136.1.122.2, remote crypto endpt.: 136.1.122.12 path mtu 1500, media mtu 1500 current outbound spi: 49FC5761 inbound esp sas: spi: 0xC8A87211(3366482449) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4414001/2862) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x49FC5761(1241274209) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4414004/2862) IV size: 8 bytes replay detection support: Y outbound ah sas:

Copyright © 2007 Internetwork Expert
outbound pcp sas:

ASAl(config)# **show xlate** 2 in use, 4 most used Global 136.1.121.11 Local 136.1.121.11 PAT Global 136.1.122.12(1025) Local 136.1.121.11(4500)

ASA1(config)# **show conn** 7 in use, 98 most used TCP out 10.0.0.100:2415 in 136.1.121.11:443 idle 0:00:40 bytes 1205 flags UIOB UDP out 136.1.122.2:4500 in 136.1.121.11:4500 idle 0:00:02 flags -

Further Reading

Configuring NAT Transparent Mode for IPSec on the VPN 3000 Concentrator

IKE Tunnel Endpoint Discovery (TED)



Objective: Configure IOS routers for tunnel end-point discovery.

Directions

- Configure devices as per the "VPN/IPsec LAN-to-LAN" scenario <u>"IOS and IOS with PSK across the PIX/ASA".</u>
- Detach crypto map VPN from Ethernet interfaces. Delete crypto map VPN.
- Create dynamic crypto map DISCOVER on R1 and R2:
 - Match access-list LO1_TO_LO2 and LO2_TO_LO1 respectively.
 Set transform-set 3DES_MD5
- Create crypto map VPN entry 10 of type IPsec-ISAKMP:
 - Attach dynamic crypto-map DISCOVER and enable peer IP discovery.
- Apply crypto map VPN to ethernet interfaces.

Final Configuration

```
R1:
!
Lelete existing crypto map
interface E0/0
no crypto map VPN
exit
!
no crypto map VPN
!
! Create dynamic crypto map
!
crypto dynamic-map DISCOVER 10
match address LO1_TO_LO2
```

Copyright © 2007 Internetwork Expert

```
set transform-set 3DES_MD5
!
! Enable TED
!
crypto map VPN 10 ipsec-isakmp dynamic DISCOVER discover
!
! Apply crypto map to the interface
interface E0/0
 crypto map VPN
R2:
!
! Delete existing crypto map
interface E0/0
 no crypto map VPN
  exit
!
no crypto map VPN
!
! Create dynamic crypto map
1
crypto dynamic-map DISCOVER 10
 match address LO2_TO_LO1
  set transform-set 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DISCOVER discover
!
! Apply crypto map to the interface
interface E0/0
  crypto map VPN
```

Verification

```
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#ping 150.1.2.2 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
. . . . . .
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/20 ms
*Mar 1 12:35:08.364: ISAKMP: received ke message (1/1)
*Mar 1 12:35:08.364: ISAKMP: GOT A PEER DISCOVERY MESSAGE FROM THE SA
MANAGER!!!
*Mar 1 12:35:08.364: src = 150.1.1.1 to 150.1.2.2, protocol 3, transform 3,
hmac 1
*Mar 1 12:35:08.364: proxy source is 150.1.1.0/255.255.255.0 and my address
(not used now) is 136.1.121.1
*Mar 1 12:35:08.368: ISAKMP (0:0): no idb in request
*Mar 1 12:35:08.368: ISAKMP (0:0): SA request profile is (NULL)
*Mar 1 12:35:08.368: ISAKMP: local port 500, remote port 500
*Mar 1 12:35:08.372: ISAKMP: set new node 0 to QM_IDLE
*Mar 1 12:35:08.372: ISAKMP: Find a dup sa in the avl tree during calling
isadb_insert sa = 82E2EF64
```

```
Copyright © 2007 Internetwork Expert
```

```
- 467 -
```

*Mar 1 12:35:08.372: ISAKMP (0:19): SA is doing unknown authentication! *Mar 1 12:35:08.372: ISAKMP (19): ID payload next-payload : 5 type : 1 addr : 136.1.121.1 protocol : 17 port : 500 : 8 length *Mar 1 12:35:08.372: ISAKMP (19): Total payload length: 12 *Mar 1 12:35:08.376: 1st ID is 136.1.121.1 *Mar 1 12:35:08.376: 2nd ID is 150.1.1.0/255.255.255.0 *Mar 1 12:35:08.376: ISAKMP (0:19): Input = IKE_MESG_FROM_IPSEC, IKE_TED_REQ *Mar 1 12:35:08.376: ISAKMP (0:19): Old State = IKE_READY New State = IKE_I_TED_RESP *Mar 1 12:35:08.376: ISAKMP (0:19): beginning peer discovery exchange *Mar 1 12:35:08.376: ISAKMP (0:19): sending packet to 150.1.2.2 my_port 500 peer_port 500 (I) PEER_DISCOVERY via Ethernet0/0:136.1.121.12 *Mar 1 12:35:08.396: ISAKMP (0:19): received packet from 136.1.122.2 dport 500 sport 500 Global (I) PEER_DISCOVERY *Mar 1 12:35:08.400: ISAKMP (0:19): processing vendor id payload *Mar 1 12:35:08.400: ISAKMP (0:19): speaking to another IOS box! *Mar 1 12:35:08.400: ISAKMP (0:19): processing ID payload. message ID = 0 *Mar 1 12:35:08.400: ISAKMP:received payload type 16 *Mar 1 12:35:08.400: ISAKMP (0:19): received response to my peer discovery probe! *Mar 1 12:35:08.404: ISAKMP (0:19): ted negotiated proxies: 0 150.1.1.0/255.255.255.0:0, 150.1.2.0/255.255.255.0:0 *Mar 1 12:35:08.404: ISAKMP (0:19): initiating IKE to 136.1.122.2 in response to probe. R1# show crypto isakmp sa detail Codes: C - IKE configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal X - IKE Extended Authentication psk - Preshared key, rsig - RSA signature renc - RSA encryption I-VRF Encr Hash Auth DH Lifetime Cap. C-id Local Remote 136.1.121.1 136.1.122.2 3des md5 psk 1 23:53:14 20 R1#show crypto ipsec sa interface: Ethernet0/0 Crypto map tag: VPN, local addr. 136.1.121.1 protected vrf: local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0) current_peer: 136.1.122.2:500 PERMIT, flags={} #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 0, #recv errors 0 local crypto endpt.: 136.1.121.1, remote crypto endpt.: 136.1.122.2 path mtu 1500, media mtu 1500 current outbound spi: A1315146 inbound esp sas:

Copyright © 2007 Internetwork Expert

```
CCIE Security Lab Workbook Volume I Version 3.0
```

```
spi: 0xCE62E629(3462587945)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
  sa timing: remaining key lifetime (k/sec): (4418894/3170)
  IV size: 8 bytes
  replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
 spi: 0xA1315146(2704363846)
  transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
  sa timing: remaining key lifetime (k/sec): (4418894/3170)
  IV size: 8 bytes
  replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

Configuring IPSec Tunnel End-Point Discovery

IPsec VPN High-Availability with HSRP

Objective: Configure IPsec tunnel high-availability using HSRP.



Directions

- Pre-configuration steps:
 - Create necessary VLANs on SW1 & SW2, and configure trunk ports.
 - Configure IP addressing as per the diagram.
 - Configure RIP as routing protocol on R2, R3, and R4.
 - Configure HSRP on R3, R4 VLAN 234 (interfaces E0/0):
 - Use virtual IP 136.X.234.254
 - Use HSRP name HSRP1
 - Configure preemption.
 - Track interface E0/1.
 - R3 should be primary.
 - Configure static default route to 136.X.234.254 on R2.
- The idea behind the high-availability is to use HSRP virtual IP address for IPsec tunnel establishment. Whether one of peers fails, the other will automatically take the active role.
- IPsec HA Configuration:
 - Configure ISAKMP policy on R2, R3, R4:
 - Use 3DES cipher.
 - Use MD5 hash.
 - Use Pre-shared keys for authentication.
 - Set ISAKMP keepalive interval to minimum value.
 - Create pre-shared keys on R3 and R4 for IP address 136.X.234.2 of R2.
 - Create pre-shared key on R2 for HSRP virtual IP address 136.X.234.254
 - Create transform-set 3DES_MD5 on R3, R4, and R2.
 - Use 3DES cipher.
 - Use MD5 hash.
 - Create access-list R1_TO_R2 on R3 and R4:

- Match IP traffic from 150.1.1.0/24 to 150.1.2.0/24.
- Create access-list R2_TO_R1 on R2:
 - Match IP traffic from 150.1.2.0/24 to 150.1.1.0/24.
- On R3 and R4 create crypto map VPN entry 10, type IPsec ISAKMP:
 - Match IP address R1_TO_R2.
 - Set peer 136.X.234.2
 - Set transform-set 3DES_MD5.
 - Enable RRI
- Assign crypto map VPN to interface E0/1 on R3 and R4 and attach it to HSRP group HSRP1.
- o On R3 and R4 redistribute static subnets into RIP.
- o On R2 create crypto map VPN entry 10 type IPsec-ISAKMP:
 - Match IP address R2_TO_R1.
 - Set peer 136.X.234.254
 - Set transform-set 3DES_MD5.
- Set up RIP timers on R1, R3, and R4 for faster convergence. Divide all timers by value of ten.

Final Configuration

```
Pre-Configuration:
```

```
SW1 & SW2:
vlan 234,134
interface range Fa 0/21 - 23
no shut
switchport trunk encaps dotlg
switchport mode trunk
SW1:
interface Fa 0/1
 switchport mode access
 switchport access vlan 134
!
interface Fa 0/2
 switchport mode access
 switchport access vlan 234
interface Fa 0/3
 switchport mode access
  switchport access vlan 134
interface Fa 0/4
 switchport mode access
 switchport access vlan 134
SW2:
interface Fa 0/3
 switchport mode access
 switchport access vlan 234
interface Fa 0/4
 switchport mode access
```

Copyright © 2007 Internetwork Expert

```
switchport access vlan 234
R1:
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
interface E 0/0
ip address 136.1.134.1 255.255.255.0
no shutdown
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
R2:
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
interface E 0/0
 ip address 136.1.234.2 255.255.255.0
no shutdown
T
ip route 0.0.0.0 0.0.0.0 136.1.234.254
R3:
interface E 0/0
ip address 136.1.134.3 255.255.255.0
no shutdown
!
! Configure HSRP
interface E 0/1
 ip address 136.1.234.3 255.255.255.0
standby 1 ip 136.1.234.254
standby 1 preempt
standby 1 track E 0/0 20
standby 1 priority 110
standby 1 name HSRP1
no shutdown
!
router rip
 ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
R4:
interface E 0/0
ip address 136.1.134.4 255.255.255.0
no shutdown
!
! Configure HSRP
interface E 0/1
ip address 136.1.234.4 255.255.255.0
standby 1 ip 136.1.234.254
standby 1 preempt
 standby 1 name HSRP1
no shutdown
!
router rip
```

Copyright © 2007 Internetwork Expert

```
ver 2
 no auto
 network 136.1.0.0
 network 150.1.0.0
R3 & R4:
crypto isakmp policy 10
auth pre
hash md5
encr 3des
!
! Configure pre-shared key
!
crypto isakmp key CISCO address 136.1.234.2
!
! Shorten keepalive interval
!
crypto isakmp keepalive 10
!
! Configure access-list to match traffic
ip access-list ext R1_T0_R2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
I.
! Create transform-set
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
!
! Configure crypto map with RRI
crypto map VPN 10 ipsec-isakmp
 match address R1_TO_R2
 set transform 3DES_MD5
  set peer 136.1.234.2
  reverse
!
! Apply crypto-map and enable redundancy
!
interface E0/1
 crypto map VPN redundancy HSRP1
!
! Redistribute static routes from RRI
!
router rip
redistribute static
R2:
crypto isakmp policy 10
auth pre
hash md5
encr 3des
I
1
1
crypto isakmp key CISCO address 136.1.234.254
crypto isakmp keepalive 10
!
!
ip access-list ext R2_T0_R1
```

Copyright © 2007 Internetwork Expert

```
permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
!
!
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
!
!
crypto map VPN 10 ipsec-isakmp
 match address R2_T0_R1
 set transform 3DES_MD5
 set peer 136.1.234.254
!
1
interface E0/0
 crypto map VPN
Tune up RIP convergence:
R1, R3, R4:
router rip
 timers basic 3 18 18 24
```

Verification

```
Primary path:
```

```
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
. . . . . .
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms
R2#show crypto isakmp sa
                               state
                                             conn-id slot
dst
               src
136.1.234.254 136.1.234.2
                              QM_IDLE
                                                  1
                                                          Ω
R2#show crypto ips sa
interface: Ethernet0/0
   Crypto map tag: VPN, local addr. 136.1.234.2
   protected vrf:
   local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.234.254:500
     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.: 136.1.234.2, remote crypto endpt.: 136.1.234.254
     path mtu 1500, media mtu 1500
```

```
Copyright © 2007 Internetwork Expert
```

```
current outbound spi: ABB177EC
     inbound esp sas:
     spi: 0x6BBA47F9(1807370233)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4499195/3565)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0xABB177EC(2880534508)
       transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4499195/3565)
        IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R3#show crypto isakmp sa
dst src state
136.1.234.254 136.1.234.2 QM_IDLE
                                              conn-id slot
                                                 1
                                                         0
R3#show crypto ipsec sa
interface: Ethernet0/1
   Crypto map tag: VPN, local addr. 136.1.234.254
  protected vrf:
   local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.234.2:500
    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 0, #recv errors 0
    local crypto endpt.: 136.1.234.254, remote crypto endpt.: 136.1.234.2
     path mtu 1500, media mtu 1500
     current outbound spi: 6BBA47F9
     inbound esp sas:
     spi: 0xABB177EC(2880534508)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4604708/3508)
        IV size: 8 bytes
        replay detection support: Y
```

```
inbound ah sas:
```

Copyright © 2007 Internetwork Expert

```
inbound pcp sas:
     outbound esp sas:
      spi: 0x6BBA47F9(1807370233)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4604708/3508)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R3#show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:31:02
  Virtual IP address is 136.1.234.254
  Active virtual MAC address is 0000.0c07.ac01
   Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 1.333 secs
  Preemption enabled
  Active router is local
  Standby router is 136.1.234.4, priority 100 (expires in 9.523 sec)
  Priority 110 (configured 110)
    Track interface Ethernet0/0 state Up decrement 20
  IP redundancy name is "HSRP1" (cfgd)
R3#show cry map tag VPN
Redundancy Group: HSRP1
Crypto Map "VPN" 10 ipsec-isakmp
        Peer = 136.1.234.2
        Extended IP access list R1 TO R2
            access-list R1_T0_R2 permit ip 150.1.1.0 0.0.0.255 150.1.2.0
0.0.0.255
        Current peer: 136.1.234.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                3DES_MD5,
        Reverse Route Injection Enabled
        Interfaces using crypto map VPN:
               Ethernet0/1
R1#show ip route rip
    136.1.0.0/24 is subnetted, 2 subnets
R
       136.1.234.0 [120/1] via 136.1.134.3, 00:00:07, Ethernet0/0
                    [120/1] via 136.1.134.4, 00:00:24, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
R
        150.1.2.0 [120/1] via 136.1.134.3, 00:00:07, Ethernet0/0
Shutdown E0/0 on R3 to make primary path fail:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface ethernet 0/0
R3(config-if)#shut
```

Copyright © 2007 Internetwork Expert

```
R3#show standby
Ethernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:00:29
  Virtual IP address is 136.1.234.254
  Active virtual MAC address is 0000.0c07.ac01
   Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
   Next hello sent in 0.836 secs
  Preemption enabled
  Active router is 136.1.234.4, priority 100 (expires in 9.836 sec)
  Standby router is local
  Priority 90 (configured 110)
    Track interface Ethernet0/0 state Down decrement 20
  IP redundancy name is "HSRP1" (cfgd)
R2#show crypto isakmp sa
dst
               src
                                state
                                              conn-id slot
136.1.234.254
               136.1.234.2
                              MM_NO_STATE
                                                1 0 (deleted)
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
. . . . . .
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/12/12 ms
R4#show crypto isakmp sa
                                              conn-id slot
dst
                src
                               state
136.1.234.254
              136.1.234.2 QM_IDLE
                                                    1
                                                          0
R4#show cry ips sa
interface: Ethernet0/1
    Crypto map tag: VPN, local addr. 136.1.234.254
   protected vrf:
   local ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   current_peer: 136.1.234.2:500
     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 0, #recv errors 0
     local crypto endpt.: 136.1.234.254, remote crypto endpt.: 136.1.234.2
     path mtu 1500, media mtu 1500
     current outbound spi: 30B73525
     inbound esp sas:
      spi: 0x7AAA7507(2057991431)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
        sa timing: remaining key lifetime (k/sec): (4472014/3552)
        IV size: 8 bytes
        replay detection support: Y
```

CCIE Security Lab Workbook Volume I Version 3.0

```
inbound ah sas:
     inbound pcp sas:
    outbound esp sas:
     spi: 0x30B73525(817313061)
        transform: esp-3des esp-md5-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
       sa timing: remaining key lifetime (k/sec): (4472014/3552)
       IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
R1#show ip route rip
    136.1.0.0/24 is subnetted, 2 subnets
R
       136.1.234.0 [120/1] via 136.1.134.4, 00:00:02, Ethernet0/0
     150.1.0.0/24 is subnetted, 2 subnets
       150.1.2.0 [120/1] via 136.1.134.4, 00:00:02, Ethernet0/0
R
```

Further Reading

IPsec High Availability

IPsec High Availability with NAT and HSRP

Objective: Configure IPsec tunnel across NAT enabling bi-directional tunnel initiation.



Directions

- Configure devices as per the scenario "VPN/Advanced Topics" <u>"IPsec High Availability with HSRP"</u>.
- Remove IPsec configuration from R3/R4.
- Configure NAT on R3 and R4:
 - o Make E0/1 outside interface and E0/0 inside
 - Configure static mapping for IP 136.X.134.1 to 136.X.234.1 with redundancy via HSRP group HSRP1.
- Re-configure IPsec on R2 to use peer IP address 136.X.234.1. Reconfigure ISAKMP key accordingly.
- Configure IPsec on R1:
 - Configure ISAKMP policy:
 - Use pre-shared keys for authentication.
 - Use 3DES cipher.
 - Use MD5 hash.
 - o Configure ISAKMP pre-shared key for IP address 136.X.234.2
 - Create IPsec transform-set 3DES_MD5:
 - Use 3DES cipher.
 - Use MD5 hash.
 - Create dynamic crypto map DYNAMIC entry 10
 - Apply transform-set 3DES_MD5
 - Enable RRI
 - Create crypto map VPN entry 10 and attach dynamic crypto map DYNAMIC.
 - Apply crypto-map VPN to interface E0/0.

```
Final Configuration
```

```
R3 & R4:
interface E0/1
 no crypto map VPN
! Static NAT mapping with HSRP redundancy support
!
ip nat inside source static 136.1.134.1 136.1.234.1 red HSRP1
1
inter E0/1
ip nat outside
I
inter E0/0
ip nat inside
R2:
crypto map VPN 10
no set peer 136.1.234.254
set peer 136.1.234.1
!
! Change ISAKMP peer IP address
1
crypto isakmp key CISCO addr 136.1.234.1
R1:
crypto isakmp policy 10
auth pre
hash md5
encr 3des
!
crypto isakmp key CISCO addr 136.1.234.2
1
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5
crypto dynamic-map DYNAMIC 10
set transform 3DES_MD5
!
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
1
interface E0/0
 crypto map VPN
```

Verification

```
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
IIIII
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
R3#show standby
Ethernet0/1 - Group 1
State is Active
5 state changes, last state change 00:09:59
Virtual IP address is 136.1.234.254
```

```
Copyright © 2007 Internetwork Expert
```

```
Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.880 secs
  Preemption enabled
  Active router is local
  Standby router is 136.1.234.4, priority 100 (expires in 8.874 sec)
  Priority 110 (configured 110)
    Track interface Ethernet0/0 state Up decrement 20
  IP redundancy name is "HSRP1" (cfgd)
R2#sho ip arp
                          Age (min) Hardware Addr Type Interface
Protocol Address
Internet 136.1.234.3
                                        0050.5476.4101 ARPA Ethernet0/0
                                187
Internet 136.1.234.2
                                        0003.e335.1240 ARPA Ethernet0/0
                                  _
Internet 136.1.234.1
Internet 136.1.234.4
                                        0050.5476.4101 ARPA Ethernet0/0
                                 14
                                       0050.8004.8b61 ARPA Ethernet0/0
0000.0c07.ac01 ARPA Ethernet0/0
                                 187
Internet 136.1.234.254
                                 15
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface ethernet 0/0
R3(config-if)#shutdown
136.1.234.1 ARP entry was replaced by gratituous ARP from R4:
R2#sho ip arp
Protocol Address
                          Age (min) Hardware Addr Type Interface
Internet 136.1.234.3
Internet 136.1.234.2
                           189
                                       0050.5476.4101 ARPA Ethernet0/0
                                 -
                                       0003.e335.1240 ARPA Ethernet0/0
0050.8004.8b61 ARPA Ethernet0/0
Internet 136.1.234.1
                                  0
Internet 136.1.234.4
                                 189
                                       0050.8004.8b61 ARPA Ethernet0/0
Internet 136.1.234.254
                                   0
                                       0000.0c07.ac01 ARPA Ethernet0/0
R2#ping 150.1.1.1 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
No IPsec re-negotiation took place since IPsec endpoint neve changed.
R2#show crypto ipsec sa
interface: Ethernet0/0
    Crypto map tag: VPN, local addr. 136.1.234.2
   protected vrf:
   local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
   current_peer: 136.1.234.1:4500
     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 1, #recv errors 0
     local crypto endpt.: 136.1.234.2, remote crypto endpt.: 136.1.234.1
     path mtu 1500, media mtu 1500
```

```
Copyright © 2007 Internetwork Expert
```

```
current outbound spi: B57901EF
inbound esp sas:
spi: 0xAF5F4F7C(2942259068)
   transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel UDP-Encaps, }
  slot: 0, conn id: 2000, flow_id: 1, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4490451/2831)
   IV size: 8 bytes
  replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
 spi: 0xB57901EF(3044606447)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel UDP-Encaps, }
  slot: 0, conn id: 2001, flow_id: 2, crypto map: VPN
   sa timing: remaining key lifetime (k/sec): (4490451/2831)
   IV size: 8 bytes
  replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

NAT - Static Mapping Support with HSRP for High Availability

IPsec Pass-Through Inspection on the PIX/ASA

Objective: Configure the ASA firewall to inspect IKE sessions and open pinholes in ACLs dynamically.



Directions

- Configure devices as per the scenario "VPN/IPsec LAN-to-LAN" "IOS and IOS with Digital Certificates across the PIX/ASA".
- Remove access-list line permitting ESP traffic from the acl OUTSIDE_IN.
- Configure L3/L4 class-map IKE_TRAFFIC and match udp port 500 with it.
- Configure policy-map "global_policy":
 - For class IKE_TRAFFIC configure IPsec inspection.

Final Configuration

```
ASA1:

class-map IKE_TRAFFIC

match port udp eq isakmp

!

policy-map global_policy

class IKE_TRAFFIC

inspect ipsec-pass-thru

!

no access-list OUTSIDE_IN permit esp any any
```

Verification

```
R2#ping 150.1.1.1 source loopback 0
```

Type escape sequence to abort.

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

```
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 150.1.2.2
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 8/8/8 ms
ASA1(config) # show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTSIDE_IN; 3 elements
access-list OUTSIDE_IN line 1 extended permit udp any any eq isakmp (hitcnt=2)
0x468d7962
access-list OUTSIDE_IN line 2 extended permit tcp any host 10.0.0.100 eq www
(hitcnt=8) 0x59f08b76
access-list OUTSIDE_IN line 3 extended permit udp any host 10.0.0.100 eq ntp
(hitcnt=6) 0x8189f120
ASA1(config)# show service-policy global
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: rsh, packet 0, drop 0, reset-drop 0
      Inspect: rtsp, 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: skinny, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
      Inspect: sip, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
    Class-map: IKE_TRAFFIC
      Inspect: ipsec-pass-thru _default_ipsec_passthru_map, packet 10, drop 0,
reset-drop 0
ASA1(config)# show conn
13 in use, 209 most used
UDP out 10.0.0.100:123 in 136.1.121.1:123 idle 0:00:53 flags -
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:22 bytes 248
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:30 bytes 0
ESP out 136.1.122.2 in 136.1.121.1 idle 0:01:22 bytes 248
ESP out 0.0.0.0 in 0.0.0.0 idle 0:01:30 bytes 0
UDP out 136.1.122.2:500 in 136.1.121.1:500 idle 0:01:22 flags -
UDP out 136.1.122.2:123 in 10.0.0.100:123 idle 0:00:34 flags -
```

Further Reading

Using Modular Policy Framework Configuring Application Layer Protocol Inspection

L2TP over IPsec between the ASA and Windows 2000 PC

Objective: Configure the ASA firewall to support remote L2TP over IPsec connections.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" • "The PIX/ASA Easy VPN/WebVPN".
- The goal of this lab is to set up remote VPN connection using L2TP over IPsec as tunneling protocol. For IPsec part, authentication is performed using the pre-shared keys.
- Configure the workstation using the guide: "How to configure an L2TP/IPSec connection by using Preshared Key Authentication" at http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q240262
- Configure the ASA firewall as follows:

o IPsec settings:

- Enable ISAKMP on the outside interface of the ASA
- Create an ISAKMP policy to use pre-shared keys for authentication and 3DES/SHA1/Group2 as cipher/hash/DH group.
 - Create a wildcard pre-shared key CISCO
 - Create an IPSec transform-set 3DES MD5 TRANS as follows:

- Use 3DES/MD5 as cipher/hash
- Configure transport mode
- Create an access-list L2TP and match UDP traffic from the outside interface to any host port 1701 (L2TP)
- Create a dynamic crypto map DYNAMIC as follows:
 - Match access-list L2TP
 - Set transform-set 3DES_MD5_TRANS
- Create a crypto map VPN and assign the dynamic crypto map DYNAMIC_VPN to it.
- Assign the crypto map VPN to outside interface.
- IP addressing and username:
 - Create an IP local address pool L2TP with the address range 20.0.0.1 20.0.0.254
 - Create local username CISCO with password CISCO1234, specify MSCHAP keyword with it. This way it will be hashed to be used with MSCHAP authentication.
- Create group-policy "L2TP" as follows:
 - Configure IPsec and L2TP-IPsec as the tunneling protocols.
 - Configure default-domain value "internetworkexpert.com".
 - Use DNS server IP address 10.0.0.100.
- Assign group-policy "L2TP" to user "CISCO", and configure "L2TPover-IPsec" as user's tunneling protocol.
- Modify the built-in default tunnel-group "DefaultRAGroup" generalattributes as follows:
 - Assign local address pool L2TP to the group.
 - Use LOCAL authentication server group.
 - Apply default group policy "L2TP".
- Modify the built-in default tunnel-group "DefaultRAGroup" pppattributes to use "MS-CHAP-v2" as the authentication protocol.
- Modify the built-in default tunnel-group "DefaultRAGroup" ipsecattributes to use pre-shared key "CISCO".

Final Configuration

```
ASA1:
! Define a new group policy for L2TP connections
!
group-policy L2TP internal
group-policy L2TP attributes
 dns-server value 10.0.0.100
vpn-tunnel-protocol IPSec 12tp-ipsec
default-domain value internetworkexpert.com
!
! Create local user and apply the group policy to it
1
username CISCO password CISCO1234 mschap
!
! Note that user's tunneling protocol is L2TP over IPsec
!
username CISCO attributes
vpn-group-policy L2TP
vpn-tunnel-protocol l2tp-ipsec
1
! Modify built-in default tunnel-group
! Apply the L2TP group-policy within
1
tunnel-group DefaultRAGroup general-attributes
address-pool L2TP
default-group-policy L2TP
authentication-server-group LOCAL
! Define PPP attributes
!
tunnel-group DefaultRAGroup ppp-attributes
authentication ms-chap-v2
1
! Define a pre-share ISAKMP key
!
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key CISCO
!
! Enable and configure ISAKMP on the outside
1
crypto isakmp enable outside
crypto isakmp identity address
crypto isakmp policy 10
 auth pre-share
  encr 3des
 hash shal
 group 1
!
crypto ipsec transform-set DES_MD5_TRANS esp-des esp-md5-hmac
crypto ipsec transform-set DES_MD5_TRANS mode transport
!
access-list L2TP extended permit udp any any eq 1701
1
crypto dynamic-map DYNAMIC 10 match address L2TP
crypto dynamic-map DYNAMIC 10 set transform-set DES_MD5_TRANS
crypto map VPN 10 ipsec-isakmp dynamic DYNAMIC
crypto map VPN interface outside
```

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

sysopt connection permit-vpn

erification		
eate new L2TP	VPN connection:	
	2TP Tunnel ? X	
	General Options Security Networking Sharing	
	Host name or IP address of destination (such as microsoft.com or 123.45.6.78):	
	136.1.123.12	
	- First connect	
	Windows can first connect the public network, such as the Internet, before trying to establish this virtual connection.	
	Dial another connection first:	
	T Chamiens is backbased as a superstand	
_	Show icon in taskbar when connected	
	OK Cancel	

Uptional (encryption (connect even if no encryption)
- Logon s	ecurity
C Use	Extensible Authentication Protocol (EAP)
	<u> </u>
	Properties
Allow	w these protocols
	Unencrypted password (PAP)
	Shiva Password Authentication Protocol (SPAP)
	Challenge Handshake Authentication Protocol (CHAP)
Г	Microsoft CHAP (MS-CHAP)
	Allow older MS-CHAP version for Windows 95 servers
•	Microsoft CHAP Version 2 (MS-CHAP v2)
	Windows logon name and password (and domain if any)

CCIE Security Lab Workbook Volume I Version 3.0

	<u>S</u> etting
nponents checked are used by thi	connection:
Network Monitor Driver	
Internet Protocol (TCP/IP) Ele and Printer Sharipo for Mi	rosoft Networks
SNetwork Load Balancing	
Client for Microsoft Networks	
Install Uninstal	Properties
escription Ilows other computers to access r Ising a Microsoft network.	sources on your comput

	L2TP Tunnel Status	? ×
	General Details	
	- Connection	
	Statue	Connected
	Duration:	00.00.29
	Puratori.	00.00.23
	Activity	
	Sent — 🖳 —	- Received
	Butes: 4.978	317
	Compression: 0%	0%
	Errors: 0	0
	Properties Disconnect	
		Close
	L2TP Tunnel Status	
	General Details	
		1
	Property Value	
	Server type PPP	
	Authentication MS CHAP V	12
	IPSEC Encryption IPSec, ESP	3DES 🔜
	Compression (none)	
	PPP multilink framing Utf	
		Class
Al(config)# •	show crypto isakmp sa	
	men of the thermit be	
Active SA: 1) (A tunnel will report 1 Active or	d 1 Rekey SI during rekey)
tal IKE SA: 1		a i hency of during ierey /
TKE Peer: 1	0.0.100	
Type : u	ser Role : responder	2
		-

Copyright © 2007 Internetwork Expert

```
ASA1(config)# show cry ips sa
interface: outside
    Crypto map tag: DYNAMIC, seq num: 10, local addr: 136.1.123.12
      access-list L2TP permit udp any any eq 1701
      local ident (addr/mask/prot/port): (136.1.123.12/255.255.255.255/17/0)
      remote ident (addr/mask/prot/port): (10.0.0.100/255.255.255.255/17/1701)
      current_peer: 10.0.0.100, username: CISCO
      dynamic allocated peer ip: 20.0.0.1
      #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
      #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 24, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-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.: 136.1.123.12, remote crypto endpt.: 10.0.0.100
      path mtu 1500, ipsec overhead 58, media mtu 1500
      current outbound spi: A5D2904C
    inbound esp sas:
      spi: 0x9A975A34 (2593610292)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 125, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (kB/sec): (92766/712)
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xA5D2904C (2782040140)
         transform: esp-3des esp-md5-hmac none
         in use settings ={RA, Transport, }
         slot: 0, conn_id: 125, crypto-map: DYNAMIC
         sa timing: remaining key lifetime (kB/sec): (92771/712)
         IV size: 8 bytes
         replay detection support: Y
ASA1(config)# 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
     136.1.23.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:19, outside
R
     136.1.100.0 255.255.255.0 [120/1] via 136.1.123.3, 0:00:19, outside
R
     136.1.121.0 255.255.255.0 is directly connected, inside
С
     136.1.123.0 255.255.255.0 is directly connected, outside
C
     20.0.0.1 255.255.255.255 [1/0] via 136.1.123.3, outside
S
     10.0.0.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:19, outside
R
     150.1.2.0 255.255.255.0 [120/2] via 136.1.123.3, 0:00:19, outside
R
     150.1.1.0 255.255.255.0 [120/1] via 136.1.121.1, 0:00:03, inside
R
ASA1(config)# show vpn-sessiondb remote
```

Copyright © 2007 Internetwork Expert

Session Type:]	Remote			
Username	:	CISCO			
Index	:	1			
Assigned IP	:	20.0.0.1	Public IP	:	10.0.0.100
Protocol	:	L2TPOverIPSec	Encryption	:	3DES
Hashing	:	MD5			
Bytes Tx	:	1460	Bytes Rx	:	6572
Client Type	:	Microsoft	Client Ver	:	5.0
Group Policy	:	L2TP			
Tunnel Group	:	DefaultRAGroup			
Login Time	:	10:27:36 UTC Fri Jan 2	6 2007		
Duration	:	0h:05m:02s			
Filter Name	:				
NAC Result	:	N/A			
Posture Toker	1:				
ASA1(config)#	ŧ]	ping 20.0.0.1			
Type escape s	se	quence to abort.			
Sending 5, 10	0.	-byte ICMP Echos to 20.	0.0.1, timeout	: :	is 2 seconds:
Success rate	i	s 100 percent (5/5), ro	und-trip min/a	v	g/max = 40/40/40 ms

Further Reading

Configuring L2TP over IPSec L2TP Over IPsec Between Windows 2000/XP PC and PIX/ASA 7.2 Using Preshared Key

VPN3k and PPTP Client

Objective: Configure VPN3k to support users connecting via PPTP.



Directions

- Configure devices as per the scenario "VPN/Common Configurations" <u>"VPN3k Easy VPN/WebVPN"</u>.
- Create an IP address pool globally on VPN3k with address range "20.0.0.1-20.0.0.254".
- Configure default group to accept PPTP connections.
- Additionally, enable MSCAP for PPP authentication.
- Create a local user named "CISCO" with password "CISCO1234".
- Configure address assignment policy to use local address pools.
- Enable client reverse route injection.
- Configure PPTP client on Windows PC.

Final Configuration

VPN3k:

Change Base group settings:

Cisco Systems, Inc. VPN 3000 Concent	trator [¥PN3K] -	Microsoft Interne	t Explorer	
<u>Eile Edit View Favorites Tools H</u> e	lp (⇔ Back →	🖉 🚱	Address 🛃 https://136.3	1.113.11/access.html 🗾 🌆
VPN 300	0			Main Help Support Logout
Concentr	ator Series	Manager		Logged in: admir
			Config	uration Administration Monitoring
-Denfiguration Interfaces Co	onfiguration U	ser Managemer	nt Base Group	
G	eneral IPSec	Client Config	Client FW HW Clien	t PPTP/L2TP WebVPN NAC
Groups	18		General Parameter	'S
	Attribute		Value	Description
-D-Administration	Access Hours	-No Restrictions	-	Select the access hours for this group.
-⊞ <mark>Monitoring</mark>	Simultaneous Logins	3		Enter the number of simultaneous logins for users in this group.
	Minimum Pas <i>s</i> word Length	8		Enter the minimum password length for users in this group.
	Allow Alphabetic- Only Passwords	ঘ		Enter whether to allow users with alphabetic-only passwords to be added to this group.
CISCO SYSTEMS	Idle Timeout	30		(minutes) Enter the idle timeout for this group. When set to 0, WebVPN sessions use the Default Idle Timeout value specified in Configuration 1
Base Group/Default User Parameters				Internet

<u>File Edit View Favorites Tool</u>	oncentrator [¥PN3K] - s Help (⇒ Back →	Microsoft Interne • => • 区 😰	Address 🛃 https://136	.1.113.11/access.html	
VPN Conce	3000 entrator Series	Manager	Cunfi	Main Help Support L Logged in:	_ogout admin
<u>Configuration</u> <u>Interfaces</u>	Secondary DNS			Enter the IP address of the secondary DNS server.	
Httsvstem 	Primary WINS			Enter the IP address of the primary WINS server for this group.	
<u>Users</u> <u>Delicy Management</u> <u>Inneling and Security</u> <u>Administration</u> <u>Monitoring</u>	Secondary WINS			Enter the IP address of the secondary WINS server.	
	Tunneling Protocols	✓ PPTP ✓ L2TP ✓ IPSec ✓ L2TP over II ✓ L2TP over II ✓ WebVPN	?Sec	Select the tunneling protocols group can connect with.	this
	Strip Realm			Check to remove the realm qualifier of the username durin authentication.	g
	DHCP Network Scope			Enter the IP sub-network to which users within this group v be assigned when using the concentrator as a DHCP Pros	will sy.
Cisco Systems	Apply C	ancel			•

Enable PPTP as tunneling protocol

🖻 Cisco Systems, Inc. VPN 3000 Co	ncentrator [VPN3K] - Mie	rosoft Internet Explor	er	_ 🗆 ×
<u>File Edit View Favorites Tools</u>	Help 🗘 Back 👻	⇒ ∽ 区 😰 🛛 A <u>d</u> dre	ss 🙋 https://136.1.113.11/access.html	<u> </u>
VPN 3	3000		Main Help	Support Logout
Conce	ntrator Series N	Aanager		Logged in: admin
			Configuration Administr	ation Monitoring
<u> Configuration</u> <u> Interfaces</u> <u> System</u>	Configuration User Management Base Group			
	General IPSec (Client Config Client	FW HW Client PPTP/L2TP We	bVPN NAC
Base Group Groups		PPTP/L2	2TP Parameters	
	Attribute	Value	Description	
Handbergeneration Handbergeneration Holdeneration	Use Client Address		Check to accept and use an ${\rm I\!P}$ add from the client.	lress received
⊕- <u>Monitoring</u>	PPTP Authentication Protocols	□ PAP □ CHAP □ MSCHAPv1 □ MSCHAPv2 □ EAP Proxy	Check the authentication protocols to the online help for authentication dependencies. Unchecking all op that no authentication is require	allowed. Refer protocol tions means ed.
	PPTP Encryption	□ Required □ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption meth connections for this group.	ods for PPTP
	PPTP Compression		Check to enable MPPC compress connections for this group.	ion for PPTP
CISCO SYSTEMS	L2TP Authentication	□ PAP ☞ CHAP ☞ MSCHAPv1	Check the authentication protocols to the online help for authentication dependencies. Unchecking all on	allowed. Refer protocol tions means
Base Group/Default User Parameters			🕒 🤷 Int	ernet

Configure PPP Authentication:

Cisco Systems, Inc. VPN 3000 Cor	centrator [VPN3	K] - Microsoft Interne	t Explorer	- 🗆 ×
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help 🗘 Ba	ack 🔹 🔿 🔹 🛃	Address 🛃 https://136.1.113.11/access.html	-
VPN 3	000		Main Help Supp	ort Logout
Concer	ntrator Ser	ies Manager	Logg	ed in: admin
			Configuration Administration	Monitoring
	Configuratior	i User Managemer	t Users Add	
	This section le override group	ts you add a user. U o values. neral VIPSec VPPT	ncheck the Inherit? box and enter a new value t	>
<u>Tunneling and Security</u>	Includy Oc	I	lentity Parameters	
<u>Administration</u> Monitoring	Attribute Value Description			
	Username	CISCO	Enter a unique username.	
	Password	kololololololok	Enter the user's password. The password must s the group password requirements.	atisfy
	Verify	Actorication Actorication	Verify the user's password.	
	Group	-Base Group- 💌	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.	
CISCO SYSTEMS	Add	Cancel		
Ser Parameters				//

Add new user "CISCO" with password "CISCO1234":

Create an IP address pool (global):

🕗 Cisco Systems, Inc. VPN 3000 Co	ncentrator [¥PN3K] - Microsoft Interne	t Explorer	_ 🗆 🗙
<u>File Edit Yiew Favorites Tools</u>	: <u>H</u> elp	Address 🖉 https://136.1.113.11/access.html	
VPN 3	3000	Main Help	Support Logout
Conce	entrator Series Manager		Logged in: admin
		Configuration Administra	ntion Monitoring
Interfaces	Configuration System Address	Management Pools Add	
<u> </u>	Add an address pool.		
Pools	Range Start 20.0.0.1	Enter the start of the IP pool address rang	ge.
	Range End 20.0.0.254	Enter the end of the IP pool address rang	e.
	Subnet Mask 255.255.255.0 Add Cancel	Enter the subnet mask of the IP pool address rang Enter 0.0.0.0 to use default behavior.	z. ress range.
CISCO SYSTEMS			
IP Address Pools		📔 🖉 Inte	ernet //

Configure address assignment from local pools:


Enable Client RRI:



Verification

Lost name or IP address of destination (123.45.6.78): 136.1.113[11 First connect Windows can first connect the public Internet, before trying to establish this Dial another connection first:	such as microsoft.com or network, such as the virtual connection.	
	¥	

	piton (connect even if no enclypiton)
Logon securi	ty
C Use <u>E</u> xte	nsible Authentication Protocol (EAP)
	<u>×</u>
	Properties
Allow the	se protocols
<u>Г</u> <u>U</u> ne	ncrypted password (PAP)
□ <u>S</u> hiv	a Password Authentication Protocol (SPAP)
🗖 <u>C</u> hal	lenge Handshake Authentication Protocol (CHAP)
Micr	osoft CHAP (MS-CHAP)
	Allow older MS-CHAP version for <u>W</u> indows 95 servers
🔽 Mjer	osoft CHAP Version 2 (MS-CHAP v2)
E Ford	45 CHAP based protocols automatically use mu
Wind	dows logon name and password (and domain if any)

TO_VPN3000 ? X
General Options Security Networking Sharing
Type of VPN server 1 am calling:
Point to Point Tunneling Protocol (PPTP)
<u>S</u> ettings
Components checked are used by this connection:
Internet Protocol (TCP/IP) Image: Strain S
Install Uninstall Properties
OK Cancel
Connect TO_VPN3000
User name: CISCO
Password: Save Password
Courses I Course I Hole

<u>Edit View Favorites T</u> ools	; Help 🦙 B	ack ·	•=> • (•) 🗄) A <u>d</u> dr	ess 🎑 ht	tps://136.1.11	3.11/access.	html	-
VPN 3	3000							Main	Help S	upport Lo
Conce	entrator Ser	ries	6 Mana	igen	ľ				L	ogged in: a
							Configura	tion Adn	ninistrat	ion Monit
nfiguration	LAN-to-1	LAN-to-LAN Sessions				(emote 4	Access Sessi	ions Man	agemen	t Sessions
<u>ninistration</u> nitoring Routing Table	Connectio Name	on	IP Address	Pr	otocol E	ncryptio	on Login Time	Duration	n Byte Tx	s Bytes Rx
Dynamic Filters DFilterable Event Log DSystem Status System Status		No LAN-to-LAN Sessions								
	Username		signed Address blic IP	Gro		otocol ryption	Login Time Duration	<u>Client</u> <u>Type</u> Version	<u>Bytes</u> <u>Tx</u> <u>Bytes</u>	<u>NAC</u> <u>Result</u> <u>Posture</u>
		20 10.	0.0.0.1 0.0.100	Ba Gro	se P up RC	PTP 4-128 ateless	Jan 29 23:46:26 0:01:14	N/A N/A	12 1609	<u>I oken</u> Unknown
	Managen Administra	ient itor	Session IP Addr	as ess	[<u>L</u> 4 Protocol	N-to-L.	AN Session cryption	s <u>Remote</u> Login	Access	Sessions
CISCO SYSTEMS	admin		10.0.0.1	00	HTTP	3DES-	168 SSLv3	Jan 29 2	3:47:13	0:00:26

Check connected sessions on VPN3k:

Further Reading

Configuring the VPN 3000 Concentrator PPTP With Cisco Secure ACS for Windows RADIUS Authentication

Using ISAKMP Profiles

Objective: Configure router to support ezVPN client connections and IPsec LAN-to-LAN connections simultaneously.



Directions

- Pre-configure devices as follows:
 - Create the necessary VLANs, and configure the switchports respectively as per the diagram.
 - Configure IP addressing as per the diagram.
 - Configure RIP as routing protocol on all devices.
 - Advertise Loopback interfaces on R1 and R2 into RIP.
- The goal is to provide support for remote ezVPN clients as well as L2L connections terminating on the same router and the same interface.
- This is possible withf "ISAKMP profiles" feature. As soon as ISAKMP negotiations reveal client's identity, it is possible to apply certain ISAKMP policies to a given client.
- Specifically you may decide to enable Xauth and Mode Config for a client group.
- Configure access-control on the ASA to permit IPsec traffic as follows:
 - Create and apply to the outside interface access-list OUTSIDE_IN:
 - Permit ISAKMP traffic from outside.
 - Permit ESP traffic from outside.
- We are going to configure L2L tunnel on R1 to use IKE Aggressive mode along with hostname identity.
- Configure an IPsec LAN-to-LAN tunnel on R1 as follows:

- o Configure hostname "R1" and domain-name "internetworkexpert.com".
- o Create ISAKMP profile named "AGGRESSIVE":
 - Initiate aggressive mode.
 - Use hostname (FQDN) for identity.
 - Use the default keyring.
- Create ISAKMP policy with priority 10:
 - Use pre-shared keys authentication.
 - Use 3DES for cipher.
 - Use MD5 for hash.
 - Use DH Group 2.
- Create ISAKMP key "LAN2LAN" for address 136.X.122.2 (R2).
- Create transform-set 3DES_MD5
 - Use 3DES for cipher.
 - Use MD5 for hash.
- Create access-list "LO1_TO_LO2":
 - Permit IP traffic from 150.X.1.0/24 to 150.X.2.0/24.
- Create crypto-map VPN entry 10 of type IPsec-ISAKMP
 - Match address LO1_TO_LO2.
 - Set peer 136.X.122.2.
 - Set transform-set 3DES_MD5.
- Associate ISAKMP profile "AGGRESSIVE" with crypto map "VPN".
- Apply crypto-map "VPN" to interface E0/0.
- Configure common IPsec settings on R2 as follows:
 - Create ISAKMP policy as follows:
 - Authentication via pre-shared key.
 - Encryption 3DES.
 - Hash MD5.
 - DH Group 2 (to match DH group of ezVPN client).
 - Create IPsec transform-set 3DES MD5 as follows:

- Use 3DES cipher.
- Use MD5 hash.
- Configure IPsec settings for ezVPN server on R2 as follows:
 - Enable and configure AAA as follows:
 - Disable authentication on the console line.
 - Create AAA list "EZVPN" for local login authentication.
 - Create AAA list "EZVPN" for local network authorization.
 - Create local username "CISCO" with password "CISCO1234".
 - Create local address pool named "EZVPN" with address range "20.0.0.1-20.0.0.254".
 - Assign this pool to the ISAKMP client configuration process.
 - Create ISAKMP profile named "EZVPN" as follows:
 - Match remote group named "EZVPN".
 - Enable client authentication via AAA list "EZVPN".
 - Enable ISAKMP authorization using AAA list "EZVPN".
 - Respond to configuration mode requests.
 - Create split access-list named "SPLIT_TUNNEL" and permit only network "136.1.0.0/16" within.
 - Create ISAKMP client configuration group named "EZVPN" as follows:
 - Configure pre-shared key "EZVPN".
 - Use local address pool "EZVPN".
 - Use split access-list "SPLIT_TUNNEL".
 - Create dynamic crypto map named "DYNAMIC" as follows:
 - Set transform-set 3DES_MD5.
 - Enable RRI.
- Configure IPsec settings for L2L tunnel on R2 as follows:
 - Create crypto keyring named "LAN2LAN":
 - Assign key "LAN2LAN" to host "R1.internetworkexpert.com"
 - Create ISAKMP profile "LAN2LAN" as follows:

- Match identity based on domain-name "internetworkexpert.com".
- Use address as self-identity.
- Use keyring "LAN2LAN".
- Create access-list "LO2_TO_LO1" to match traffic from Loopback0 of R2 to Loopback0 of R1.
- Create crypto-map named "VPN" entry 10 on R2 as follows:
 - Match address "LO2_TO_LO1".
 - Set transform-set "3DES_MD5".
 - Set peer 136.1.121.1
- Create crypto-map named "VPN" entry 20 on R2 to use dynamic crypto map named "DYNAMIC".
- Apply crypto map VPN to interface Ethernet 0/0.

Final Configuration

```
Pre-Configuration
```

```
ASA1:
1
! IP addressing
1
interface Ethernet0/0
no shut
nameif outside
security-level 0
ip address 136.1.122.12 255.255.255.0
!
interface Ethernet0/1
no shut
 nameif inside
 security-level 100
ip address 136.1.121.12 255.255.255.0
!
! RIP configuration
!
router rip
 version 2
no auto-summary
 network 136.1.0.0
SW1 & SW2:
!
! create VLANs and configure trunk links
1
vlan 121,122
interface range Fa 0/21 - 23
 switchport trunk encapsulation dotlq
 switchport mode trunk
no shut
```

```
SW1:
!
! Configure switchports
I
interface Fa 0/1
switchport host
switchport access vlan 121
T
interface Fa 0/2
switchport host
switchport access vlan 122
SW2:
!
! Configure switchports
!
interface Fa 0/12
switchport host
switchport access vlan 122
!
interface Fa 0/20
switchport host
switchport access vlan 121
R1:
interface E 0/0
no shut
ip add 136.1.121.1 255.255.255.0
!
interface Loopback0
ip address 150.1.1.1 255.255.255.0
1
router rip
ver 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E 0/0
no shut
ip add 136.1.122.2 255.255.255.0
T
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 150.1.0.0
ASA1:
access-list OUTSIDE_IN extended permit udp any any eq isakmp
access-list OUTSIDE_IN extended permit esp any any
!
access-group OUTSIDE_IN in interface outside
ISAKMP Profiles:
R1:
```

Copyright © 2007 Internetwork Expert

```
hostname R1
ip domain-name internetworkexpert.com
1
! Create ISAKMP profile for aggressive mode
1
crypto isakmp profile AGGRESSIVE
  self-identity fqdn
  initiate mode aggressive
  keyring default
!
! Configure ISAKMP policy & PSK
!
crypto isakmp policy 10
authentication pre-share
hash md5
 encryption 3des
 group 2
I
crypto isakmp key LAN2LAN address 136.1.122.2
!
! Create transform set
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! Access-List to classify VPN traffic
I
ip access-list extended LO1_TO_LO2
 permit ip 150.1.1.0 0.0.0.255 150.1.2.0 0.0.0.255
!
! Create crypto-map
1
crypto map VPN 10 ipsec-isakmp
match address LO1_TO_LO2
set transform 3DES_MD5
set peer 136.1.122.2
!
! Associate profile with crypto map
!
crypto map VPN isakmp-profile AGGRESSIVE
1
! Apply the crypto map
1
interface E 0/0
crypto map VPN
R2:
!
! COMMON CONFIG
!
!
! Create ISAKMP policy (Phase 1) common to L2L and ezVPN clients
!
crypto isakmp policy 10
authentication pre-share
 hash md5
encryption 3des
group 2
!
!
! Create transform set
```

Copyright © 2007 Internetwork Expert

```
crypto ipsec transform-set 3DES_MD5 esp-3des esp-md5-hmac
1
! EZVPN CONFIG
1
!
! Configure AAA stuff required for ezVPN
1
aaa new-model
! Disable console auth
1
aaa authentication login CONSOLE none
!
! Define AAA lists we referenced in ezVPN ISAKMP profile
!
aaa authentication login EZVPN local
aaa authorization network EZVPN local
!
! Create a user for Xauth
1
username CISCO password CISCO1234
1
! Configure local address pool for remote users
! Configure ISAKMP to use this address pool
ip local pool EZVPN 20.0.0.1 20.0.0.254
crypto isakmp client configuration address-pool local EZVPN
1
! ISAKMP policy specific for ezVPN clients (they have group ID)
! Note Mode Config and Xauth configuration
crypto isakmp profile EZVPN
  match identity group EZVPN
  client authentication list EZVPN
  isakmp authorization list EZVPN
  client configuration address respond
!
! Split-tunnel ACL for remote ezVPN users
ip access-list extended SPLIT_TUNNEL
permit ip 136.1.0.0 0.0.0.255 any
!
! ISAKMP group policy for ezVPN group named "EZVPN"
!
crypto isakmp client configuration group EZVPN
 key EZVPN
 pool EZVPN
  acl SPLIT_TUNNEL
I
! Dynamic crypto map for ezVPN clients
!
crypto dynamic-map DYNAMIC 10
 set transform-set 3DES_MD5
 reverse-route
1
! LAN2LAN TUNNEL CONFIG
!
```

```
! Create a keyring for L2L connections
!
crypto keyring LAN2LAN
 pre-shared-key hostname R1.internetworkexpert.com key LAN2LAN
I
! Create a profile to match incoming L2L connection
!
crypto isakmp profile LAN2LAN
  keyring LAN2LAN
  self-identity address
   match identity host domain internetworkexpert.com
1
! Access-List to classify L2L VPN traffic
1
ip access-list extended LO2_TO_LO1
  permit ip 150.1.2.0 0.0.0.255 150.1.1.0 0.0.0.255
!
! COMMON CONFIG
!
1
! Create crypto-map
1
crypto map VPN 10 ipsec-isakmp
match address LO2_TO_LO1
set transform 3DES MD5
set peer 136.1.121.1
!
! Dynamic entry
I
crypto map VPN 20 ipsec-isakmp dynamic DYNAMIC
!
! Apply crypto map to Ethernet interface
1
interface E 0/0
crypto map VPN
```

Verification

```
Initiate L2L tunnel from R1:
R1#ping 150.1.2.2 source loopback 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
Packet sent with a source address of 150.1.1.1
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/12 ms
Snip from the output of "debug crypto isakmp" command on R1:
*Mar 1 01:32:47.040: ISAKMP: received ke message (1/1)
*Mar 1 01:32:47.040: ISAKMP (0:0): SA request profile is AGGRESSIVE
*Mar 1 01:32:47.040: ISAKMP: local port 500 remote port 500
      1 01:32:47.040: ISAKMP: local port 500, remote port 500
*Mar 1 01:32:47.040: ISAKMP: set new node 0 to QM_IDLE
*Mar 1 01:32:47.044: ISAKMP: insert sa successfully sa = 82E36154
*Mar 1 01:32:47.044: ISAKMP (0:1): Found ADDRESS key in keyring default
*Mar 1 01:32:47.044: ISAKMP (0:1): constructed NATET worder 02 TP
      1 01:32:47.044: ISAKMP (0:1): constructed NAT-T vendor-03 ID
*Mar 1 01:32:47.044: ISAKMP (0:1): constructed NAT-T vendor-02 ID
```

Copyright © 2007 Internetwork Expert

*Mar 1 01:32:47.321: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_FQDN *Mar 1 01:32:47.325: ISAKMP (1): ID payload next-payload : 13 : 2 type FQDN name : R1.internetworkexpert.com protocol : 17 : 0 port length : 29 Snip of output from the "debug crypto isakmp" command on R2: *Mar 1 01:34:05.725: ISAKMP (5): Process ID payload type : 2 FQDN name : R1.internetworkexpert.com protocol : 17 : 0 port length : 25 *Mar 1 01:34:05.725: ISAKMP (0:5): peer matches LAN2LAN profile *Mar 1 01:34:05.725: ISAKMP: Looking for a matching key for 136.1.121.1 in default *Mar 1 01:34:05.729: ISAKMP: Looking for a matching key for 136.1.121.1 in TAN2TAN *Mar 1 01:34:05.729: ISAKMP: Looking for a matching key for 136.1.121.1 in EZVPN : success *Mar 1 01:34:05.729: ISAKMP (0:5): processing vendor id payload *Mar 1 01:34:05.729: ISAKMP (0:5): vendor ID seems Unity/DPD but major 157 mismatch *Mar 1 01:34:05.729: ISAKMP (0:5): vendor ID is NAT-T v3 *Mar 1 01:34:05.729: ISAKMP (0:5): processing vendor id payload *Mar 1 01:34:05.729: ISAKMP (0:5): vendor ID seems Unity/DPD but major 123 mismatch 1 01:34:05.733: ISAKMP (0:5): vendor ID is NAT-T v2 *Mar *Mar 1 01:34:05.733: ISAKMP (0:5): Found HOST key in keyring LAN2LAN *Mar 1 01:34:05.733: ISAKMP (0:5) local preshared key found *Mar 1 01:34:05.733: ISAKMP : Scanning profiles for xauth ... LAN2LAN EZVPN Self-ID on R2. Note that R1 and R2 use different ID types! *Mar 1 01:34:06.367: ISAKMP (5): ID payload next-payload : 10 type : 1 : 136.1.122.2 addr protocol : 17 : 0 port length : 8 *Mar 1 01:34:06.367: ISAKMP (5): Total payload length: 12 *Mar 1 01:34:06.367: ISAKMP (0:5): constructed HIS NAT-D *Mar 1 01:34:06.367: ISAKMP (0:5): constructed MINE NAT-D *Mar 1 01:34:06.367: ISAKMP (0:5): sending packet to 136.1.121.1 my_port 500 peer_port 500 (R) AG_INIT_EXCH *Mar 1 01:34:06.371: ISAKMP (0:5): Input = IKE MESG FROM PEER, IKE AM EXCH *Mar 1 01:34:06.371: ISAKMP (0:5): Old State = IKE_READY New State = IKE_R_AM2 *Mar 1 01:34:06.747: ISAKMP (0:5): received packet from 136.1.121.1 dport 500 sport 500 Global (R) AG_INIT_EXCH *Mar 1 01:34:06.751: ISAKMP (0:5): processing HASH payload. message ID = 0 1 01:34:06.751: ISAKMP:received payload type 17 *Mar *Mar 1 01:34:06.751: ISAKMP (0:5): Detected NAT-D payload *Mar 1 01:34:06.751: ISAKMP (0:5): recalc my hash for NAT-D *Mar 1 01:34:06.751: ISAKMP (0:5): NAT match MINE hash

Copyright © 2007 Internetwork Expert



Copyright © 2007 Internetwork Expert

```
PERMIT, flags={}
 #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.: 136.1.122.2, remote crypto endpt.: 136.1.121.200
 path mtu 1500, media mtu 1500
  current outbound spi: 868AECA9
  inbound esp sas:
   spi: 0x74428D90(1950518672)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2004, flow_id: 5, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4462340/3457)
     IV size: 8 bytes
     replay detection support: Y
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x868AECA9(2257251497)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2005, flow_id: 6, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4462340/3457)
     IV size: 8 bytes
     replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
protected vrf:
local ident (addr/mask/prot/port): (150.1.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (150.1.1.0/255.255.255.0/0/0)
current_peer: 136.1.121.1:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 13, #pkts encrypt: 13, #pkts digest 13
 #pkts decaps: 13, #pkts decrypt: 13, #pkts verify 13
 #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.: 136.1.122.2, remote crypto endpt.: 136.1.121.1
  path mtu 1500, media mtu 1500
  current outbound spi: FBC85DAB
  inbound esp sas:
   spi: 0xD81A6A49(3625609801)
     transform: esp-3des esp-md5-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 2002, flow_id: 3, crypto map: VPN
     sa timing: remaining key lifetime (k/sec): (4449378/646)
     IV size: 8 bytes
     replay detection support: Y
```

```
Copyright © 2007 Internetwork Expert
```

CCIE Security Lab Workbook Volume I Version 3.0

```
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xFBC85DAB(4224212395)
  transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2003, flow_id: 4, crypto map: VPN
    sa timing: remaining key lifetime (k/sec): (4449378/644)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Further Reading

Cisco - DMVPN and Easy VPN Server with ISAKMP Profiles

IOS Firewall

Common Configuration

Objective: Pre-configure devices for IOS firewall scenarios.



Directions

- Create VLANs 13, 23 on SW1 and SW2 and assign switchports to respective VLANs.
- Configure IP addressing as per the diagram, create Loopback0 interfaces on R1 and R2.
- Configure RIP as routing protocol between R1, R2, and R3. Advertise Loopback0 interfaces on R1 and R2 into RIP.

Final Configuration

```
SW1 & SW2:
vlan 13,23
!
! Configure trunks
1
interface range Fa0/21 - 23
switchport trunk encaps dotlq
switchport mode trunk
SW1:
interface Fa0/1
switchport host
switchport access vlan 13
!
interface Fa0/2
switchport host
switchport access vlan 23
1
interface Fa0/3
switchport host
switchport access vlan 13
SW2:
interface Fa0/3
```

Copyright © 2007 Internetwork Expert

```
switchport host
 switchport access vlan 23
R1:
interface E0/0
no shut
ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E0/0
no shut
ip address 136.1.23.2 255.255.255.0
!
interface Loopback0
ip address 150.1.2.2 255.255.255.0
!
router rip
 ver 2
no auto
network 136.1.0.0
network 150.1.0.0
R3:
interface E0/0
no shut
ip address 136.1.13.3 255.255.255.0
!
interface E0/1
no shut
ip address 136.1.23.3 255.255.255.0
!
router rip
ver 2
no auto
 network 136.1.0.0
```

Verification

```
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, 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
```

Copyright © 2007 Internetwork Expert

Gateway of last resort is not set 136.1.0.0/24 is subnetted, 2 subnets 136.1.13.0 is directly connected, Ethernet0/0 C 136.1.23.0 [120/1] via 136.1.13.3, 00:00:01, Ethernet0/0 R 150.1.0.0/24 is subnetted, 2 subnets 150.1.2.0 [120/2] via 136.1.13.3, 00:00:01, Ethernet0/0 R 150.1.1.0 is directly connected, Loopback0 С R2#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, 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 136.1.0.0/24 is subnetted, 2 subnets 136.1.13.0 [120/1] via 136.1.23.3, 00:00:09, Ethernet0/0 R С 136.1.23.0 is directly connected, Ethernet0/0 150.1.0.0/24 is subnetted, 2 subnets С 150.1.2.0 is directly connected, Loopback0 150.1.1.0 [120/2] via 136.1.23.3, 00:00:09, Ethernet0/0 R R2#ping 150.1.1.1 source loopback 0 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds: Packet sent with a source address of 150.1.2.2 ..!!! Success rate is 60 percent (3/5), round-trip min/avg/max = 4/4/4 ms

Basic Access-Lists

Objective: Configure router to implement basic filtering policy using extended access-lists.



Directions

- Configure devices as per the scenarion "IOS Firewall/Access Lists" "<u>Common Configuration</u>".
- Conside R1 to be on the inside of the firewall, and R2 on the outside.
- Apply ingress and egress access-lists to interface E0/1 of R3.
- The security policy states the following permissions for inside networks:
 - Permit access to WWW applications.
 - Permit remote access to outside servers via standard virtual terminal access protocols.
 - Permit access to e-mail send/receive services.
 - Inside users should be able use outside DNS and access outside FTP servers by means of active FTP mode.
 - Inside users should be able to traceroute and ping to outside.
- The security policy states the following permissions for outside networks:
 - Inside server at IP address "150.1.1.1" should be accessible from outside via HTTP and active FTP.
 - Inside server should be protected from "fragmented" attacks.
 - Packets for sessions initiated from inside should be permitted. For TCP sessions, use only one line of access-list configuration.
 - Make sure pMTU discovery process works.
- The key problem with basic access-list is that they have no idea of sessions tracking, i.e. they are stateless. So if you permit a packet from inside wint egress ACL, you should make sure that there is a mirrored entry within ingress ACL.
- Remember the common protocols port numbers.

- Also, keep in mind that popular FTP protocol has two functional modes:
 - Active, where client connects to server on port 21, and server opens data connection source from port 20 back to client on port specified by client.
 - Passive, where client connects to server, server tells client the port number for data connection, and client initiates data connection on that port.
- Know that common UNIX and IOS traceroute implementation sends out UDP packets on port range "33434-33464" by default, and awaits two kinds of ICMP messages in reply "Time-Exceeded" or "Port-Unreachable".
- Additionally, pMTU discovery process needs ICMP message type 3 with code 4 "Packet too Big" to be permitted from outside.
- Remember that you may permit packets from established TCP session using keyword "established" in access-list entry. It actually matches any packets having "ACK" or "RST" bits set.
- You can match non-initial fragments of IP traffic using "fragments" keyword. Remember tht non-initial fragments have no information about upper level protocol, such as ports.
- Always remember that router-generated traffic is not inspected by egress access-lists. However, the returning traffic is subject to check by ingress ACL, so make sure you permitted any routing and management traffic.
- Make a useful habit of adding an explicit "deny ip any any log" at the end of your access-lists. This may greatly easy the troubleshooting on your lab exam.
- Bearing this in mind, create an extended access-list OUTBOUND to reflect security policy as follows:
 - Permit TCP from any to ports 80, 443, 23, 22, 25, 110/143 (HTTP, HTTPs, Telnet, SSH, SMTP, POP3/IMAP)
 - Permit UDP from any to port 53 (DNS)
 - Permit TCP from any to ports 21, 20 (Active FTP)
 - Permit UDP from any to port range 33434 33464 (UNIX style traceroute)
 - Permit ICMP echo from any to any
 - Permit TCP from host 150.1.2.100 ports 80 and 20, 21 to any (HTTP/Active FTP traffic returning from internal server)
- Create an extended access-list INBOUND as follows:
 - Permit RIP traffic
 - o Deny any non-initial fragments to internal servers' global address
 - Permit TCP from any to 150.1.2.100 ports 80 and 20, 21 (HTTP, FTP)
 - Permit TCP established sessions from any

- o Permit returning DNS traffic
- Permit inbound ICMP echo-reply, port-unreachable, and timeexceeded (Ping-reply, Traceroute)
- Permit inbound ICMP packet-too-big (pMTU discovery)

Final Configuration

```
R3:
!
! Egress ACL
!
ip access-list extended OUTBOUND
remark == HTTP/HTTPs
remark == SSH/Telnet
permit tcp any any eq 80
 permit tcp any any eq 443
 permit tcp any any eq 22
 permit tcp any any eq 23
 remark == SMTP POP3/IMAP DNS
 permit tcp any any eq 25
 permit tcp any any eq 110
 permit tcp any any eq 143
 permit udp any any eq 53
 remark == FTP, Traceroute, Pings
 permit tcp any any range 20 21
 permit udp any any range 33434 33464
 permit icmp any any echo
 remark == Traffic from internal server (HTTP/FTP)
 permit tcp host 150.1.1.1 eq 80 any
 permit tcp host 150.1.1.1 range 20 21 any
 deny ip any any log
1
! Ingress ACL
1
ip access-list extended INBOUND
 remark == Permit inbound RIP updates
permit udp any any eq rip
 remark == Block non-initial frags to server
 deny ip any host 150.1.1.1 fragments
 remark == Permit HTTP/Active FTP to server
 permit tcp any host 150.1.1.1 eq 80
 permit tcp any host 150.1.1.1 range 20 21
 remark == Returning TCP traffic for inside TCP session
```

CCIE Security Lab Workbook Volume I Version 3.0

```
permit tcp any any established
remark == Active FTP data channel
permit tcp any eq 20 any
remark == Returning DNS traffic
permit udp any eq 53 any
remark == Pings, Traceroute and pMTU disc returning traffic
permit icmp any any echo-reply
permit icmp any any port-unreachable
permit icmp any any time-exceeded
permit icmp any any packet-too-big
deny ip any any log
1
! Apply access-lists
interfac E0/1
 ip access-group OUTBOUND out
 ip access-group INBOUND in
```

Verification

```
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (8 matches)
    20 deny ip any host 150.1.1.1 fragments
   30 permit tcp any host 150.1.1.1 eq www
    40 permit tcp any host 150.1.1.1 range ftp-data ftp
   50 permit tcp any any established
   60 permit tcp any eq ftp-data any
   70 permit udp any eq domain any
   80 permit icmp any any echo-reply
   90 permit icmp any any port-unreachable
   100 permit icmp any any time-exceeded
   110 permit icmp any any packet-too-big
   120 deny ip any any log
Extended IP access list OUTBOUND
   10 permit tcp any any eq www
    20 permit tcp any any eq 443
   30 permit tcp any any eq 22
   40 permit tcp any any eq telnet
   50 permit tcp any any eq smtp
   60 permit tcp any any eq pop3
   70 permit tcp any any eq 143
   80 permit udp any any eq domain
   90 permit tcp any any range ftp-data ftp
   100 permit udp any any range 33434 33464
   110 permit icmp any any echo
    120 permit tcp host 150.1.1.1 eq www any
   130 permit tcp host 150.1.1.1 range ftp-data ftp any
    140 deny ip any any log
R1#ping 150.1.2.2
```

Copyright © 2007 Internetwork Expert

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R1#trace 150.1.2.2
Type escape sequence to abort.
Tracing the route to 150.1.2.2
  1 136.1.13.3 4 msec 0 msec 0 msec
  2 136.1.23.2 4 msec * 0 msec
R1#telnet 150.1.2.2
Trying 150.1.2.2 ... Open
Password required, but none set
[Connection to 150.1.2.2 closed by foreign host]
R1#telnet 150.1.2.2 80
Trying 150.1.2.2, 80 ... Open
R1#disc 1
Closing connection to 150.1.2.2 [confirm]
R1#telnet 150.1.2.2 8080
Trying 150.1.2.2, 8080 ...
% Destination unreachable; gateway or host down
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (34 matches)
    20 deny ip any host 150.1.1.1 fragments
    30 permit tcp any host 150.1.1.1 eq www
    40 permit tcp any host 150.1.1.1 range ftp-data ftp
    50 permit tcp any any established (16 matches)
    60 permit tcp any eq ftp-data any
70 permit udp any eq domain any
    80 permit icmp any any echo-reply (11 matches)
    90 permit icmp any any port-unreachable (2 matches)
    100 permit icmp any any time-exceeded
    110 permit icmp any any packet-too-big
    120 deny ip any any log
Extended IP access list OUTBOUND
    10 permit tcp any any eq www (12 matches)
    20 permit tcp any any eq 443
    30 permit tcp any any eq 22
    40 permit tcp any any eq telnet (20 matches)
    50 permit tcp any any eq smtp
    60 permit tcp any any eq pop3
    70 permit tcp any any eq 143
    80 permit udp any any eq domain
    90 permit tcp any any range ftp-data ftp
    100 permit udp any any range 33434 33464 (3 matches)
    110 permit icmp any any echo (10 matches)
    120 permit tcp host 150.1.1.1 eq www any
    130 permit tcp host 150.1.1.1 range ftp-data ftp any
    140 deny ip any any log (1 match)
R2>ping 150.1.1.1
Type escape sequence to abort.
```

Copyright © 2007 Internetwork Expert

Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5) R2>telnet 150.1.1.1 80 Trying 150.1.1.1, 80 ... Open R2>disc 1 Closing connection to 150.1.1.1 [confirm]

Further Reading

Transit Access Control Lists: Filtering at Your Edge Path Maximum Transmission Unit (PMTU) Black Hole-Router Cisco - Access Control Lists and IP Fragments

Reflexive Access-Lists

Objective: Configure router to filter traffic using reflexive access-lists.



Directions

- Configure devices as per the scenario "IOS Firewall/Access Lists" "<u>Common Configuration</u>".
- The goal is to permit TCP/UDP/ICMP traffic from R1 to R2, but not vice versa. This could be achieved using the concept of reflective ACL.
- The idea of reflexive ACL is pretty simple: take a packet flow, extract session information (src/dst IP and ports) and create dynamic entry in access-list that is applied in opposite direction, to permit the "mirrored" traffic flow.
- This basic "session" idea works well with most simple protocols, like HTTP and Telnet. However, complex protocols like FTP has more complex behavior, which could not be interpreted properly by simply reflecting a traffic flow.
- Additionally, reflexive ACLs scales poorly, since router open all the pinholes temporarily and needs to age them out, constantly keeping the track of every new "session".
- Also, by default a router-originated traffic is not subject to "reflection", unless you use local policy routing to divert it into loopback interface, therefore making it "ingress".
- Create access-list OUTBOUND on R3 as follows:
 - Permit TCP traffic from any to any, and reflect sessions into access-list named "MIRROR".
 - Configure the same behavior for ICMP and UDP traffic.
- Create access-list INBOUND on R3 as follows:
 - Evaluate the access list named "MIRROR", i.e. permit only the mirrored sessions.

- Additionally, in order to "reflect" the local router RIP updates, create local policy routing as follows:
 - Create named access-list "RIP" and match UDP traffic from any to any port 520.
 - o Create interface Loopback0 with arbitraty IP address.
 - Create route-map named "LOCAL":
 - Match access-list "RIP" and set interface Loopback0
 - Apply this route-map as local policy.

Final Configuration

```
R3:
!
! Outbound access-list, mirror all outbound sessions
!
ip access-list extended OUTBOUND
permit tcp any any reflect MIRROR
permit udp any any reflect MIRROR
permit icmp any any reflect MIRROR
!
! Ingress ACL, permit only the "returning" packets
!
ip access-list extended INBOUND
evaluate MIRROR
!
! Select RIP traffic
!
ip access-list extended RIP
permit udp any any eq rip
!
! Create loopback for PBR
!
interface Loopback0
ip address 3.3.3.3 255.255.255.0
1
! Create route-map to divert RIP traffic to loopback
1
route-map LOCAL 10
match ip address RIP
set interface Loopback0
!
ip local policy route-map LOCAL
!
! Apply ACLs
1
interface E0/1
ip access-group OUTBOUND out
 ip access-group INBOUND in
```

Verification

```
With some IOS versions, local policy routing may refuse to route multicast
packets. Configure static RIP neighbors in such case:
R3:
router rip
neighbor 136.1.23.2
 passive E0/1
R2:
router rip
neighbor 136.1.23.3
passive E0/0
R3#show ip access-lists
Extended IP access list INBOUND
    10 evaluate MIRROR
Reflexive IP access list MIRROR
     permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (13 matches)
(time left 297)
Extended IP access list OUTBOUND
    10 permit tcp any any reflect MIRROR
    20 permit udp any any reflect MIRROR
    30 permit icmp any any reflect MIRROR
Extended IP access list RIP
    10 permit udp any any eq rip (15 matches)
R1>telnet 150.1.2.2
Trying 150.1.2.2 ... Open
R2>
R3#show ip access-lists
Extended IP access list INBOUND
    10 evaluate MIRROR
Reflexive IP access list MIRROR
     permit tcp host 150.1.2.2 eq telnet host 136.1.13.1 eq 11009 (31 matches)
(time left 294)
    permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (18 matches)
(time left 295)
Extended IP access list OUTBOUND
    10 permit tcp any any reflect MIRROR
    20 permit udp any any reflect MIRROR
    30 permit icmp any any reflect MIRROR
Extended IP access list RIP
    10 permit udp any any eq rip (19 matches)
R1>ping 150.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R1>
R3#show ip access-lists MIRROR
Reflexive IP access list MIRROR
     permit icmp host 150.1.2.2 host 136.1.13.1 (19 matches) (time left 292)
     permit udp host 136.1.23.2 eq rip host 136.1.23.3 eq rip (25 matches)
```

```
Copyright © 2007 Internetwork Expert
```

(time left 291)

Further Reading

<u>Configuring IP Session Filtering (Reflexive Access Lists)</u> <u>Cisco - Configuring Commonly Used IP ACLs</u>

Dynamic Access-Lists

Objective: Configure router for lock & key security with local AAA.



Directions

- Configure devices as per the scenario "IOS Firewall/Access Lists" "<u>Common Configuration</u>".
- Dynamic access-list is a type of access policy which is activated by a user logging into router.
- The key factor here is "access-enable" command, which activates all dynamic access entries in all access-lists.
- This command may be assigned to a particular user's profile, or be attached to a virtual terminal line.
- You may pass two optional arguments to "access-enable" command:
 - The "host" keyword, which create dynamic ACL entry ONLY for a host that triggered the authentication session.
 - The "timeout" keyword, which specifies inactivity timeout to remove the dynamic ACL entry.
- While creating dynamic template entry in access-list you may also specify "absolute" timeout with "timeout" keyword.
- If you have configured AAA on a router, remember to configure "exec" authorization appropriately, as by default exec commands are not authorized.
- To apply the dynamic ACL feature with AAA configure as follows:
 - Enable AAA, configure and apply AAA list to disable console authentication.
 - Configure local "exec" authorization.
 - Create user named "CISCO" with password "CISCO1234" and assign it autocommand "access-enable host timeout 10".
 - Create access-list "INBOUND" as follows:
 - Permit telnet traffic to IP address 136.X.23.3 (E0/1 of R3).
 - Permit RIP updates inbound.

- With dynamic entry named ACCESS permit ICMP traffic from any to any. Specify absolute timeout of 30 minutes.
- Deny and log everything else.
- Apply acess-list INBOUND to interface Ethernet 0/1 of R3.
- By configuring global command "access-list dynamic-extended" you permit users to extend absolute timeout by fixed value every time they reauthenticate with router.

Final Configuration

```
R3:
aaa new-model
aaa authentication login CONSOLE none
aaa authorization exec default local
1
username CISCO password CISCO1234
username CISCO autocommand access-enable host timeout 10
!
line con 0
login authentication CONSOLE
I
! Ingress ACL with dynamic templates
ip access-list extended INBOUND
permit tcp any host 136.1.23.3 eq 23
permit udp any any eq 520
dynamic ACCESS timeout 30 permit icmp any any
deny ip any any log
!
1
interface E0/1
ip access-group INBOUND in
```

Verification

```
R3#show ip access-lists
Extended IP access list INBOUND
   10 permit tcp any host 136.1.23.3 eq telnet
   20 permit udp any any eq rip (48 matches)
   30 Dynamic ACCESS permit icmp any any
   40 deny ip any any log
Extended IP access list RIP
   10 permit udp any any eq rip (271 matches)
R2#telnet 136.1.23.3
Trying 136.1.23.3 ... Open
User Access Verification
Username: CISCO
Password: CISCO1234
```

Copyright © 2007 Internetwork Expert

```
[Connection to 136.1.23.3 closed by foreign host]
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit tcp any host 136.1.23.3 eq telnet (723 matches)
    20 permit udp any any eq rip (93 matches)
    30 Dynamic ACCESS permit icmp any any
       permit icmp host 136.1.23.2 any
   40 deny ip any any log
Extended IP access list RIP
    10 permit udp any any eq rip (291 matches)
R2#ping 150.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.1.1.1, timeout is 2 seconds:
11111
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R2#
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit tcp any host 136.1.23.3 eq telnet (723 matches)
    20 permit udp any any eq rip (96 matches)
    30 Dynamic ACCESS permit icmp any any
       permit icmp host 136.1.23.2 any (5 matches) (time left 595)
   40 deny ip any any log
Extended IP access list RIP
    10 permit udp any any eq rip (291 matches)
```

Further Reading

Configuring Lock-and-Key Security (Dynamic Access Lists)

Stateful Inspection with CBAC

Objective: Configure router for stateful inspection of session traffic.



Directions

- Configure devices as per the scenario "IOS Firewall" "<u>Common</u> <u>Configuration</u>".
- CBAC is a stateful IOS firewall feature. Unlike reflexive ACL is has more intelligence, inspecting session traffic and parsing protocol operations.
- The way CBAC originally worked was as follows:
 - Apply pre-configured inspection rule to egress/ingress traffic (depends on configuration). Find out if there are any additional sessions that a protocol intiates (like FTP).
 - If there is an access-list configured in direction opposite to traffic flow, open a temporaty pinhole in it, permitting session traffic to come back.
 - Additionally, parse the protocol state-machine to find any misbehavior.
- With recent IOS versions, CBAC no longer "patch" access-lists, rather returning traffic is matched directly against state-table. This speed up the actual firewall traffic processing, but you won't see any more "pinholes" in access-lists.
- In this task we are going to apply the simple form of traffic inspection, processing generic TCP, UDP and ICMP sessions. Note that ICMP inspection as a new 12.2T feature, that was unavailable in original CBAC. With 12.3T an inspection of router-generated traffic was also added.
- Create inspection rule named INSPECT as follows:
 - Inspect TCP, UDP, ICMP traffic.
 - Additionally, inspect FTP traffic.
- Create access-list named "INBOUND" as follows:
 - Permit RIP routing updates
 - Deny & log everything else.

- Apply access-group "INBOUND" to E0/1 ingress direction.
- Apply inspection rule "INSPECT" to egress direction on interface E0/1.

Final Configuration

```
R3:

ip inspect name INSPECT tcp

ip inspect name INSPECT udp

ip inspect name INSPECT icmp

!

FTP-specific inspection

! Uses port-map to apply the rule

!

ip inspect name INSPECT ftp

ip access-list extended INBOUND

permit udp any any eq rip

deny ip any any log

interface E0/1

ip access-group INBOUND in

ip inspect INSPECT out
```

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name INSPECT
   tcp alert is on audit-trail is off timeout 3600
   udp alert is on audit-trail is off timeout 30
   icmp alert is on audit-trail is off timeout 10
   ftp alert is on audit-trail is off timeout 3600
Interface Configuration
 Interface Ethernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is INSPECT
   tcp alert is on audit-trail is off timeout 3600
   udp alert is on audit-trail is off timeout 30
   icmp alert is on audit-trail is off timeout 10
    ftp alert is on audit-trail is off timeout 3600
  Inbound access list is INBOUND
  Outgoing access list is not set
R3#show ip access-lists
Extended IP access list INBOUND
    10 permit udp any any eq rip (21 matches)
    20 deny ip any any log
```

R3#**show ip port-map ftp**

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

Default mapping: ftp system defined port 21 Inspection is not applied to route-generated traffic: R3#ping 150.1.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds: *Mar 1 17:01:17.914: %SEC-6-IPACCESSLOGDP: list INBOUND denied icmp 150.1.2.2 -> 136.1.23.3 (0/0), 1 packet.... Success rate is 0 percent (0/5)R1#ping 150.1.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 150.1.2.2, timeout is 2 seconds: 11111 Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms R1# R3#**sh** ip acce Extended IP access list INBOUND permit icmp any host 136.1.13.1 time-exceeded permit icmp any host 136.1.13.1 unreachable permit icmp any host 136.1.13.1 timestamp-reply permit icmp any host 136.1.13.1 echo-reply (5 matches) 10 permit udp any any eq rip (99 matches) 20 deny ip any any log (5 matches) R1#telnet 150.1.2.2 Trying 150.1.2.2 ... Open R2> R3#show ip inspect sessions Established Sessions Session 82C79F24 (136.1.13.1:11010)=>(150.1.2.2:23) tcp SIS_OPEN R3#sh ip acce Extended IP access list INBOUND permit tcp host 150.1.2.2 eq telnet host 136.1.13.1 eq 11010 (8 matches) 10 permit udp any any eq rip (105 matches) 20 deny ip any any log (5 matches)

Further Reading

Configuring Context-Based Access Control
CBAC Port-to-Application Mapping

Objective: Configure router to use non-standard ports for traffic inspection.



Directions

- Configure devices as per the scenario "IOS Firewall" <u>"Stateful Inspection</u> with CBAC".
- Imagine we have a web-server at 150.X.2.2 listening on port 21 and FTP server somewhere on outside network listening on port 8080.
- To inspect an application traffic, CBAC has a table of port-mappings. There are some system defined ports, like "21,80,25". You can not map HTTP service to port 21 directly, since it's system-defined. However, you can use an acess-list to specify list of "server" which have standard port re-mapped.
- Create a standard access-list number 99 and permit host 150.X.2.2 with it.
- Map application "HTTP" to port 21 for servers in access-list 99.
- Map FTP protocol to port 8080 globally.
- Add protocol HTTP to inspection rule "INSPECT".

Final Configuration

```
R3:
access-list 99 permit host 150.1.2.2
!
ip port-map http port 21 list 99
ip port-map ftp port 8080
!
ip inspect name INSPECT http
```

Verification

```
R3(config)#ip port-map http port 21
Command fail: the port 21 has already been defined for ftp by the system.
No change can be made to the system defined port mappings.
R3(config)#ip port-map http port 21 list 99
R3#show ip port-map | inc http
Host specific: http port 21 in list 99 user defined
```

Copyright © 2007 Internetwork Expert

Default mapping: http	port 80	system defined
R3 #show ip port-map inc Default mapping: tftp Default mapping: ftp Default mapping: ftp	ftp port 69 port 21 port 8080	system defined system defined user defined

Further Reading

Configuring Port to Application Mapping

Preventing DoS Attacks with CBAC

Objective: Configure router limit number of half-open sessions with CBAC feature.



Directions

- Configure devices as per the scenario "IOS Firewall" "<u>Common</u> <u>Configuration</u>".
- In addition to protocol inspection CBAC has built-in DoS prevention feature, similar to TCP intercept.
- However, in contrast to TCP intercept, CBAC intercept works with any inspected session, even UDP.
- The only supported mode, in comparison with TCP intercept, is "watch" mode: sessions are not proxied and are rather monitored. The equivalent to TCP Intercept "watch-timeout" is "tcp synwait-time" with CBAC.
- CBAC cessions are limited using two basic rate-limiting features:
 - Total number of half-open (non-established) session.
 - One-minute half-open sessions rate.
 - There are high and low limits for both limits.
- For TCP you may specify additional parameters as follows:
 - Connection establishment/inactivity/teardown timeouts.
 - Per-host limits & block time.
- You may also specify UDP sessions timeout and DNS session timeout separately.
- CBAC intercept feature is usually implemented to protect servers, rather than control users sessions, though there may be exceptions.
- Create inspection rule "PROTECT" as follows:
 Inspect TCP, UDP and ICMP traffic.
- Configure global CBAC intercept parameters as follows:
 - Start clamping when total number of half-open sessions reaches 1000, and stop when it falls below 900.

- Start clamping when one-minute rate reaches 100 and stop when it falls below 90.
- Set per-host limit of half-open sessions to 50. Block a host for 5 minutes when the threshold is reached.
- Set number of seconds spent in connection establishment phase for TCP to 15 seconds.
- Create an extended access-list named "INBOUND" as follows:
 - Permit RIP updates.
 - o Deny and log everything else.
- Apply inspection rule named "PROTECT" outbound on E0/0.
- Apply access-list "INBOUND" ingress on E0/0.

Final Configuration

```
R3:
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1000
ip inspect one-minute low 90
ip inspect one-minute high 100
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 50 block-time 5
ip inspect name PROTECT tcp
ip inspect name PROTECT udp
ip inspect name PROTECT icmp
ip access-list extended INBOUND
permit udp any any eq rip
deny ip any any log
interface E0/0
ip inspect PROTECT out
ip access-group INBOUND in
```

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [90:100] connections
max-incomplete sessions thresholds are [900:1000]
max-incomplete tcp connections per host is 50. Block-time 5 minutes.
tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name PROTECT
tcp alert is on audit-trail is off timeout 3600
udp alert is on audit-trail is off timeout 10
```

Copyright © 2007 Internetwork Expert

Interface Configuration Interface Ethernet0/0 Inbound inspection rule is not set Outgoing inspection rule is PROTECT tcp alert is on audit-trail is off timeout 3600 udp alert is on audit-trail is off timeout 30 icmp alert is on audit-trail is off timeout 10 Inbound access list is INBOUND Outgoing access list is not set Check to see if TCP SYN Wait timeout works: R3#debug ip inspect events INSPECT special events debugging is on R3# R2#telnet 150.1.1.100 3030 Trying 150.1.1.100, 3030 ... % Connection timed out; remote host not responding R3# *Mar 1 18:54:42.877: CBAC 136.1.23.2:11011 <- RST (150.1.1.100:3030) seq 0 wnd 4128 *Mar 1 18:54:42.877: CBAC (136.1.23.2:11011) RST -> 150.1.1.100:3030 seq 3660436220 wnd 0

Further Reading

Configuring Context-Based Access Control

CBAC Performance Tuning

Objective: Tune CBAC for effective router performance.



Directions

- Configure devices as per the scenario "IOS Firewall" <u>"Stateful Inspection</u> with CBAC".
- The core of CBAC algorithm is formed by protocol inspection logic and session state table. In order to make CBAC more effective under heavy load conditions, you should take in accountint the following:
 - State table is hashed structured, with configurable number of entries. Try to make hashtable size close to the average number of concurrect sessions passing through the firewall.
 - By default, protocol inspection logic generates alerts when it finds inconsistence in protocol tracking. This may cause additional CPU load under inensive traffic. Consider disable the alerts globally or per protocol in order to improve performance.
- There's also an additional CBAC feature called session audit. It permits you to log every session statistics for accounting or audit purposes naturally. Audit may be enable globally or per-protocol.
- In order to improve performance, disable CBAC alerts, but retain alerting for ICMP sessions.
- Keeping CBAC audit globally disabled, enable it for TCP sessions only.
- Change hashtable size to 4096, in order to accommodate to intensive traffic flow.

Final Configuration

```
R3:
ip inspect alert-off
!
ip inspect name INSPECT icmp alert on
!
! Audit trails
!
no ip inspect audit-trail
ip inspect name INSPECT tcp audit-trail on
```

Copyright © 2007 Internetwork Expert

Verification

```
R3#show ip inspect all
Session audit trail is disabled
Session alert is dlsabled
one-minute (sampling period) thresholds are [90:100] connections
max-incomplete sessions thresholds are [900:1000]
max-incomplete tcp connections per host is 50. Block-time 5 minutes.
tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name INSPECT
    tcp alert is off audit-trail is on timeout 3600
    udp alert is off audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is off audit-trail is off timeout 3600
Interface Configuration
 Interface Ethernet0/1
  Inbound inspection rule is not set
  Outgoing inspection rule is INSPECT
    tcp alert is off audit-trail is on timeout 3600
    udp alert is off audit-trail is off timeout 30
    icmp alert is on audit-trail is off timeout 10
    ftp alert is off audit-trail is off timeout 3600
  Inbound access list is INBOUND
  Outgoing access list is not set
Verify audit trails:
R1#telnet 150.1.2.2
Trying 150.1.2.2 ... Open
R2>exit
R3#
*Mar 1 20:34:34.483: %FW-6-SESS_AUDIT_TRAIL: tcp session initiator
(136.1.13.1:11011) sent 36 bytes -- responder (150.1.2.2:23) sent 44 bytes
```

Further Reading

<u>Cisco IOS Firewall Performance Improvements</u> <u>Configuring Context-Based Access Control</u>

Authentication Proxy with RADIUS

Objective: Configure router to filter traffic based on application-level criteria.



Directions

- Pre-configure devices as follows:
 - o Create VLANs 13, 23 and 100.
 - Configure IP addressing on Ethernet interfaces.
 - Configure Serial link between R3 and R2.
 - Configure RIP as routing protocol.
 - Create and advertise into RIP interface Loopback0 on R1.
- The idea behind Authentication Proxy is to download per-user access profile (ACL rules) and merge it with interface access-group.
- To authenticate user, an HTTP session is intercepted and authentication is performed by router.
- Configure Authentication Proxy settings on R3 as follows:
 - Enable AAA; configure & apply AAA list to disable console line authentication. This may have implications with some IOS versions, where HTTP server uses AAA list assigned to console for HTTP

authentication. If this is the case, configure console line in sync with HTTP authentication requirements.

- o Configure RADIUS server 10.0.0.100 with key CISCO.
- o Configure default login authentication via RADIUS.
- Configure auth-proxy authorization via RADIUS.
- Enable local HTTP server, and configure it to use AAA authentication.
- Create an authentication proxy rule named "PROXY" and apply it to interface E0/1.
- Create access-list 100 as follows:
 - Permit RIP updates.
 - Deny and log everythig else.
 - Apply access-group ingress to interface E0/1
- Configure ACS as follows:
 - Add R3 as RADIUS client.
 - Enable per-user RADIUS attributes and permit "Cisco AV-Pair" in user profiles.
 - Create user "PROXY" with password "CISCO1234" and create the following Cisco AV-Pair attributes:
 - auth-proxy:priv-lvl=15
 - auth-proxy:proxyacl#1=permit icmp any any
 - auth-proxy:proxyacl#2=permit tcp any any

Final Configuration

```
Pre-Configuration:
```

```
SW1 & SW2:
vlan 13,200,100
!
! Configure trunks
!
interface range Fa0/21 - 23
switchport trunk encaps dot1q
switchport mode trunk
SW1:
interface Fa0/1
switchport host
switchport access vlan 13
!
interface Fa0/2
switchport host
switchport access vlan 100
!
interface Fa0/3
switchport host
```

switchport access vlan 13

```
interface Fa0/20
switchport host
 switchport access vlan 100
SW2:
interface Fa0/3
switchport host
switchport access vlan 200
T
interface Fa0/20
switchport host
switchport access vlan 200
R1:
interface E0/0
no shut
ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E 0/0
no shut
ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
no shut
ip address 136.1.23.2 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 10.0.0.0
R3:
interface E 0/0
no shut
ip add 136.1.13.3 255.255.255.0
interface E 0/1
no shut
ip add 136.1.200.3 255.255.255.0
!
interface Serial 1/3
no shut
clockrate 64000
ip address 136.1.23.3 255.255.255.0
T
router rip
ver 2
no auto
network 136.1.0.0
Auth Proxy:
```

```
R3:
aaa new-model
!
! Safequard console
!
aaa authentication login CONSOLE none
!
line console 0
login authentication CONSOLE
1
! Configure AAA settings for auth-proxy
!
aaa authentication login default group radius
aaa authorization auth-proxy default group radius
!
radius-server host 10.0.0.100 key CISCO
!
! Configure HTTP server & HTTP auth via AAA
!
ip http server
ip http authentication aaa
!
! Auth proxy rule
1
ip auth-proxy name PROXY http
!
! Inbound access-list
I
ip access-list extended 100
permit udp any any eq RIP
remark == permit TACACS+/RADIUS traffic
remark == if you have them on outside interface
deny ip any any log
interface E0/1
 ip access-group 100 in
 ip auth-proxy PROXY
```

ACS:

Within Interface Configuration permit per-user TACACS+/RADIUS Attributes:



Permit "cisco av-pair" attribute in user profile:

🗧 Cisco	oSecure AC	5 - Microso	oft Interne	et Explo	rer	_ 🗆 ×
<u>File</u>	<u>E</u> dit ⊻iew	F <u>a</u> vorites	<u>I</u> ools <u>H</u>	<u>H</u> elp	← Back • ⇒ • 🔕 🔮 🛛 Address 🖉 http://127.0.0.1:4397/	•
Cis	CO SYSTEMS	Int	terfac	e Co	nfiguration	×
أس	Մաստ	Edit	lonido			-
	User Setup	7				
	Group Setup				RADIUS (Cisco IOS/PIX 6.x)	
463	Shared Profile Components]				
	Network Configuration		User	r Gro	oup	
	System Configuration	1			[026/009/001] cisco-av-pair	
	Interface			V	[026/009/101] cisco-h323-credit-amount	
	Configuratio	n			[026/009/102] cisco-h323-credit-time	
	Administratio	'n			[026/009/103] cisco-h323-return-code	
0	E. down of U.			v	[026/009/104] cisco-h323-prompt-id	
90	Databases			5	[026/009/105] cisco-h323-day-and-time	
	Posture			•	[026/009/106] cisco-h323-redirect-number	
	vandadon			V	[026/009/107] cisco-h323-preferred-lang	
	Network Acce Profiles	SS		N	[026/009/108] cisco-h323-redirect-ip-addr	
01	Reports and	1		N	[026/009/109] cisco-h323-billing-model	
	Activity			N	[026/009/110] cisco-h323-currency	-
<u>اتھ</u>	Online Documentatio				Submit Cancel	
Appl	et startStop s	started				🔮 Internet

CiscoSecure ACS -	Microsoft Internet Explorer	_ 🗆 ×
<u>File Edit View Fa</u>	avorites Iools Help 🗘 🖙 Back 🔹 🖘 🖉 👔 🖓 Address 🛃 http://127.0.0.1:4397/	-
CISCO SYSTEMS	User Setup	×
milliumillium	Edit	- E
User Setup	User: PROXY (New User)	
Sterup Shared Profile Components	Account Disabled	
Network Configuration	Supplementary User Info	?
System Configuration	Real Name Description	
Administration Control		
Databases	User Setup	<u>?</u>
Validation Validation	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate	
Reports and Activity	Password *******	
Applet dialup_filter st	SubmitCancel	net

Add new user "PROXY" with password "CISCO1234":

Configure auth-proxy attributes in user profile.	Configure	auth-proxy	attributes	in	user	profile:
--	-----------	------------	------------	----	------	----------

🤌 CiscoSe	cure AC	5 - Microso	ft Inter	net Expl	orer							_ 🗆 ×
<u>Eile E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	🖙 Back	· → ⇒ →	8	A <u>d</u> dress	🖉 http://12	27.0.0.1:4397/		-
Cisco	Systems Size	Us	ser S	etup								×
tillitu	tlilliu.		Ľ F	ailed at	ttempts	since last	t succes	sful logi	n: O			
Use Set	vr up		I	🗌 Reset	t current	t failed at	tempts:	count oi	n submit			
Set	up up		2									
Com	red Prome iponents work				~				IQ Attribu	+05	9	
Con	figuration tem		I [00	09\001]	cisco-a	iv-pair	/ PIA U.	X KADIL			 	
Con	figuration erface figuratio	n				auth-p auth-p icmp a	roxy:pr roxy:pr ny any	iv-lvl= oxyacl\$	=15 ∮1=permit	*		
Adr Con	ninistratio trol	n.				auth-p tcp an	roxy:pr y any	oxyacl\$	∮2=permit	Ŧ		
Date Date	abases sture											
Nets Prof	idation vork Acce iles	\$5										
Rep Act	orts and ivity						?	Back to He	lp			-
	ine umentatio	n					Sub	mit C	ancel			
Applet d	ialup_filte	r started									🕜 Internet	

Add	R3	as	RADIUS	client	on	ACS:

🖉 Cis	scoSed	ure AC	5 - Microso	oft Inter	net Explo	orer) ×
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	⇔ Back 👻 ≖	⇒ - 🖉 🛃	Address 🧔	http://127.0.0.1	4397/	•	11
C	ISCO S	YSTEMS	Ne	etwo	k Co	nfiguratio	n					×
		սիս			N OOI	ingulate						
			Edit									ヨ日
	User Setu	'P										
	Grou Setu	ip ip					Add A	AA C	lient			
4 ja	Shari Comp	ed Profile onents		AA Clie	ent Hos	tname	R3					
R	Netw Conf	rork iguratio					136.1.23.	3	<u>^</u>			
S.	Syst Conf	em iguratio		AA CII	ent IP A	aaress			-			
	Inter Conf	rface iguratio	n K	ey			cisco –					
-72	Adm Cont	inistratio rol		uthent	icate U	sing	RADIUS (C	sco IOS/PI	IX 6.0)			
øC	Exte	rnal Use bases		🗖 Sing	gle Conr	nect TACACS	6+ AAA Clien	t (Record s	stop in accoun	ting on failure).		
000	B Post Vali	ure dation		🗖 Log	Update	/Watchdog	Packets from	n this AAA	Client			
	Netw	ork Acce	ss	🗖 Log	RADIUS	3 Tunneling I	Packets from	this AAA (Client			
		es orte ord		🗆 Rep	lace RA	DIUS Port in	fo with Useri	name from	this AAA Clien	t		
	Acti	vity vity					400					
g) Onlii Docu	ne mentatio	n			Sub	mit Sub	omit + Appl	y Cancel			-1-
ar 😂	pplet sta	artStop s	started							🔹 🚺 🔮 Inter	rnet –	

Verification

```
R3#debug aaa authentication
AAA Authentication debugging is on
R3#debug aaa authorization
AAA Authorization debugging is on
R3#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
```

Test PC:

🗿 Authentication Proxy Login Page - Microsoft Internet Explorer	
j Eile Edit View Favorites Iools Help ← Back → → → 🐼 🚺 Address 🖗 http://150.1.1	.1
T T	
Username: PROXY	
Password:	
ОК	
	-
2 Done	internet

CCIE Security Lab Workbook Volume I Version 3.0



<snip>

```
*Mar 1 22:28:31.315: AAA/AUTHEN/START (4167353654): port='Ethernet0/1'
list='default' action=LOGIN service=LOGIN
*Mar 1 22:28:31.315: AAA/AUTHEN/START (4167353654): found list default
*Mar 1 22:28:31.315: AAA/AUTHEN/START (4167353654): Method=radius (radius)
*Mar 1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETUSER
*Mar 1 22:28:31.319: AAA/AUTHEN/CONT (4167353654): continue
      1 22:28:31.319: AAA/AUTHEN/CONT (4167353654): continue_login
(user='(undef)')
*Mar 1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETUSER
*Mar 1 22:28:31.319: AAA/AUTHEN(4167353654): Method=radius (radius)
      1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETPASS
*Mar
*Mar 1 22:28:31.319: AAA/AUTHEN/CONT (4167353654): continue_login
(user='PROXY')
*Mar 1 22:28:31.319: AAA/AUTHEN(4167353654): Status=GETPASS
*Mar 1 22:28:31.323: AAA/AUTHEN(4167353654): Method=radius (radius)
*Mar 1 22:28:31.323: RADIUS: Pick NAS IP for u=0x82ECC30C tableid=0
      1 22:28:31.323: RADIUS: Pick NAS IP for u=0x82ECC30C tableid=0
cfg_addr=0.0.0.0 best_addr=136.1.23.3
*Mar 1 22:28:31.323: RADIUS: ustruct sharecount=1
*Mar 1 22:28:31.323: Radius: radius_port_info() success=1 radius_nas_port=1
*Mar 1 22:28:31.323: RADIUS(00000000): Send Access-Request to 10 0 0 100:16
      1 22:28:31.323: RADIUS(0000000): Send Access-Request to 10.0.0.100:1645
id 21645/9, len 84
*Mar 1 22:28:31.327: RADIUS: authenticator BB ED AA B9 32 98 61 51 - A5 9F A7
29 CF 38 AD F0
      1 22:28:31.327: RADIUS:
                                  NAS-IP-Address
                                                                    136.1.23.3
*Mar
                                                         [4]
                                                                б
*Mar 1 22:28:31.327: RADIUS:
                                                                    60001
                                                         [5]
                                  NAS-Port
                                                                б
*Mar 1 22:28:31.327: RADIUS:
                                  NAS-Port-Type
                                                         [61] 6
                                                                    Virtual
[5]
*Mar 1 22:28:31.327: RADIUS: User-Name
                                                                7
                                                                     "PROXY"
                                                         [1]
*Mar 1 22:28:31.331: RADIUS:
                                                                    "136.1.200.200"
                                  Calling-Station-Id
                                                         [31]
                                                               15
*Mar 1 22:28:31.331: RADIUS: User-Password
                                                         [2]
                                                                18
                                                                    *
*Mar 1 22:28:31.331: RADIUS: Service-Type
                                                         [6]
                                                                6
                                                                    Outbound
[5]
```

Copyright © 2007 Internetwork Expert

*Mar 1 22:28:31.411: RADIUS: Received from id 21645/9 10.0.0.100:1645, Access-Accept, len 181 *Mar 1 22:28:31.415: RADIUS: authenticator 35 55 0E 8A 76 28 14 EF - 90 82 89 E1 B6 3D D8 EF *Mar 1 22:28:31.415: RADIUS: Framed-IP-Address [8] 6 255,255,255,255 *Mar 1 22:28:31.415: RADIUS: Vendor, Cisco [26] 30 *Mar 1 22:28:31.415: RADIUS: Cisco AVpair [1] 24 "auth-proxy:privlvl=15" *Mar 1 22:28:31.415: RADIUS: Vendor, Cisco [26] 49 *Mar 1 22:28:31.415: RADIUS: Cisco AVpair [1] 43 "authproxy:proxyacl#1=permit icmp any any" *Mar 1 22:28:31.419: RADIUS: Vendor, Cisco *Mar 1 22:28:31.419: RADIUS: Cisco AVpair [26] 48 [1] 42 "authproxy:proxyacl#2=permit tcp any any" *Mar 1 22:28:31.419: RADIUS: Class [25] 28 *Mar 1 22:28:31.419: RADIUS: 43 41 43 53 3A 30 2F 36 66 31 64 2F 38 38 30 31 [CACS:0/6f1d/8801] 31 37 30 33 2F 36 30 30 30 31 *Mar 1 22:28:31.423: RADIUS: [1703/60001] *Mar 1 22:28:31.423: RADIUS: saved authorization data for user 82ECC30C at 82BC2E78 *Mar 1 22:28:31.427: AAA/AUTHEN(4167353654): Status=PASS *Mar 1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): Port='Ethernet0/1' list='default' service=AUTH-PROXY *Mar 1 22:28:31.427: AAA/AUTHOR/HTTP: Ethernet0/1(476008236) user='PROXY' *Mar 1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTD(476008236). cond AV service=auth-proxv *Mar 1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): send AV cmd* *Mar 1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): found list "default" *Mar 1 22:28:31.427: Ethernet0/1 AAA/AUTHOR/HTTP(476008236): Method=radius (radius) *Mar 1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:priv-lvl=15" *Mar 1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:proxyacl#1=permit icmp any any" *Mar 1 22:28:31.431: RADIUS: cisco AVPair "auth-proxy:proxyacl#2=permit tcp any any" *Mar 1 22:28:31.431: AAA/AUTHOR (476008236): Post authorization status = PASS_ADD R3#**show ip access-lists** Extended IP access list 100 permit icmp host 136.1.200.200 any permit tcp host 136.1.200.200 any (7 matches) 10 permit udp any any eq rip 20 deny ip any any log (20 matches)

R3#show ip auth-proxy cache

Authentication Proxy Cache Client IP 136.1.200.200 Port 1248, timeout 60, state HTTP_ESTAB

G Further Reading

Implementing Authentication Proxy

Content Filtering with IOS Firewall

Objective: Configure router for URL filtering using Websense application.



Directions

- Pre-configure devices as follows:
 - o Create VLANs 13, 23 and 100.
 - Configure IP addressing on Ethernet interfaces.
 - Configure Serial link between R3 and R2.
 - Configure RIP as routing protocol.
 - Create and advertise into RIP interface Loopback0 on R1.
- The goal of the task is to configure HTTP application filtering to achieve the following:
 - Filter all java applets from HTTP responses.
 - Filter URLs using Websense server.
 - Permit domain 'cisco.com' to be accessed at any time.
 - In case if Websense server fails, router should permit any HTTP request.

- Configure R3 as follows:
 - Create access-list number 1, and deny everything with it. It will be used for java filtering.
 - o Configure URL server at 10.0.0.100, use vendor "Websense".
 - o Configure inspection rule named INSPECT as follows:
 - Inspect HTTP traffic and enable java filtering with access-list 1 as well as URL filtering.
 - Configure URL filtering to exempt domain "cisco.com" from filtering and always permit it.
 - Configure url-filtering allow-mode, which instructs router to bypass filtering if filtering server is unavailable.
 - Apply inspection rule "INSPECT" ingress to interface E0/1.

Final Configuration

```
Pre-Configuration:
```

```
SW1 & SW2:
vlan 13,200,100
!
! Configure trunks
interface range Fa0/21 - 23
 switchport trunk encaps dotlq
 switchport mode trunk
SW1:
interface Fa0/1
switchport host
switchport access vlan 13
1
interface Fa0/2
switchport host
switchport access vlan 100
interface Fa0/3
switchport host
switchport access vlan 13
interface Fa0/20
switchport host
 switchport access vlan 100
SW2:
interface Fa0/3
switchport host
switchport access vlan 200
interface Fa0/20
 switchport host
 switchport access vlan 200
```

```
R1:
interface E0/0
no shut
ip address 136.1.13.1 255.255.255.0
!
interface Loopback0
ip address 150.1.1.1 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 150.1.0.0
R2:
interface E 0/0
no shut
ip add 10.0.0.2 255.255.255.0
!
interface Ser 0/1
no shut
ip address 136.1.23.2 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
network 10.0.0.0
R3:
interface E 0/0
no shut
ip add 136.1.13.3 255.255.255.0
!
interface E 0/1
no shut
ip add 136.1.200.3 255.255.255.0
!
interface Serial 1/3
no shut
clockrate 64000
ip address 136.1.23.3 255.255.255.0
!
router rip
ver 2
no auto
network 136.1.0.0
Content Filtering:
R3:
!
! Access-list for java-filtering
!
access-list 1 deny any
1
! Websense Server
!
ip urlfilter server vendor websense 10.0.0.100
!
! Inspection rule to activate filtering
```

Copyright © 2007 Internetwork Expert

www.InternetworkExpert.com

- 558 -

ip inspect name INSPECT http java-list 1 urlfilter

! Configure cisco.com as 'exclusively permitted' domain
ip urlfilter exclusive-domain permit cisco.com
!
! Enable allow-mode
!
ip urlfilter allow-mode on
!
! Apply inspection rule
!
interface Ethernet 0/1
ip inspect INSPECT in

Verification

If you have functional Websense server you should see something like this on your console: R3(config)#ip urlfilter server vendor websense 10.0.0.100 R3(config)# *Mar 1 23:03:46.566: %URLF-5-SERVER_UP: Connection to an URL filter server(10.0.0.100) is made, the router is returning from ALLOW MODE R3#**show ip inspect all** Session audit trail is disabled Session alert is dlsabled one-minute (sampling period) thresholds are [90:100] connections max-incomplete sessions thresholds are [900:1000] max-incomplete tcp connections per host is 50. Block-time 5 minutes. tcp synwait-time is 15 sec -- tcp finwait-time is 5 sec tcp idle-time is 3600 sec -- udp idle-time is 30 sec dns-timeout is 5 sec Inspection Rule Configuration Inspection name INSPECT http java-list 1 url-filter is on alert is off audit-trail is off timeout 3600 Interface Configuration Interface Ethernet0/1 Inbound inspection rule is INSPECT http java-list 1 url-filter is on alert is off audit-trail is off timeout 3600 Outgoing inspection rule is not set Inbound access list is not set Outgoing access list is not set Check urlfilter configuration, note the server port. Sometimes you may need to open a pinhole for it in access-lists: R3#show ip urlfilter config Websense URL Filtering is ENABLED Primary Websense server configurations

Copyright © 2007 Internetwork Expert

CCIE Security Lab Workbook Volume I Version 3.0

Further Reading

Firewall Websense URL Filtering