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\textsuperscript{TM} lab material is completely coincidental.
# Table of Contents

**IDENTITY MANAGEMENT** ................................................................. 1  
**NETWORK ADMISSION CONTROL** .................................................. 1  
  ACS Setup for NAC ................................................................. 1  
  NAC L3 IP With the ASA and Cisco VPN Client ....................... 14  
  NAC L3 IP with VPN3k and Cisco VPN Client ......................... 22
Identity Management

Network Admission Control

ACS Setup for NAC

Objective: Configure ACS server for NAC tasks.

Directions

- In this scenario we are going to develop a simple NAC policy on ACS server to be later used in specific NAC scenarios.
- The first step is to install a digital certificate on ACS server in order to permit PEAP/EAP-TLS authentication methods. Both of them use digital certificates to authenticate endpoints.
- There are two basic ways to install a digital certificate:
  - Enroll with Certification Authority.
  - Install self-signed certificate.
- Of them the latest it the most simple one. Be aware though, that you will later need to install self-signed certificate as trusted on endpoint hosts, running Cisco Trust Agent software.
- Generate & Install self-signed certificate under “System Configuration” of ACS.
- Next, you will need to enable PEAP along with “Posture Validation” under “System Configuration/Global Authentication Setup”.
- Now you need to create a Network Access Profile for NAC. ACS has some “template” NAPs for NAC scenarios, which we are going to customize.
- Generate & activate NAP named “NAC_L3_IP” from “NAC L3 IP” template. Apply & Restart and then restart the system services.
- The created profile already has some posture validation and authorization settings. We are now going to customize them to suit our need.
- Check to see the already configure Posture Validation policies, and modify the existing condition for ‘Healthy’ APT to verify if client OS type is “Windows”.
- This way, a client host is only considered Healthy if it runs Windows along with Cisco Trust Agent v1.0 or greater.
Next, modify the authorization attributes for NAC Policy. When you created the template, two downloadable ACLs have been created: for ‘Healthy’ and for ‘Quarantined’ hosts.

Modify the downloadable access-list for ‘Quarantined’ posture named ‘NACSAMPLE_QUARANTINE_ACL/L3_EXAMPLE’ as follows:

- Permit only “ICMP echo”
- Permit “HTTP to host 10.0.0.100”.

Finally, under “Posture Validation” of newly create Network Access Profile modify URL redirection for “Quarantined” token as set it to http://10.0.0.100.

### Final Configuration

**ACS:**

Generate & install self-signed certificate:

![CiscoSecure ACS - Microsoft Internet Explorer](image)

**System Configuration**

**Generate Self-Signed Certificate**

- **Certificate subject**: cn=ACS, o=IE
- **Certificate file**: c:\ACS.cer
- **Private key file**: c:\ACS.key
- **Private key password**: ********
- **Retype private key password**: ********
- **Key length**: 2048 bits
- **Digest to sign with**: SHA-1
- **Install generated certificate**: 

![Submit Cancel](image)
Configure Global Authentication for PEAP and Posture Validation:

![Global Authentication Setup](image)

- **PEAP**
  - Allow EAP-MSCHAPv2
  - Allow EAP-GTC
  - Allow posture validation
  - Cisco client initial message:
  - PEAP session timeout (minutes): 120
  - Enable Fast Reconnect:

- **EAP-FAST**
  - EAP-FAST Configuration

- **EAP-TLS**
  - Allow EAP-TLS
Create new NAP for NAC L3 IP from template:
The current configuration has been changed. 'Apply and Restart' to adopt the new settings.
Modify Internal Posture Validation policy created from template:
Modify Posture Validation Rule:

Posture Validation

Posture Validation Rule - NAC-SAMPLE-CTA-POLICY

Condition Sets
- Cisco:PA:PA-Name contains Cisco Trust Agent
- Cisco:PA:PA-Version >= 1.0.0.0

- Match 'OR' inside Condition and 'AND' between Condition Sets
- Match 'AND' inside Condition and 'OR' between Condition Sets

Condition Sets

Posture Token: Cisco:PA
Notification String: [ ]

Submit | Clone | Delete | Cancel
Add check for OS type:
Posture Validation

Condition Sets
Cisco PA PA-Name contains Cisco Trust Agent
Cisco PA PA-Version >= 1.0.0.0
Cisco PA OS-Type contains Windows

Match 'OR' inside Condition and 'AND' between Condition Sets
Match 'AND' inside Condition and 'OR' between Condition Sets

Posture Token: 
Cisco PA Healthy
Notification String: 
Submit Clone Delete Cancel
Modify downloadable ACL for 'Quarantine' posture:
Shared Profile Components

Edit

Downloadable IP ACL Content

Name: L3.EXAMPLE

ACL Definitions

```plaintext
permit icmp any any echo
permit tcp any host 10.0.0.100 eq 80
```
Modify Posture Validation for created NAP:

![Network Access Profiles](image_url)
Add URL Redirect for 'Quarantine' Posture:

### Further Reading

**General NAC:**

- [Implementing Network Admission Control - Phase One Configuration and Deployment](#)
- [Network Admission Control (NAC) FAQ](#)
- [Network Admission Control (NAC) Framework Deployment Guide](#)
- [Network Admission Control (NAC) Framework Configuration Guide](#)

**ACS Configuration:**

- [Shared Profile Components](#)
- [System Configuration: Authentication and Certificates](#)
- [Posture Validation](#)
- [Network Access Profiles](#)
**NAC L3 IP With the ASA and Cisco VPN Client**

**Objective:** Configure the ASA firewall for NAC with remote VPN connections.

**Directions**

- Configure ACS server as per the scenario “Identity Management/Network Admission Control” “ACS Setup for NAC”.
- Configure devices as per the scenario “VPN/Easy VPN” “PIX/ASA and Cisco VPN Client with Split-Tunneling/Xauth/RRI”.
- ASA configuration is as follows:
  
  o Configure RADIUS server for NAC as follows:
    
    - Name this group as “RADIUS”.
    - Specify host 10.0.0.100 on outside.
    - Use key CISCO.
    - Configure RADIUS network client on ACS respectively.

  o Configure tunnel-group EZVPN for NAC:
    
    - Specify NAC authentication server group “RADIUS”.

  o Create NAC default access-list named NAC_DEFAULT:
- Permit UDP from port 21862 to any only (EAPoUDP traffic from connecting host).
  - Configure group-policy EZVPN:
    - Enable NAC.
    - Specify NAC default access-list NAC_DEFAULT.
  - Client configuration:
    - Import ACS certificate. Obtain file containing ACS certificate in PEM format (by default), e.g. ACS.cer. You must have created it when you configured ACS server.
    - Physically put this file into directory on Test PC, e.g. into “c:\mycerts”.
    - Go to Cisco Trust Agent home directory (by default it’s “C:\Program Files\Cisco Systems\CiscoTrustAgent”) and execute from there:
      `ctcert.exe /add c:\mycerts\ACS.cer /store “Root”`
    - You are now ready to connect Cisco VPN Client to the ASA.
    - There is a bug on Windows Server VPN Client installations where Cisco VPN Client is unable to add static route to “split-tunneled” network via connection interface.
    - This prevents Cisco Trust Agent from communicating correctly with the ASA, since EOU transactions are initiate from the inside ASA interface IP address by default (which is in our split-tunnel list).
    - This problem could be remediated by tunneling everything, though this may not be the desirable solution.
    - This bug could also be fixed by issuing manual “route add” command to the split tunneled network - see details in final configuration.

**Final Configuration**

ASA1:
```
access-list NAC_DEFAULT extended permit udp any eq 21862 any !
group-policy EZVPN attributes
  nac enable
  nac-default-acl value NAC_DEFAULT !
tunnel-group EZVPN general-attributes
default-group-policy EZVPN
  nac-authentication-server-group RADIUS
```
ACS:

Add network client:

![Image of ACS Network Configuration for ASA1](image-url)
Test PC:

As soon as you have VPN Client connected check the routing table:

```
C:"\route print
Interface List:
   0x1: .............................. MS TCP Loopback interface
   0x2: 0c 29 fc 6f 6f ........ VMware Accelerated AMD PCNet Adapter
   0x4: 00 0c 29 18 6f 6f ........ VMware Accelerated AMD PCNet Adapter
   0x2000004 ...00 05 9a 3c 78 00 ...... Cisco Systems VPN Adapter

Active Routes:
Network Destination          Netmask     Gateway         Interface  Metric
  10.0.0.0        255.255.255.0  172.16.3.4       172.16.3.223     3
  20.0.0.0        255.0.0.0      192.0.0.1        192.168.1.100     1
  20.255.255.255  255.255.255.255 200.3.4.1        200.3.4.1        1
  127.0.0.0       255.0.0.0      127.0.0.1        127.0.0.1        1
  192.168.1.100   255.255.255.255 192.168.1.100   192.168.1.100     1
  255.255.255.255  255.255.255.255 255.255.255.255 255.255.255.255 1
Default Gateway:         172.16.3.1
```

Execute command "route add 136.1.121.0 255.255.255.0 20.0.0.1":

Verification

ASA1(config)# debug nac all
ASA1(config)# eou reval all
1 seAssions.list has
NAC 'RevalidateS All' request by adAdministrative a1ction - 1 sessions
NAC EAP Access Accept - 20.0.0.1
NAC EAP Access Accept - 20.0.0.1, user:IE-SERVER3:IEAdmin
NAC EAP Access Accept - 20.0.0.1, Reval Period:36000 seconds
NAC Access Accept - 20.0.0.1, Posture Token:Healthy
NAC Access Accept - 20.0.0.1, Status Query Period:300 seconds
NAC PV complete - 20.0.0.1, posture:Healthy
NAC 'Revalidate All' complete

ASA1(config)# show vpn-sessiondb remote

<table>
<thead>
<tr>
<th>Session Type: Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username     : CISCO</td>
</tr>
<tr>
<td>Index        : 1</td>
</tr>
<tr>
<td>Assigned IP  : 20.0.0.1</td>
</tr>
<tr>
<td>Protocol     : IPSec</td>
</tr>
<tr>
<td>Hashing      : MD5</td>
</tr>
<tr>
<td>Bytes Tx     : 3872</td>
</tr>
</tbody>
</table>
Client Type: WinNT                  Client Ver: 4.8.01.0300
Group Policy: EZVPN
Tunnel Group: EZVPN
Login Time: 04:09:58 UTC Sat Feb 3 2007
Duration: 0h:15m:18s
Filter Name: #ACSACL#-IP-NAC_SAMPLE_HEALTHY_ACL-45c43e78
NAC Result: Accepted
Posture Token: Healthy

ASA1(config)# show access-list #ACSACL#-IP-NAC_SAMPLE_HEALTHY_ACL-45c43e78
access-list #ACSACL#-IP-NAC_SAMPLE_HEALTHY_ACL-45c43e78; 1 elements (dynamic)
permit ip any any (hitcnt=0) 0xfeed89fe

Test PC:

C:\>route add 136.1.121.0 mask 255.255.255.0 20.0.0.1
C:\>cd c:\program files\cisco systems\ciscotrustagent
C:\Program Files\Cisco Systems\CiscoTrustAgent>ctstat

Cisco Trust Agent Statistics
Current Time: Sat Feb 03 04:41:01 2007
CTA Version: 2.0.0.30

Session Information
Session Number (Hex): 01000000
Session Type: EOU
IP Address: 136.1.121.12:1924
System Posture Token Value: Healthy
Received on: Sat Feb 03 04:38:16 2007
Total Postures Received: 4
Last E9 Response was "No Status Change"
Plugin Vendor/Application: 9/1
Application Posture Token Value: Healthy
Received: Sat Feb 03 04:38:16 2007
Posture Request last received: Sat Feb 03 04:38:16 2007
Length of last response to Posture Req: 12
Sent: Sat Feb 03 04:38:16 2007

Plugin:
Vendor: Cisco Systems
Application ID: 1
Status: Operational
Application ID: 2
Status: Operational

C:\Program Files\Cisco Systems\CiscoTrustAgent>
ACS:

Reports & Activity/Passed Authentications:
Further Reading

ASA: Configuring Network Admission Control
Cisco Trust Agent Administrator Guide 2.0
NAC L3 IP with VPN3k and Cisco VPN Client

Objective: Configure VPN3k for NAC with Cisco VPN Client remote connections.

Directions

- Configure ACS server as per the scenario “Identity Management/Network Admission Control” “ACS Setup for NAC”.
- Configure devices as per the scenario “VPN/Easy VPN” “VPN3k and Cisco VPN Client with Split-Tunneling”
- Configure VPN3k for NAC:
  - Add RADIUS authentication server for Posture Validation.
  - Add rules for RADIUS traffic to Public Filter:
    - Permit UDP ports 1645 and 1646
  - Configure ACS to support new network client.
  - Create filter named NAC_DEFAULT:
    - Add rule “EAPoUDP” and permit inbound anybody from UDP port 21862 to any with this rule.
- Configure NAC settings for group “EZVPN”:
- Enable NAC.
- Configure default NAC access-list “NAC_DEFAULT”.

- Client configuration:
  - Import ACS certificate. Obtain file containing ACS certificate in PEM format (by default), e.g. ACS.cer. You must have created it when you configured ACS server.
  - Physically put this file into directory on Test PC, e.g. into “c:\mycerts”.
  - Go to Cisco Trust Agent home directory (by default it’s “C:\Program Files\Cisco Systems\CiscoTrustAgent”) and execute from there:
    
    `ctacert.exe /add c:\mycerts\ACS.cer /store “Root”`

- You are now ready to connect Cisco VPN Client to the ASA.
- There is a bug on Windows Server VPN Client installations where Cisco VPN Client is unable to add static route to “split-tunneled” network via connection interface.
- This prevents Cisco Trust Agent from communicating correctly with the ASA, since EOU transactions are initiate from the inside ASA interface IP address by default (which is in our split-tunnel list).
- This problem could be remediated by tunneling everything, though this may not be the desirable solution.
- This bug could also be fixed by issuing manual “route add” command to the split tunneled network - see details in final configuration.
Final Configuration

VPN3k:

Add new RADIUS server (use the usual key "CISCO"): 

![VPN3k Configuration Screen](image-url)
Configure ACS server respectivity to support RADIUS client:
Configure Rule for Outgoing RADIUS traffic Out:

Rule Name: Outgoing RADIUS Out
Direction: Outbound
Action: Forward
Protocol: UDP
TCP Connection: Don't Care
Source Address:

Configure and add a new filter rule.

Name of this filter rule. The name must be unique.
Select the data direction to which this rule applies.
Specify the action to take when this filter rule applies.
Select the protocol to which this rule applies. For other protocols, enter the protocol number.
Select whether this rule should apply to an established TCP connection.
TCP/UDP Source Port

Port: Range
or Range: 0 to 65535

TCP/UDP Destination Port

Port: Range
or Range: 1645 to 1645

ICMP Packet Type

0 to 255

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.

For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.

For ICMP, specify the range of ICMP packet types that this rule checks.
Configure Rule for Outgoing RADIUS traffic In:

Configure and add a new filter rule.

**Rule Name**: Outgoing RADIUS In

**Direction**: Inbound

**Action**: Forward

**Protocol**: TCP

**Source Address**

Specify the source address for the filter rule.
VPN 3000 Concentrator Series Manager

TCP/UDP Source Port

- Port: Range
- or Range: 1645 to 1645

TCP/UDP Destination Port

- Port: Range
- or Range: 0 to 65535

ICMP Packet Type

- 0 to 255

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.

For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.

For ICMP, specify the range of ICMP packet types that this rule checks.
Assign both rules to the Public filter:

Add, remove, prioritize, and configure rules that apply to a filter.

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.
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.

<table>
<thead>
<tr>
<th>Current Rules in Filter</th>
<th>Actions</th>
<th>Available R</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT-T In (forward/in)</td>
<td>&lt;&lt; Add</td>
<td>OSPF In (forward/in)</td>
</tr>
<tr>
<td>RIP In (forward/in)</td>
<td></td>
<td>OSPF Out (forward/out)</td>
</tr>
<tr>
<td><strong>Outgoing RADIUS In (forward/in)</strong></td>
<td>&lt;&lt; Insert Above</td>
<td>Incoming HTTP In (to)</td>
</tr>
<tr>
<td>GRE Out (forward/out)</td>
<td></td>
<td>Any In (forward/in)</td>
</tr>
<tr>
<td>IKE Out (forward/out)</td>
<td>Remove &gt;&gt;</td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>PPTP Out (forward/out)</td>
<td></td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>L2TP Out (forward/out)</td>
<td>Move Up</td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>ICMP Out (forward/out)</td>
<td>Move Down</td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>VRRP Out (forward/out)</td>
<td></td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>NAT-T Out (forward/out)</td>
<td>Assign SA to Rule</td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td>RIP Out (forward/out)</td>
<td>Done</td>
<td>Any Out (forward/out)</td>
</tr>
<tr>
<td><strong>Outgoing RADIUS Out (forward/out)</strong></td>
<td></td>
<td>Any Out (forward/out)</td>
</tr>
</tbody>
</table>

Copyright © 2007 Internetwork Expert  www.InternetworkExpert.com
Create rule to permit EAPoUDP traffic:
TCP/UDP Source Port

Port \( \text{Range} \)

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.

TCP/UDP Destination Port

Port \( \text{Range} \)

or Range 21862 to 21852

For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.

ICMP Packet Type

0 to 255

For ICMP, specify the range of ICMP packet types that this rule checks.
Create NAC default rule to permit EAPoUDP traffic only:
Add, remove, prioritize, and configure rules that apply to a filter.

**Filter Name:** NAC_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.
### Network Access Control Parameters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Inherit?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NAC</td>
<td>☑</td>
<td></td>
<td>Check to enable Network Admission Control. NAC is supported only for IPSec as over IPSec tunnels.</td>
</tr>
<tr>
<td>Status Query Timer</td>
<td>300</td>
<td>☑</td>
<td>Time period between status queries to the peer. A Status response from the peer indicates whether or not the peer's PC is online. Enter a value in seconds. Range: 30-180. Default value: 300. Time period before a machine posture validation and the...</td>
</tr>
</tbody>
</table>
Configure NAC settings for group EZVPN:

Verification

Test PC:

Connect Cisco VPN Client, and add static route:
C:\Program Files\Cisco Systems\CiscoTrustAgent>ctastat

CXA Statistics Reporting Tool
Cisco Trust Agent Statistics
Current Time: Sat Feb 03 05:56:34 2007
CXA Version: 2.0.0.30

Session Information
Session Number (Hex): 01000000
Session Type: ECU
IP Address: 136.1.111.11:1024
System Posture Token Value: Healthy
Received on: Sat Feb 03 05:14:13 2007
Total Postures Received: 5
Last SQ Response was "No Status Change"
Plugin Vendor/Application: 9.1
Application Posture Token Value: Healthy
Received: Sat Feb 03 05:11:13 2007
Posture Request Last received: Sat Feb 03 05:14:13 2007
Length of last response to Posture Req: 42
Sent: Sat Feb 03 05:14:13 2007

Plug-ins:
Vendor: Cisco Systems
Application ID: 1
Status: Operational
Application ID: 2
Status: Operational

C:\Program Files\Cisco Systems\CiscoTrustAgent>
VPN3k:

**Check Remote VPN session under Monitoring/Sessions:**
VPN 3000 Concentrator Series Manager

IPSec Session

- Session ID: 2
- Remote Address: 20.0.0.1
- Encryption Algorithm: 3DES-168
- Idle Time: 00:00:00

Encapsulation Mode

- Mode: Aggressive
- Mode: Tunnel

Bytes Received

- 2536
- Rekey Time Interval: 28800 seconds

Network Admission Control

- Status Query Time Interval: 300 seconds
- Hold-Off Time Remaining: 0 seconds
- Time Until Next Revalidation: 3362 seconds
- EAPoUDP Session Age: 2638 seconds
- Posture Token: Healthy
ACS:

*Reports & Activity: Passed Authentications*

![Cisco Secure ACS interface](image-url)

<table>
<thead>
<tr>
<th>Time</th>
<th>Message- Type</th>
<th>User- Name</th>
<th>Group- Name</th>
<th>Caller- ID</th>
<th>NAS- Port</th>
<th>NAS- IP- Address</th>
<th>Network Access Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:14:11</td>
<td>Authen OK</td>
<td>IE- SERVER3:IEAdm</td>
<td>...</td>
<td>136.1.100.200:1006</td>
<td>136.1.113.11</td>
<td>NAC_L3_IP</td>
<td></td>
</tr>
<tr>
<td>04:03:24</td>
<td>Authen OK</td>
<td>CISCO</td>
<td>Default group</td>
<td>...</td>
<td>CISCO</td>
<td>136.1.113.11 (Default)</td>
<td></td>
</tr>
<tr>
<td>08:38:13</td>
<td>Authen OK</td>
<td>IE- SERVER3:IEAdm</td>
<td>...</td>
<td>136.1.100.200:S</td>
<td>136.1.123.12</td>
<td>NAC_L3_IP</td>
<td></td>
</tr>
</tbody>
</table>
Further Reading

VPN 3000 Network Access Device 4.7.1 NAC Administration and Configuration