Copyright Information

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^{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

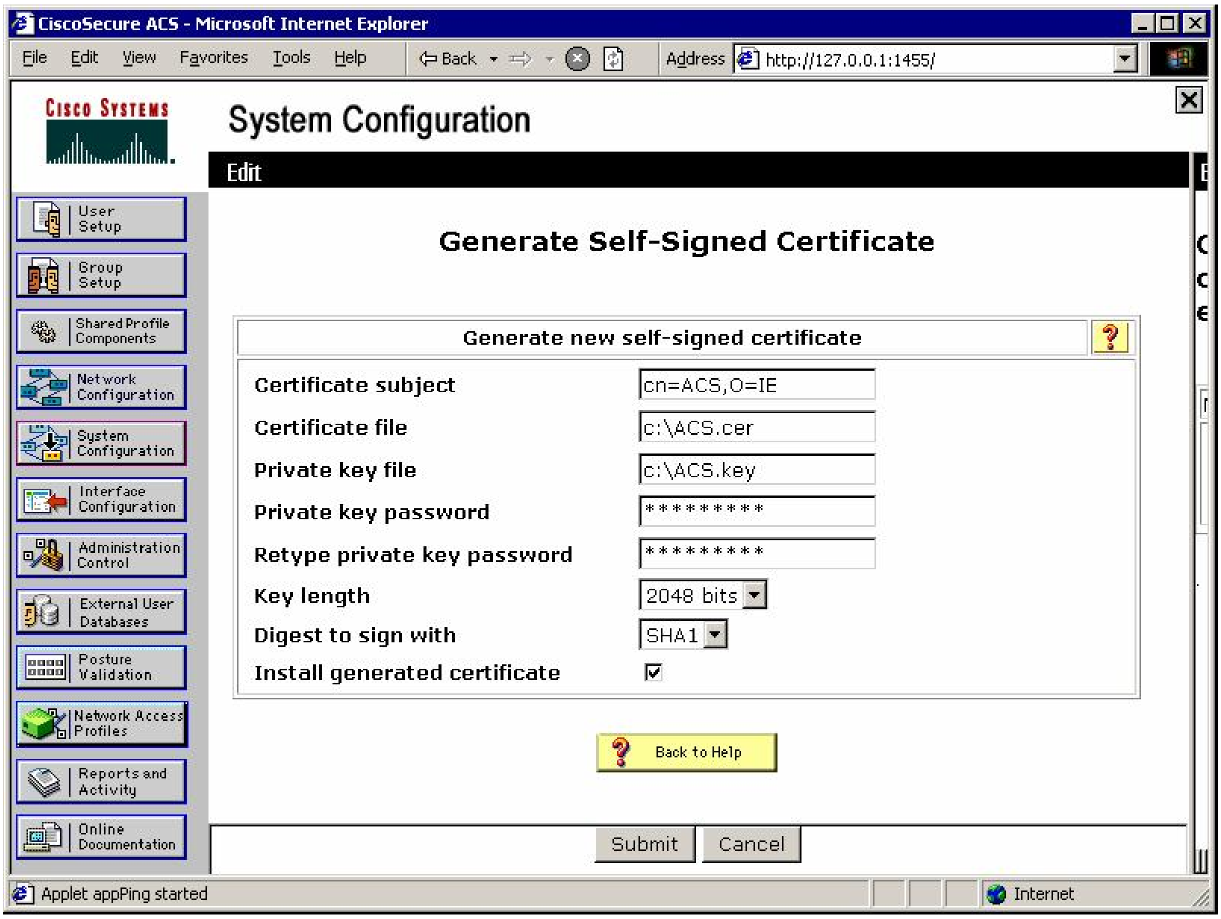
- In this scenario we are going to develop a simple NAC policy on ACS server to be later used in specific NAC scenarios.
- The first step is to install a digital ceritificate on ACS server in order to permit PEAP/EAP-TLS authentication methods. Both of them use digital ceritificates to authenticate endpoints.
- There are two basic ways to install a digital ceritificate:
  - Enroll with Certification Authority.
  - Install self-signed ceritificate.
- 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 ceritificate 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 'Qurantined' hosts.
- Modify the downloadble access-list for 'Quarantine' posture named 'NAC_SAMPLE_QURANTINE_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 "Quarantine" token as set it to http://10.0.0.100.

Final Configuration

ACS:

Generate & install self-signed ceritificate:



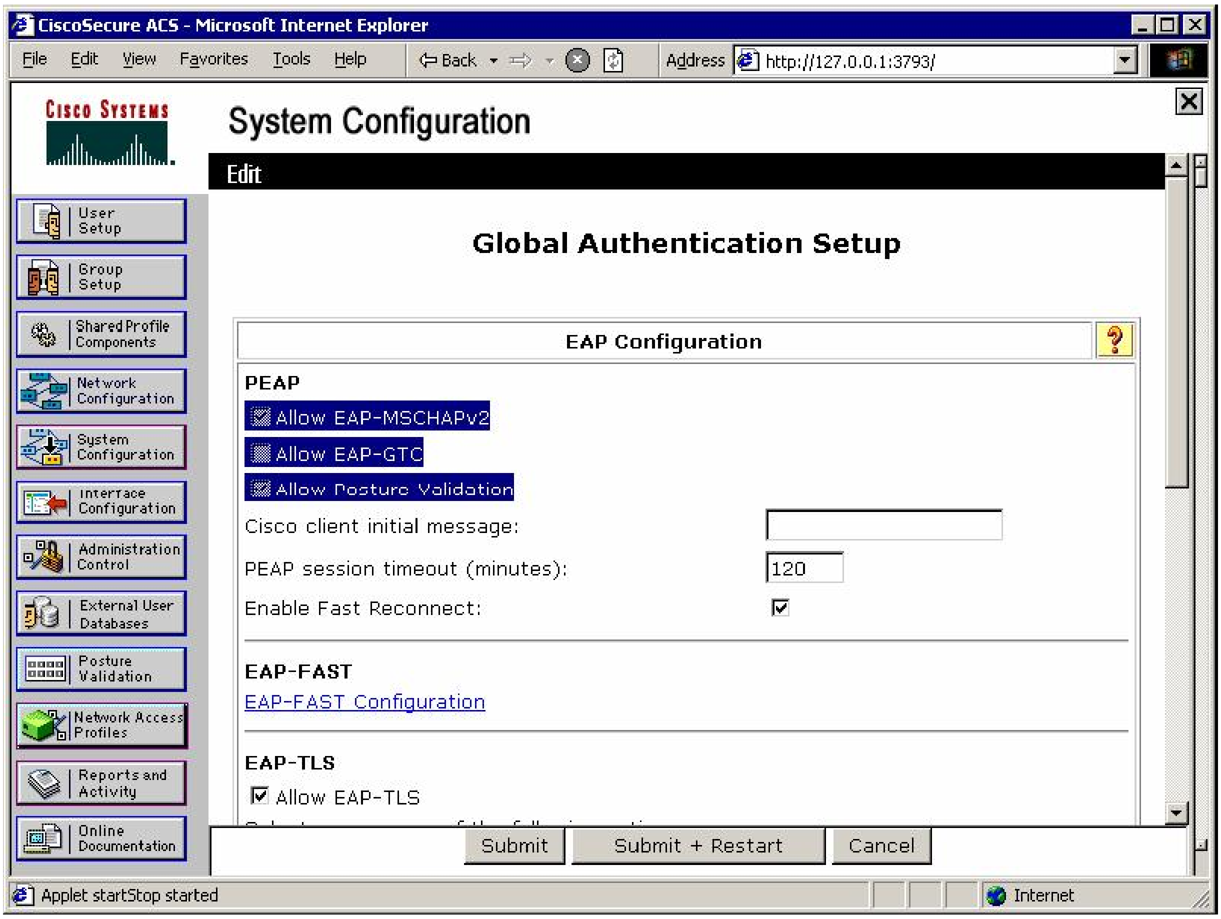
System Configuration

Edit

Generate Self-Signed Certificate

Generate new 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	SHA1
Install generated certificate	☑

Configure Global Authentication for PEAP and Posture Validation:



Global Authentication Setup

EAP Configuration

PEAP

☑ Allow EAP-MSCHAPv2

☑ Allow EAP-GTC

☑ Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

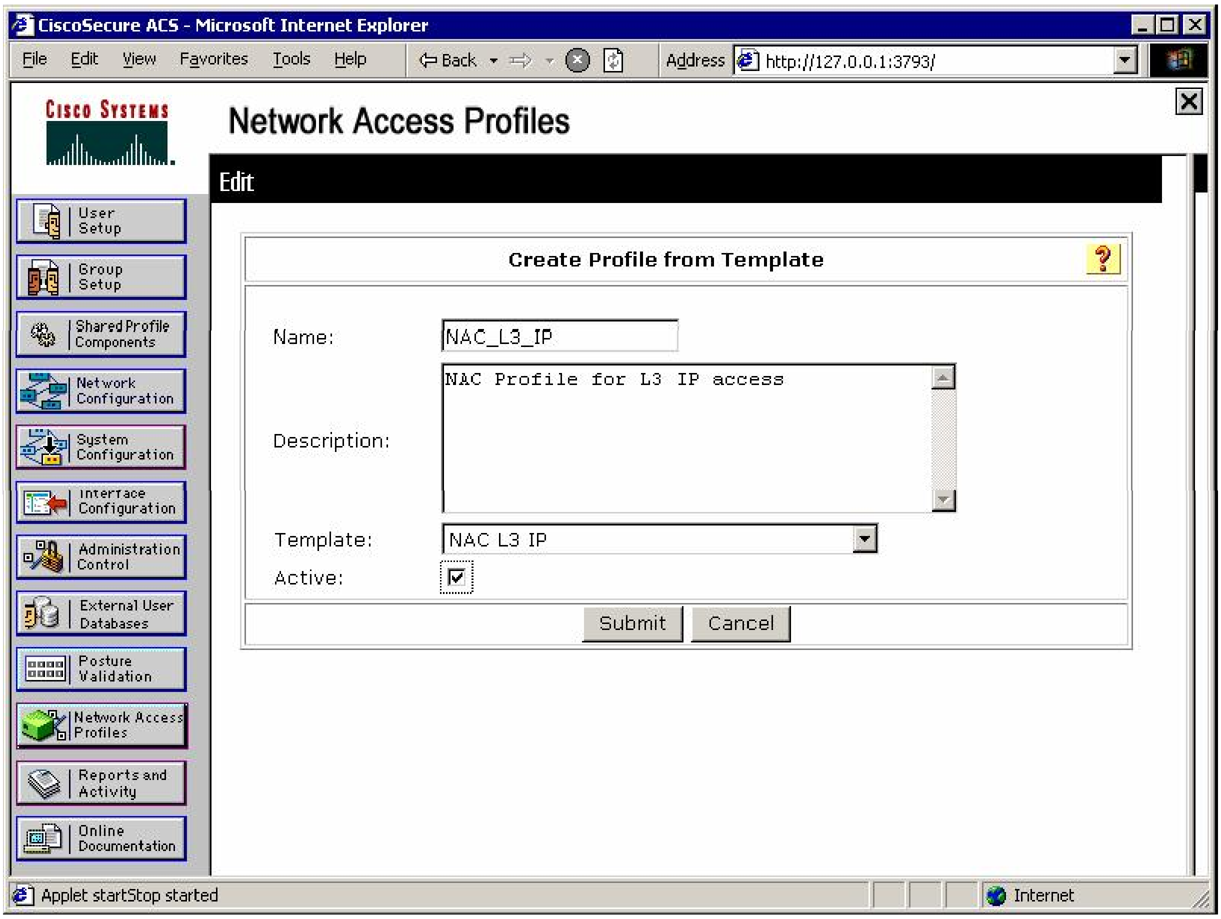
EAP-FAST

EAP-FAST Configuration

EAP-TLS

☑ Allow EAP-TLS

Create new NAP for NAC L3 IP from template:



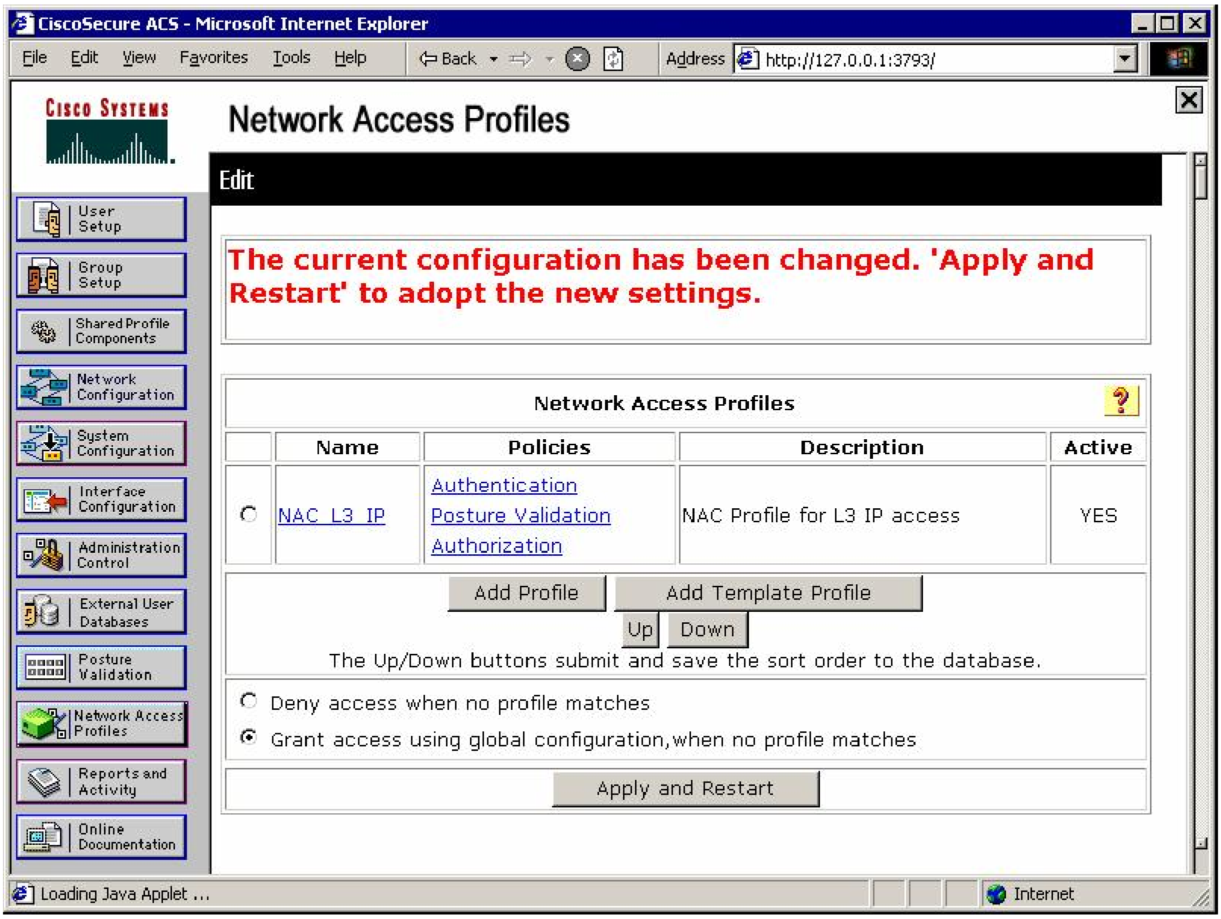
Create Profile from Template

Name: NAC_L3_IP

Description: NAC Profile for L3 IP access

Template: NAC L3 IP

Active: ☑



Network Access Profiles

Edit

The current configuration has been changed. 'Apply and Restart' to adopt the new settings.

Network Access Profiles

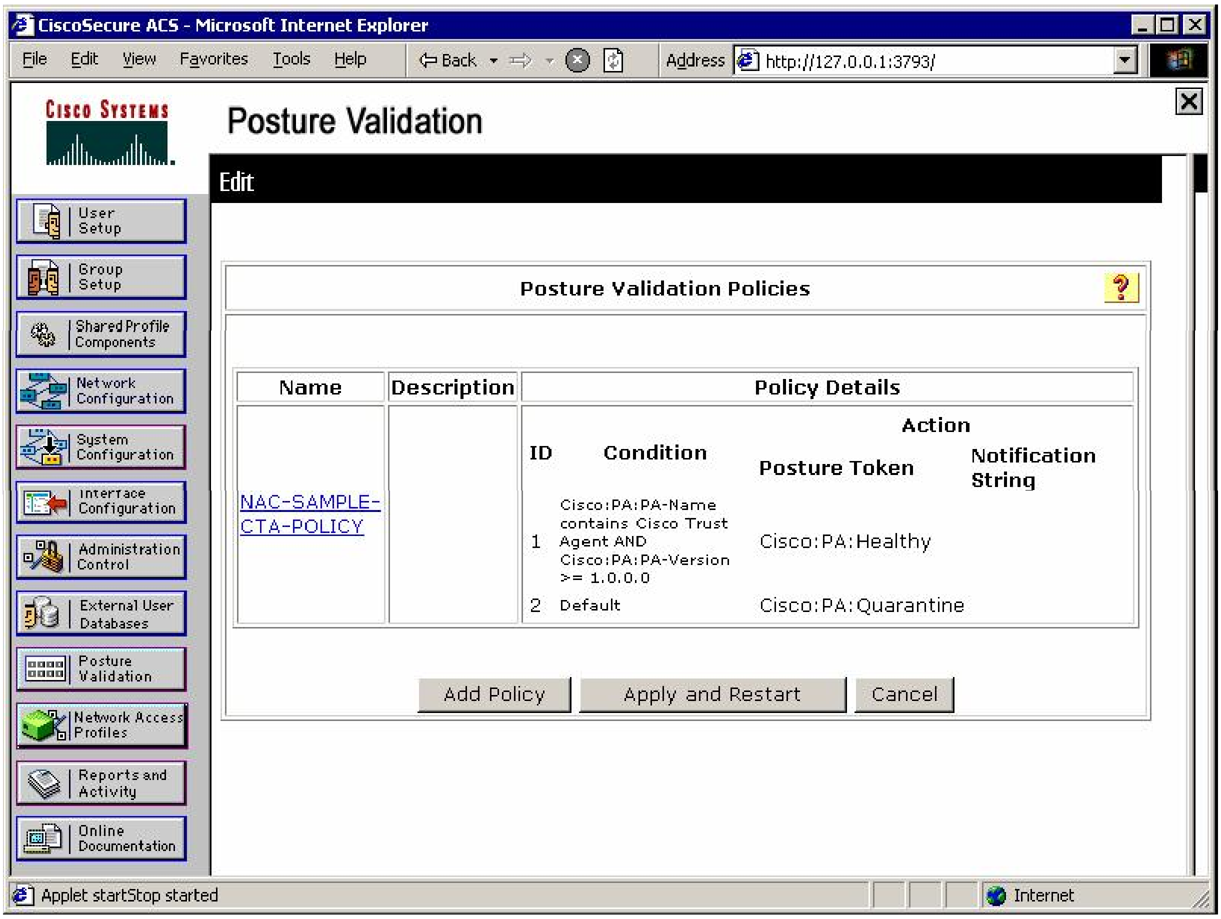
	Name	Policies	Description	Active
○	NAC_L3_IP	Authentication Posture Validation Authorization	NAC Profile for L3 IP access	YES

The Up/Down buttons submit and save the sort order to the database.

○ Deny access when no profile matches

● Grant access using global configuration,when no profile matches

Modify Internal Posture Validation policy created from template:



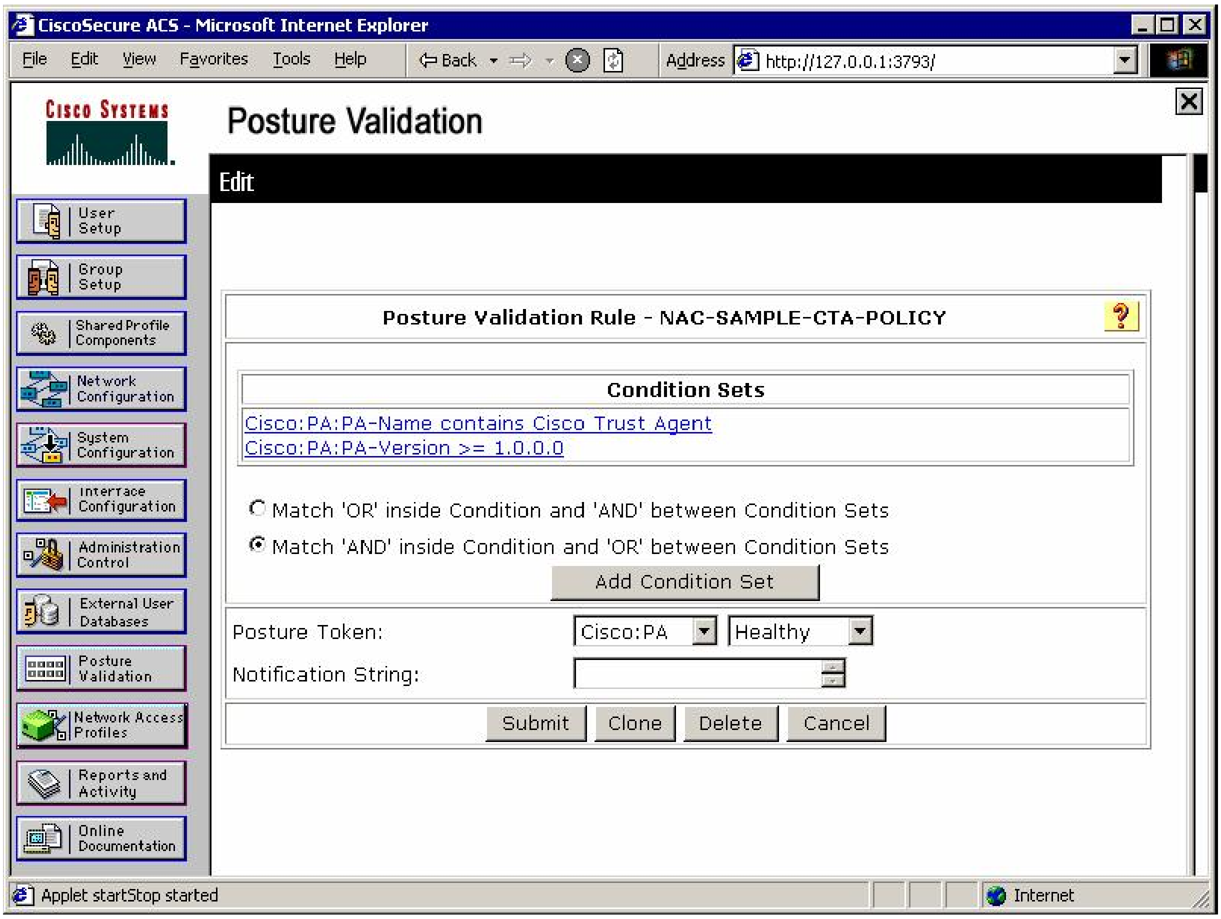
Posture Validation

Edit

Posture Validation Policies

Name	Description	Policy Details			
		ID	Condition	Action	
				Posture Token	Notification String
NAC-SAMPLE-CTA-POLICY		1	Cisco:PA:PA-Name contains Cisco Trust Agent AND Cisco:PA:PA-Version >= 1.0.0.0	Cisco:PA:Healthy	
		2	Default	Cisco:PA:Quarantine	

Modify Posture Validation Rule:



Posture Validation Rule - NAC-SAMPLE-CTA-POLICY

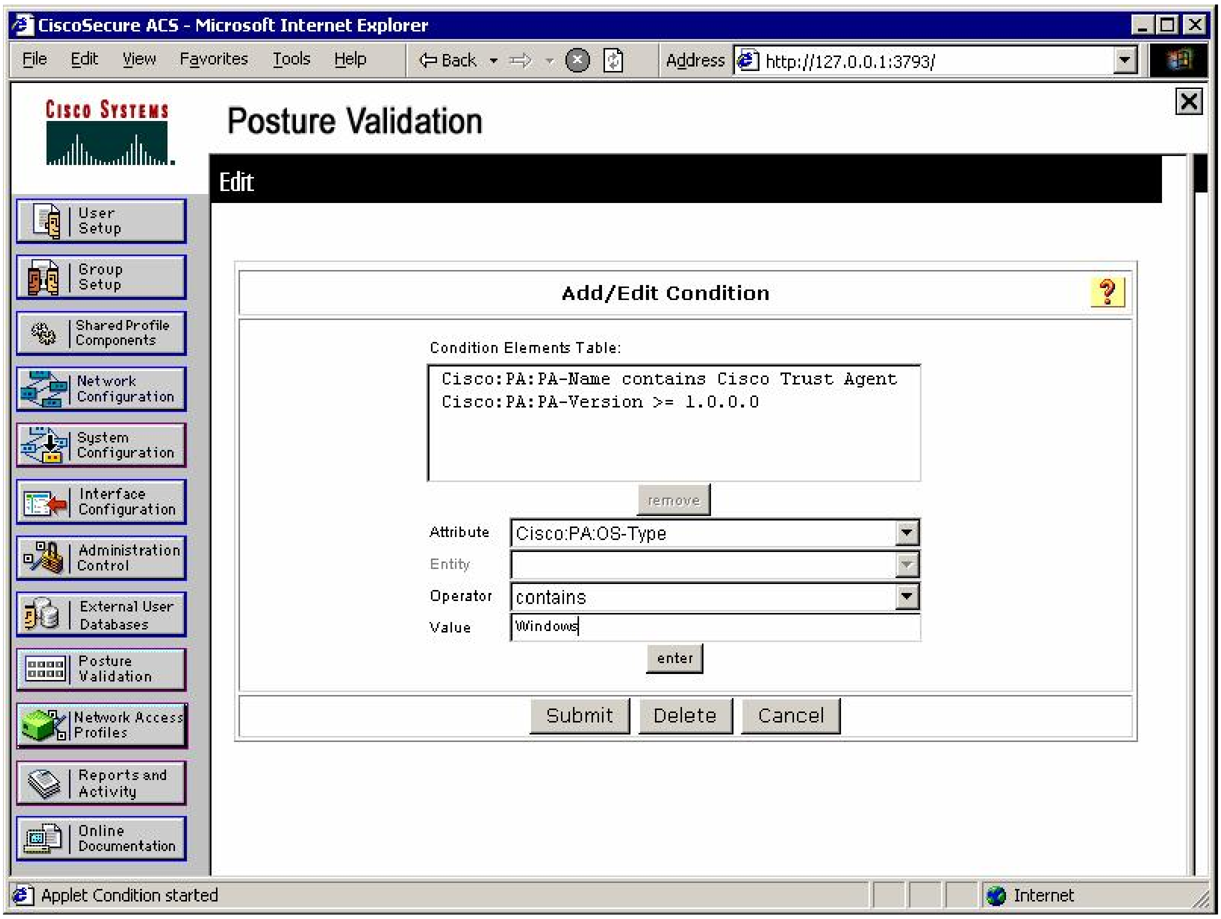
Condition Sets

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

Posture Token: Cisco:PA Healthy
Notification String:

Add check for OS type:



Condition Elements Table:

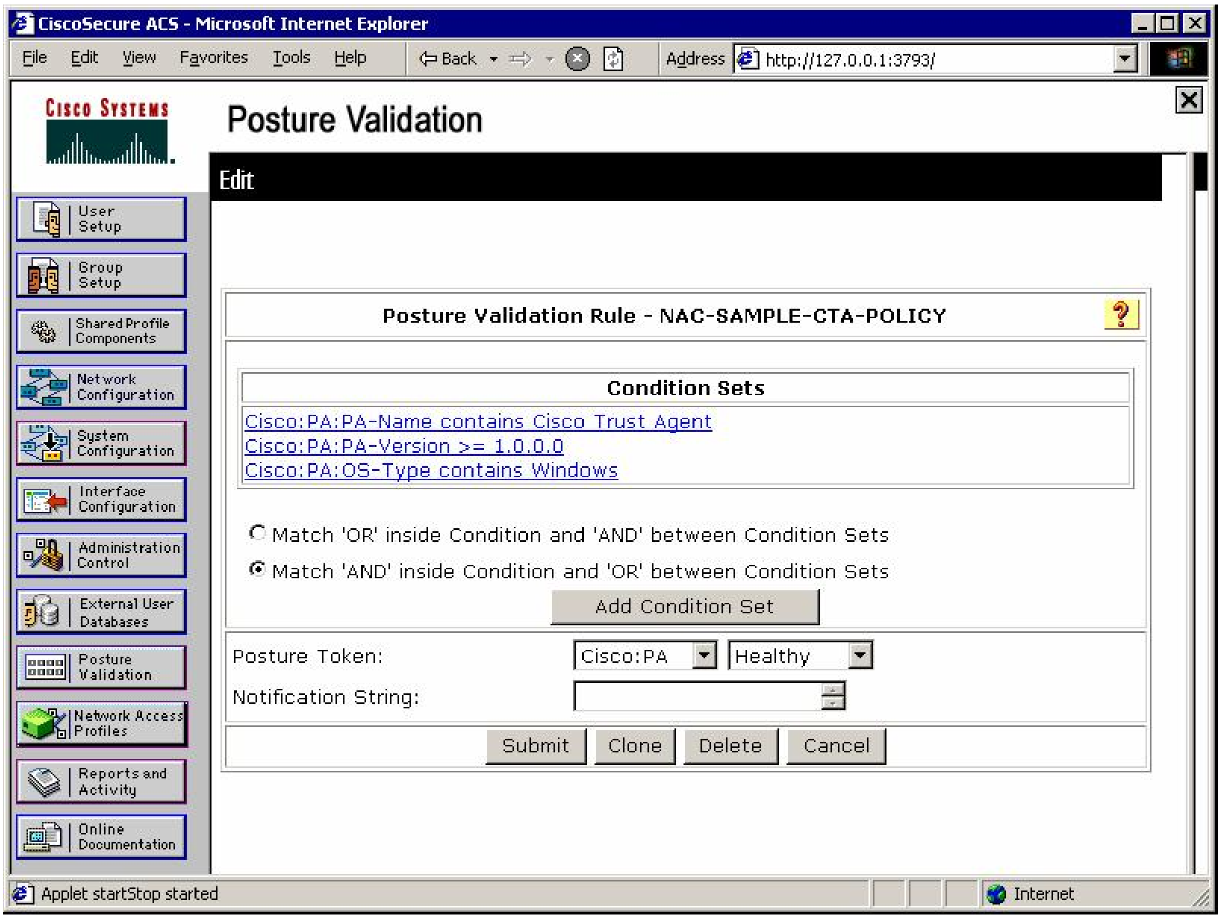
```
Cisco:PA:PA-Name contains Cisco Trust Agent
Cisco:PA:PA-Version >= 1.0.0.0
```

Attribute: Cisco:PA:OS-Type

Entity:

Operator: contains

Value: Windows



Posture Validation

Edit

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
Cisco:PA:OS-Type contains Windows

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

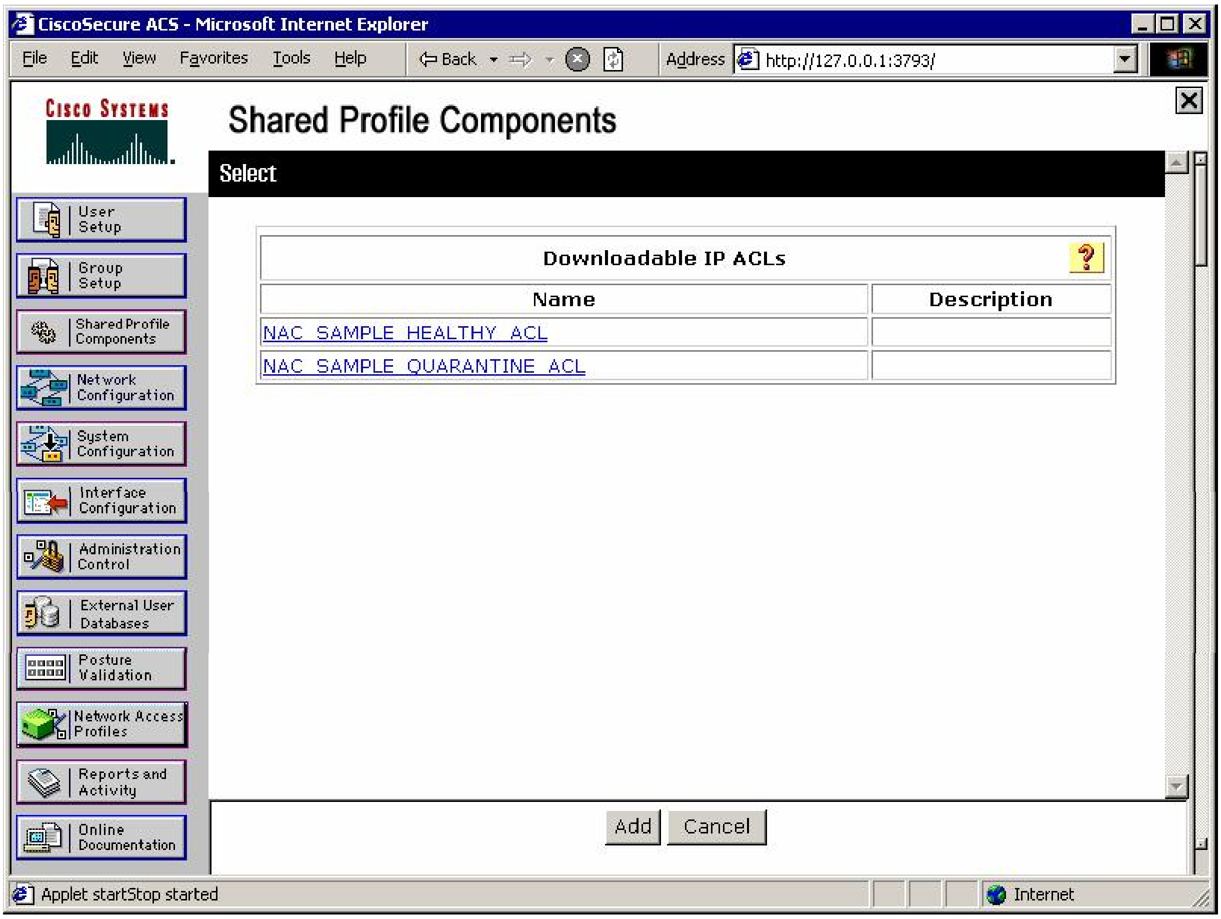
Add Condition Set

Posture Token: Cisco:PA Healthy

Notification String:

Submit Clone Delete Cancel

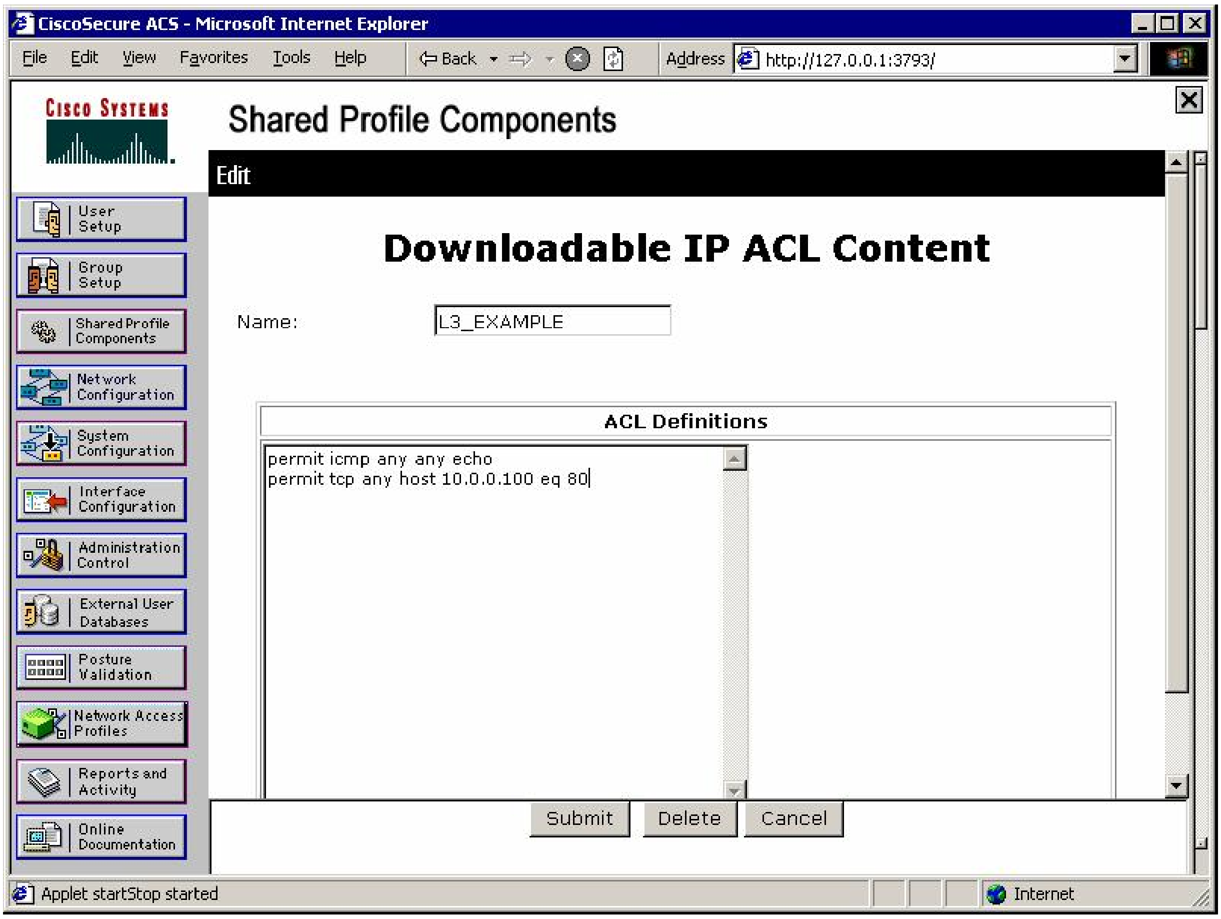
Modify downloadable ACL for 'Quarantine' posture:



Shared Profile Components

Select

Downloadable IP ACLs	
Name	**Description**
NAC_SAMPLE_HEALTHY_ACL	
NAC_SAMPLE_QUARANTINE_ACL	



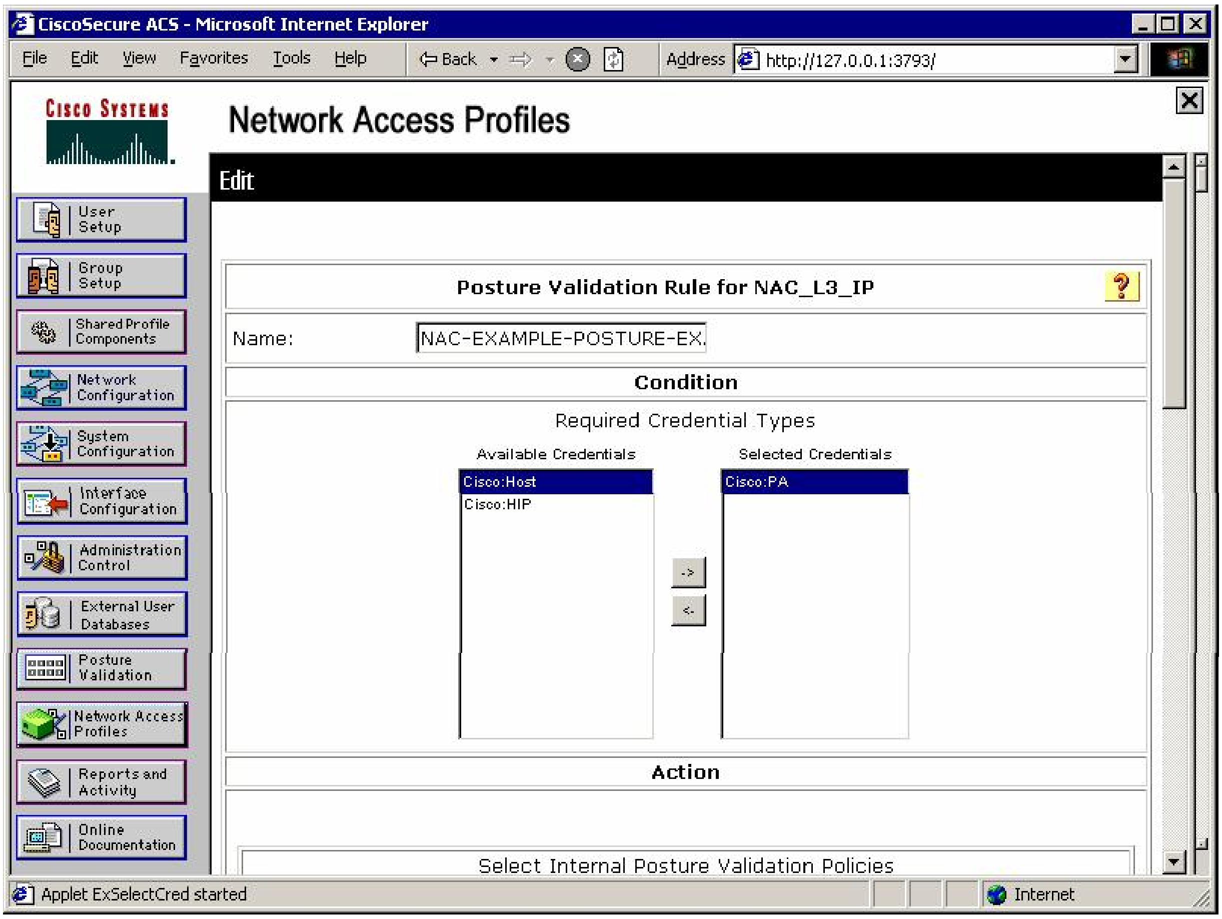
Downloadable IP ACL Content

Name: L3_EXAMPLE

ACL Definitions

```
permit icmp any any echo
permit tcp any host 10.0.0.100 eq 80
```

Modify Posture Validation for created NAP:



Posture Validation Rule for NAC_L3_IP

Name: NAC-EXAMPLE-POSTURE-EX.

Condition

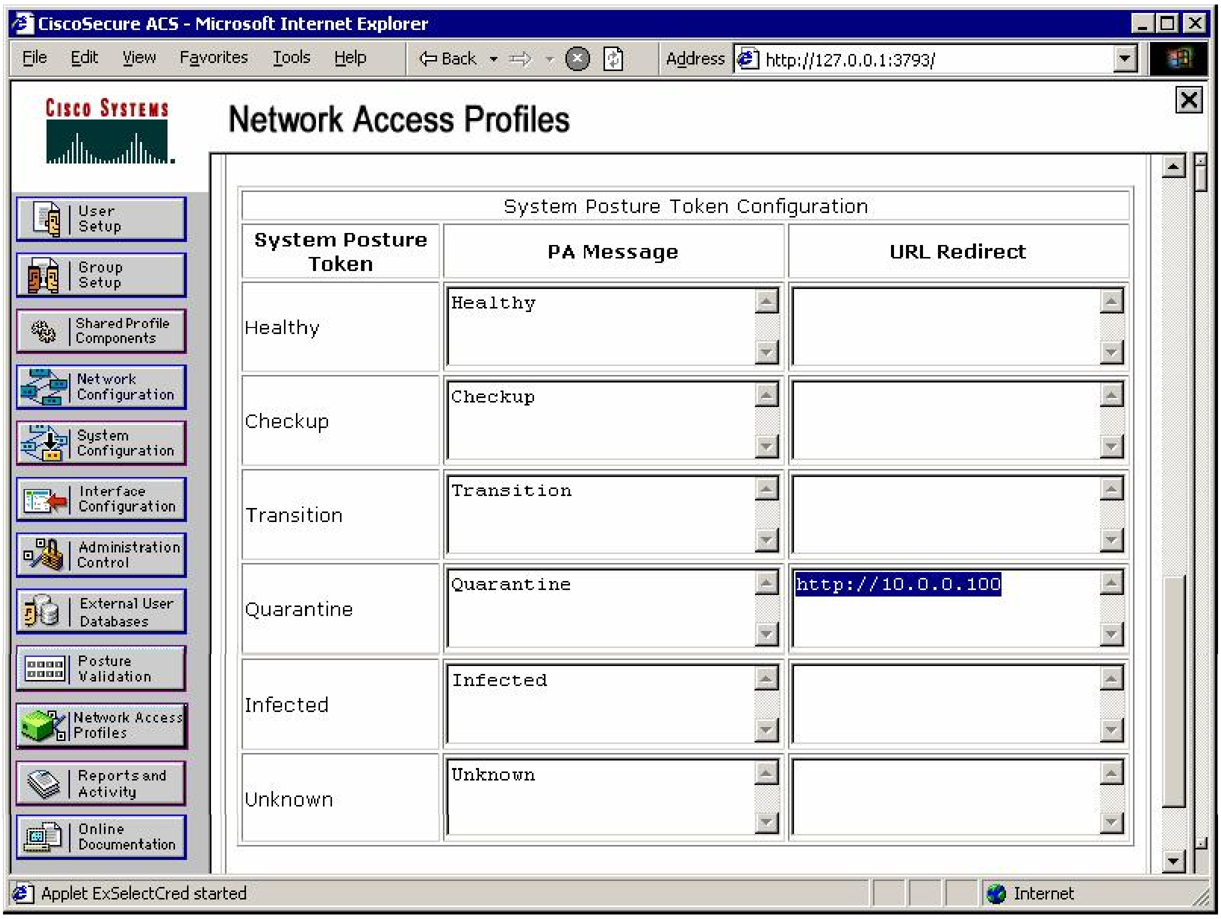
Required Credential Types

Available Credentials	Selected Credentials
Cisco:Host	Cisco:PA
Cisco:HIP	

Action

Select Internal Posture Validation Policies

Add URL Redirect for 'Quarantine' Posture:



Network Access Profiles

System Posture Token Configuration

System Posture Token	PA Message	URL Redirect
Healthy	Healthy	
Checkup	Checkup	
Transition	Transition	
Quarantine	Quarantine	http://10.0.0.100
Infected	Infected	
Unknown	Unknown	

Further Reading

General NAC:

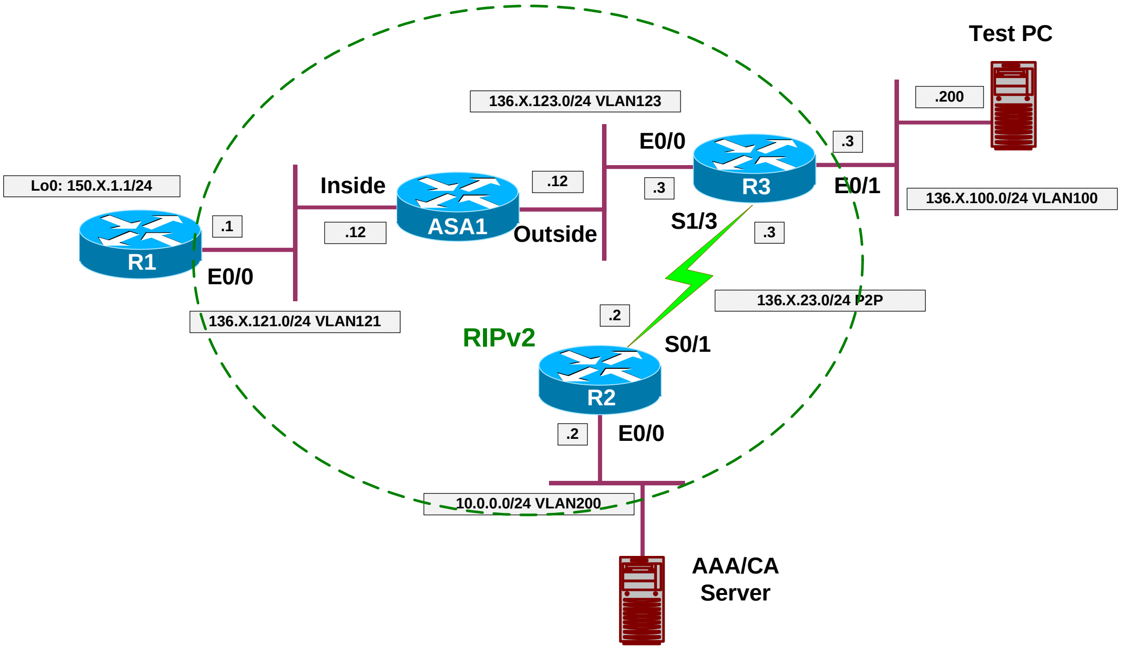
Implementing Network Admission Control - Phase One Configuration and Deployment
Network Admission Control (NAC) FAQ
Network Admission Control (NAC) Framework Deployment Guide
Network Admission Control (NAC) Framework Configuration Guide

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

      ’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.

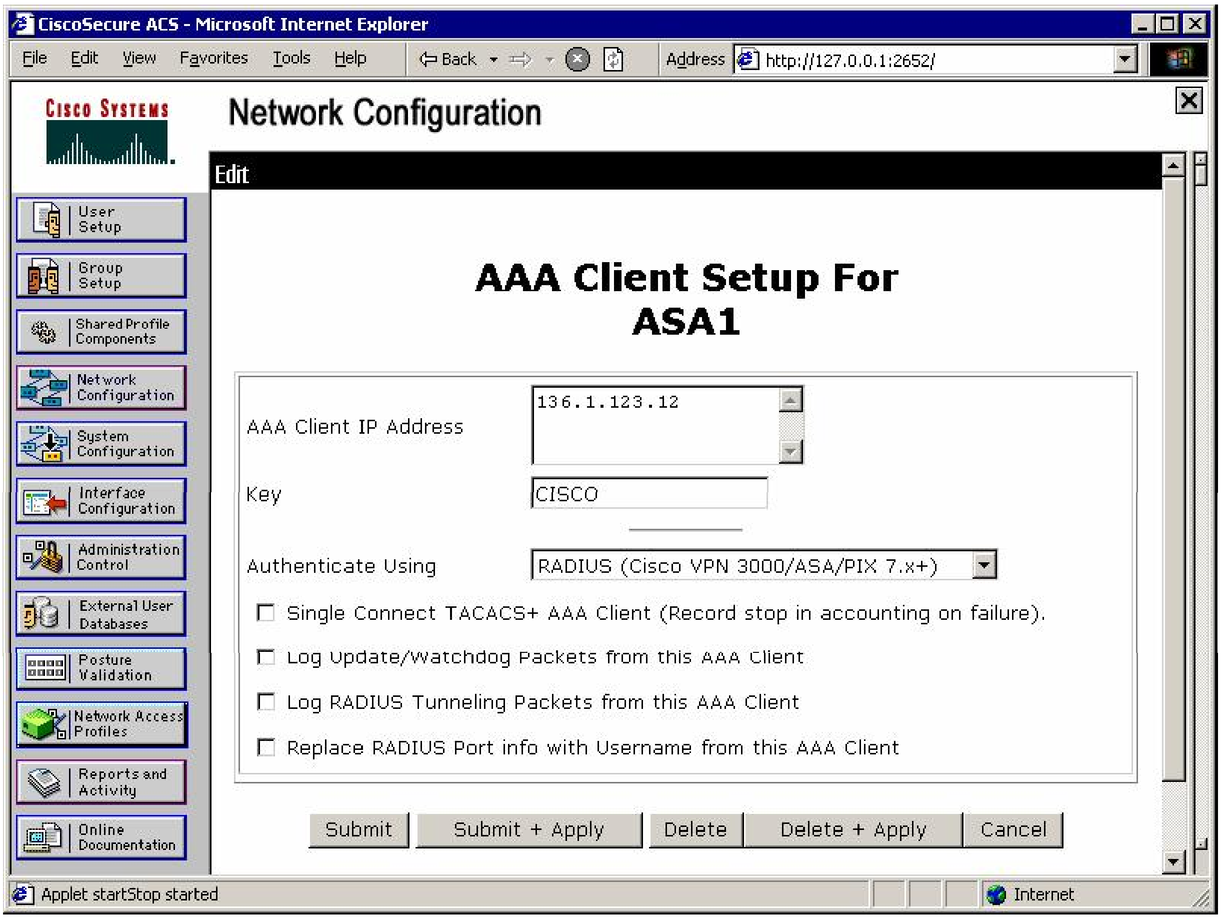
Final Configuration

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:



Network Configuration

Edit

AAA Client Setup For ASA1

AAA Client IP Address: 136.1.123.12

Key: CISCO

Authenticate Using: RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

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

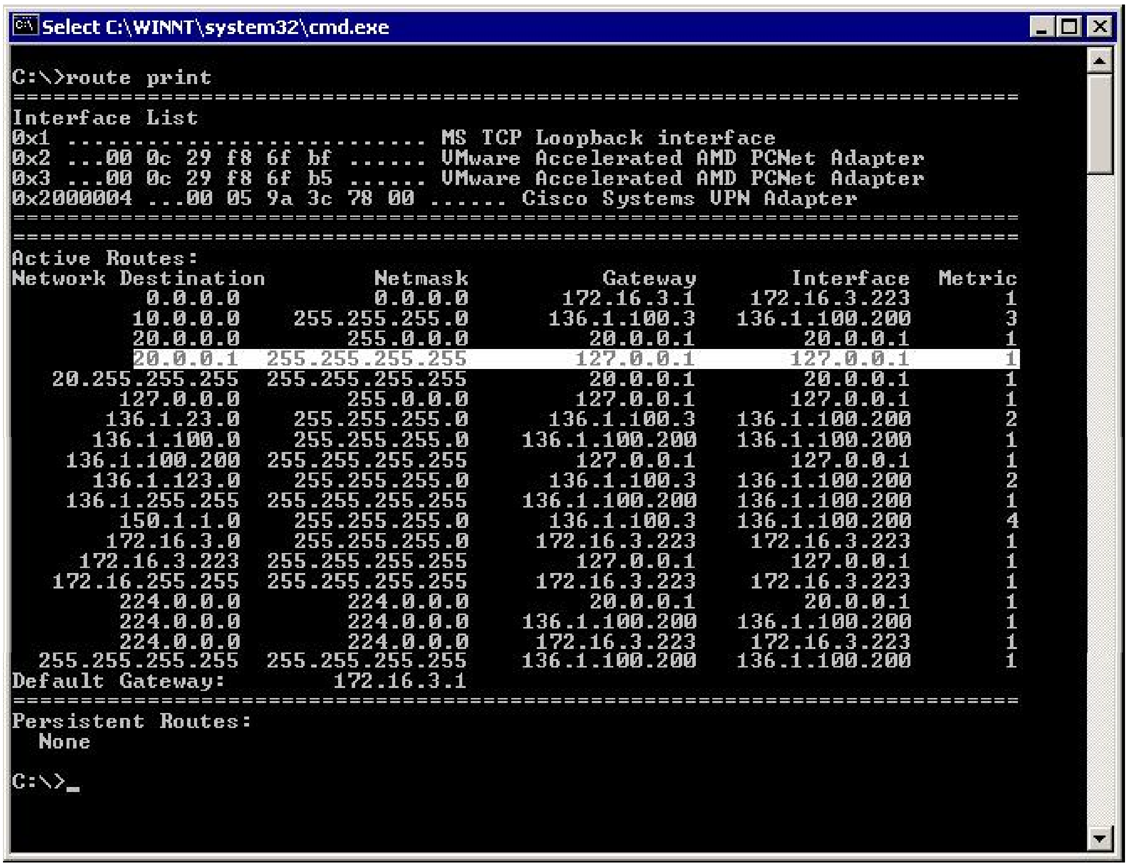
□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

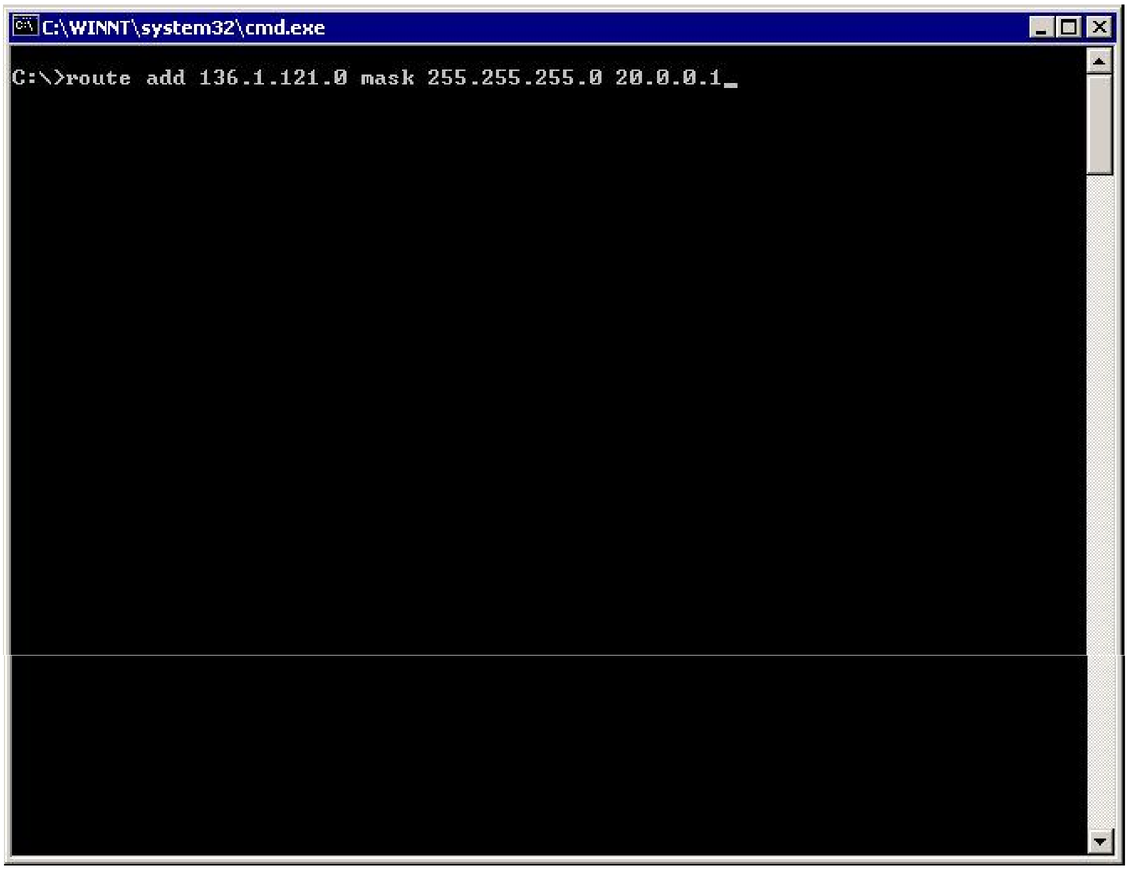
Test PC:

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



```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0c 29 f8 6f bf ...... VMware Accelerated AMD PCNet Adapter
0x3 ...00 0c 29 f8 6f b5 ...... VMware Accelerated AMD PCNet Adapter
0x2000004 ...00 05 9a 3c 78 00 ...... Cisco Systems VPN Adapter
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       172.16.3.1    172.16.3.223       1
         10.0.0.0    255.255.255.0      136.1.100.3   136.1.100.200       3
         20.0.0.0        255.0.0.0         20.0.0.1        20.0.0.1       1
         20.0.0.1  255.255.255.255        127.0.0.1       127.0.0.1       1
   20.255.255.255  255.255.255.255         20.0.0.1        20.0.0.1       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       136.1.23.0    255.255.255.0      136.1.100.3   136.1.100.200       2
      136.1.100.0    255.255.255.0    136.1.100.200   136.1.100.200       1
    136.1.100.200  255.255.255.255        127.0.0.1       127.0.0.1       1
      136.1.123.0    255.255.255.0      136.1.100.3   136.1.100.200       2
    136.1.255.255  255.255.255.255    136.1.100.200   136.1.100.200       1
        150.1.1.0    255.255.255.0      136.1.100.3   136.1.100.200       4
       172.16.3.0    255.255.255.0     172.16.3.223    172.16.3.223       1
     172.16.3.223  255.255.255.255        127.0.0.1       127.0.0.1       1
   172.16.255.255  255.255.255.255     172.16.3.223    172.16.3.223       1
        224.0.0.0        224.0.0.0         20.0.0.1        20.0.0.1       1
        224.0.0.0        224.0.0.0    136.1.100.200   136.1.100.200       1
        224.0.0.0        224.0.0.0     172.16.3.223    172.16.3.223       1
  255.255.255.255  255.255.255.255    136.1.100.200   136.1.100.200       1
Default Gateway:        172.16.3.1
===========================================================================
Persistent Routes:
  None

C:\>_
```

Execute command "route add 136.1.121.0 255.255.255.0 20.0.0.1":



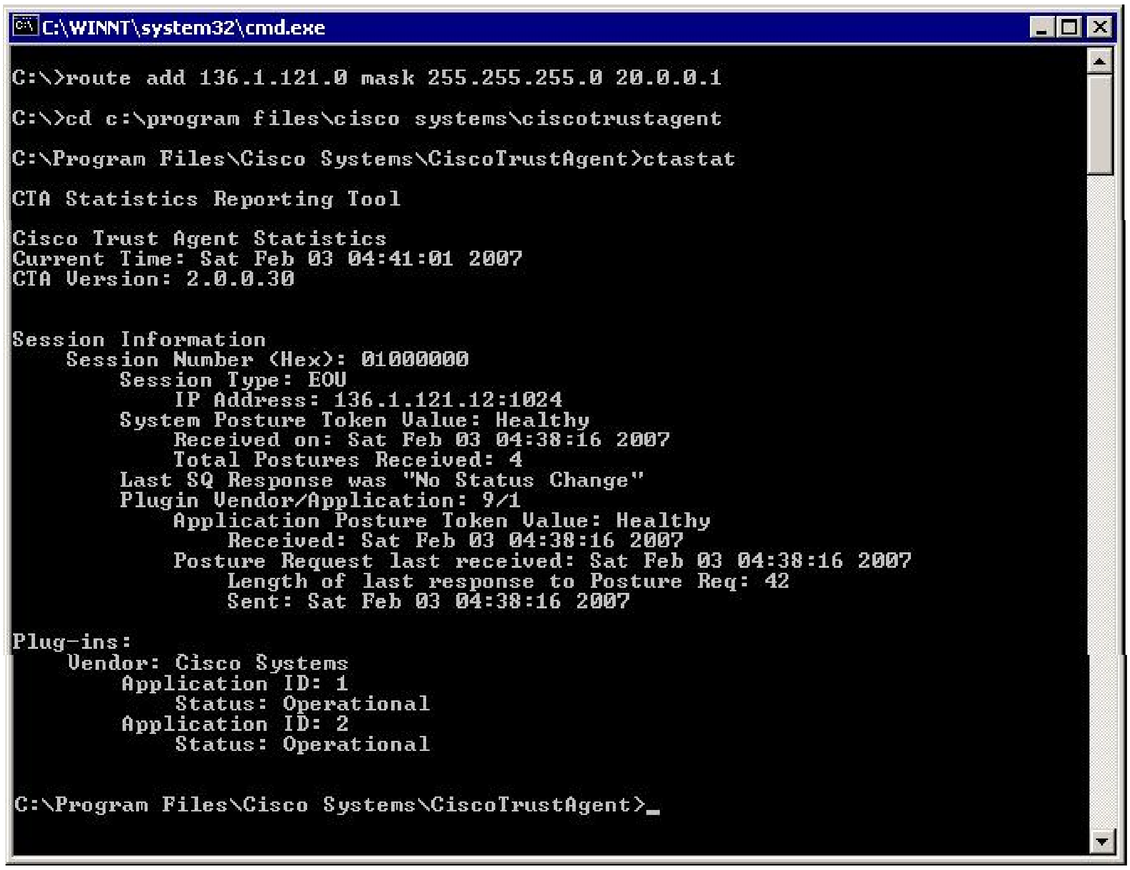
```
C:\>route add 136.1.121.0 mask 255.255.255.0 20.0.0.1_
```

Verification

```
ASA1(config)# debug nac all
ASA1(config)# eou reval all
1 seAssions.list has
NAC 'RevalidateS All' request by adAministrative 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

Session Type: Remote

Username     : CISCO
Index        : 1
Assigned IP  : 20.0.0.1               Public IP    : 136.1.100.200
Protocol     : IPSec                  Encryption   : 3DES
Hashing      : MD5
Bytes Tx     : 3872                   Bytes Rx     : 2128
```

```
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)
access-list #ACSACL#-IP-NAC_SAMPLE_HEALTHY_ACL-45c43e78 line 1 extended permit
ip any any (hitcnt=0) 0xfefd8fe
```

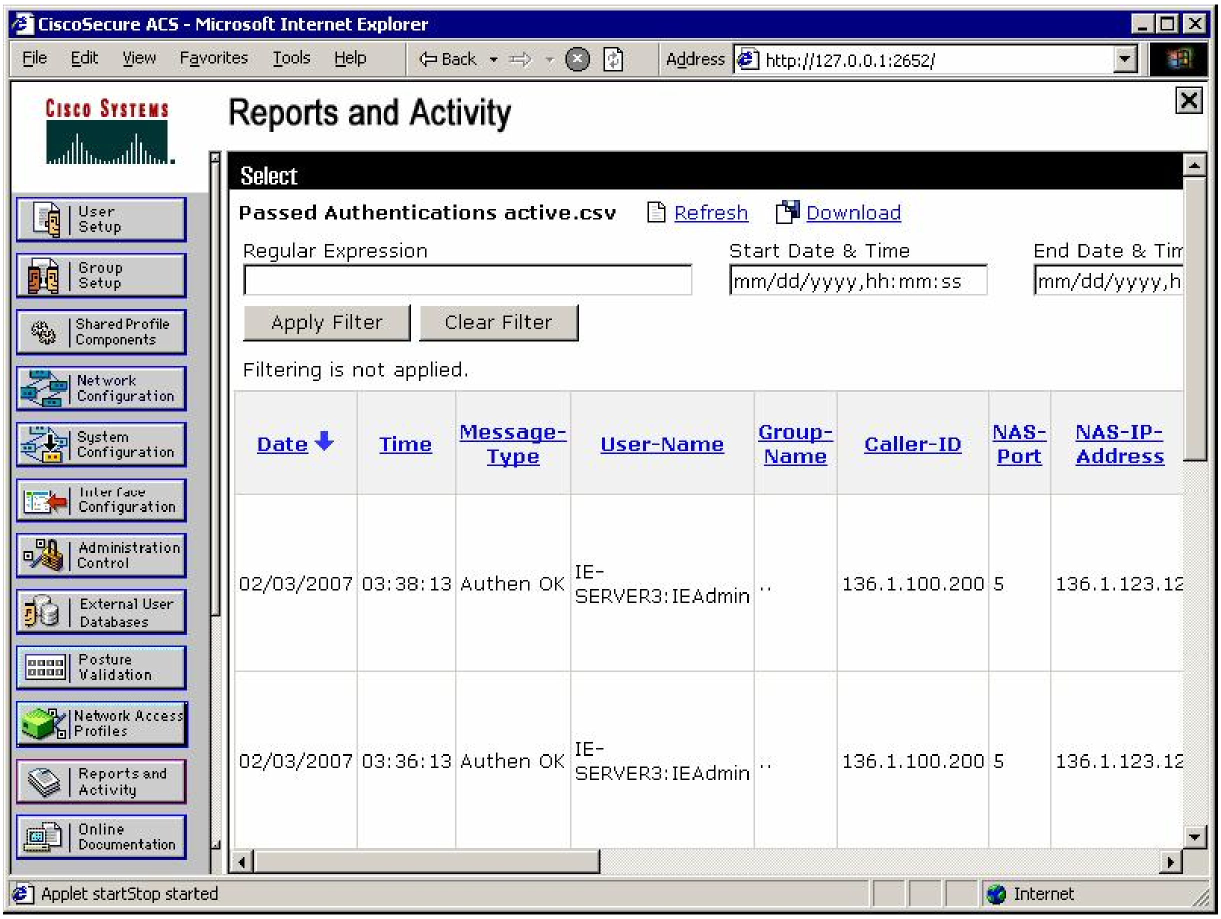
Test PC:



```
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>ctastat

CTA Statistics Reporting Tool

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: 136.1.121.12:1024
        System Posture Token Value: Healthy
            Received on: Sat Feb 03 04:38:16 2007
            Total Postures Received: 4
        Last SQ 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: 42
                Sent: Sat Feb 03 04:38:16 2007

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


C:\Program Files\Cisco Systems\CiscoTrustAgent>_
```

ACS:

Reports & Activity/Passed Authentications:



Passed Authentications active.csv

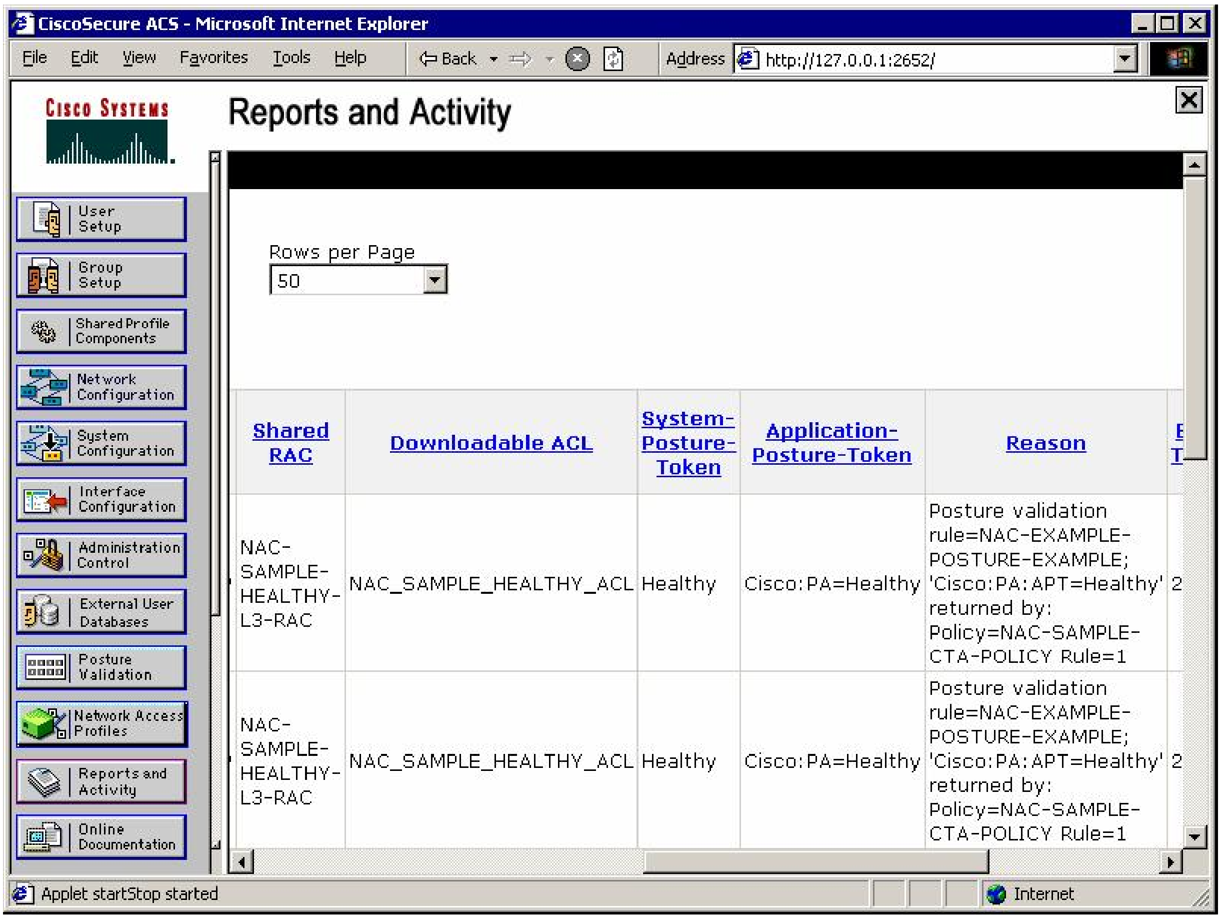
Regular Expression

Start Date & Time mm/dd/yyyy,hh:mm:ss

End Date & Tim mm/dd/yyyy,h

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
02/03/2007	03:38:13	Authen OK	IE-SERVER3:IEAdmin	..	136.1.100.200	5	136.1.123.12
02/03/2007	03:36:13	Authen OK	IE-SERVER3:IEAdmin	..	136.1.100.200	5	136.1.123.12



Reports and Activity

Rows per Page
50

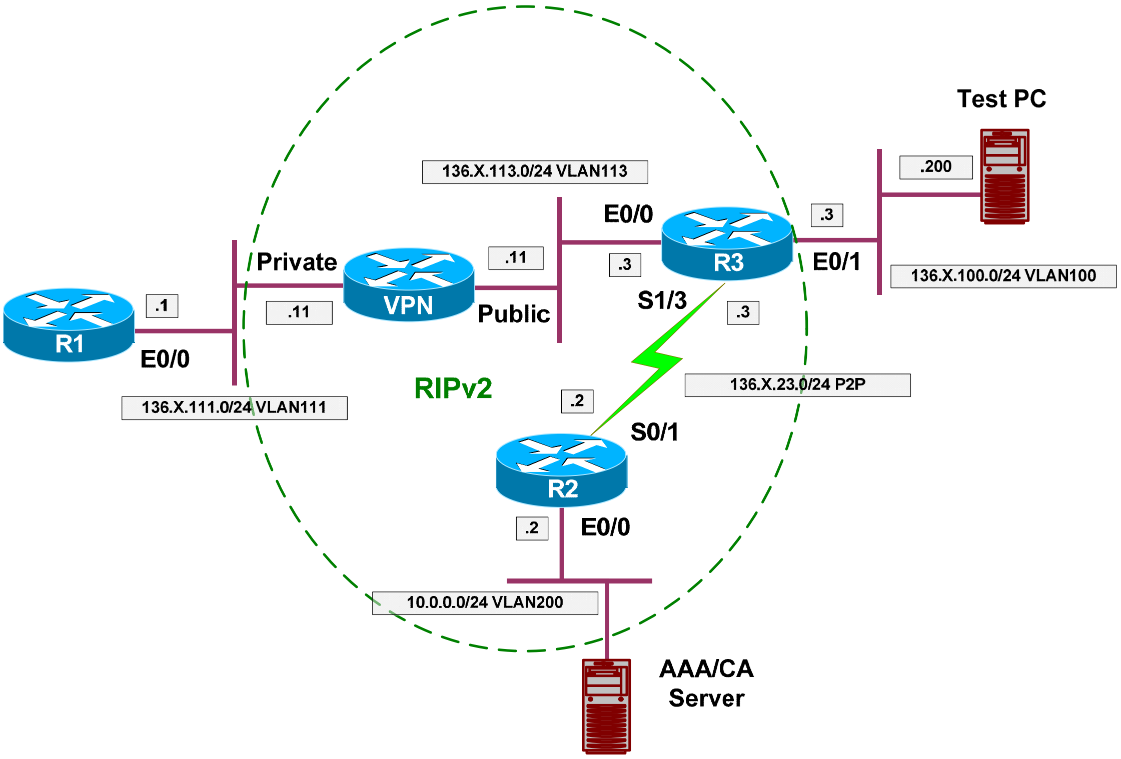
Shared RAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	E T
NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL	Healthy	Cisco:PA=Healthy	Posture validation rule=NAC-EXAMPLE-POSTURE-EXAMPLE; 'Cisco:PA:APT=Healthy' returned by: Policy=NAC-SAMPLE-CTA-POLICY Rule=1	2
NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL	Healthy	Cisco:PA=Healthy	Posture validation rule=NAC-EXAMPLE-POSTURE-EXAMPLE; 'Cisco:PA:APT=Healthy' returned by: Policy=NAC-SAMPLE-CTA-POLICY Rule=1	2

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:
  - o Add RADIUS authentication server for Posture Validation.
  - o Add rules for RADIUS traffic to Public Filter:
    - Permit UDP ports 1645 and 1646
  - o Configure ACS to support new network client.
  - o Create filter named NAC_DEFAULT:
    - Add rule “EAPoUDP” and permit inbound anybody from UDP port 21862 to any with this rule.
  - o Confiugre 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:

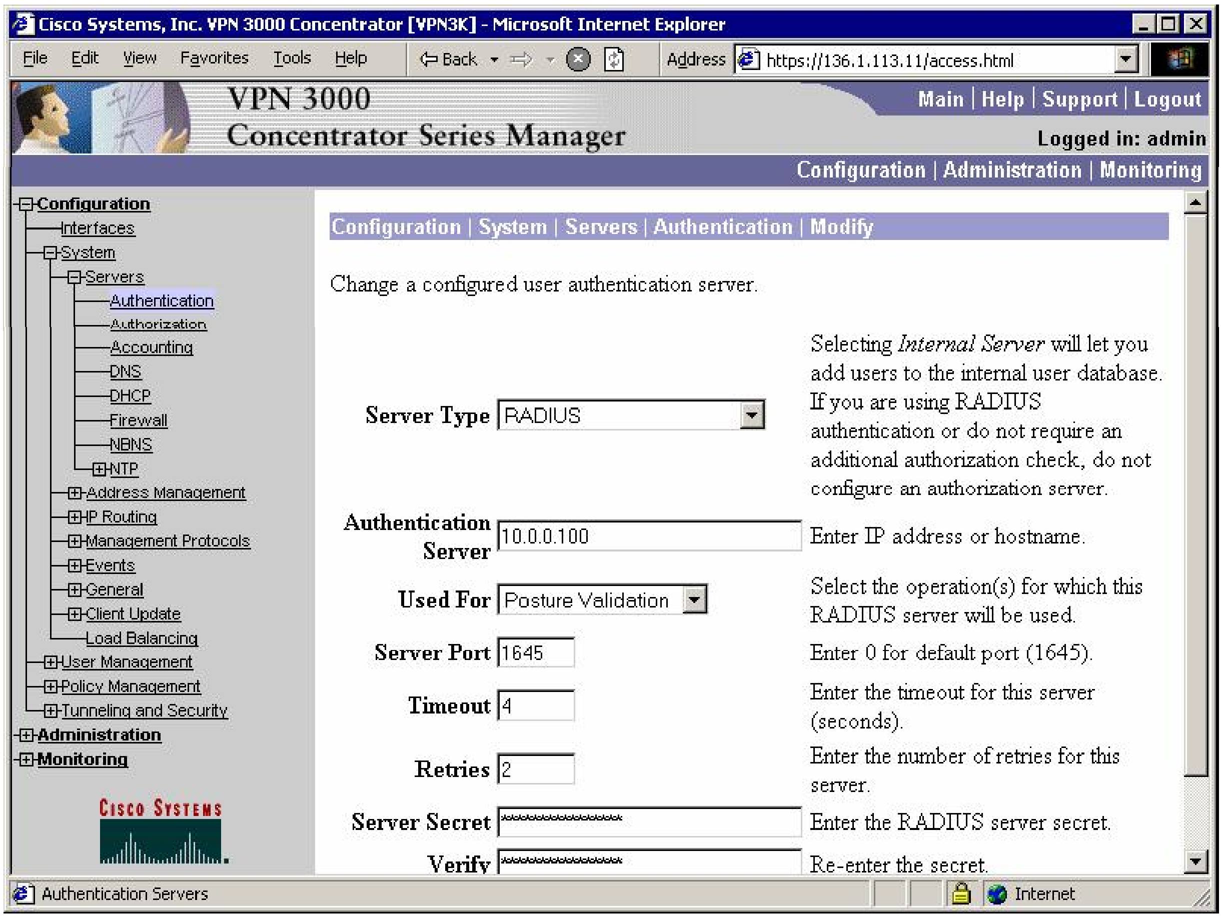
      ’ctacert.exe /add c:\mycerts\ACS.cer /store “Root”’

- 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"):

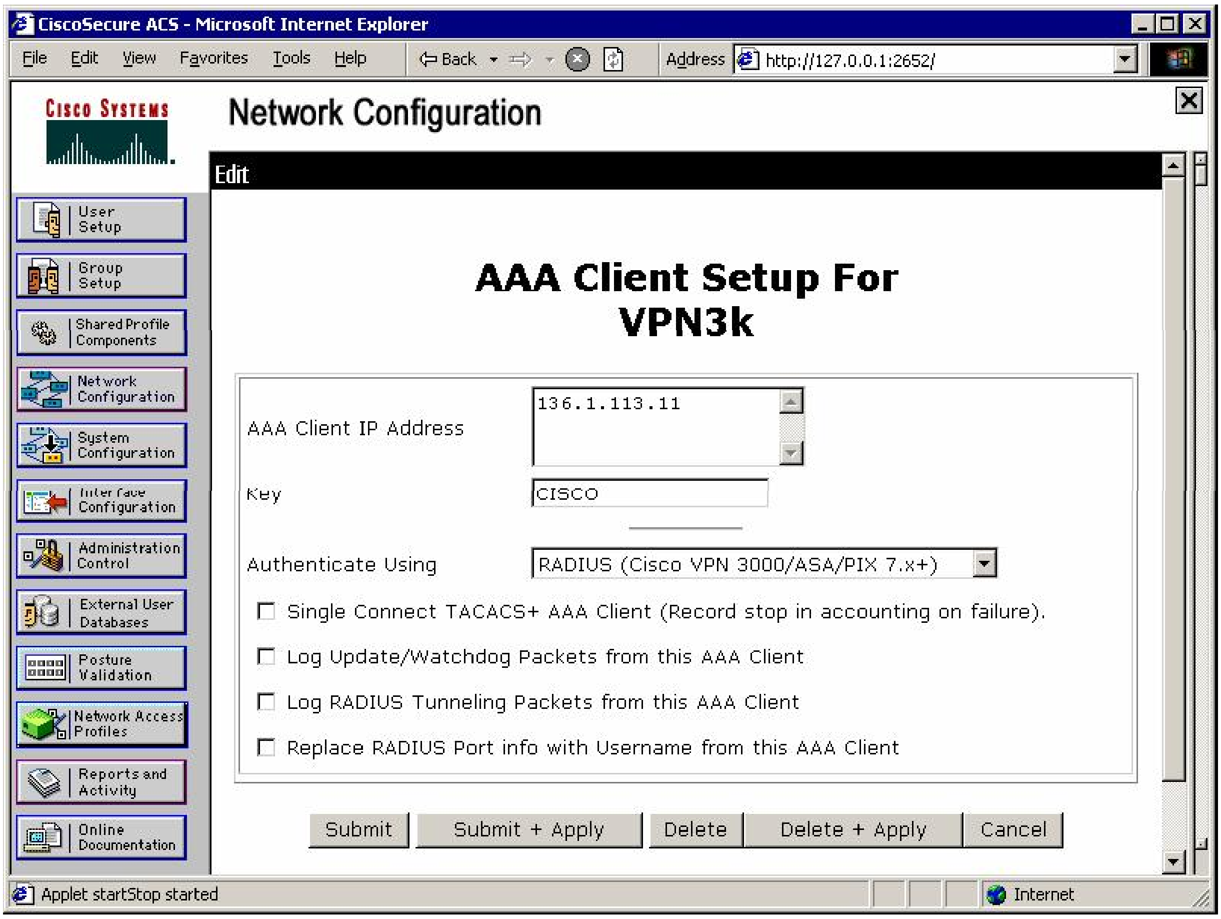


Configuration | System | Servers | Authentication | Modify

Change a configured user authentication server.

Server Type	RADIUS	Selecting *Internal Server* 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 Server	10.0.0.100	Enter IP address or hostname.
Used For	Posture Validation	Select the operation(s) for which this RADIUS server will be used.
Server Port	1645	Enter 0 for default port (1645).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.
Server Secret	****************	Enter the RADIUS server secret.
Verify	****************	Re-enter the secret.

Configure ACS server repsectivty to support RADIUS client:



Network Configuration

Edit

AAA Client Setup For VPN3k

AAA Client IP Address: 136.1.113.11

Key: CISCO

Authenticate Using: RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

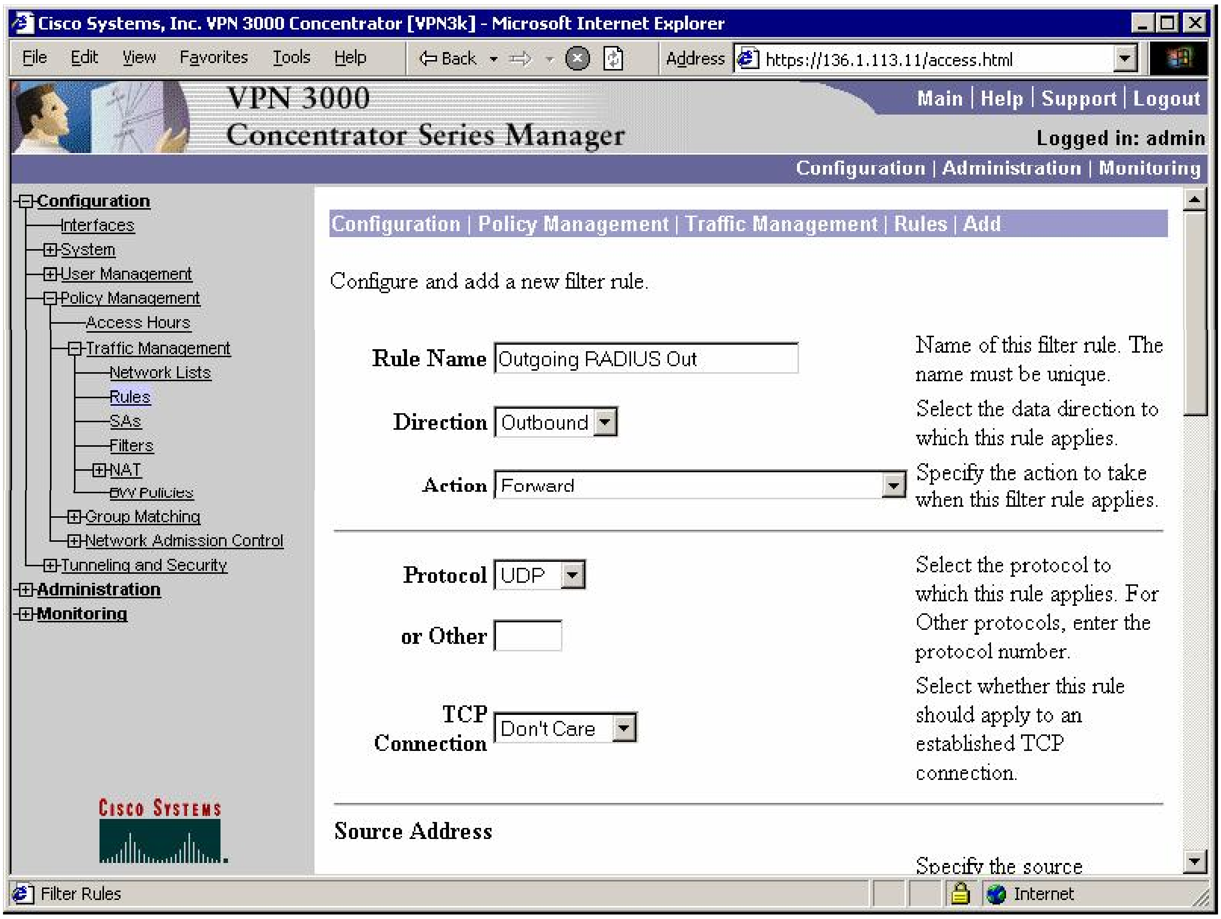
☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

☐ Log Update/Watchdog Packets from this AAA Client

☐ Log RADIUS Tunneling Packets from this AAA Client

☐ Replace RADIUS Port info with Username from this AAA Client

Configure Rule for Outgoing RADIUS traffic Out:



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Rules
Internet

Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name Outgoing RADIUS Out — Name of this filter rule. The name must be unique.

Direction Outbound — Select the data direction to which this rule applies.

Action Forward — Specify the action to take when this filter rule applies.

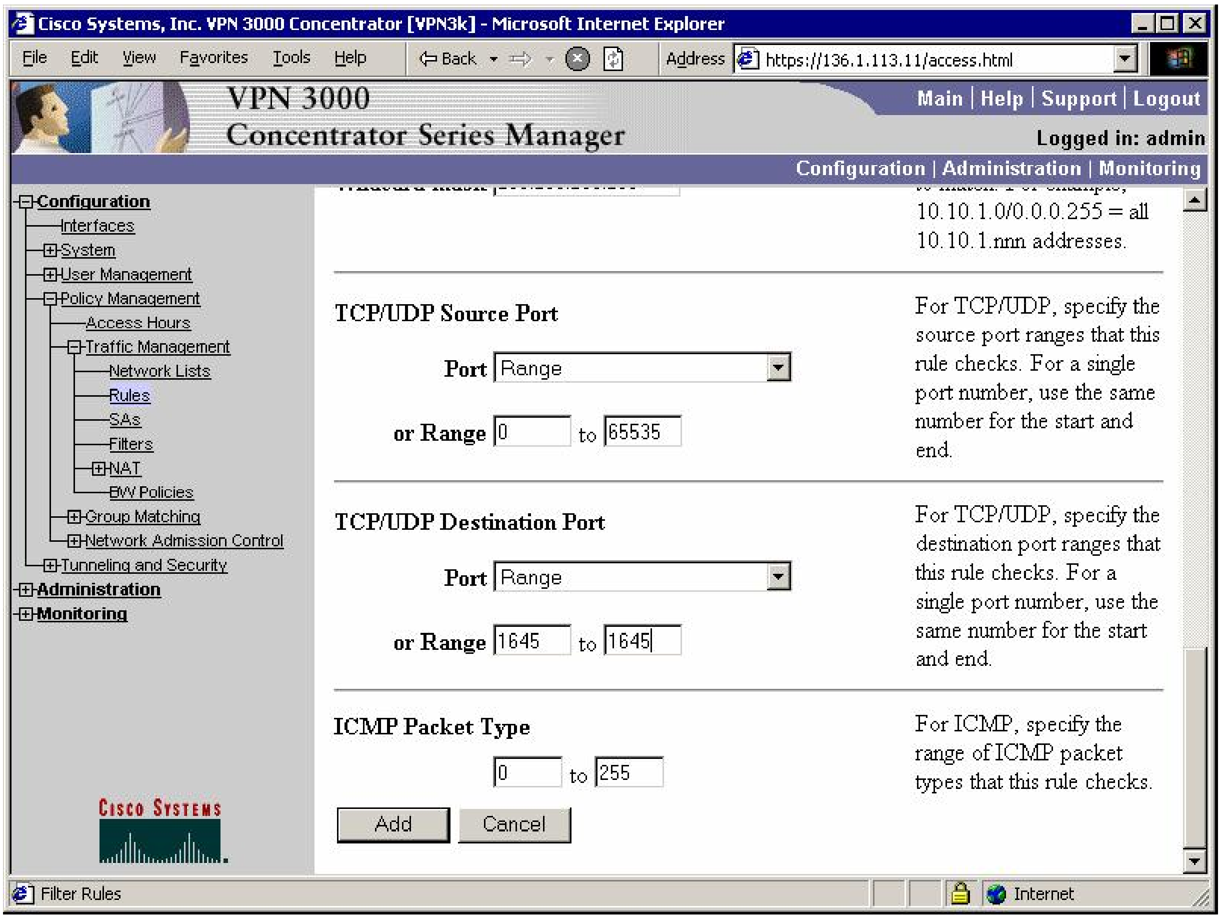
Protocol UDP — Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

or Other

TCP Connection Don't Care — Select whether this rule should apply to an established TCP connection.

Source Address

Specify the source


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Rules
Internet

10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

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.

TCP/UDP Destination Port

Port Range

or Range 1645 to 1645

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.

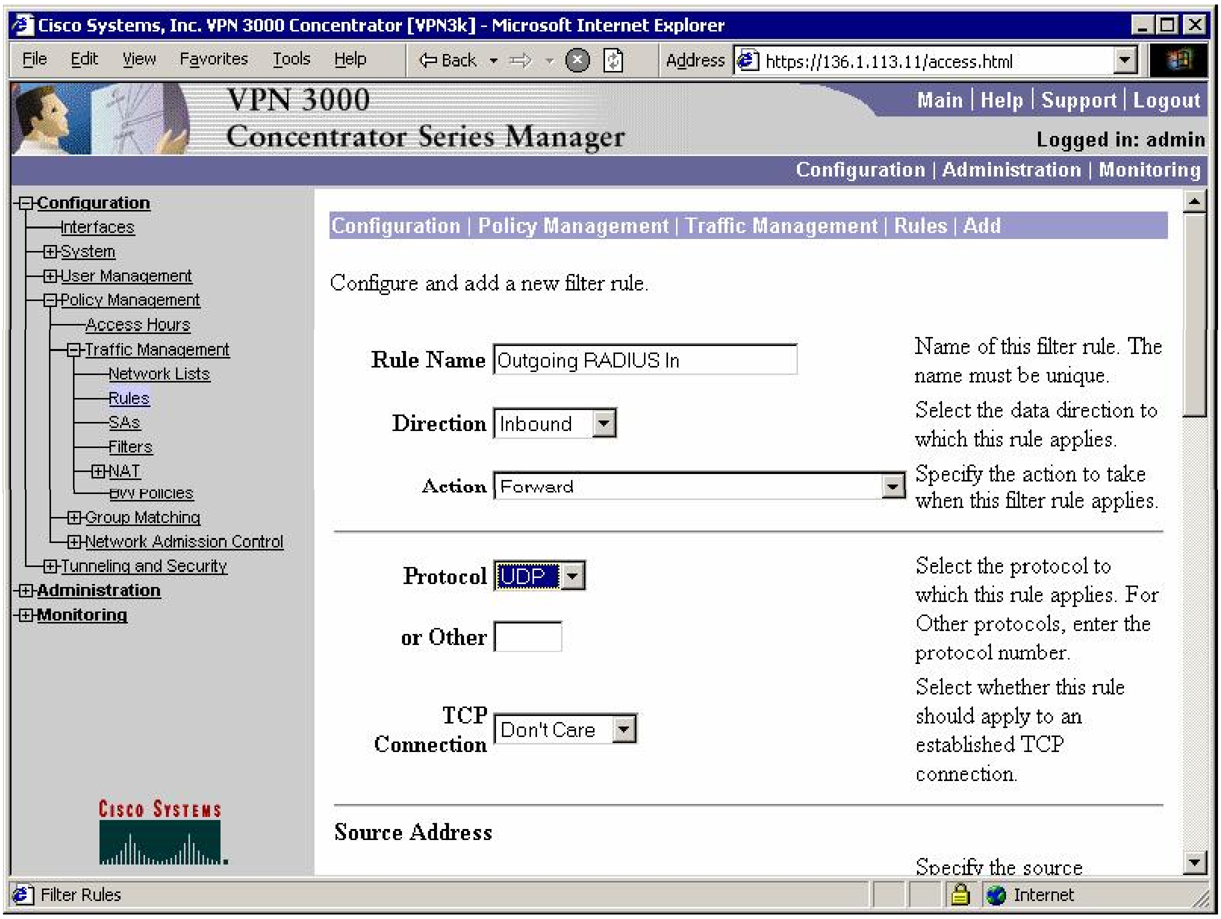
ICMP Packet Type

0 to 255

For ICMP, specify the range of ICMP packet types that this rule checks.

Add Cancel

Configure Rule for Outgoing RADIUS traffic In:



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Rules
Internet

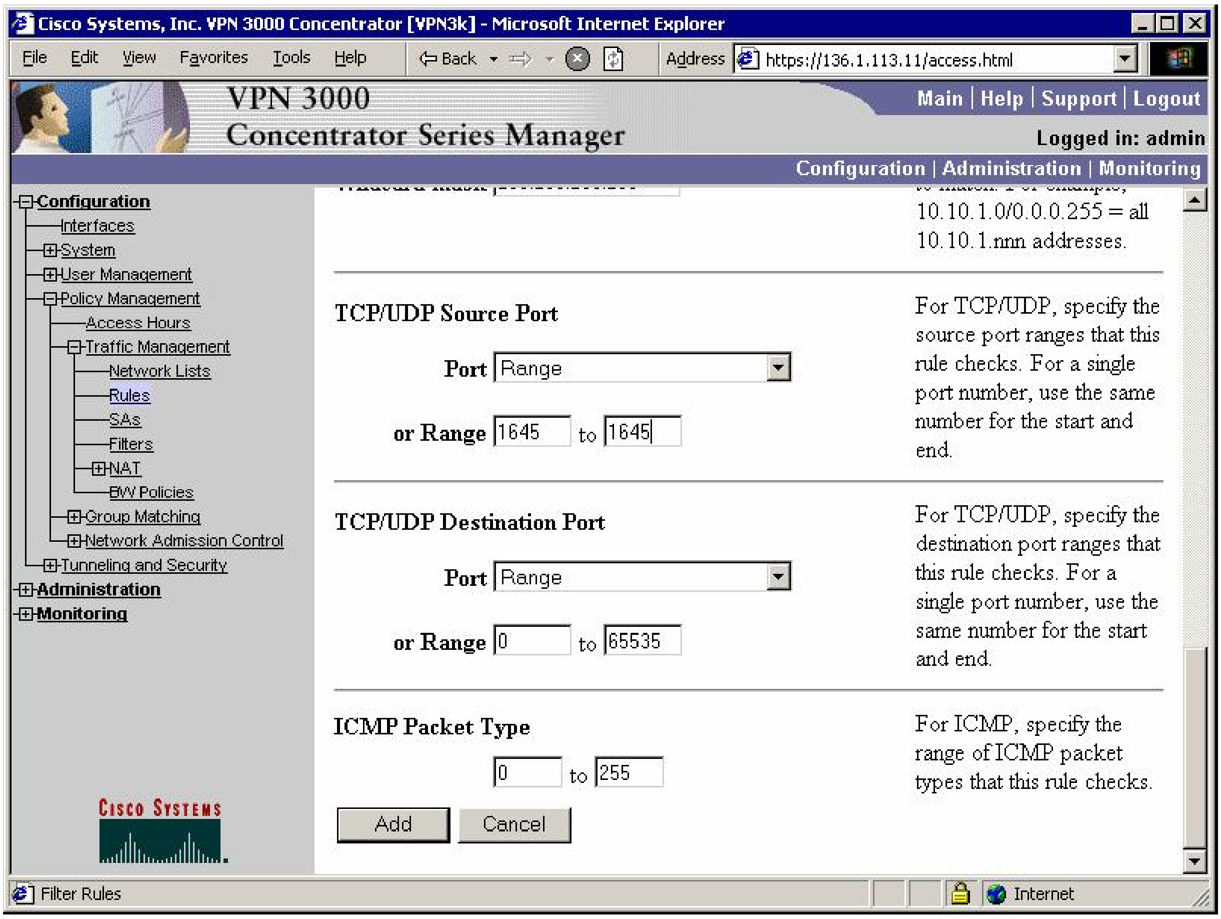
Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name	Outgoing RADIUS 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.
Protocol	UDP	Select the protocol to which this rule applies. For Other protocols, enter the protocol number.
or Other		
TCP Connection	Don't Care	Select whether this rule should apply to an established TCP connection.

Source Address

Specify the source


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Rules
Internet

10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

TCP/UDP Source Port

Port: Range

or Range: 1645 to 1645

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: Range

or Range: 0 to 65535

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.

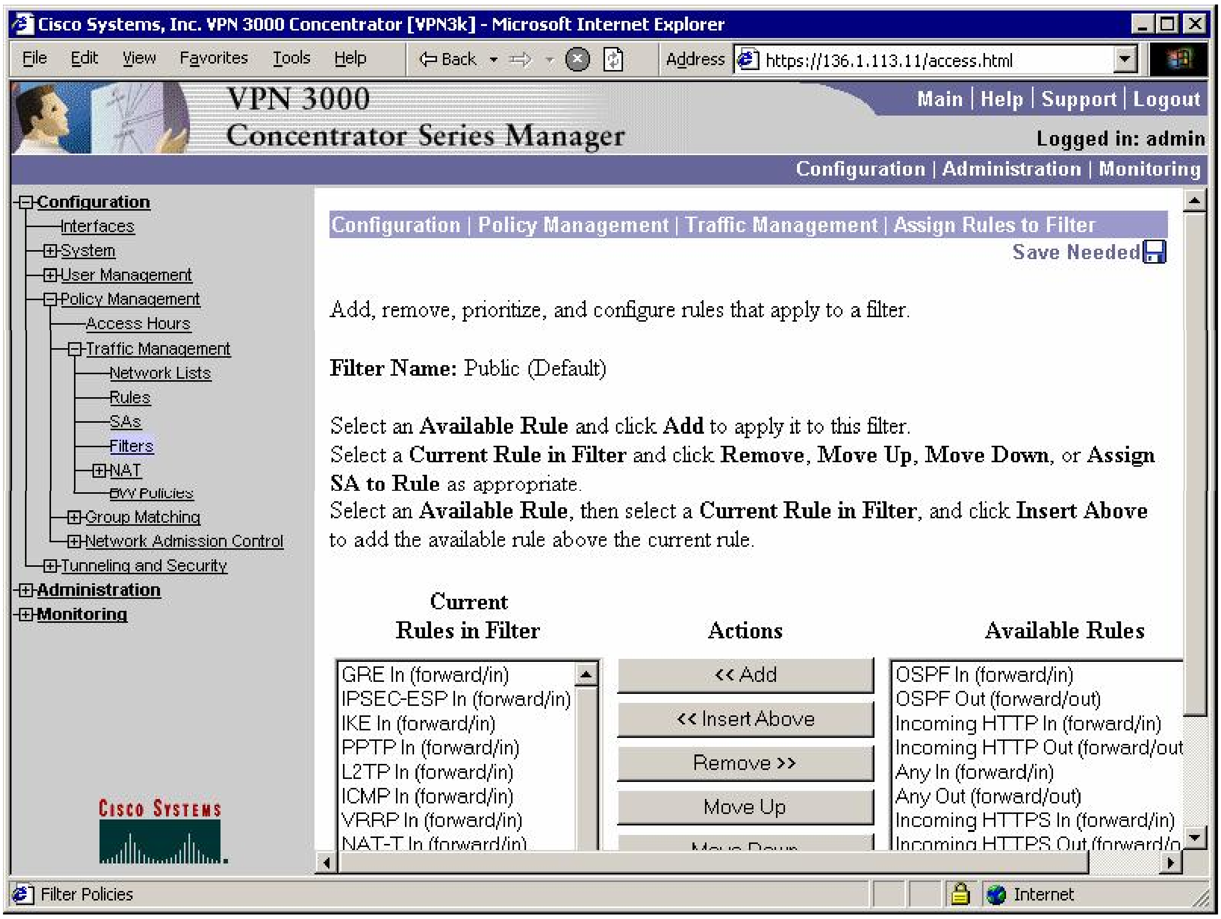
ICMP Packet Type

0 to 255

For ICMP, specify the range of ICMP packet types that this rule checks.

Add | Cancel

Assign both rules to the Public filter:



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Policies
Internet

Configuration | Policy Management | Traffic Management | Assign Rules to Filter

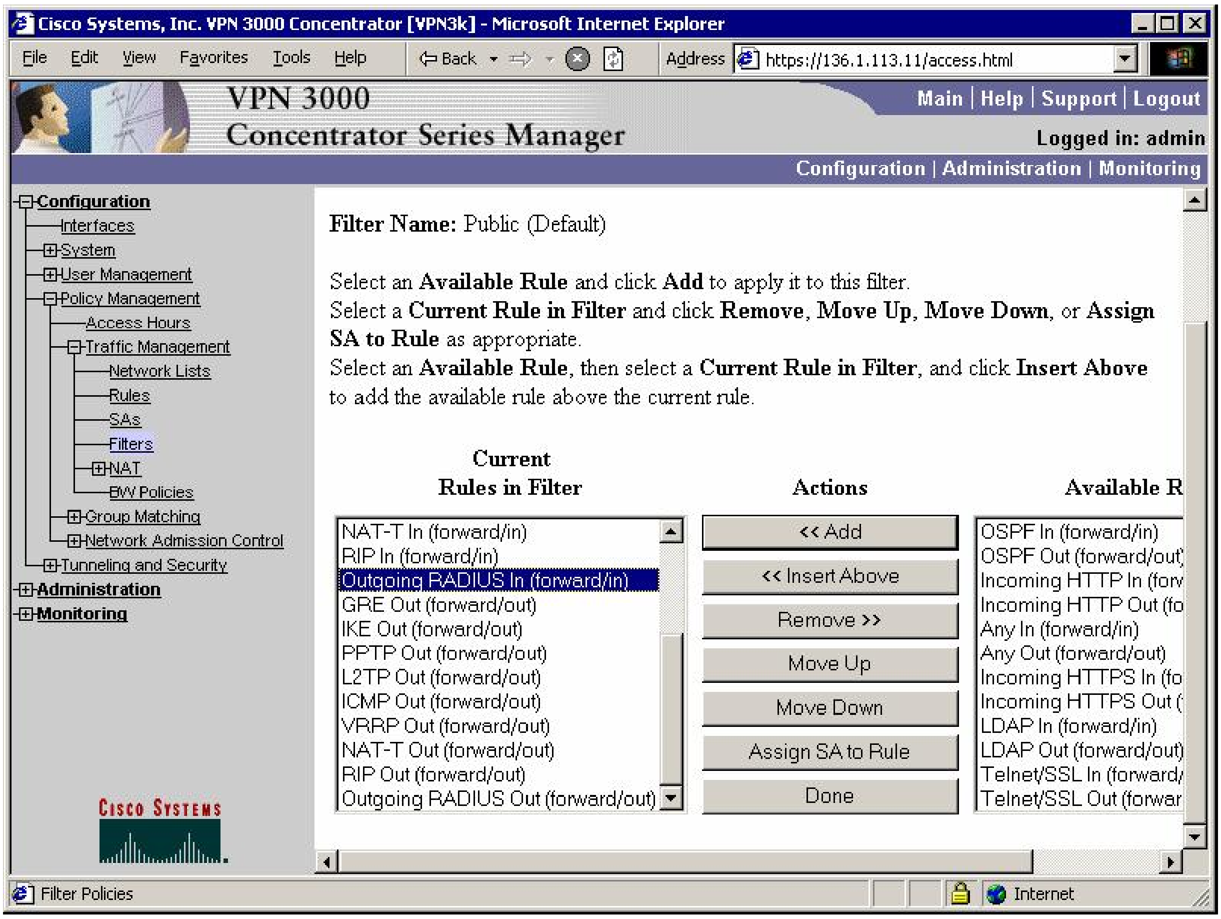
Save Needed

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.

Current Rules in Filter	Actions	Available Rules
GRE In (forward/in)	<< Add	OSPF In (forward/in)
IPSEC-ESP In (forward/in)		OSPF Out (forward/out)
IKE In (forward/in)	<< Insert Above	Incoming HTTP In (forward/in)
PPTP In (forward/in)		Incoming HTTP Out (forward/out
L2TP In (forward/in)	Remove >>	Any In (forward/in)
ICMP In (forward/in)		Any Out (forward/out)
VRRP In (forward/in)	Move Up	Incoming HTTPS In (forward/in)
NAT-T In (forward/in)	Move Down	Incoming HTTPS Out (forward/o



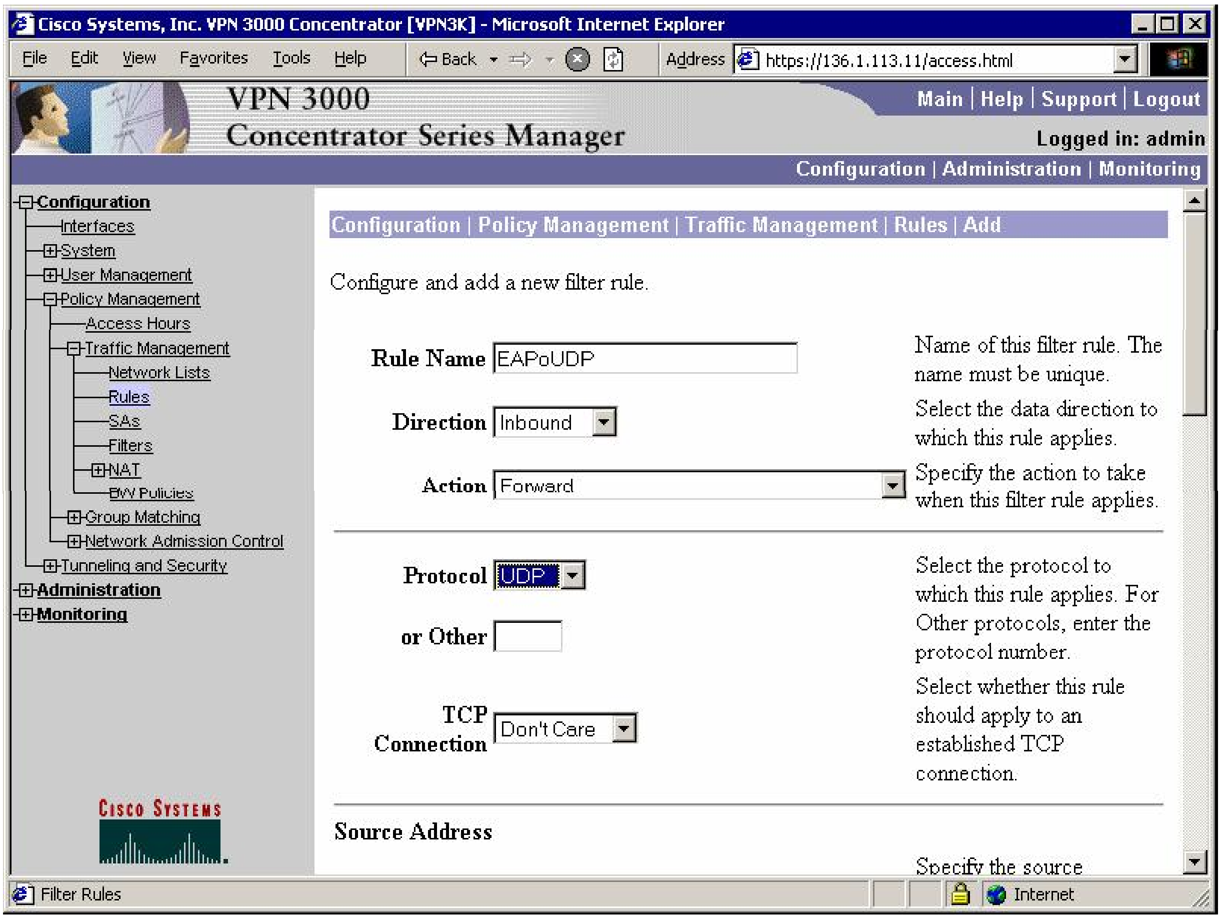
Cisco Systems, Inc. VPN 3000 Concentrator [VPN3k] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Policies
Internet

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.

Current Rules in Filter	Actions	Available R
NAT-T In (forward/in)	<< Add	OSPF In (forward/in)
RIP In (forward/in)	<< Insert Above	OSPF Out (forward/out)
Outgoing RADIUS In (forward/in)	Remove >>	Incoming HTTP In (forw
GRE Out (forward/out)	Move Up	Incoming HTTP Out (fo
IKE Out (forward/out)	Move Down	Any In (forward/in)
PPTP Out (forward/out)	Assign SA to Rule	Any Out (forward/out)
L2TP Out (forward/out)	Done	Incoming HTTPS In (fo
ICMP Out (forward/out)		Incoming HTTPS Out (
VRRP Out (forward/out)		LDAP In (forward/in)
NAT-T Out (forward/out)		LDAP Out (forward/out)
RIP Out (forward/out)		Telnet/SSL In (forward/
Outgoing RADIUS Out (forward/out)		Telnet/SSL Out (forwar

Create rule to permit EAPoUDP traffic:



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Rules
Internet

Configuration | Policy Management | Traffic Management | Rules | Add

Configure and add a new filter rule.

Rule Name EAPoUDP — 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.

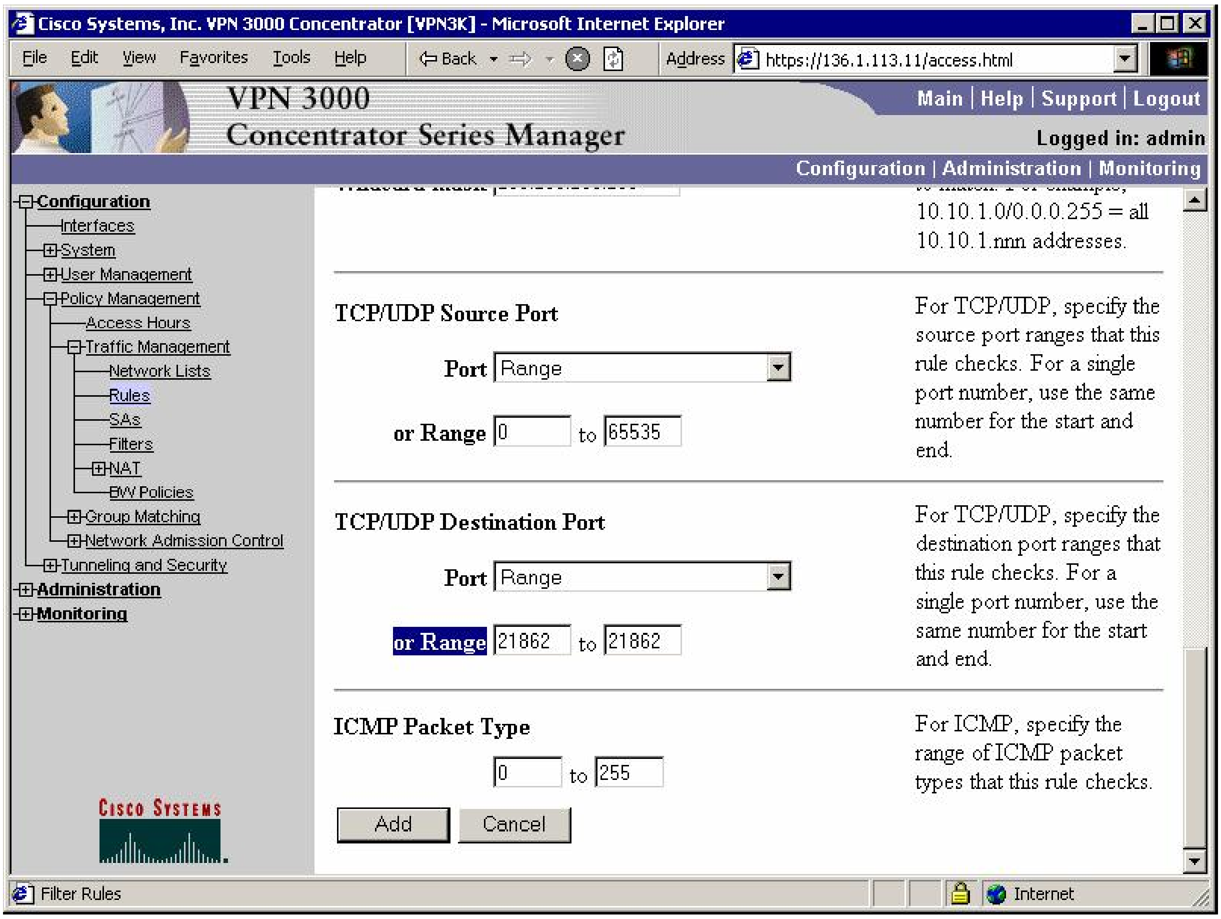
Protocol UDP — Select the protocol to which this rule applies. For Other protocols, enter the protocol number.

or Other

TCP Connection Don't Care — Select whether this rule should apply to an established TCP connection.

Source Address

Specify the source



Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Add
Cancel
Filter Rules
Internet

10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.

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.

TCP/UDP Destination Port

Port: Range

or Range: 21862 to 21862

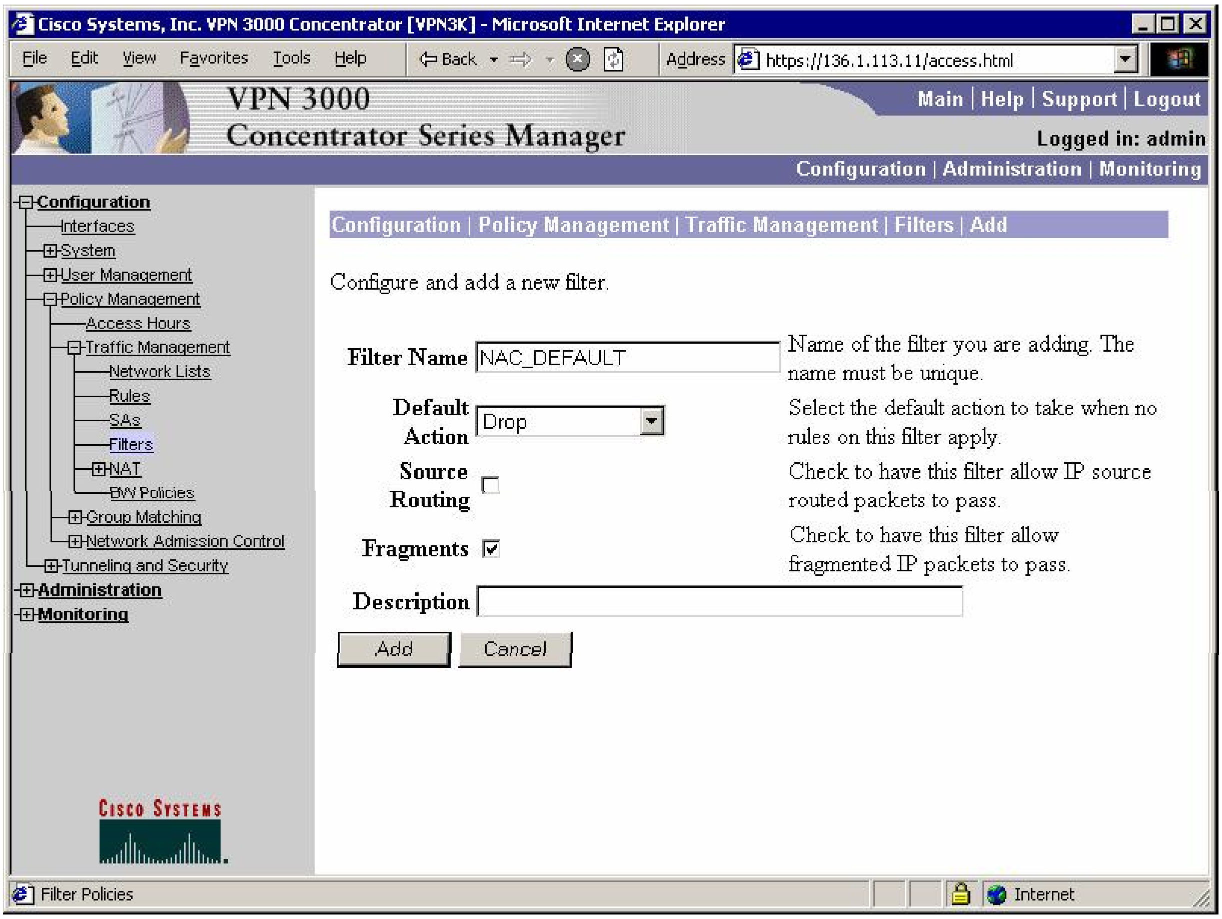
For TCP/UDP, specify the destination port ranges that this rule checks. For a single port number, use the same number for the start and end.

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:

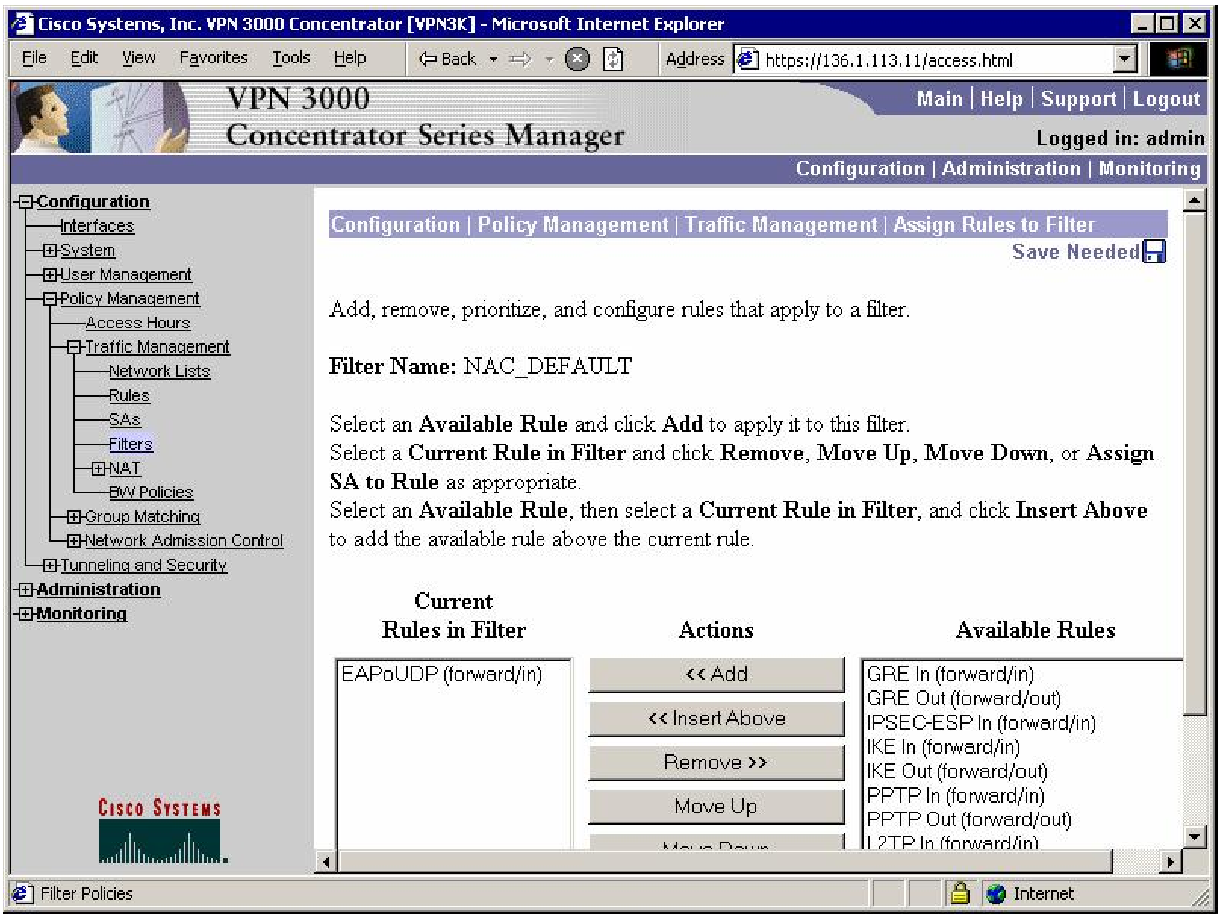

Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
BW Policies
Group Matching
Network Admission Control
Tunneling and Security
Administration
Monitoring
Cisco Systems
Filter Policies
Internet

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name	NAC_DEFAULT	Name of the filter you are adding. The name must be unique.
Default Action	Drop	Select the default action to take when no rules on this filter apply.
Source Routing	☐	Check to have this filter allow IP source routed packets to pass.
Fragments	☑	Check to have this filter allow fragmented IP packets to pass.
Description		

Add Cancel



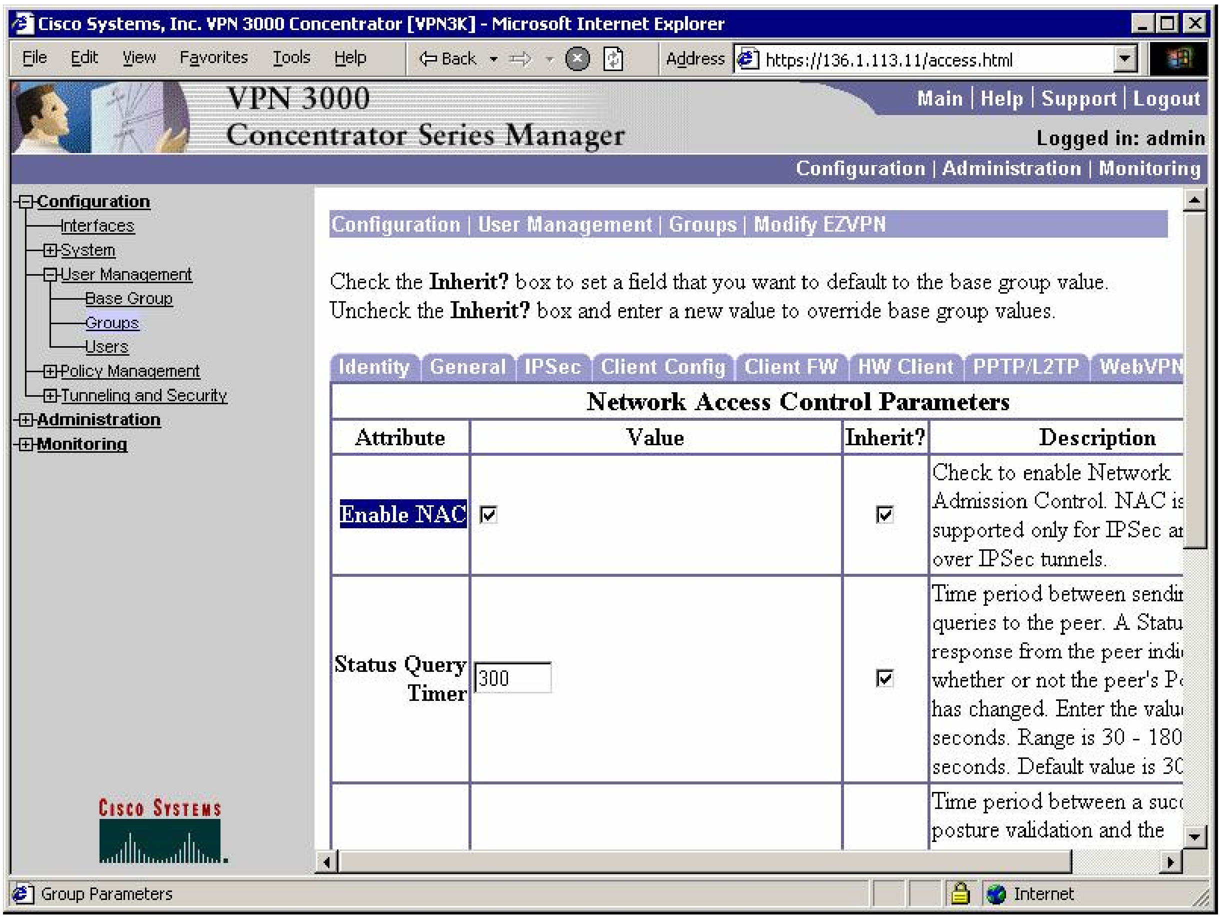
Configuration | Policy Management | Traffic Management | Assign Rules to Filter

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.

Current Rules in Filter	Actions	Available Rules
EAPoUDP (forward/in)	<< Add	GRE In (forward/in)
	<< Insert Above	GRE Out (forward/out)
	Remove >>	IPSEC-ESP In (forward/in)
	Move Up	IKE In (forward/in)
	Move Down	IKE Out (forward/out)
		PPTP In (forward/in)
		PPTP Out (forward/out)
		L2TP In (forward/in)



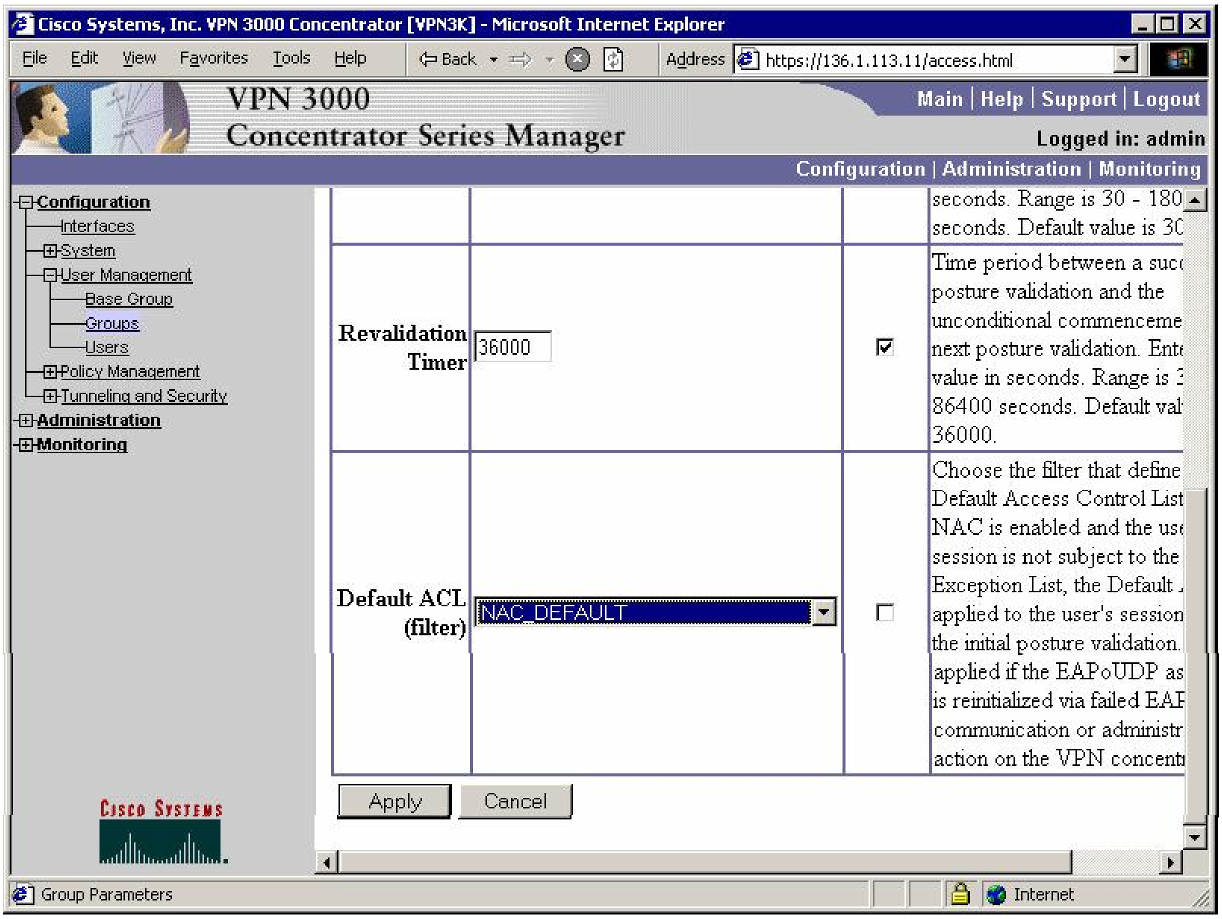
Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | User Management | Groups | Modify EZVPN
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN
Group Parameters
Internet

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Network Access Control Parameters

Attribute	Value	Inherit?	Description
Enable NAC	☑	☑	Check to enable Network Admission Control. NAC is supported only for IPSec ar over IPSec tunnels.
Status Query Timer	300	☑	Time period between sendir queries to the peer. A Statu response from the peer indi whether or not the peer's P has changed. Enter the valu seconds. Range is 30 - 180 seconds. Default value is 30
			Time period between a succ posture validation and the

Configure NAC settings for group EZVPN:


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Cisco Systems
Group Parameters
Internet

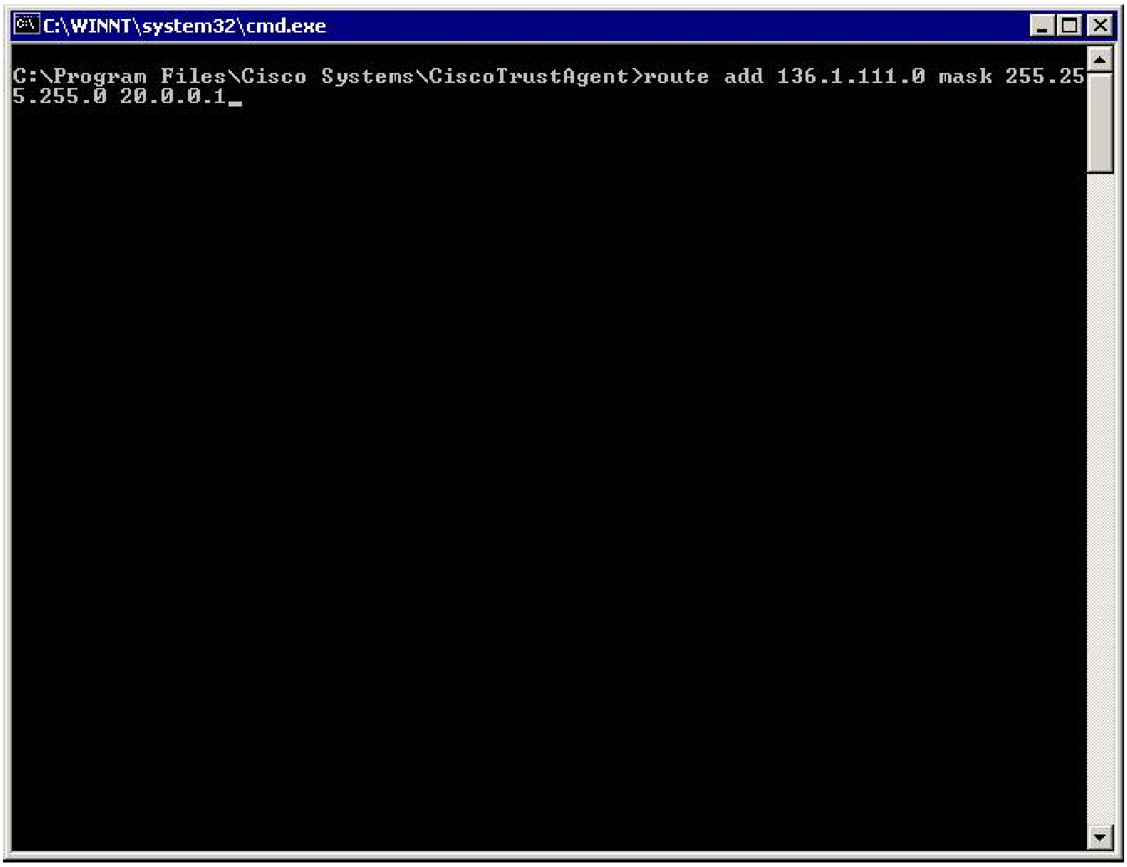
			seconds. Range is 30 - 180 seconds. Default value is 30
Revalidation Timer	36000	☑	Time period between a succ posture validation and the unconditional commenceme next posture validation. Ente value in seconds. Range is 3 86400 seconds. Default val 36000.
Default ACL (filter)	NAC_DEFAULT	☐	Choose the filter that define Default Access Control List NAC is enabled and the use session is not subject to the Exception List, the Default applied to the user's session the initial posture validation. applied if the EAPoUDP as is reinitialized via failed EAP communication or administr action on the VPN concentr

Apply Cancel

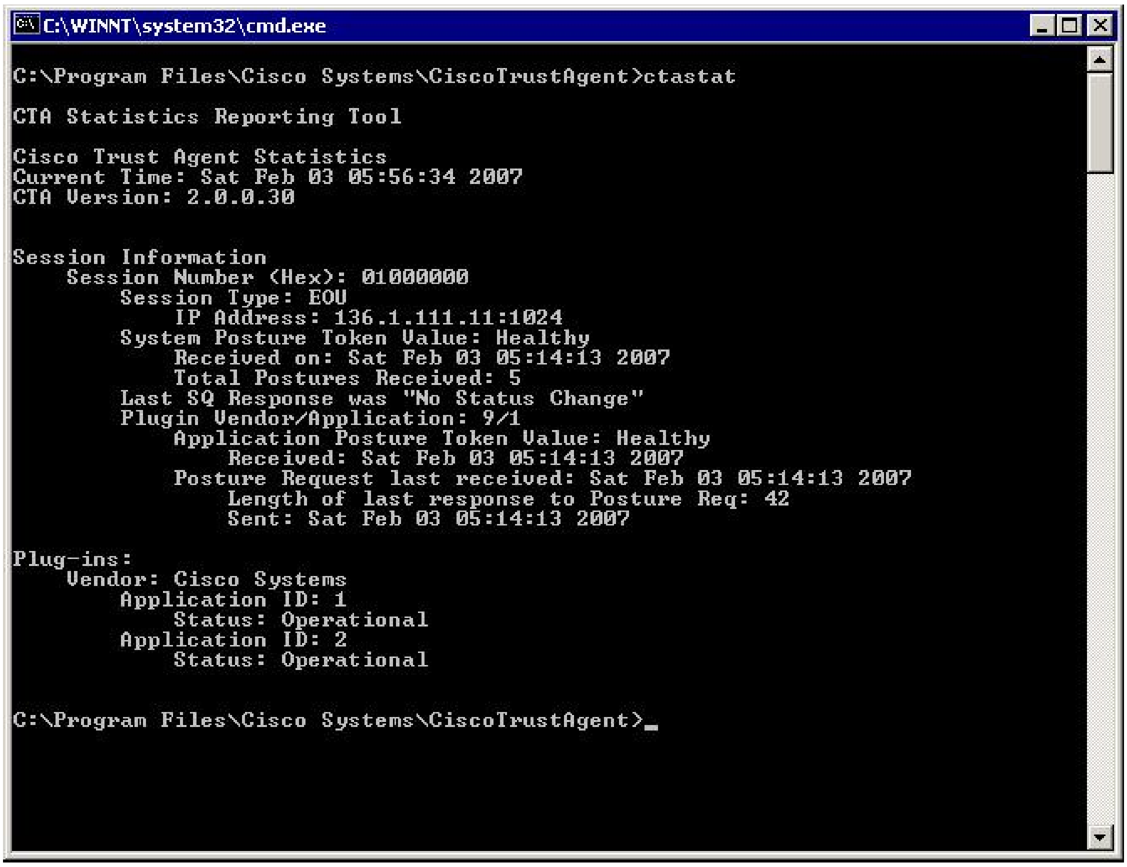
Verification

Test PC:

Connect Cisco VPN Client, and add static route:



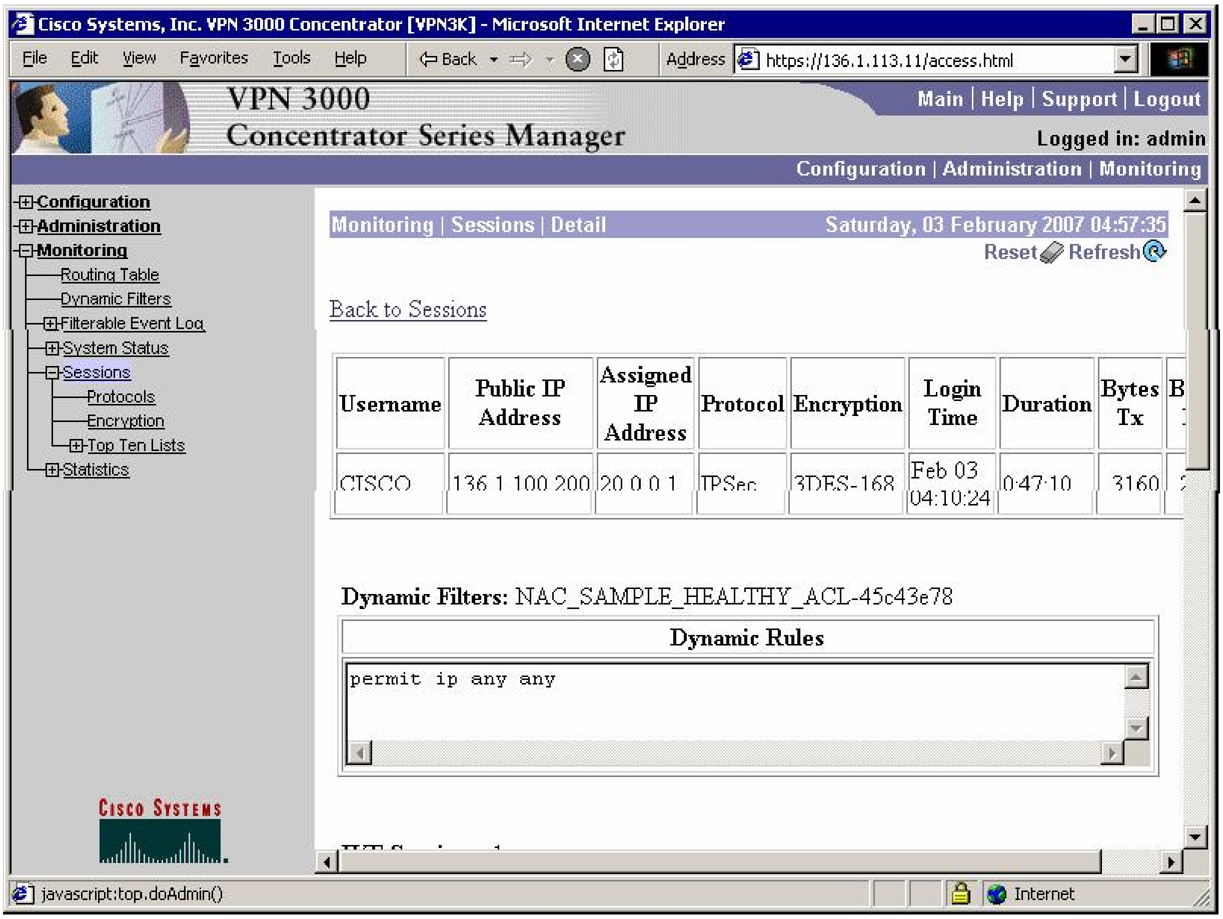
```
C:\Program Files\Cisco Systems\CiscoTrustAgent>route add 136.1.111.0 mask 255.25
5.255.0 20.0.0.1_
```



```
C:\Program Files\Cisco Systems\CiscoTrustAgent>ctastat

CTA Statistics Reporting Tool

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


Session Information
    Session Number (Hex): 01000000
        Session Type: EOU
            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 05:14:13 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:



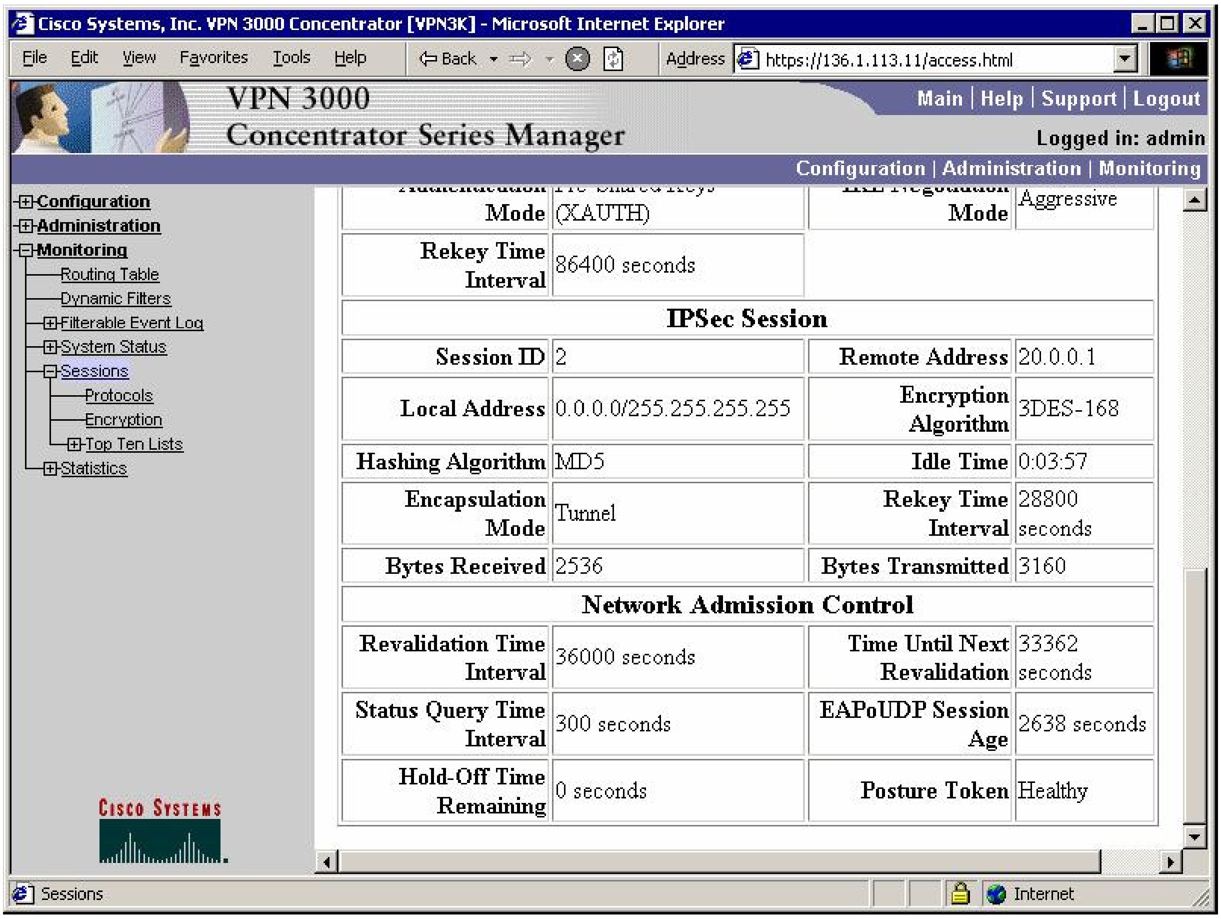
Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Dynamic Filters
Filterable Event Log
System Status
Sessions
Protocols
Encryption
Top Ten Lists
Statistics
Cisco Systems
Monitoring | Sessions | Detail
Saturday, 03 February 2007 04:57:35
Reset
Refresh
Back to Sessions
javascript:top.doAdmin()
Internet

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	B
CISCO	136.1.100.200	20.0.0.1	IPSec	3DES-168	Feb 03 04:10:24	0:47:10	3160	2

Dynamic Filters: NAC_SAMPLE_HEALTHY_ACL-45c43e78

Dynamic Rules

```
permit ip any any
```


Cisco Systems, Inc. VPN 3000 Concentrator [VPN3K] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://136.1.113.11/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Monitoring
Routing Table
Dynamic Filters
Filterable Event Log
System Status
Sessions
Protocols
Encryption
Top Ten Lists
Statistics
Cisco Systems
Sessions
Internet

Mode	(XAUTH)	Mode	Aggressive
Rekey Time Interval	86400 seconds		

IPSec Session

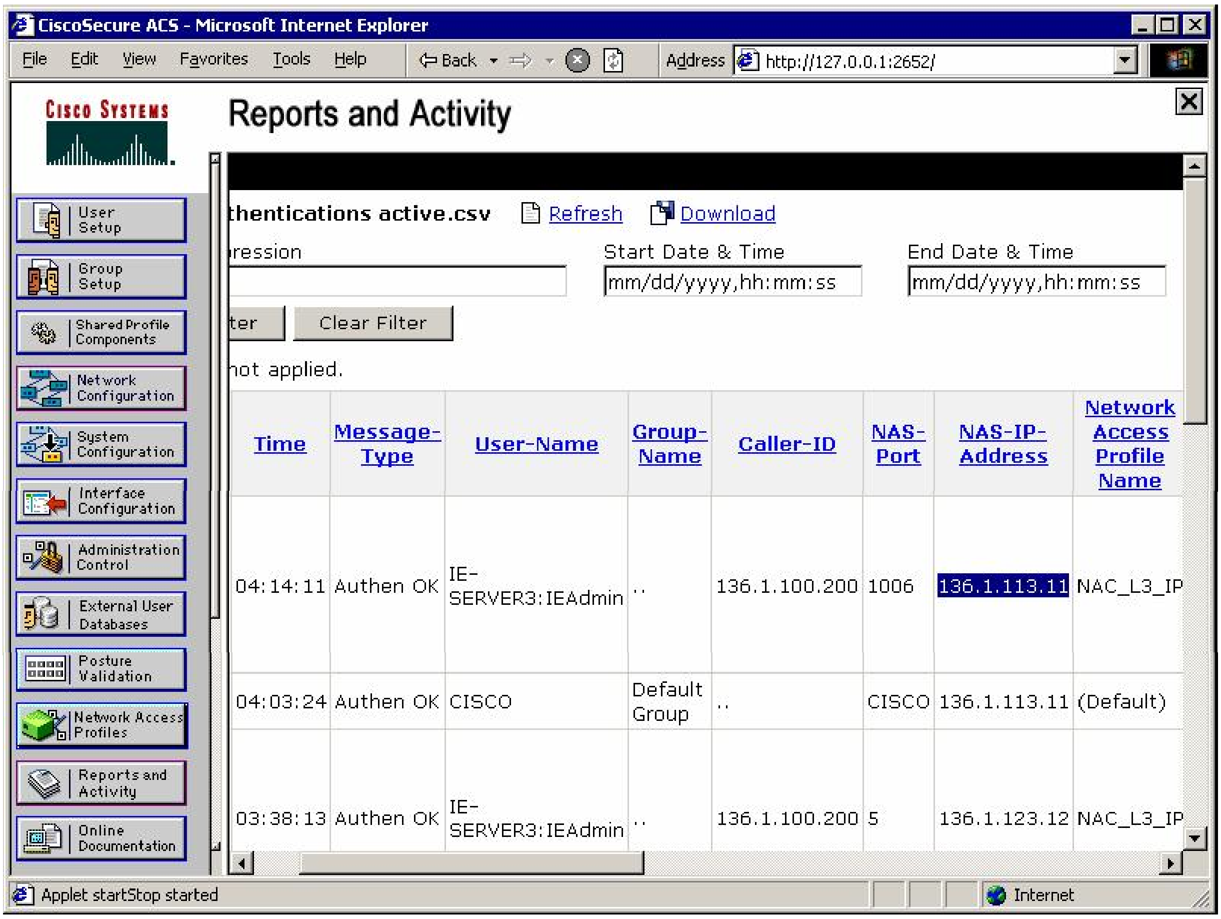
Session ID	2	Remote Address	20.0.0.1
Local Address	0.0.0.0/255.255.255.255	Encryption Algorithm	3DES-168
Hashing Algorithm	MD5	Idle Time	0:03:57
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Bytes Received	2536	Bytes Transmitted	3160

Network Admission Control

Revalidation Time Interval	36000 seconds	Time Until Next Revalidation	33362 seconds
Status Query Time Interval	300 seconds	EAPoUDP Session Age	2638 seconds
Hold-Off Time Remaining	0 seconds	Posture Token	Healthy

ACS:

Reports & Activity: Passed Authentications

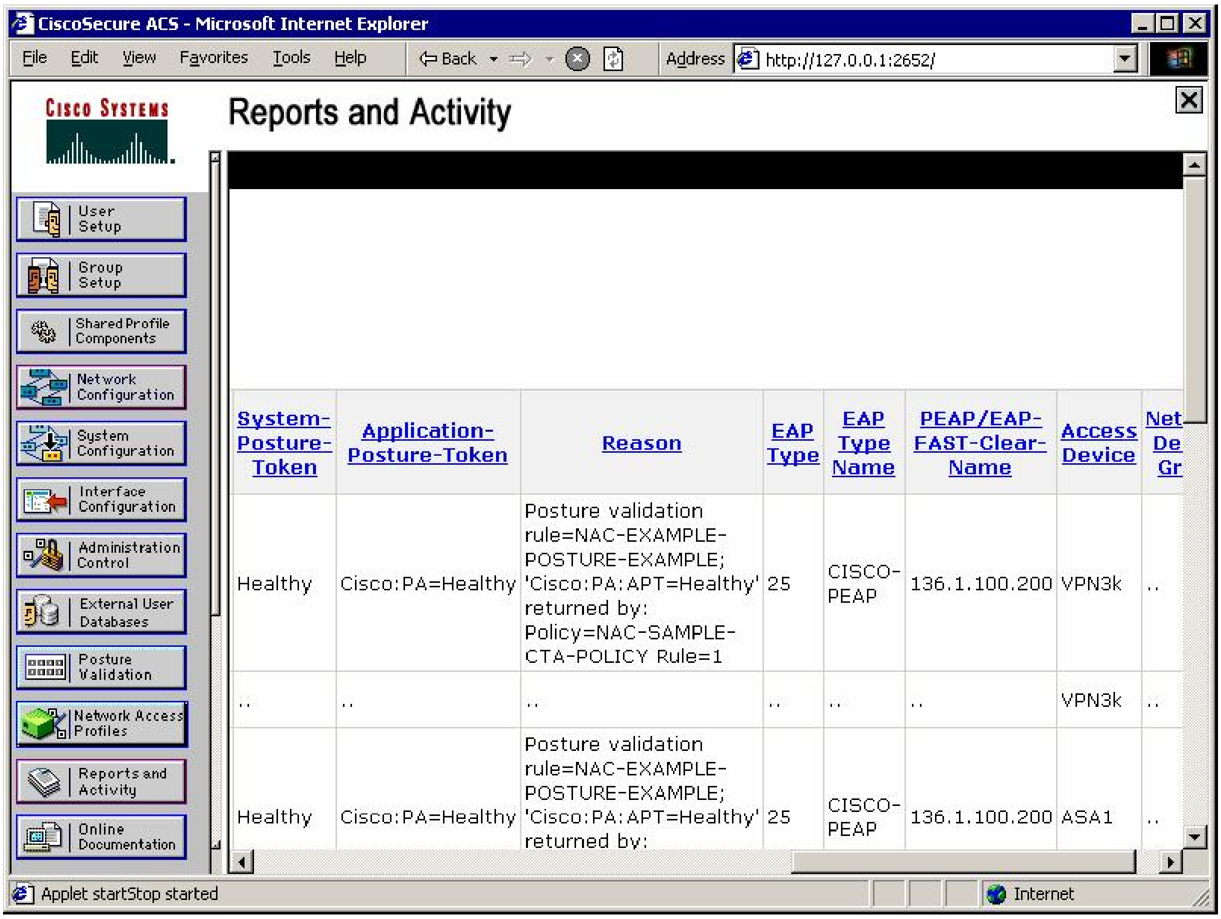


thentications active.csv

ression | Start Date & Time: mm/dd/yyyy,hh:mm:ss | End Date & Time: mm/dd/yyyy,hh:mm:ss

not applied.

Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name
04:14:11	Authen OK	IE-SERVER3:IEAdmin	..	136.1.100.200	1006	136.1.113.11	NAC_L3_IP
04:03:24	Authen OK	CISCO	Default Group	..	CISCO	136.1.113.11	(Default)
03:38:13	Authen OK	IE-SERVER3:IEAdmin	..	136.1.100.200	5	136.1.123.12	NAC_L3_IP



Reports and Activity

System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name	PEAP/EAP-FAST-Clear-Name	Access Device	Net De Gr
Healthy	Cisco:PA=Healthy	Posture validation rule=NAC-EXAMPLE-POSTURE-EXAMPLE; 'Cisco:PA:APT=Healthy' returned by: Policy=NAC-SAMPLE-CTA-POLICY Rule=1	25	CISCO-PEAP	136.1.100.200	VPN3k	..
..	..	..	..	..	..	VPN3k	..
Healthy	Cisco:PA=Healthy	Posture validation rule=NAC-EXAMPLE-POSTURE-EXAMPLE; 'Cisco:PA:APT=Healthy' returned by:	25	CISCO-PEAP	136.1.100.200	ASA1	..

Further Reading

VPN 3000 Network Access Device 4.7.1 NAC Administration and Configuration