White Paper

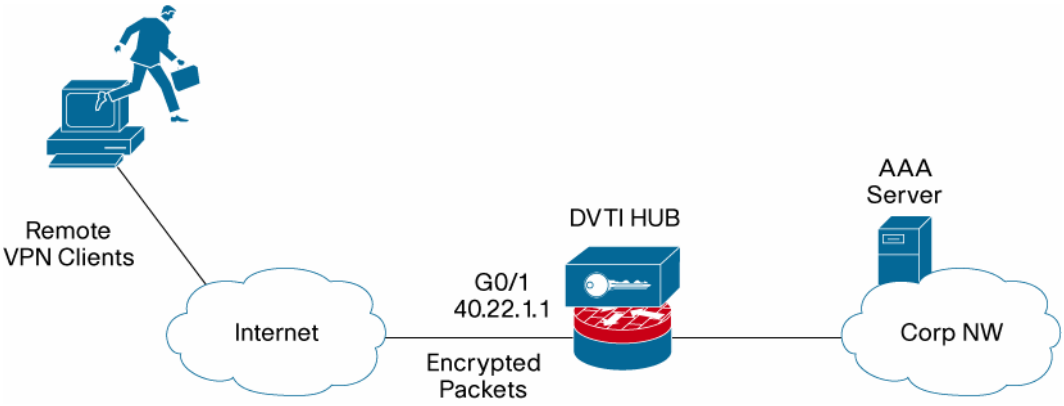
Configuring NAC with IPSec Dynamic Virtual Tunnel Interface

This document describes how Network Admission Control (NAC) works with IP Security (IPsec) Dynamic Virtual Tunnel Interface (DVTI).

TOPOLOGY

The network topology is shown in Figure 1. The Windows client is running Cisco® VPN Client 4.0, while the Cisco 7200 hub router is running Cisco IOS® Software Release 12.4.4T using DVTI to terminate the IPsec connections. NAC is applied on the virtual template, and Cisco Secure Access Control Server (ACS) 3.3 is used as the authentication, authorization, and accounting (AAA) server for IPsec and NAC.

Figure 1. Network Topology



INITIAL SETUP

The PC running Cisco VPN Client 4.0 connects to the DVTI hub, and Internet Key Exchange (IKE) Authorization, Xauth and Mode-Config are completed through exchanges with the AAA server. Once the IPsec security associations (SA) are up, a virtual access interface is cloned from the DVTI virtual template. We have applied access control list (ACL) and NAC statements on the virtual template, which are inherited by the virtual access interface. The hub kicks off eopoudp authentication with the client, and exchanges eop over radius messages with the AAA server. The resulting PEAP session between client and AAA server is used to gather the Clients' posture. The client is running Cisco Trust Agent and sends its posture. The AAA server uses this posture for health assessment of the Client and sends appropriate access accept/reject messages to the hub.

In this sample test scenario, the posture validation is done based on the client OS string. Based on the posture, the RADIUS server sends an ACL (first sends ACL name, then hub gets the actual ACL) to the hub router. The hub router applies the ACL on the virtual access interface, allowing the client to send traffic to the corporate network, if it is healthy

In this scenario, the RADIUS server is Cisco Secure ACS 3.3, and is used for IPsec (IKE authorization, Xauth, and Mode-Cfg) and also for NAC. The minimum IPsec AAA attributes like IP Address, Preshared Keys etc are used. For more information on Easy VPN server

and IPSec Radius attributes, please refer to:
http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455b6a.html

The NAC setup is rudimentary in this test example. The client is not running any antivirus software. Posture validation is based on the client OS string—if it contains “Windows” it is defined as healthy and an ‘ip any any’ ACL is pushed down to be applied to the virtual access interface. For more NAC deployment scenarios, please refer to the NAC documentation at:
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

DVTI AND NAC CONFIGURATION

The DVTI and NAC configuration is shown below:

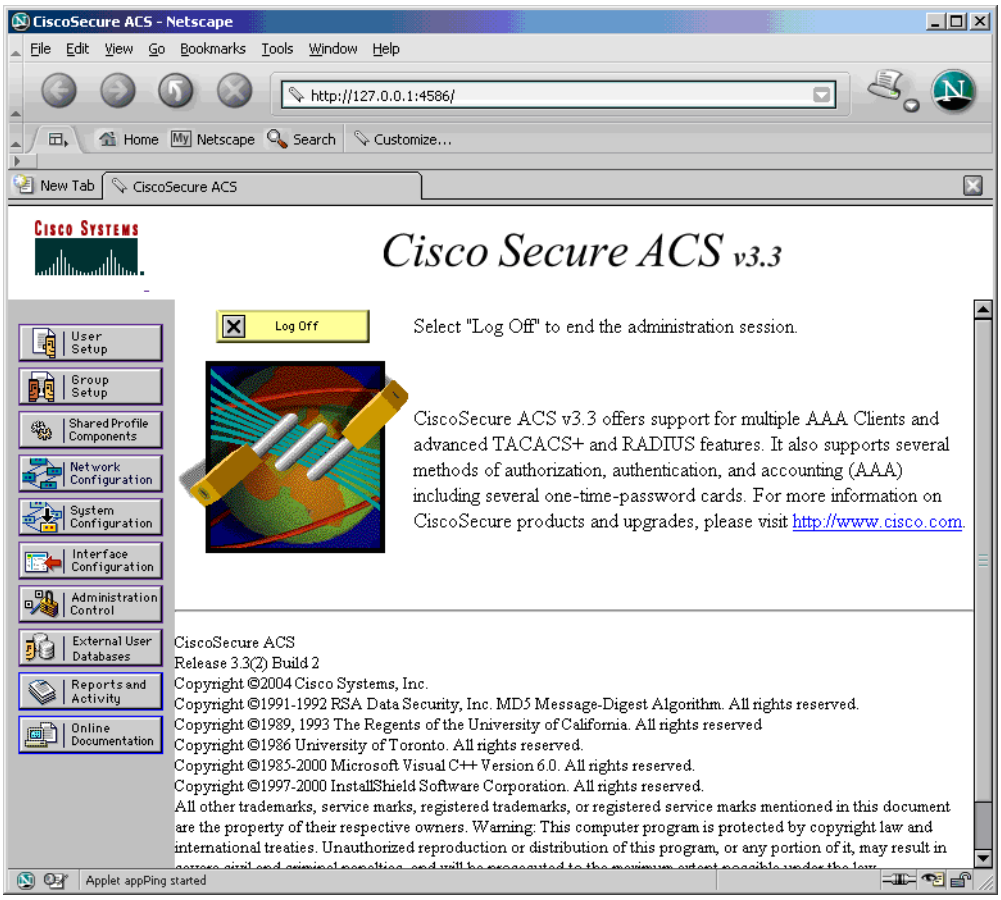
```
crypto isakmp profile nac
   match identity group nac
   client authentication list VPN-AAA
   isakmp authorization list VPN-AAA
   client configuration address respond
   virtual-template 1
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback10
 ip access-group 101 in
 ip admission vti-nac
 load-interval 30
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile nac
!
access-list 101 permit udp any any eq 21862
```


CONFIGURING CISCO SECURE ACS 3.3

Cisco Secure ACS Version

Figure 2 shows the **ACS version information**.

Figure 2. ACS Version

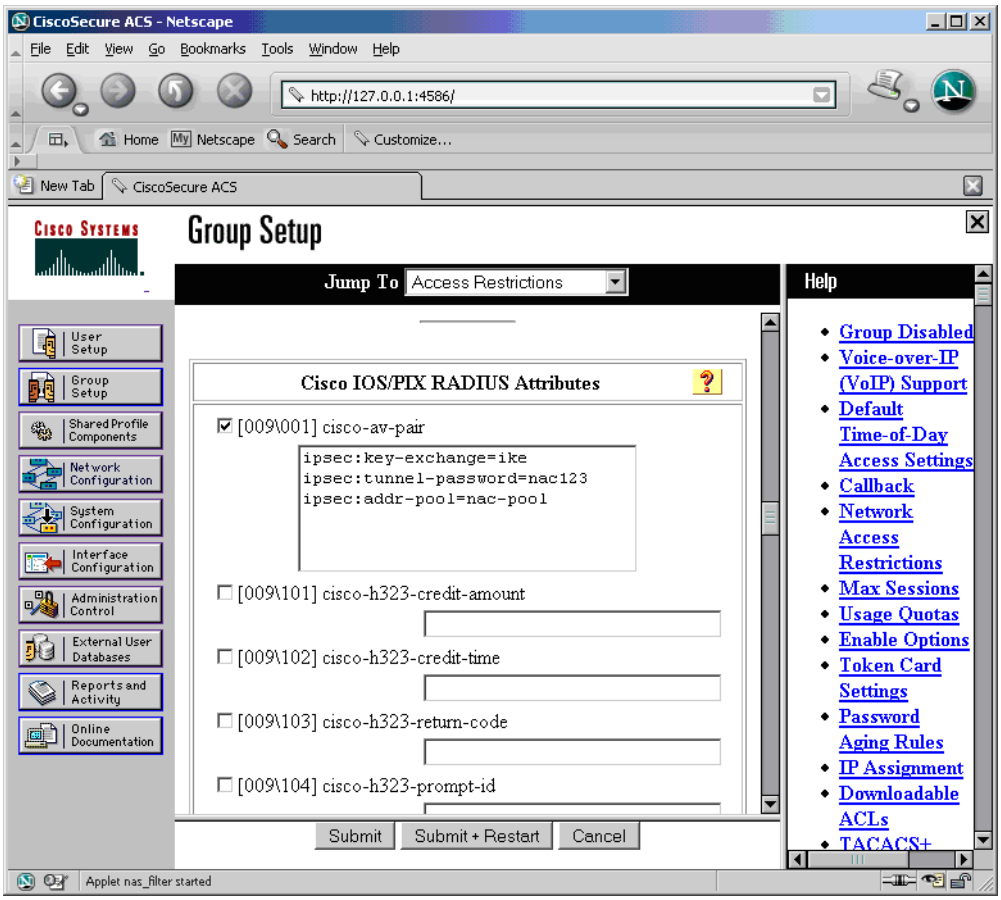


IPsec Group Attributes

```
EzVPN Groupname  = nac
```

Figure 3 shows the **IPSec Group attributes defined on ACS**.

Figure 3. IPSec Group Attributes

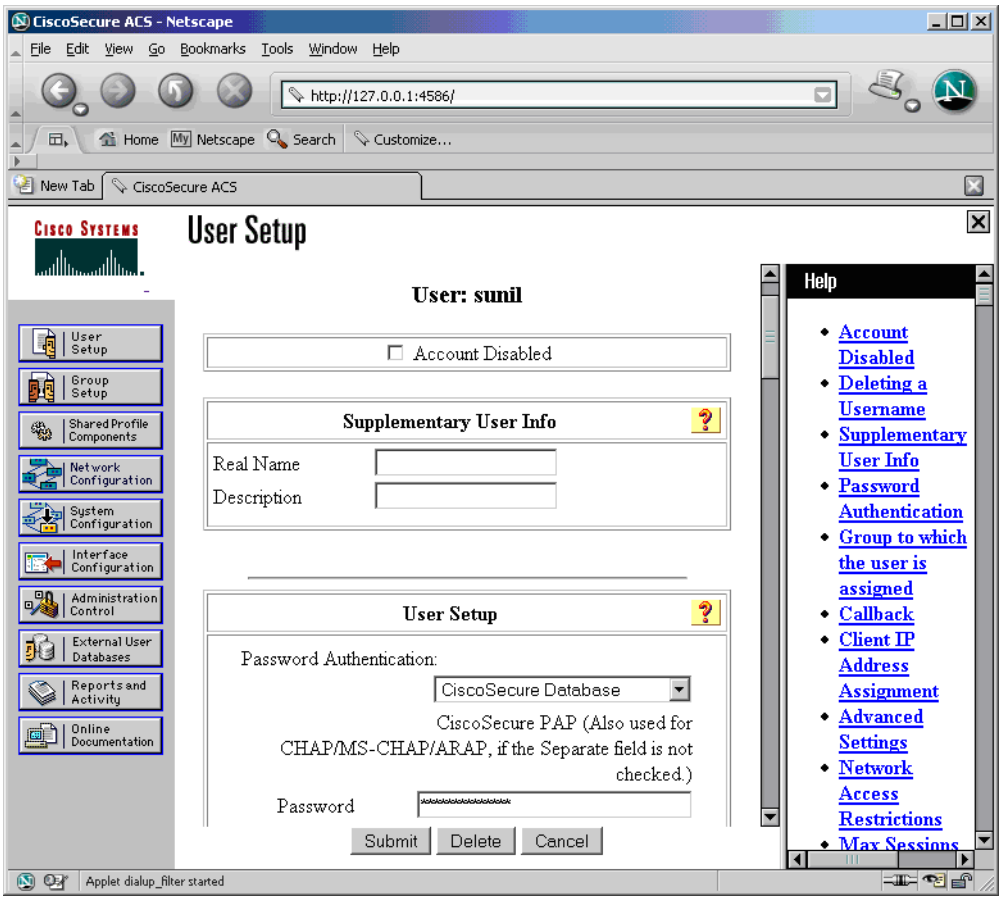


IPsec Xauth Username

```
Username = sunil
```

Figure 4 shows the **username and password defined for the vpn client**.

Figure 4. IPSec Xauth Username



Defining NAC External Database for Posture Validation

We define a Validation Policy that says a posture with an OS string containing “Windows” is declared as “healthy”. Figure 5 shows the **ACS External database definitions**.

Figure 5. ACS External Database

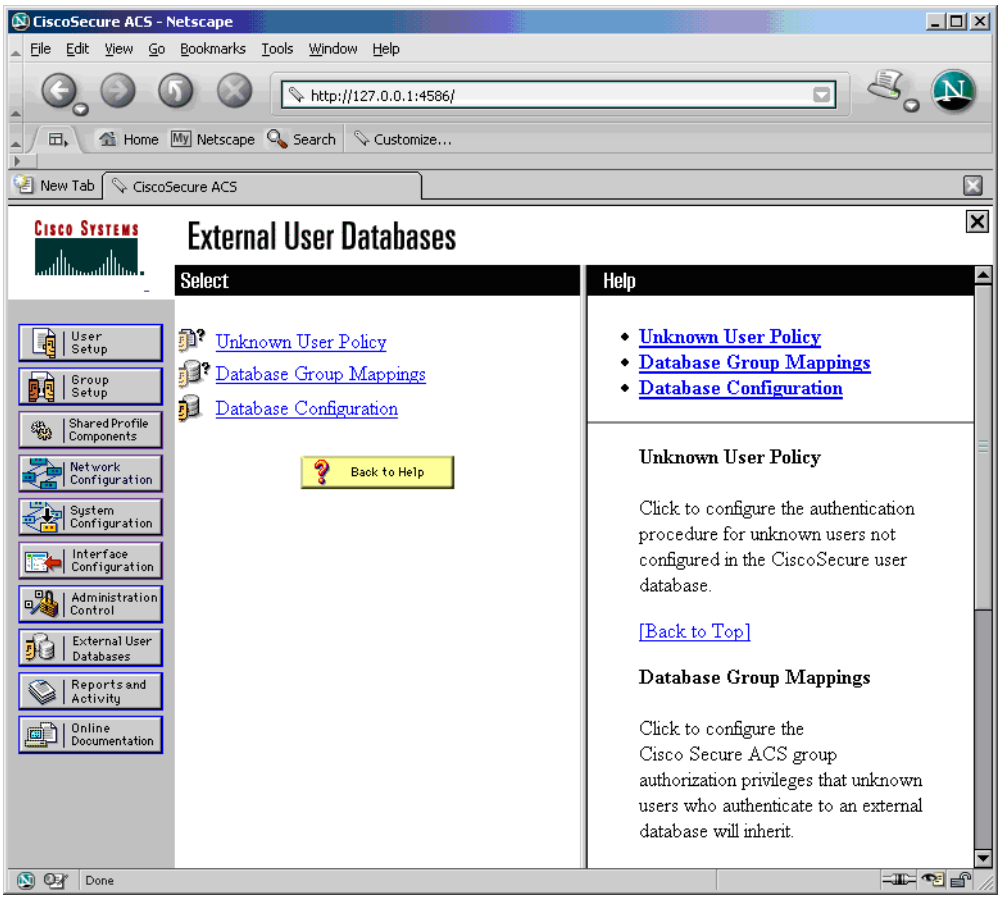


Figure 6 shows the **ACS External Databases**. Pick “Network Admission Control.”

Figure 6. ACS External Database

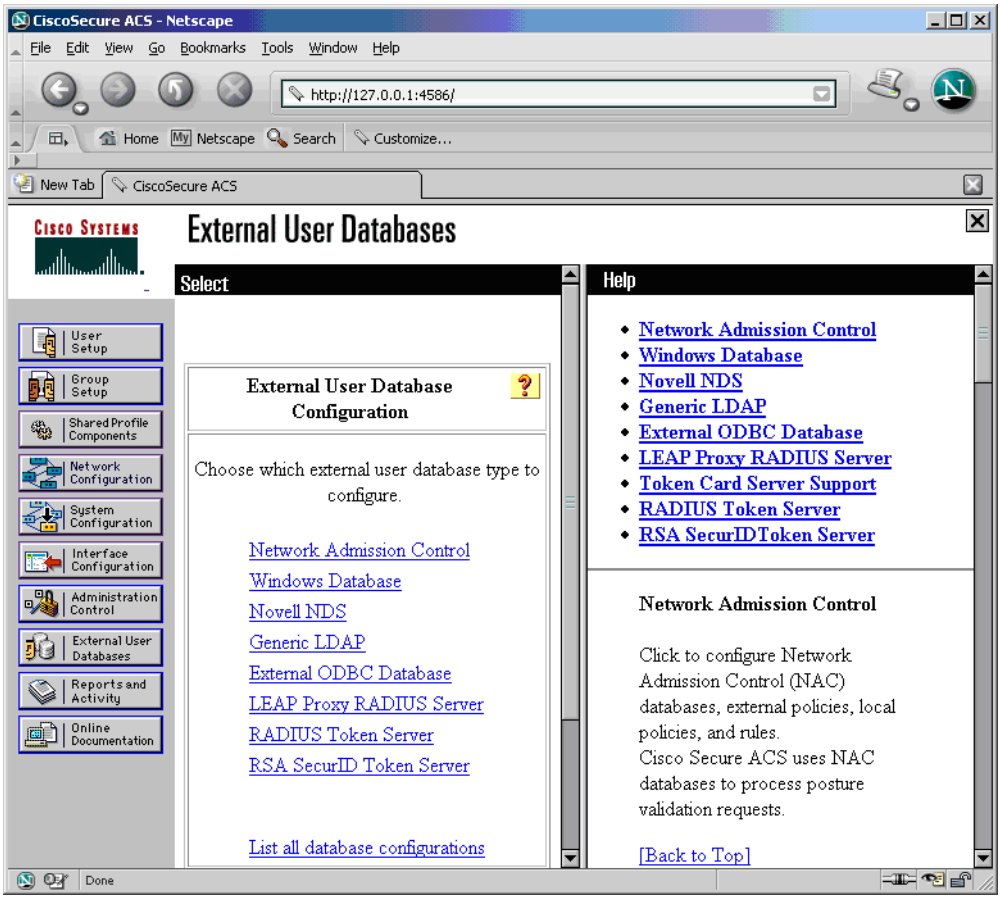


Figure 7 shows **creating a new NAC database**.

Figure 7. ACS NAC Database

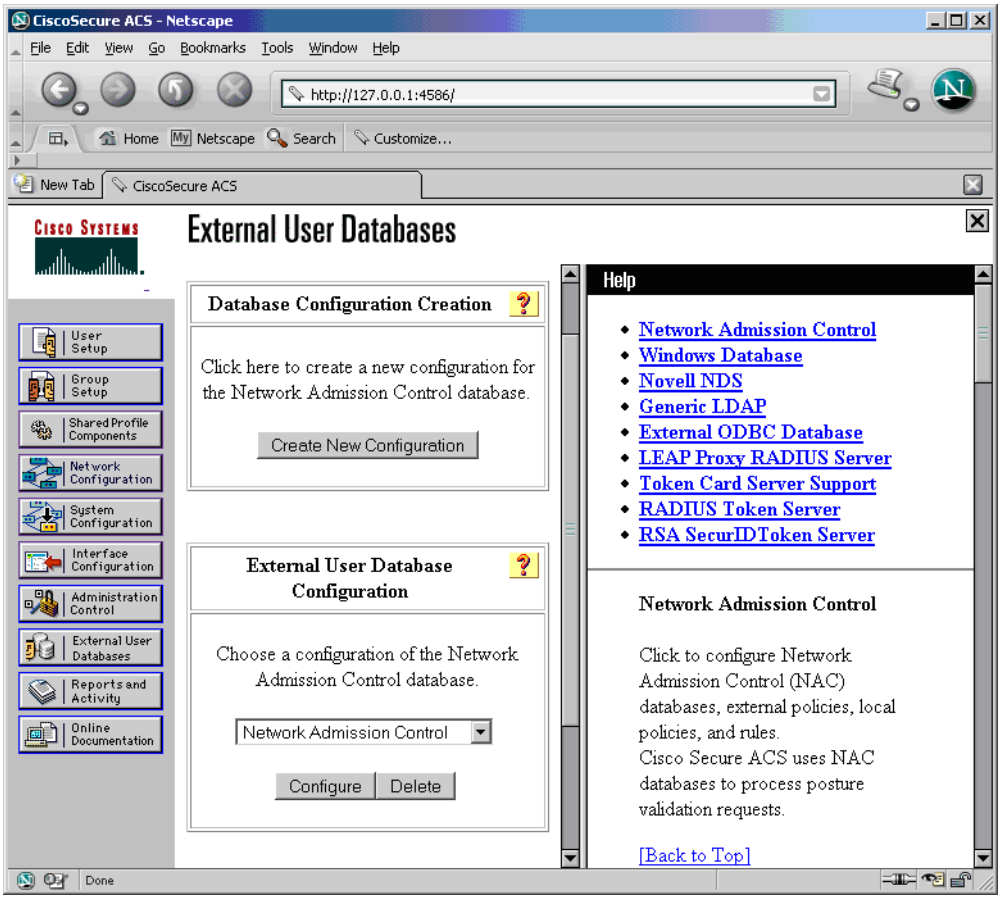


Figure 8 shows **creating the NAC Credential Validation Policies**.

Figure 8. NAC Credential Policy Configuration

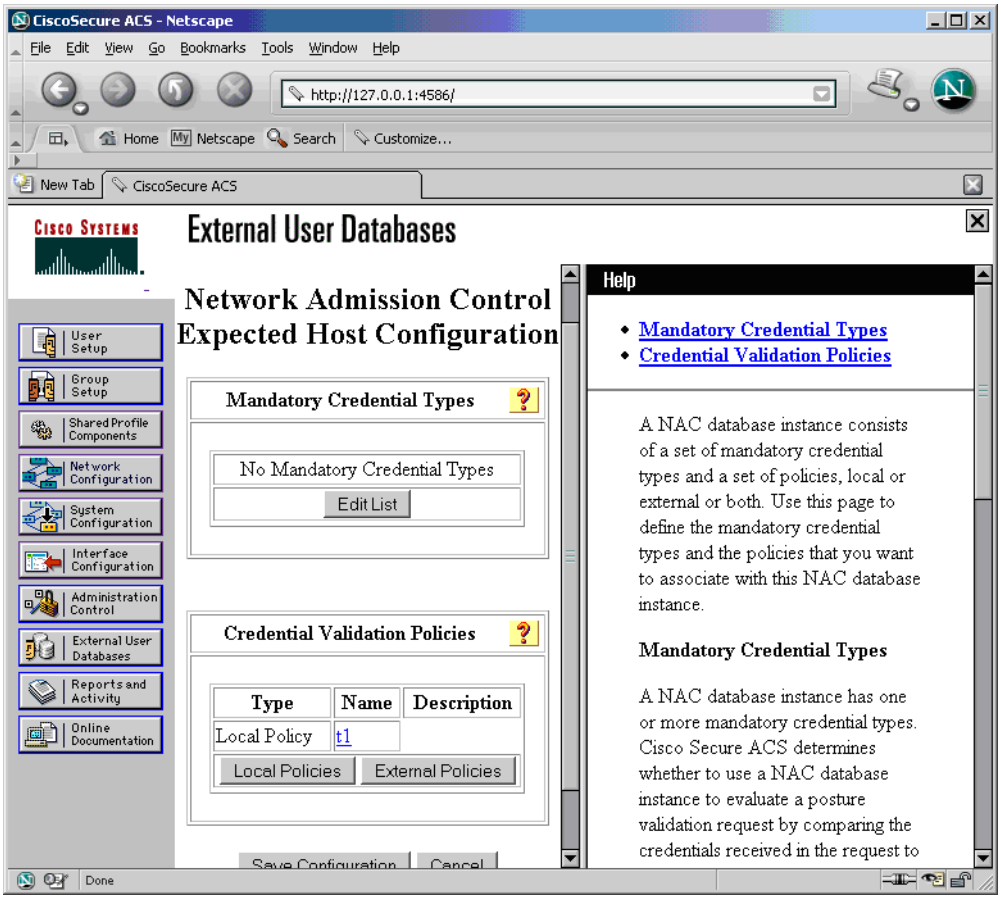
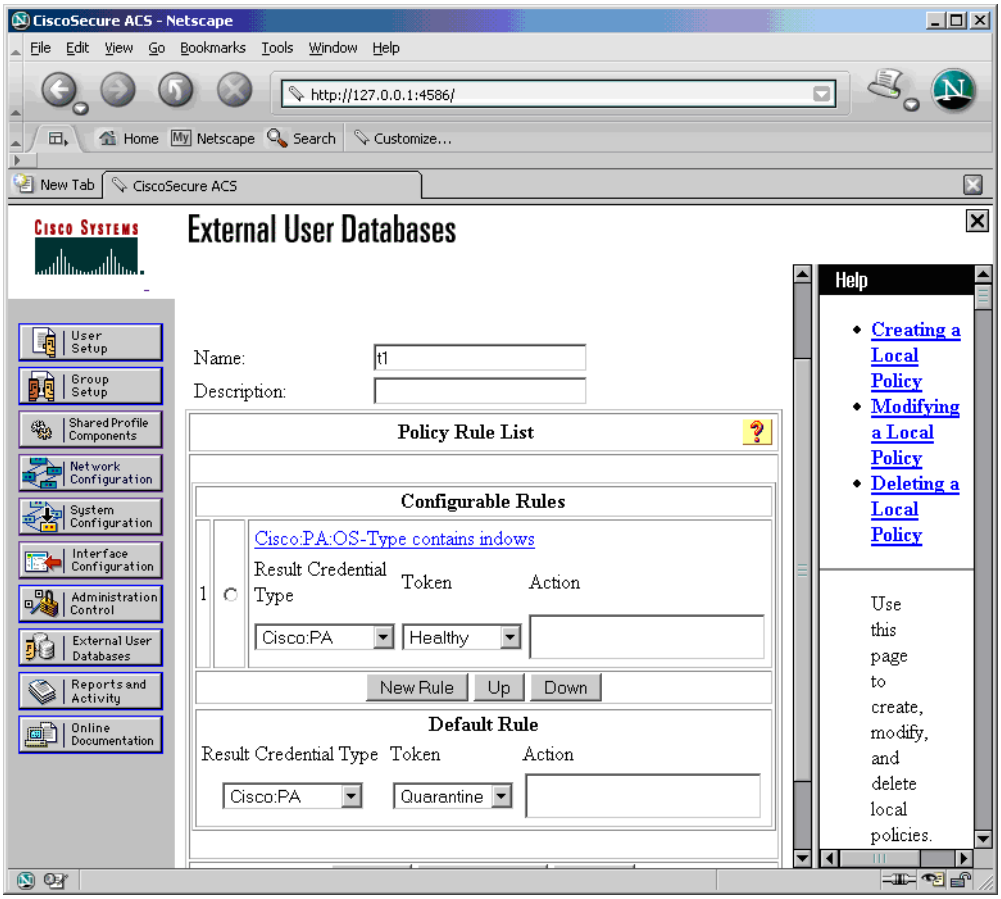


Figure 9 shows **creating a new Policy Rule List for Client posture validation**.

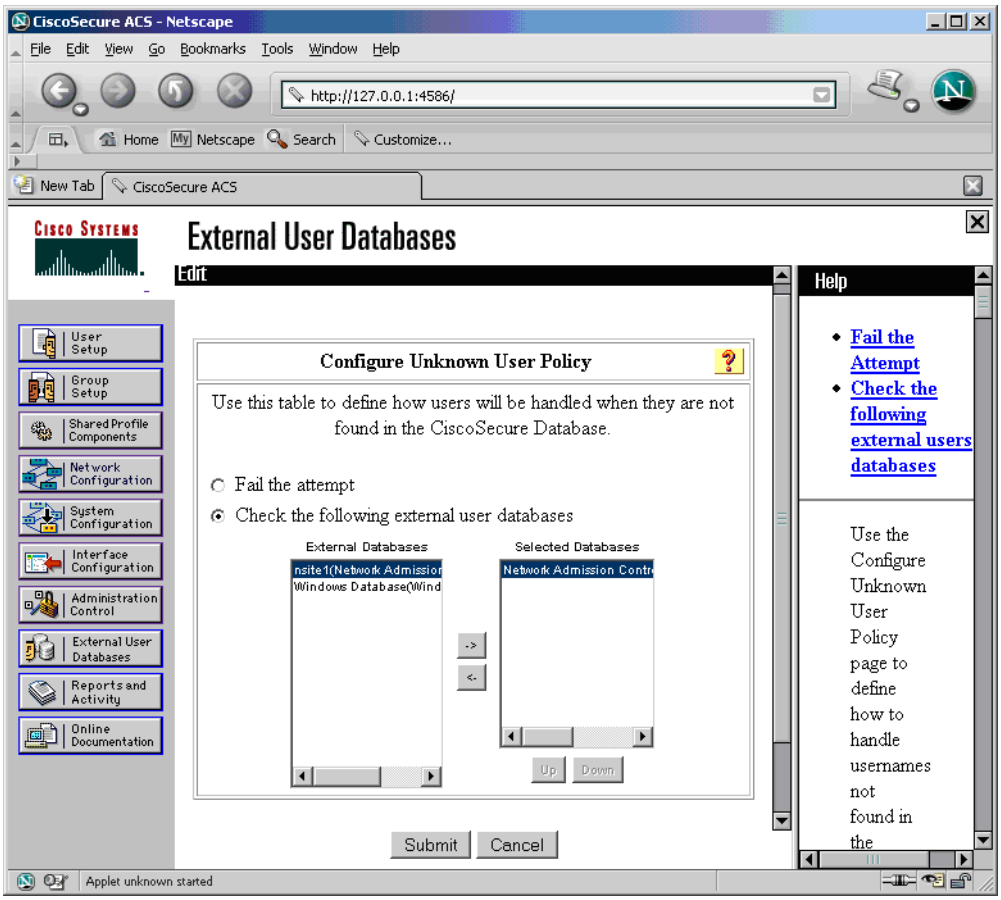
Figure 9. NAC Policy Rules



Defining the Unknown User Policy

Any unknown users are searched in the NAC database (Figure 10).

Figure 10. ACS Unknown User Policies



NAC Database Group Mappings

Maps the previously configure posture token “Windows” in the NAC database to the group “Healthy” (Figure 11).

Figure 11. Unknown User to NAC Database Mappings

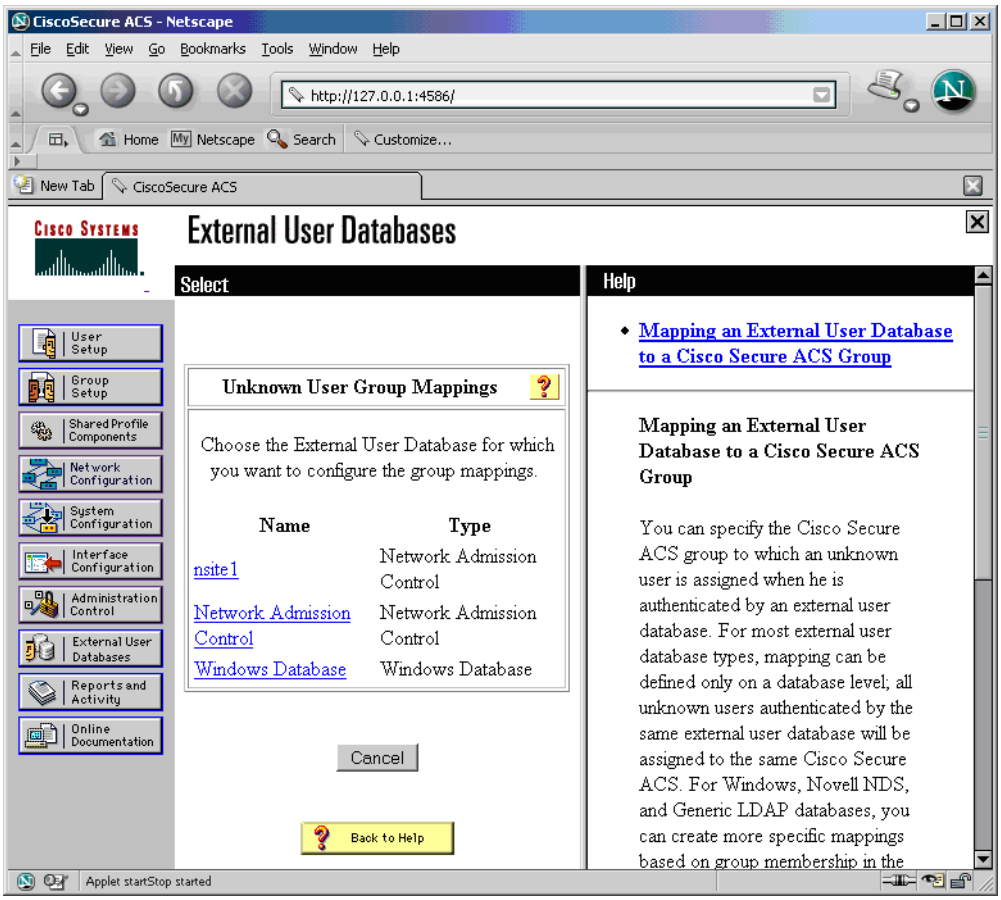
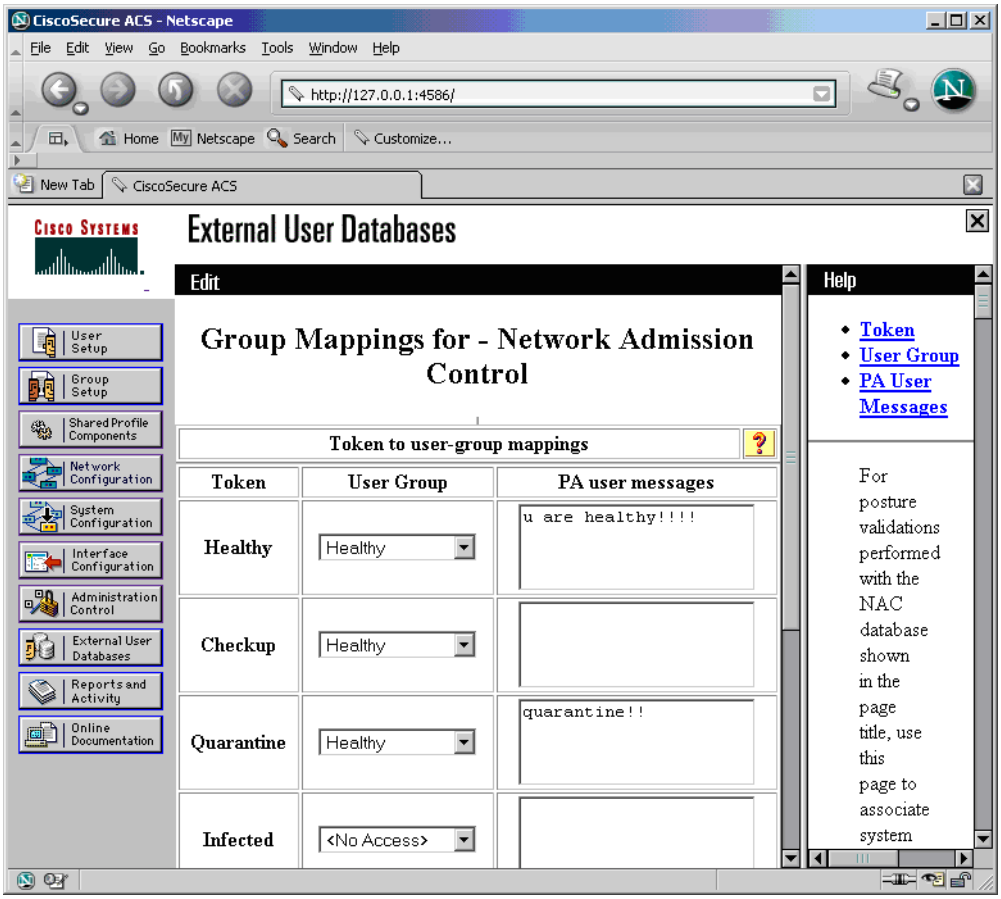


Figure 12 shows the **Group mappings for NAC Database**.

Figure 12. NAC Group Mappings



Defining the User Group “Healthy”

The Healthy group is associated with an ACL to be sent to the hub router (Figure 13).

Figure 13. NAC Group Settings

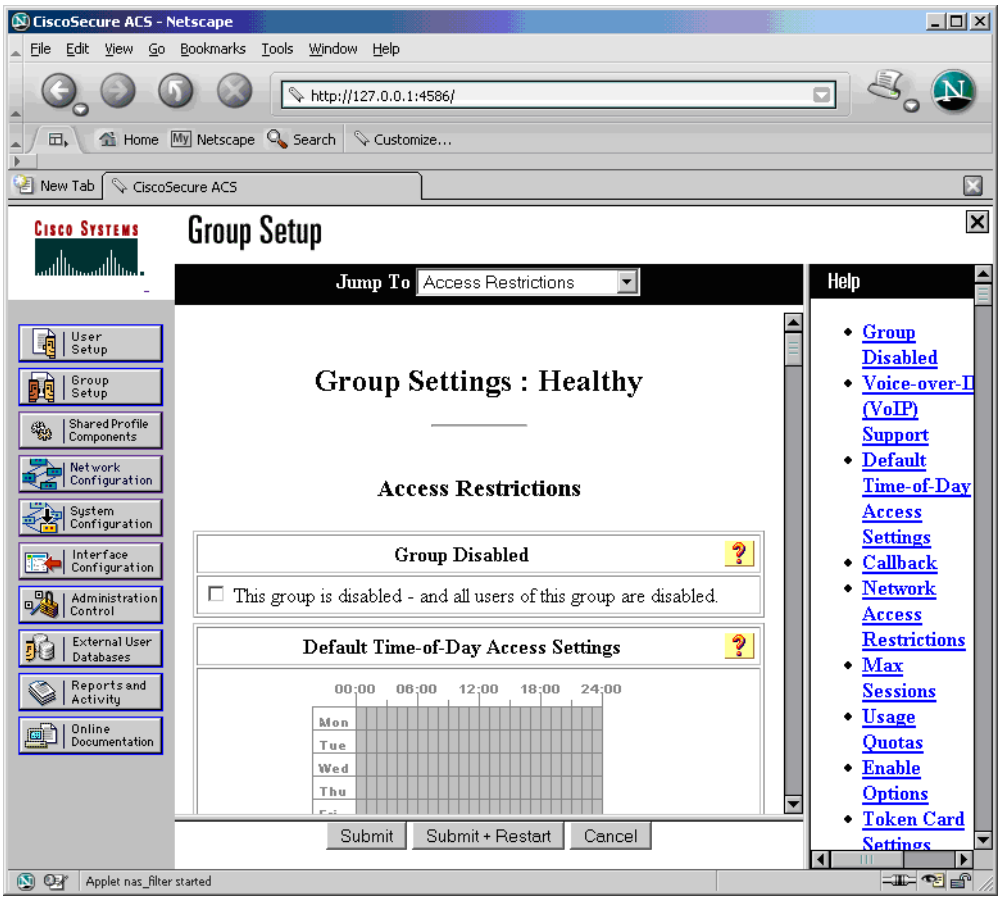
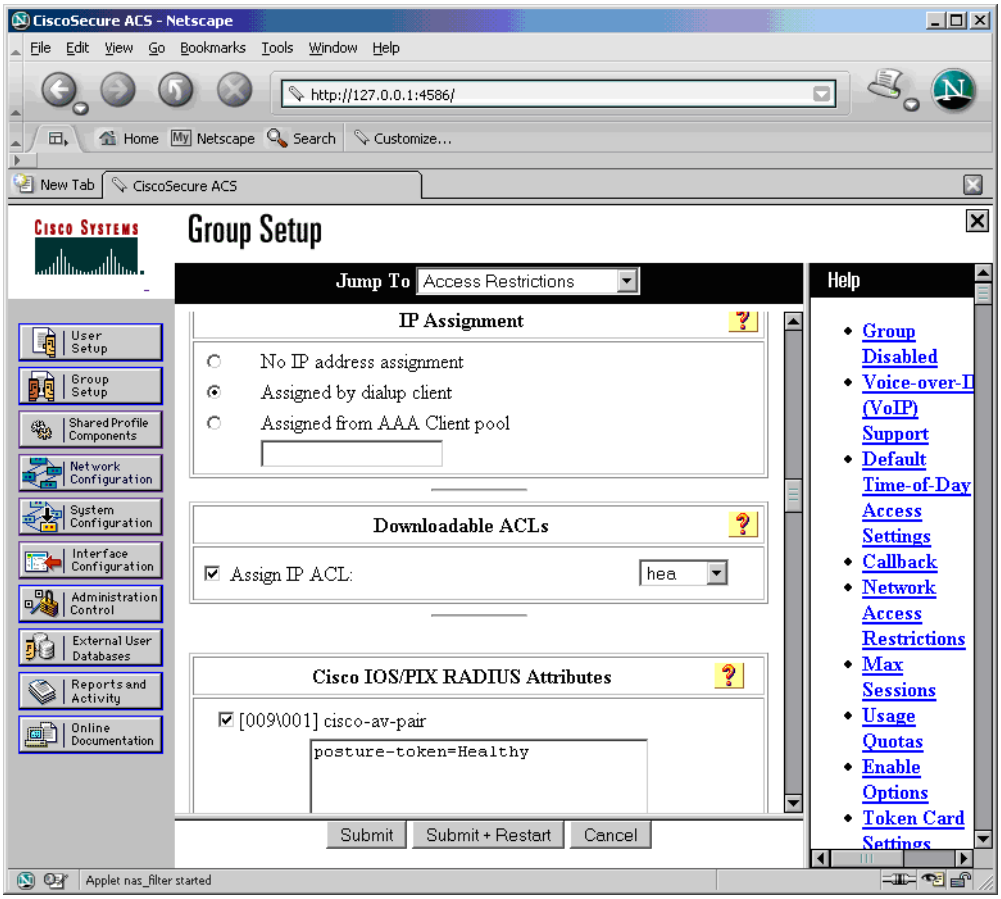


Figure 14 shows the **Group settings**.

Figure 14. NAC Group Settings



Defining the Healthy ACL

Figure 15 shows the **ACL definition**.

Figure 15. NAC ACL

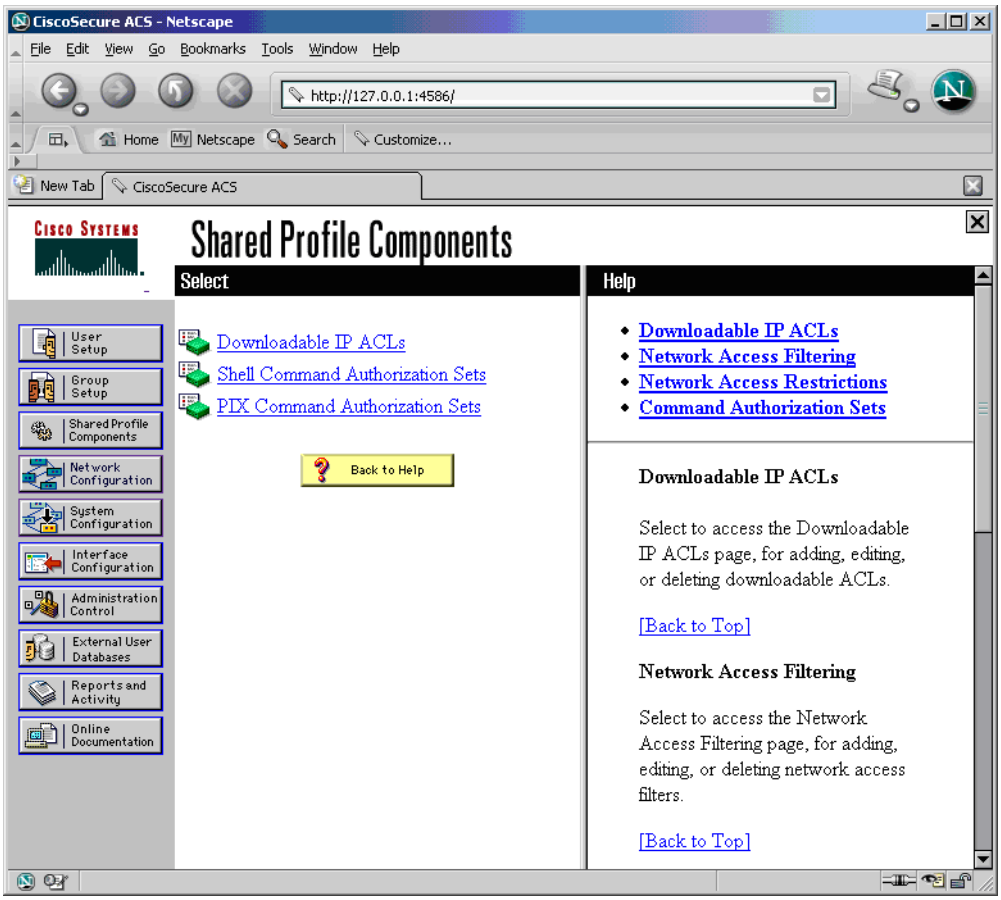


Figure 16 shows the **ACL definition**.

Figure 16. NAC ACL

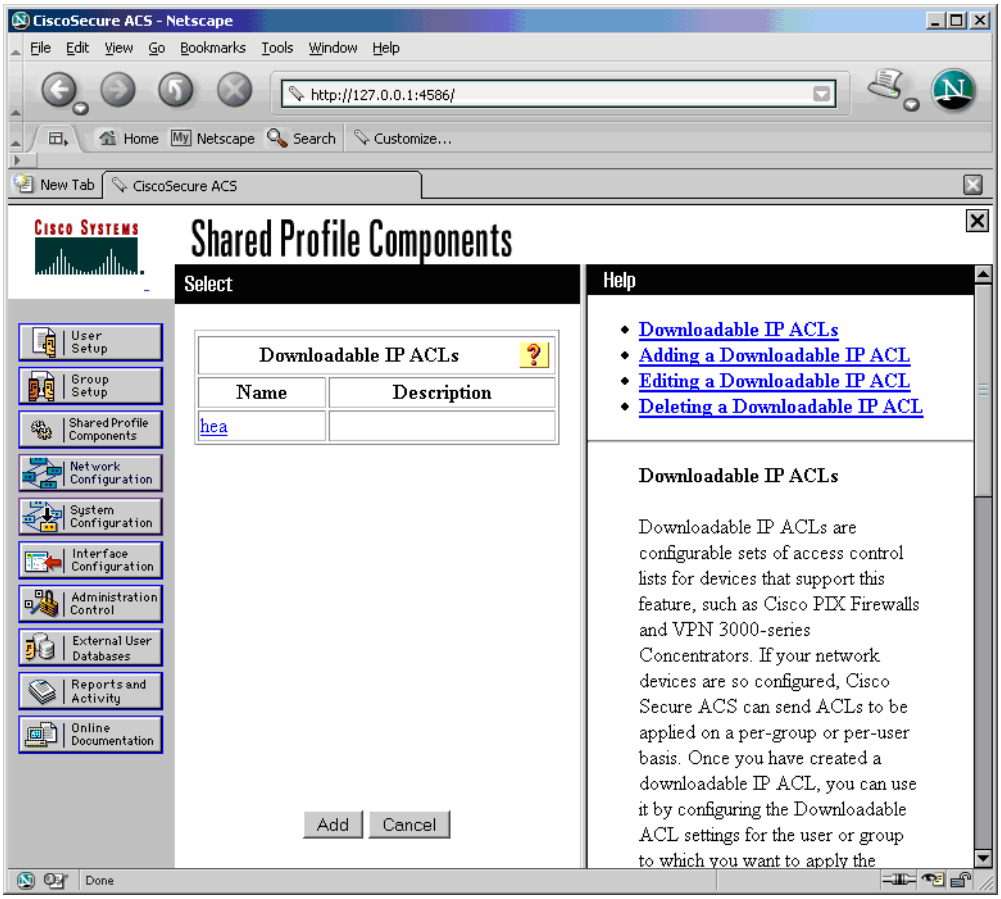


Figure 17 shows the **ACL definition**.

Figure 17. NAC ACL

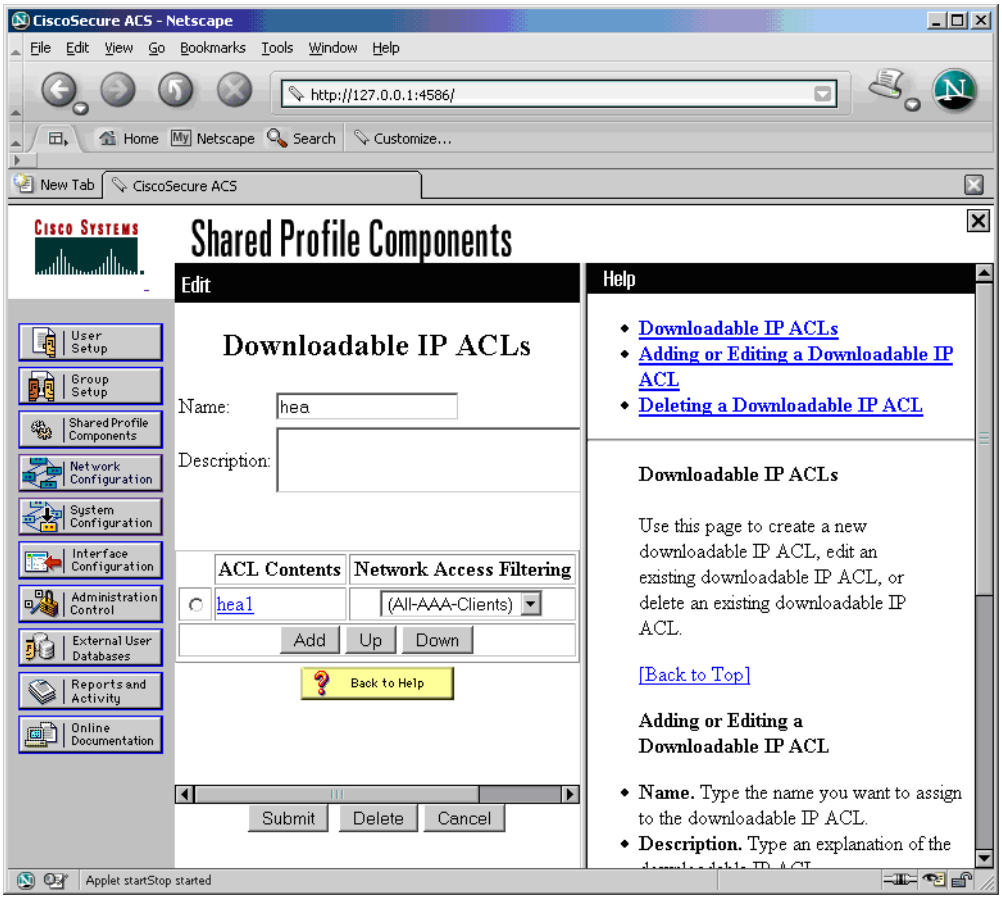
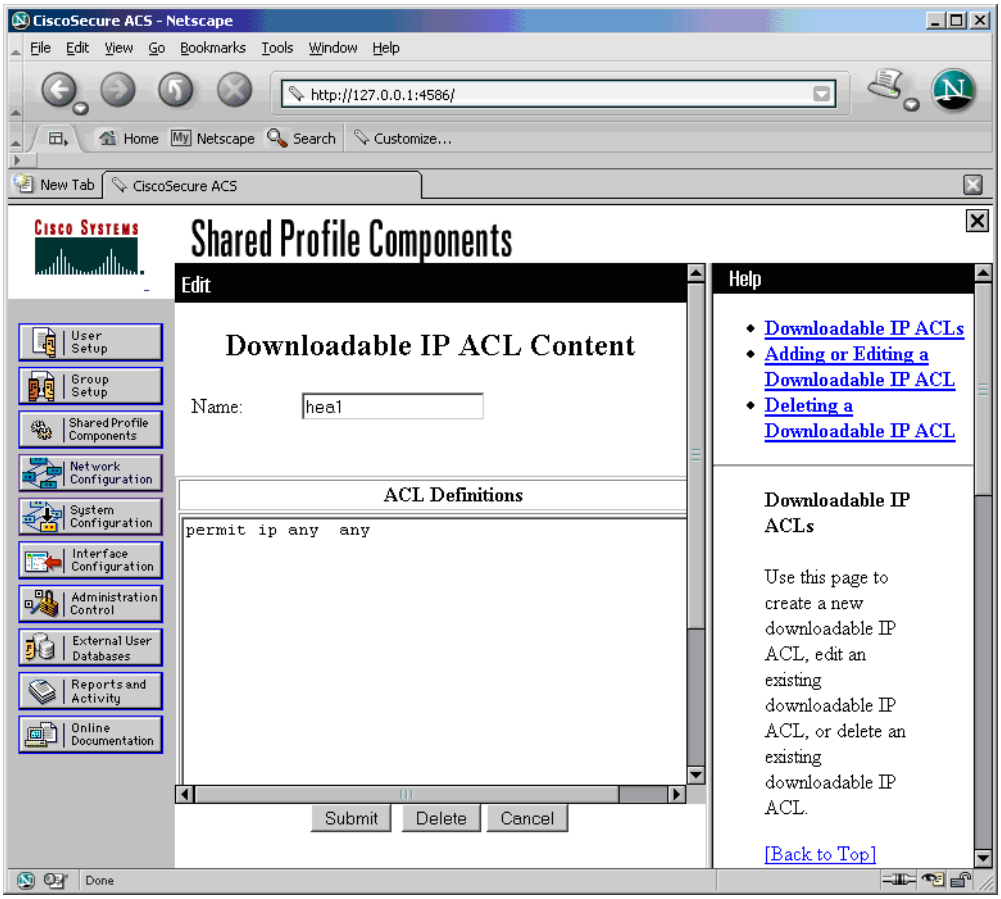


Figure 18 shows the **ACL definition**.

Figure 18. NAC ACL



DEBUGS AND SHOW COMMANDS

Before the Client Connects

```
7200-VTI-2#sh access-lists
Extended IP access list 101
    10 permit udp any any eq 21862
7200-VTI-2#
```

While the Client Connects

```
Dec  7 19:11:41: RADIUS(00000014): Send Access-Request to 24.1.1.3:1645 id 1645/29, len
100
Dec  7 19:11:41: RADIUS:  authenticator DB B1 3C 29 71 0E BD FA - 6B 46 0C ED 5C E7 96 80
Dec  7 19:11:41: RADIUS:  User-Name           [1]   5   “nac”
Dec  7 19:11:41: RADIUS:  User-Password       [2]   18  *
Dec  7 19:11:41: RADIUS:  Calling-Station-Id  [31]  11  “40.30.1.1”
Dec  7 19:11:41: RADIUS:  NAS-Port-Type       [61]  6   Virtual                  [5]
```



```
Dec  7 19:11:41: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
Dec  7 19:11:41: RADIUS:  NAS-Port            [5]   6   2
Dec  7 19:11:41: RADIUS:  NAS-Port-Id         [87]  16  “103.121.138.76”
Dec  7 19:11:41: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
Dec  7 19:11:41: RADIUS:  NAS-IP-Address      [4]   6   24.100.1.22
Dec  7 19:11:41: RADIUS: Received from id 1645/29 24.1.1.3:1645, Access-Accept, len 148
Dec  7 19:11:41: RADIUS:  authenticator DC D3 E6 DB 06 39 D8 08 - 5D EA 7F 13 00 56 22 48
Dec  7 19:11:41: RADIUS:  Vendor, Cisco       [26]  30
Dec  7 19:11:41: RADIUS:   Cisco AVpair       [1]   24  “ipsec:key-exchange=ike”
Dec  7 19:11:41: RADIUS:  Vendor, Cisco       [26]  36
Dec  7 19:11:41: RADIUS:   Cisco AVpair       [1]   30  “ipsec:tunnel-password=nac123”
Dec  7 19:11:41: RADIUS:  Vendor, Cisco       [26]  32
Dec  7 19:11:41: RADIUS:   Cisco AVpair       [1]   26  “ipsec:addr-pool=nac-pool”
Dec  7 19:11:41: RADIUS:  Class               [25]  30


Dec  7 19:11:53: RADIUS(00000015): Send Access-Request to 24.1.1.3:1645 id 1645/30, len 90
Dec  7 19:11:53: RADIUS:  authenticator 76 EF D8 81 87 92 55 2C - 06 47 2F 2C 65 48 52 EF
Dec  7 19:11:53: RADIUS:  User-Name           [1]   7   “sunil”
Dec  7 19:11:53: RADIUS:  User-Pass:53: RADIUS:   61 2F 31 38 36 34 30 31 31 36 2F 32
[a/18640116/2]
Dec  7 19:11:53: RADIUS(00000015): Received from id 1645/30
AAA/AUTHOR/IKE: Processing AV addr
Dec  7 19:11:53: ISAKMP:(13006):AAA Authen: No group atts addedword
Dec  7 19:11:53: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  Authentication PASSED  User=sunil
Group=nac  Client_public_addr=40.30.1.1  Server_public_addr=40.22.1.1      [2]   18  *
Dec  7 19:11:53: RADIUS:  C
Dec  7 19:11:53: ISAKMP:(13006):ISAKMP/author: setting up the authorization request for
nac


Dec  7 19:11:53: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer 40.30.1.1:500
Id: nac 7 19:
Dec  7 19:11:53: %CRYPTO-6-EZVPN_CONNECTION_UP: (Server)  Mode=CLIENT_OR_NEM_PLUS
Client_type=UNKNOWN  User=sunil  Group=nac  Client_public_addr=40.30.1.1
Server_public_addr=40.22.1.1  Assigned_client_addr=192.168.1.4  11:
Dec  7 19:11:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,


RADIUS:  NAS-Port-OU Init Validation for idb= Virtual-Access2 src_mac= 0000.7f11.6a5a
src_ip= 192.168.1.4
Dec  7 19:11:54: eou-ev:30.3.143.24: msg = 33(eventEouCreateSession)
Dec  7 19:11:54: AAA/BIND(00000016): Bind i/f
Dec  7 19:11:54:     eou_auth 192.168.1.4: initial state eou_initialize has enter
Dec  7 19:11:54: eou-obj_create:192.168.1.4: EAPoUDP Session Created
Dec  7 19:11:54: eou-obj_link:192.168.1.4: EAPoUDP Session added to Hash tableType
[61]
Dec  7 19:11:54: %EOU-6-SESSION: IP=192.168.1.4| HOST=DETECTED| Interface=Virtual-Access2
6   Vir
Dec  7 19:11:54:     eou_auth 192.168.1.4: during state eou_initialize, got event
1(eouCheckProfile)
Dec  7 19:11:54: @@@ eou_auth 192.168.1.4: eou_initialize -> eou_initialize
```



```
Dec  7 19:11:54: eou-ev:192.168.1.4: msg = 3(eventEouStartHello)
Dec  7 19:11:54:     eou_auth 192.168.1.4: during state eou_initialize, got event
3(eouStartHello)
Dec  7 19:11:54: @@@ eou_auth 192.168.1.4: eou_initialize -> eou_hello
Dec  7 19:11:54: eou-ev:Starting Retransmit timer 3(192.168.1.4)
Dec  7 19:11:54: eou-ev:eou_send_hello_request: Send Hello Request host= 10.1.1.1
eou_port= 5566 (hex)


Dec  7 19:11:54: TLV M:1 R:0 Type=ASSOCIATION ID Length=4 Association=-864887300
Dec  7 19:11:54:     eou_auth 192.168.1.4: during state eou_hello, got event
5(eouHelloResponse)         [5]
Dec  7 19:11:54: @@@ eou_auth 192.168.1.4: eou_hello -> eou_client19:11:5
Dec  7 19:11:54: %EOU-6-CTA: IP=192.168.1.4| CiscoTrustAgent=DETECTED3: RADIUS:  NAS-Port
[5]   6   2
Dec  7 19:11:53: RADIUS:  NAS-Port-Id         [87]  16  “103.121.138.76”
Dec  7 19:11:53: RADIUS:  NAS-IP-Address      [4]   6   24.100.1.22
Dec  7 19:11:53: RADIUS: Received from id 1645/30 24.1.1.3:1645, Access-Accept, len 56


Dec  7 19:12:00: RADIUS:  Service-Type        [6]   6   EAPoUDP                   [25]
Dec  7 19:12:00: RADIUS:  NAS-IP-Address      [4]   6   24.100.1.22
Dec  7 19:12:00: RADIUS: Received from id 1645/40 24.1.1.3:1645, Access-Accept, len 327
Dec  7 19:12:00: RADIUS:  authenticator C1 BC 26 5A A6 D5 F3 83 - 50 F7 43 FC EC 36 65 A0
Dec  7 19:12:00: RADIUS:  Session-Timeout     [27]  6   300
Dec  7 19:12:00: RADIUS:  NAS-IP-Address      [4]   6   24.100.1.22
Dec  7 19:12:00: EAPoUDP (rx) Flags:128 Ver=1 opcode=4 Len=0 MsgId=3140505256 Assoc
ID=3120086995
Dec  7 19:12:00:     eou_auth 192.168.1.4: during state eou_authenticated, got event
7(eouResultAck)
Dec  7 19:12:00: @@@ eou_auth 192.168.1.4: eou_authenticated -> eou_authenticated
Dec  7 19:12:00: eou-ev:Starting Status Query timer 300(192.168.1.4)
Dec  7 19:12:00: RADIUS: Received from id 1645/41 24.1.1.3:1645, Access-Accept, len 128
```

After IPSec Connection Is Up

```
7200-VTI-2# sh cry isa sa de
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
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime Cap.

13006 40.22.1.1       40.30.1.1               ACTIVE 3des sha       2  05:57:41 CDX
       Engine-id:Conn-id =  VAM2+:6

7200-VTI-2#
```



```
7200-VTI-2# sh access-li
Extended IP access list 101
     permit ip host 192.168.1.4 any (53 matches)
    10 permit udp any any eq 21862 (33 matches)
Extended IP access list xACSACLx-IP-hea-42f77dc1
    10 permit ip any any
7200-VTI-2#


7200-VTI-2# sh eou all
-----------------------------------------------------------------
Address         Interface       AuthType   Posture-Token Age(min)
-----------------------------------------------------------------
192.168.1.4     Virtual-Access2 EAP        Healthy         2

7200-VTI-2#


7200-VTI-2# sh eou ip 192.168.1.4
Address             : 192.168.1.4
Interface           : Virtual-Access2
AuthType            : EAP
PostureToken        : Healthy
Age(min)            : 2
URL Redirect        : NO URL REDIRECT
ACL Name            : #ACSACL#-IP-hea-42f77dc1
User Name           : ASWAN_2:Administrator
Revalidation Period : 300 Seconds
Status Query Period : 300 Seconds
Current State       : AUTHENTICATED

7200-VTI-2#


7200-VTI-2# sh run int virtual-template 1
Building configuration...

Current configuration : 198 bytes
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback10
 ip access-group 101 in
 ip admission vti-nac
 load-interval 30
```



```
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile nac
end

7200-VTI-2#


7200-VTI-2# sh run int virtual-access 2
Building configuration...

Current configuration : 286 bytes
!
interface Virtual-Access2
 mtu 1514
 ip unnumbered Loopback10
 ip access-group 101 in
 ip admission vti-nac
 load-interval 30
 tunnel source 40.22.1.1
 tunnel destination 40.30.1.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile nac
 no tunnel protection ipsec initiate
end

7200-VTI-2#


7200-VTI-2# sh int virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback10 (10.1.1.1)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel source 40.22.1.1, destination 40.30.1.1
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPsec (profile “nac”)
  Last input never, output never, output hang never
```



```
  Last clearing of “show interface” counters 00:05:41
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
     70 packets input, 8234 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     22 packets output, 2616 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
7200-VTI-2#


7200-VTI-2# sh cry ips sa


interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 40.22.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.4/255.255.255.255/0/0)
   current_peer 40.30.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 22, #pkts encrypt: 22, #pkts digest: 22
    #pkts decaps: 70, #pkts decrypt: 70, #pkts verify: 70
    #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.: 40.22.1.1, remote crypto endpt.: 40.30.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x631B0487(1662715015)

     inbound esp sas:
      spi: 0xB68D31FE(3062706686)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2011, flow_id: VAM2+:11, crypto map: Virtual-Access2-head-0
        sa timing: remaining key lifetime (k/sec): (4392206/10591)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```



```
      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x631B0487(1662715015)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2012, flow_id: VAM2+:12, crypto map: Virtual-Access2-head-0
         sa timing: remaining key lifetime (k/sec): (4392214/10590)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
7200-VTI-2#


7200-VTI-2# sh ip cef 192.168.1.4 de
192.168.1.4/32, version 58, epoch 0
0 packets, 0 bytes
  tag information set
    local tag: implicit-null
  via 0.0.0.0, Virtual-Access2, 0 dependencies
    next hop 0.0.0.0, Virtual-Access2
    valid adjacency
7200-VTI-2#
```

Screen Captures on Client

Figures 19–22 show the **screenshots from the VPN Client PC, showing the tunnel establishment and Posture validation response**.

Figure 19. VPN Client Settings

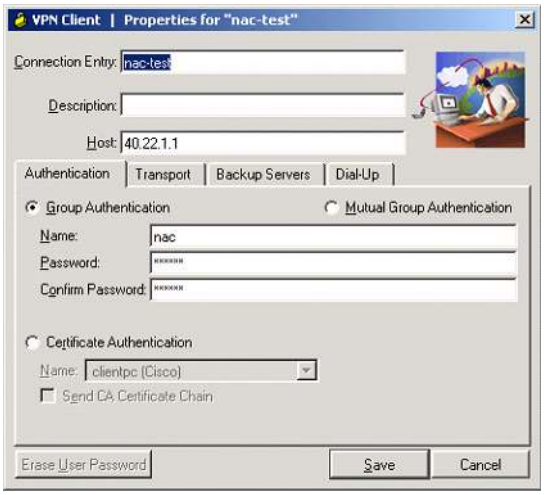


Figure 20. Xauth Username/Password

Figure 21. Posture Validated Message

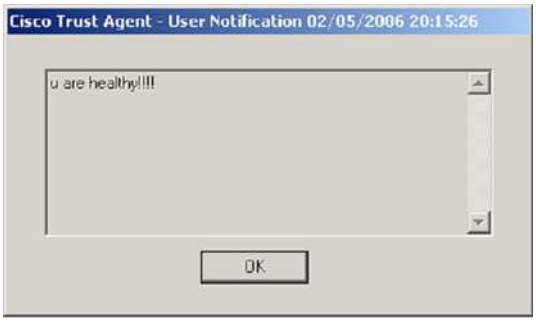
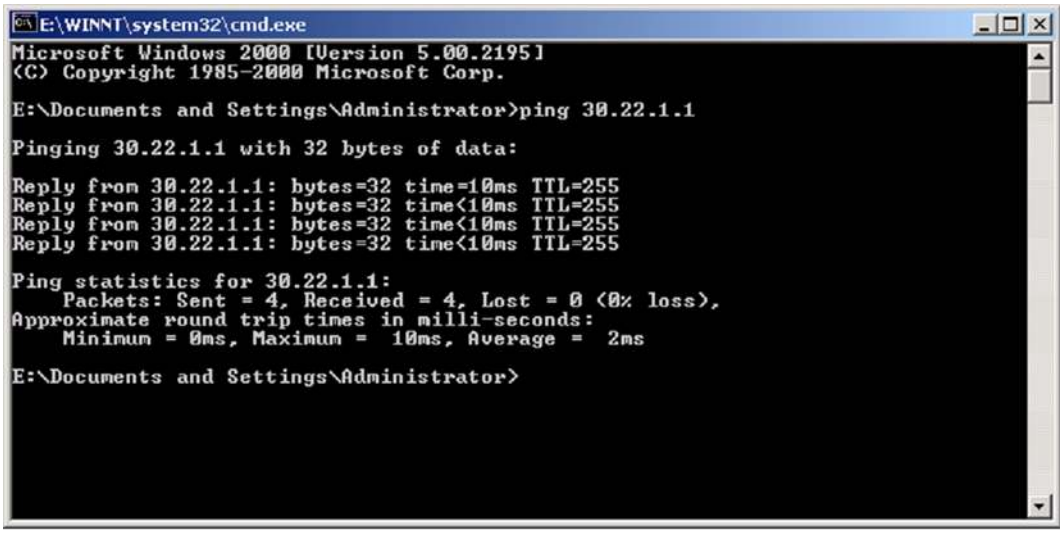


Figure 22. ICMP Traffic to Corporate Network



CONFIGURATIONS

Cisco 7200 Hub Router Configuration

```
7200-VTI-2#sh ver
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(4)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Thu 27-Oct-05 05:59 by ccai

ROM: System Bootstrap, Version 12.3(4r)T3, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(15), RELEASE SOFTWARE (fc3)

7200-VTI-2 uptime is 45 minutes
System returned to ROM by reload at 18:20:18 EST Wed Jan 25 2006
System restarted at 18:23:04 EST Wed Dec 7 2005
System image file is “disk2:c7200-adventerprisek9-mz.124-4.T”
Last reload reason: Reload Command


PCI bus mb1 (Slots 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb1 has a total of 0 bandwidth points.
This configuration is within the PCI bus capacity and is supported.

PCI bus mb2 (Slots 2, 4 and 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 600 bandwidth points.
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document “Cisco 7200 Series Port Adaptor Hardware
Configuration Guidelines” on Cisco.com <http://www.cisco.com>
```



```
for c7200 bandwidth points oversubscription and usage guidelines.


3 Gigabit Ethernet interfaces
1 Virtual Private Network (VPN) Module
509K bytes of NVRAM.

62720K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
16384K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2102

7200-VTI-2#
7200-VTI-2#


7200-VTI-2#sh run
Building configuration...

Current configuration : 5838 bytes
!
! Last configuration change at 19:04:51 EST Wed Dec 7 2005
! NVRAM config last updated at 19:03:54 EST Wed Dec 7 2005
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
service compress-config
!
hostname 7200-VTI-2
!
boot-start-marker
boot system flash disk2:c7200-adventerprisek9-mz.124-4.T
boot-end-marker
!
enable password lab
!
aaa new-model
!
!
aaa authentication login VPN-AAA group radius
aaa authentication eou default group radius
aaa authorization network VPN-AAA group radius
aaa accounting update periodic 30
aaa accounting network VPN-AAA start-stop group radius
!
```



```
aaa session-id common
!
resource policy
!
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
ip cef
!
!
!
!
ip vrf test
 rd 150:150
 route-target export 150:150
 route-target import 150:150
!
no ip domain lookup
ip domain name aswan.com
ip admission name vti-nac eapoudp inactivity-time 120
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
eou logging
username lab password 0 lab
username sunil password 0 lab
!
!
controller ISA 6/1
!
crypto keyring DMVPN-KEY
  pre-shared-key address 49.100.1.1 key mgmt123
crypto logging session
```



```
crypto logging ezvpn
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
 lifetime 21600
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 60 3
crypto isakmp nat keepalive 60
!
crypto isakmp client configuration group nac
 key nac123
 pool nac-pool
crypto isakmp profile MGMT-DMVPN
   keyring DMVPN-KEY
   match identity address 49.100.1.1 255.255.255.255
   keepalive 180 retry 60
crypto isakmp profile nac
   match identity group nac
   client authentication list VPN-AAA
   isakmp authorization list VPN-AAA
   client configuration address respond
   virtual-template 1
!
crypto ipsec security-association lifetime seconds 10800
crypto ipsec security-association idle-time 600
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
crypto ipsec transform-set GRE-TS esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROF
 set security-association lifetime seconds 12000
 set security-association idle-time 1800
 set transform-set GRE-TS
 set isakmp-profile MGMT-DMVPN
!
crypto ipsec profile nac
 set transform-set TS
 set isakmp-profile nac
!
```



```
!
!
!
!
!
interface Tunnel0
 description To 7301-MGMT (MGMT-24Net)
 ip address 24.200.1.22 255.255.255.0
 ip mtu 1400
 ip nhrp authentication mgmt
 ip nhrp map 24.200.1.254 49.100.1.1
 ip nhrp network-id 101
 ip nhrp holdtime 900
 ip nhrp nhs 24.200.1.254
 tunnel source GigabitEthernet0/1
 tunnel destination 49.100.1.1
 tunnel protection ipsec profile DMVPN-PROF
!
interface Loopback0
 description OSPF/BGP/LDP Src/ID
 ip address 30.100.1.22 255.255.255.255
!
interface Loopback1
 description AAA/Syslog/SNMP Src (MGMT-24Net)
 ip address 24.100.1.22 255.255.255.255
!
interface Loopback10
 description DVTI src-ip
 ip address 10.1.1.1 255.255.255.255
 load-interval 30
!
interface GigabitEthernet0/1
 description To Titan-AGG f3/27 (Internet Link)
 ip address 40.22.1.1 255.255.255.0
 load-interval 30
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
 description To GSR-Sol-P (MPLS Link)
 ip address 30.22.1.1 255.255.255.0
 load-interval 30
 duplex full
 speed 100
```



```
 media-type rj45
 no negotiation auto
 mpls label protocol ldp
 mpls ip
 mpls mtu 4470
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback10
 ip access-group 101 in
 ip admission vti-nac
 load-interval 30
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile nac
!
router eigrp 10
 passive-interface Loopback1
 network 24.100.1.22 0.0.0.0
 network 24.200.1.0 0.0.0.255
 auto-summary
 eigrp router-id 40.22.1.1
!
router ospf 20
 router-id 30.100.1.22
 log-adjacency-changes
 network 30.22.1.0 0.0.0.255 area 0
 network 30.100.1.22 0.0.0.0 area 0
!
router bgp 200
 bgp router-id 30.100.1.22
 bgp log-neighbor-changes
 neighbor 30.100.1.101 remote-as 200
 neighbor 30.100.1.101 update-source Loopback0
 !
 address-family ipv4
 no neighbor 30.100.1.101 activate
 no auto-summary
 no synchronization
 exit-address-family
```



```
 !
 address-family vpnv4
 neighbor 30.100.1.101 activate
 neighbor 30.100.1.101 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf test
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 exit-address-family
!
ip local pool nac-pool 192.168.1.1 192.168.1.250 group nac
ip classless
ip route 0.0.0.0 0.0.0.0 40.22.1.2
no ip http server
no ip http secure-server
!
!
!
ip radius source-interface Loopback1
logging alarm critical
logging facility local1
logging source-interface Loopback1
logging 24.1.1.2
access-list 101 permit udp any any eq 21862
snmp-server community public RO
snmp-server community nsite-rw RW
snmp-server trap-source Loopback1
snmp-server source-interface informs Loopback1
snmp-server contact sunilc
snmp-server chassis-id 7200-VTI-2
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server host 100.1.1.44 version 2c public
!
!
!
mpls ldp router-id Loopback0
radius-server host 24.1.1.3 auth-port 1645 acct-port 1646
radius-server key cisco123
radius-server vsa send accounting
!
control-plane
!
!
```



```
!
!
!
!
gatekeeper
 shutdown
!
alias exec seli show cry eli
alias exec sisa show cry isa sa count
alias exec sips show cry ipsec sa count
alias exec scpu show proc cpu | e 0.0
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
!
ntp clock-period 17179760
ntp source GigabitEthernet0/1
ntp update-calendar
ntp server 40.21.1.1
!
end

7200-VTI-2#
```


Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in USA C11-361561-00 08/06