Cisco Certified Network Associate Security

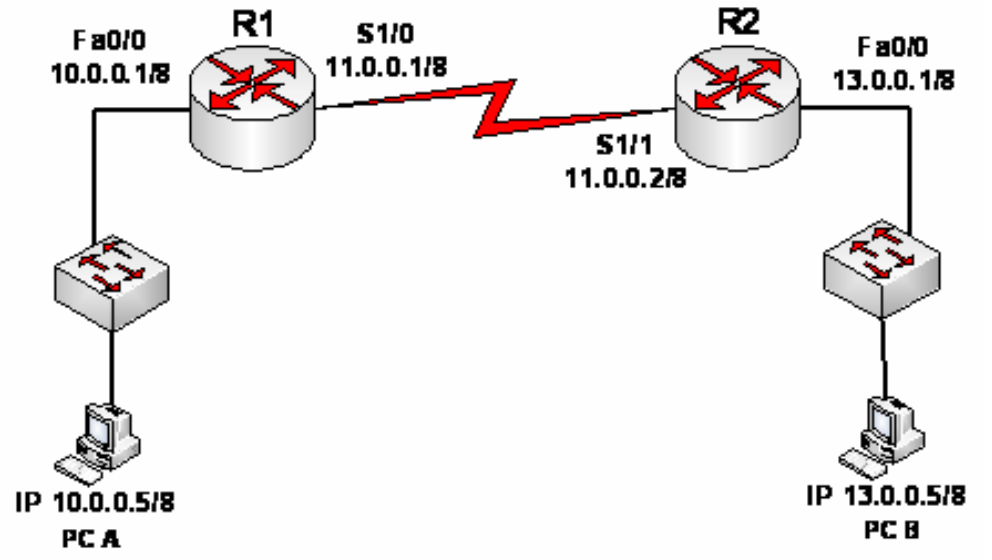
Lab Manual

Developed by : Ahmed Saeed
Network Manager
Yasir Imran
Sr.Network Engineer

LAB # 1

Securing the Router for Administrative Access

LAB # 1.1 Configure and Encrypt Passwords on Routers R1



Step 1: Configure a minimum password length for all router passwords.

```
R1(config)#security passwords min-length 6
```

Step 2: Configure the enable secret password.

R1(config)#enable secret yasir
% Password too short - must be at least 6 characters. Password configuration failed
R1(config)#

Configure enable secret password min-length 6 character

```
R1(config)#enable secret yasir123
```

Step 3: Configure basic console, auxiliary port, and virtual access lines.

```
R1(config)#line console 0
R1(config-line)#password ciscocon
R1(config-line)#login
R1(config-line)#logging synchronous

R1(config)#line aux 0
R1(config-line)#password ciscoauxpass
R1(config-line)#login
```

Configure the password on the vty lines for router R1.

```
R1(config)#line vty 0 4
R1(config-line)#password yasir123
R1(config-line)#login local
```

Show Command

```
R1#sh running-config
Building configuration...

Current configuration : 2267 bytes
!
version 12.4
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 $1$6p4q$f3GvBjAJxAemKsKtEfpSf.
!
no aaa new-model
ip cef
!
!
!
!
no ip domain lookup
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 11.0.0.1 255.255.255.0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
!
!
!
!
control-plane
!
!
!
line con 0
password cttc123
 logging synchronous
 login
line aux 0
 password yasir123
 login
line vty 0 4
 password yasir123
 login local
!
!
end

R1#
```

Step 4: Encrypt clear text passwords.

```
R1(config)# service password-encryption
```

Show command

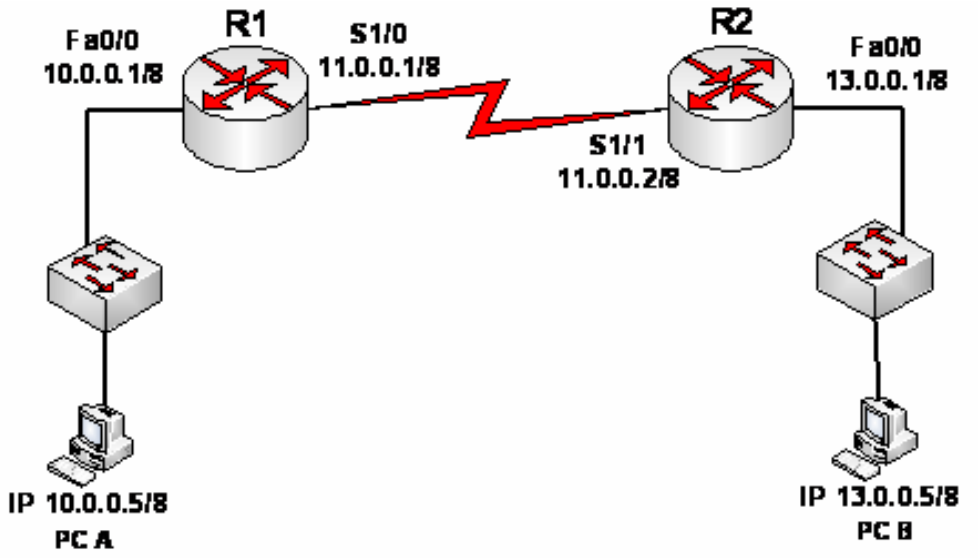
```
R1#sh running-config
Building configuration...

Current configuration : 2267 bytes
!
version 12.4
no service password-encryption
!
```

```
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 $1$6p4q$f3GvBjAJxAemKsKtEfpSf.
!
no aaa new-model
ip cef
!
!
!
username yasir privilege 15 password 7 030752180500
!
no ip domain lookup
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 11.0.0.1 255.255.255.0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
!
!
!
!
```

```
control-plane
!
!
!
line con 0
password 7 104D1D0D06464058
 logging synchronous
 login
line aux 0
 password 7 111018161E005A5E57
 login
line vty 0 4
 password 7 111018161E005A5E57
 login local
!
!
End
```

LAB # 1.2

Configure a Login Warning Banner on Routers R1



Step 1: Configure a warning message to display prior to login.

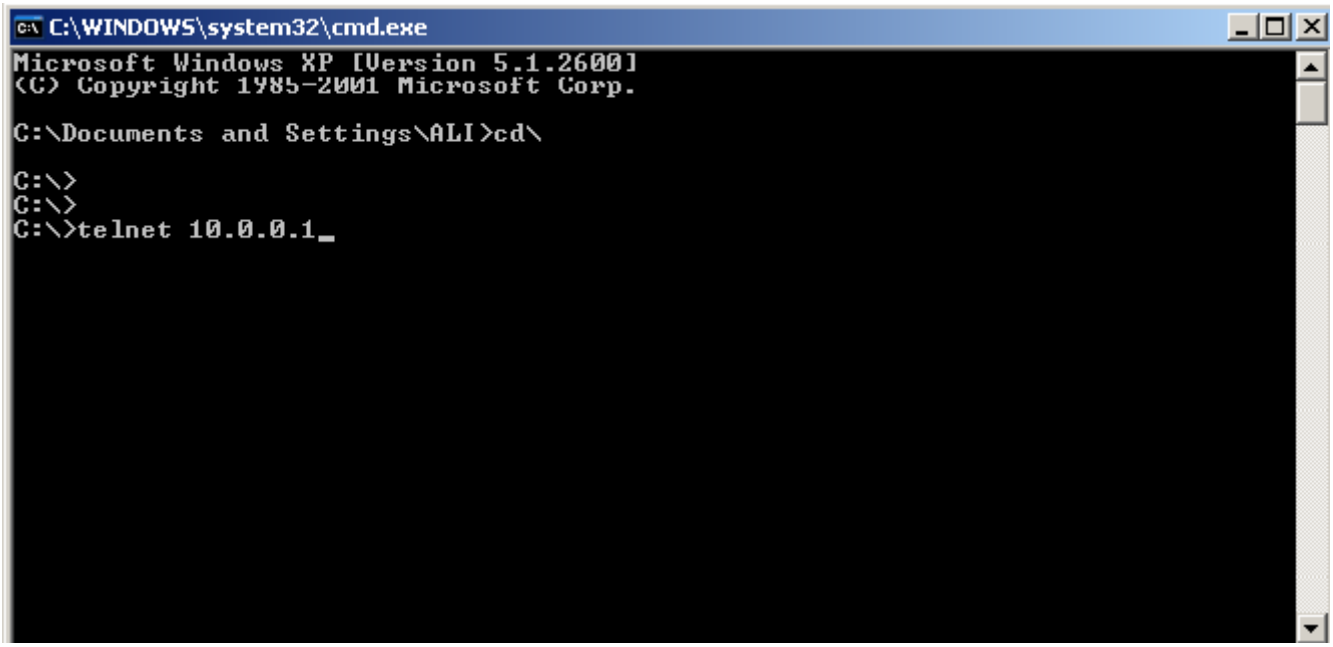
```
R1(config)#banner motd $Unauthorized access strictly prohibited and
prosecuted to the full extent of the law$

R1(config)#exit
```

Show Interface

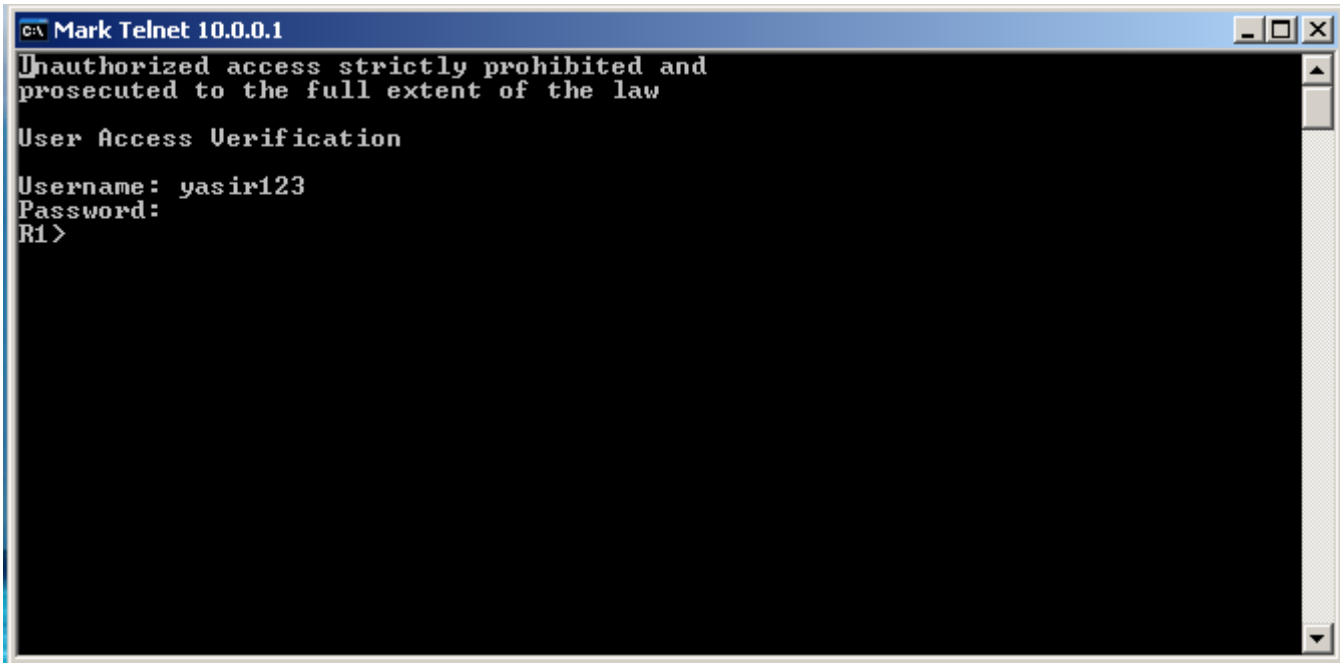
R1#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	NVRAM	up	up
FastEthernet0/1	unassigned	YES	NVRAM	administratively down	down
Serial1/0	11.0.0.1	YES	NVRAM	up	up
Serial1/1	unassigned	YES	NVRAM	administratively down	down
Serial1/2	unassigned	YES	NVRAM	administratively down	down
Serial1/3	unassigned	YES	NVRAM	administratively down	down

Telnet From PC to R1

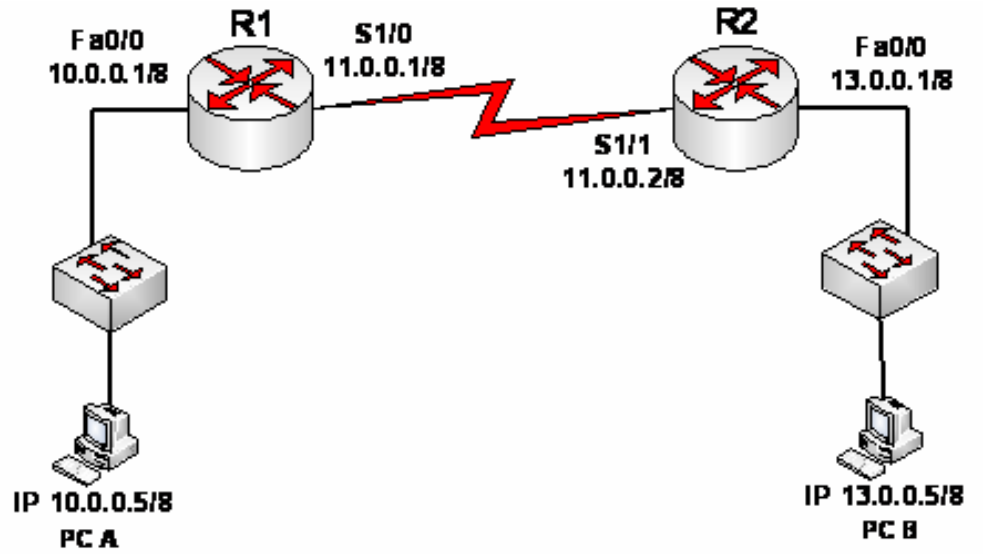


Now you can see login warning banner on R1



LAB 1.3

Configure Enhanced Username Password Security on Routers R1



Step 1: Create a new user account using the username command.

```
R1(config)#username yasir123 password  cttc123
```

Step 2: Create a new user account with a secret password.

```
R1(config)#username imran secret cttc123
```

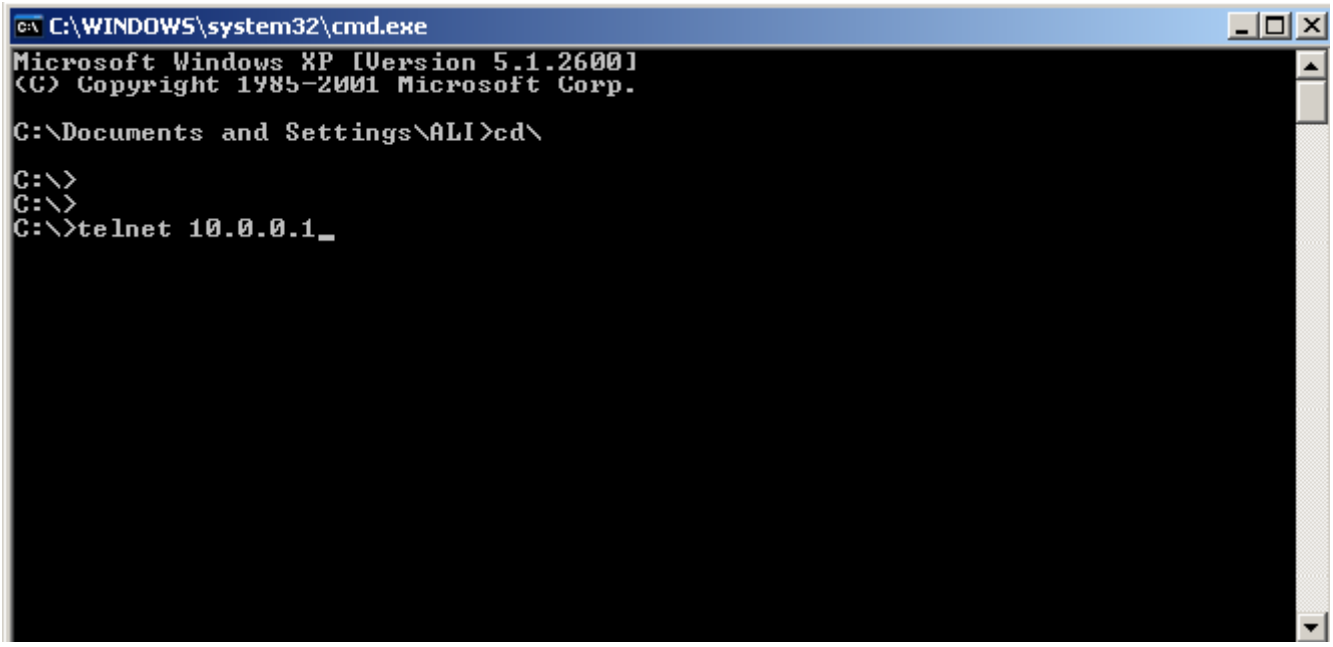
Show Commands

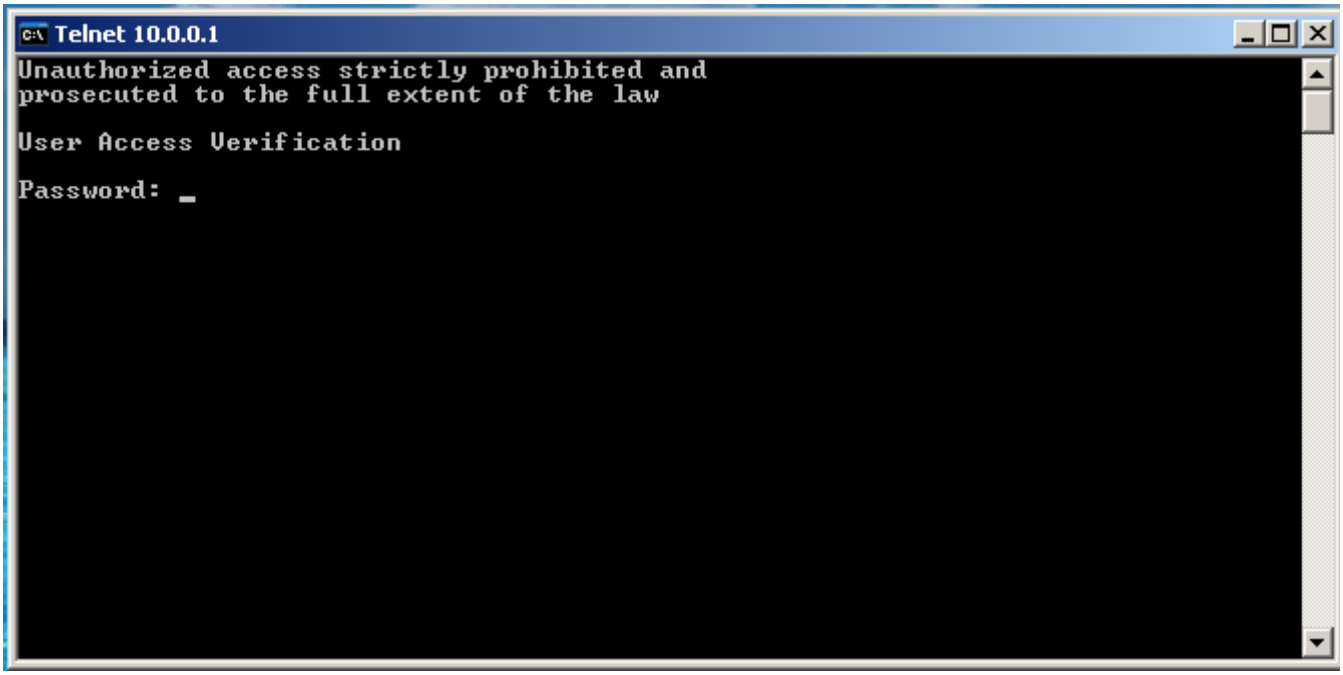
```
R1#sh running-config
Building configuration...

Current configuration : 2512 bytes
!
version 12.4
service password-encryption
!
hostname R1
!
!
security passwords min-length 6
enable secret 5 $1$6p4q$f3GvBjAJxAemKsKtEfpSf.
!
no aaa new-model
ip cef
!
!
!
!
no ip domain lookup
!
!
username yasir privilege 15 password 7 030752180500
username yasir123 password 7 121A1103115A5E57
username imran secret 5 $1$tKoa$.H/1Gk9NbJIlvYtPhx1j90
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

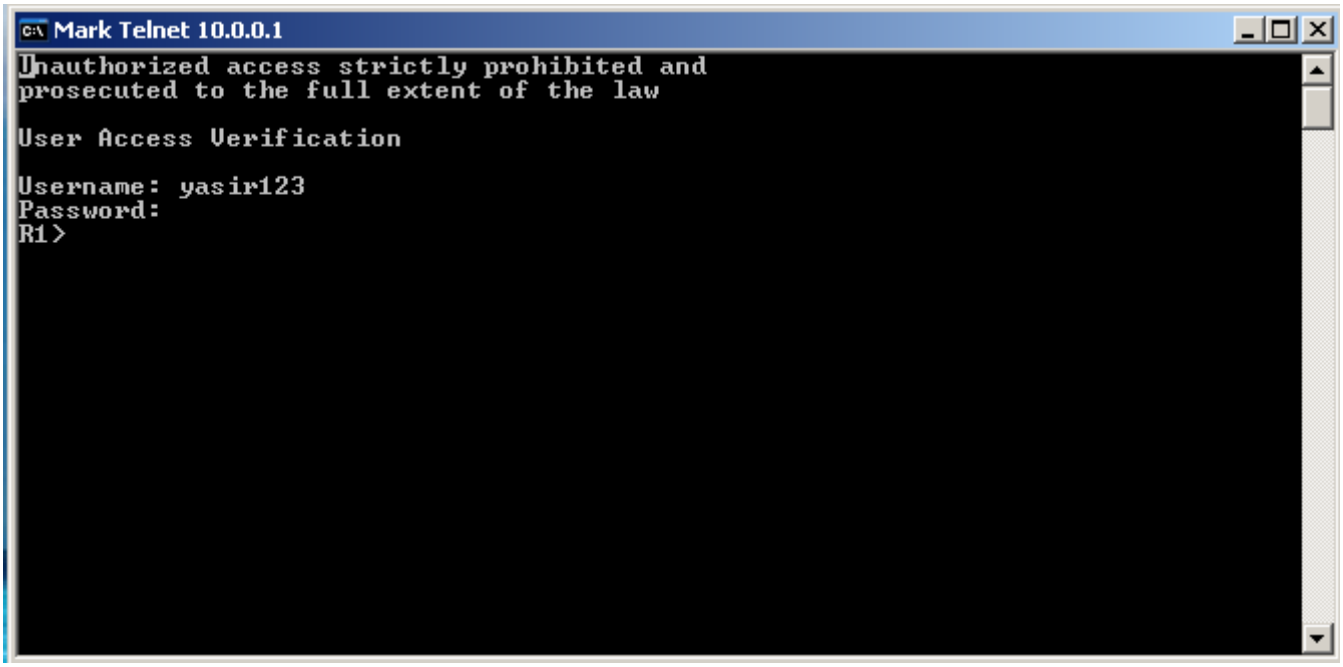
```
interface Serial1/0
 ip address 11.0.0.1 255.255.255.0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
!
!
!
control-plane
!
!
banner motd ^CUnauthorized access strictly prohibited and
prosecuted to the full extent of the law^C
!
line con 0
 password 7 104D1D0D06464058
 logging synchronous
 login local
line aux 0
 password 7 111018161E005A5E57
 login
line vty 0 4
 password 7 111018161E005A5E57
 login local
!
!
end

R1#
```

Step 3: Test the new account by logging from virtual terminal line.

```
R1(config)# line vty 0 4
R1(config-line)#login local
R1(config-line)#end
R1#exit
```

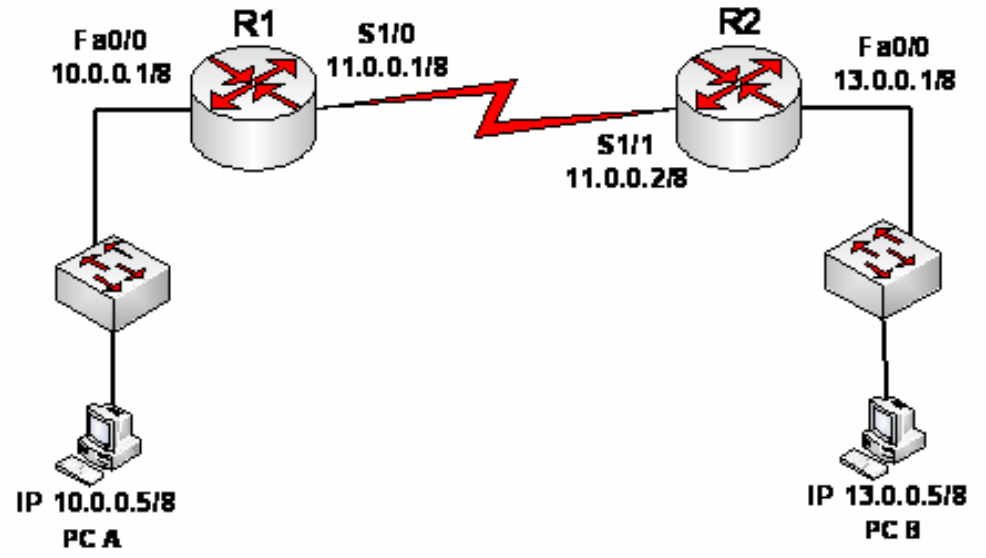

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\ALI>cd\
C:\>
C:\>
C:\>telnet 10.0.0.1


Telnet 10.0.0.1
Unauthorized access strictly prohibited and
prosecuted to the full extent of the law
User Access Verification
Password:



LAB # 1.4

Configure Enhanced Virtual Login Security on Routers R1



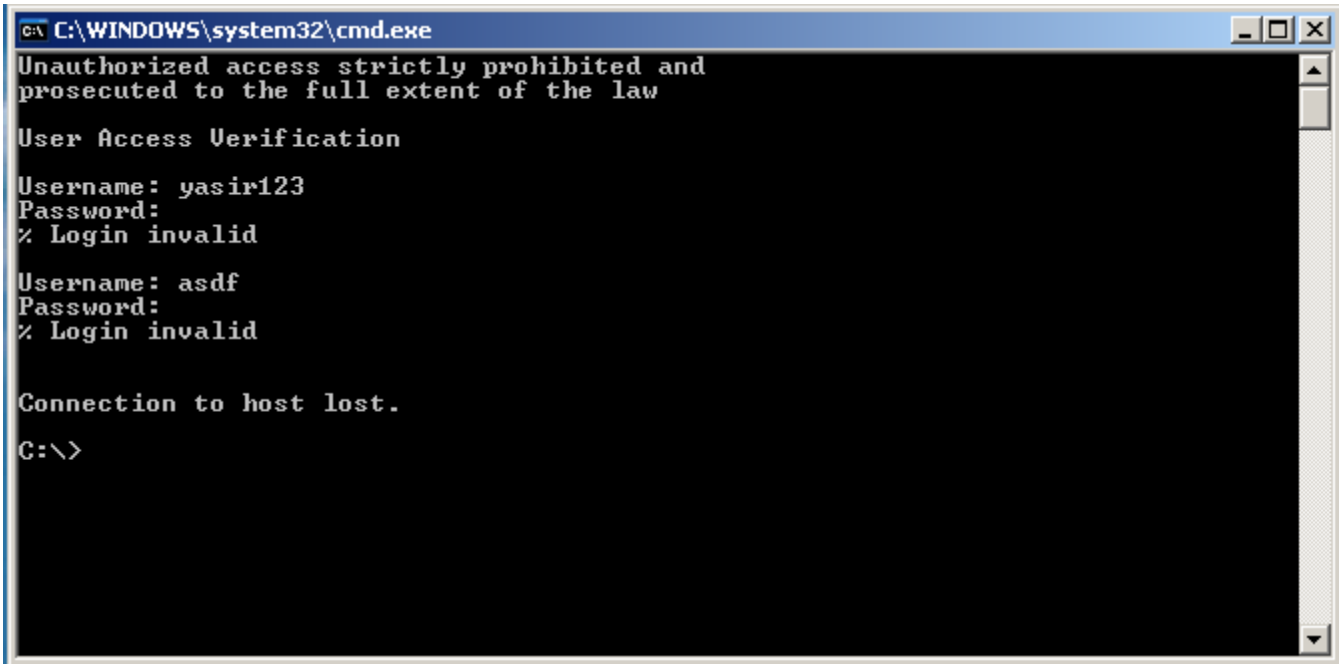
Step 1: Configure the router to watch for login attacks.

```
R1#show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
Router NOT enabled to watch for login Attacks


R1(config)#login block-for 60 attempts 2 within 30
```

```
R1#show login
     A default login delay of 1 seconds is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 30 seconds or less,
     logins will be disabled for 60 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 4 seconds.
         Login failures for current window: 0.
     Total login failures: 0.

R1#
```

Step 2: Configure the router to log login activity.

```
R1(config)#login on-success log
R1(config)#login on-failure log every 2
R1(config)#exit
```




```
R1#
```

```
*Mar  1 01:17:34.211: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: yasir123] [Source: 10.0.0.5
] [localport: 23] [Reason: Login Authentication Failed - BadPassword] at 01:17:34 UTC Fri Mar 1
2002
R1#
*Mar  1 01:17:36.995: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching failures is 14 sec
s, [user: asdf] [Source: 10.0.0.5] [localport: 23] [Reason: Login Authentication Failed - BadUse
r] [ACL: sl_def_acl] at 01:17:36 UTC Fri Mar 1 2002
R1#
```

Verification Commands

```
R1#show login failures
Total failed logins: 3
Detailed information about last 50 failures

Username      SourceIPAddr   lPort     Count          TimeStamp
yasir123       10.0.0.5       23         2          01:17:34 UTC Fri Mar 1 2002
asdf           10.0.0.5       23         1          01:17:36 UTC Fri Mar 1 2002
```

```
R1#show login
    A default login delay of 1 seconds is applied.
    No Quiet-Mode access list has been configured.
    Every 2 failed login is logged.

    Router enabled to watch for login Attacks.
    If more than 2 login failures occur in 30 seconds or less,
    logins will be disabled for 60 seconds.

    Router presently in Quiet-Mode.
    Will remain in Quiet-Mode for 34 seconds.
    Denying logins from all sources.

R1#
```

```
R1#
*Mar  1 01:18:36.995: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because block period time
 out at 01:18:36 UTC Fri Mar 1 2002
R1#
```

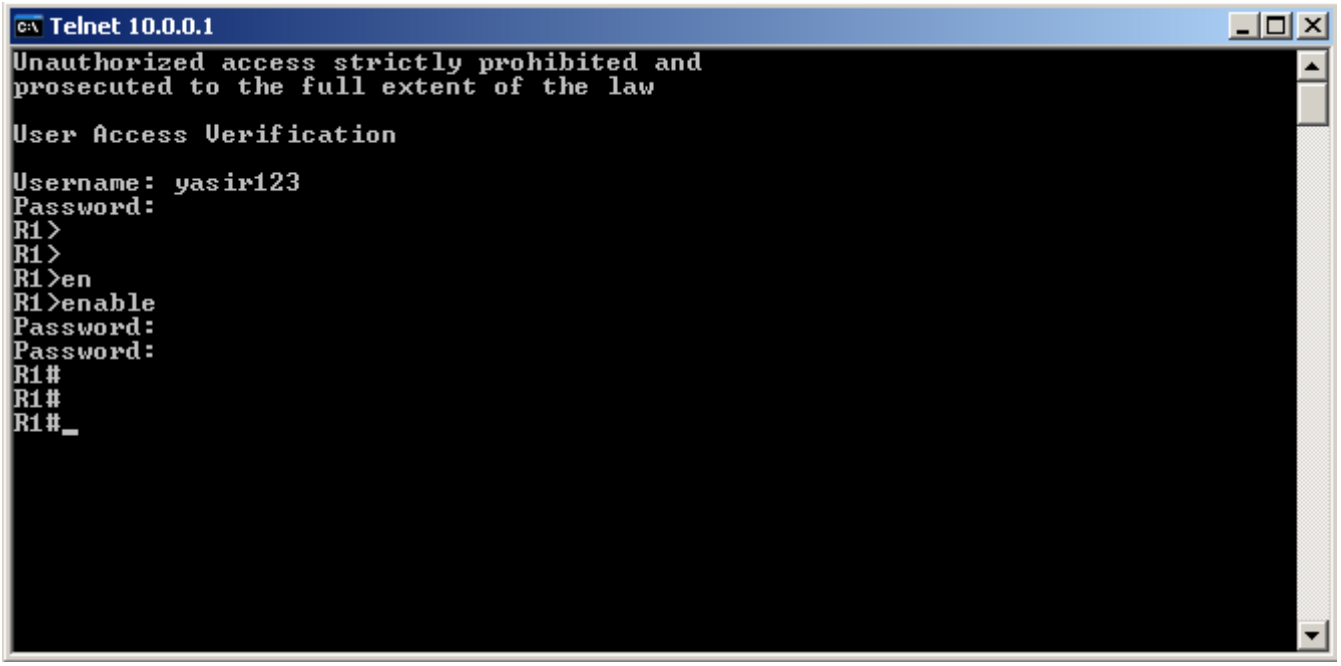
```
R1#show login
```

A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
Every 2 failed login is logged.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 30 seconds or less
logins will be disabled for 60 seconds.

Router presently in Normal-Mode.
Current Watch Window
Time remaining: 8 seconds.
Login failures for current window: 0.
Total login failures: 3.

R1#



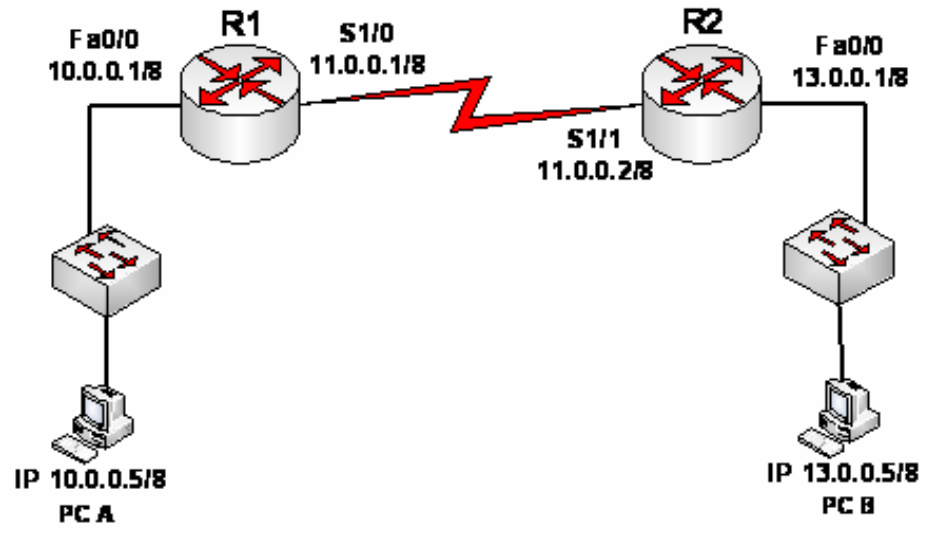
R1#show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
Every 2 failed login is logged.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 30 seconds or less,
logins will be disabled for 60 seconds.

Router presently in Normal-Mode.
Current Watch Window
Time remaining: 18 seconds.
Login failures for current window: 0.
Total login failures: 3.

LAB # 1.5

Configure the SSH Server on Router R1



Step 1: Configure a domain name.

```
R1#conf t
R1(config)#ip domain-name yasirb4u3.4shared.com
```

Step 2: Configure a privileged user for login from the SSH client.

```
R1(config)#username yasir privilege 15 secret cttc123
```

Step 3: Configure the vty lines.

```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

Step 4: Generate the RSA encryption key pair for the router.

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.yasirb4u3.4shared.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar  1 01:30:15.643:  RSA key size needs to be atleast 768 bits for ssh version 2
R1(config)#
*Mar  1 01:30:15.651: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#
```

Step 5: Verify the SSH configuration.

```
R1#show ip ssh

R1#sh ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
R1#
```

Step 6: Configure SSH timeouts and authentication parameters.

```
R1(config)#ip ssh time-out 90
R1(config)#ip ssh authentication-retries 2
```

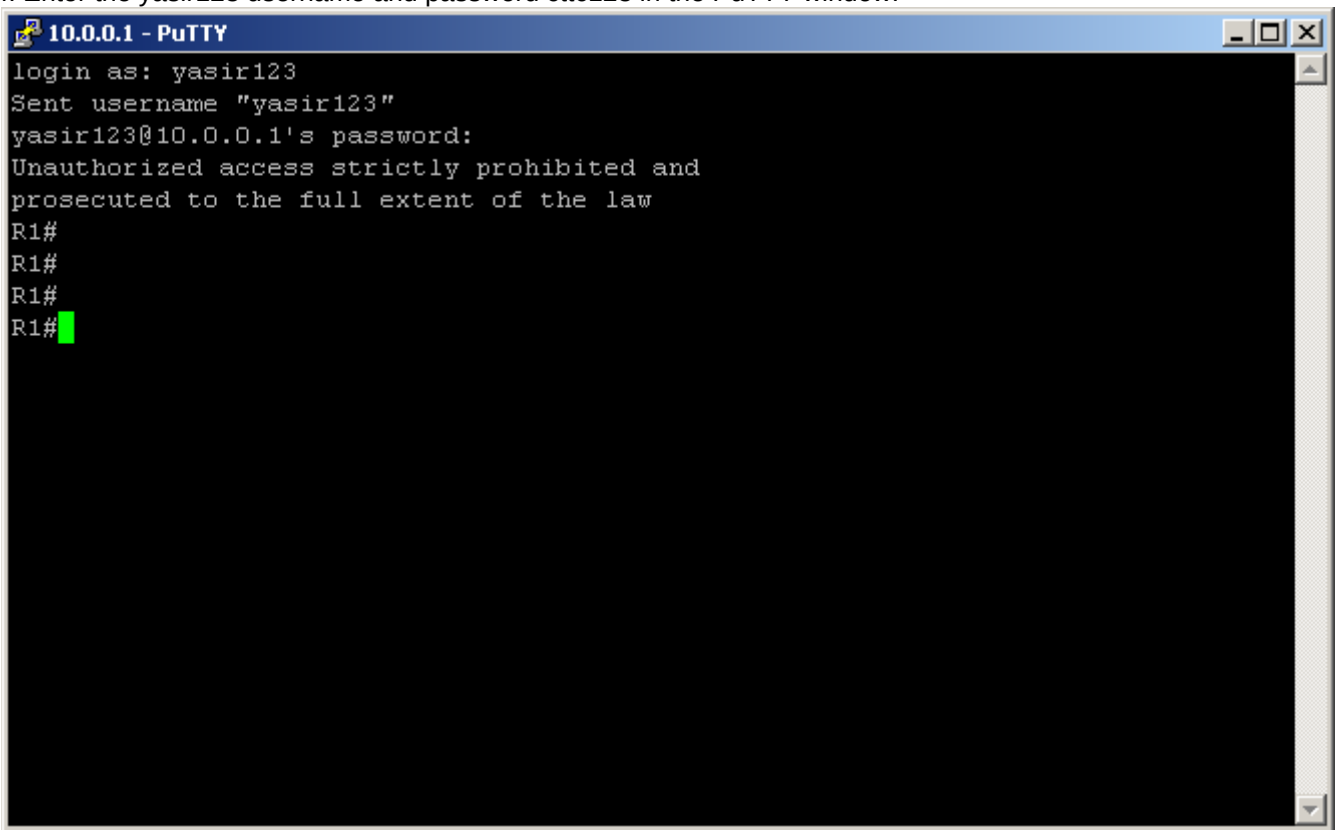
```
R1#sh ip ssh
SSH Enabled - version 1.5
Authentication timeout: 90 secs; Authentication retries: 2
R1#
```

Step 3: Verify SSH connectivity to R1 from PC.

a. Launch PuTTY by double-clicking the putty.exe icon.
b. Input the R1 Fa0/0 IP address 10.0.0.1 in the **Host Name or IP address** field.
c. Verify that the **SSH** radio button is selected.

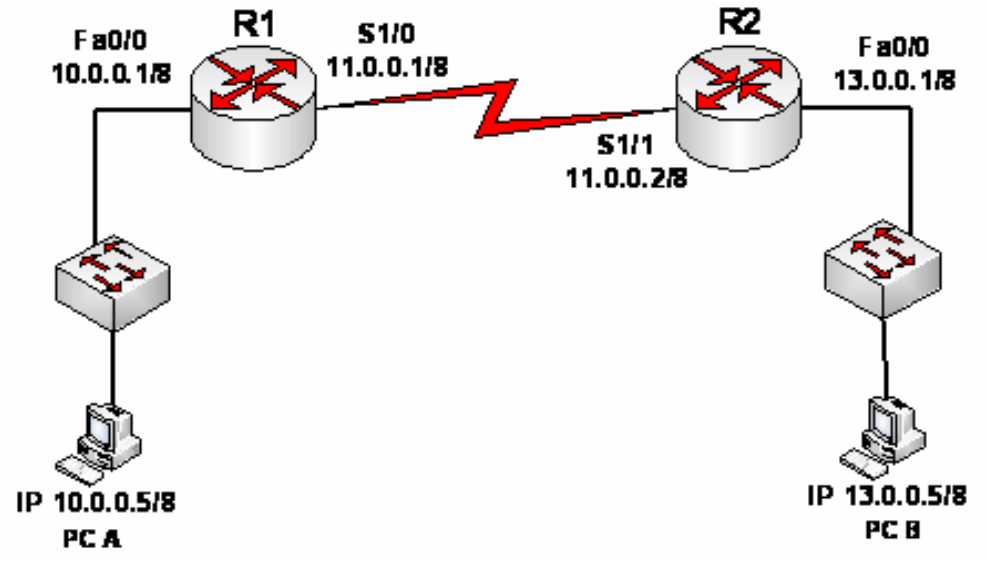
CCNA Security

d. Click **Open**.
e. In the PuTTY Security Alert window, click **Yes**.
f. Enter the yasir123 username and password cttc123 in the PuTTY window.



LAB # 1.6

Create an SDM user and enable the HTTP secure server on R1.



a. Create a privilege-level 15 username and password on R1.

```
R1(config)#username yasir privilege 15 password cttc
```

b. Enable the HTTP secure server on R1.

```
R1(config)#ip http secure-server

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 19 17:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 19 17:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue
"write memory" to save new certificate
```

c. Enable local HTTP authentication on R1.

```
R1(config)#ip http authentication local
R1(config)#end
```

Start SDM.

a. From PC-A, run the SDM application and enter the IP address of R1 FA0/0 (10.0.0.1) or open a
web browser and navigate to https://10.0.0.1

Cannot find server - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

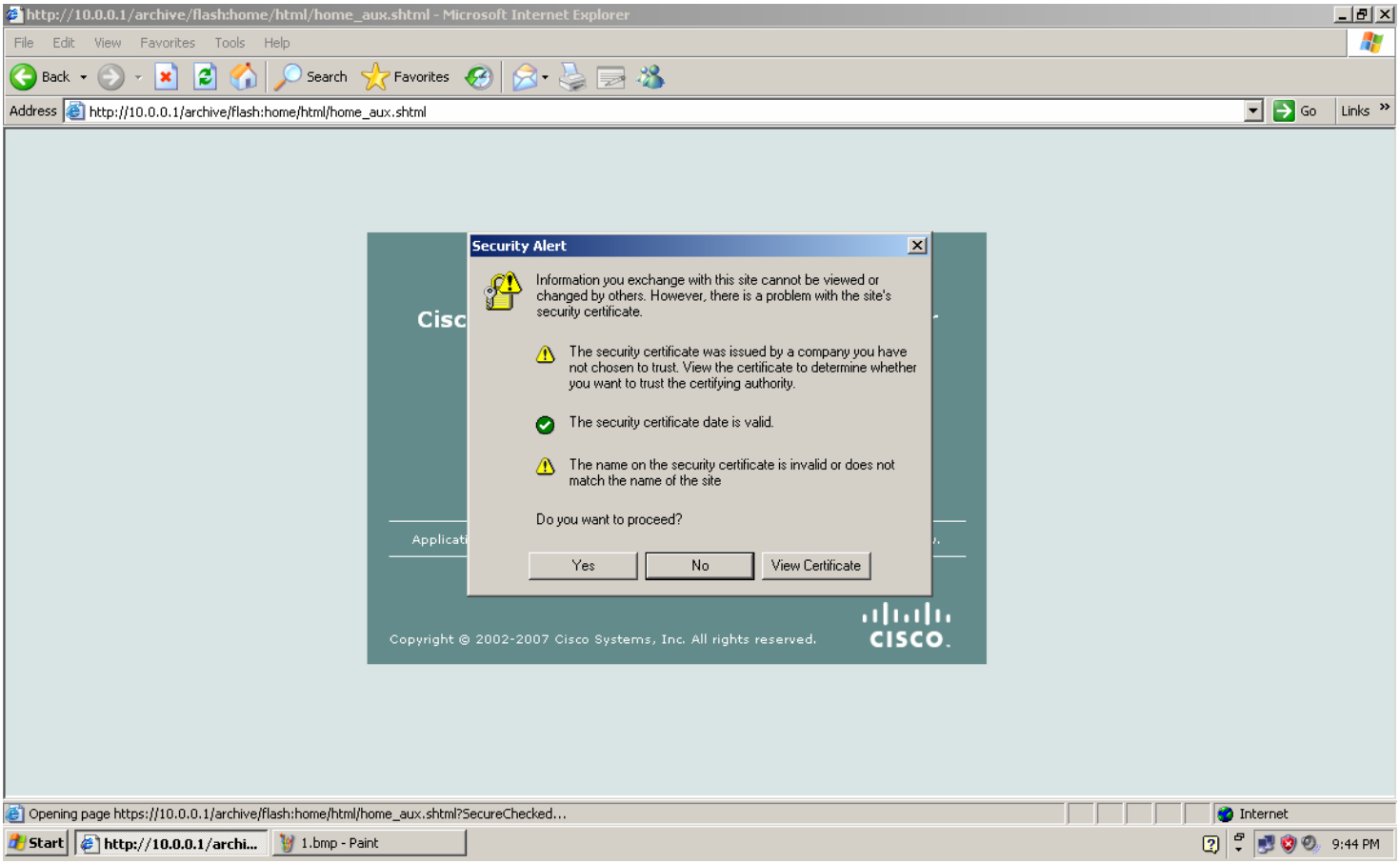
Address http://10.0.0.1 Go

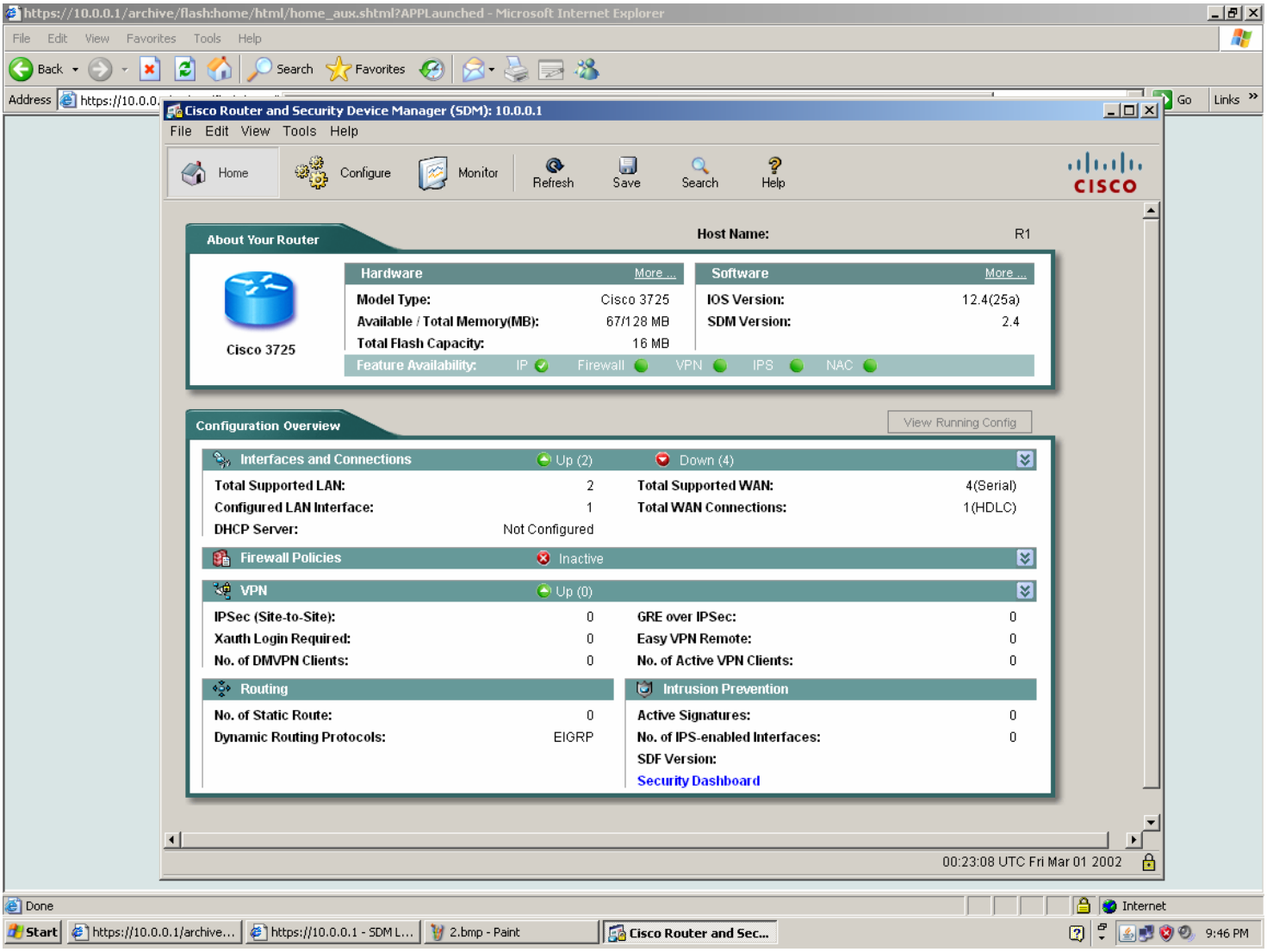
The page cannot be displayed

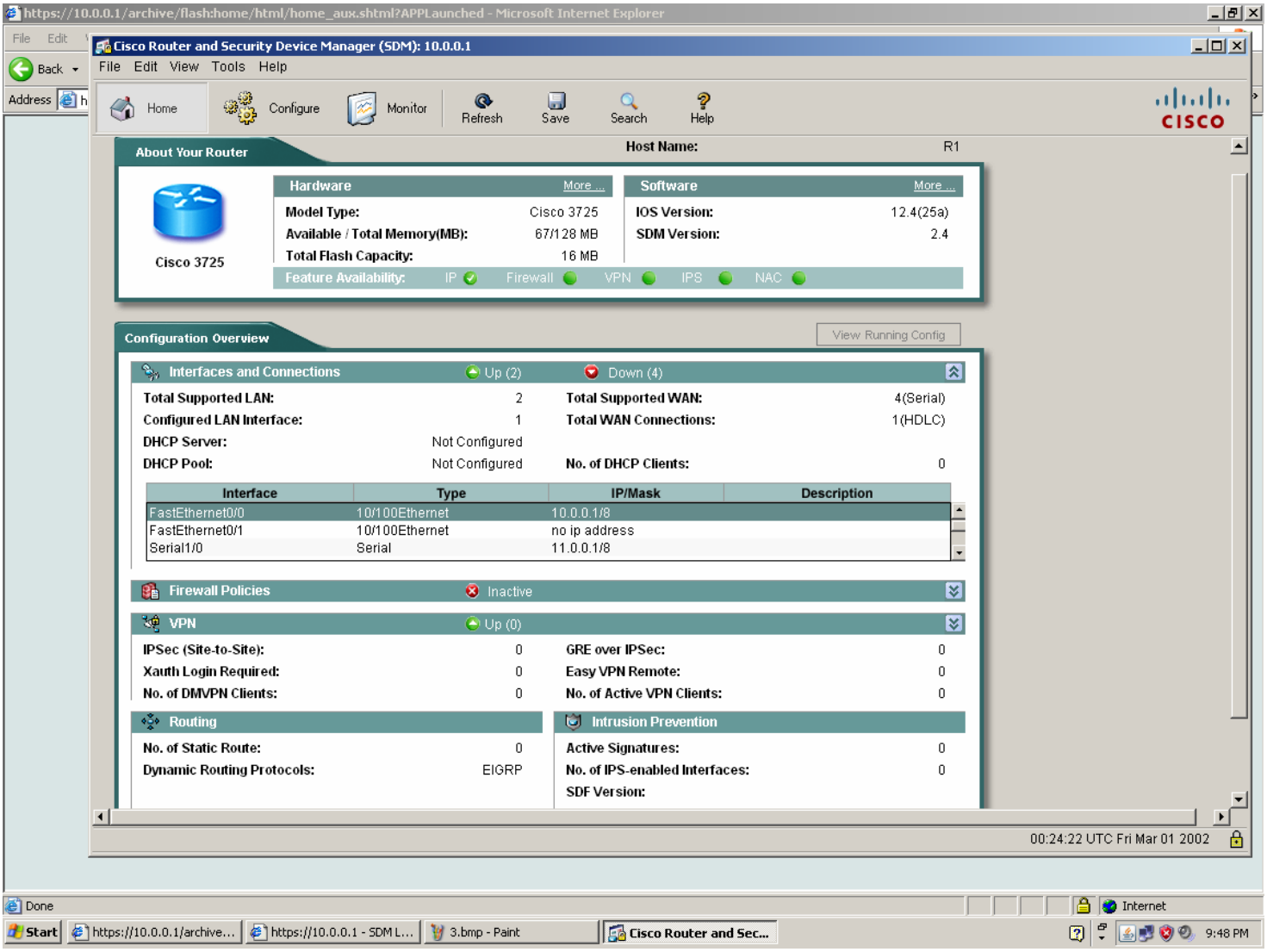
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

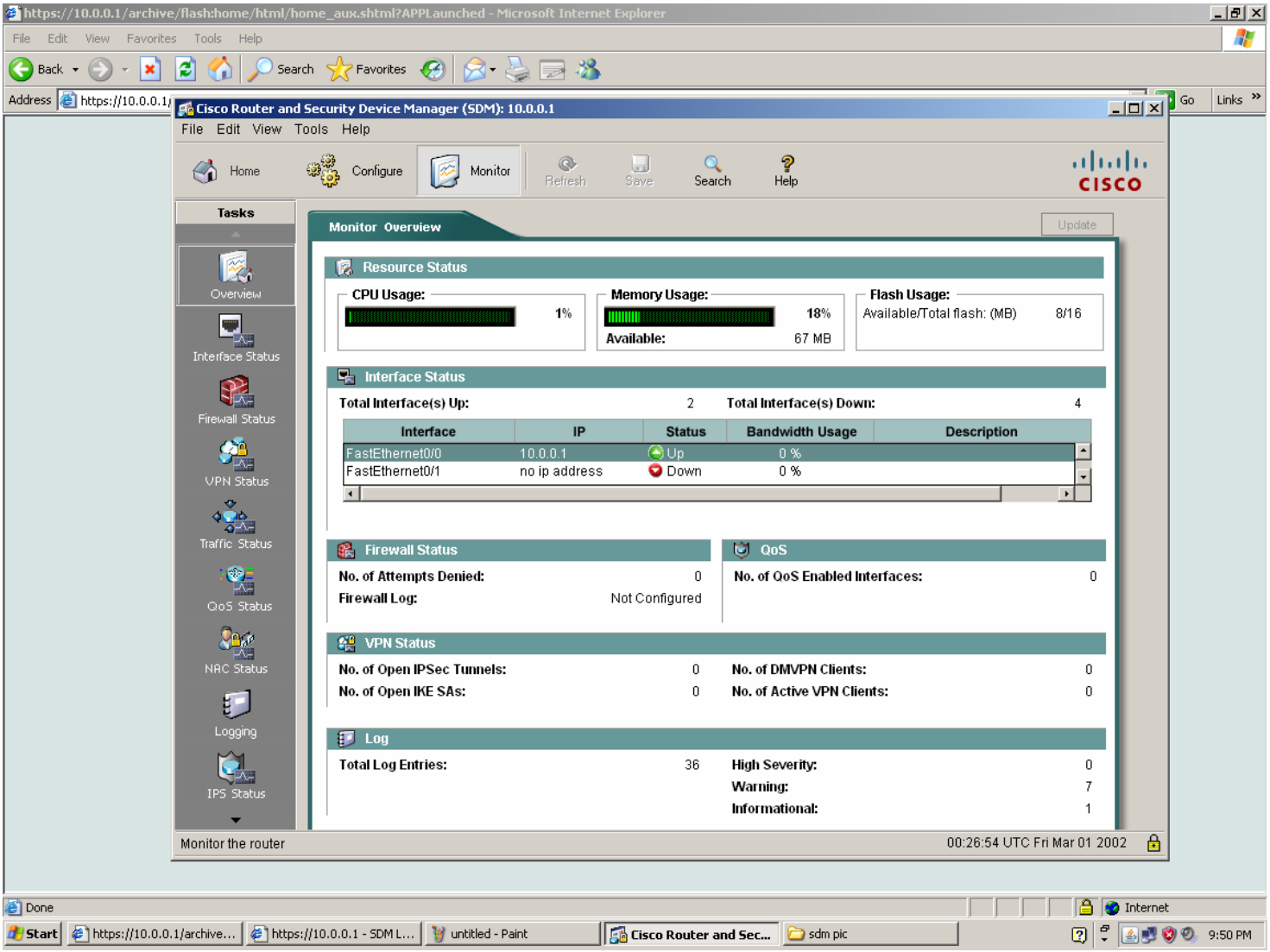
Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- To check your connection settings, click the **Tools** menu, and then click **Internet Options**. On the **Connections** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
- See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
    1. Click the **Tools** menu, and then click **Internet Options**.
    2. On the **Connections** tab, click **LAN Settings**.
    3. Select **Automatically detect settings**, and then click **OK**.
- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, and then click **Internet Options**. On the Advanced tab, scroll


http://10.0.0.1/archive/flash:home/html/home_aux.shtml - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10.0.0.1/archive/flash:home/html/home_aux.shtml
Go Links
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate
Copyright © 2002-2007 Cisco Systems, Inc. All rights reserved.
CISCO.
Opening page https://10.0.0.1/archive/flash:home/html/home_aux.shtml?SecureChecked...
Internet
Start
http://10.0.0.1/archi...
1.bmp - Paint
9:44 PM


https://10.0.0.1/archive/flash:home/html/home_aux.shtml?APPLaunched - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.0.0.
Go Links
Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home Configure Monitor Refresh Save Search Help
CISCO
About Your Router
Host Name: R1
Cisco 3725
Hardware More ...
Model Type: Cisco 3725
Available / Total Memory(MB): 67/128 MB
Total Flash Capacity: 16 MB
Software More ...
IOS Version: 12.4(25a)
SDM Version: 2.4
Feature Availability: IP Firewall VPN IPS NAC
Configuration Overview
View Running Config
Interfaces and Connections Up (2) Down (4)
Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 4(Serial)
Total WAN Connections: 1(HDLC)
Firewall Policies Inactive
VPN Up (0)
IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0
Routing
No. of Static Route: 0
Dynamic Routing Protocols: EIGRP
Intrusion Prevention
Active Signatures: 0
No. of IPS-enabled Interfaces: 0
SDF Version:
Security Dashboard
00:23:08 UTC Fri Mar 01 2002
Done
Internet
Start
https://10.0.0.1/archive...
https://10.0.0.1 - SDM L...
2.bmp - Paint
Cisco Router and Sec...
9:46 PM

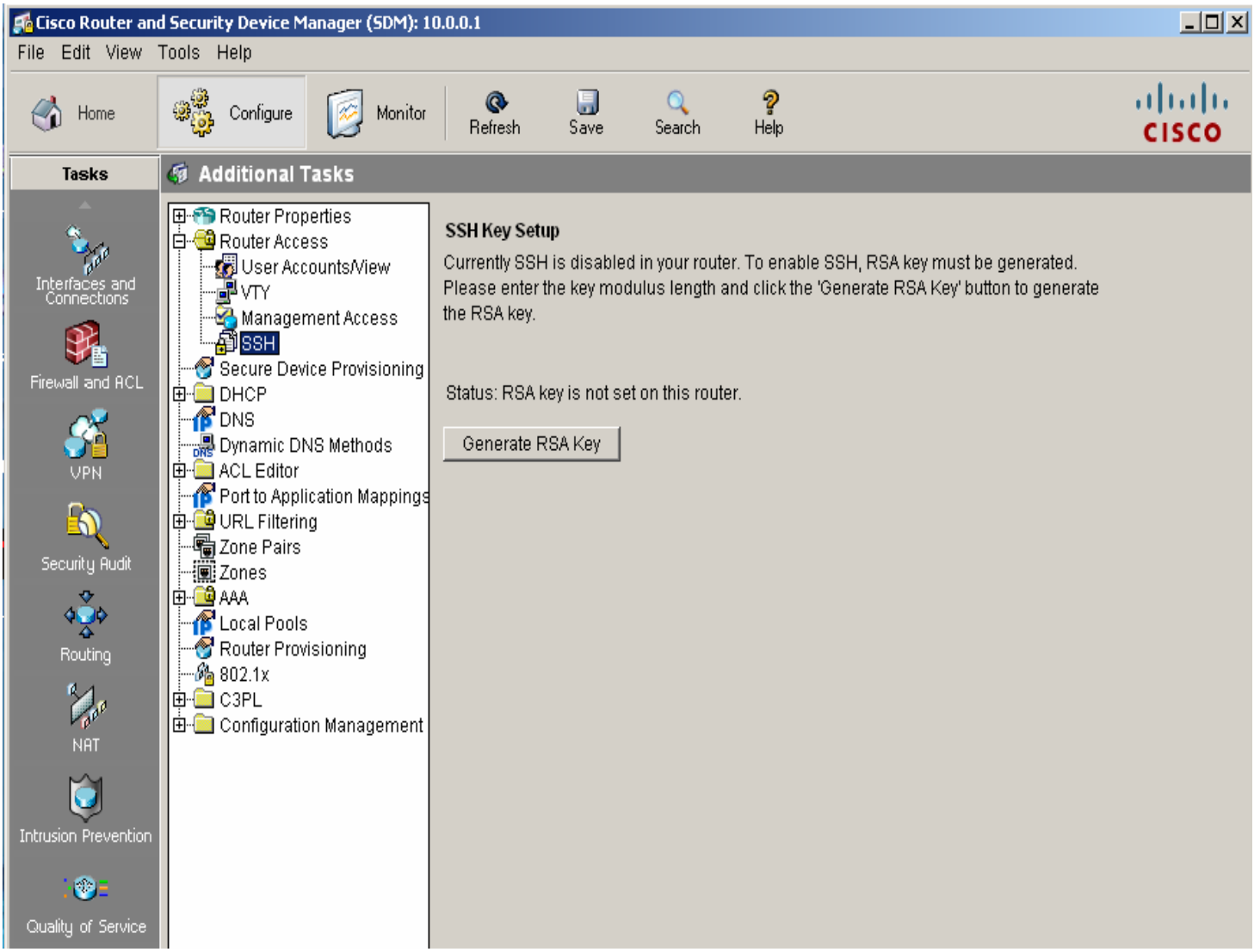

https://10.0.0.1/archive/flash:home/html/home_aux.shtml?APPLaunched - Microsoft Internet Explorer
Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
About Your Router
Host Name: R1
Cisco 3725
Hardware More ...
Model Type: Cisco 3725
Available / Total Memory(MB): 67/128 MB
Total Flash Capacity: 16 MB
Software More ...
IOS Version: 12.4(25a)
SDM Version: 2.4
Feature Availability: IP Firewall VPN IPS NAC
Configuration Overview
View Running Config
Interfaces and Connections Up (2) Down (4)
Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
DHCP Pool: Not Configured
Total Supported WAN: 4(Serial)
Total WAN Connections: 1(HDLC)
No. of DHCP Clients: 0
Interface Type IP/Mask Description
FastEthernet0/0 10/100Ethernet 10.0.0.1/8
FastEthernet0/1 10/100Ethernet no ip address
Serial1/0 Serial 11.0.0.1/8
Firewall Policies Inactive
VPN Up (0)
IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0
Routing
No. of Static Route: 0
Dynamic Routing Protocols: EIGRP
Intrusion Prevention
Active Signatures: 0
No. of IPS-enabled Interfaces: 0
SDF Version:
00:24:22 UTC Fri Mar 01 2002
Done
Internet
Start
https://10.0.0.1/archive...
https://10.0.0.1 - SDM L...
3.bmp - Paint
Cisco Router and Sec...
9:48 PM



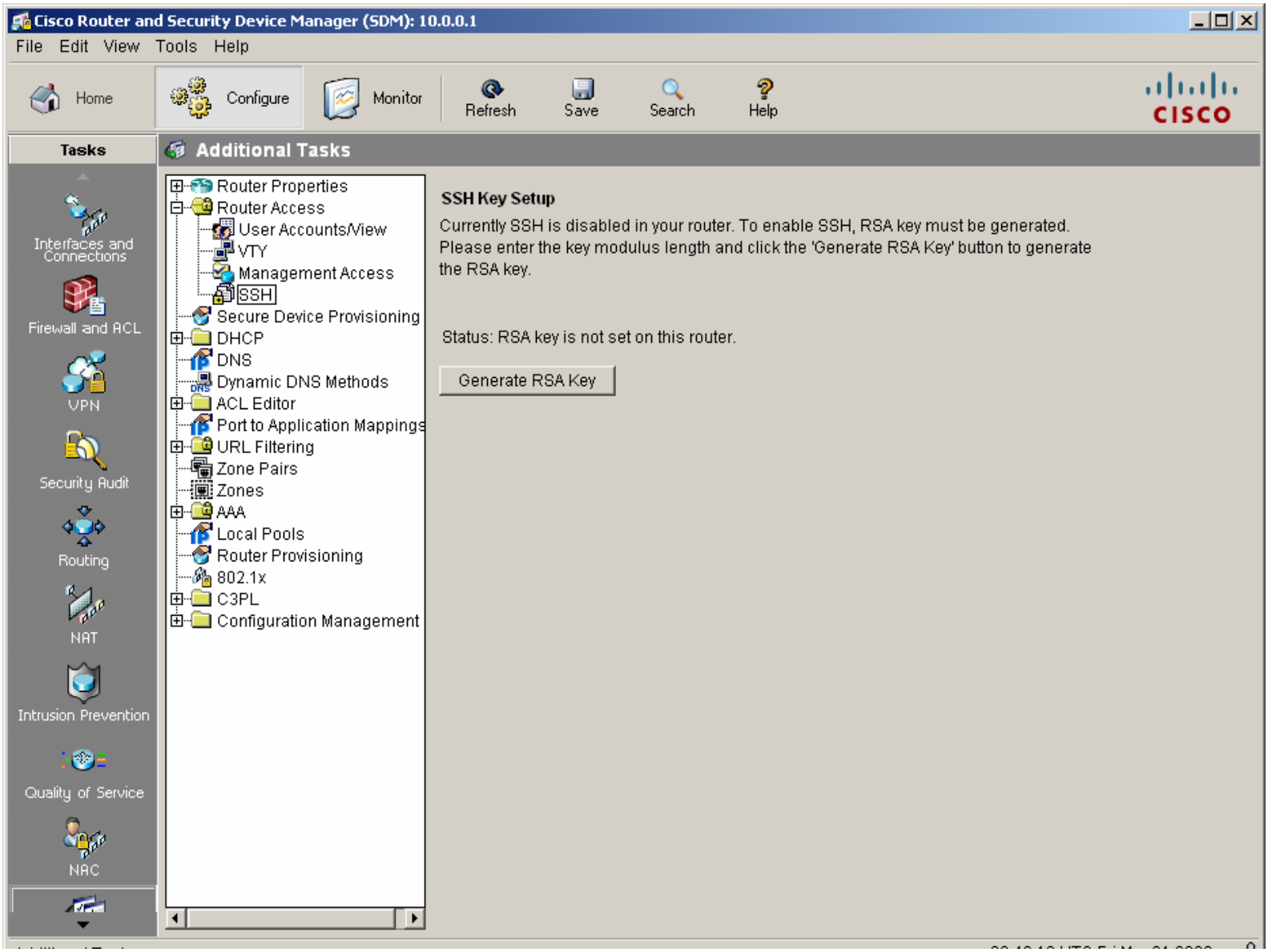
LAB # 1.7

Configure the SSH on Router R1 with SDM

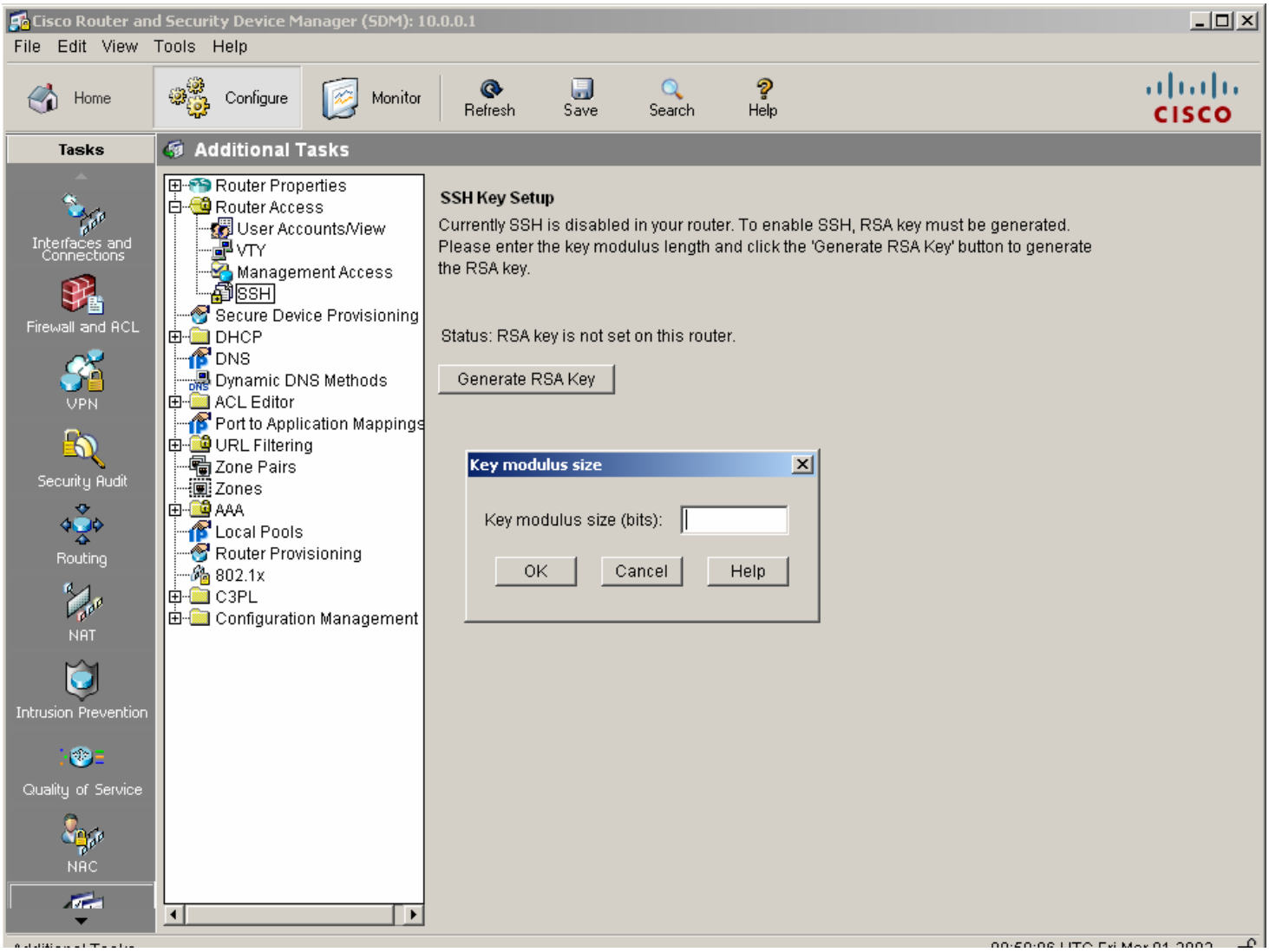
Click on configure then click on additional task



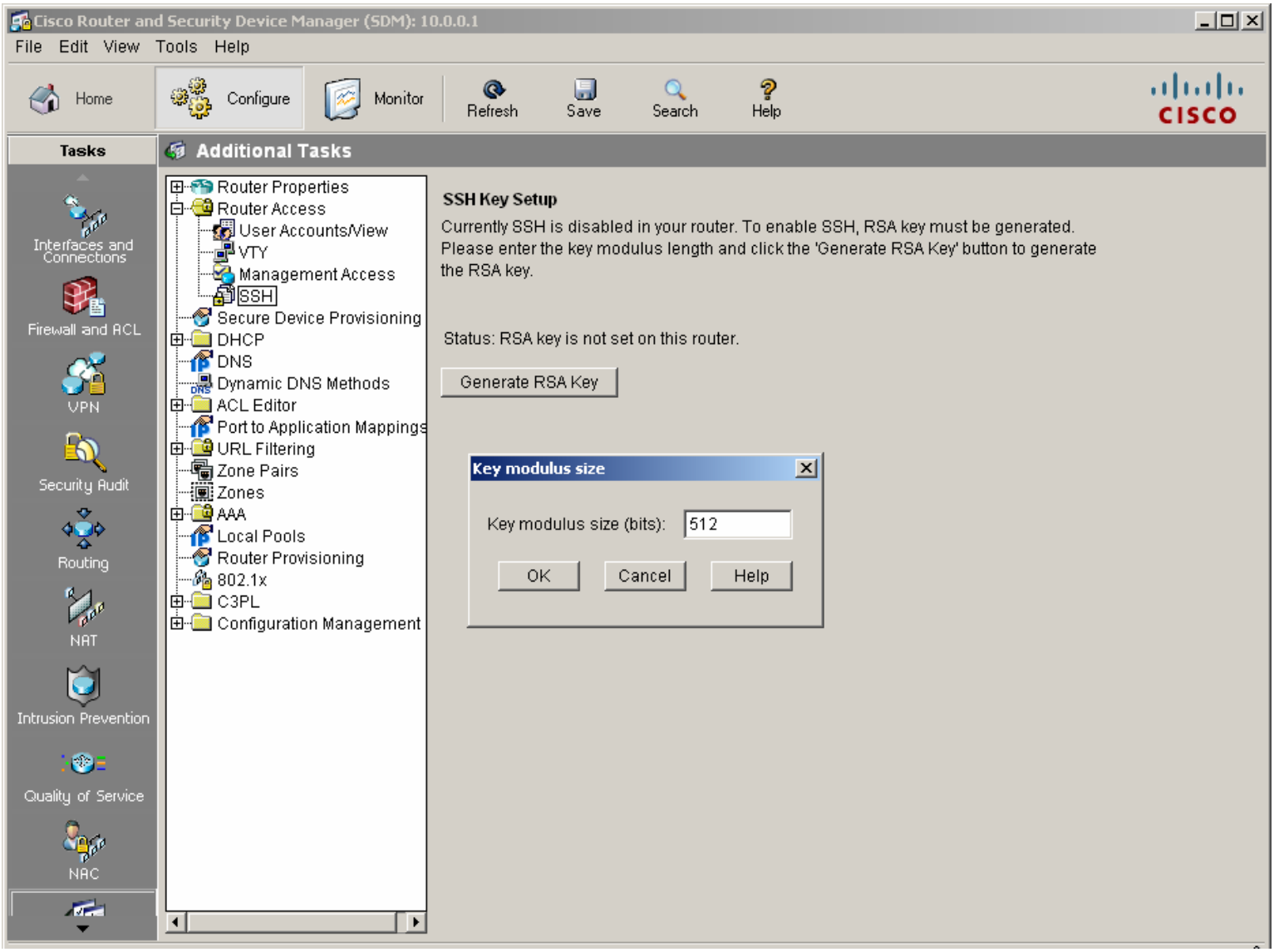
Click on Router Access and then click on SSH



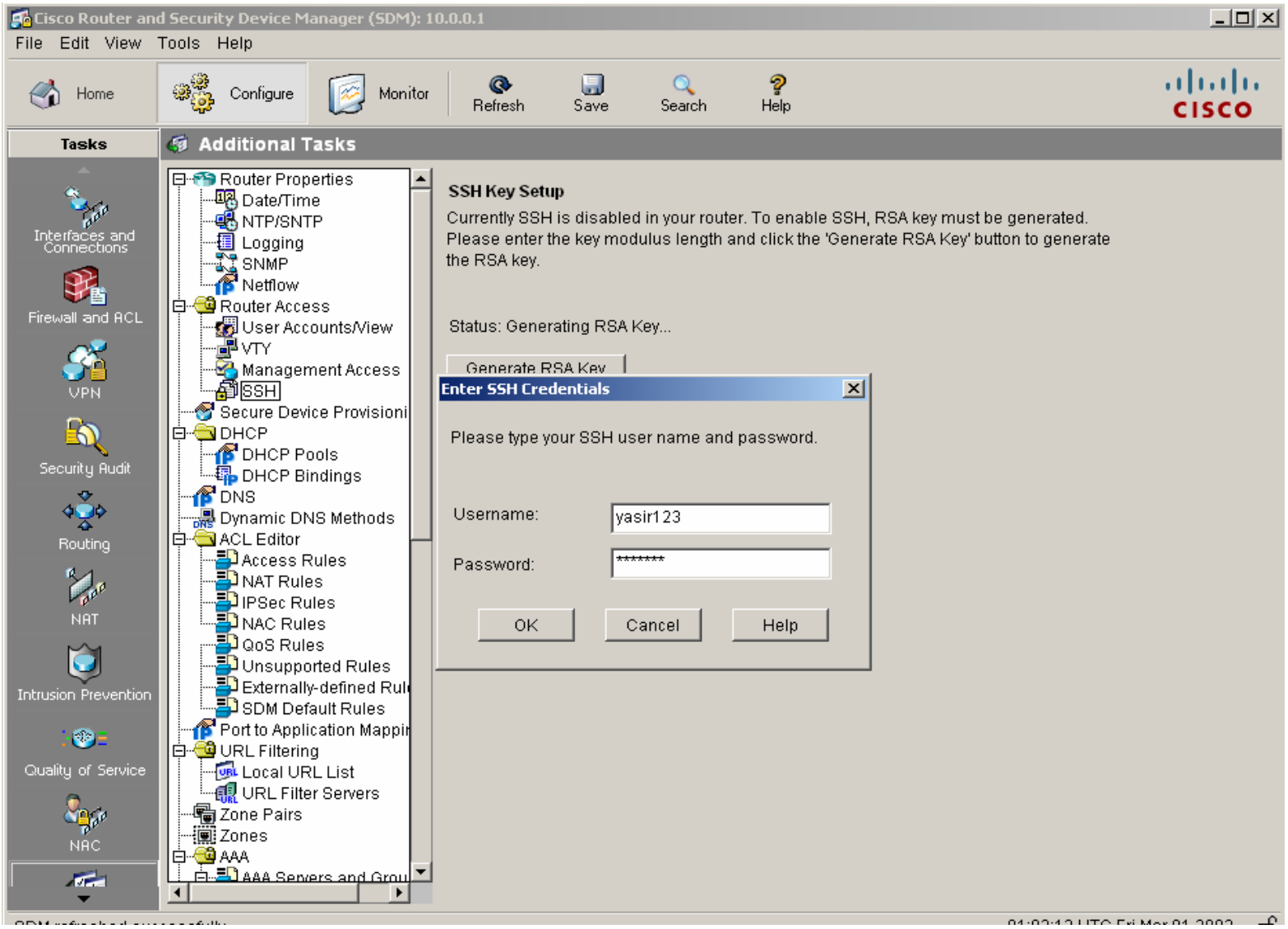
Click on Genrate RSA Key



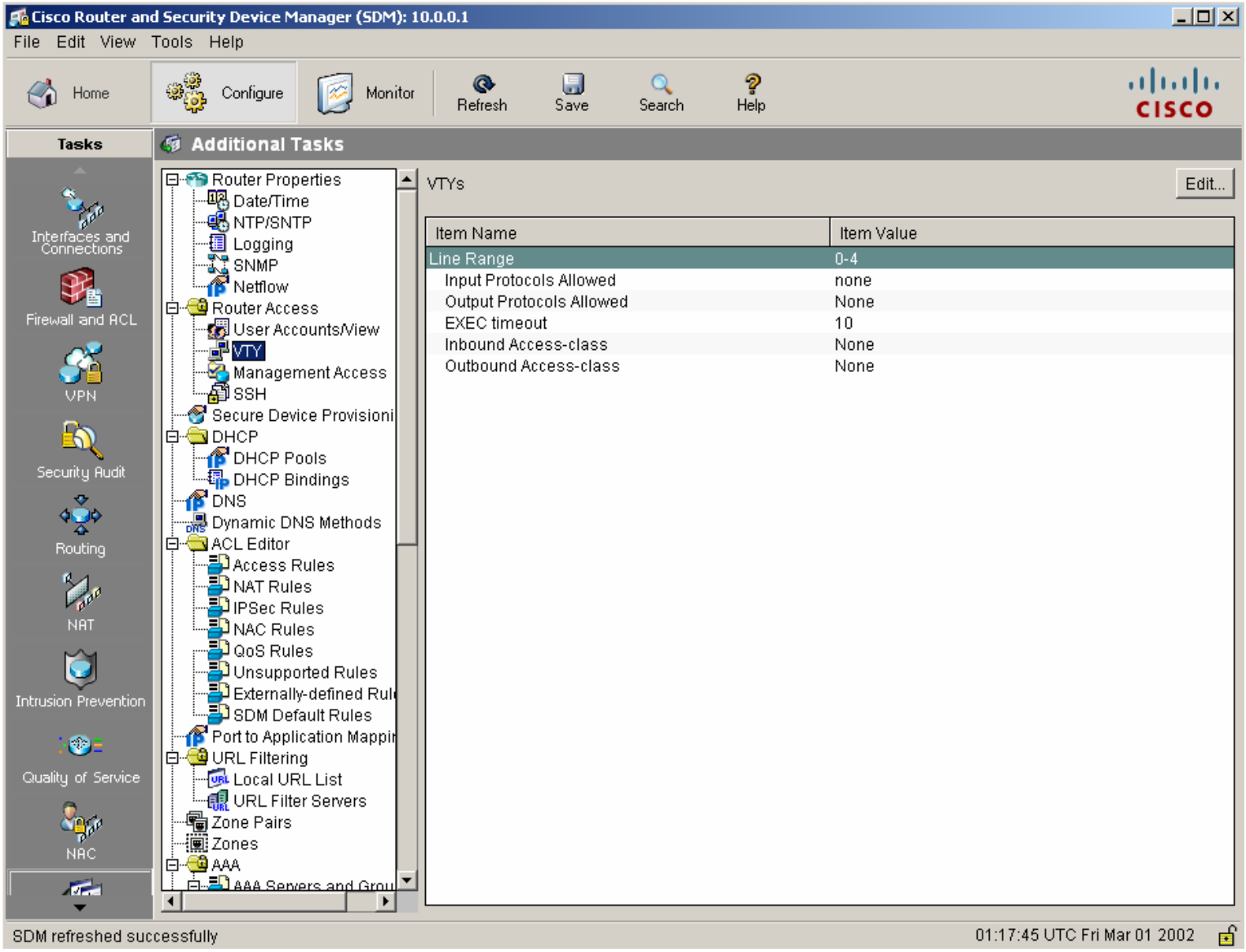
Enter Value of Key modules Size and Press ok



Enter Username and password for SSH

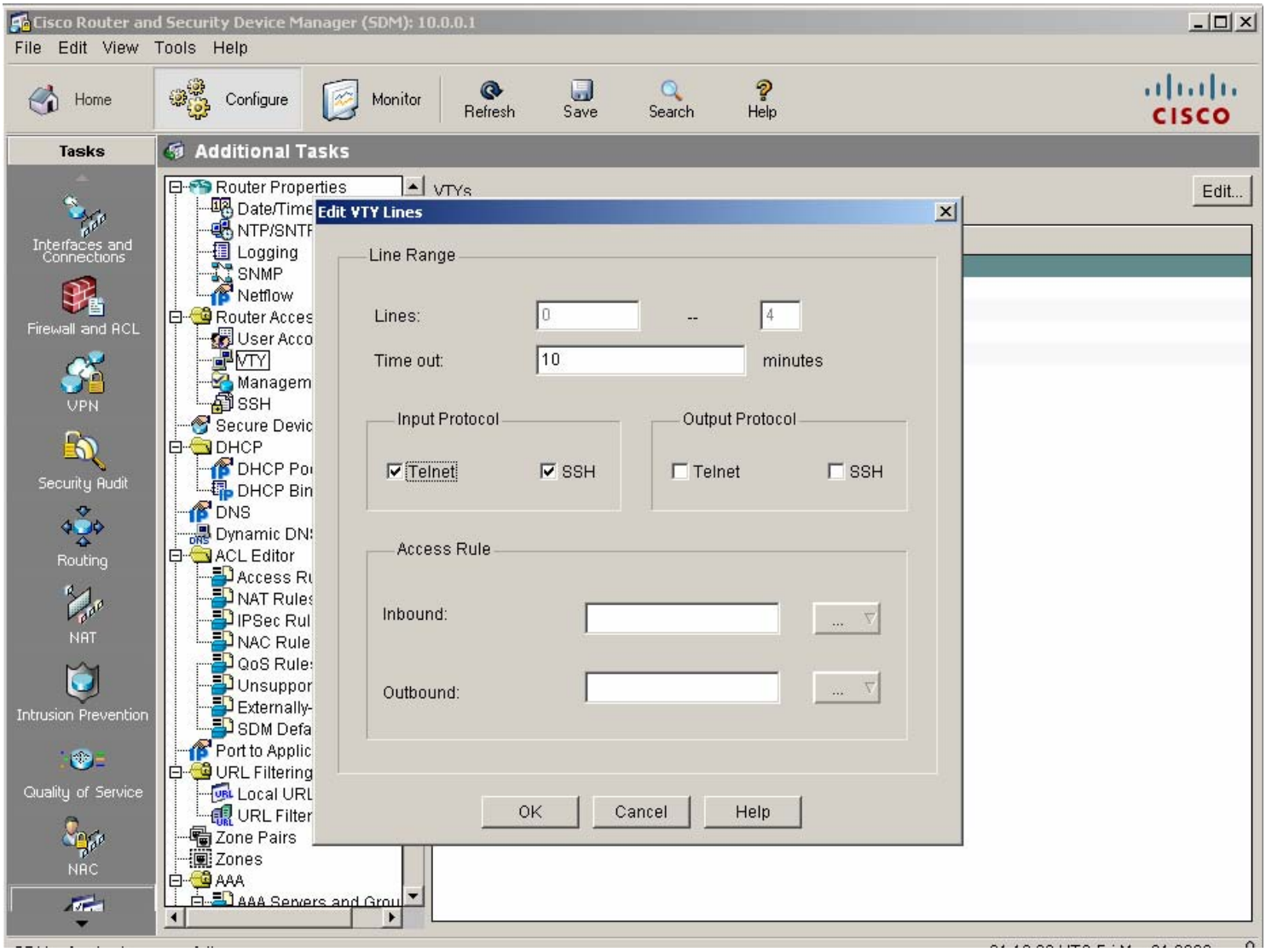


Then Click on VTY and Click on Edit

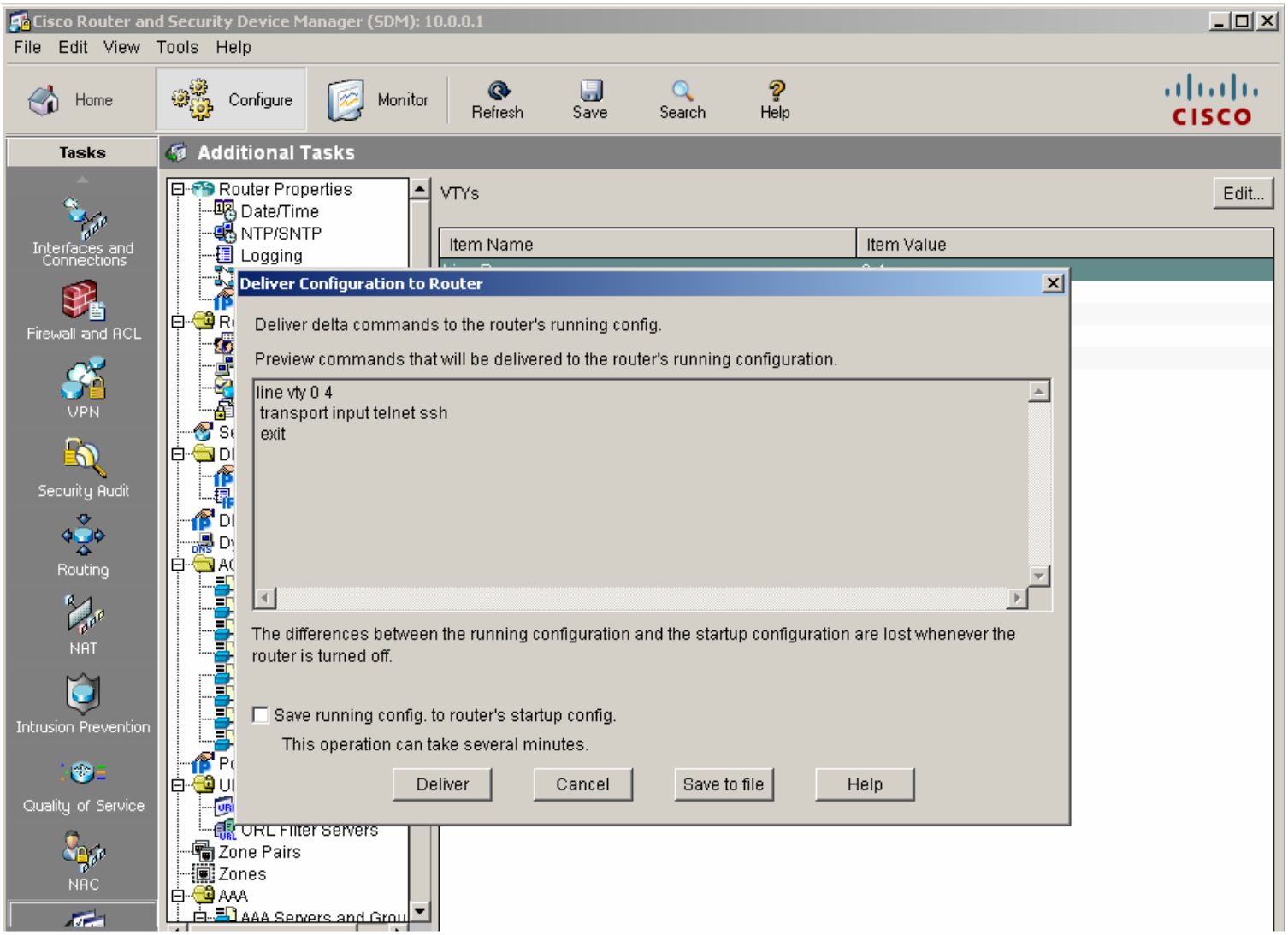


Set Line Range for virtual SSH and Telnet

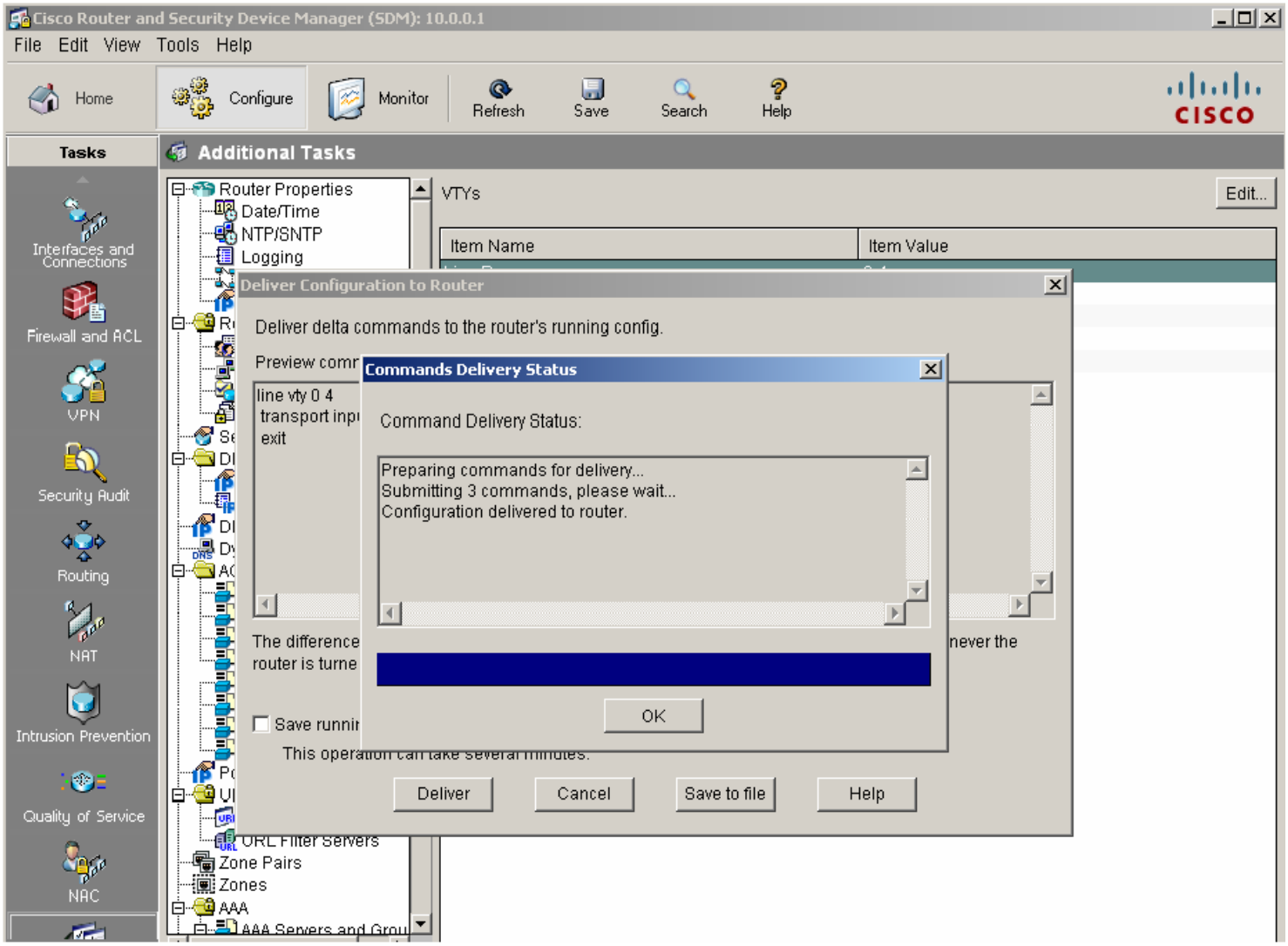
Click on ok



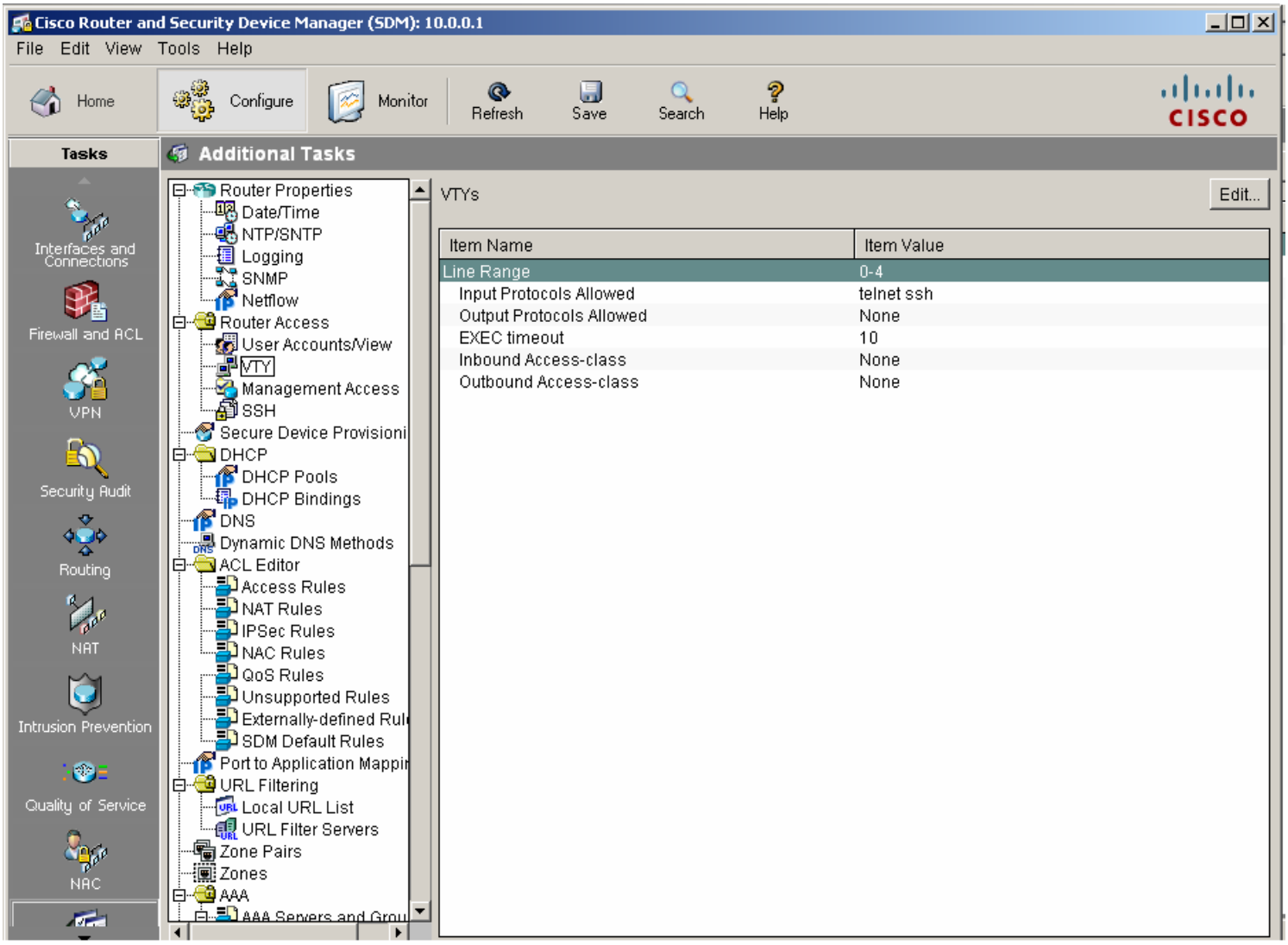
This command will be deliver on the Router and press Deliver Button


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Router Properties
Date/Time
NTP/SNTP
Logging
Zone Pairs
Zones
AAA
VTYs
Edit...
Item Name
Item Value
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview commands that will be delivered to the router's running configuration.
line vty 0 4
transport input telnet ssh
exit
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.
Save running config. to router's startup config.
This operation can take several minutes.
Deliver
Cancel
Save to file
Help

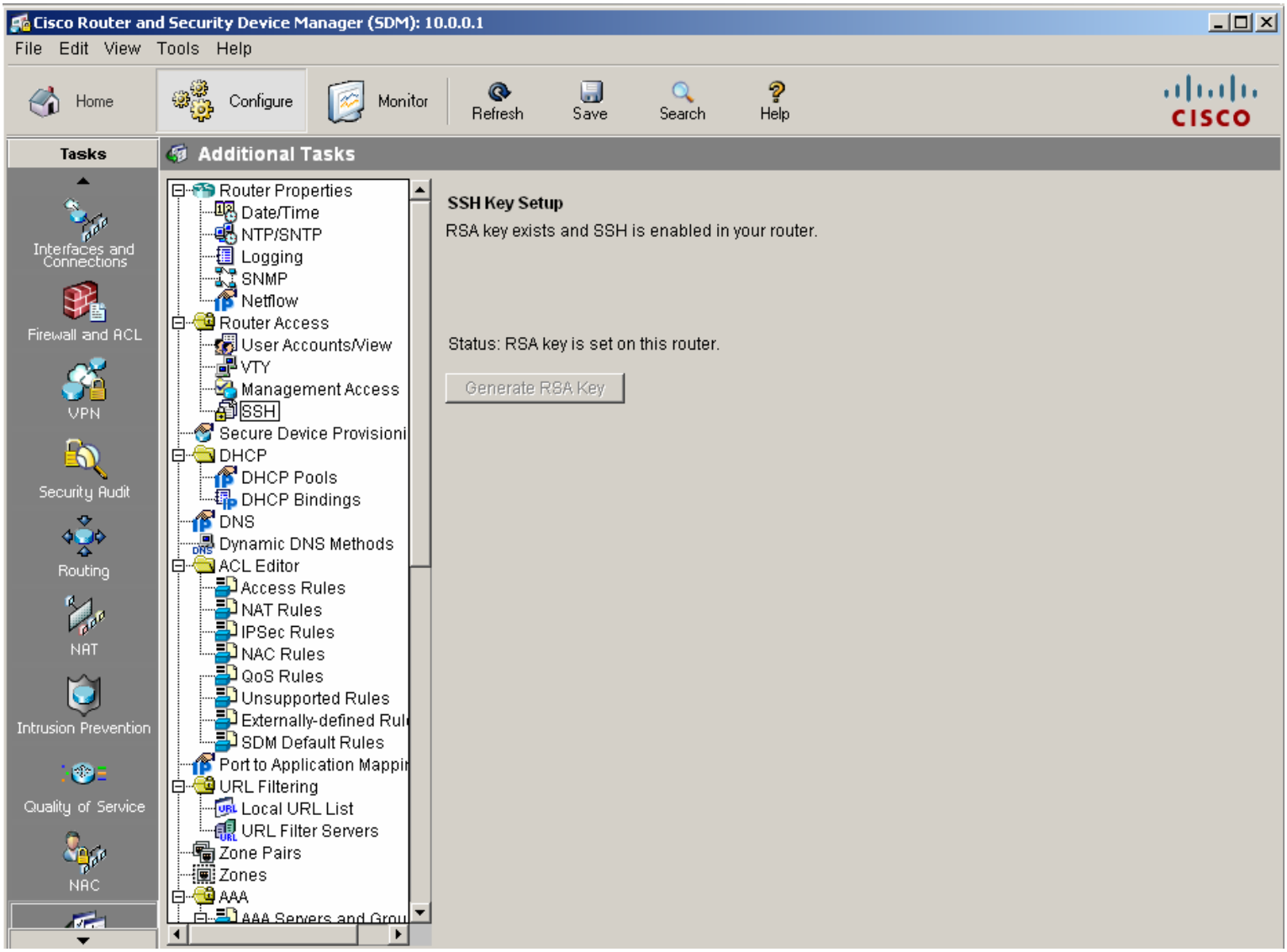
Click on ok



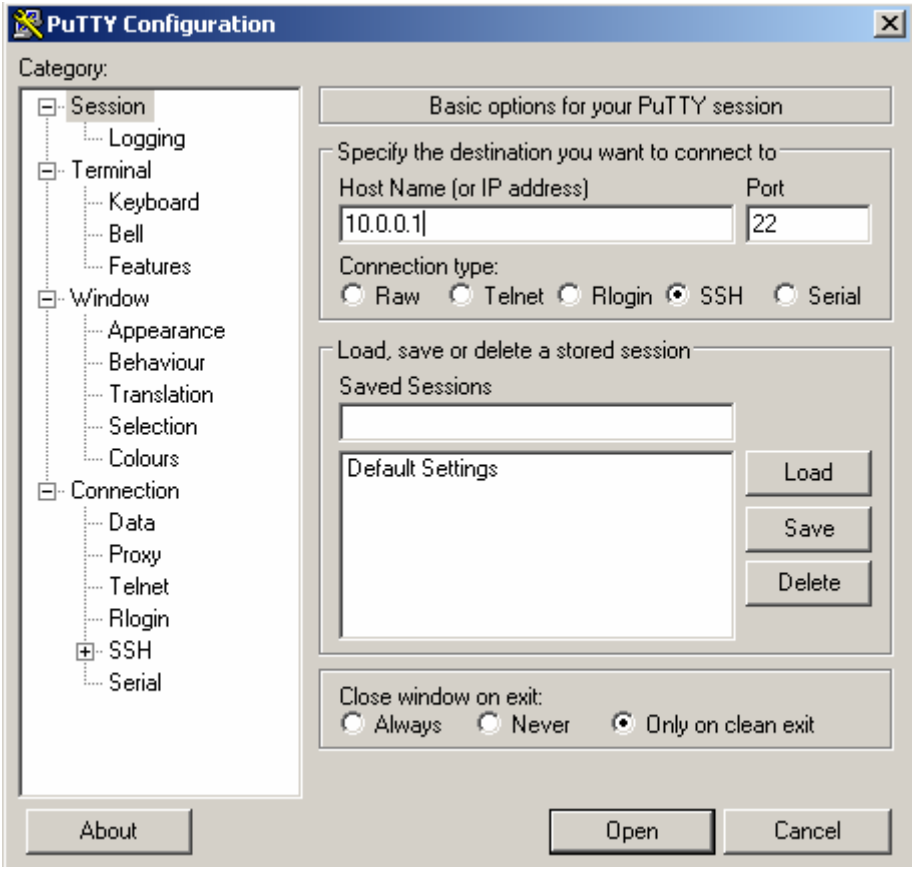
Virtual Lines are configure for telnet and ssh



Your RSA key is generate

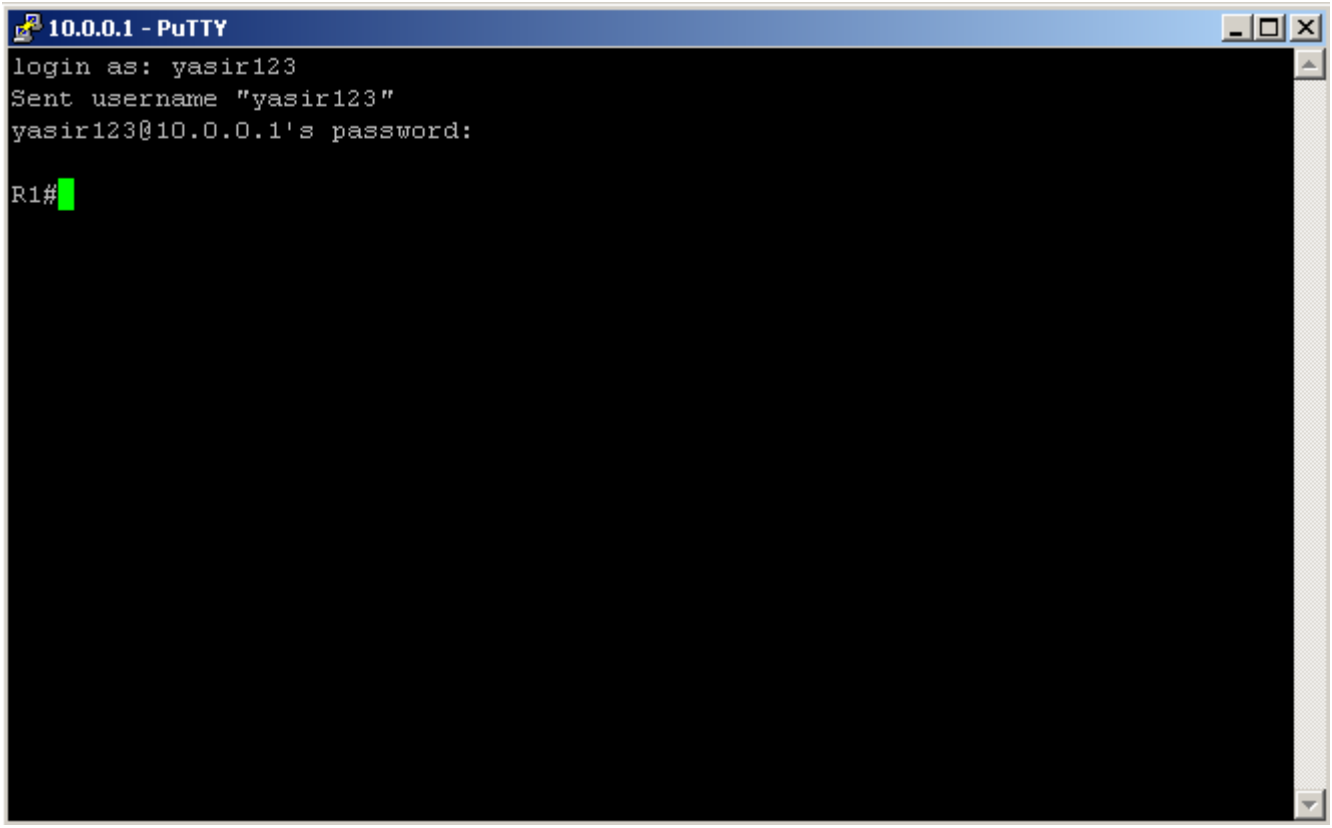


Verfiy you SSH from PC A with Putty software


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
10.0.0.1
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

Click on Yes

Enter Login name and password

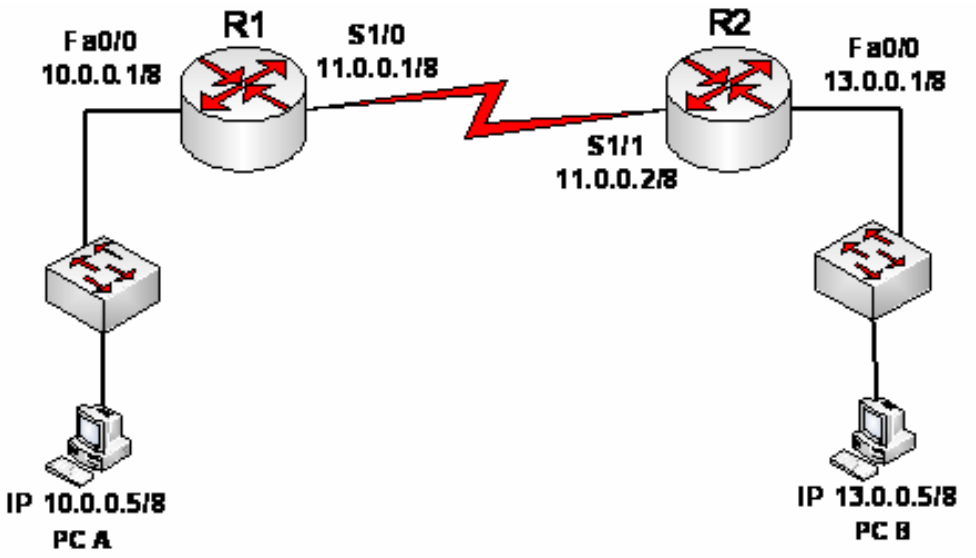


Configure Administrative Roles

Create multiple administrative roles or views on routers R1

Lab 2.

Enable Root View on R1



Step 1: Enable AAA on router R1.

To define views, AAA must be enabled.

```
R1#config t
R1(config)#aaa new-model
R1(config)#exit
```

Step 2: Enable the root view.

```
R1# enable view
Password: yasir123
```

```
*Dec 16 22:41:17.483: %PARSER-6-VIEW_SWITCH: successfully set to view
'root'.
```

Create New Views for the Admin1, Admin2, and Tech Roles on R1

Step 1: Create the admin1 view, establish a password, and assign privileges.

```
R1(config)#parser view admin1
R1(config-view)#
*Dec 16 22:45:27.587: %PARSER-6-VIEW_CREATED: view 'admin1'
successfully created.


R1(config-view)#secret yasir123
R1(config-view)#

R1(config-view)#commands exec include all show
R1(config-view)#commands exec include all config terminal
R1(config-view)#commands exec include all debug
R1(config-view)#end
```

Verify the admin1 view.

```
R1#enable view admin1
Password:yasir123

*Dec 16 22:56:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
'admin1'
R1#show parser view
Current view is 'admin1'
```

```
R1#?
Exec commands:
configure         Enter configuration mode
debug             Debugging functions (see also 'undebug')
enable            Turn on privileged commands
exit              Exit from the EXEC
show              Show running system information
```

```
R1#show ?
aaa               Show AAA values
accounting        Accounting data for active sessions
adjacency         Adjacent nodes
alignment         Show alignment information
appfw             Application Firewall information
archive           Archive of the running configuration information
arp               ARP table
```

2: Create the admin2 view, establish a password, and assign privileges.

```
R1#enable view
Password:yasir123
*Dec  1 00:05:50.239: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
```

```
R1(config)#parser view admin2
R1(config-view)#
*Dec 16 23:02:27.587: %PARSER-6-VIEW_CREATED: view 'admin2’

R1(config-view)#secret cttc123
R1(config-view)#
```

Verify the admin2

```
R1(config-view)#end

R1#enable view admin2
Password: cttc123
*Dec 16 23:05:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
'admin2'
R1#show parser view
R1# Current view is ‘admin2’
```

```
R1#?
Exec commands:
Enable       Turn on privileged commands
exit         Exit from the EXEC
show         Show running system information
```

```
R1#enable view
Password:yasir123

1 00:08:01.055: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.


R1(config)#parser view tech
R1(config-view)#
*Dec 16 23:10:27.587: %PARSER-6-VIEW_CREATED: view 'tech’ successfully created.


R1(config-view)#secret techpasswd
R1(config-view)#


R1(config-view)#commands exec include show version
R1(config-view)#commands exec include show interfaces
R1(config-view)#commands exec include show ip interface brief
R1(config-view)#commands exec include show parser view
```

Verify the tech view.

```
R1#enable view tech
Password:techpasswd
*Dec 16 23:13:46.971: %PARSER-6-VIEW_SWITCH: successfully set to view
```

```
'tech'

R1#show parser view

 1 00:09:25.211: %PARSER-6-VIEW_SWITCH: successfully set to view 'tech'.

R1#?
Exec commands:
enable      Turn on privileged commands
exit        Exit from the EXEC
show        Show running system information




R1#show ?
  flash:      display information about flash: file system
  interfaces  Interface status and configuration
  ip          IP information
  parser      Display parser information
  slot0:      display information about slot0: file system
  version     System hardware and software status
```

Create the ahmed superview, establish a password, and assign view

```
R13#enable view
Password:

R13#
*Mar  1 00:12:49.691: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.

R13#configure terminal
R13(config)#parser view ahmed superview

*Mar  1 00:13:28.915: %PARSER-6-SUPER_VIEW_CREATED: super view 'ahmed' successfully created.

R13(config-view)#secret ahmed123

R13(config-view)#view admin1
R13(config-view)#view admin

*Mar  1 00:14:24.851: %PARSER-6-SUPER_VIEW_EDIT_ADD: view admin1 added to superview ahmed.

R13(config-view)#view admin2
R13(config-view)#

*Mar  1 00:14:26.679: %PARSER-6-SUPER_VIEW_EDIT_ADD: view admin2 added to superview ahmed.

R13(config-view)#view tech
R13(config-view)#

*Mar  1 00:14:38.263: %PARSER-6-SUPER_VIEW_EDIT_ADD: view tech added to superview ahmed.
R13(config-view)#
```

R13#enable view ahmed
Password:

R13#
*Mar 1 00:16:11.851: %PARSER-6-VIEW_SWITCH: successfully set to view 'ahmed'.
R13#

R13#show parser view
Current view is 'ahmed'
R13#

R13#?
Exec commands:
  configure Enter configuration mode
  enable   Turn on privileged commands
  exit   Exit from the EXEC
  show   Show running system information

R13#

R13#show ?
  aaa   Show AAA values
  access-expression   List access expression
  access-lists   List access lists
  accounting   Accounting data for active sessions
  adjacency   Adjacent nodes
  alarm-interface   Display information about a specific Alarm
                         Interface Card
  aliases   Display alias commands
  alignment   Show alignment information
  appfw   Application Firewall information
  archive   Archive of the running configuration information
  arp   ARP table
  async   Information on terminal lines used as router
                         interfaces
  auto   Show Automation Template
  backhaul-session-manager Backhaul Session Manager information
  backup   Backup status
  bcm560x   BCM560x HW Table
  bridge   Bridge Forwarding/Filtering Database [verbose]
  buffers   Buffer pool statistics
  call   Show call
  caller   Display information about dialup connections
 --More—

R13(config)#?
Configure commands:
  aaa   Authentication, Authorization and Accounting.
  access-list   Add an access list entry
  alarm-interface   Configure a specific Alarm Interface Card
  alias   Create command alias
  appfw   Configure the Application Firewall policy
  archive   Archive the configuration

```
 arp                     Set a static ARP entry
 async-bootp             Modify system bootp parameters
 backhaul-session-manager  Configure Backhaul Session Manager
 banner                  Define a login banner
 bba-group               Configure BBA Group
 boot                    Modify system boot parameters
 bridge                  Bridge Group.
 buffers                 Adjust system buffer pool parameters
 busy-message            Display message when connection to host fails
 call                    Configure Call parameters
 call-history-mib        Define call history mib parameters
 carrier-id              Name of the carrier associated with this trunk
                        group
 cdp                     Global CDP configuration subcommands
 chat-script             Define a modem chat script
--More--


R13#enable
Password:
R13#
```

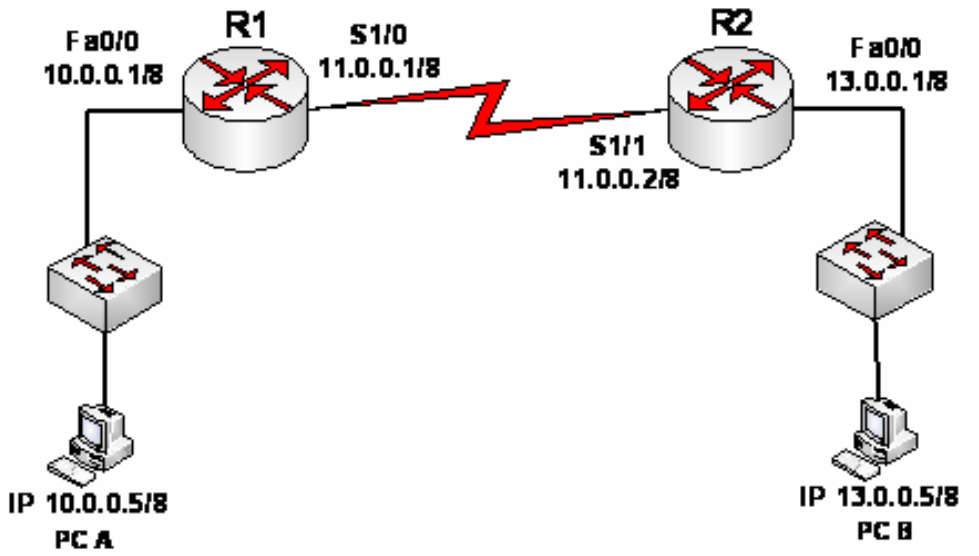
```
R13#sh running-config
Building configuration...

Current configuration : 2936 bytes
!
version 12.4
no service password-encryption
!
hostname R1
!
!
enable secret 5 $1$oHAV$/Ur1rGf5lgStRFgeAcL7g1
!
aaa new-model
!
!
ip cef
!
!
no ip domain lookup
!
!
!
username yasir privilege 15 password 0 cisco
!
!

!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 11.0.0.1 255.255.255.0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
control-plane
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 3
line vty 0 4
!
parser view admin1
 secret 5 $1$ZXjU$BijAXGbBC7vGG6n.HyaNK1
 commands exec include all configure terminal
 commands exec include configure
 commands exec include all show
!
parser view admin2
 secret 5 $1$5PxG$6gIUYP5VOcvQG8XlnL4ul0
!
parser view tech
 secret 5 $1$Vz3X$x2jZcC810b94vOnhylB.V.
 commands exec include show ip interface brief
 commands exec include show ip interface
 commands exec include show ip
 commands exec include show version
 commands exec include show parser view
 commands exec include show parser
 commands exec include show interfaces
 commands exec include show
!
parser view ahmed superview
 secret 5 $1$cn/J$Pz5RSAxvANAhRGDohVwDm0
 view admin1
```

```
 view admin2
 view tech
!
!
!
end

R13#
```

LAB # 3

Configure syslog Support on R1 and PC-A



Step 1: Install the syslog server.

Step 2: Configure R1 to log messages to the syslog server using the CLI.

```
R1(config)#logging 10.0.0.5
```

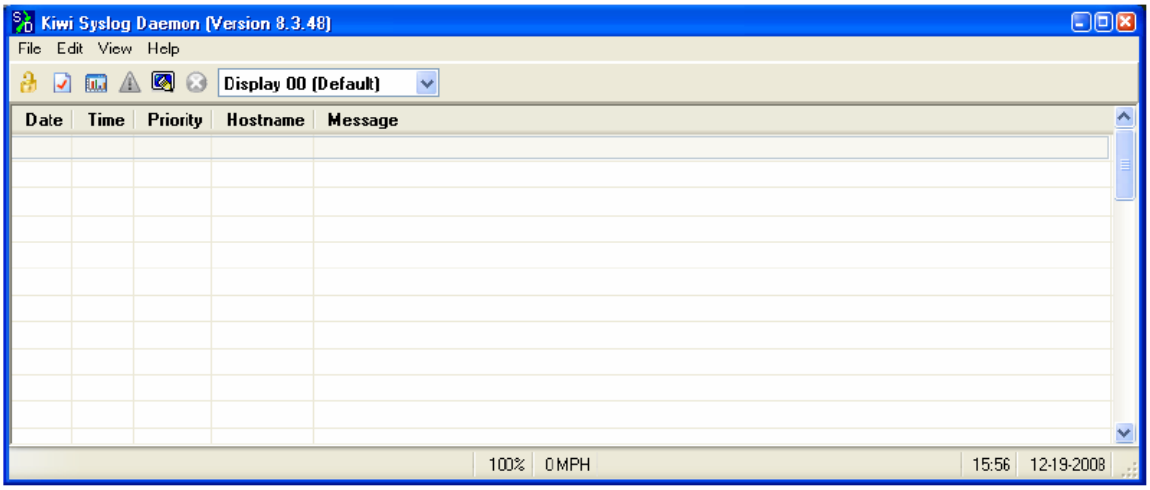
Step 3: Configure the logging severity level on R1.

```
R1(config)#logging trap ?

<0-7>  Logging severity level
alerts           Immediate action needed           (severity=1)
critical         Critical conditions               (severity=2)
```

```
debugging         Debugging messages                (severity=7)
emergencies       System is unusable                (severity=0)
errors            Error conditions                  (severity=3)
informational     Informational messages            (severity=6)
notifications     Normal but significant conditions (severity=5)
warnings          Warning conditions                (severity=4)


R1(config)#logging trap warnings


R1#show logging
Syslog logging: enabled (0 messages dropped, 1 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering
disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 271 messages logged, xml
disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: disabled, xml disabled,
filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level warnings, 0 message lines logged
Logging to 192.168.1.3 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
0 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
```

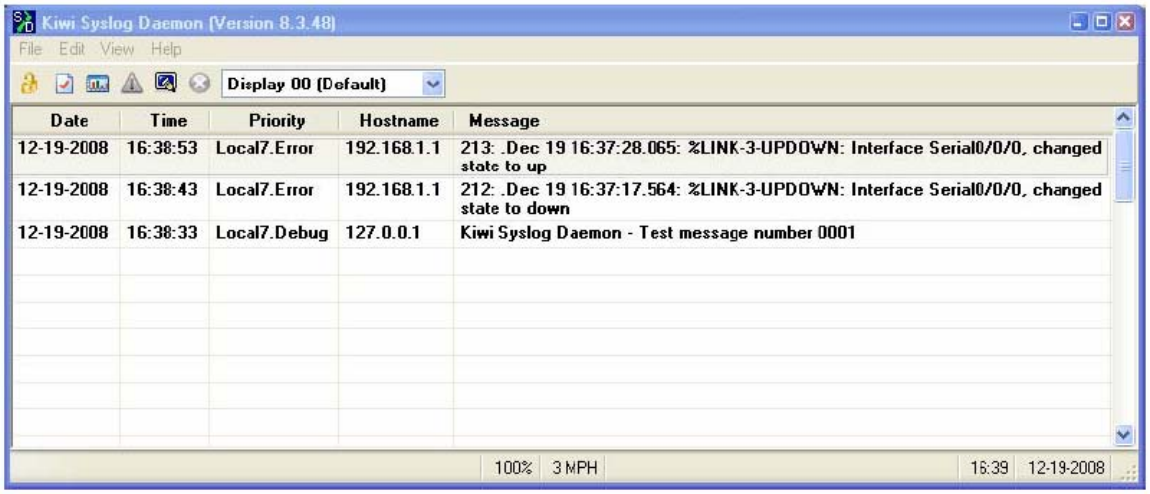
Step 6: Start the Kiwi Syslog Server.

Open the Kiki Syslog Daemon application on your desktop or click the **Start** button and select **Programs > Kiwi Enterprises > Kiwi Syslog Daemon**.



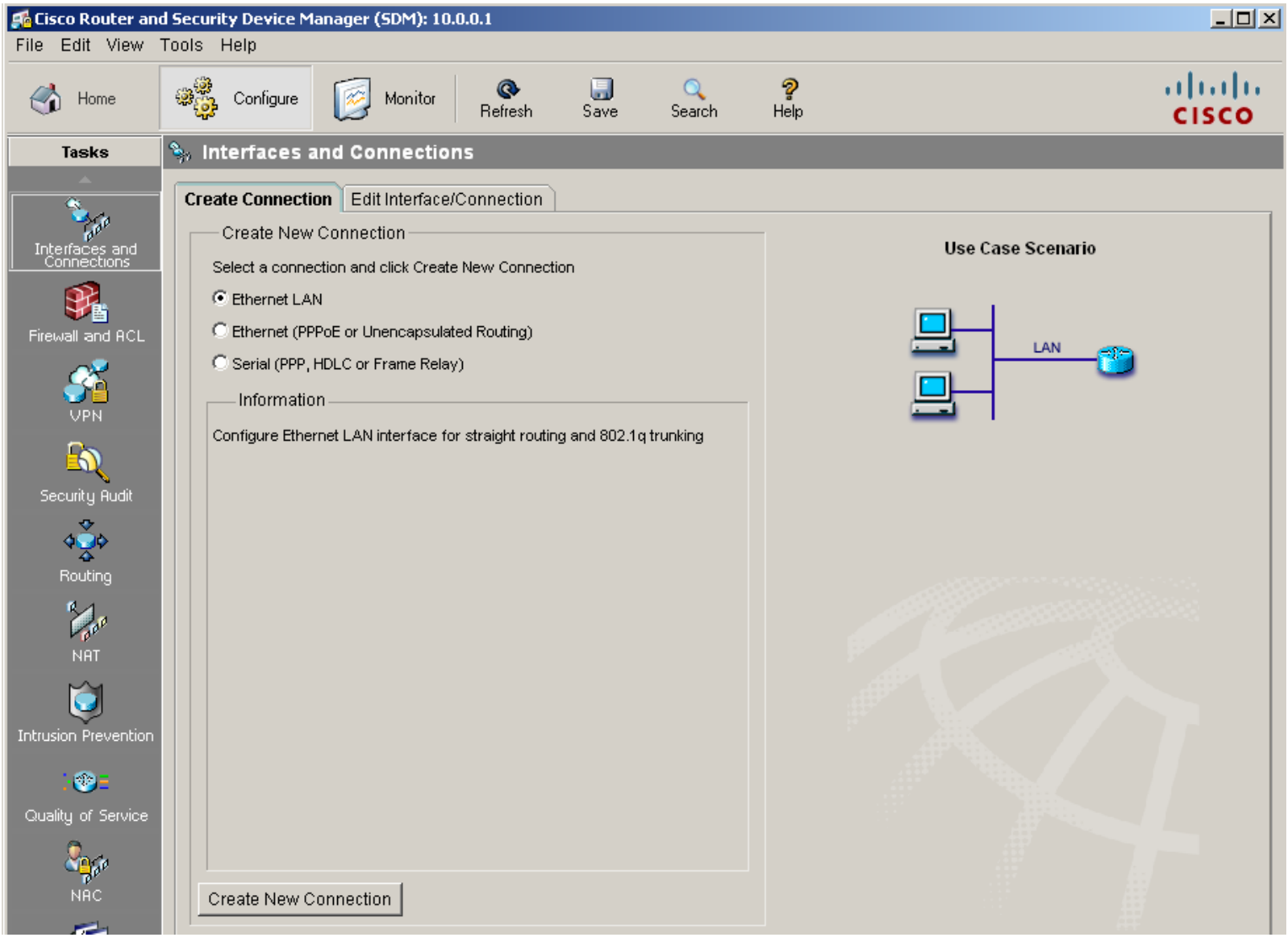
Verify that logging to the syslog server is occurring.

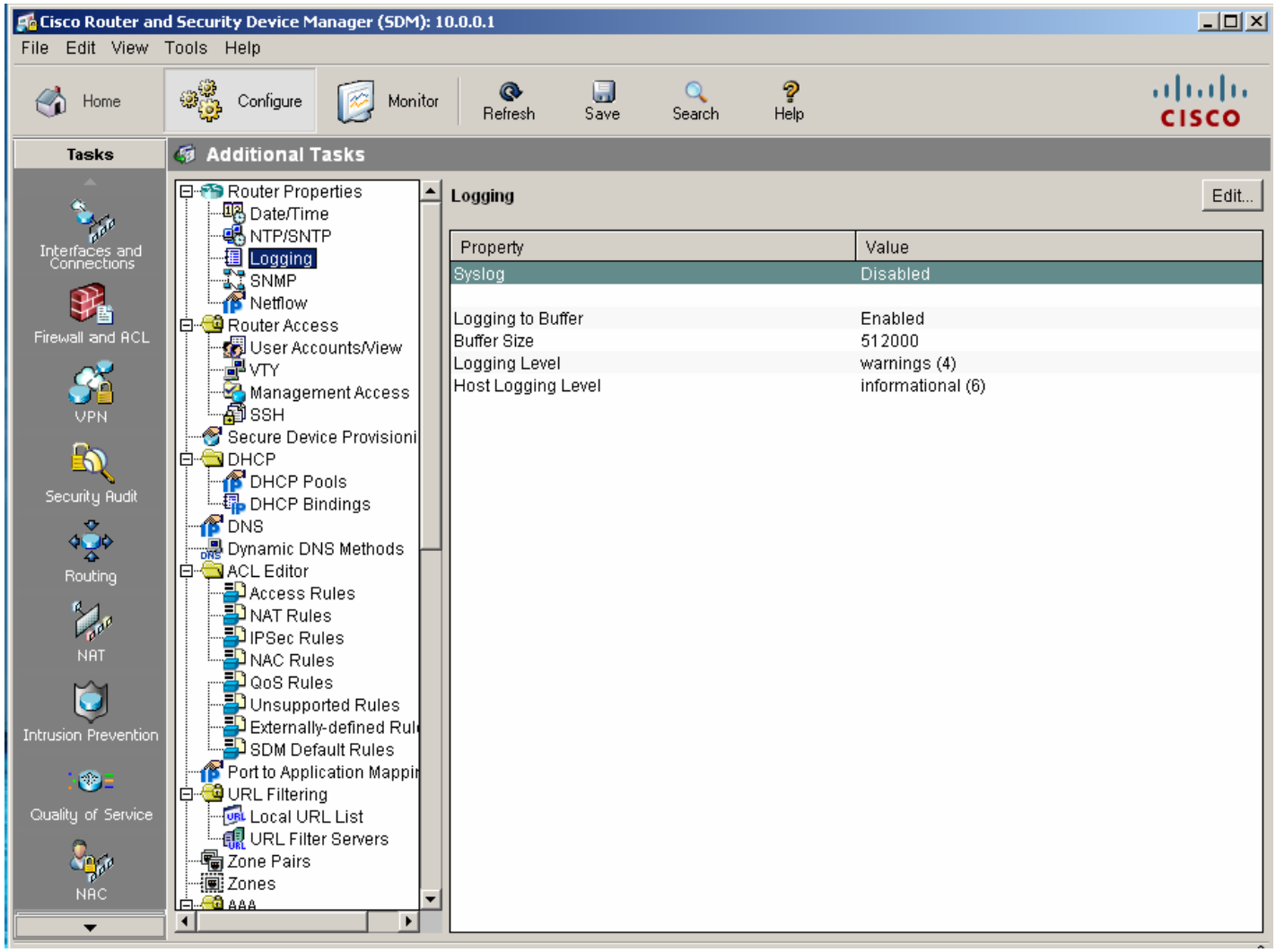
```
R1(config)#interface S0/0/0
R1(config-if)#shutdown
R1(config-if)#no shutdown
```

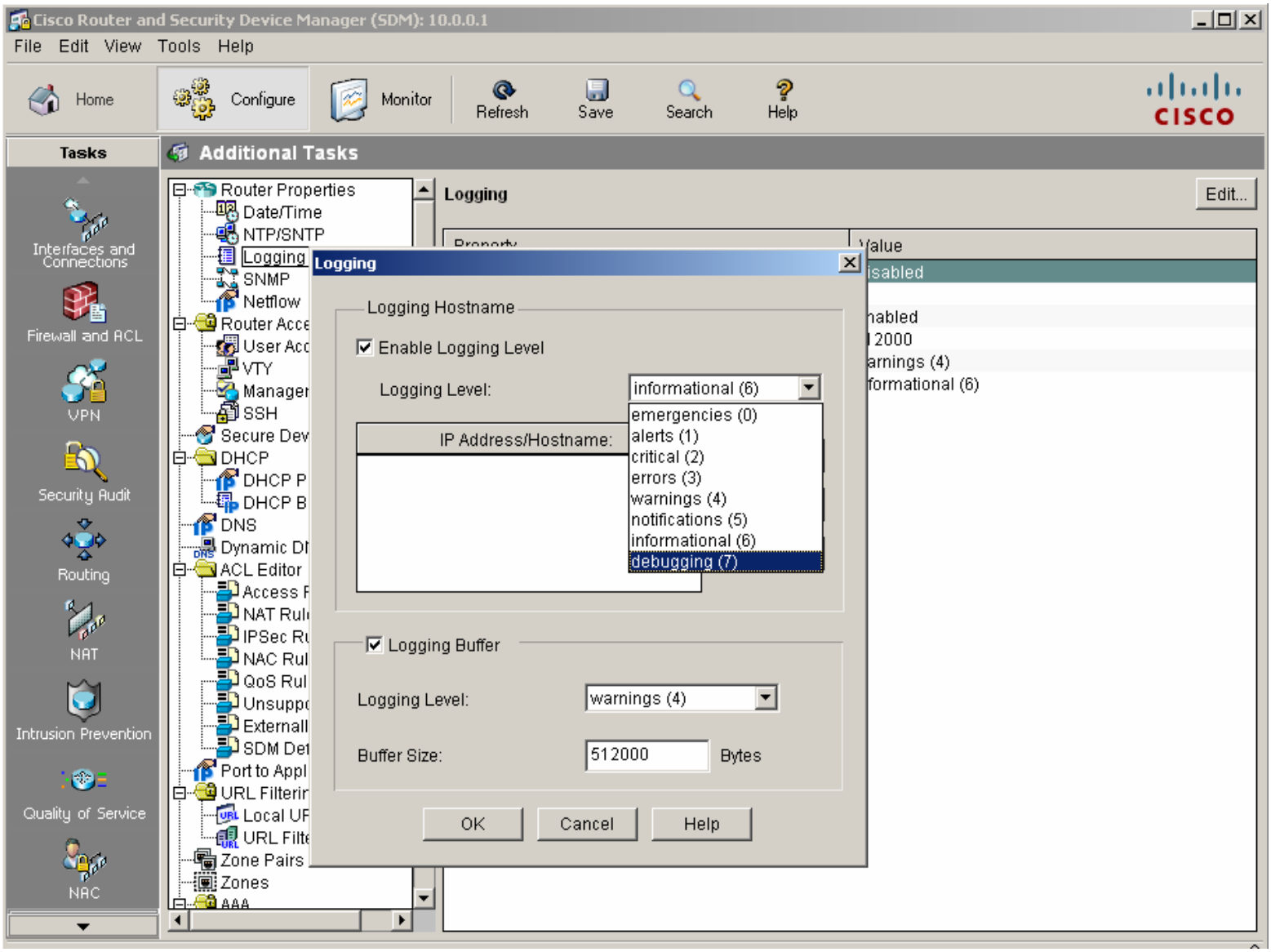


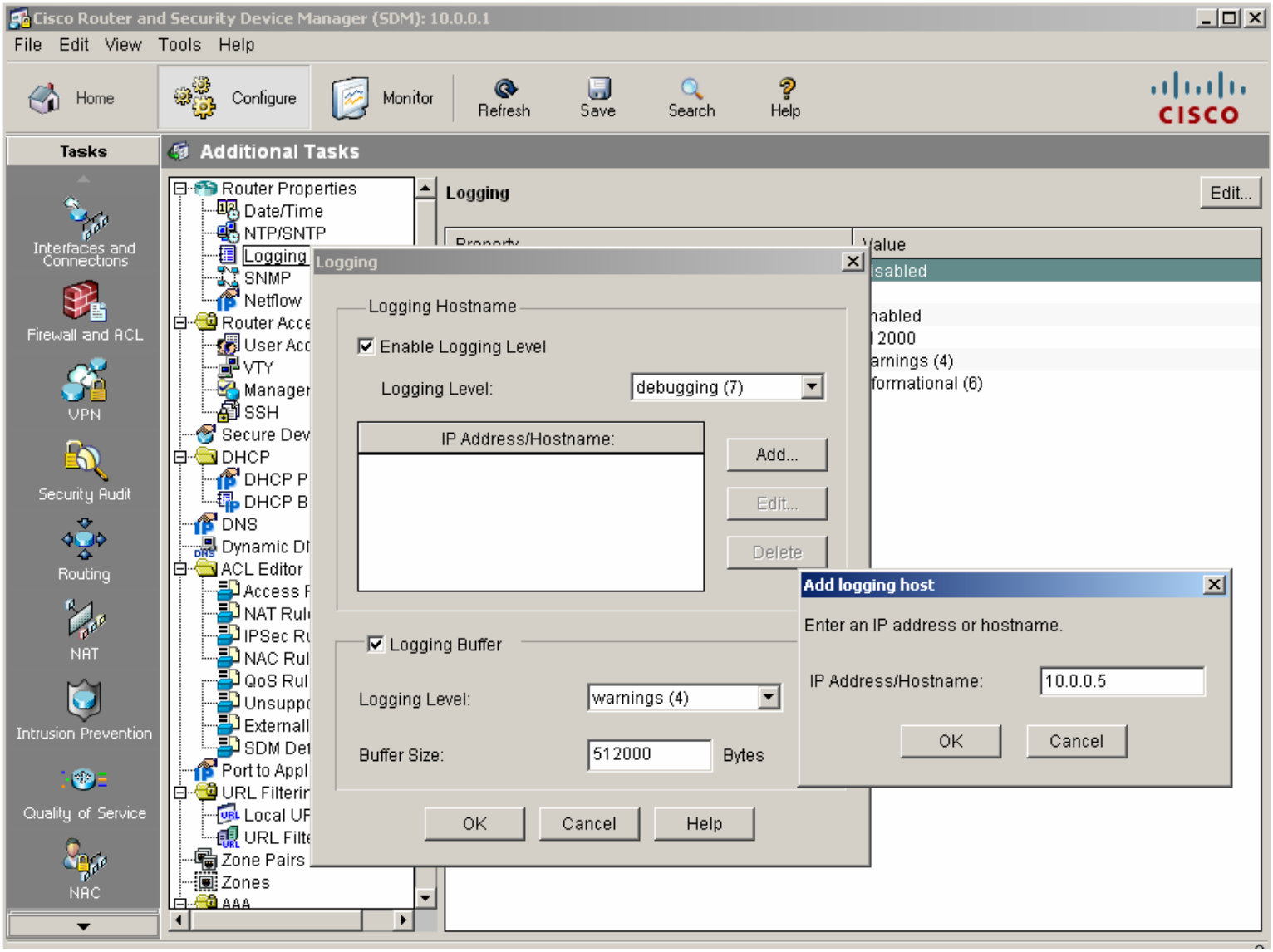
LAB # 4

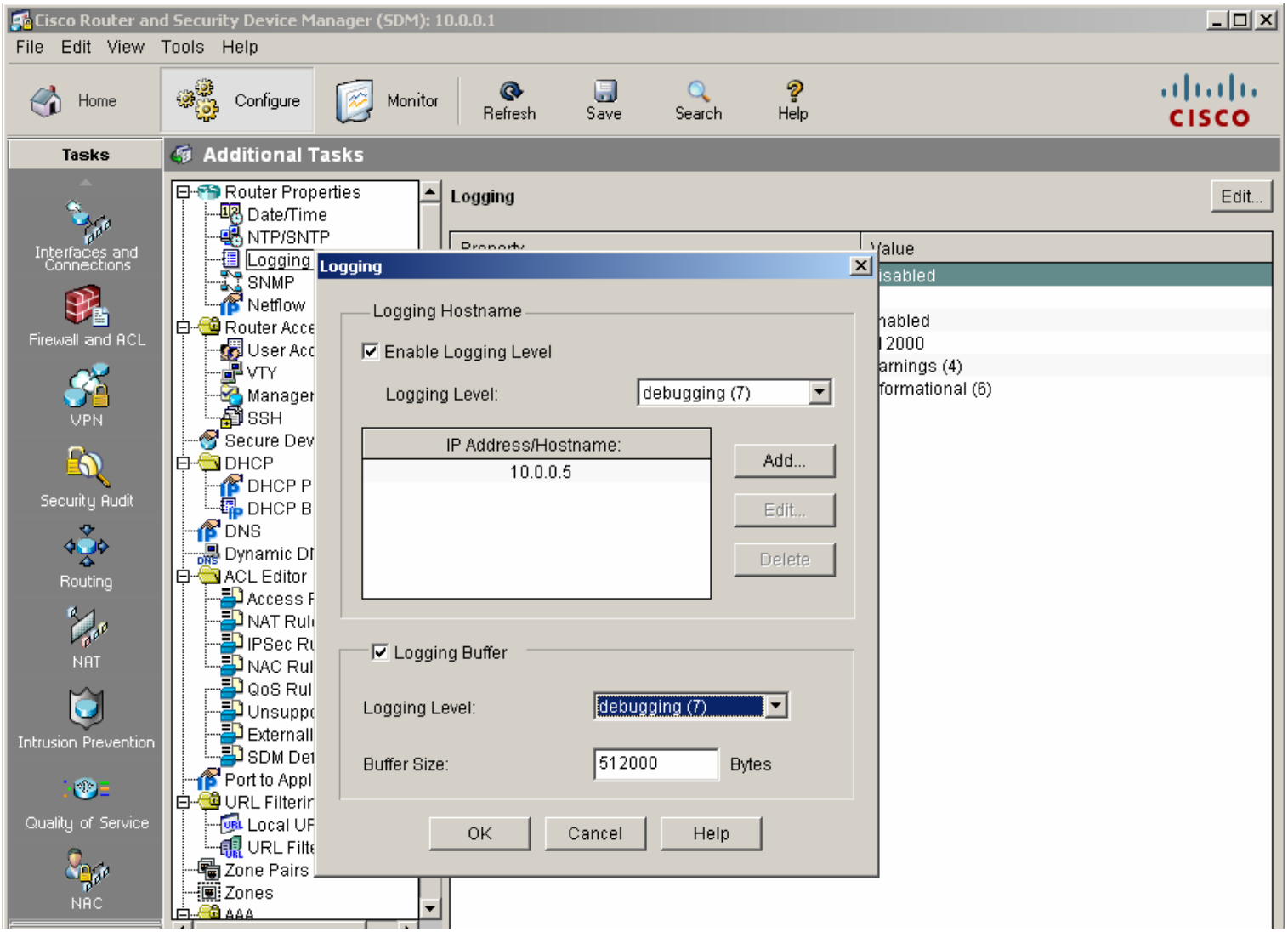
Configure Syslog with SDM

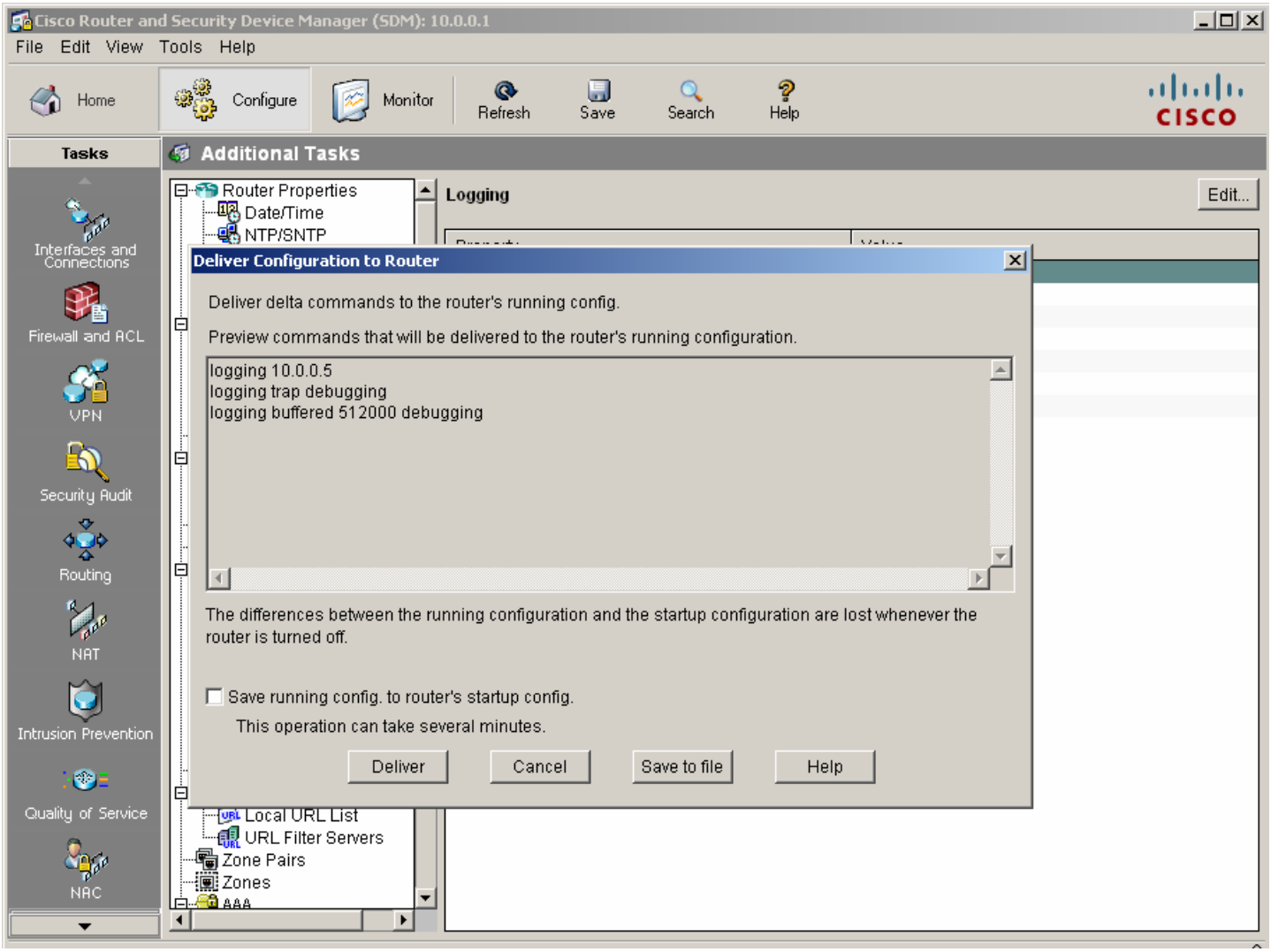


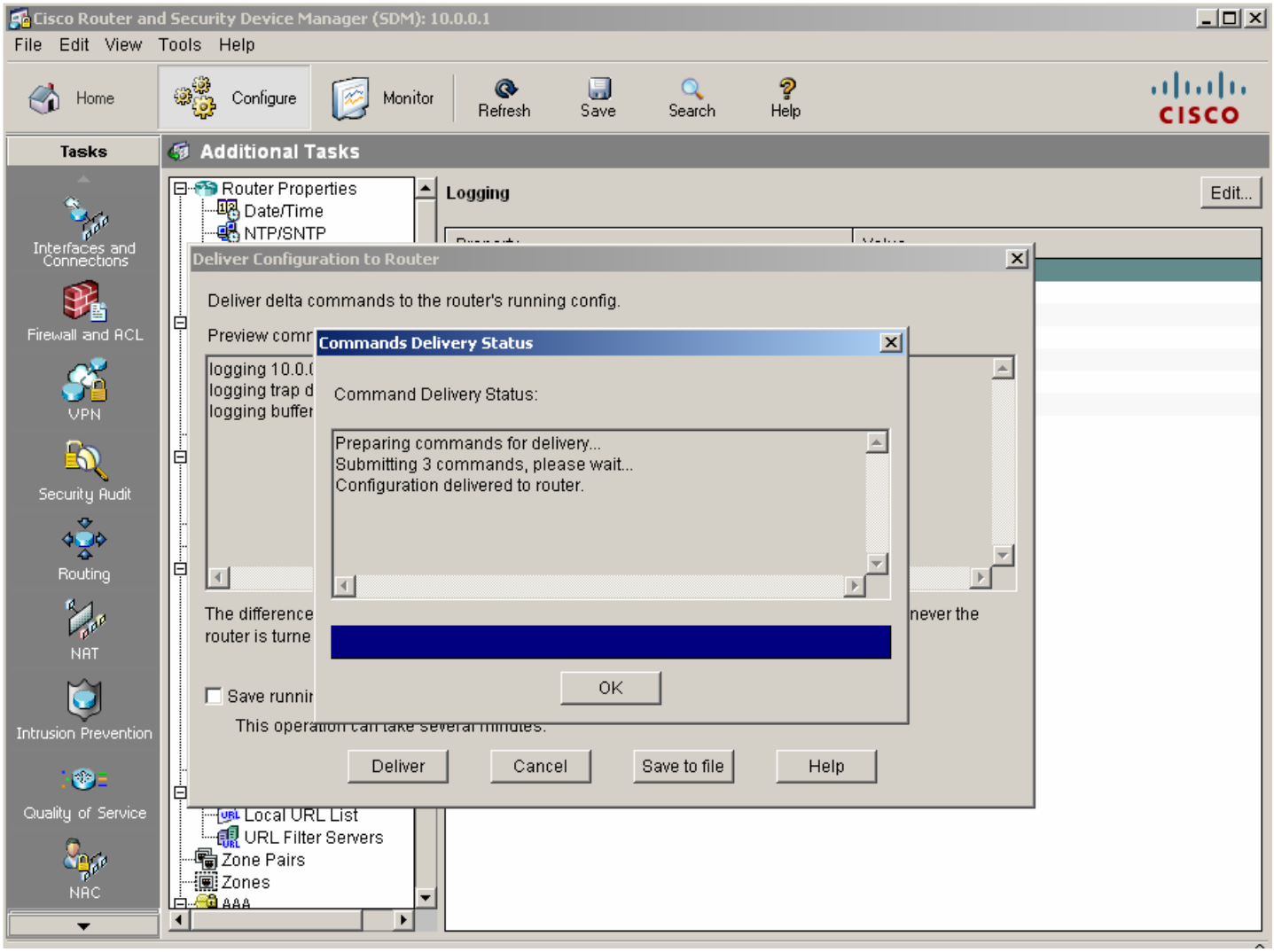

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Router Properties
Date/Time
NTP/SNTP
Logging
SNMP
Netflow
Router Access
User Accounts/View
VTY
Management Access
SSH
Secure Device Provisioni
DHCP
DHCP Pools
DHCP Bindings
DNS
Dynamic DNS Methods
ACL Editor
Access Rules
NAT Rules
IPSec Rules
NAC Rules
QoS Rules
Unsupported Rules
Externally-defined Rul
SDM Default Rules
Port to Application Mappi
URL Filtering
Local URL List
URL Filter Servers
Zone Pairs
Zones
AAA
Logging
Edit...
Property
Value
Syslog
Disabled
Logging to Buffer
Enabled
Buffer Size
512000
Logging Level
warnings (4)
Host Logging Level
informational (6)

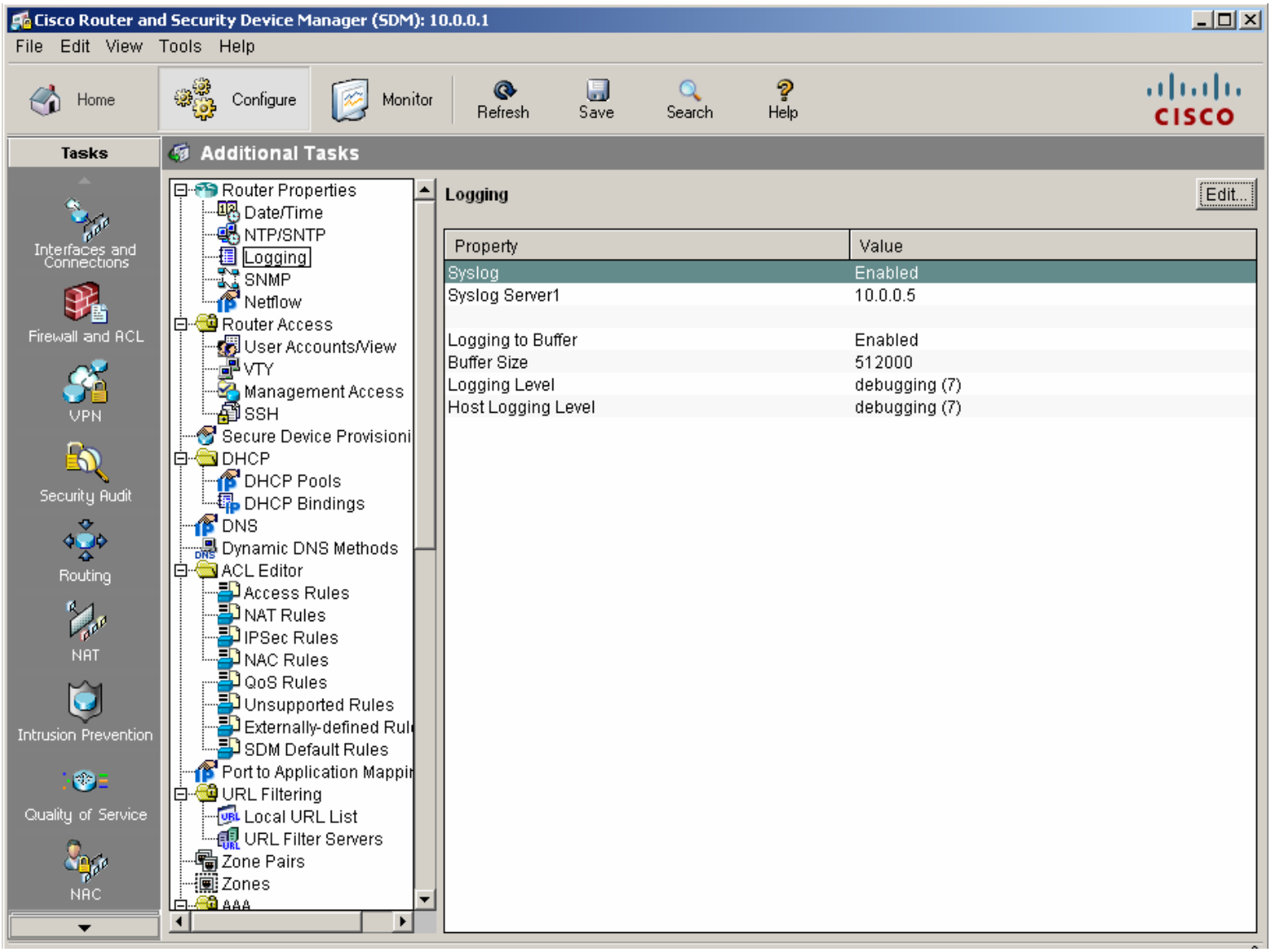

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Router Properties
Date/Time
NTP/SNTP
Logging
SNMP
Netflow
Router Acce
User Acc
VTY
Manager
SSH
Secure Dev
DHCP
DHCP P
DHCP B
DNS
Dynamic DI
ACL Editor
Access F
NAT Rul
IPSec Ru
NAC Rul
QoS Rul
Unsuppo
Externall
SDM Def
Port to Appl
URL Filterir
Local UF
URL Filte
Zone Pairs
Zones
AAA
Logging
Edit...
Value
isabled
nabled
2000
arnings (4)
formational (6)
Logging
Logging Hostname
Enable Logging Level
Logging Level:
informational (6)
emergencies (0)
alerts (1)
critical (2)
errors (3)
warnings (4)
notifications (5)
informational (6)
debugging (7)
IP Address/Hostname:
Logging Buffer
Logging Level:
warnings (4)
Buffer Size:
512000
Bytes
OK
Cancel
Help


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Router Properties
Date/Time
NTP/SNTP
Logging
SNMP
Netflow
Router Acce
User Acc
VTY
Manager
SSH
Secure Dev
DHCP
DHCP P
DHCP B
DNS
Dynamic DI
ACL Editor
Access F
NAT Rul
IPSec Ru
NAC Rul
QoS Rul
Unsuppo
External
SDM Def
Port to Appl
URL Filterir
Local UF
URL Filte
Zone Pairs
Zones
AAA
Logging
Edit...
Value
isabled
nabled
2000
arnings (4)
formational (6)
Logging
Logging Hostname
Enable Logging Level
Logging Level:
debugging (7)
IP Address/Hostname:
Add...
Edit...
Delete
Logging Buffer
Logging Level:
warnings (4)
Buffer Size:
512000
Bytes
OK
Cancel
Help
Add logging host
Enter an IP address or hostname.
IP Address/Hostname:
10.0.0.5
OK
Cancel


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Additional Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Router Properties
Date/Time
NTP/SNTP
Logging
SNMP
Netflow
Router Acce
User Acc
VTY
Manager
SSH
Secure Dev
DHCP
DHCP P
DHCP B
DNS
Dynamic Df
ACL Editor
Access F
NAT Rul
IPSec Ru
NAC Rul
QoS Rul
Unsuppo
External
SDM Def
Port to Appl
URL Filterir
Local UF
URL Filte
Zone Pairs
Zones
AAA
Logging
Edit...
Value
isabled
nabled
2000
arnings (4)
formational (6)
Logging
Logging Hostname
Enable Logging Level
Logging Level:
debugging (7)
IP Address/Hostname:
10.0.0.5
Add...
Edit...
Delete
Logging Buffer
Logging Level:
debugging (7)
Buffer Size:
512000
Bytes
OK
Cancel
Help

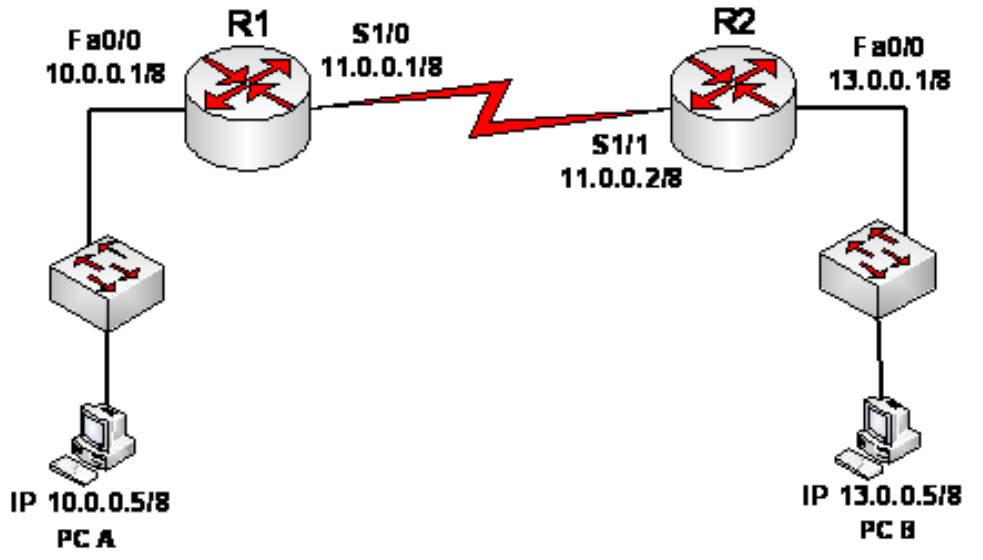

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Router Properties
Date/Time
NTP/SNTP
Local URL List
URL Filter Servers
Zone Pairs
Zones
AAA
Logging
Edit...
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview commands that will be delivered to the router's running configuration.
logging 10.0.0.5
logging trap debugging
logging buffered 512000 debugging
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.
Save running config. to router's startup config.
This operation can take several minutes.
Deliver
Cancel
Save to file
Help


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Router Properties
Date/Time
NTP/SNTP
Logging
Edit...
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview comm
logging 10.0.0
logging trap d
logging buffer
Commands Delivery Status
Command Delivery Status:
Preparing commands for delivery...
Submitting 3 commands, please wait...
Configuration delivered to router.
OK
The difference
router is turne
never the
Save runnir
This operation can take several minutes.
Deliver
Cancel
Save to file
Help
Local URL List
URL Filter Servers
Zone Pairs
Zones
AAA


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Router Properties
Date/Time
NTP/SNTP
Logging
SNMP
Netflow
Router Access
User Accounts/View
VTY
Management Access
SSH
Secure Device Provisioni
DHCP
DHCP Pools
DHCP Bindings
DNS
Dynamic DNS Methods
ACL Editor
Access Rules
NAT Rules
IPSec Rules
NAC Rules
QoS Rules
Unsupported Rules
Externally-defined Rul
SDM Default Rules
Port to Application Mappi
URL Filtering
Local URL List
URL Filter Servers
Zone Pairs
Zones
AAA
Logging
Edit...
Property
Value
Syslog
Enabled
Syslog Server1
10.0.0.5
Logging to Buffer
Enabled
Buffer Size
512000
Logging Level
debugging (7)
Host Logging Level
debugging (7)

Lab # 5

AutoSecure to Secure R1



Use the AutoSecure Cisco IOS feature.

```
R1#auto secure
--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***
AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]:
Press ENTER to
accept the default of 1 in square brackets.

Interface         IP-Address        OK? Method  Status         Protocol
FastEthernet0/0   10.0.0.1          YES NVRAM administratively down
FastEthernet0/1   unassigned        YES NVRAM   up             up
Serial1/0         11.0.0.1          YES NVRAM administratively down
Serial1/1                           YES NVRAM   up             up


Enter the interface name that is facing the internet: serial 1/0
Securing Management plane services...
Disabling service finger
```

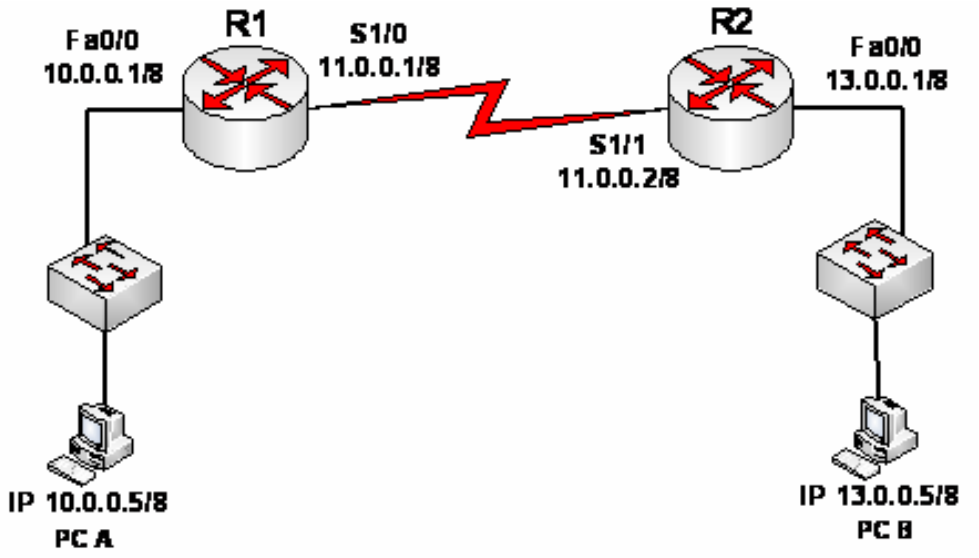
```
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Here is a sample Security Banner to be shown
at every access to device. Modify it to suit your
enterprise requirements.
Authorized Access only
This system is the property of So-&-So-Enterprise.
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access this
device. All activities performed on this device
are logged. Any violations of access policy will result
in disciplinary action.
Enter the security banner {Put the banner between
k and k, where k is any character}:

# Unauthorized Access Prohibited #

Enable secret is either not configured or
is the same as enable password
Enter the new enable secret: cisco12345
Confirm the enable secret : cisco12345
Enter the new enable password: cisco67890
Confirm the enable password: cisco67890
Configuration of local user database

Enter the username: admin
Enter the password: cisco12345
Confirm the password: cisco12345
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 60

Maximum Login failures with the device: 2

Maximum time period for crossing the failed login attempts: 30

Configure SSH server? [yes]: Press ENTER to accept the default of yes

Enter the domain-name: yasirb4u3.4shared.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
Disabling mop on Ethernet interfaces
Securing Forwarding plane services...
Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected
```

```
to internet
Configure CBAC Firewall feature? [yes/no]: no
Tcp intercept feature is used prevent tcp syn attack
on the servers in the network. Create autosec_tcp_intercept_list
to form the list of servers to which the tcp traffic is to
be observed

Enable tcp intercept feature? [yes/no]: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
banner motd ^C Unauthorized Access Prohibited ^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$FmV1$.xZUegmNYFJwJv/oFwwvG1
enable password 7 045802150C2E181B5F
username admin password 7 01100F175804575D72
aaa new-model
aaa authentication login local_auth local
line con 0
login authentication local_auth
exec-timeout 5 0
transport output telnet
line aux 0
login authentication local_auth
exec-timeout 10 0
transport output telnet
line vty 0 4
login authentication local_auth
transport input telnet
line tty 1
login authentication local_auth
exec-timeout 15 0
login block-for 60 attempts 2 within 30
ip domain-name ccnasecurity.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
no ip redirects
no ip proxy-arp
```

```
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface FastEthernet0/1
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface Serial0/0/0
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
interface Serial0/0/1
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
interface Vlan1
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end

Apply this configuration to running-config? [yes]: <ENTER>
Applying the config generated to running-config
The name for the keys will be: R3.ccnasecurity.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R3#
000037: *Dec 19 21:18:52.495 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration
has been Modified on this device
```

LAB # 6

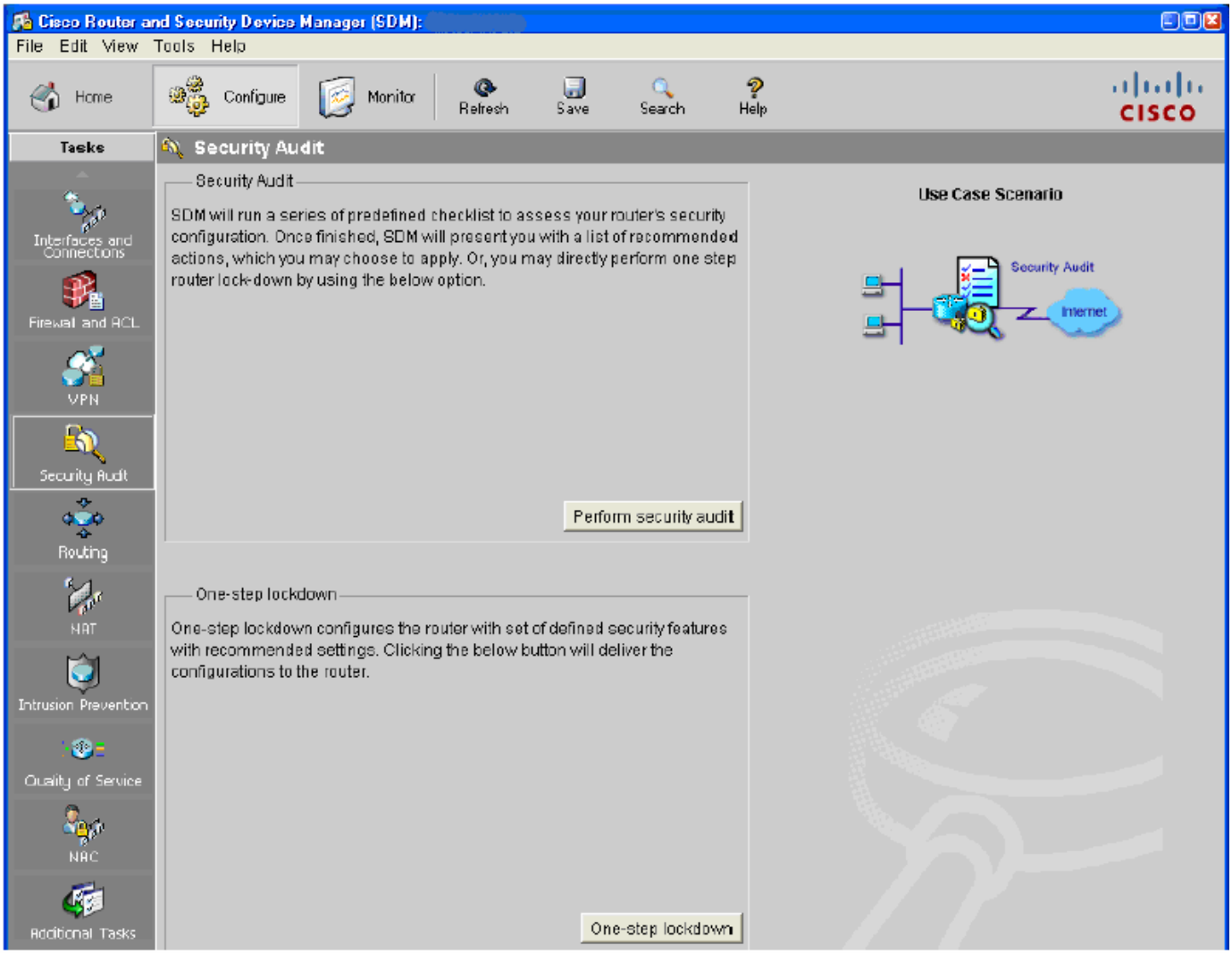
SDM Security Audit Tool on R1 to Identify Security Risks



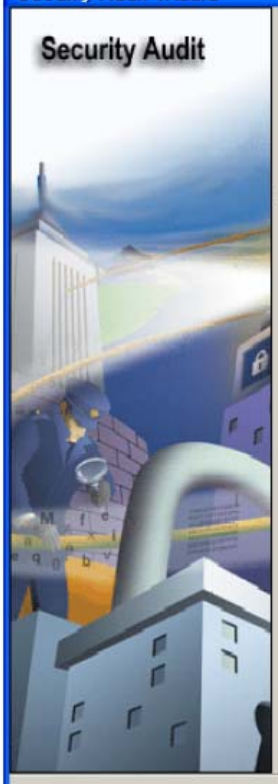
Create an SDM user and enable the HTTP secure server on R1.

```
R1(config)#username yasir privilege 15 secret  cttc123


R1(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 19 17:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 19 17:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue
"write memory" to save new certificate


R1(config)#ip http authentication local
R1(config)#end
```

Start SDM from PC-A


Cisco Router and Security Device Manager (SDM):
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
cisco
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
SDM will run a series of predefined checklist to assess your router's security configuration. Once finished, SDM will present you with a list of recommended actions, which you may choose to apply. Or, you may directly perform one step router lock-down by using the below option.
Perform security audit
One-step lockdown
One-step lockdown configures the router with set of defined security features with recommended settings. Clicking the below button will deliver the configurations to the router.
One-step lockdown
Use Case Scenario
Security Audit
Internet

Security Audit Wizard



Welcome to the security audit wizard

Security audit is a feature that examines your existing router configuration and then provides a list of recommended configuration changes in order to make your router and network more secure.

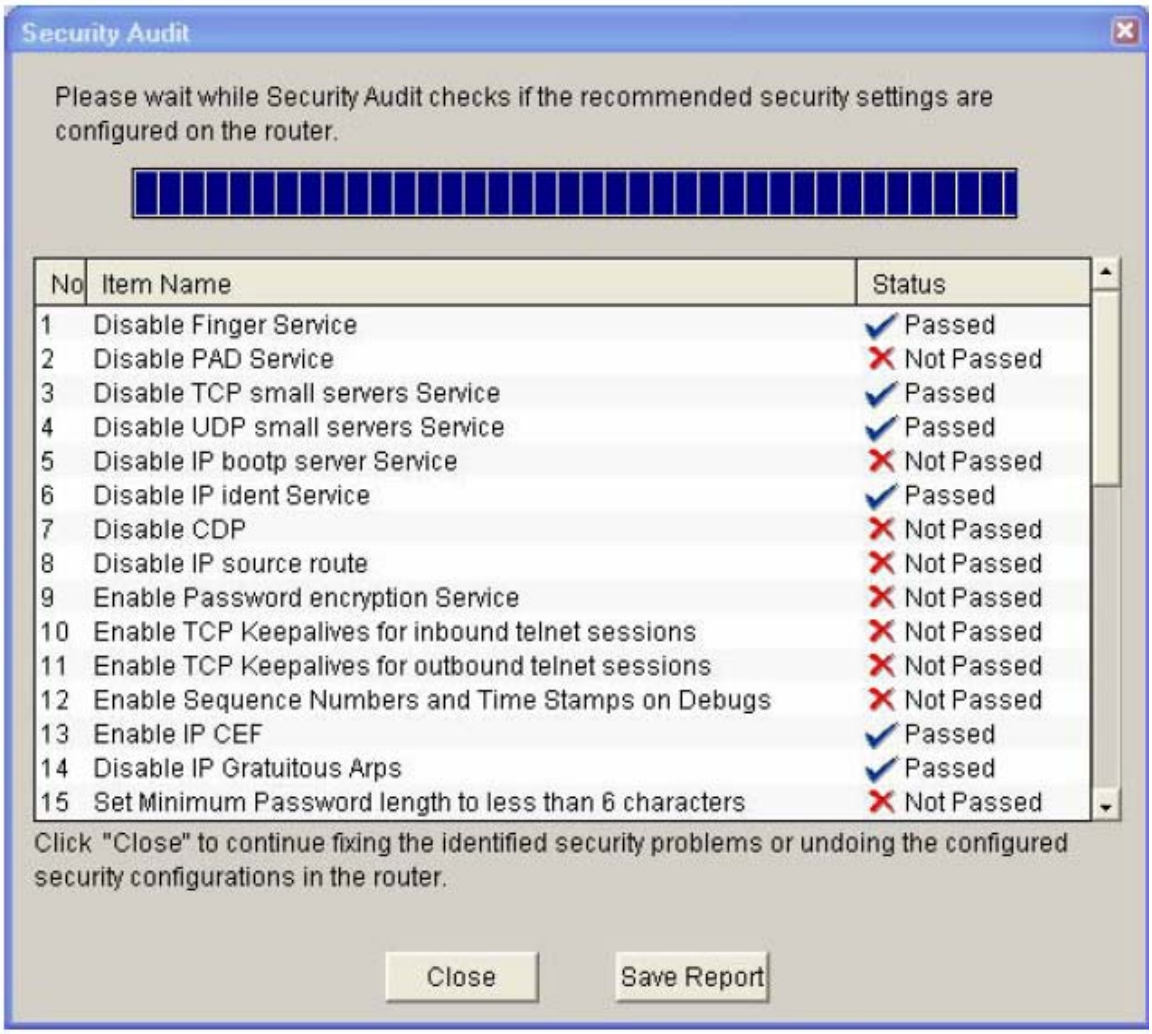
For a complete list of functions security audit checks for, see the On-line help topics.

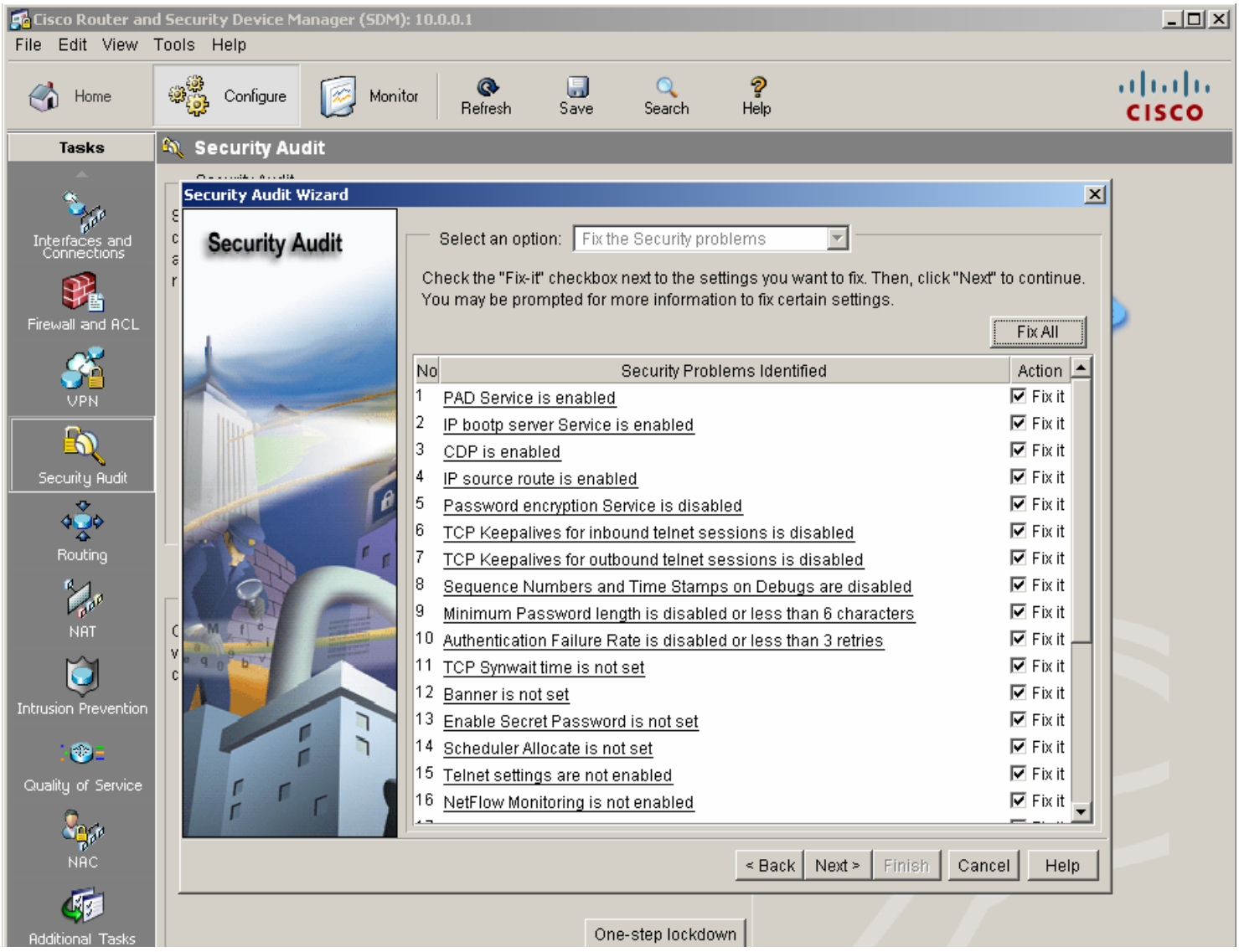
Security audit will

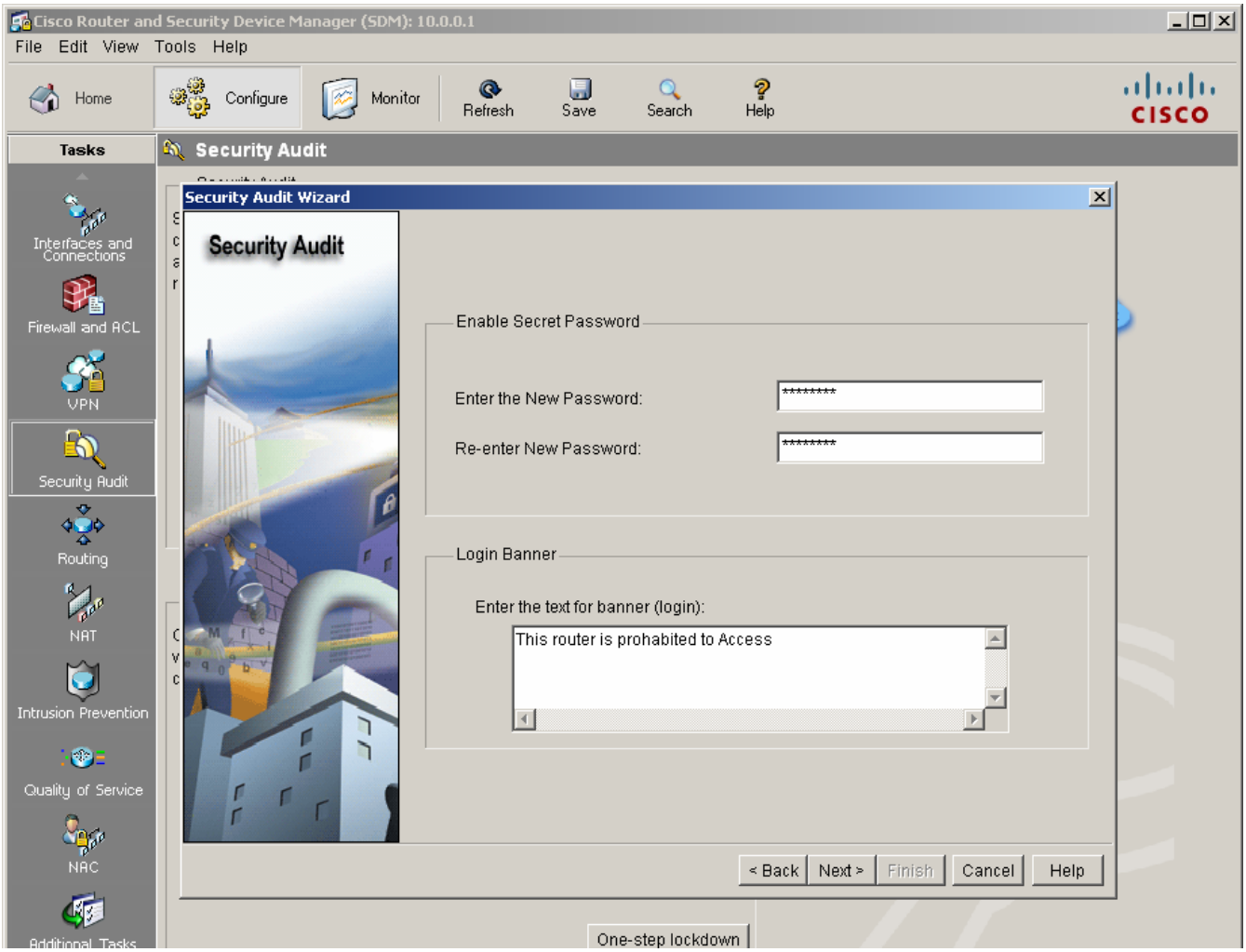
- Check the router's running config. against a list of predefined security configuration settings.
- List identified problems then provide recommendations for fixing them.
- Allow the user to choose which identified problem(s) to fix then display the appropriate user interface for fixing them.
- Configures the router with user chosen security configuration.

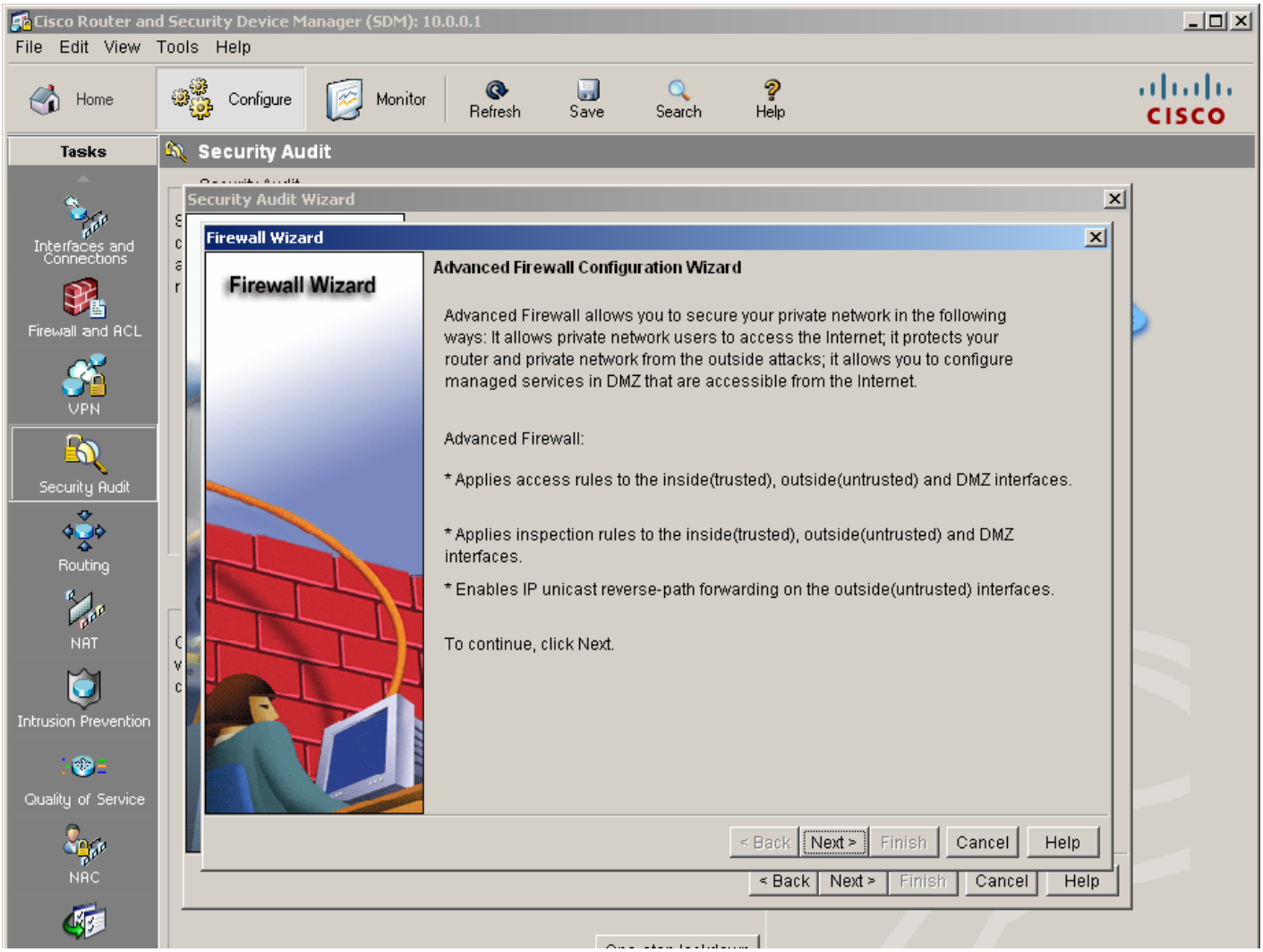
To continue click next.

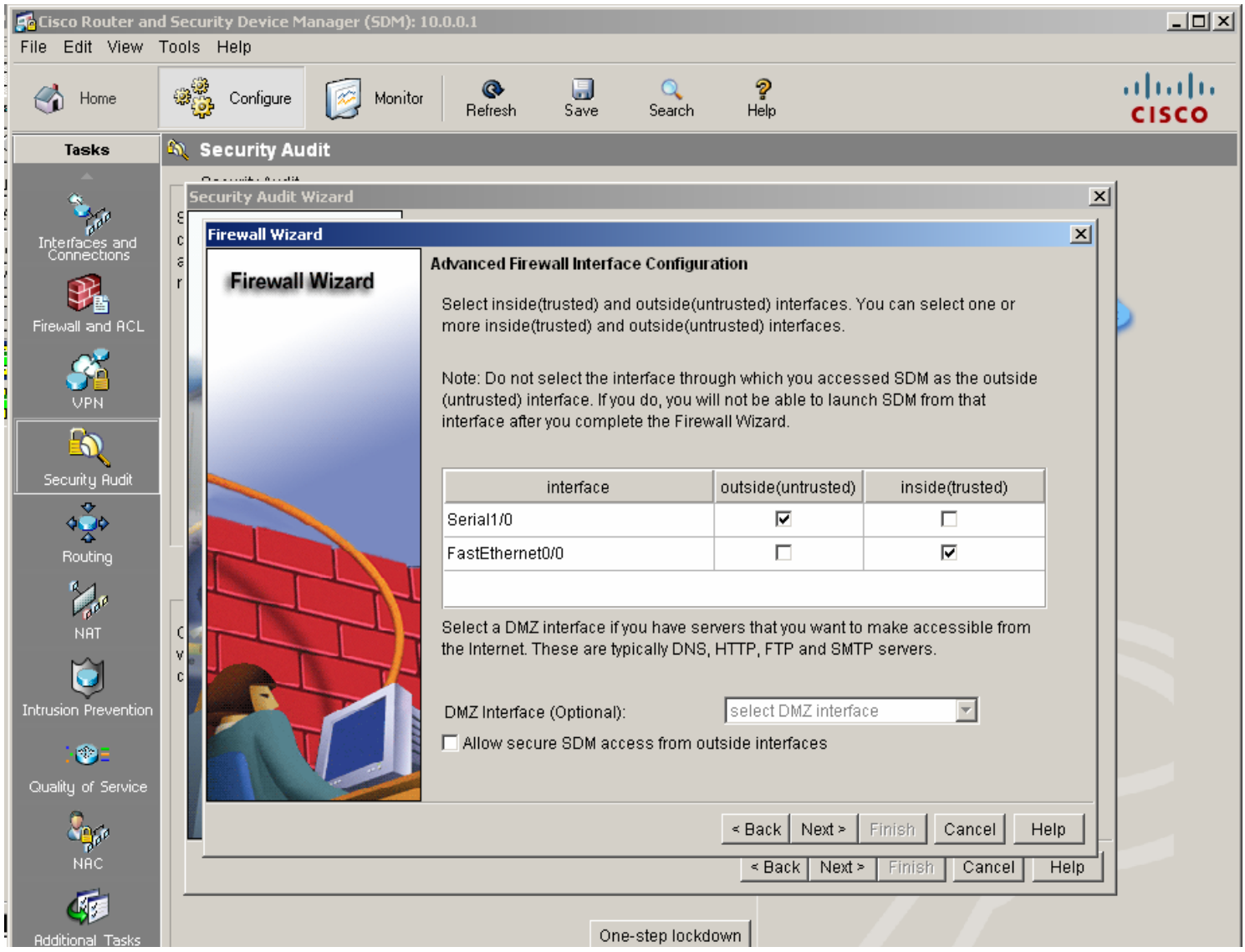
< Back | Next > | Finish | Cancel | Help

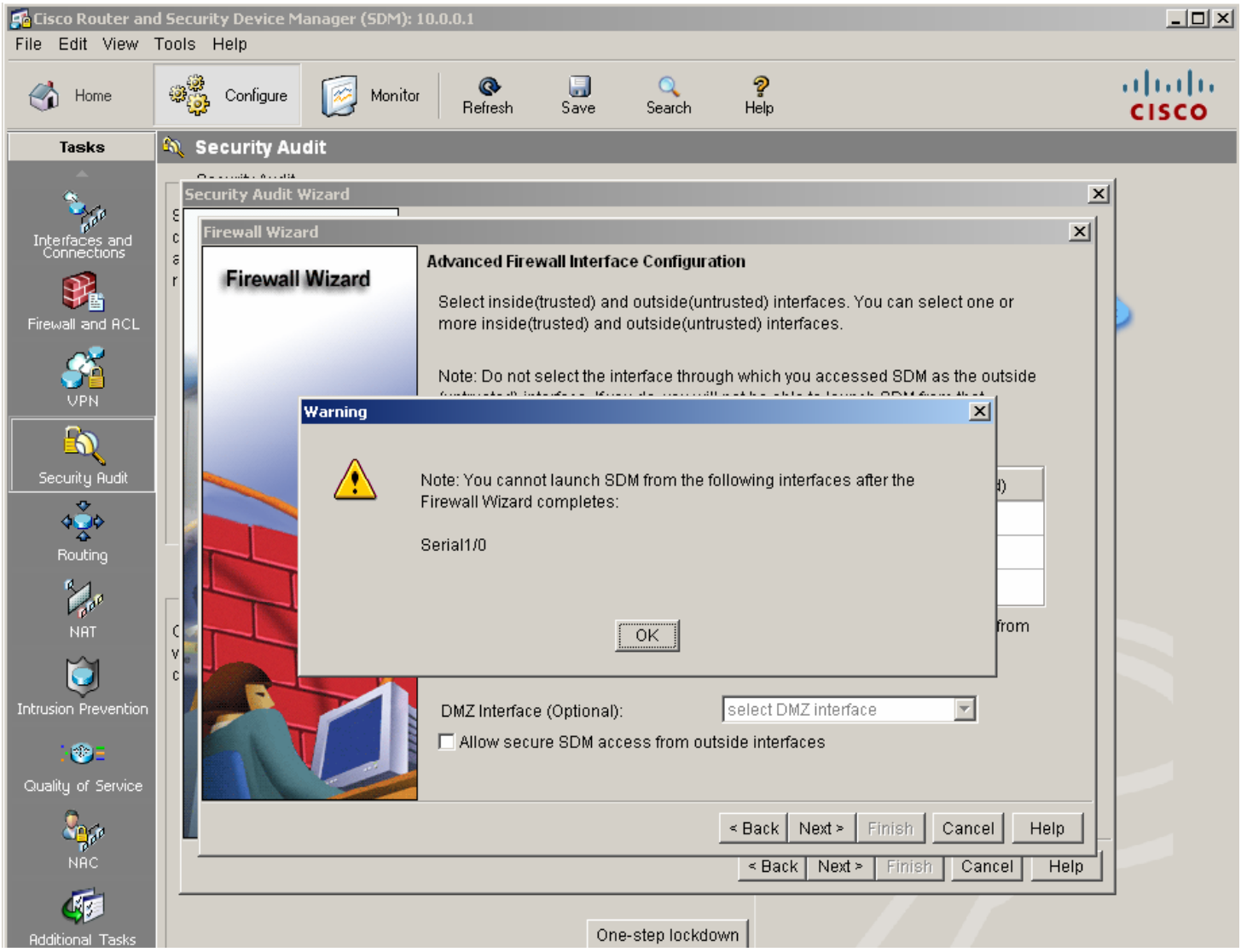

Security Audit
Please wait while Security Audit checks if the recommended security settings are configured on the router.
No
Item Name
Status
1 Disable Finger Service Passed
2 Disable PAD Service Not Passed
3 Disable TCP small servers Service Passed
4 Disable UDP small servers Service Passed
5 Disable IP bootp server Service Not Passed
6 Disable IP ident Service Passed
7 Disable CDP Not Passed
8 Disable IP source route Not Passed
9 Enable Password encryption Service Not Passed
10 Enable TCP Keepalives for inbound telnet sessions Not Passed
11 Enable TCP Keepalives for outbound telnet sessions Not Passed
12 Enable Sequence Numbers and Time Stamps on Debugs Not Passed
13 Enable IP CEF Passed
14 Disable IP Gratuitous Arps Passed
15 Set Minimum Password length to less than 6 characters Not Passed
Click "Close" to continue fixing the identified security problems or undoing the configured security configurations in the router.
Close
Save Report

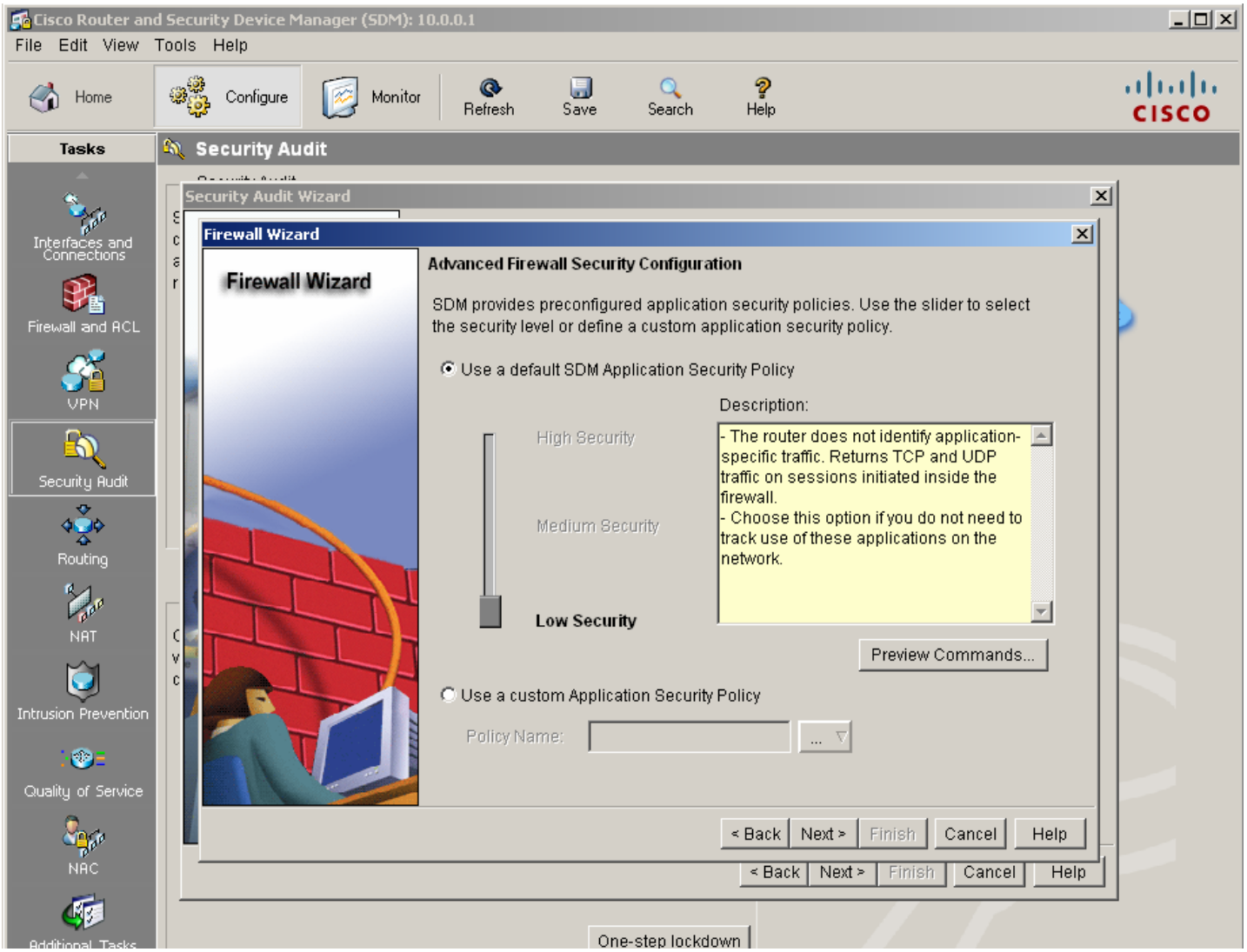

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Security Audit
Select an option: Fix the Security problems
Check the "Fix-it" checkbox next to the settings you want to fix. Then, click "Next" to continue.
You may be prompted for more information to fix certain settings.
Fix All
No
Security Problems Identified
Action
1 PAD Service is enabled Fix it
2 IP bootp server Service is enabled Fix it
3 CDP is enabled Fix it
4 IP source route is enabled Fix it
5 Password encryption Service is disabled Fix it
6 TCP Keepalives for inbound telnet sessions is disabled Fix it
7 TCP Keepalives for outbound telnet sessions is disabled Fix it
8 Sequence Numbers and Time Stamps on Debugs are disabled Fix it
9 Minimum Password length is disabled or less than 6 characters Fix it
10 Authentication Failure Rate is disabled or less than 3 retries Fix it
11 TCP Synwait time is not set Fix it
12 Banner is not set Fix it
13 Enable Secret Password is not set Fix it
14 Scheduler Allocate is not set Fix it
15 Telnet settings are not enabled Fix it
16 NetFlow Monitoring is not enabled Fix it
< Back
Next >
Finish
Cancel
Help
One-step lockdown

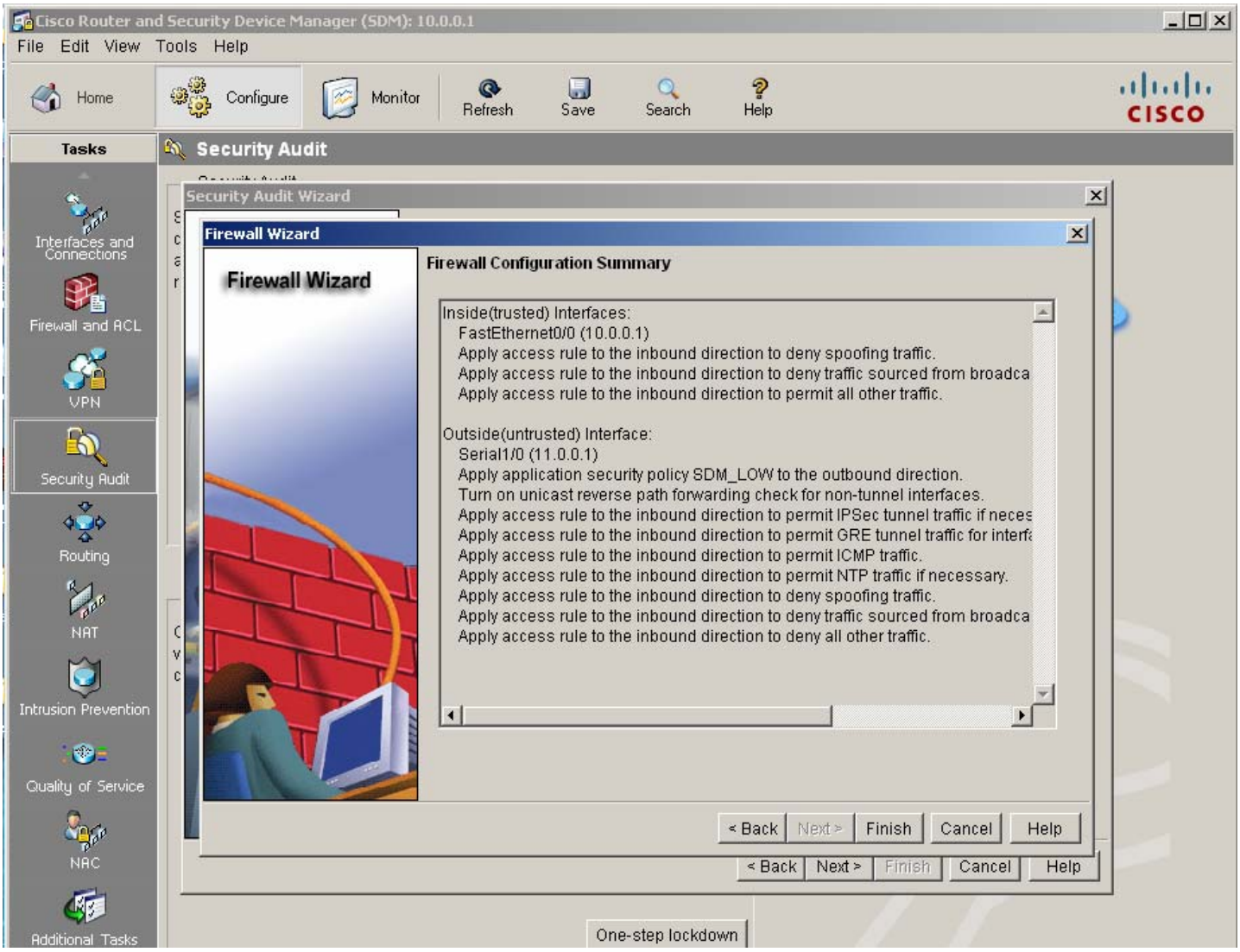

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Security Audit
Enable Secret Password
Enter the New Password:
****
Re-enter New Password:
****
Login Banner
Enter the text for banner (login):
This router is prohibited to Access
< Back
Next >
Finish
Cancel
Help
One-step lockdown

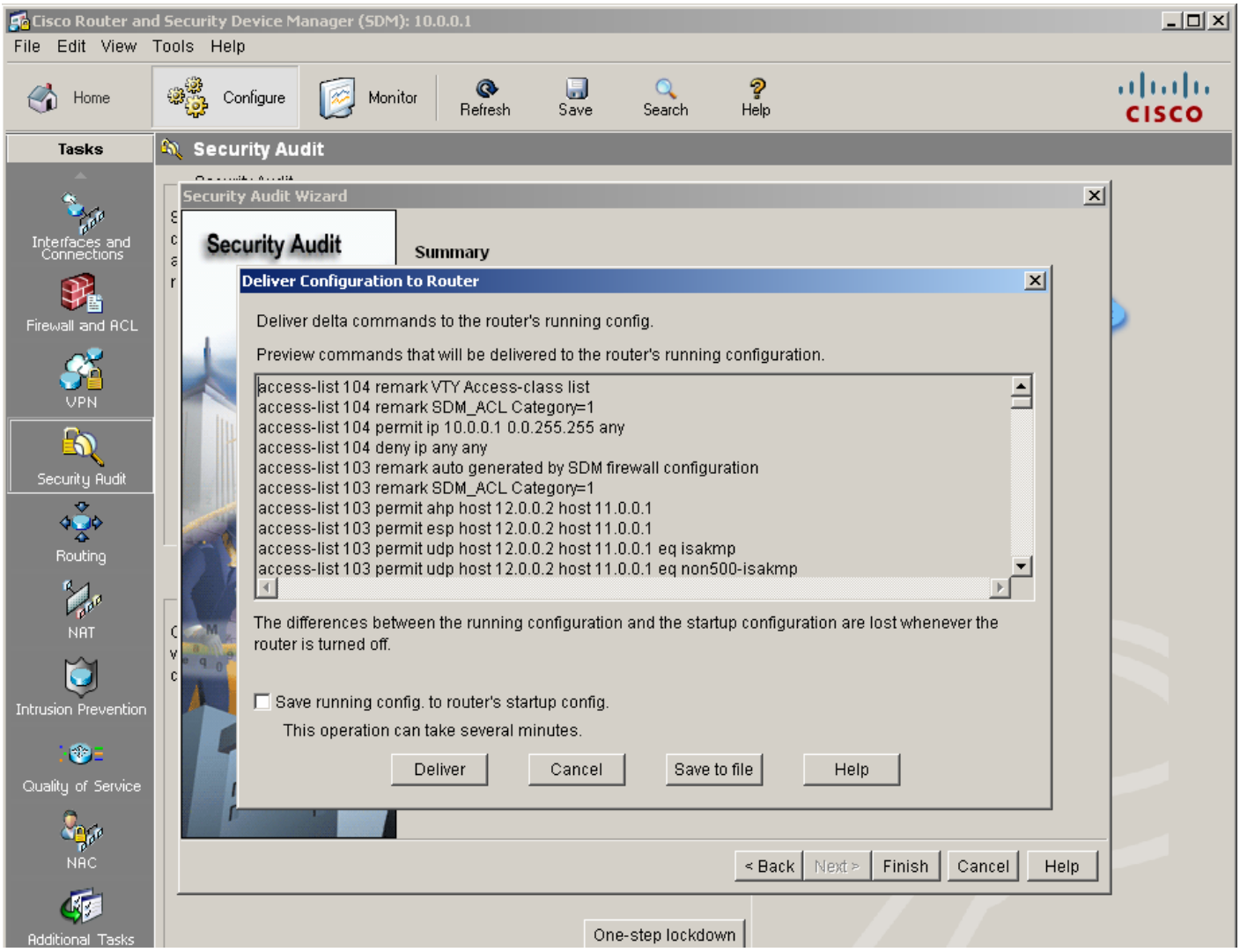

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Security Audit
Security Audit Wizard
Firewall Wizard
Firewall Wizard
Advanced Firewall Configuration Wizard
Advanced Firewall allows you to secure your private network in the following ways: It allows private network users to access the Internet; it protects your router and private network from the outside attacks; it allows you to configure managed services in DMZ that are accessible from the Internet.
Advanced Firewall:
* Applies access rules to the inside(trusted), outside(untrusted) and DMZ interfaces.
* Applies inspection rules to the inside(trusted), outside(untrusted) and DMZ interfaces.
* Enables IP unicast reverse-path forwarding on the outside(untrusted) interfaces.
To continue, click Next.
< Back
Next >
Finish
Cancel
Help
< Back
Next >
Finish
Cancel
Help

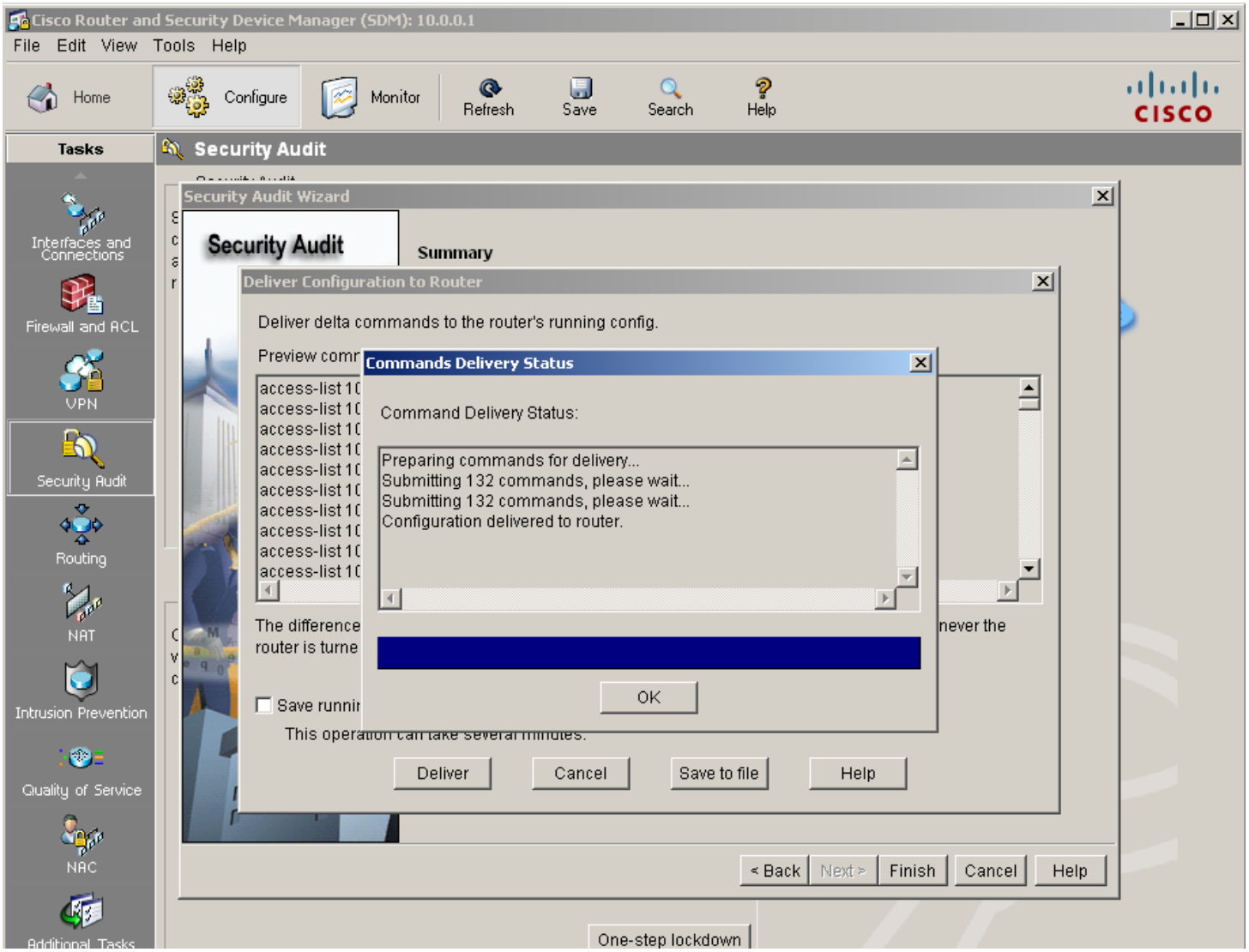

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Security Audit
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit Wizard
Firewall Wizard
Firewall Wizard
Advanced Firewall Interface Configuration
Select inside(trusted) and outside(untrusted) interfaces. You can select one or more inside(trusted) and outside(untrusted) interfaces.
Note: Do not select the interface through which you accessed SDM as the outside (untrusted) interface. If you do, you will not be able to launch SDM from that interface after you complete the Firewall Wizard.
interface
outside(untrusted)
inside(trusted)
Serial1/0
FastEthernet0/0
Select a DMZ interface if you have servers that you want to make accessible from the Internet. These are typically DNS, HTTP, FTP and SMTP servers.
DMZ Interface (Optional):
select DMZ interface
Allow secure SDM access from outside interfaces
< Back
Next >
Finish
Cancel
Help
< Back
Next >
Finish
Cancel
Help
One-step lockdown

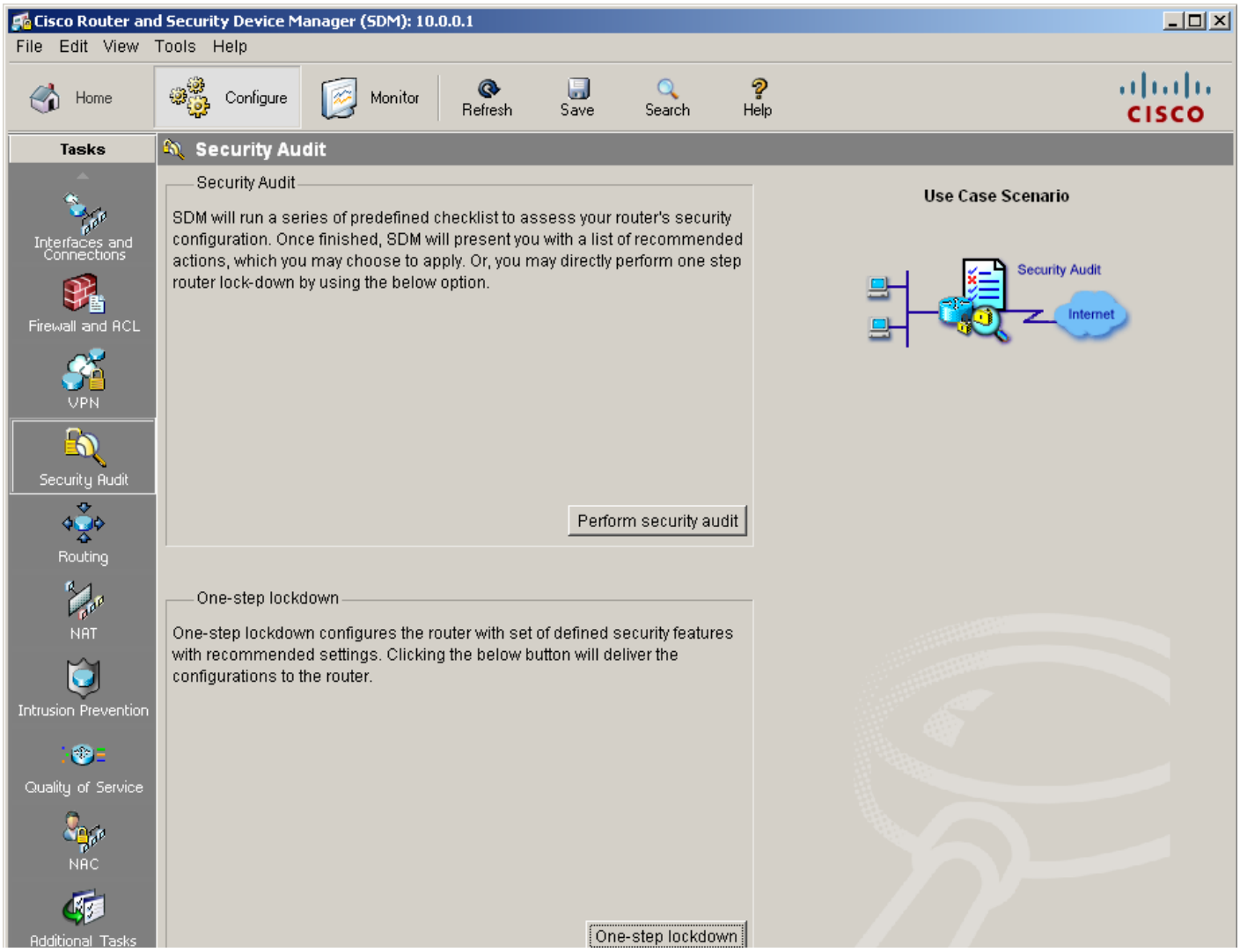

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Firewall Wizard
Firewall Wizard
Advanced Firewall Interface Configuration
Select inside(trusted) and outside(untrusted) interfaces. You can select one or more inside(trusted) and outside(untrusted) interfaces.
Note: Do not select the interface through which you accessed SDM as the outside
Warning
Note: You cannot launch SDM from the following interfaces after the Firewall Wizard completes:
Serial1/0
OK
DMZ Interface (Optional):
select DMZ interface
Allow secure SDM access from outside interfaces
< Back
Next >
Finish
Cancel
Help
< Back
Next >
Finish
Cancel
Help
One-step lockdown


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Security Audit
Security Audit Wizard
Firewall Wizard
Firewall Wizard
Advanced Firewall Security Configuration
SDM provides preconfigured application security policies. Use the slider to select the security level or define a custom application security policy.
Use a default SDM Application Security Policy
Description:
High Security
Medium Security
Low Security
- The router does not identify application-specific traffic. Returns TCP and UDP traffic on sessions initiated inside the firewall.
- Choose this option if you do not need to track use of these applications on the network.
Preview Commands...
Use a custom Application Security Policy
Policy Name:
< Back
Next >
Finish
Cancel
Help
One-step lockdown


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Firewall Wizard
Firewall Wizard
Firewall Configuration Summary
Inside(trusted) Interfaces:
FastEthernet0/0 (10.0.0.1)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to permit all other traffic.
Outside(untrusted) Interface:
Serial1/0 (11.0.0.1)
Apply application security policy SDM_LOW to the outbound direction.
Turn on unicast reverse path forwarding check for non-tunnel interfaces.
Apply access rule to the inbound direction to permit IPSec tunnel traffic if neces
Apply access rule to the inbound direction to permit GRE tunnel traffic for interf
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to deny all other traffic.
< Back
Next >
Finish
Cancel
Help
< Back
Next >
Finish
Cancel
Help
One-step lockdown

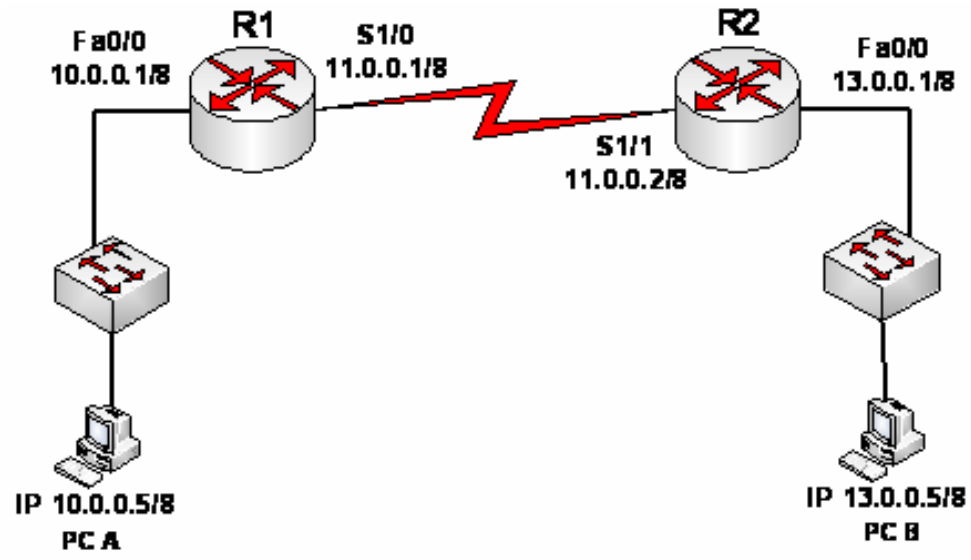

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Security Audit
Summary
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview commands that will be delivered to the router's running configuration.
access-list 104 remark VTY Access-class list
access-list 104 remark SDM_ACL Category=1
access-list 104 permit ip 10.0.0.1 0.0.255.255 any
access-list 104 deny ip any any
access-list 103 remark auto generated by SDM firewall configuration
access-list 103 remark SDM_ACL Category=1
access-list 103 permit ahp host 12.0.0.2 host 11.0.0.1
access-list 103 permit esp host 12.0.0.2 host 11.0.0.1
access-list 103 permit udp host 12.0.0.2 host 11.0.0.1 eq isakmp
access-list 103 permit udp host 12.0.0.2 host 11.0.0.1 eq non500-isakmp
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.
Save running config. to router's startup config.
This operation can take several minutes.
Deliver
Cancel
Save to file
Help
< Back
Next >
Finish
Cancel
Help
One-step lockdown


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit Wizard
Security Audit
Summary
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Commands Delivery Status
Command Delivery Status:
Preparing commands for delivery...
Submitting 132 commands, please wait...
Submitting 132 commands, please wait...
Configuration delivered to router.
OK
Deliver
Cancel
Save to file
Help
< Back
Next >
Finish
Cancel
Help
One-step lockdown

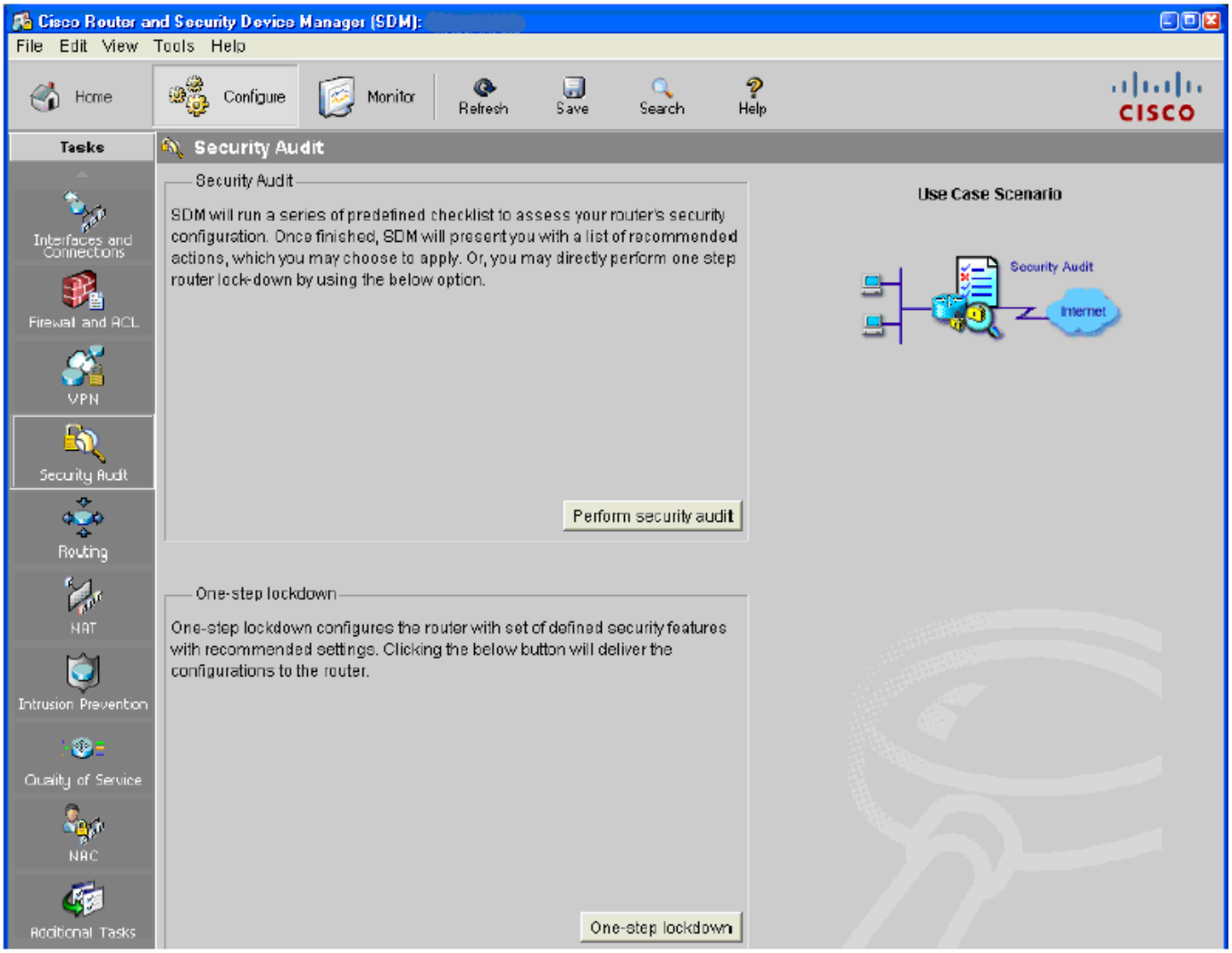

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
SDM will run a series of predefined checklist to assess your router's security configuration. Once finished, SDM will present you with a list of recommended actions, which you may choose to apply. Or, you may directly perform one step router lock-down by using the below option.
Perform security audit
One-step lockdown
One-step lockdown configures the router with set of defined security features with recommended settings. Clicking the below button will deliver the configurations to the router.
One-step lockdown
Use Case Scenario
Security Audit
Internet

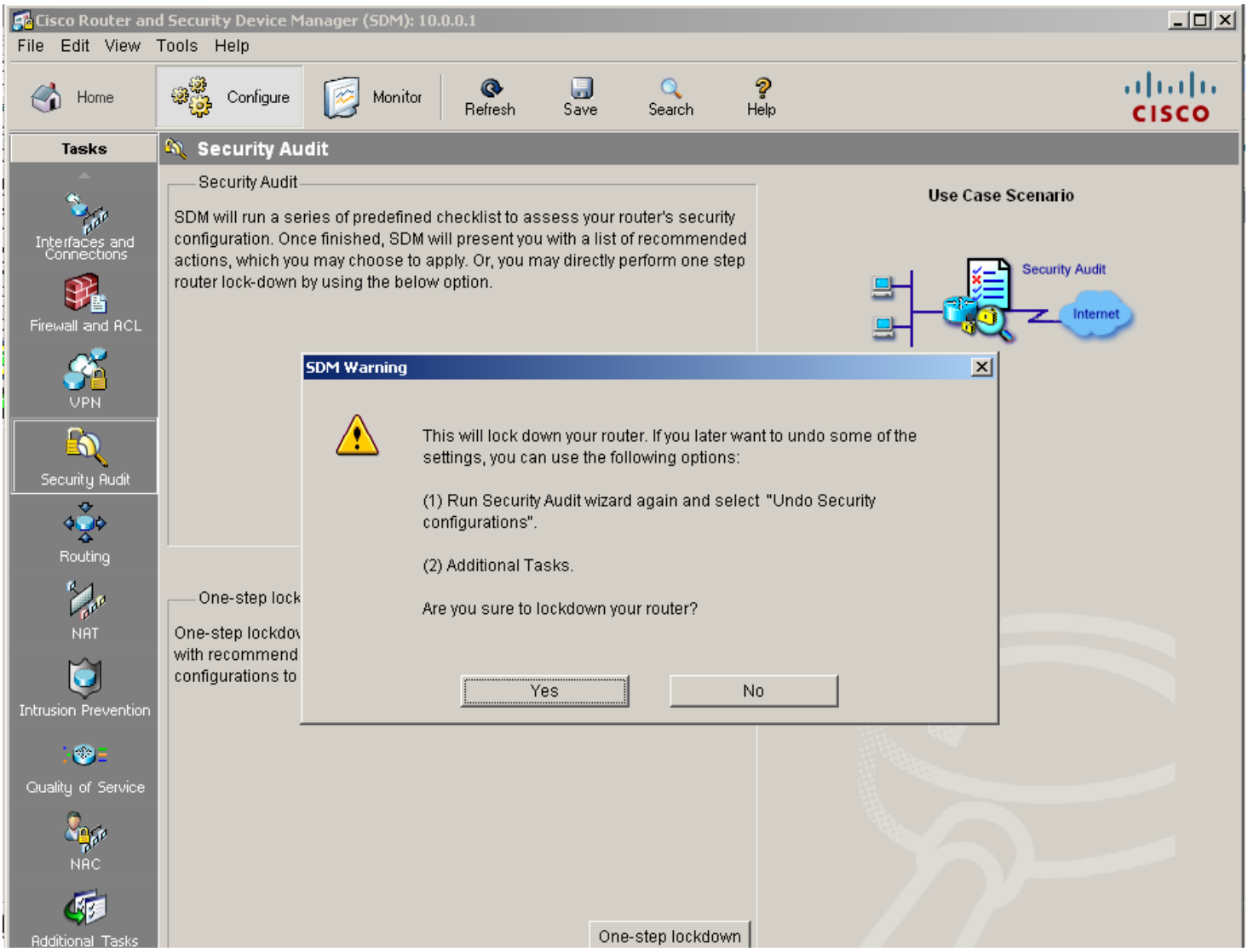
Lab # 7

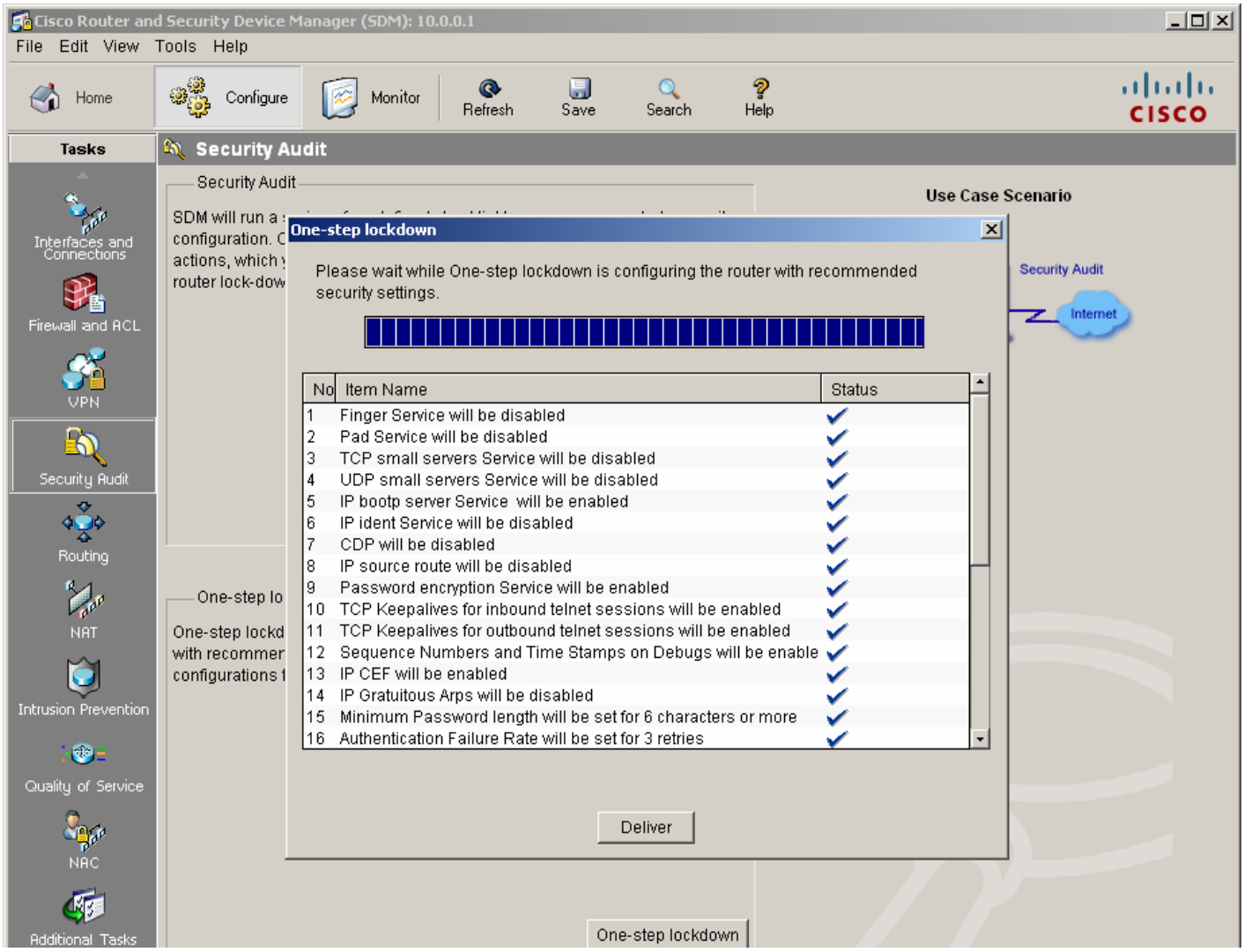
One Step-Lockdown

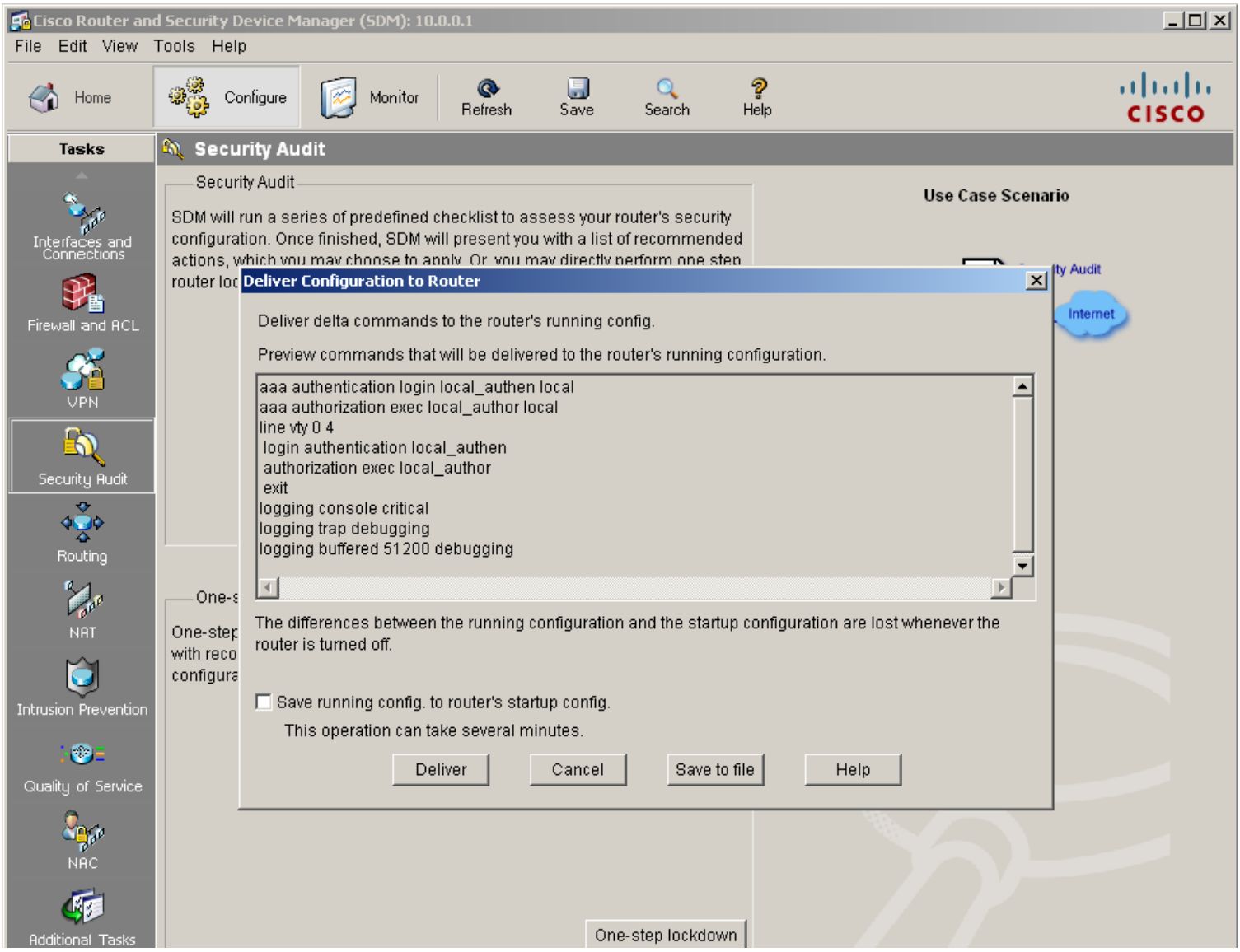


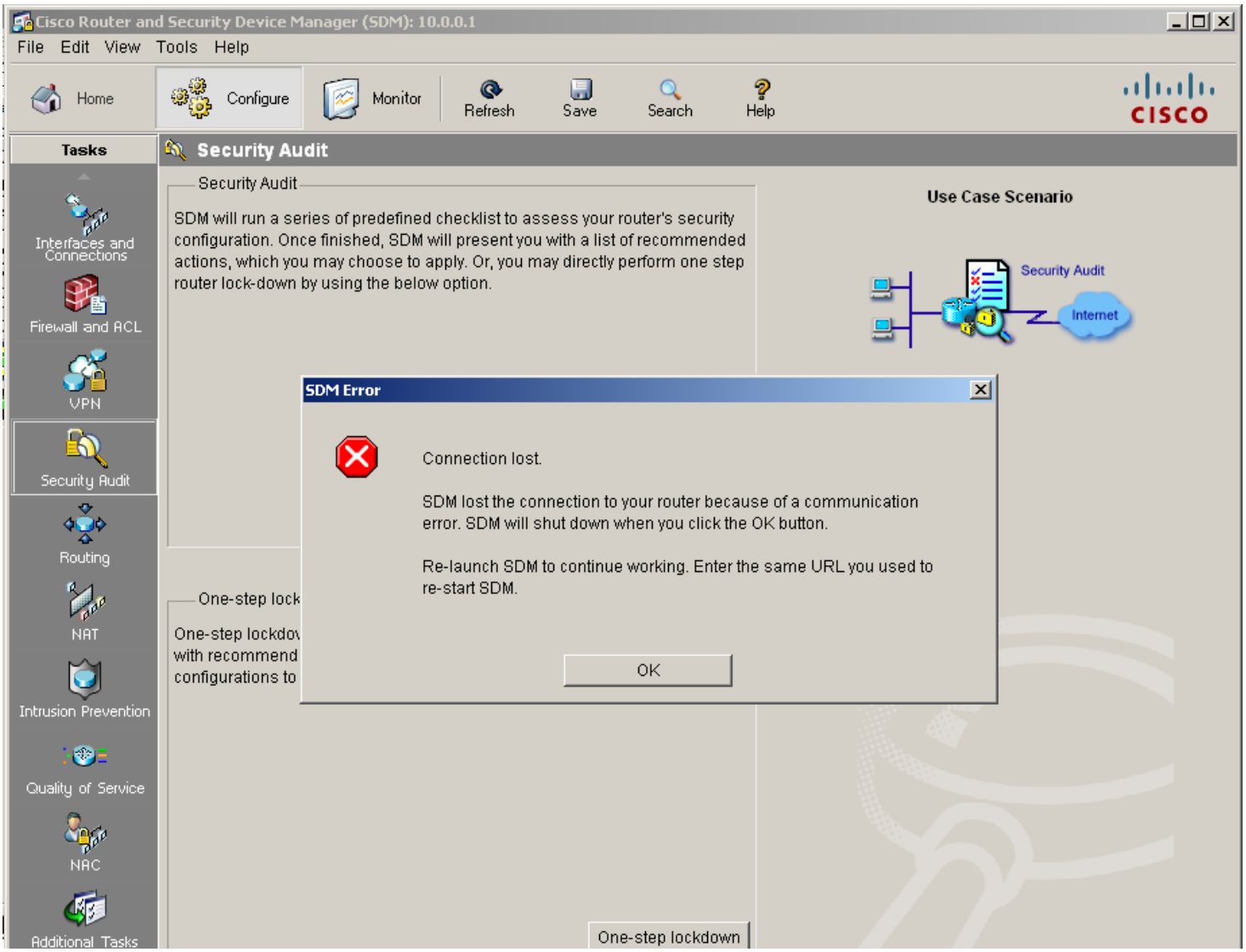
Stat SDM from PC-A Just like above we have configure SDM


Cisco Router and Security Device Manager (SDM):
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
SDM will run a series of predefined checklist to assess your router's security configuration. Once finished, SDM will present you with a list of recommended actions, which you may choose to apply. Or, you may directly perform one step router lock-down by using the below option.
Perform security audit
One-step lockdown
One-step lockdown configures the router with set of defined security features with recommended settings. Clicking the below button will deliver the configurations to the router.
One-step lockdown
Use Case Scenario
Security Audit
Internet

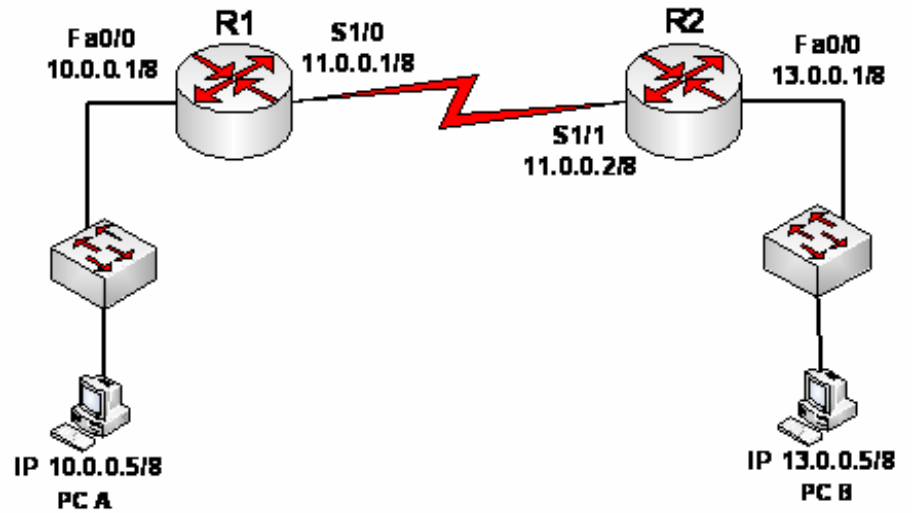

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
SDM will run a series of predefined checklist to assess your router's security configuration. Once finished, SDM will present you with a list of recommended actions, which you may choose to apply. Or, you may directly perform one step router lock-down by using the below option.
Use Case Scenario
Security Audit
Internet
One-step lock
One-step lockdo
with recommend
configurations to
One-step lockdown
SDM Warning
This will lock down your router. If you later want to undo some of the settings, you can use the following options:
(1) Run Security Audit wizard again and select "Undo Security configurations".
(2) Additional Tasks.
Are you sure to lockdown your router?
Yes
No


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
Use Case Scenario
Security Audit
Internet
One-step lockdown
Please wait while One-step lockdown is configuring the router with recommended security settings.
No
Item Name
Status
1 Finger Service will be disabled
2 Pad Service will be disabled
3 TCP small servers Service will be disabled
4 UDP small servers Service will be disabled
5 IP bootp server Service will be enabled
6 IP ident Service will be disabled
7 CDP will be disabled
8 IP source route will be disabled
9 Password encryption Service will be enabled
10 TCP Keepalives for inbound telnet sessions will be enabled
11 TCP Keepalives for outbound telnet sessions will be enabled
12 Sequence Numbers and Time Stamps on Debugs will be enable
13 IP CEF will be enabled
14 IP Gratuitous Arps will be disabled
15 Minimum Password length will be set for 6 characters or more
16 Authentication Failure Rate will be set for 3 retries
Deliver
One-step lockdown


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Security Audit
Security Audit
SDM will run a series of predefined checklist to assess your router's security configuration. Once finished, SDM will present you with a list of recommended actions, which you may choose to apply. Or, you may directly perform one step
Use Case Scenario
Internet
Deliver Configuration to Router
Deliver delta commands to the router's running config.
Preview commands that will be delivered to the router's running configuration.
aaa authentication login local_authen local
aaa authorization exec local_author local
line vty 0 4
login authentication local_authen
authorization exec local_author
exit
logging console critical
logging trap debugging
logging buffered 51200 debugging
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.
Save running config. to router's startup config.
This operation can take several minutes.
Deliver
Cancel
Save to file
Help
One-step lockdown



LAB # 8
Configure Local Authentication Using AAA on R1



Configure the local user database.

R1(config)#**username Admin-Yasir privilege 15 secret cttc123**

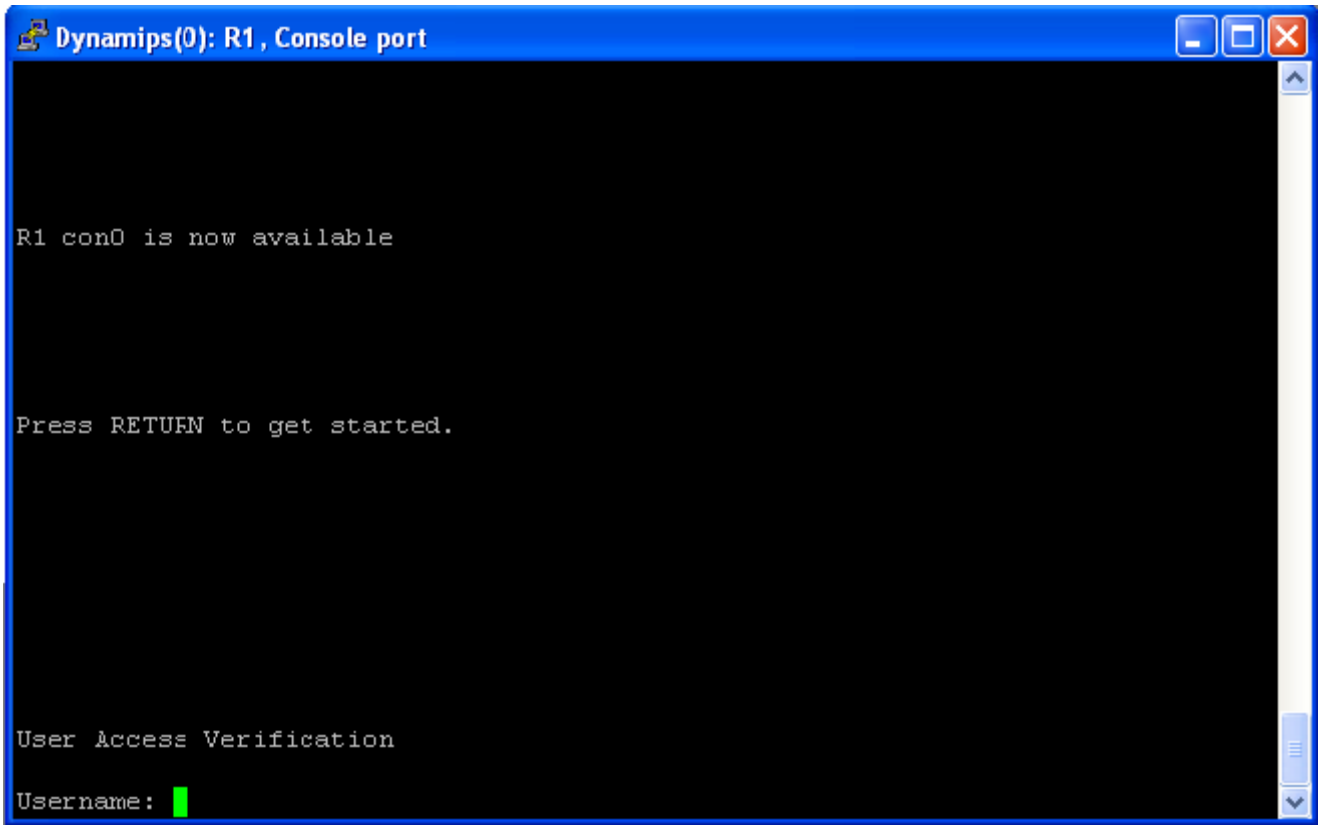
Configure AAA Local Authentication Using Cisco IOS

Enable AAA services.

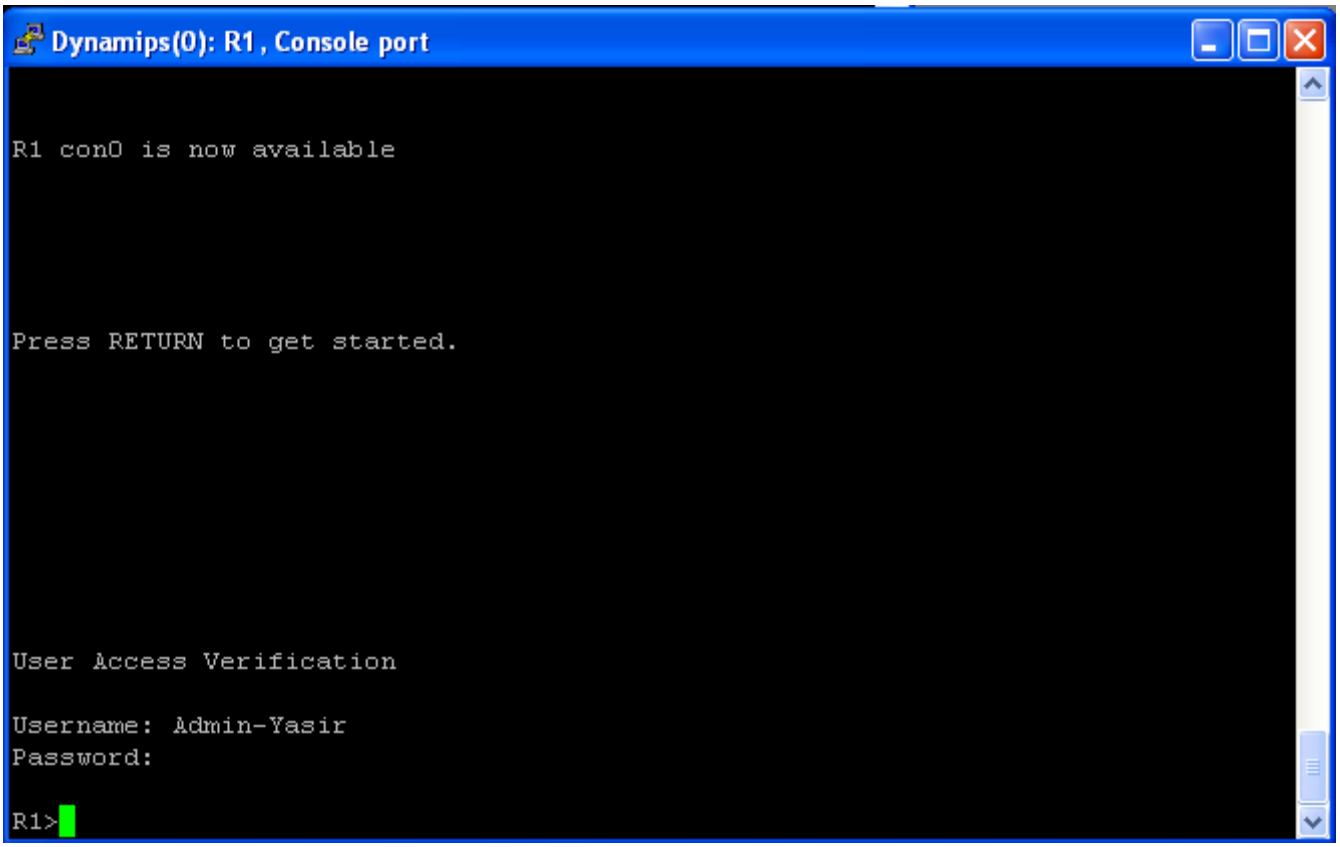
R1(config)#**aaa new-model**

Implement AAA services for console access using the local database.

R1(config)#**aaa authentication login default local none**

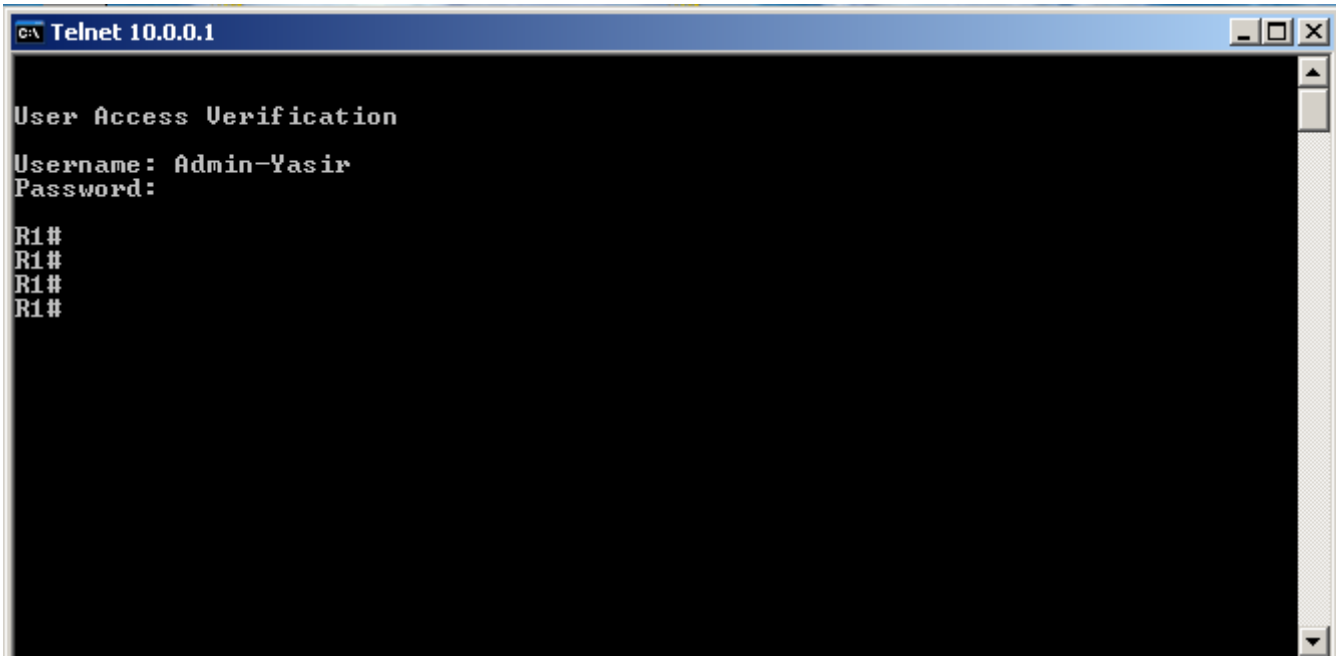


]



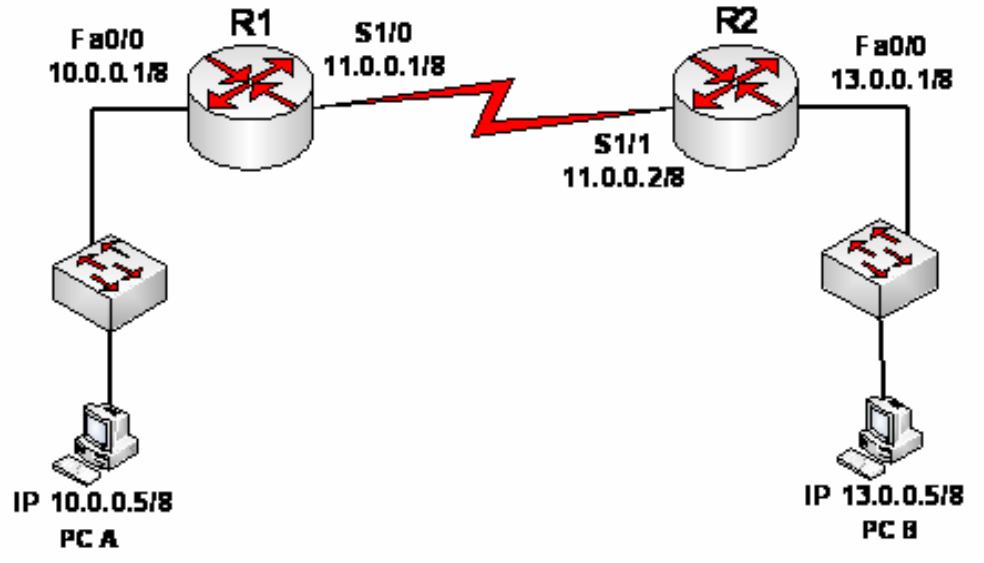
AAA authentication profile for Telnet using the local database.

R1(config)#**aaa authentication login TELNET_LINES local**
R1(config)#**line vty 0 4**
R1(config-line)#**login authentication TELNET_LINES**



LAB # 9

Configure AAA Local Authentication Using Cisco SDM



Implement AAA services and HTTP router access prior to starting SDM.

A. From the CLI global config mode, enable a new AAA model.

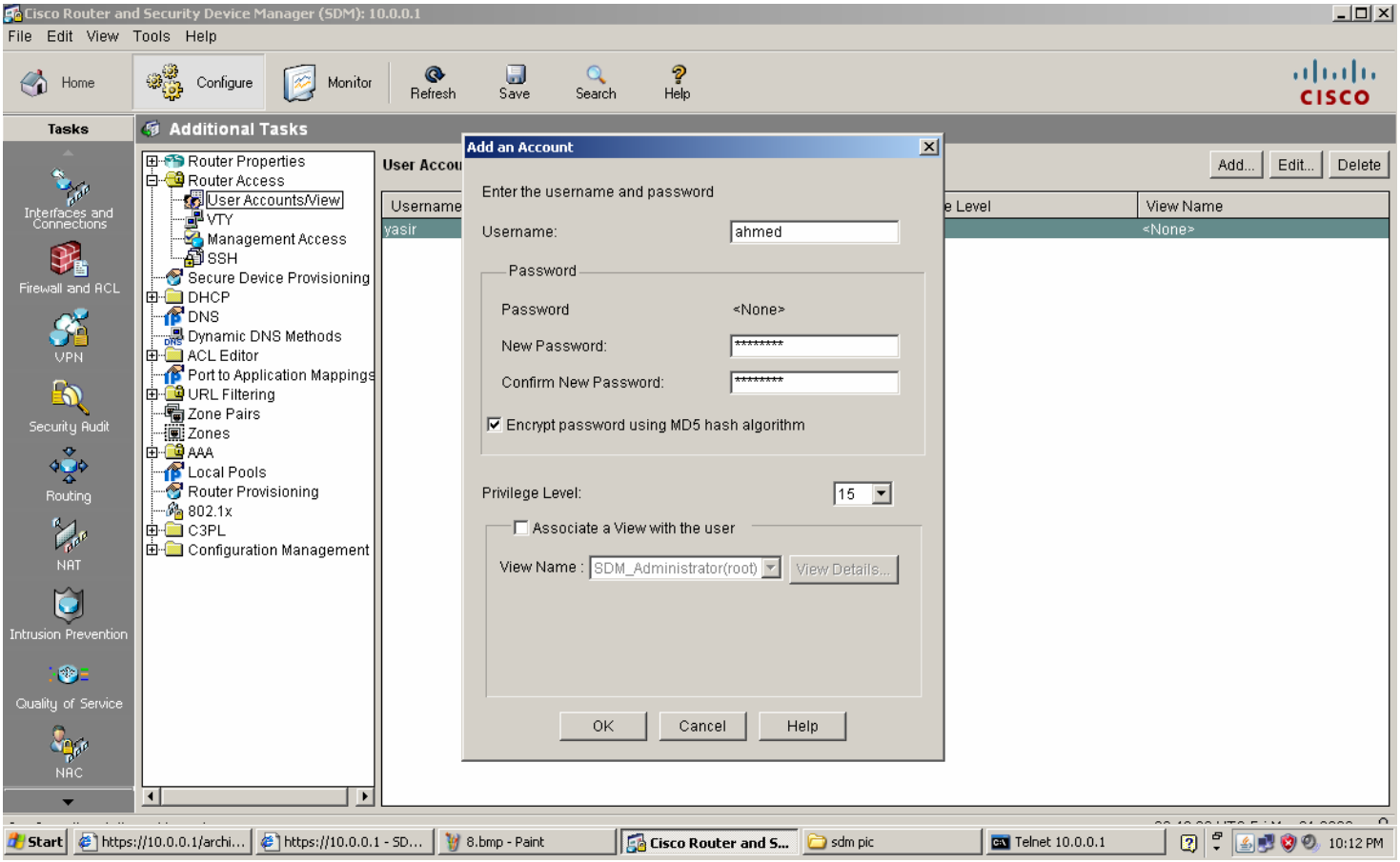
R3(config)#**aaa new-model**

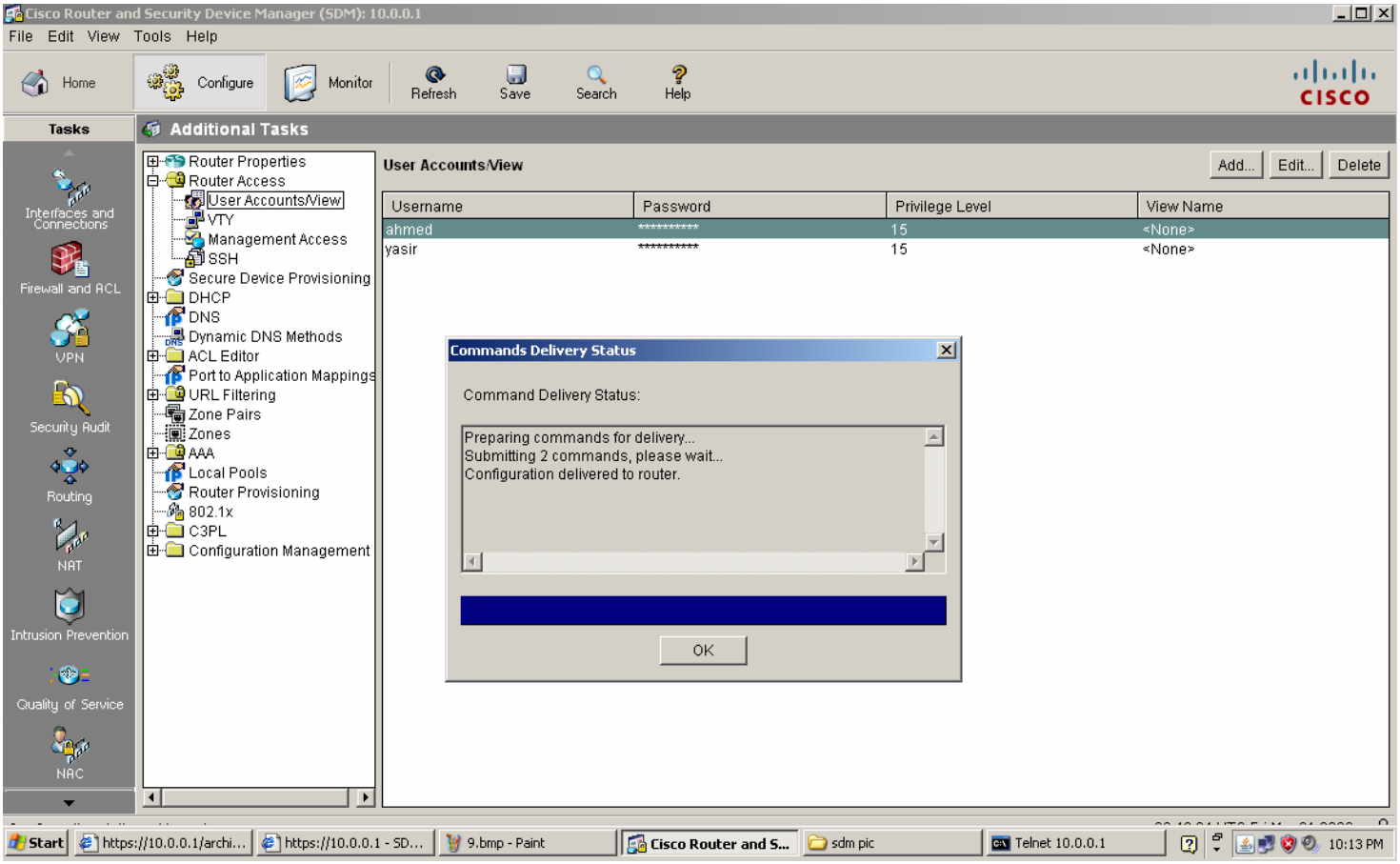
B. Enable the HTTP server on R3 for SDM access.

R3(config)#**ip http server**

Open a browser on PC-C and start SDM by entering the R1 IP address 10.0.0.1 in the address field.
Click the **Configure** button at the top of the screen**.**

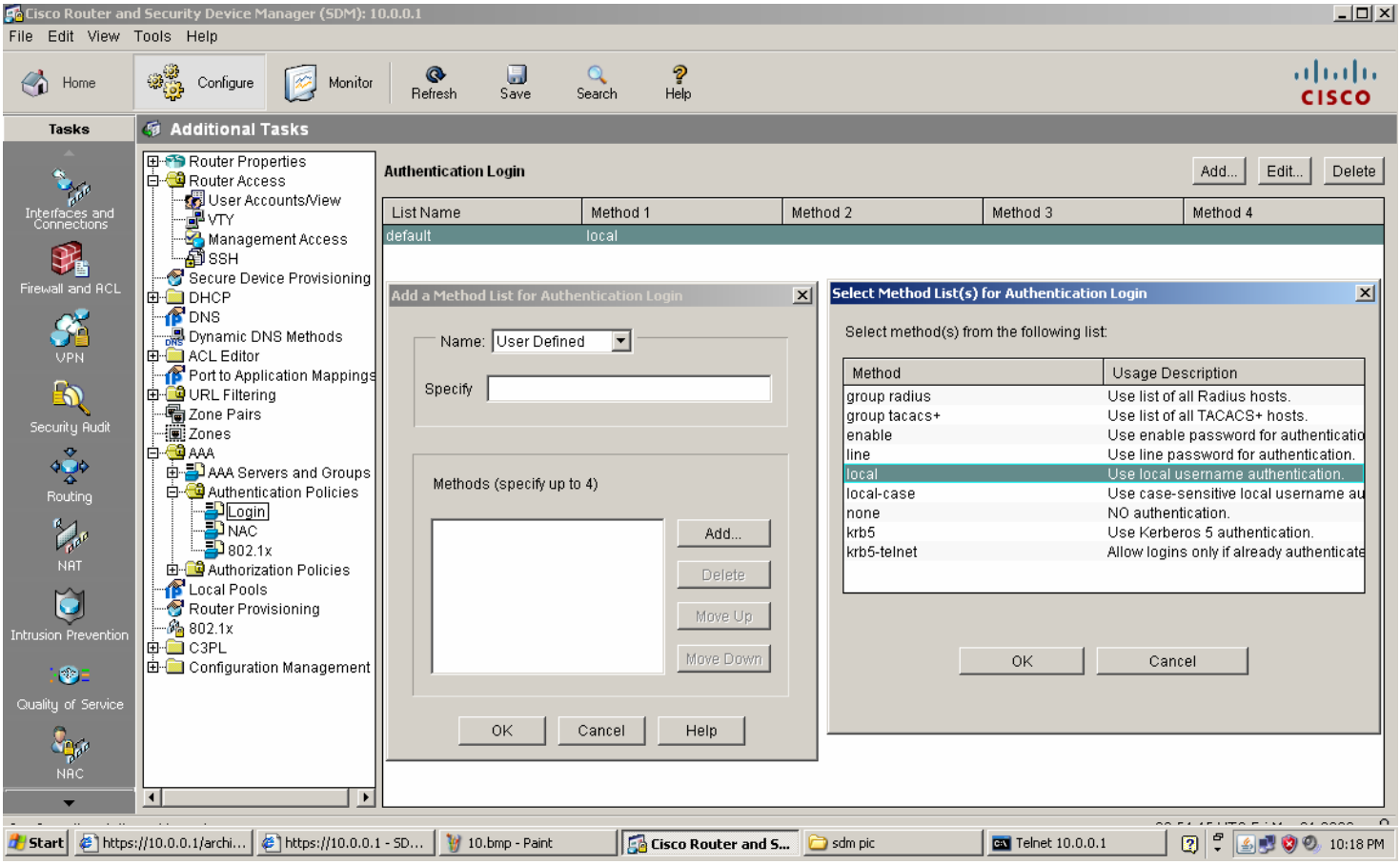
b. Select **Additional Tasks > Router Access > User Accounts/View**.
c. In the User Accounts/View window, click **Add**.

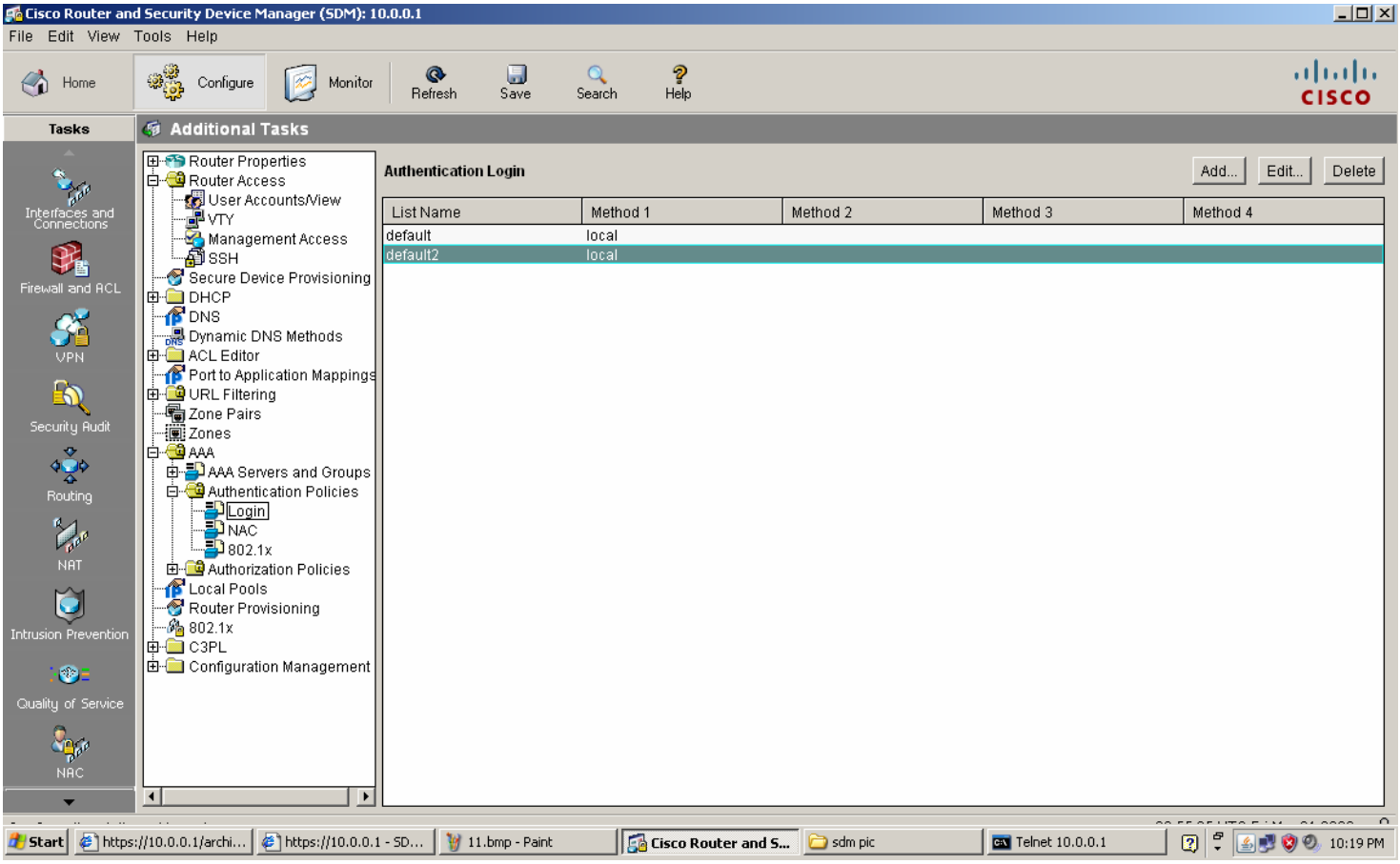




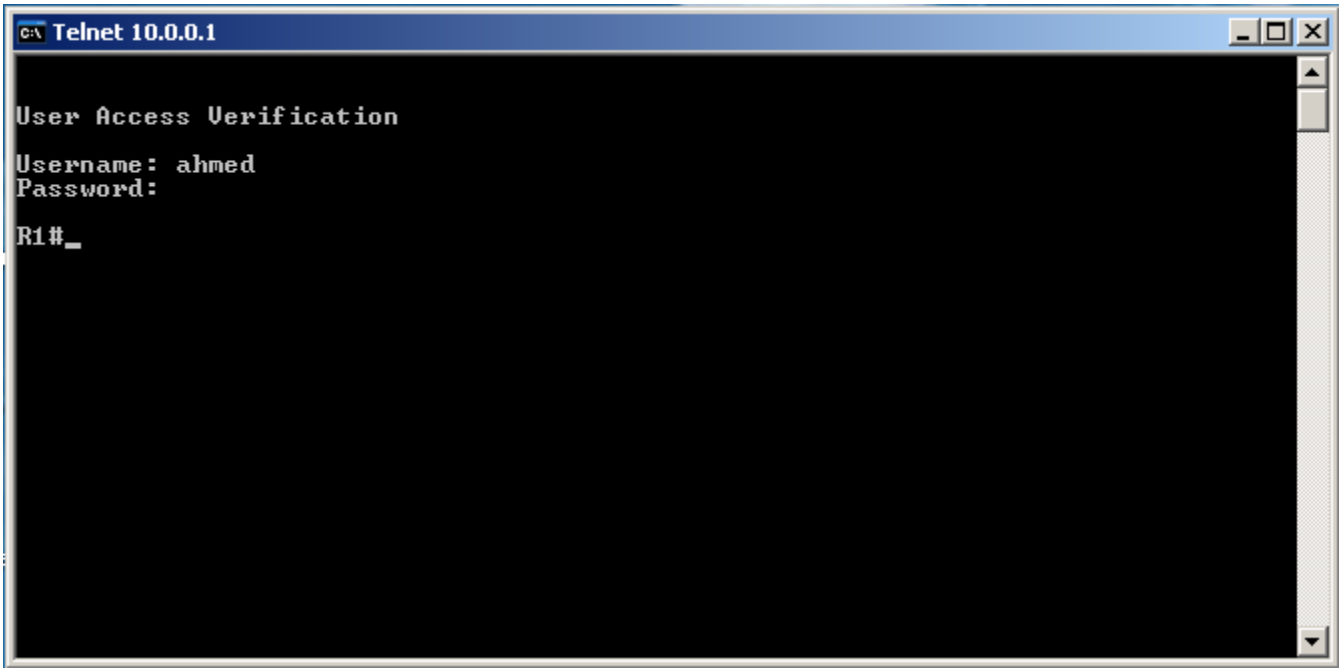
Create a AAA method list for login.

a. Click the **Configure** button at the top of the screen**.**
b. Select **Additional Tasks > AAA > Authentication Policies > Login**.
c. In the Authentication Login window, click **Add**.
d. In the Add a Method List for Authentication Login window, verify that **Default** is in the Name field.


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Router Properties
Router Access
User Accounts/View
VTY
Management Access
SSH
Secure Device Provisioning
DHCP
DNS
Dynamic DNS Methods
ACL Editor
Port to Application Mappings
URL Filtering
Zone Pairs
Zones
AAA
AAA Servers and Groups
Authentication Policies
Login
NAC
802.1x
Authorization Policies
Local Pools
Router Provisioning
802.1x
C3PL
Configuration Management
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Authentication Login
Add...
Edit...
Delete
List Name
Method 1
Method 2
Method 3
Method 4
default
local
Add a Method List for Authentication Login
Name:
User Defined
Specify
Methods (specify up to 4)
Add...
Delete
Move Up
Move Down
OK
Cancel
Help
Select Method List(s) for Authentication Login
Select method(s) from the following list:
Method
Usage Description
group radius
Use list of all Radius hosts.
group tacacs+
Use list of all TACACS+ hosts.
enable
Use enable password for authentication
line
Use line password for authentication.
local
Use local username authentication.
local-case
Use case-sensitive local username au
none
NO authentication.
krb5
Use Kerberos 5 authentication.
krb5-telnet
Allow logins only if already authenticate
OK
Cancel
Start
https://10.0.0.1/archi...
https://10.0.0.1 - SD...
10.bmp - Paint
Cisco Router and S...
sdm pic
Telnet 10.0.0.1
10:18 PM

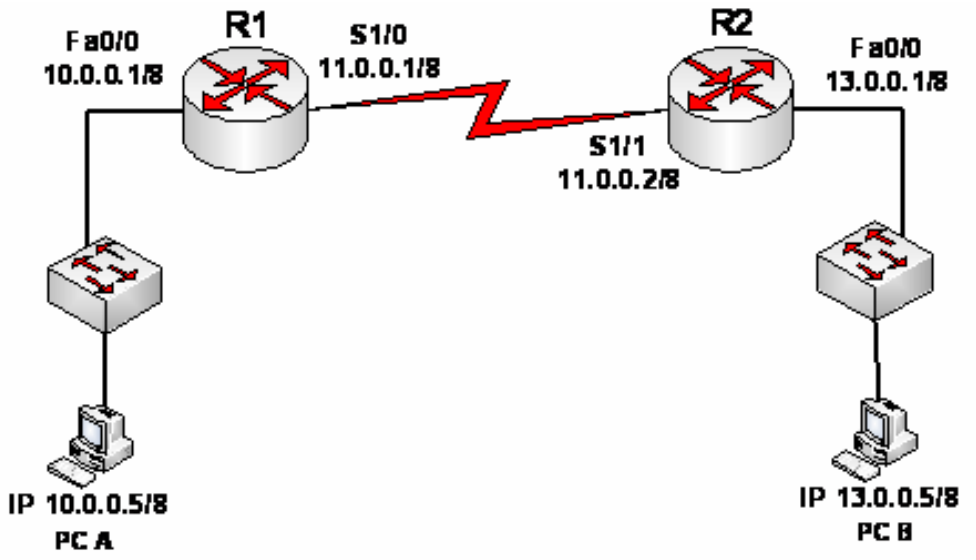

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Additional Tasks
Router Properties
Router Access
User Accounts/View
VTY
Management Access
SSH
Secure Device Provisioning
DHCP
DNS
Dynamic DNS Methods
ACL Editor
Port to Application Mappings
URL Filtering
Zone Pairs
Zones
AAA
AAA Servers and Groups
Authentication Policies
Login
NAC
802.1x
Authorization Policies
Local Pools
Router Provisioning
802.1x
C3PL
Configuration Management
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Authentication Login
Add...
Edit...
Delete
List Name
Method 1
Method 2
Method 3
Method 4
default
local
default2
local
Start
https://10.0.0.1/archi...
https://10.0.0.1 - SD...
11.bmp - Paint
Cisco Router and S...
sdm pic
Telnet 10.0.0.1
10:19 PM

Verify the AAA username and profile for console login from PC-A.



Lab # 9

Configuring an Intrusion Prevention System (IPS) Using SDM



Cisco Router and Security Device Manager (SDM): 10.0.0.1

File Edit View Tools Help

Home | Configure | Monitor | Refresh | Save | Search | Help

Tasks

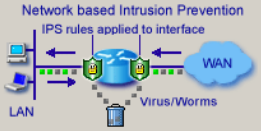
- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC

Intrusion Prevention System (IPS)

Create IPS | Edit IPS | Security Dashboard

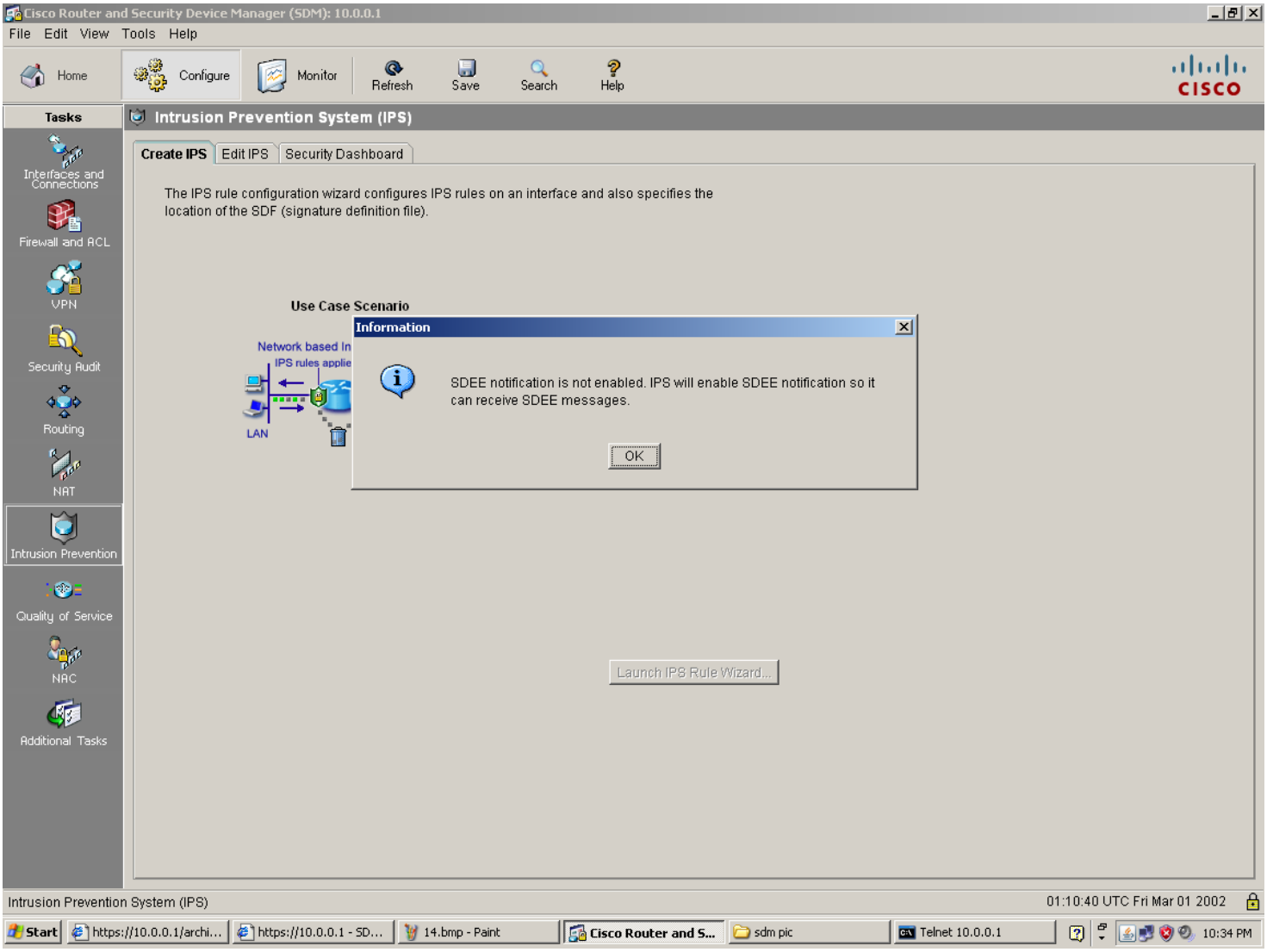
The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Use Case Scenario



Launch IPS Rule Wizard...

Start | https://10.0.0.1/archi... | https://10.0.0.1 - SD... | 13.bmp - Paint | Cisco Router and S... | sdm pic | Telnet 10.0.0.1 | 10:34 PM


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).
Use Case Scenario
Network based In
IPS rules applie
LAN
Information
SDEE notification is not enabled. IPS will enable SDEE notification so it can receive SDEE messages.
OK
Launch IPS Rule Wizard...
Intrusion Prevention System (IPS)
01:10:40 UTC Fri Mar 01 2002
Start
https://10.0.0.1/archi...
https://10.0.0.1 - SD...
14.bmp - Paint
Cisco Router and S...
sdm pic
Telnet 10.0.0.1
10:34 PM

Cisco Router and Security Device Manager (SDM): 10.0.0.1

File Edit View Tools Help

Home | Configure | Monitor | Refresh | Save | Search | Help

Tasks

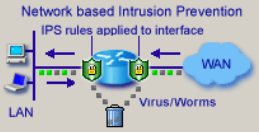
- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Intrusion Prevention System (IPS)

Create IPS | Edit IPS | Security Dashboard

The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Use Case Scenario



IPS Policies Wizard

Welcome to the IPS Policies Wizard

The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file). You must specify the direction of the traffic that should be scanned. If you do not want all traffic to be scanned, you should specify the interesting traffic to be scanned. The router loads the SDF and starts scanning the interesting traffic.

This wizard will assist you in configuring the following tasks

* Select the interface to apply the IPS rule.

* Select the traffic flow direction that should be inspected by the IPS rules.

* Specify the location of the SDF to be used by the router.

To continue, click Next.

< Back | Next > | Finish | Cancel | Help

Intrusion Prevention System (IPS) 01:11:05 UTC Fri Mar 01 2002

Start | https://10.0.0.1/archi... | https://10.0.0.1 - SD... | 15.bmp - Paint | Cisco Router and S... | sdm pic | Telnet 10.0.0.1 | 10:35 PM

Cisco Router and Security Device Manager (SDM): 10.0.0.1

File Edit View Tools Help

Home | Configure | Monitor | Refresh | Save | Search | Help

Tasks

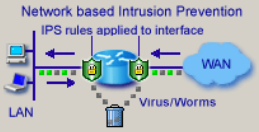
- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Intrusion Prevention System (IPS)

Create IPS | Edit IPS | Security Dashboard

The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Use Case Scenario



IPS Policies Wizard

Select Interfaces

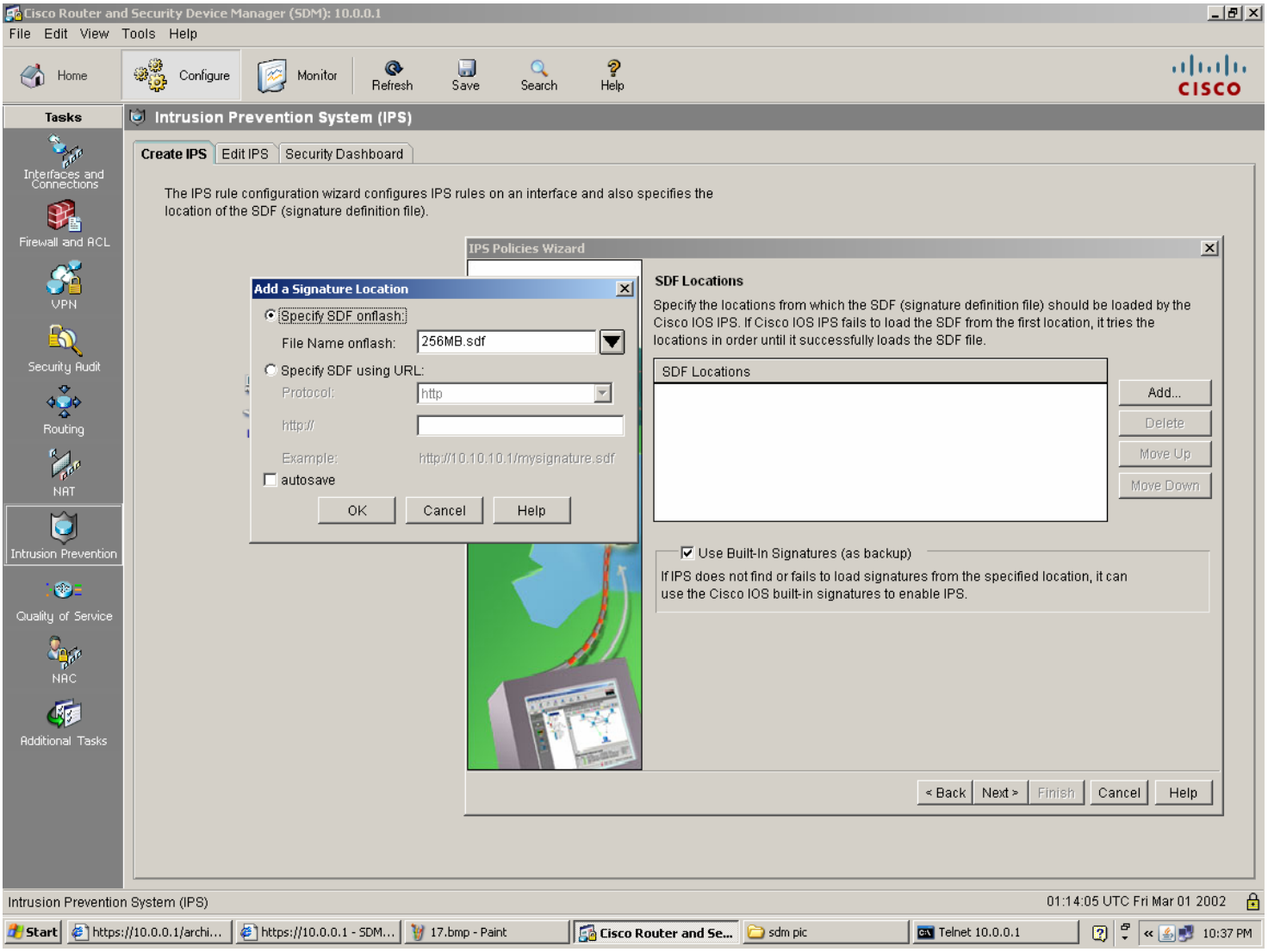
Select the interfaces to which the IPS rule should be applied. Also choose whether the rule should be applied to inbound or outbound.

Interface Name	Inbound	Outbound
FastEthernet0/0	☑	☐
FastEthernet0/1	☐	☐
Serial1/0	☑	☐
Serial1/1	☐	☐
Serial1/2	☐	☐
Serial1/3	☐	☐

< Back | Next > | Finish | Cancel | Help

Intrusion Prevention System (IPS) 01:13:30 UTC Fri Mar 01 2002

Start | https://10.0.0.1/archi... | https://10.0.0.1 - SDM... | 16.bmp - Paint | Cisco Router and Se... | sdm pic | Telnet 10.0.0.1 | 10:37 PM


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).
IPS Policies Wizard
Add a Signature Location
Specify SDF onflash:
File Name onflash:
256MB.sdf
Specify SDF using URL:
Protocol:
http
http://
Example:
http://10.10.10.1/mysignature.sdf
autosave
OK
Cancel
Help
SDF Locations
Specify the locations from which the SDF (signature definition file) should be loaded by the Cisco IOS IPS. If Cisco IOS IPS fails to load the SDF from the first location, it tries the locations in order until it successfully loads the SDF file.
SDF Locations
Add...
Delete
Move Up
Move Down
Use Built-In Signatures (as backup)
If IPS does not find or fails to load signatures from the specified location, it can use the Cisco IOS built-in signatures to enable IPS.
< Back
Next >
Finish
Cancel
Help
Intrusion Prevention System (IPS)
01:14:05 UTC Fri Mar 01 2002
Start
https://10.0.0.1/archi...
https://10.0.0.1 - SDM...
17.bmp - Paint
Cisco Router and Se...
sdm pic
Telnet 10.0.0.1
10:37 PM

Cisco Router and Security Device Manager (SDM): 10.0.0.1

File Edit View Tools Help

Home | Configure | Monitor | Refresh | Save | Search | Help

Tasks

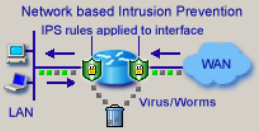
- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Intrusion Prevention System (IPS)

Create IPS | Edit IPS | Security Dashboard

The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

Use Case Scenario



IPS Policies Wizard

SDF Locations

Specify the locations from which the SDF (signature definition file) should be loaded by the Cisco IOS IPS. If Cisco IOS IPS fails to load the SDF from the first location, it tries the locations in order until it successfully loads the SDF file.

SDF Locations

flash://256MB.sdf

Add... | Delete | Move Up | Move Down

☑ Use Built-In Signatures (as backup)

If IPS does not find or fails to load signatures from the specified location, it can use the Cisco IOS built-in signatures to enable IPS.

< Back | Next > | Finish | Cancel | Help

Intrusion Prevention System (IPS) 01:14:21 UTC Fri Mar 01 2002

Start | https://10.0.0.1/archi... | https://10.0.0.1 - SDM... | 18.bmp - Paint | Cisco Router and Se... | sdm pic | Telnet 10.0.0.1 | 10:38 PM

Cisco Router and Security Device Manager (SDM): 10.0.0.1

File Edit View Tools Help

Home | Configure | Monitor | Refresh | Save | Search | Help

Tasks

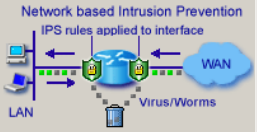
- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Intrusion Prevention System (IPS)

Create IPS | Edit IPS | Security Dashboard

The IPS rule configuration wizard configures IPS
location of the SDF (signature definition file).

Use Case Scenario



IPS Policies Wizard

Summary

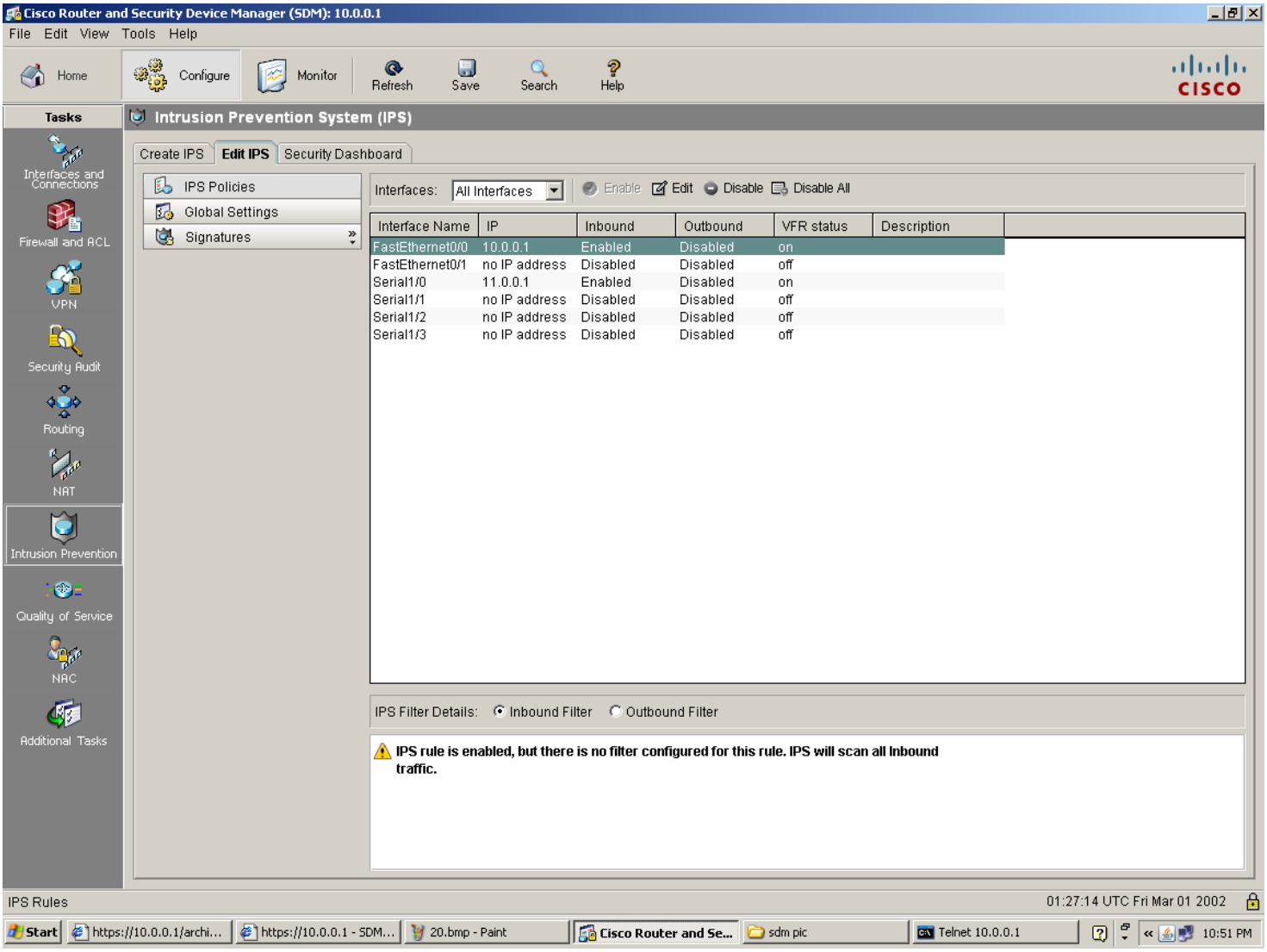
Please click 'Finish' to deliver to router

IPS rule will be applied to the incoming traffic on the following interfaces.
FastEthernet0/0
Serial1/0
Signature File location:
flash://256MB.sdf
Built-in:Enabled

< Back | Next > | Finish | Cancel | Help

Intrusion Prevention System (IPS) 01:14:35 UTC Fri Mar 01 2002

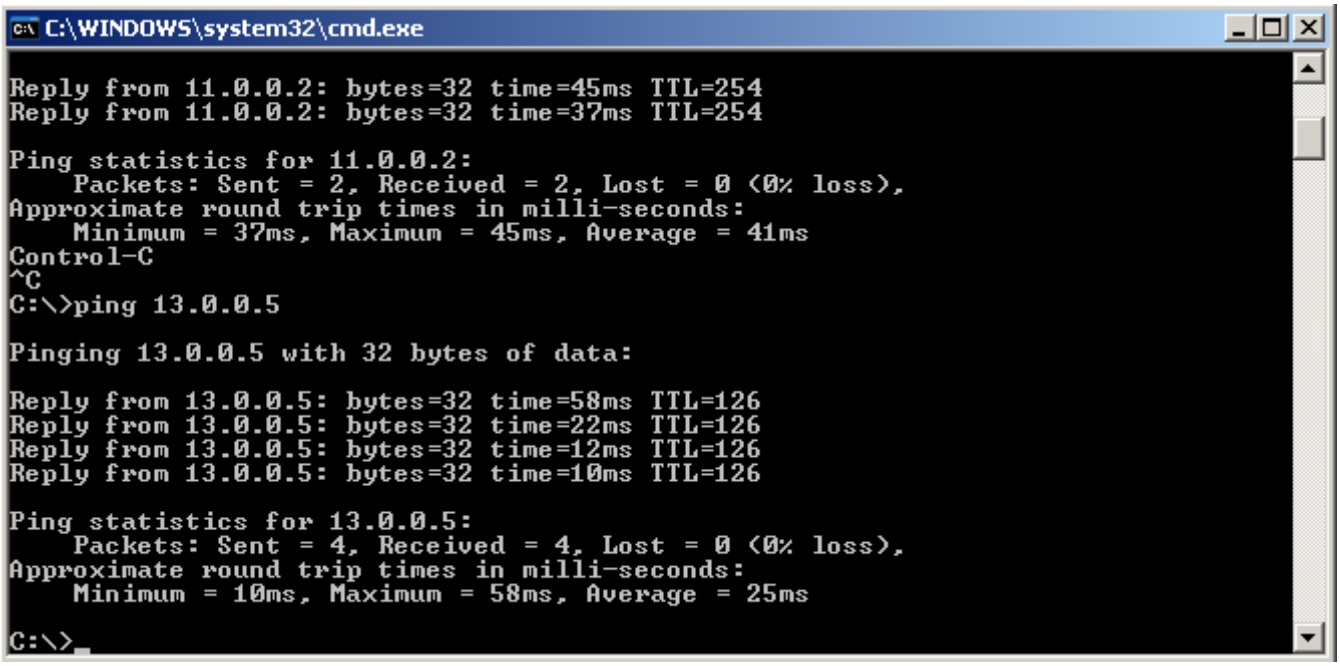
Start | https://10.0.0.1/archi... | https://10.0.0.1 - SDM... | 19.bmp - Paint | Cisco Router and Se... | sdm pic | Telnet 10.0.0.1 | 10:38 PM


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
Interfaces: All Interfaces
Enable
Edit
Disable
Disable All
Interface Name | IP | Inbound | Outbound | VFR status | Description
FastEthernet0/0 | 10.0.0.1 | Enabled | Disabled | on
FastEthernet0/1 | no IP address | Disabled | Disabled | off
Serial1/0 | 11.0.0.1 | Enabled | Disabled | on
Serial1/1 | no IP address | Disabled | Disabled | off
Serial1/2 | no IP address | Disabled | Disabled | off
Serial1/3 | no IP address | Disabled | Disabled | off
IPS Filter Details: Inbound Filter Outbound Filter
IPS rule is enabled, but there is no filter configured for this rule. IPS will scan all Inbound traffic.
IPS Rules
01:27:14 UTC Fri Mar 01 2002
Start
https://10.0.0.1/archi...
https://10.0.0.1 - SDM...
20.bmp - Paint
Cisco Router and Se...
sdm pic
Telnet 10.0.0.1
10:51 PM

Modify Signature Settings

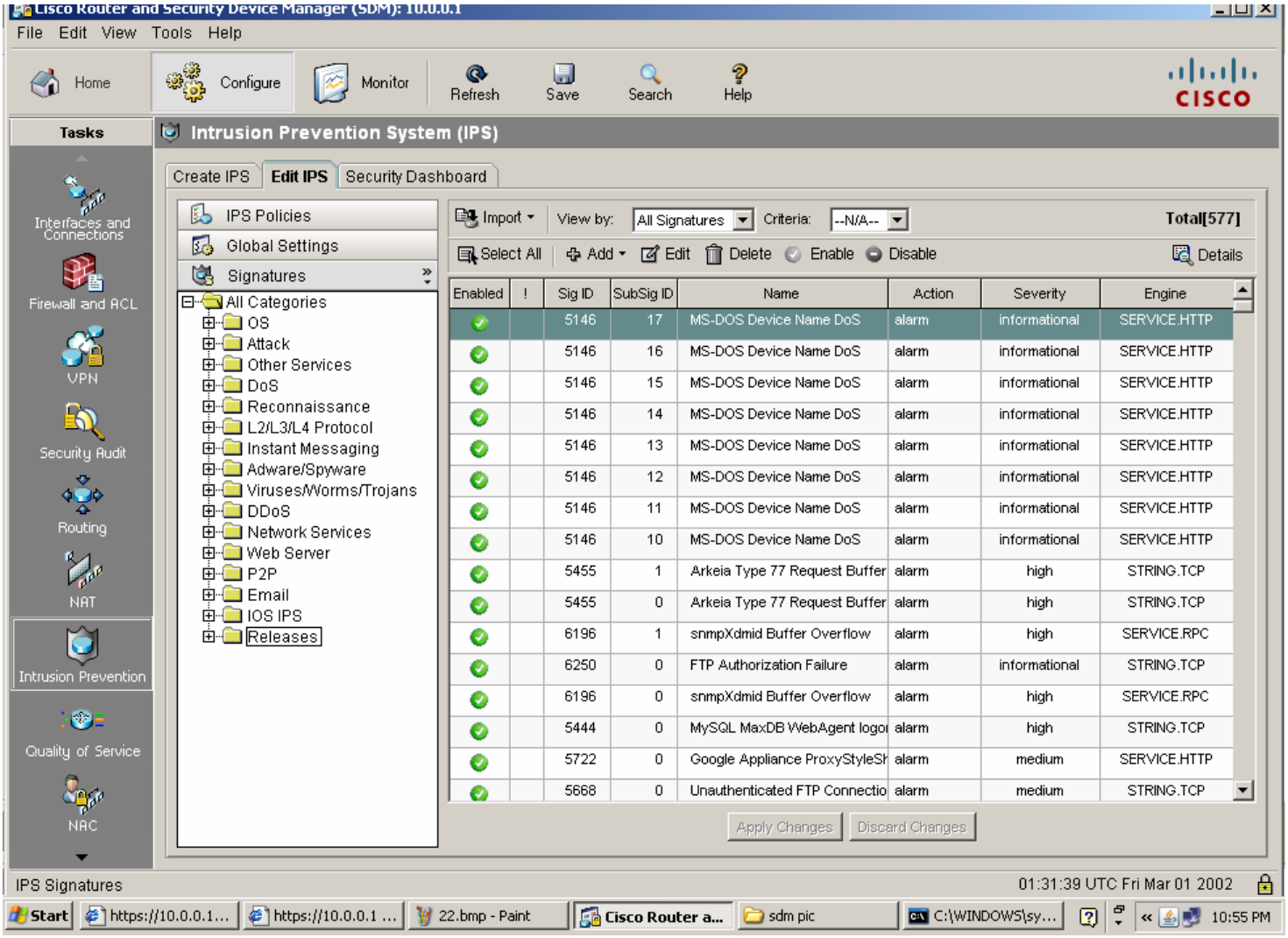
Step 1: Verify connectivity.

From PC-A, ping PC-B. The pings should be successful.

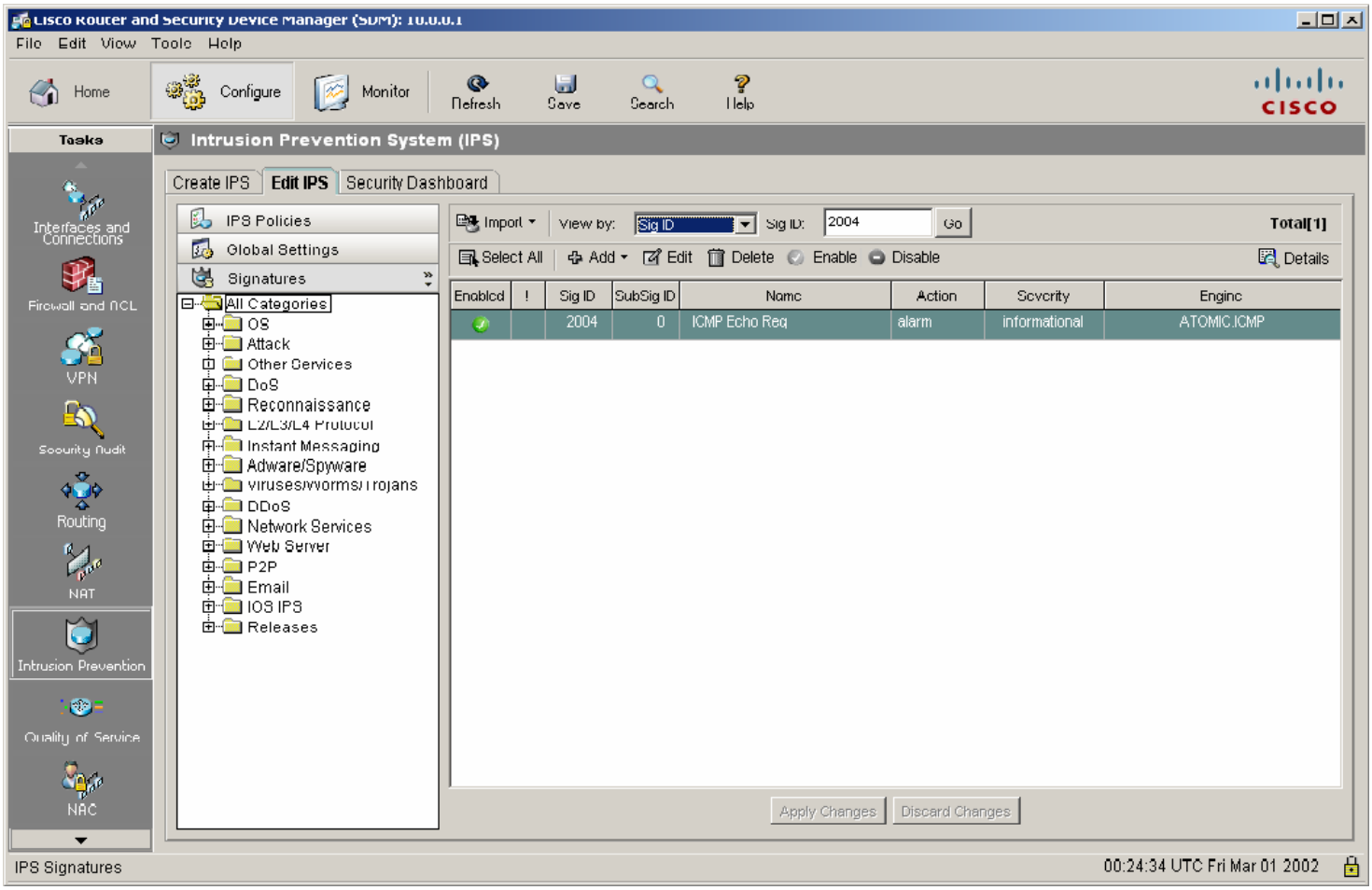


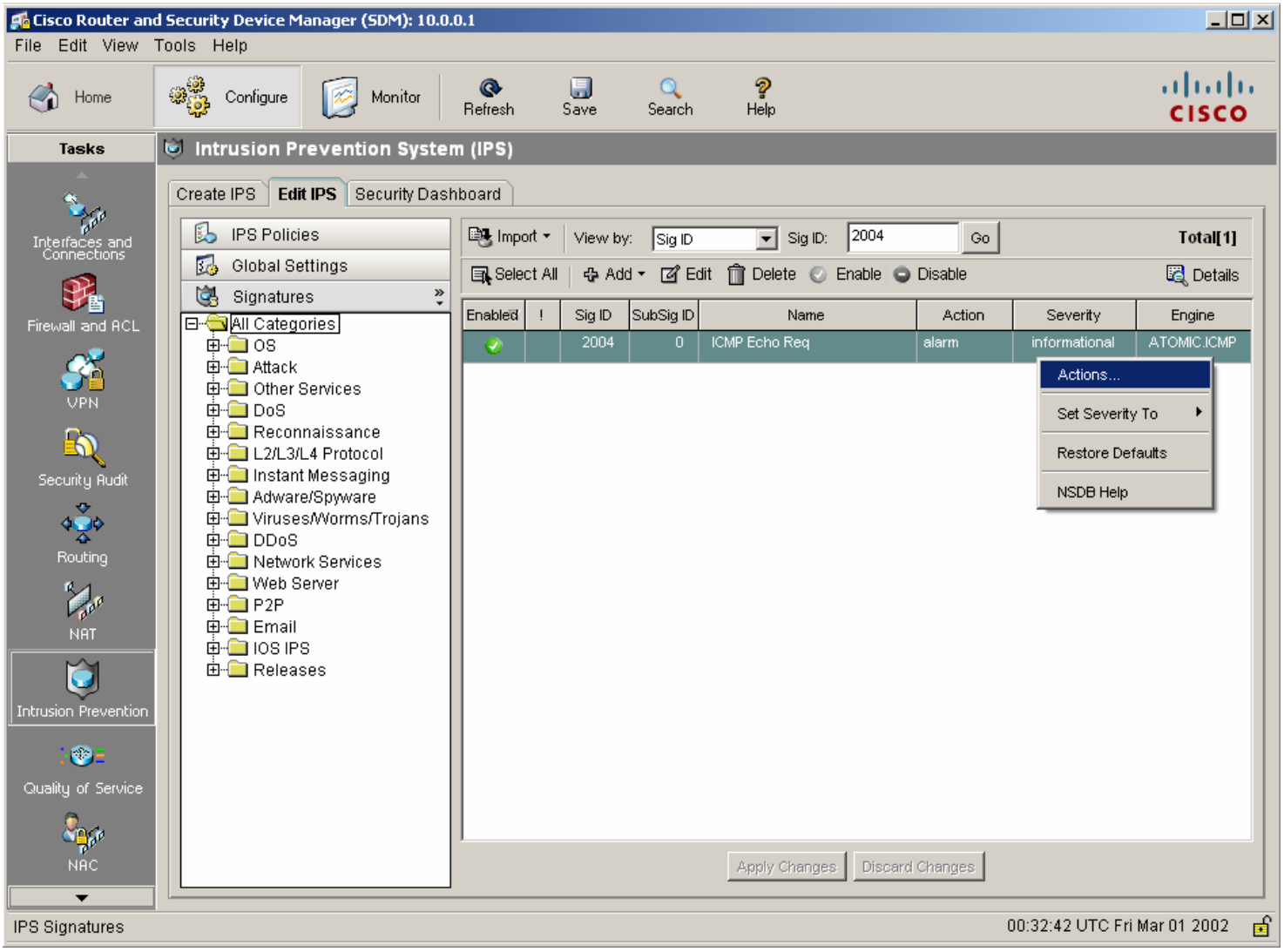
Step 2: Configure the IPS application to drop ping (echo request) traffic.

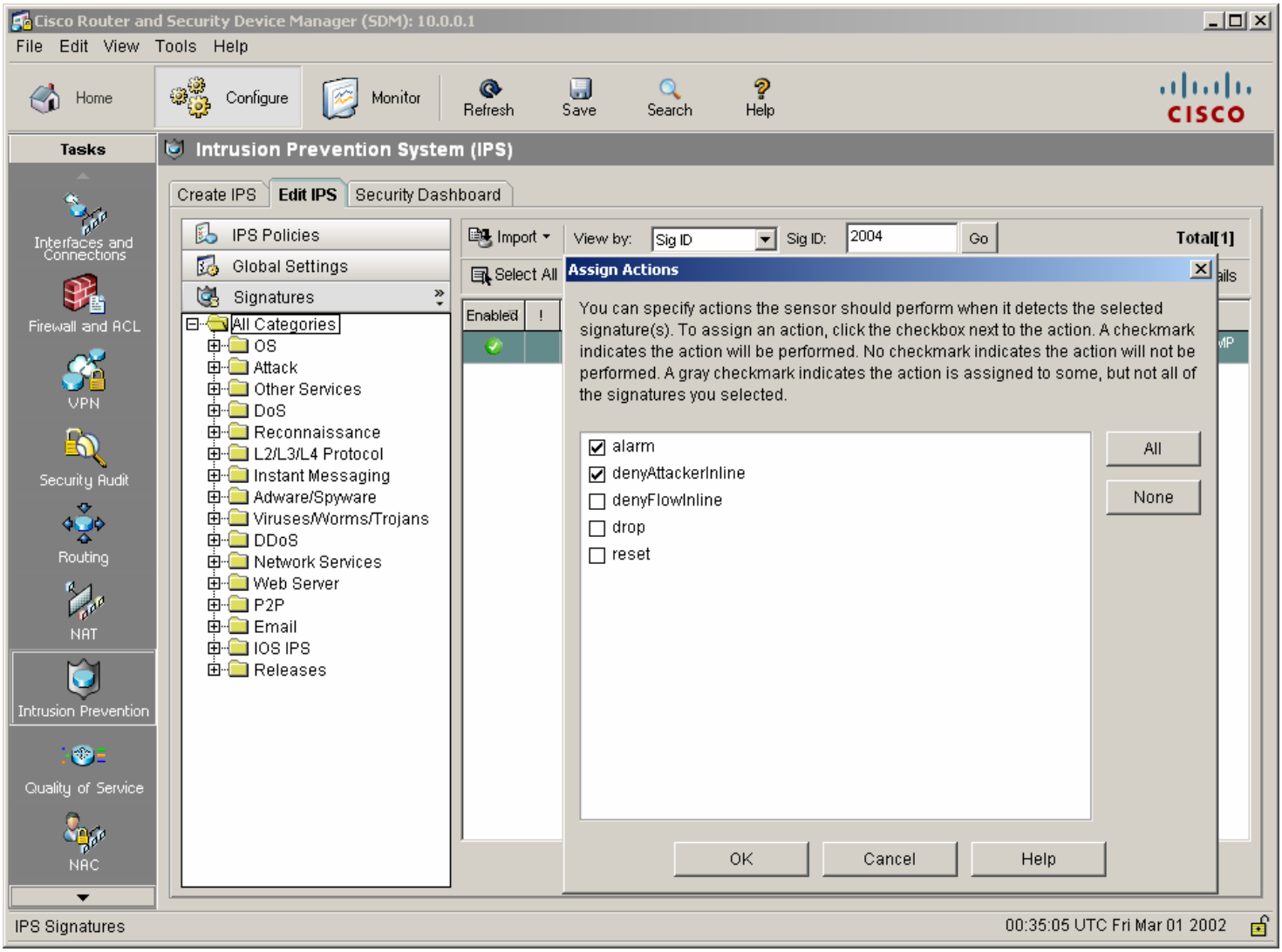
a. From SDM, click **Configure** and select **Intrusion Prevention > Edit IPS > Signatures**.

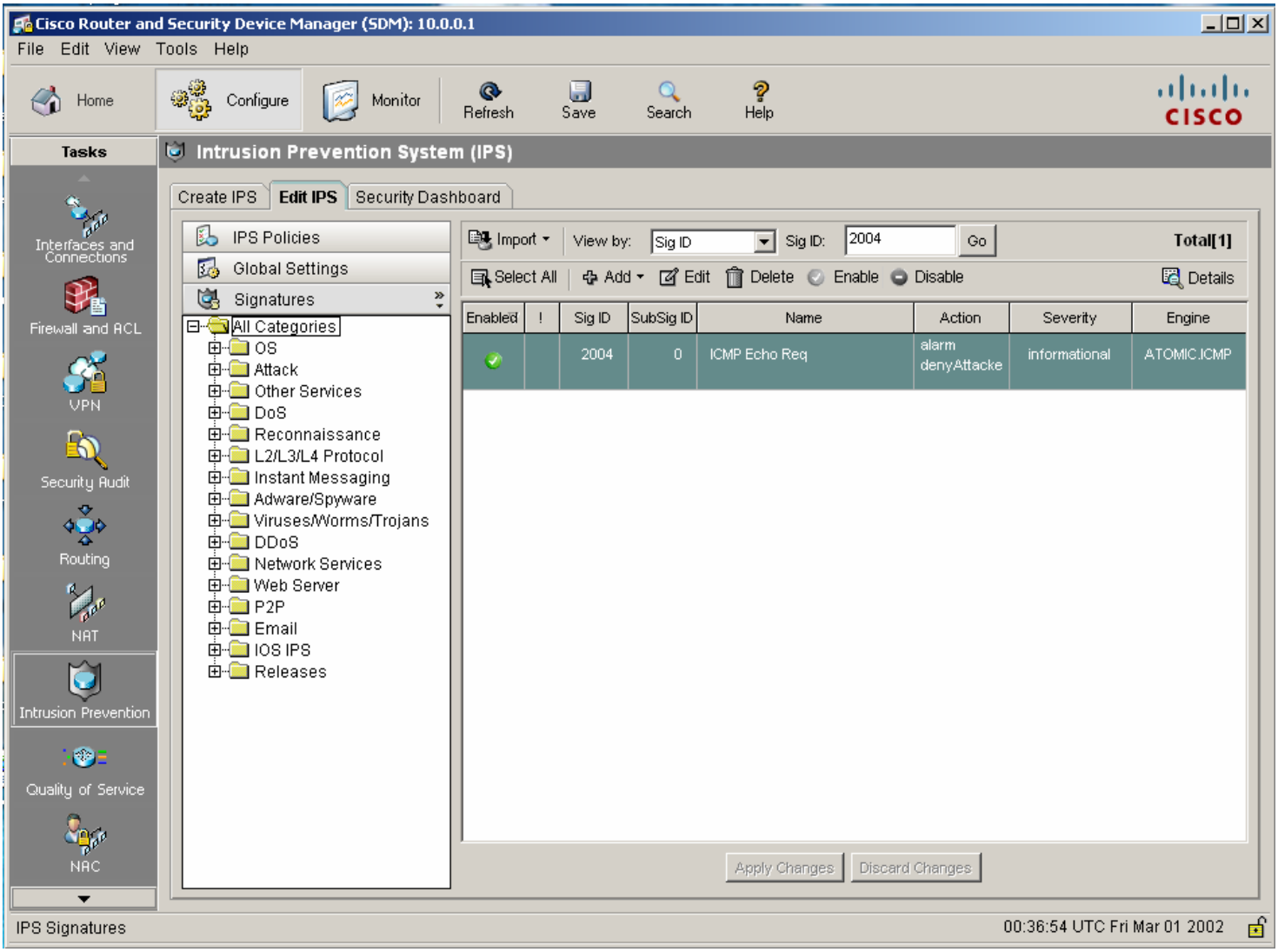


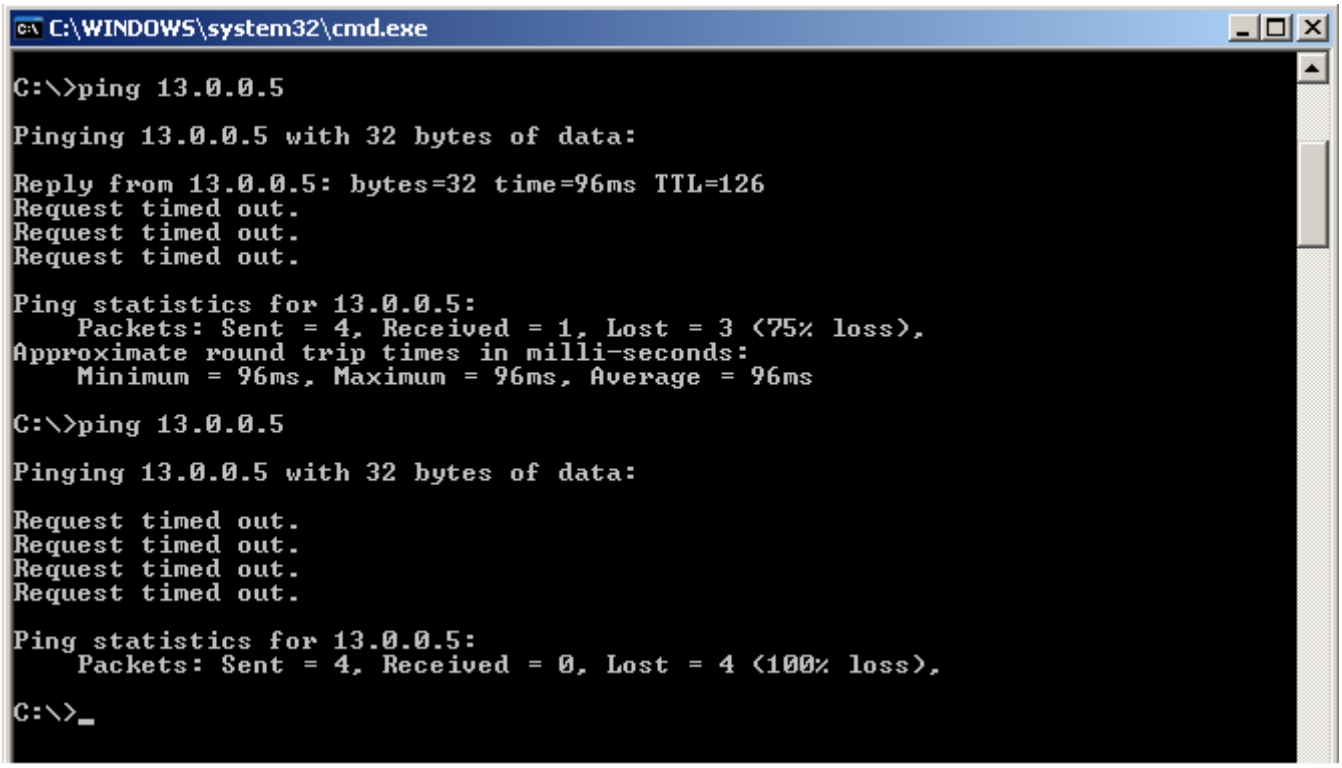
b. In the **View By** drop-down list, choose **Sig ID**.
c. In the **Sig ID** field, enter 2004, and then click **Go**.
d. Right-click the signature and choose **Actions** from the context menu.
e. Choose **Deny Packet Inline** and leave the **Produce Alert** check box checked. Click **OK**.
f. Click **Apply Changes**. Your screen should look similar to the following.

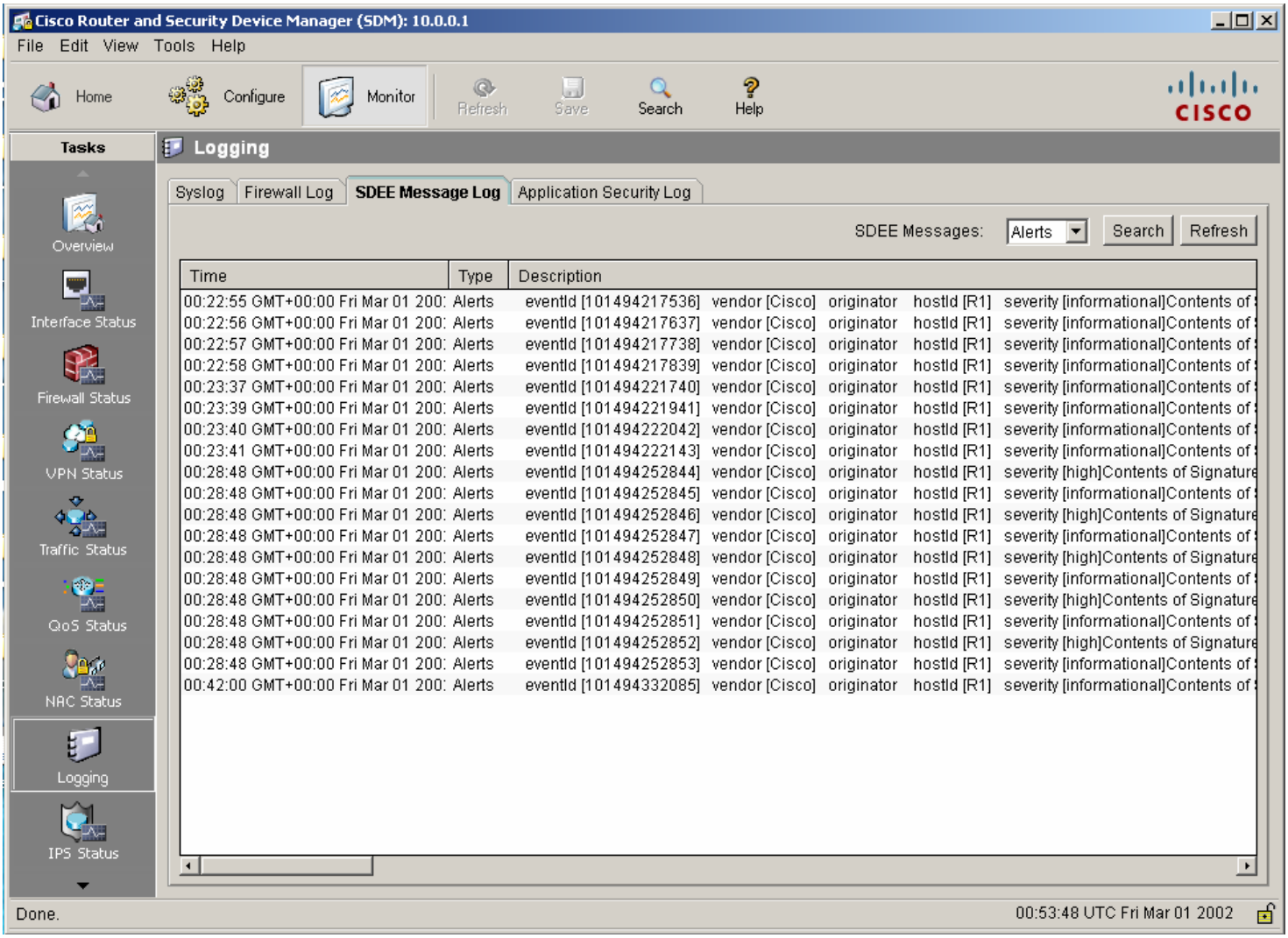

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by:
Sig ID
Sig ID:
2004
Go
Total[1]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled
!
Sig ID
SubSig ID
Name
Action
Severity
Engine
2004
0
ICMP Echo Req
alarm
informational
ATOMIC.ICMP
Apply Changes
Discard Changes
IPS Signatures
00:24:34 UTC Fri Mar 01 2002

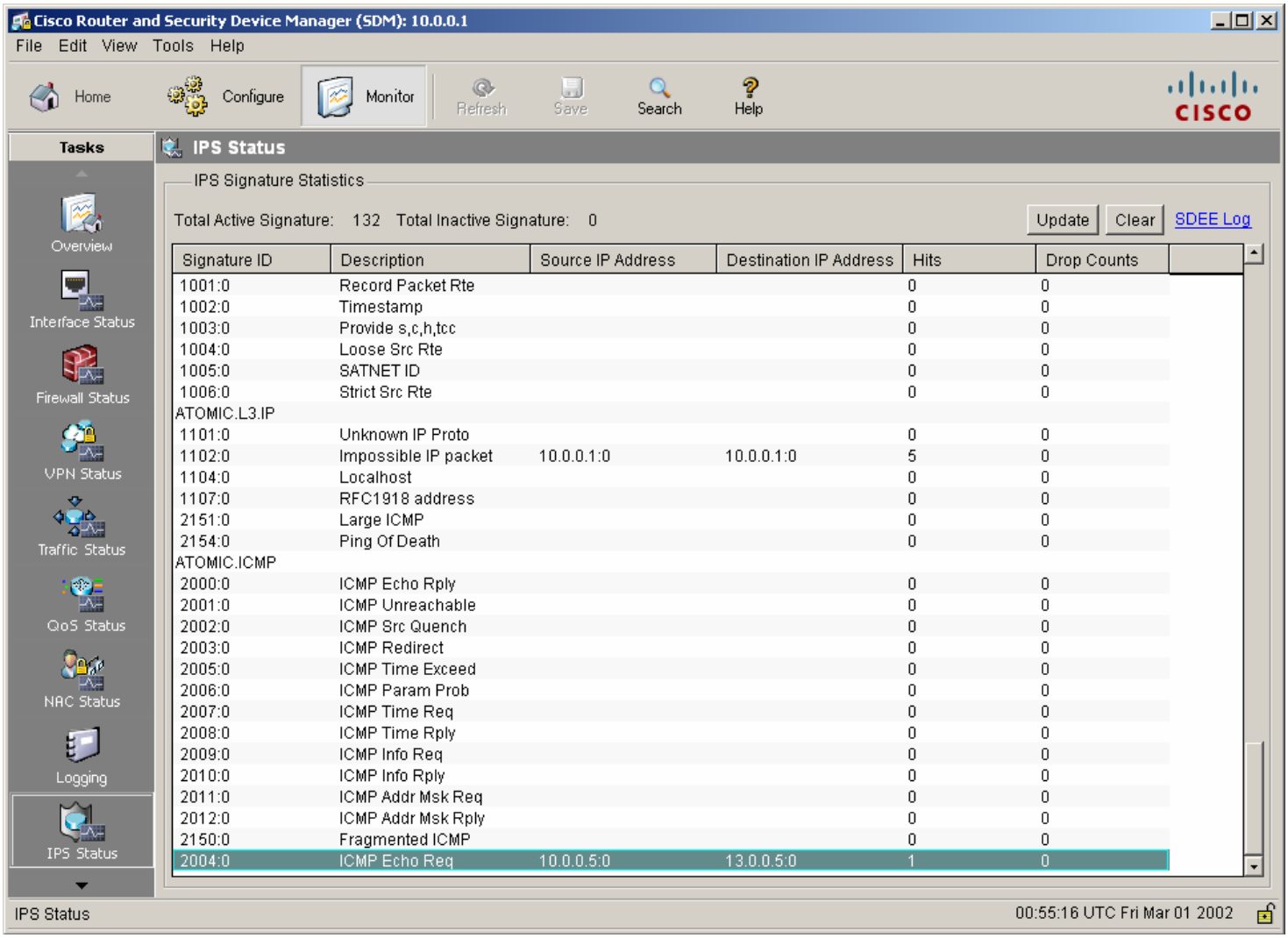

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by:
Sig ID
Sig ID:
2004
Go
Total[1]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled
!
Sig ID
SubSig ID
Name
Action
Severity
Engine
2004
0
ICMP Echo Req
alarm
informational
ATOMIC.ICMP
Actions...
Set Severity To
Restore Defaults
NSDB Help
Apply Changes
Discard Changes
IPS Signatures
00:32:42 UTC Fri Mar 01 2002

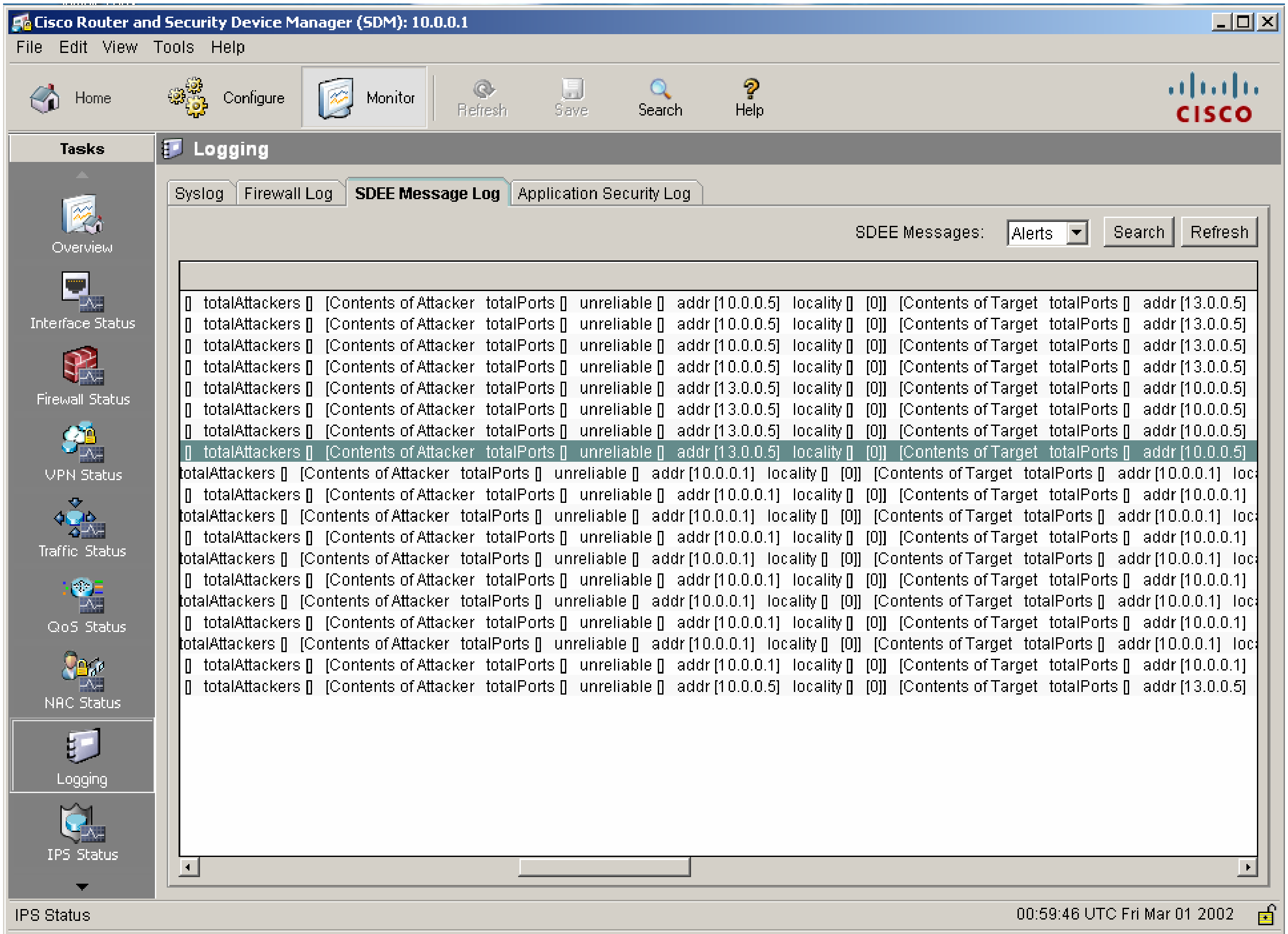

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by:
Sig ID
Sig ID:
2004
Go
Total[1]
Select All
Enabled
Assign Actions
You can specify actions the sensor should perform when it detects the selected signature(s). To assign an action, click the checkbox next to the action. A checkmark indicates the action will be performed. No checkmark indicates the action will not be performed. A gray checkmark indicates the action is assigned to some, but not all of the signatures you selected.
alarm
denyAttackerInline
denyFlowInline
drop
reset
All
None
OK
Cancel
Help
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
IPS Signatures
00:35:05 UTC Fri Mar 01 2002

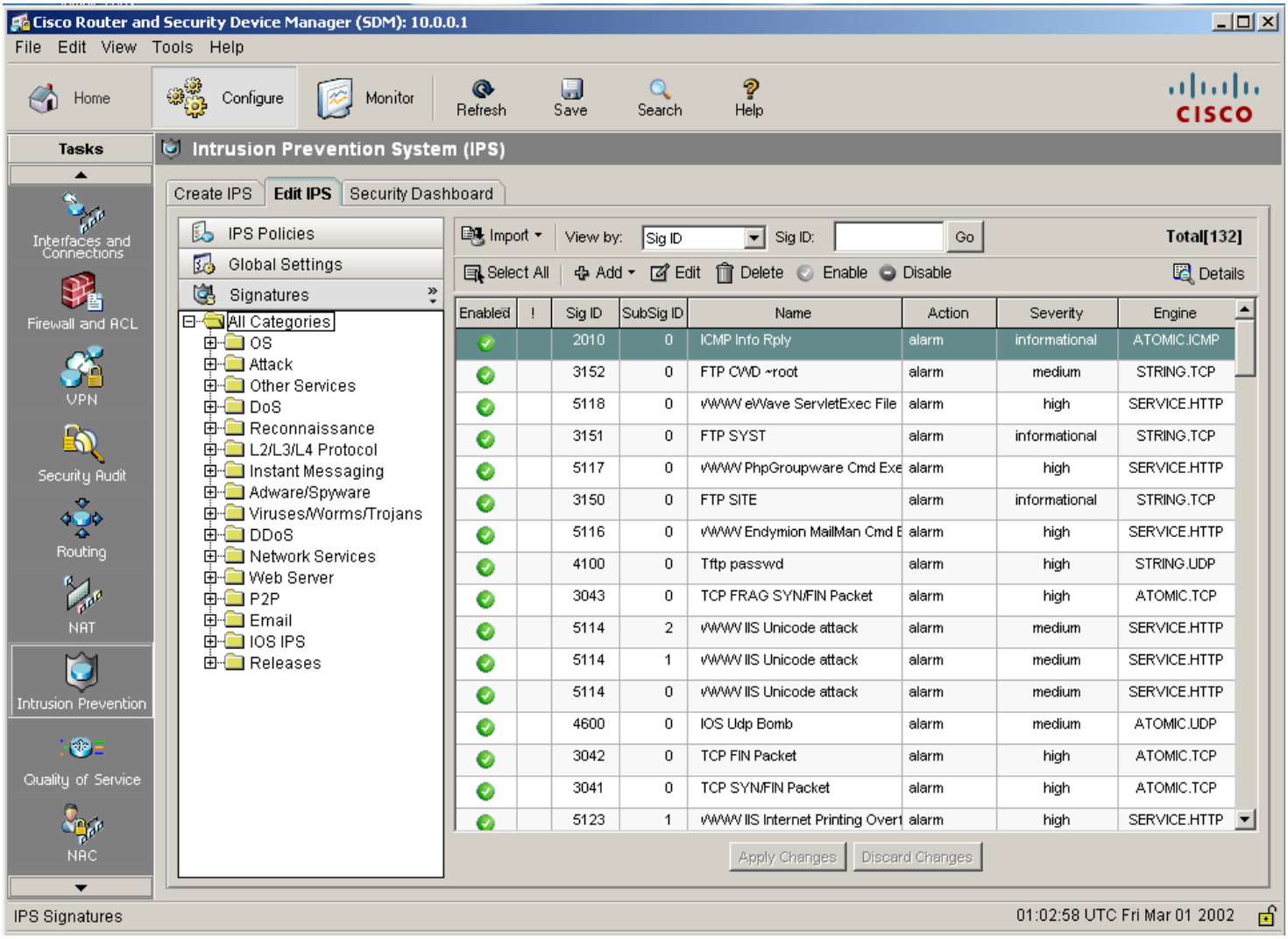

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by:
Sig ID
Sig ID:
2004
Go
Total[1]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled
!
Sig ID
SubSig ID
Name
Action
Severity
Engine
2004
0
ICMP Echo Req
alarm denyAttacke
informational
ATOMIC.ICMP
Apply Changes
Discard Changes
IPS Signatures
00:36:54 UTC Fri Mar 01 2002

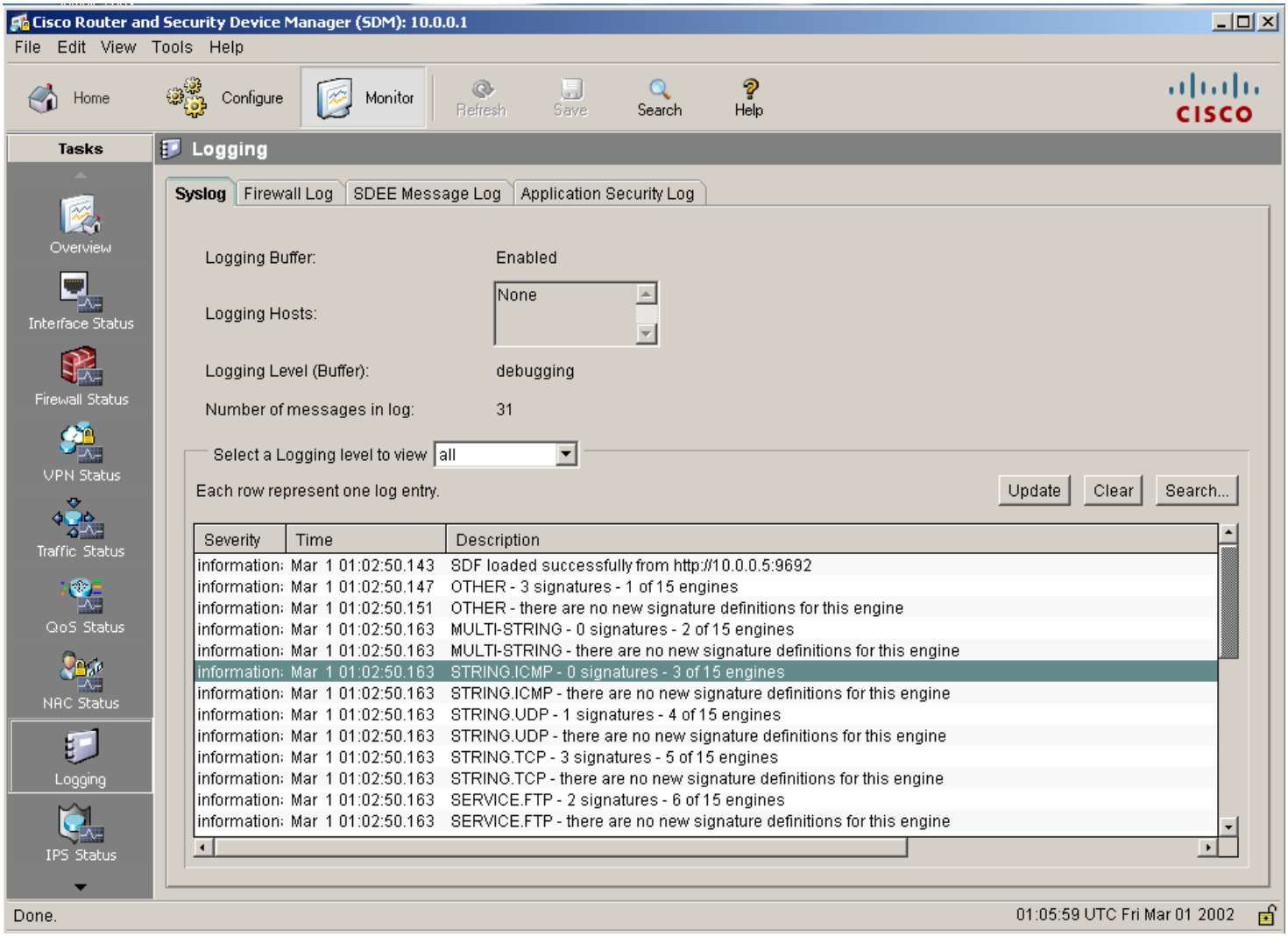

C:\WINDOWS\system32\cmd.exe
C:\>ping 13.0.0.5
Pinging 13.0.0.5 with 32 bytes of data:
Reply from 13.0.0.5: bytes=32 time=96ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 13.0.0.5:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
Minimum = 96ms, Maximum = 96ms, Average = 96ms
C:\>ping 13.0.0.5
Pinging 13.0.0.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 13.0.0.5:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

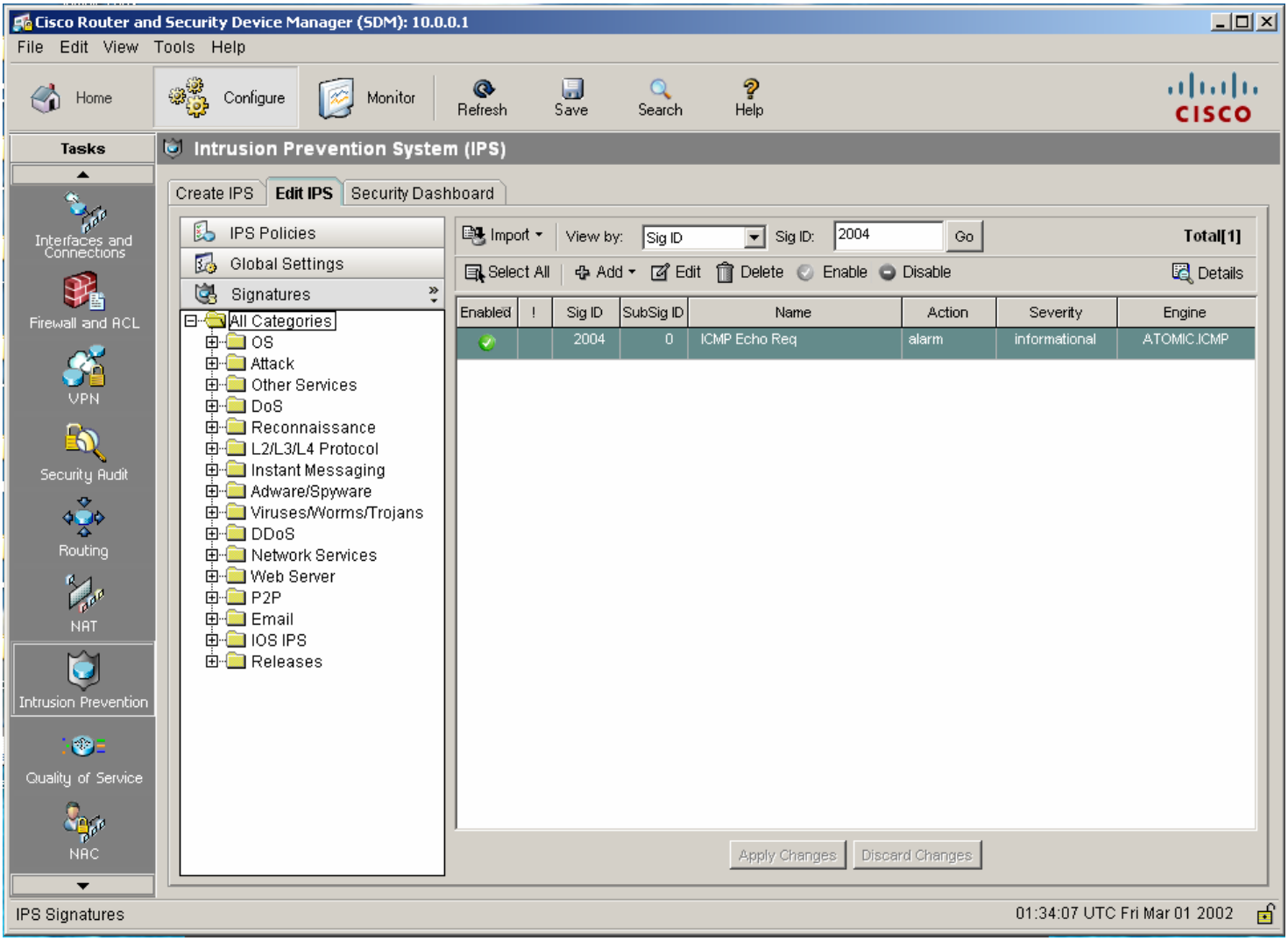

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
SDEE Messages:
Alerts
Search
Refresh
Time
Type
Description
00:22:55 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942175 36] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:56 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942176 37] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:57 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942177 38] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:58 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942178 39] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:37 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942217 40] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:39 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942219 41] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:40 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942220 42] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:41 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942221 43] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 44] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 45] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 46] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 47] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 48] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 49] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 50] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 51] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 52] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 53] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:42:00 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014943320 85] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
Done.
00:53:48 UTC Fri Mar 01 2002

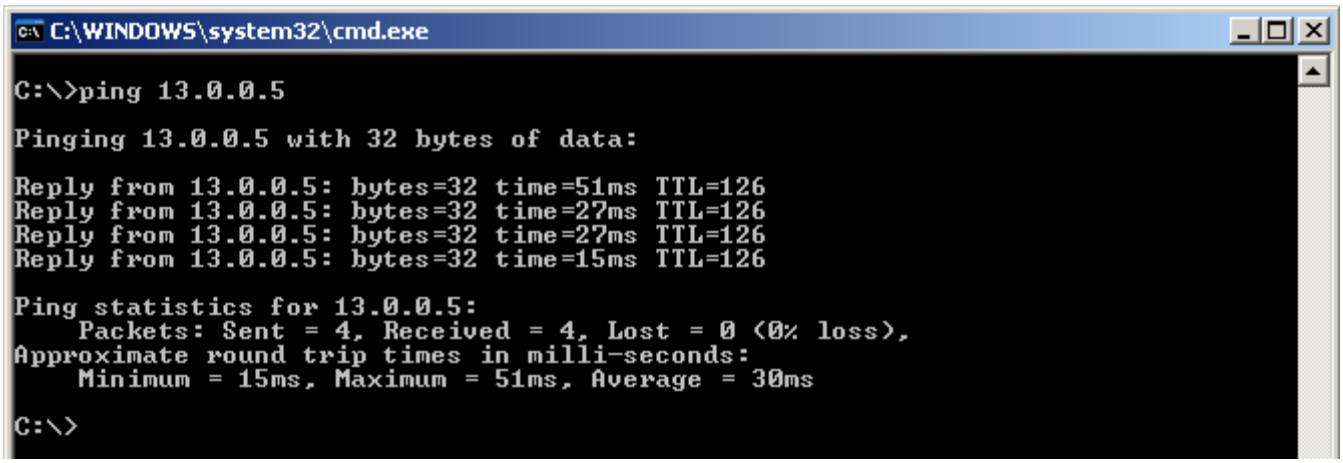

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
IPS Status
IPS Signature Statistics
Total Active Signature: 132 Total Inactive Signature: 0
Update
Clear
SDEE Log
Signature ID | Description | Source IP Address | Destination IP Address | Hits | Drop Counts
1001:0 | Record Packet Rte | | | 0 | 0
1002:0 | Timestamp | | | 0 | 0
1003:0 | Provide s,c,h,tcc | | | 0 | 0
1004:0 | Loose Src Rte | | | 0 | 0
1005:0 | SATNET ID | | | 0 | 0
1006:0 | Strict Src Rte | | | 0 | 0
ATOMIC.L3.IP
1101:0 | Unknown IP Proto | | | 0 | 0
1102:0 | Impossible IP packet | 10.0.0.1:0 | 10.0.0.1:0 | 5 | 0
1104:0 | Localhost | | | 0 | 0
1107:0 | RFC1918 address | | | 0 | 0
2151:0 | Large ICMP | | | 0 | 0
2154:0 | Ping Of Death | | | 0 | 0
ATOMIC.ICMP
2000:0 | ICMP Echo Rply | | | 0 | 0
2001:0 | ICMP Unreachable | | | 0 | 0
2002:0 | ICMP Src Quench | | | 0 | 0
2003:0 | ICMP Redirect | | | 0 | 0
2005:0 | ICMP Time Exceed | | | 0 | 0
2006:0 | ICMP Param Prob | | | 0 | 0
2007:0 | ICMP Time Req | | | 0 | 0
2008:0 | ICMP Time Rply | | | 0 | 0
2009:0 | ICMP Info Req | | | 0 | 0
2010:0 | ICMP Info Rply | | | 0 | 0
2011:0 | ICMP Addr Msk Req | | | 0 | 0
2012:0 | ICMP Addr Msk Rply | | | 0 | 0
2150:0 | Fragmented ICMP | | | 0 | 0
2004:0 | ICMP Echo Req | 10.0.0.5:0 | 13.0.0.5:0 | 1 | 0
IPS Status
00:55:16 UTC Fri Mar 01 2002

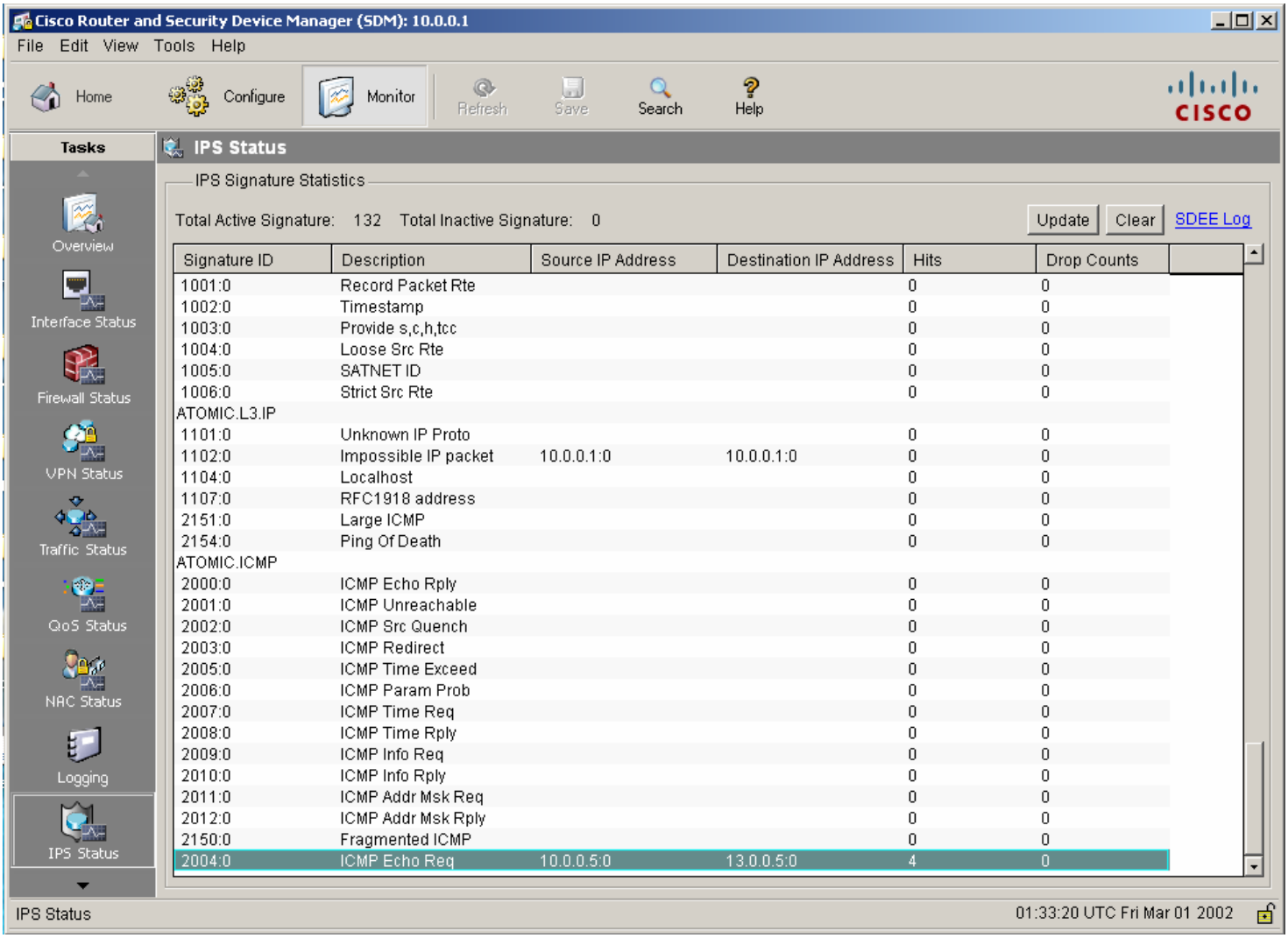

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Logging
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Syslog
Firewall Log
SDEE Message Log
Application Security Log
SDEE Messages:
Alerts
Search
Refresh
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
IPS Status
00:59:46 UTC Fri Mar 01 2002

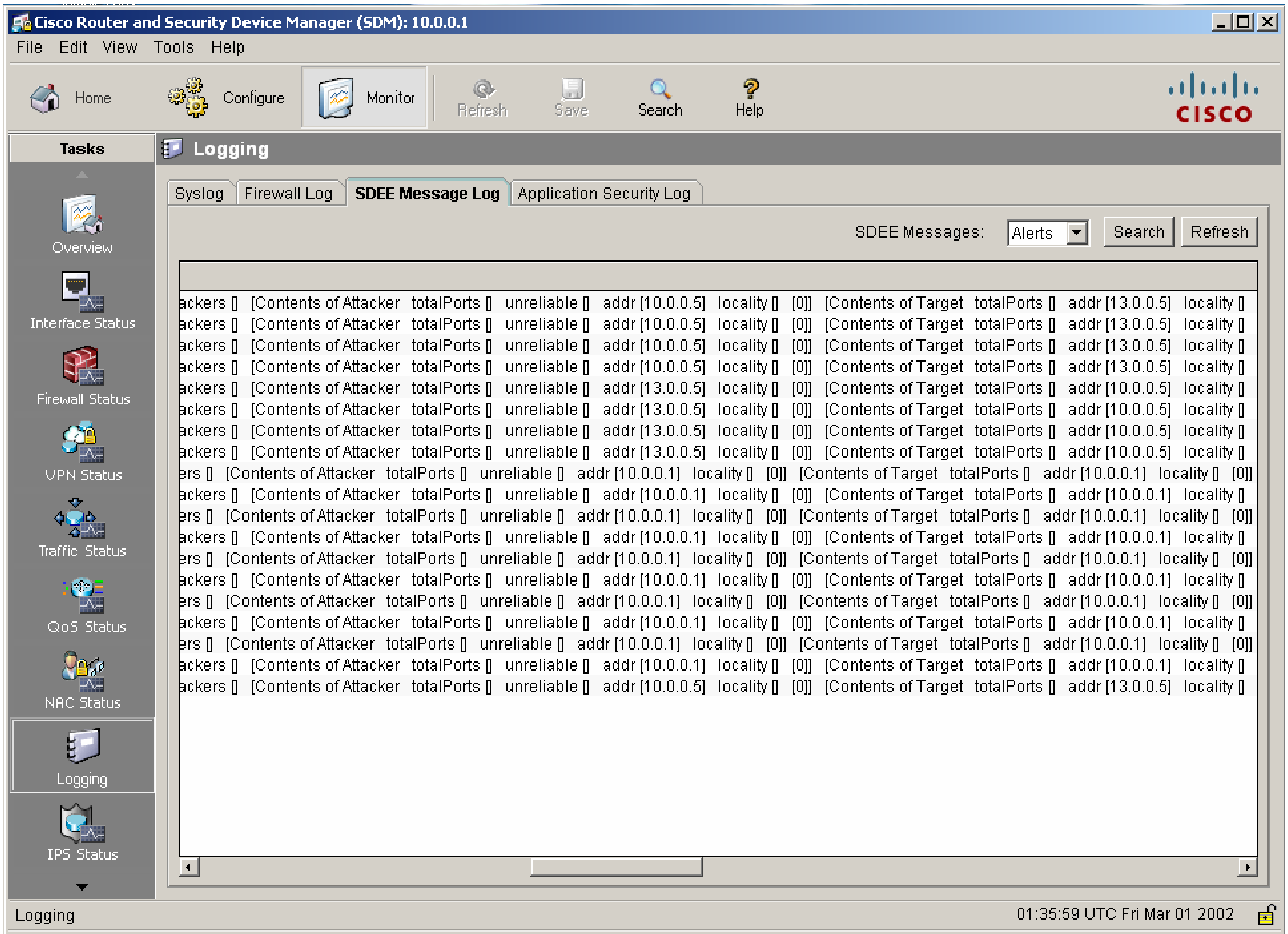

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by: Sig ID
Sig ID:
Go
Total[132]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled ! Sig ID SubSig ID Name Action Severity Engine
2010 0 ICMP Info Rply alarm informational ATOMIC.ICMP
3152 0 FTP CWD ~root alarm medium STRING.TCP
5118 0 WWW eWave ServletExec File alarm high SERVICE.HTTP
3151 0 FTP SYST alarm informational STRING.TCP
5117 0 WWW PhpGroupware Cmd Exe alarm high SERVICE.HTTP
3150 0 FTP SITE alarm informational STRING.TCP
5116 0 WWW Endymion MailMan Cmd E alarm high SERVICE.HTTP
4100 0 Tftp passwd alarm high STRING.UDP
3043 0 TCP FRAG SYN/FIN Packet alarm high ATOMIC.TCP
5114 2 WWW IIS Unicode attack alarm medium SERVICE.HTTP
5114 1 WWW IIS Unicode attack alarm medium SERVICE.HTTP
5114 0 WWW IIS Unicode attack alarm medium SERVICE.HTTP
4600 0 IOS Udp Bomb alarm medium ATOMIC.UDP
3042 0 TCP FIN Packet alarm high ATOMIC.TCP
3041 0 TCP SYN/FIN Packet alarm high ATOMIC.TCP
5123 1 WWW IIS Internet Printing Overf alarm high SERVICE.HTTP
Apply Changes
Discard Changes
IPS Signatures
01:02:58 UTC Fri Mar 01 2002

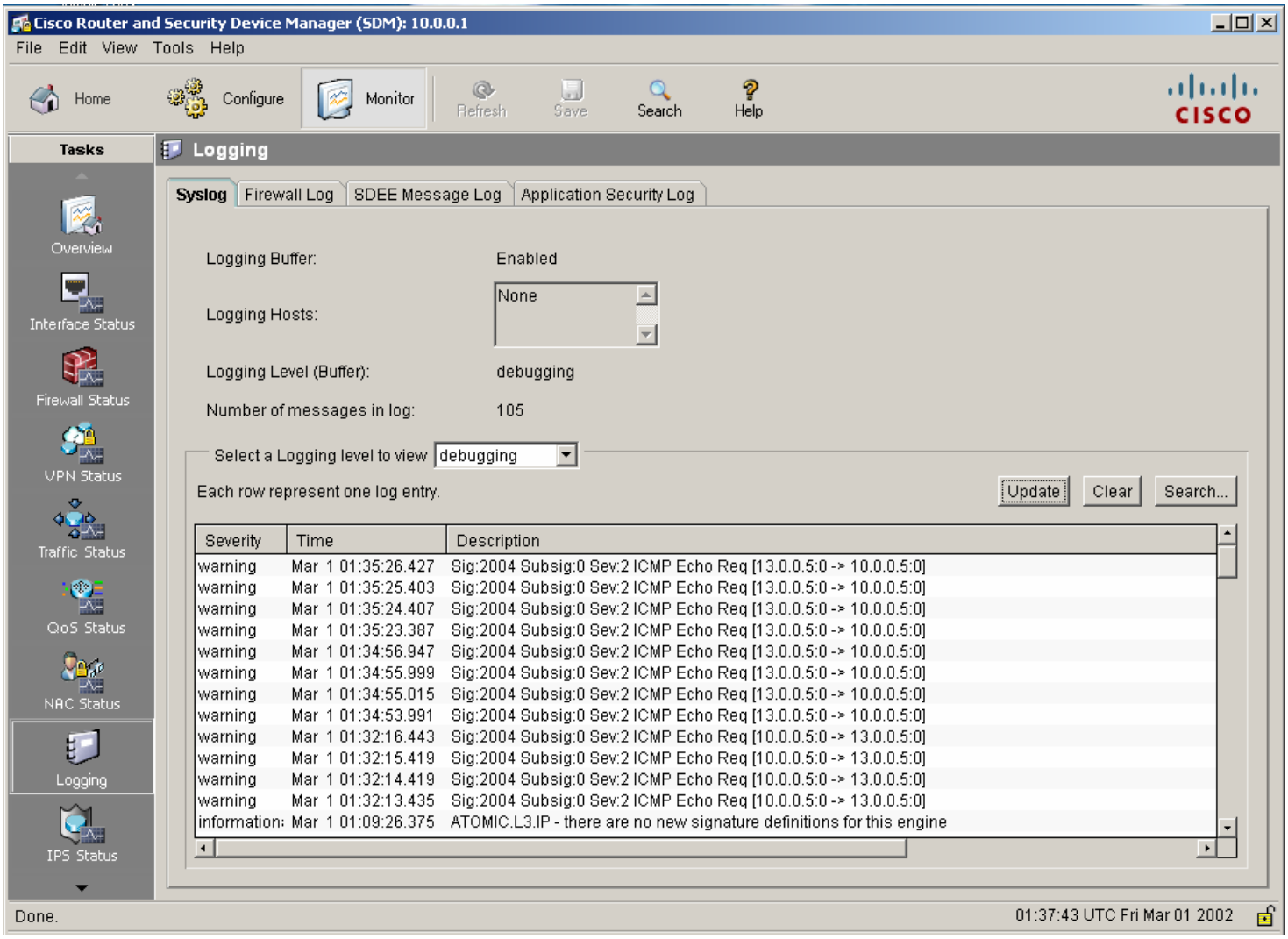

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 31
Select a Logging level to view all
Each row represent one log entry.
Update
Clear
Search...
Severity Time Description
information: Mar 1 01:02:50.143 SDF loaded successfully from http://10.0.0.5:9692
information: Mar 1 01:02:50.147 OTHER - 3 signatures - 1 of 15 engines
information: Mar 1 01:02:50.151 OTHER - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 MULTI-STRING - 0 signatures - 2 of 15 engines
information: Mar 1 01:02:50.163 MULTI-STRING - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.ICMP - 0 signatures - 3 of 15 engines
information: Mar 1 01:02:50.163 STRING.ICMP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.UDP - 1 signatures - 4 of 15 engines
information: Mar 1 01:02:50.163 STRING.UDP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.TCP - 3 signatures - 5 of 15 engines
information: Mar 1 01:02:50.163 STRING.TCP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 SERVICE.FTP - 2 signatures - 6 of 15 engines
information: Mar 1 01:02:50.163 SERVICE.FTP - there are no new signature definitions for this engine
Done.
01:05:59 UTC Fri Mar 01 2002

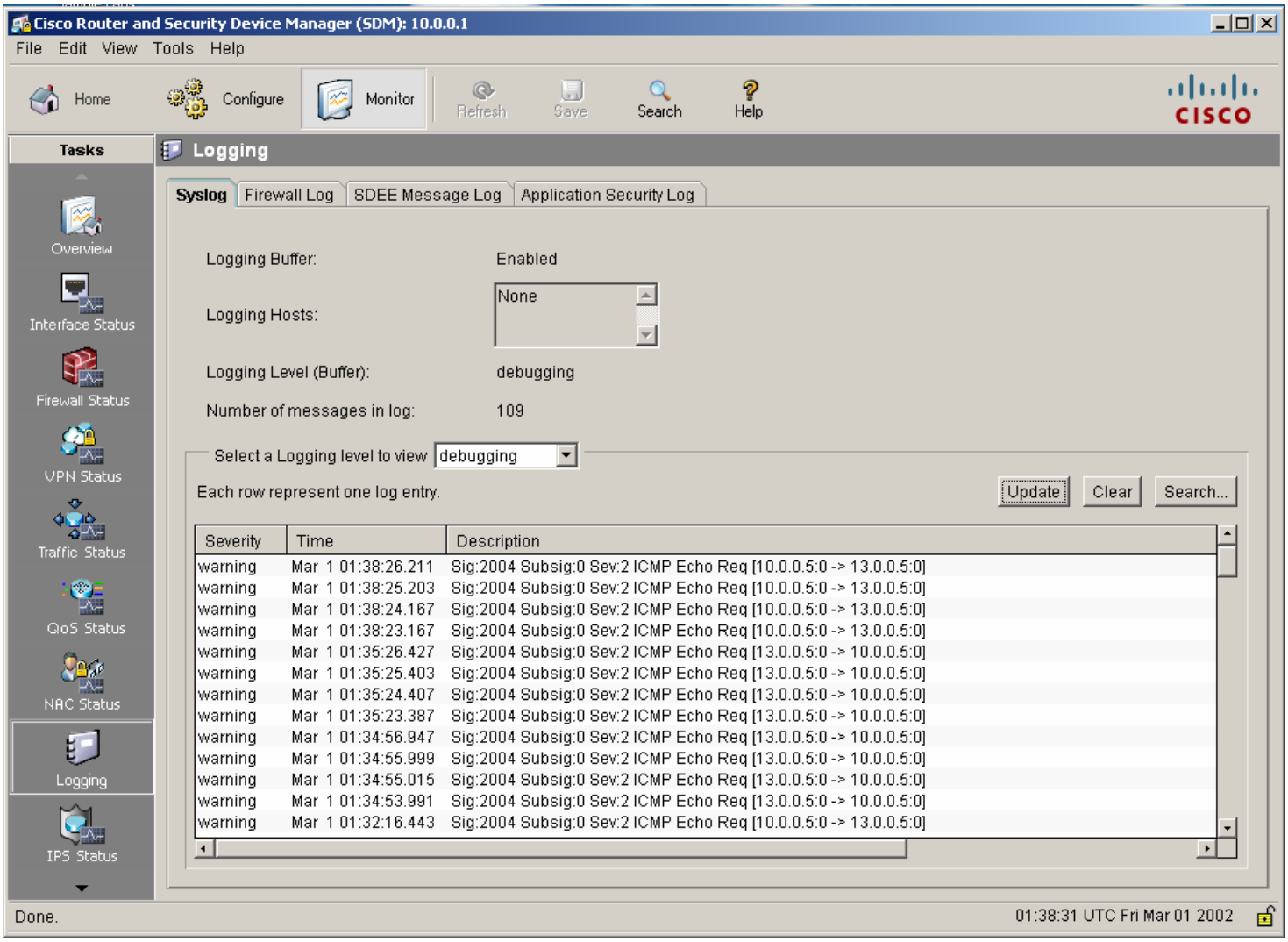

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by: Sig ID
Sig ID: 2004
Go
Total[1]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled ! Sig ID SubSig ID Name Action Severity Engine
2004 0 ICMP Echo Req alarm informational ATOMIC.ICMP
Apply Changes
Discard Changes
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
IPS Signatures
01:34:07 UTC Fri Mar 01 2002

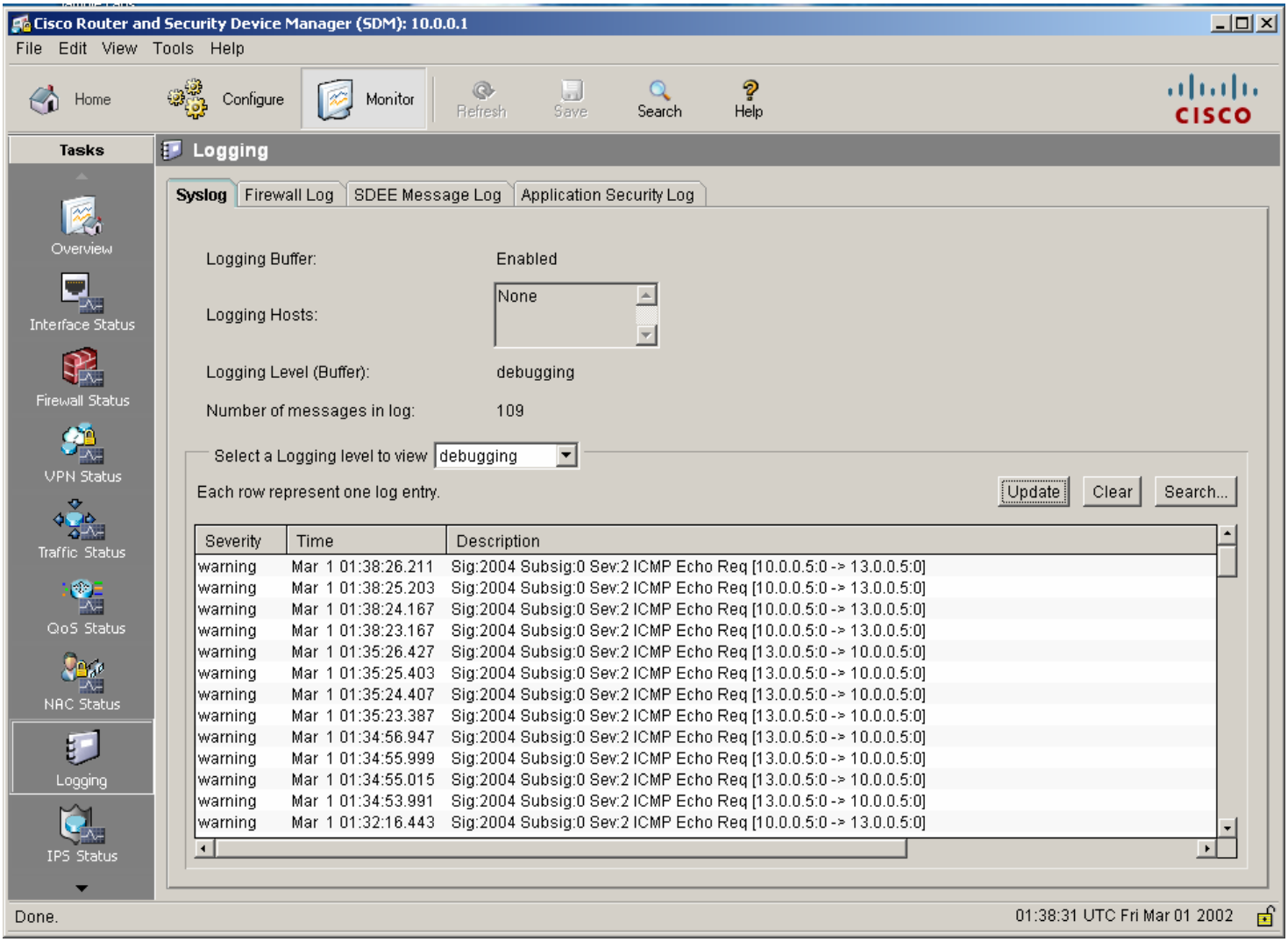

C:\WINDOWS\system32\cmd.exe
C:\>ping 13.0.0.5
Pinging 13.0.0.5 with 32 bytes of data:
Reply from 13.0.0.5: bytes=32 time=51ms TTL=126
Reply from 13.0.0.5: bytes=32 time=27ms TTL=126
Reply from 13.0.0.5: bytes=32 time=27ms TTL=126
Reply from 13.0.0.5: bytes=32 time=15ms TTL=126
Ping statistics for 13.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 15ms, Maximum = 51ms, Average = 30ms
C:\>

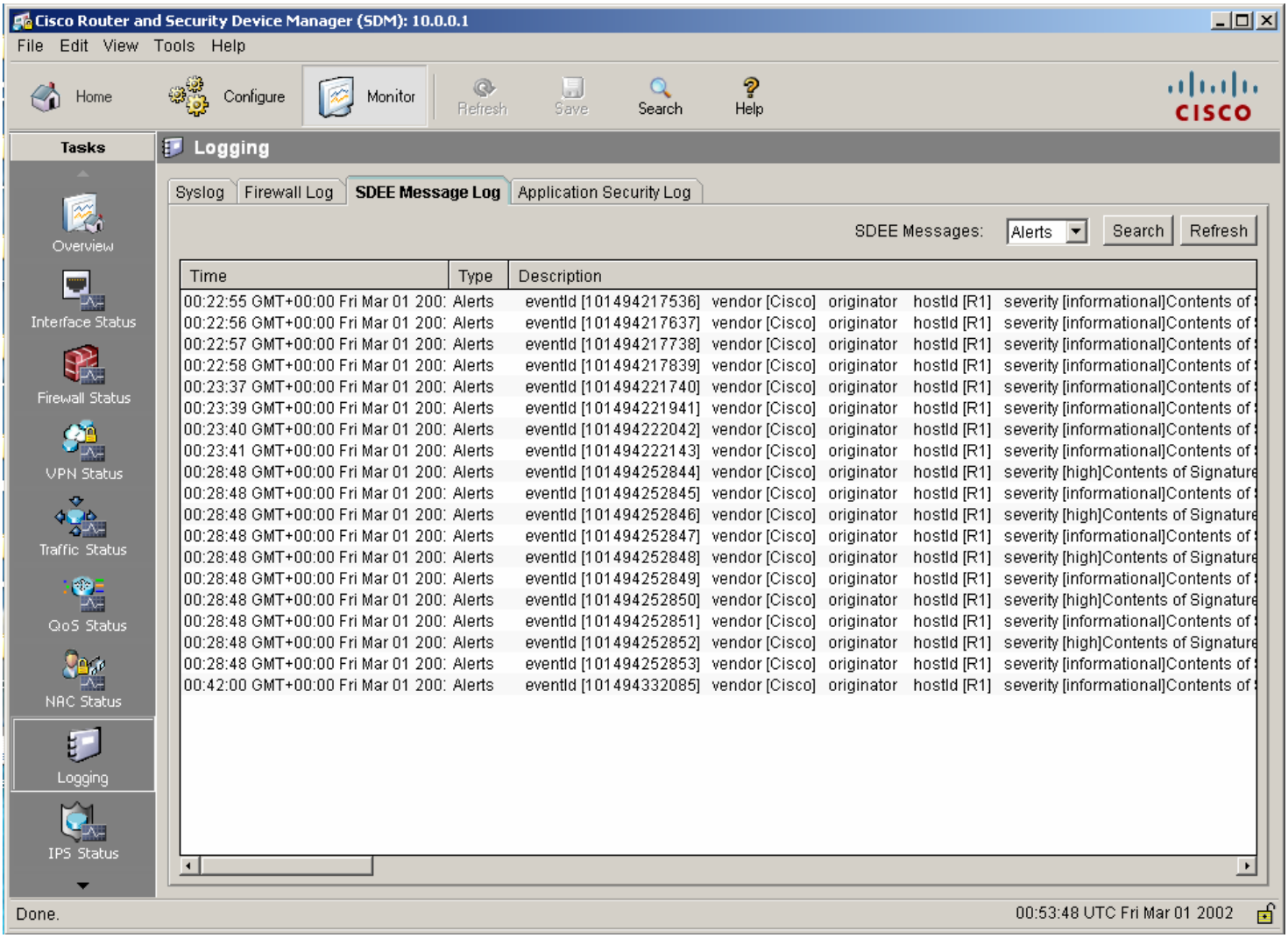

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
IPS Status
IPS Signature Statistics
Total Active Signature: 132 Total Inactive Signature: 0
Update
Clear
SDEE Log
Signature ID | Description | Source IP Address | Destination IP Address | Hits | Drop Counts
1001:0 | Record Packet Rte | | | 0 | 0
1002:0 | Timestamp | | | 0 | 0
1003:0 | Provide s,c,h,tcc | | | 0 | 0
1004:0 | Loose Src Rte | | | 0 | 0
1005:0 | SATNET ID | | | 0 | 0
1006:0 | Strict Src Rte | | | 0 | 0
ATOMIC.L3.IP
1101:0 | Unknown IP Proto | | | 0 | 0
1102:0 | Impossible IP packet | 10.0.0.1:0 | 10.0.0.1:0 | 0 | 0
1104:0 | Localhost | | | 0 | 0
1107:0 | RFC1918 address | | | 0 | 0
2151:0 | Large ICMP | | | 0 | 0
2154:0 | Ping Of Death | | | 0 | 0
ATOMIC.ICMP
2000:0 | ICMP Echo Rply | | | 0 | 0
2001:0 | ICMP Unreachable | | | 0 | 0
2002:0 | ICMP Src Quench | | | 0 | 0
2003:0 | ICMP Redirect | | | 0 | 0
2005:0 | ICMP Time Exceed | | | 0 | 0
2006:0 | ICMP Param Prob | | | 0 | 0
2007:0 | ICMP Time Req | | | 0 | 0
2008:0 | ICMP Time Rply | | | 0 | 0
2009:0 | ICMP Info Req | | | 0 | 0
2010:0 | ICMP Info Rply | | | 0 | 0
2011:0 | ICMP Addr Msk Req | | | 0 | 0
2012:0 | ICMP Addr Msk Rply | | | 0 | 0
2150:0 | Fragmented ICMP | | | 0 | 0
2004:0 | ICMP Echo Req | 10.0.0.5:0 | 13.0.0.5:0 | 4 | 0
IPS Status
01:33:20 UTC Fri Mar 01 2002

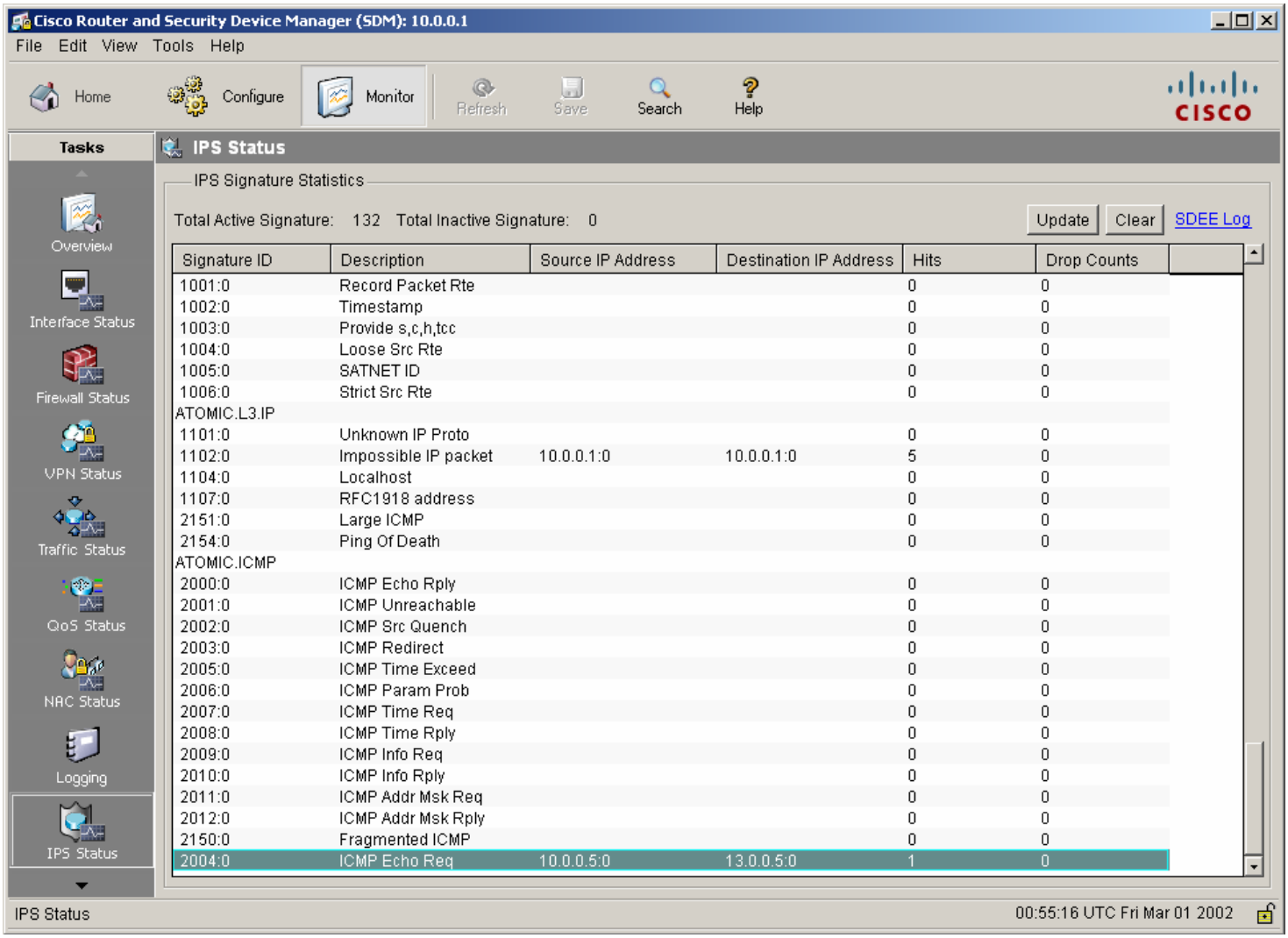

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Logging
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Syslog
Firewall Log
SDEE Message Log
Application Security Log
SDEE Messages:
Alerts
Search
Refresh
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5] locality []
ers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality [] [0]]
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality []
ers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality [] [0]]
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality []
ers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality [] [0]]
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality []
ers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality [] [0]]
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality []
ers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality [] [0]]
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] locality []
ackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5] locality []
Logging
01:35:59 UTC Fri Mar 01 2002

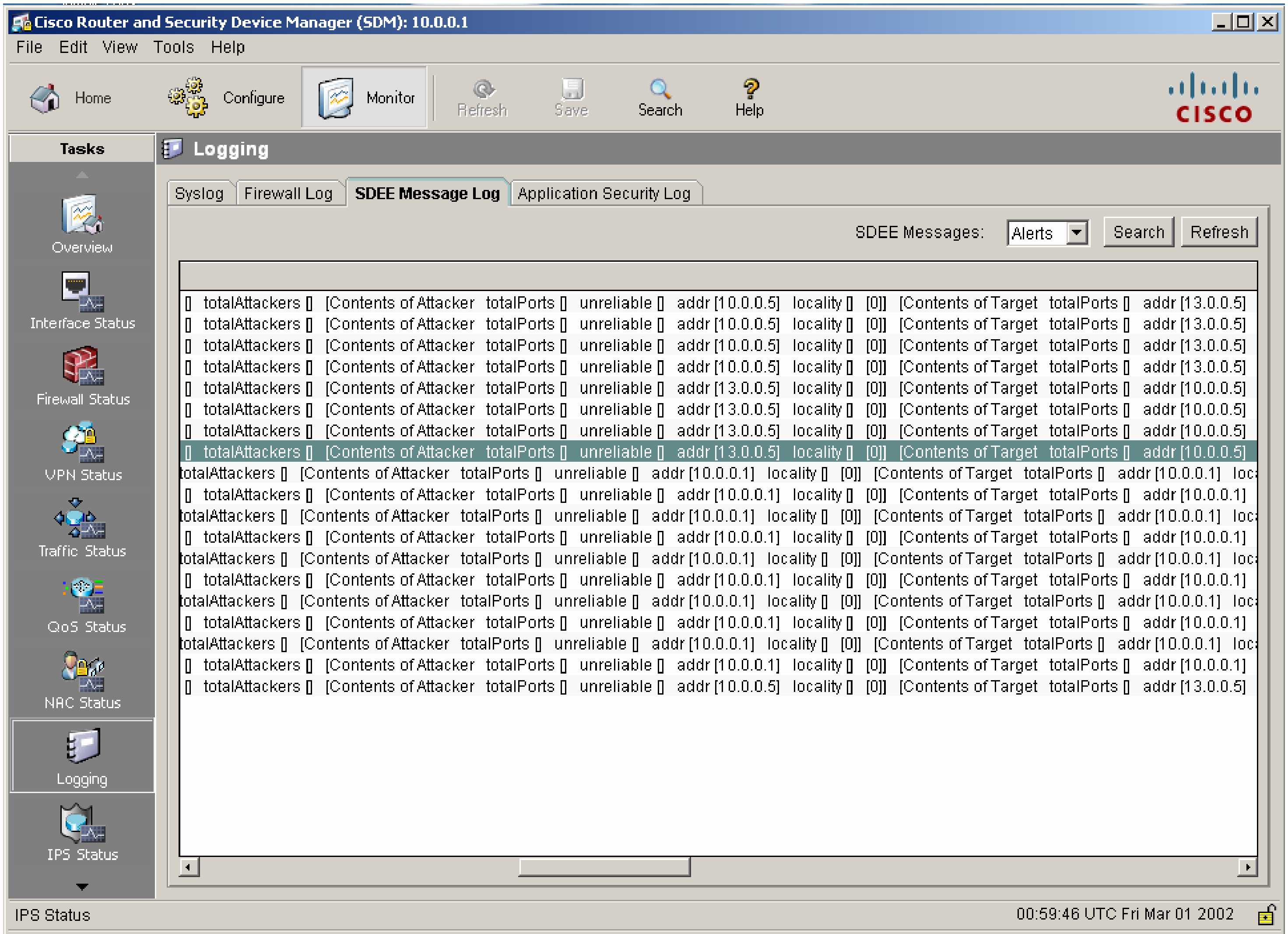

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 105
Select a Logging level to view debugging
Each row represent one log entry.
Update
Clear
Search...
Severity Time Description
warning Mar 1 01:35:26.427 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:25.403 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:24.407 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:23.387 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:56.947 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.999 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.015 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:53.991 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:32:16.443 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:32:15.419 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:32:14.419 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:32:13.435 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
information: Mar 1 01:09:26.375 ATOMIC.L3.IP - there are no new signature definitions for this engine
Done.
01:37:43 UTC Fri Mar 01 2002

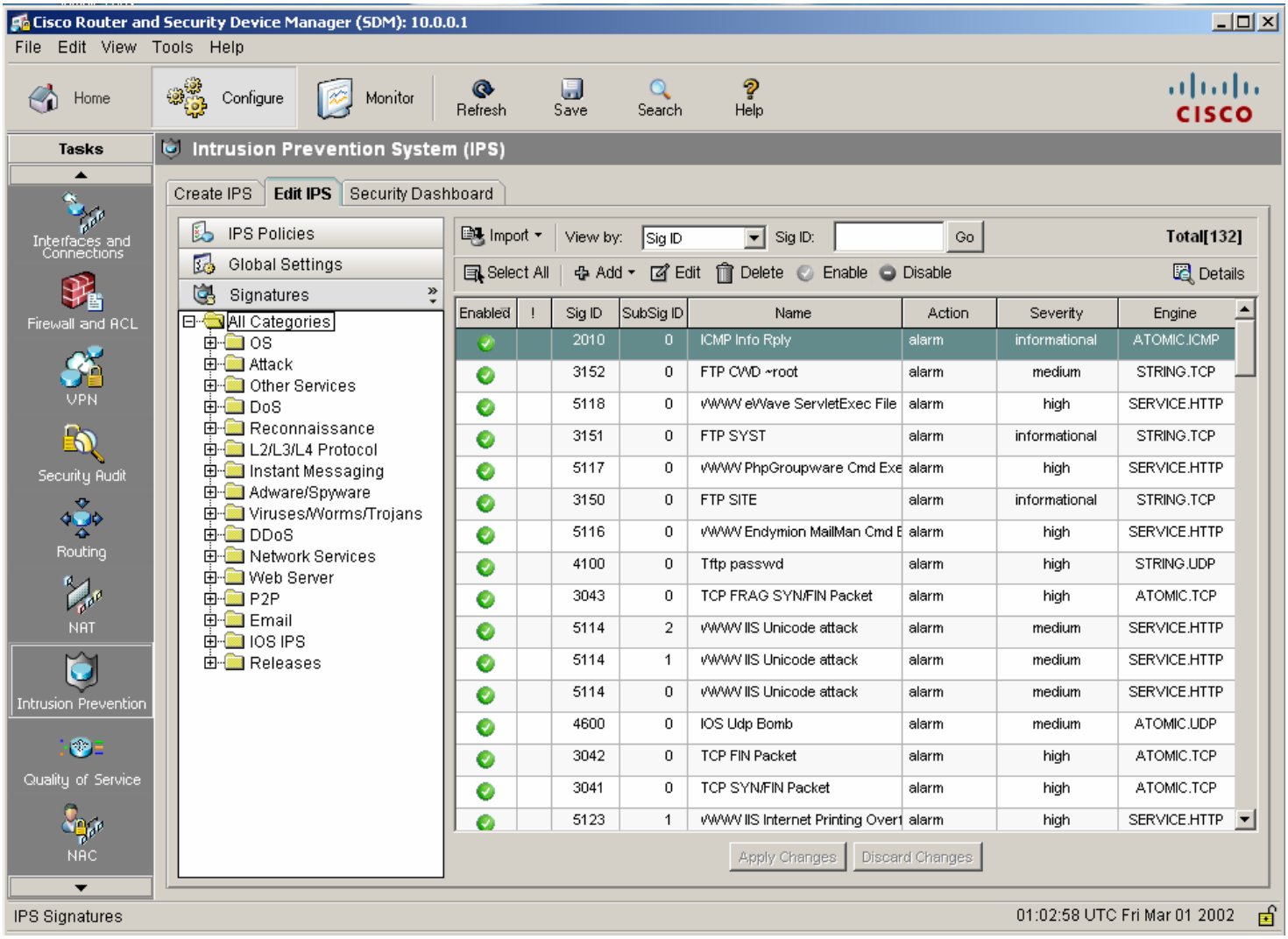

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 109
Select a Logging level to view debugging
Each row represent one log entry.
Update
Clear
Search...
Severity Time Description
warning Mar 1 01:38:26.211 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:25.203 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:24.167 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:23.167 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:35:26.427 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:25.403 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:24.407 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:23.387 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:56.947 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.999 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.015 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:53.991 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:32:16.443 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
Done.
01:38:31 UTC Fri Mar 01 2002

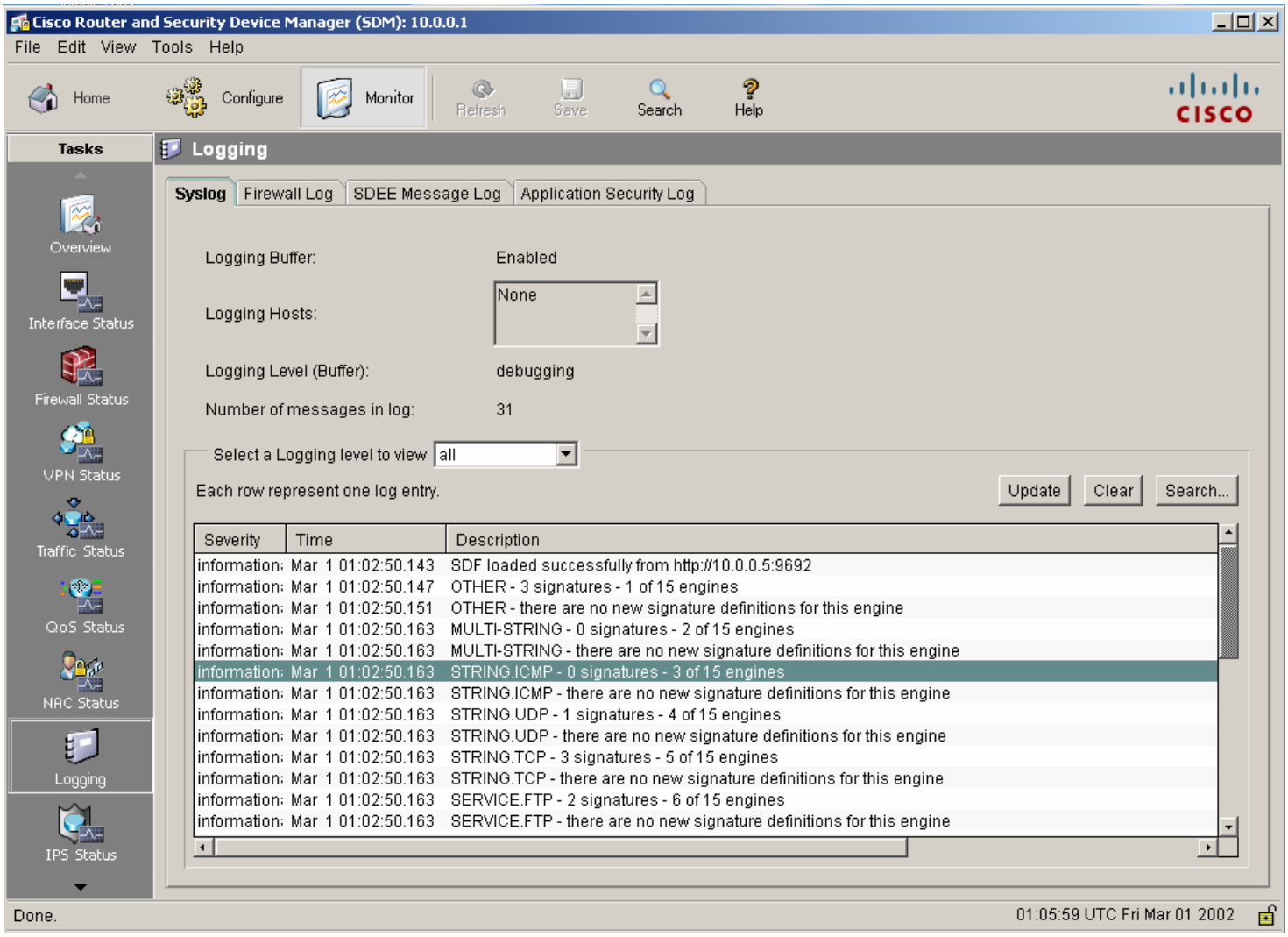

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 109
Select a Logging level to view debugging
Each row represent one log entry.
Update
Clear
Search...
Severity Time Description
warning Mar 1 01:38:26.211 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:25.203 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:24.167 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:38:23.167 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
warning Mar 1 01:35:26.427 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:25.403 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:24.407 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:35:23.387 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:56.947 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.999 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:55.015 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:34:53.991 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [13.0.0.5:0 -> 10.0.0.5:0]
warning Mar 1 01:32:16.443 Sig:2004 Subsig:0 Sev:2 ICMP Echo Req [10.0.0.5:0 -> 13.0.0.5:0]
Done.
01:38:31 UTC Fri Mar 01 2002

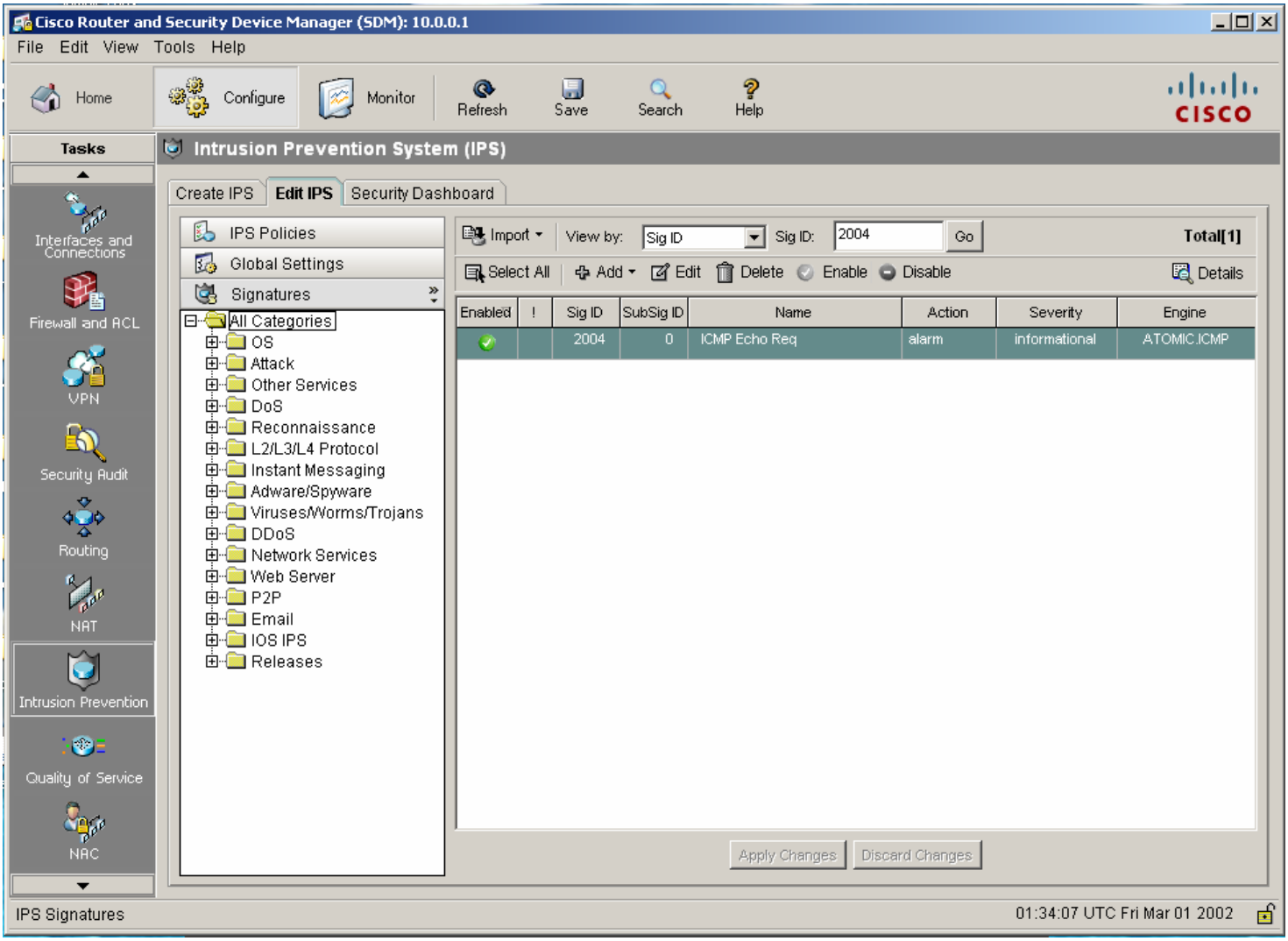

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
SDEE Messages:
Alerts
Search
Refresh
Time
Type
Description
00:22:55 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942175 36] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:56 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942176 37] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:57 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942177 38] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:22:58 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942178 39] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:37 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942217 40] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:39 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942219 41] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:40 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942220 42] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:23:41 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942221 43] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 44] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 45] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 46] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 47] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 48] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 49] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 50] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 51] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 52] vendor [Cisco] originator hostId [R1] severity [high]Contents of Signature
00:28:48 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014942528 53] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
00:42:00 GMT+00:00 Fri Mar 01 200: Alerts eventId [1014943320 85] vendor [Cisco] originator hostId [R1] severity [informational]Contents of
Done.
00:53:48 UTC Fri Mar 01 2002


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
IPS Status
IPS Signature Statistics
Total Active Signature: 132 Total Inactive Signature: 0
Update
Clear
SDEE Log
Signature ID | Description | Source IP Address | Destination IP Address | Hits | Drop Counts
1001:0 | Record Packet Rte | | | 0 | 0
1002:0 | Timestamp | | | 0 | 0
1003:0 | Provide s,c,h,tcc | | | 0 | 0
1004:0 | Loose Src Rte | | | 0 | 0
1005:0 | SATNET ID | | | 0 | 0
1006:0 | Strict Src Rte | | | 0 | 0
ATOMIC.L3.IP
1101:0 | Unknown IP Proto | | | 0 | 0
1102:0 | Impossible IP packet | 10.0.0.1:0 | 10.0.0.1:0 | 5 | 0
1104:0 | Localhost | | | 0 | 0
1107:0 | RFC1918 address | | | 0 | 0
2151:0 | Large ICMP | | | 0 | 0
2154:0 | Ping Of Death | | | 0 | 0
ATOMIC.ICMP
2000:0 | ICMP Echo Rply | | | 0 | 0
2001:0 | ICMP Unreachable | | | 0 | 0
2002:0 | ICMP Src Quench | | | 0 | 0
2003:0 | ICMP Redirect | | | 0 | 0
2005:0 | ICMP Time Exceed | | | 0 | 0
2006:0 | ICMP Param Prob | | | 0 | 0
2007:0 | ICMP Time Req | | | 0 | 0
2008:0 | ICMP Time Rply | | | 0 | 0
2009:0 | ICMP Info Req | | | 0 | 0
2010:0 | ICMP Info Rply | | | 0 | 0
2011:0 | ICMP Addr Msk Req | | | 0 | 0
2012:0 | ICMP Addr Msk Rply | | | 0 | 0
2150:0 | Fragmented ICMP | | | 0 | 0
2004:0 | ICMP Echo Req | 10.0.0.5:0 | 13.0.0.5:0 | 1 | 0
IPS Status
00:55:16 UTC Fri Mar 01 2002

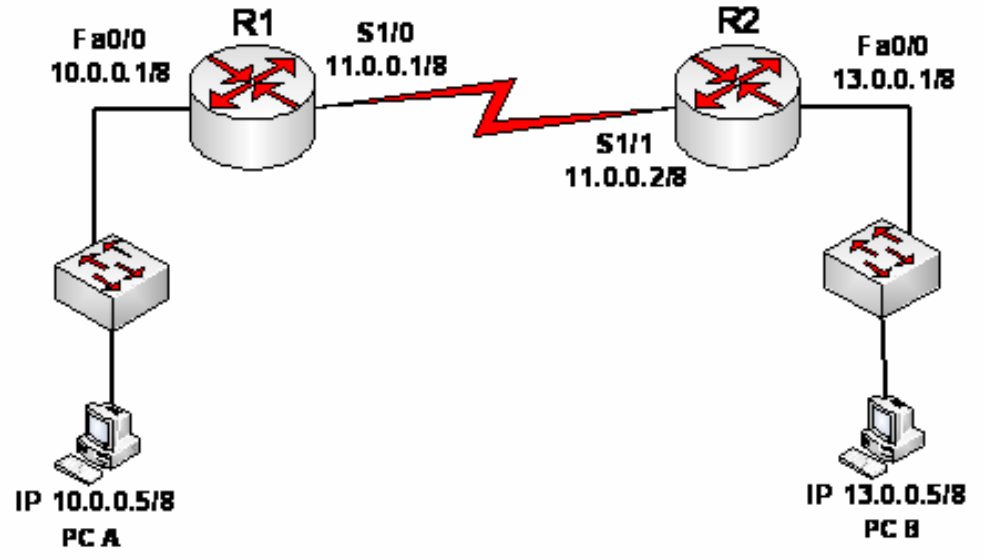

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Logging
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Syslog
Firewall Log
SDEE Message Log
Application Security Log
SDEE Messages:
Alerts
Search
Refresh
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [13.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.5]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] loc
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] loc
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] loc
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] loc
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1] loc
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.1] locality [] [0]] [Contents of Target totalPorts [] addr [10.0.0.1]
[] totalAttackers [] [Contents of Attacker totalPorts [] unreliable [] addr [10.0.0.5] locality [] [0]] [Contents of Target totalPorts [] addr [13.0.0.5]
IPS Status
00:59:46 UTC Fri Mar 01 2002

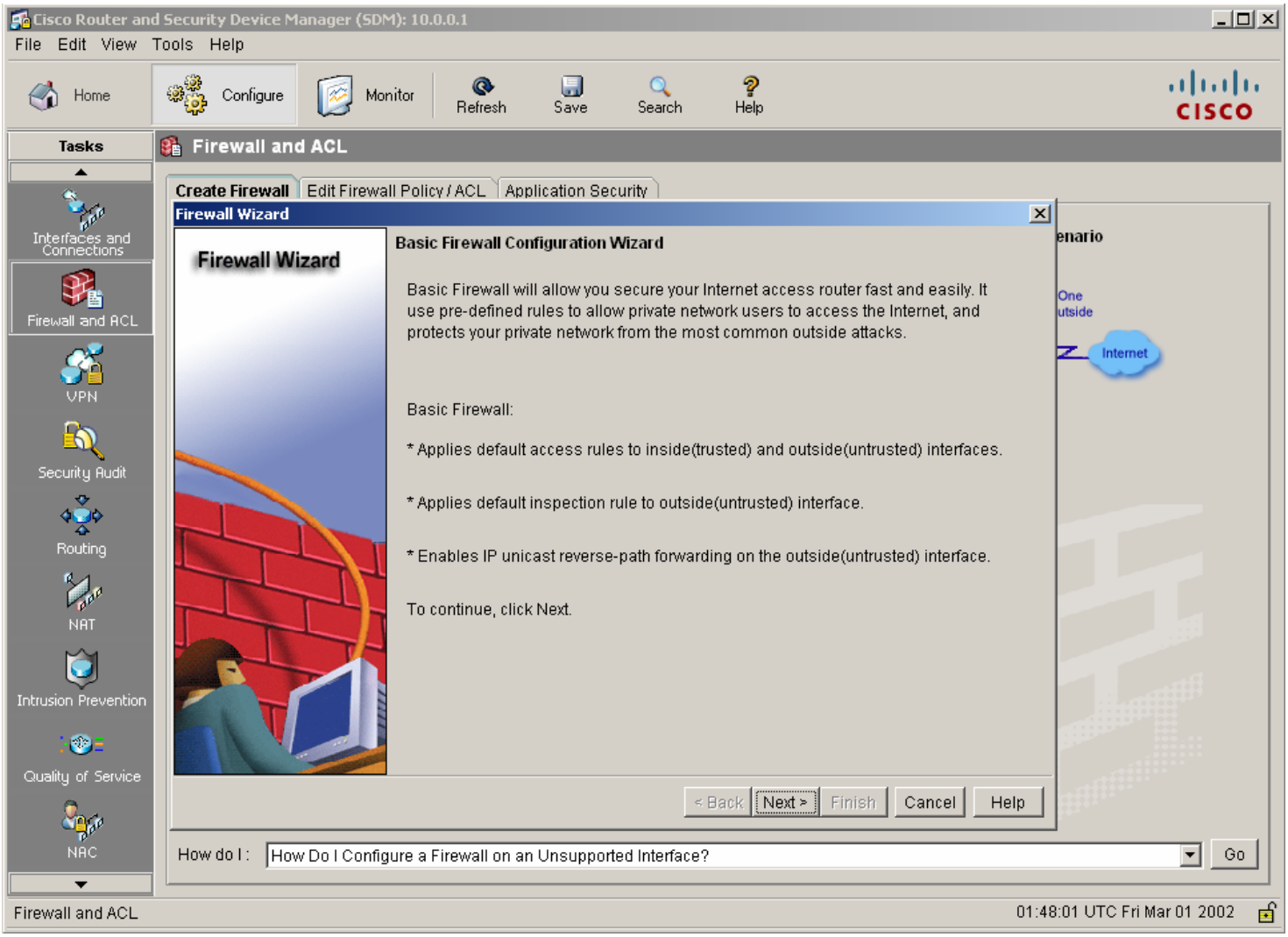

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by: Sig ID
Sig ID:
Go
Total[132]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled ! Sig ID SubSig ID Name Action Severity Engine
2010 0 ICMP Info Rply alarm informational ATOMIC.ICMP
3152 0 FTP CWD ~root alarm medium STRING.TCP
5118 0 WWW eWave ServletExec File alarm high SERVICE.HTTP
3151 0 FTP SYST alarm informational STRING.TCP
5117 0 WWW PhpGroupware Cmd Exe alarm high SERVICE.HTTP
3150 0 FTP SITE alarm informational STRING.TCP
5116 0 WWW Endymion MailMan Cmd E alarm high SERVICE.HTTP
4100 0 Tftp passwd alarm high STRING.UDP
3043 0 TCP FRAG SYN/FIN Packet alarm high ATOMIC.TCP
5114 2 WWW IIS Unicode attack alarm medium SERVICE.HTTP
5114 1 WWW IIS Unicode attack alarm medium SERVICE.HTTP
5114 0 WWW IIS Unicode attack alarm medium SERVICE.HTTP
4600 0 IOS Udp Bomb alarm medium ATOMIC.UDP
3042 0 TCP FIN Packet alarm high ATOMIC.TCP
3041 0 TCP SYN/FIN Packet alarm high ATOMIC.TCP
5123 1 WWW IIS Internet Printing Overf alarm high SERVICE.HTTP
Apply Changes
Discard Changes
IPS Signatures
01:02:58 UTC Fri Mar 01 2002

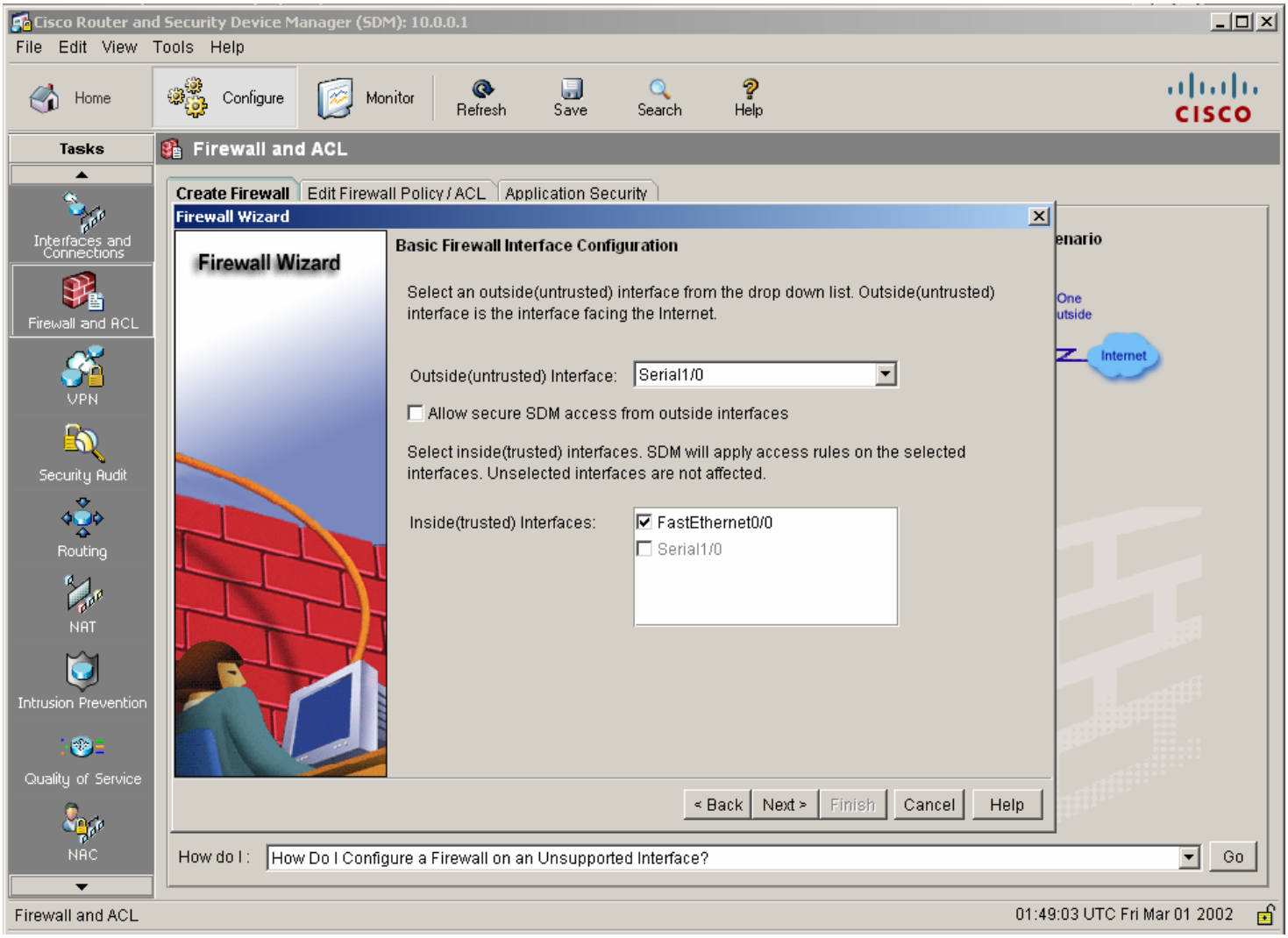

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 31
Select a Logging level to view all
Each row represent one log entry.
Update
Clear
Search...
Severity Time Description
information: Mar 1 01:02:50.143 SDF loaded successfully from http://10.0.0.5:9692
information: Mar 1 01:02:50.147 OTHER - 3 signatures - 1 of 15 engines
information: Mar 1 01:02:50.151 OTHER - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 MULTI-STRING - 0 signatures - 2 of 15 engines
information: Mar 1 01:02:50.163 MULTI-STRING - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.ICMP - 0 signatures - 3 of 15 engines
information: Mar 1 01:02:50.163 STRING.ICMP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.UDP - 1 signatures - 4 of 15 engines
information: Mar 1 01:02:50.163 STRING.UDP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 STRING.TCP - 3 signatures - 5 of 15 engines
information: Mar 1 01:02:50.163 STRING.TCP - there are no new signature definitions for this engine
information: Mar 1 01:02:50.163 SERVICE.FTP - 2 signatures - 6 of 15 engines
information: Mar 1 01:02:50.163 SERVICE.FTP - there are no new signature definitions for this engine
Done.
01:05:59 UTC Fri Mar 01 2002

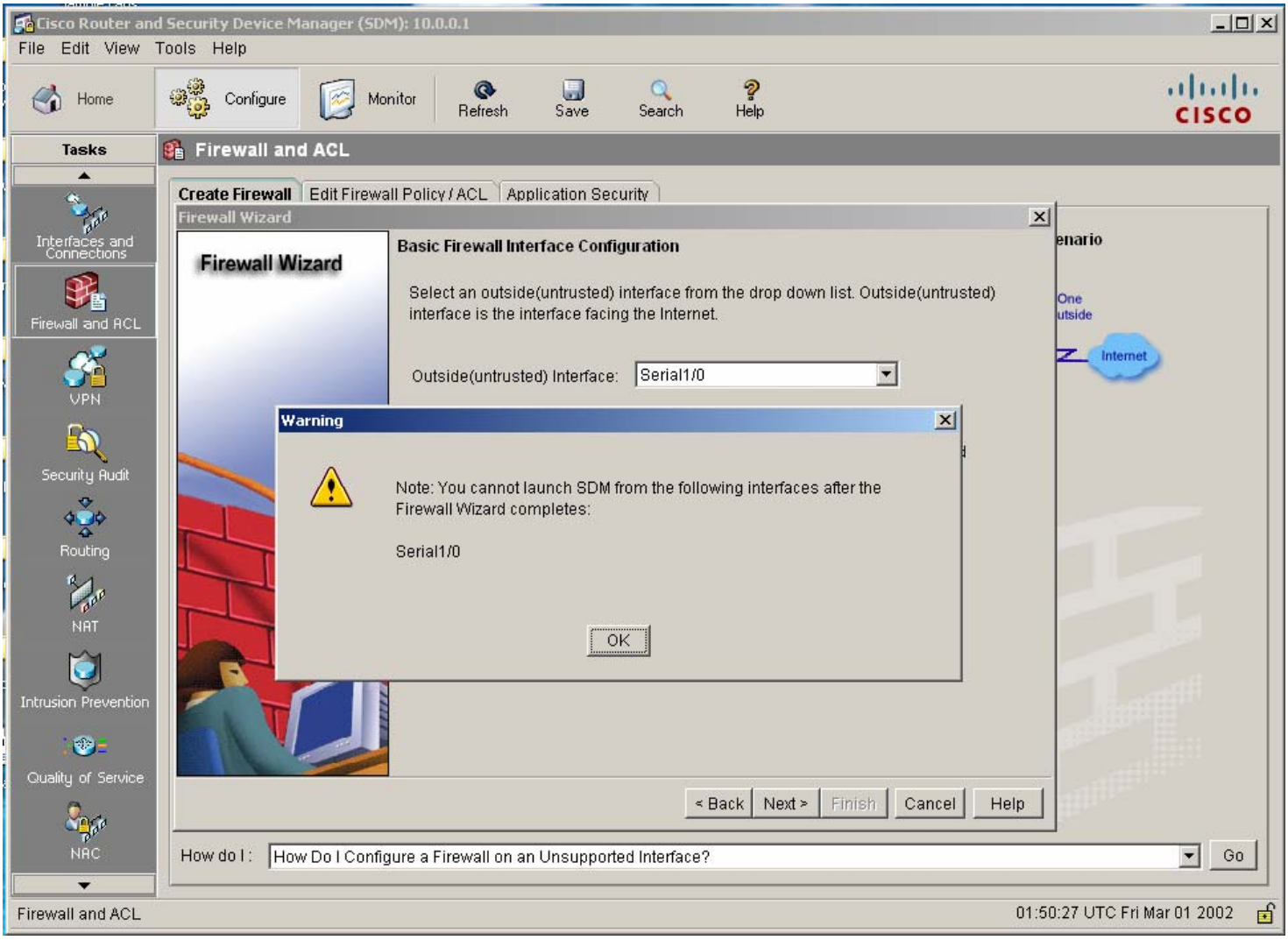

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Intrusion Prevention System (IPS)
Create IPS
Edit IPS
Security Dashboard
IPS Policies
Global Settings
Signatures
All Categories
OS
Attack
Other Services
DoS
Reconnaissance
L2/L3/L4 Protocol
Instant Messaging
Adware/Spyware
Viruses/Worms/Trojans
DDoS
Network Services
Web Server
P2P
Email
IOS IPS
Releases
Import
View by:
Sig ID
Sig ID:
2004
Go
Total[1]
Select All
Add
Edit
Delete
Enable
Disable
Details
Enabled
!
Sig ID
SubSig ID
Name
Action
Severity
Engine
2004
0
ICMP Echo Req
alarm
informational
ATOMIC.ICMP
Apply Changes
Discard Changes
IPS Signatures
01:34:07 UTC Fri Mar 01 2002

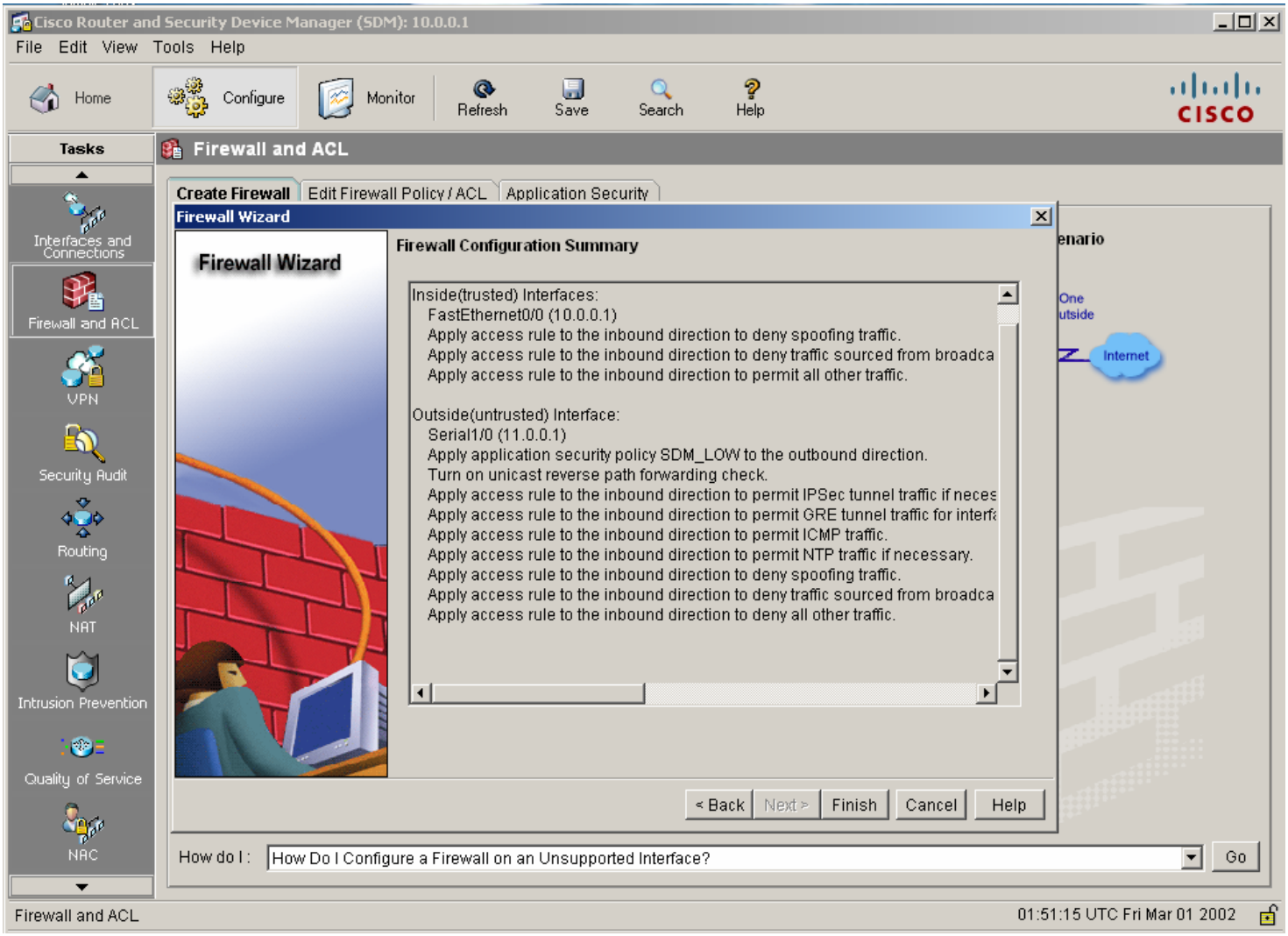
LAB # 10
Configuring Firewall

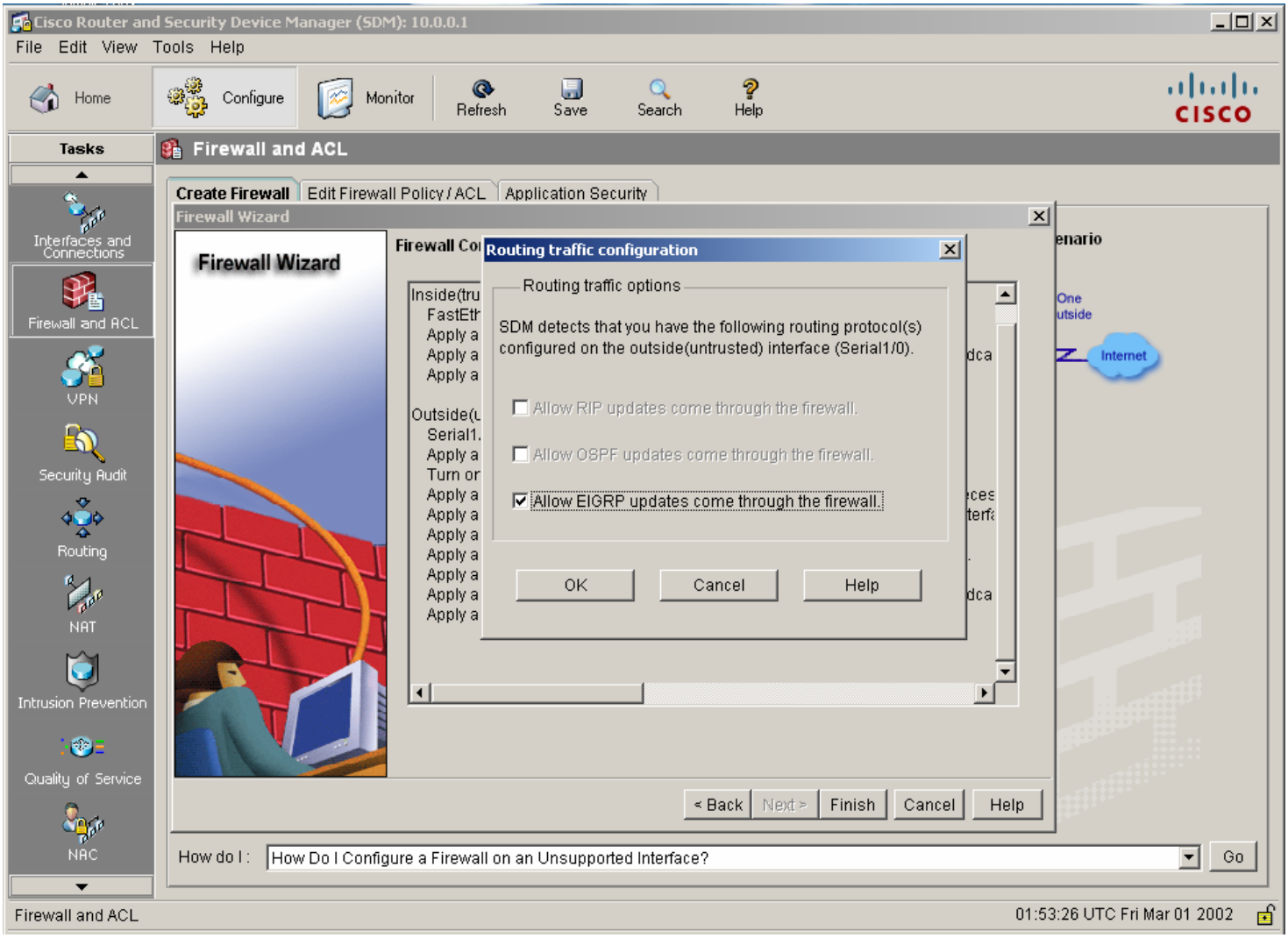


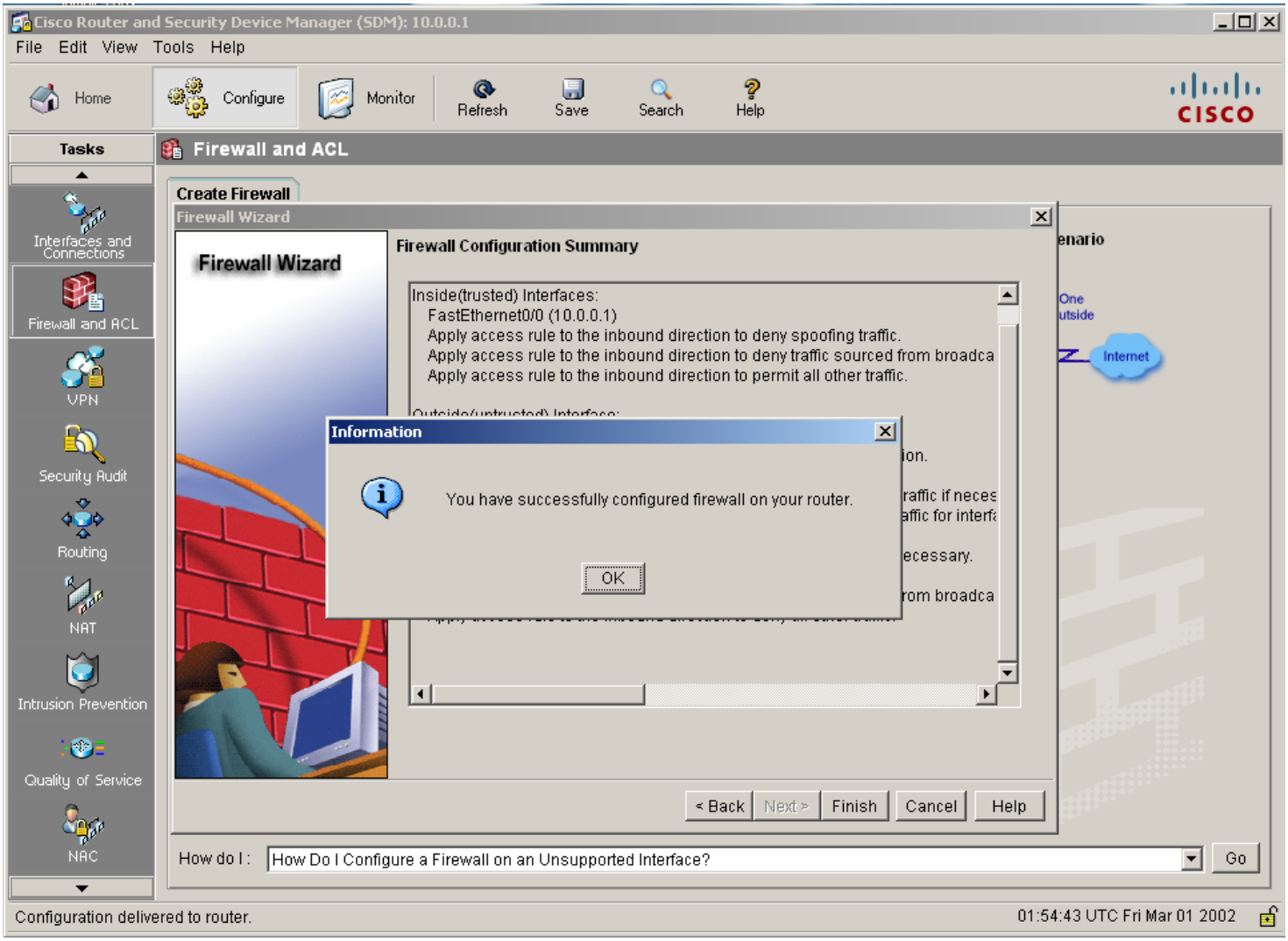

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Firewall Wizard
Firewall Wizard
Basic Firewall Configuration Wizard
Basic Firewall will allow you secure your Internet access router fast and easily. It use pre-defined rules to allow private network users to access the Internet, and protects your private network from the most common outside attacks.
Basic Firewall:
* Applies default access rules to inside(trusted) and outside(untrusted) interfaces.
* Applies default inspection rule to outside(untrusted) interface.
* Enables IP unicast reverse-path forwarding on the outside(untrusted) interface.
To continue, click Next.
< Back
Next >
Finish
Cancel
Help
enario
One
utside
Internet
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Firewall and ACL
01:48:01 UTC Fri Mar 01 2002

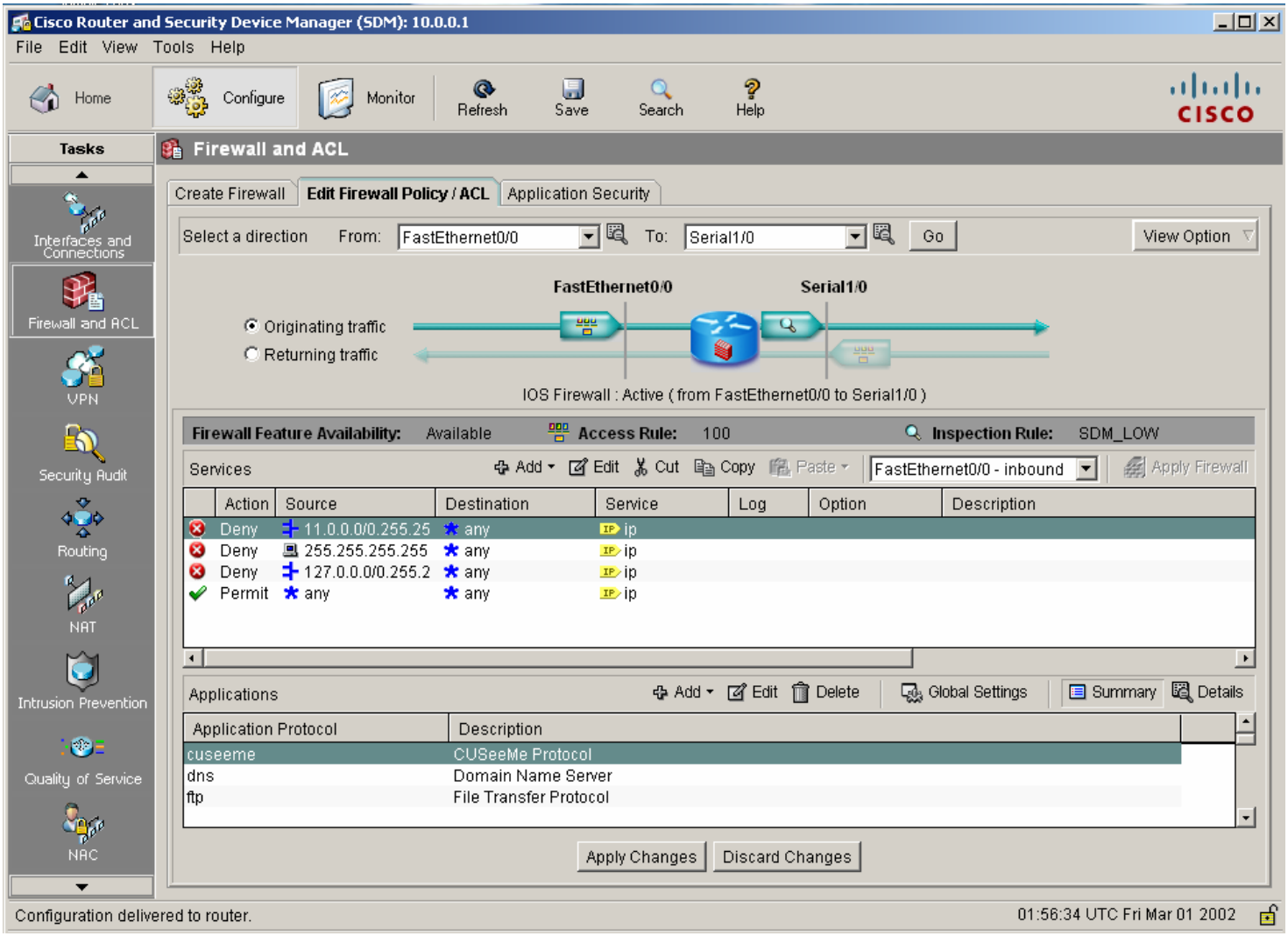

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Firewall Wizard
Firewall Wizard
Basic Firewall Interface Configuration
Select an outside(untrusted) interface from the drop down list. Outside(untrusted) interface is the interface facing the Internet.
Outside(untrusted) Interface:
Serial1/0
Allow secure SDM access from outside interfaces
Select inside(trusted) interfaces. SDM will apply access rules on the selected interfaces. Unselected interfaces are not affected.
Inside(trusted) Interfaces:
FastEthernet0/0
Serial1/0
< Back
Next >
Finish
Cancel
Help
enario
One
utside
Internet
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Firewall and ACL
01:49:03 UTC Fri Mar 01 2002

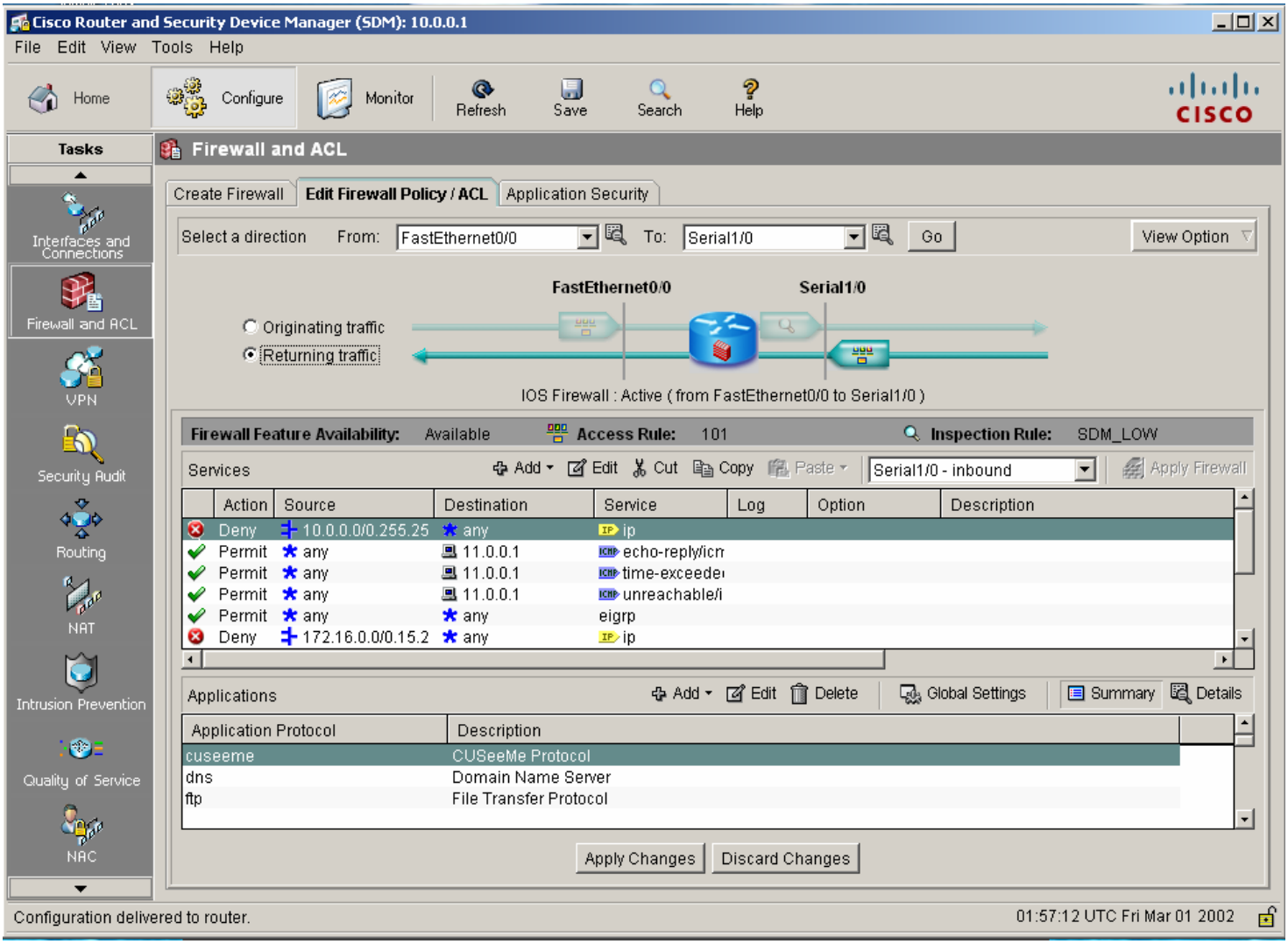

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Firewall Wizard
Firewall Wizard
Basic Firewall Interface Configuration
Select an outside(untrusted) interface from the drop down list. Outside(untrusted) interface is the interface facing the Internet.
Outside(untrusted) Interface:
Serial1/0
Warning
Note: You cannot launch SDM from the following interfaces after the Firewall Wizard completes:
Serial1/0
OK
enario
One
utside
Internet
< Back
Next >
Finish
Cancel
Help
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Firewall and ACL
01:50:27 UTC Fri Mar 01 2002

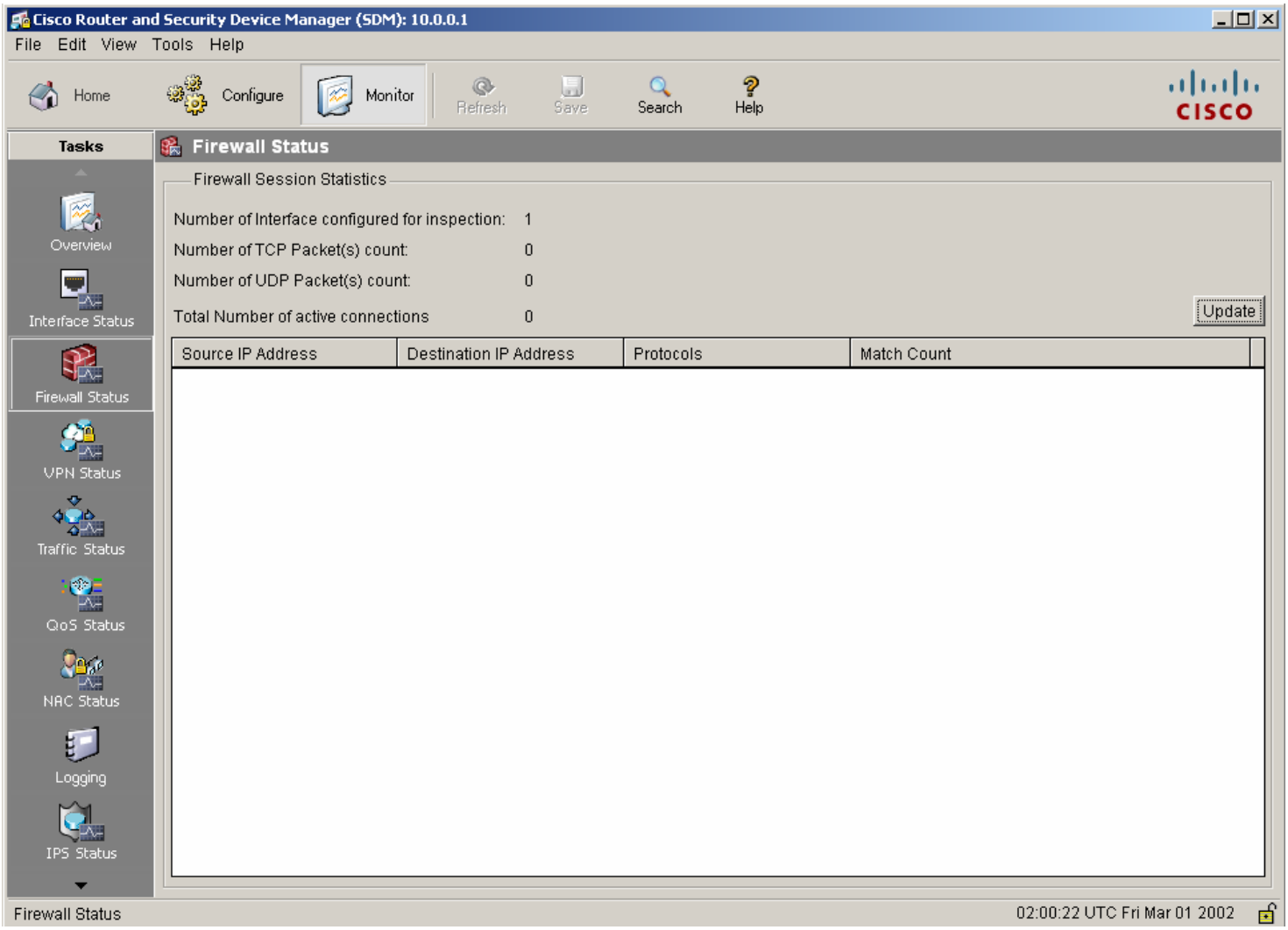

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Firewall Wizard
Firewall Wizard
Firewall Configuration Summary
Inside(trusted) Interfaces:
FastEthernet0/0 (10.0.0.1)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to permit all other traffic.
Outside(untrusted) Interface:
Serial1/0 (11.0.0.1)
Apply application security policy SDM_LOW to the outbound direction.
Turn on unicast reverse path forwarding check.
Apply access rule to the inbound direction to permit IPSec tunnel traffic if neces
Apply access rule to the inbound direction to permit GRE tunnel traffic for interf
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to deny all other traffic.
< Back
Next >
Finish
Cancel
Help
enario
One
utside
Internet
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Firewall and ACL
01:51:15 UTC Fri Mar 01 2002

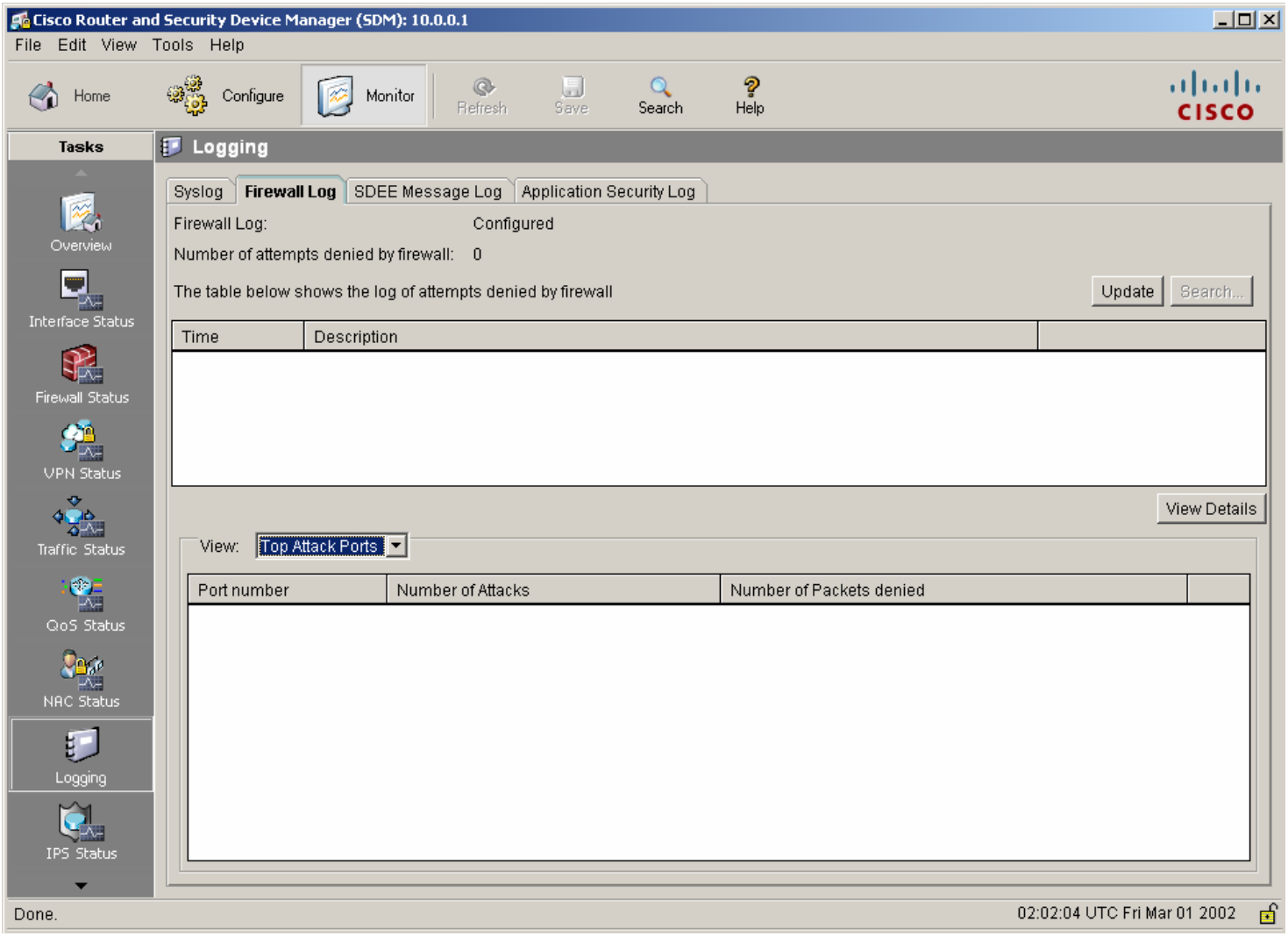

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Firewall Wizard
Firewall Wizard
Routing traffic configuration
Routing traffic options
SDM detects that you have the following routing protocol(s) configured on the outside(untrusted) interface (Serial1/0).
Allow RIP updates come through the firewall.
Allow OSPF updates come through the firewall.
Allow EIGRP updates come through the firewall.
OK
Cancel
Help
< Back
Next >
Finish
Cancel
Help
Internet
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Firewall and ACL
01:53:26 UTC Fri Mar 01 2002

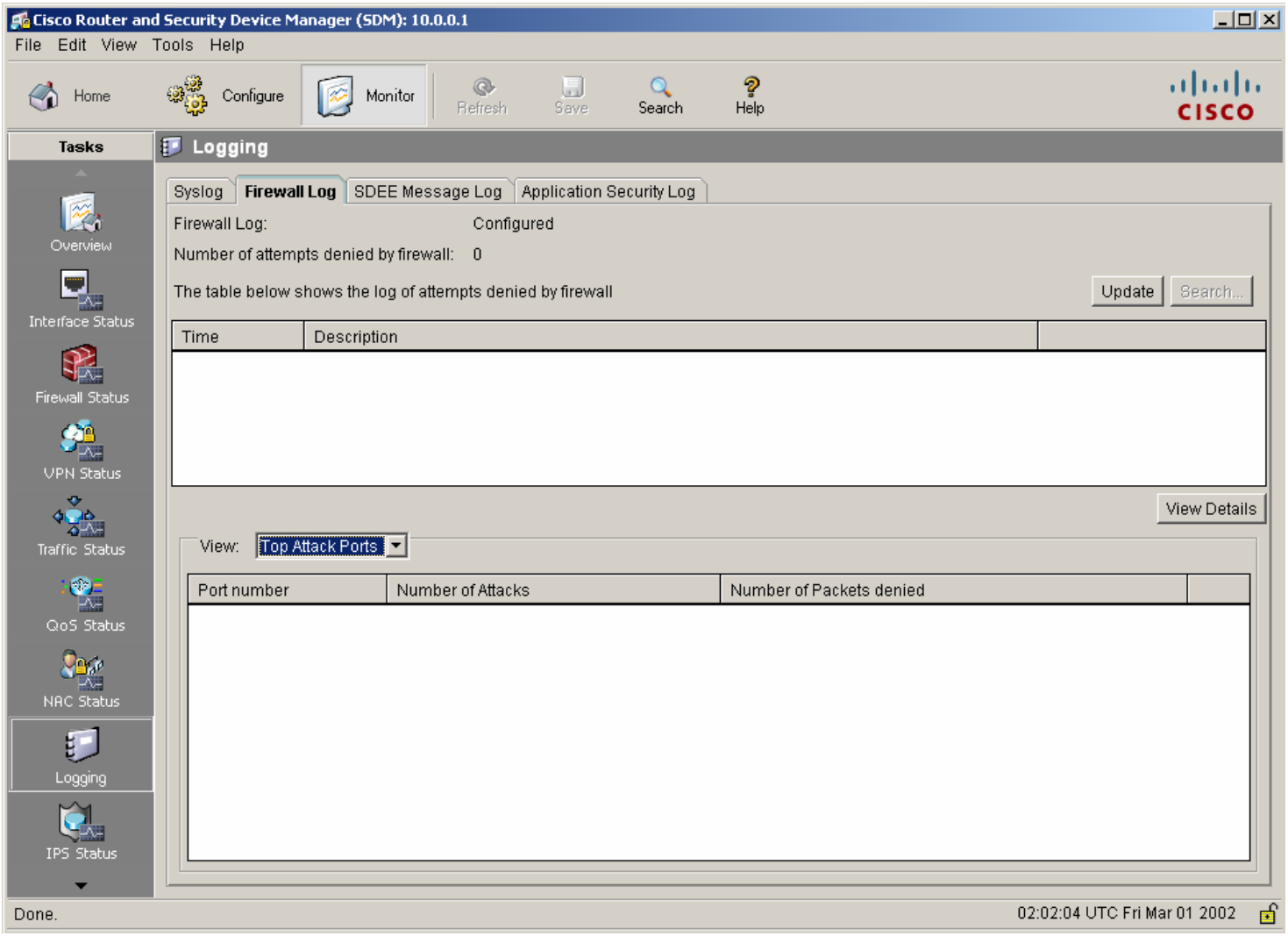

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Firewall Wizard
Firewall Wizard
Firewall Configuration Summary
Inside(trusted) Interfaces:
FastEthernet0/0 (10.0.0.1)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced from broadca
Apply access rule to the inbound direction to permit all other traffic.
Information
You have successfully configured firewall on your router.
OK
< Back
Next >
Finish
Cancel
Help
Internet
How do I :
How Do I Configure a Firewall on an Unsupported Interface?
Go
Configuration delivered to router.
01:54:43 UTC Fri Mar 01 2002

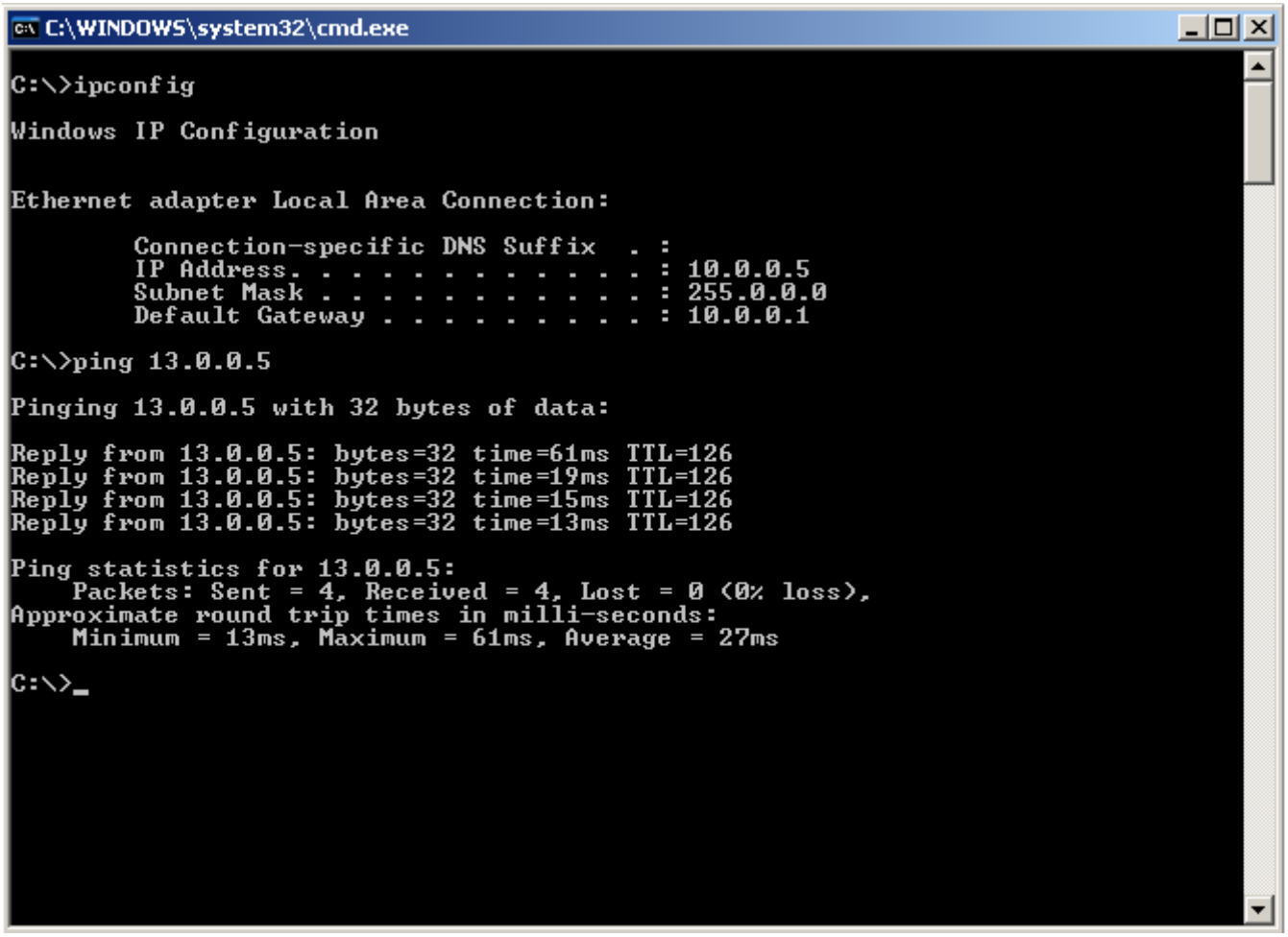

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial1/0
Go
View Option
FastEthernet0/0
Serial1/0
Originating traffic
Returning traffic
IOS Firewall : Active (from FastEthernet0/0 to Serial1/0)
Firewall Feature Availability: Available
Access Rule: 100
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Paste
FastEthernet0/0 - inbound
Apply Firewall
Action
Source
Destination
Service
Log
Option
Description
Deny 11.0.0.0/0.255.25 any ip
Deny 255.255.255.255 any ip
Deny 127.0.0.0/0.255.2 any ip
Permit any any ip
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Description
cuseeme
CUSeeMe Protocol
dns
Domain Name Server
ftp
File Transfer Protocol
Apply Changes
Discard Changes
Configuration delivered to router.
01:56:34 UTC Fri Mar 01 2002

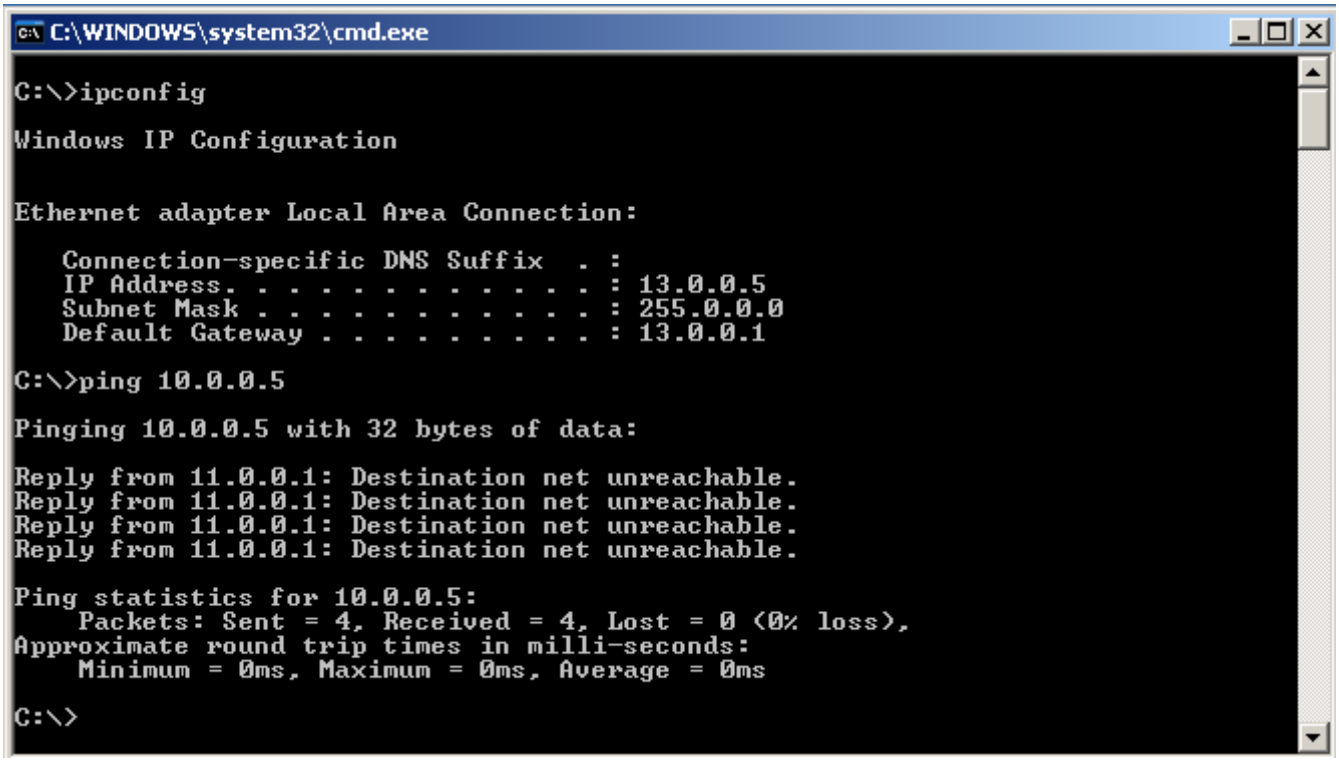

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial1/0
Go
View Option
FastEthernet0/0
Serial1/0
Originating traffic
Returning traffic
IOS Firewall : Active (from FastEthernet0/0 to Serial1/0)
Firewall Feature Availability: Available
Access Rule: 101
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Paste
Serial1/0 - inbound
Apply Firewall
Action
Source
Destination
Service
Log
Option
Description
Deny 10.0.0.0/0.255.25 any ip
Permit any 11.0.0.1 echo-reply/icm
Permit any 11.0.0.1 time-exceede
Permit any 11.0.0.1 unreachable/i
Permit any any eigrp
Deny 172.16.0.0/0.15.2 any ip
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Description
cuseeme CUSeeMe Protocol
dns Domain Name Server
ftp File Transfer Protocol
Apply Changes
Discard Changes
Configuration delivered to router.
01:57:12 UTC Fri Mar 01 2002

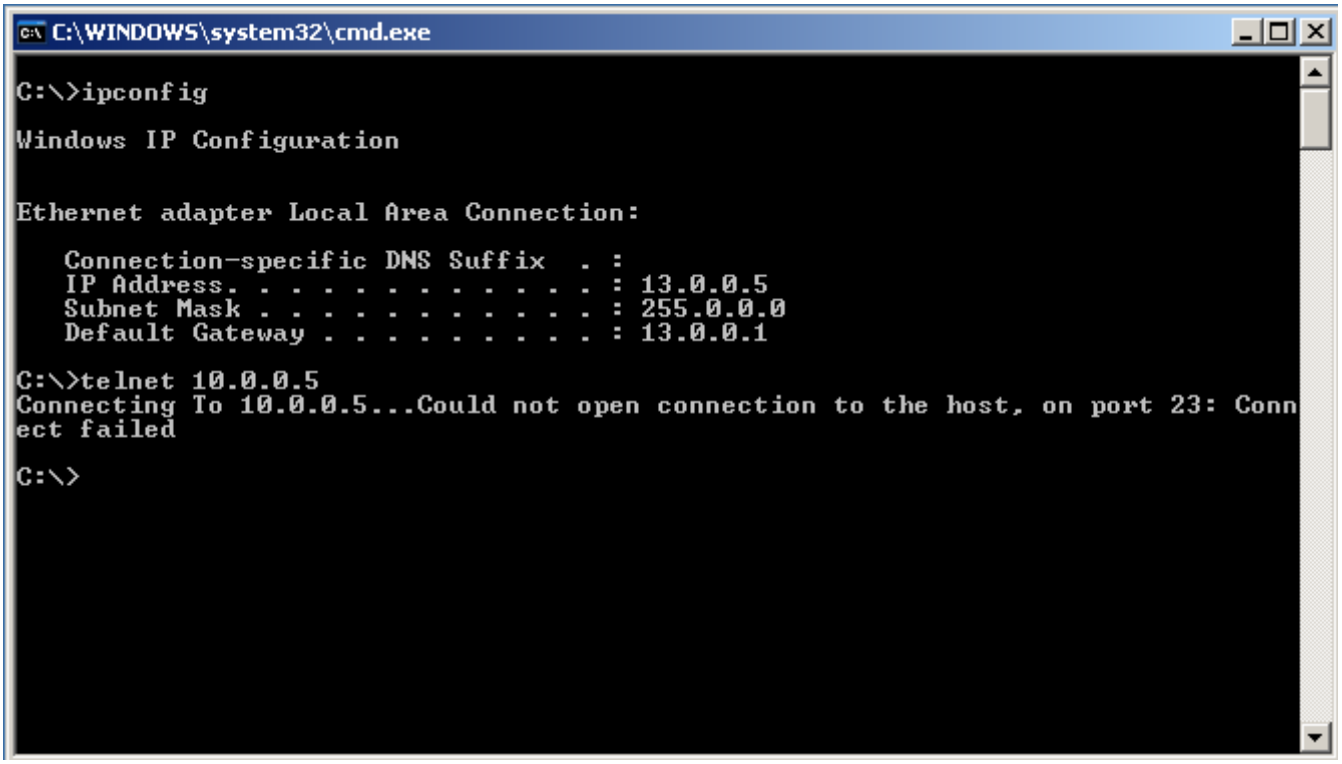

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Firewall Status
Firewall Session Statistics
Number of Interface configured for inspection: 1
Number of TCP Packet(s) count: 0
Number of UDP Packet(s) count: 0
Total Number of active connections 0
Update
Source IP Address
Destination IP Address
Protocols
Match Count
Firewall Status
02:00:22 UTC Fri Mar 01 2002

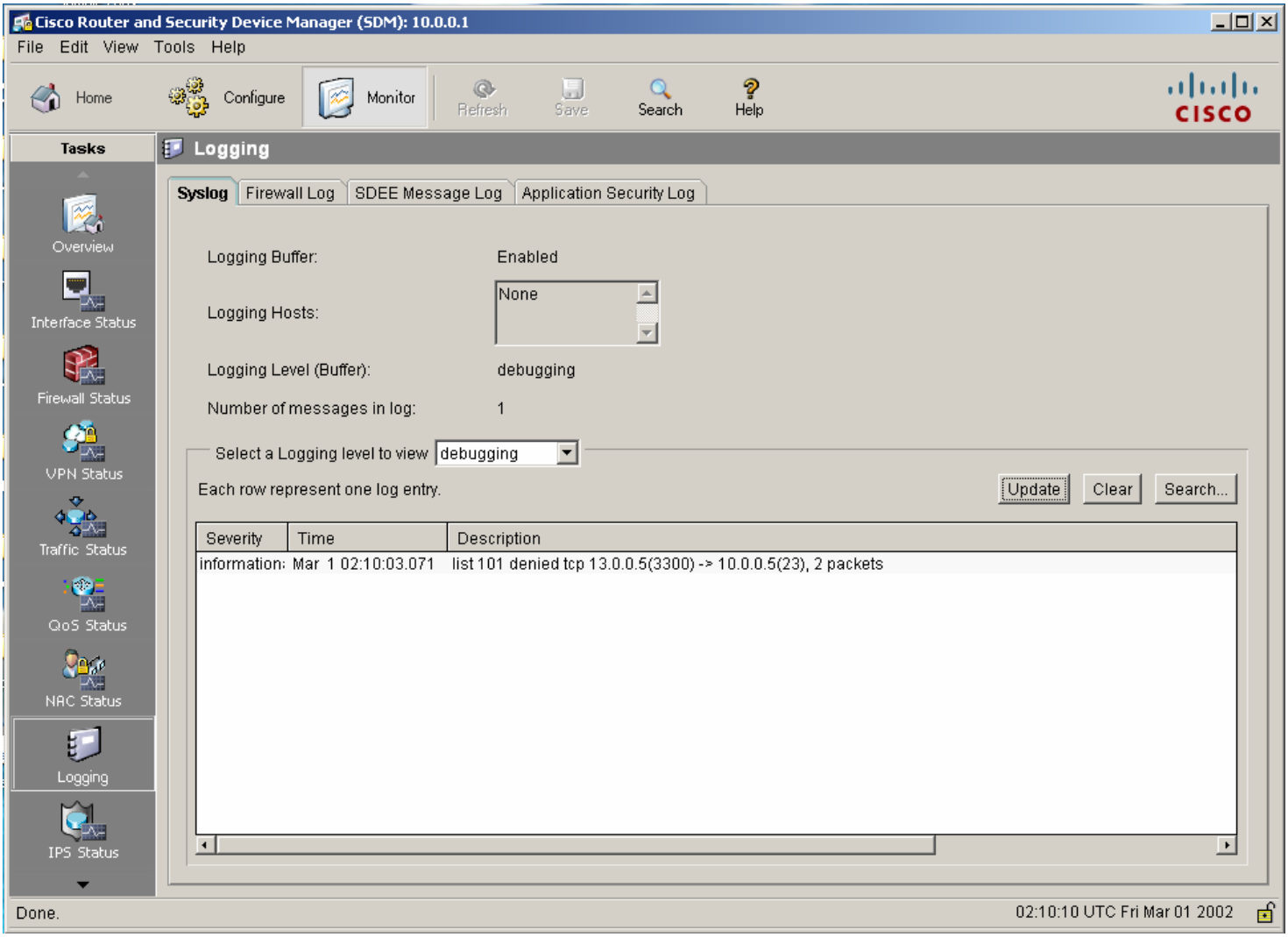

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Firewall Log: Configured
Number of attempts denied by firewall: 0
The table below shows the log of attempts denied by firewall
Update
Search...
Time
Description
View Details
View: Top Attack Ports
Port number
Number of Attacks
Number of Packets denied
Done.
02:02:04 UTC Fri Mar 01 2002

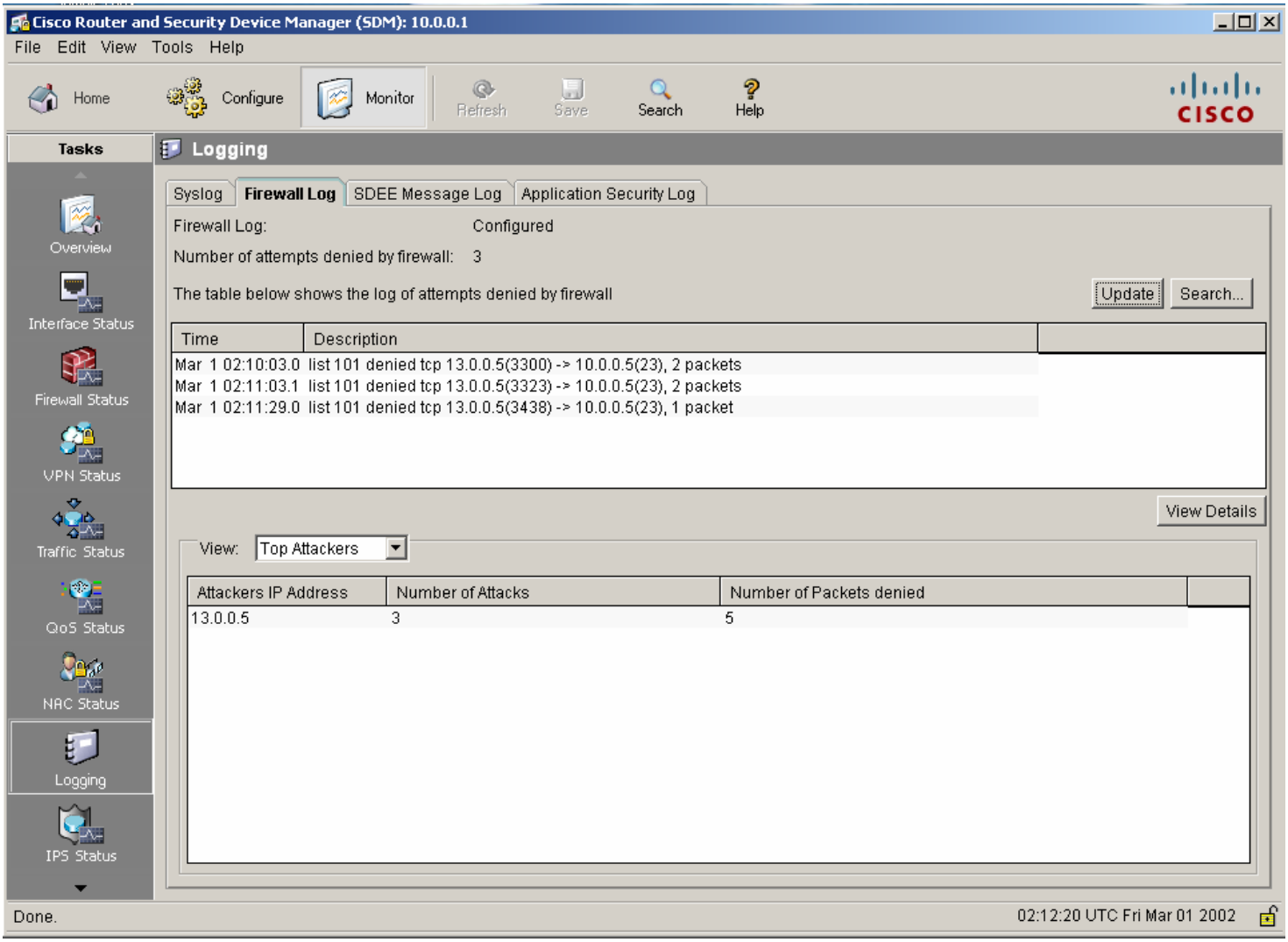

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Firewall Log: Configured
Number of attempts denied by firewall: 0
The table below shows the log of attempts denied by firewall
Update
Search...
Time
Description
View Details
View: Top Attack Ports
Port number
Number of Attacks
Number of Packets denied
Done.
02:02:04 UTC Fri Mar 01 2002

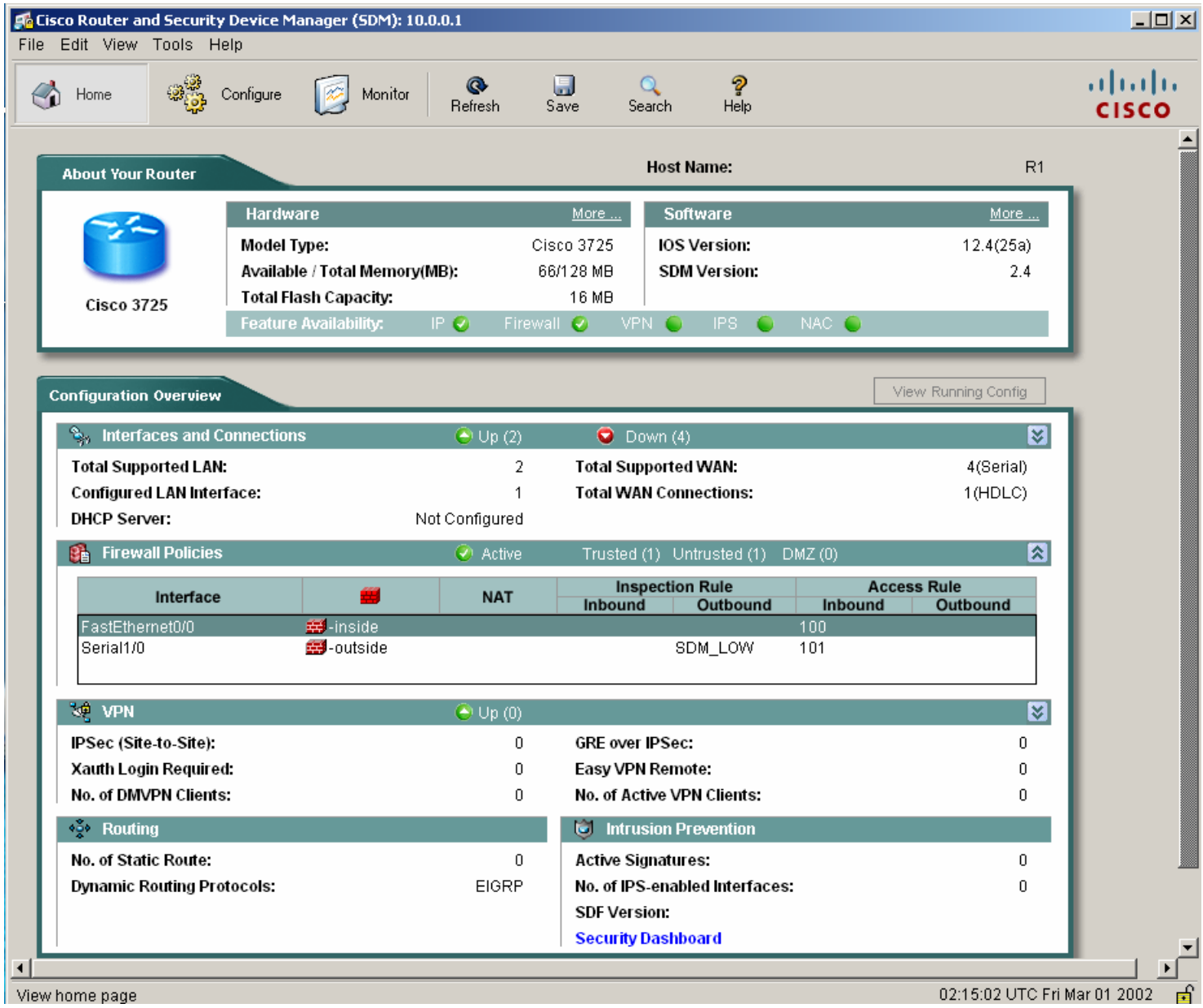

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.0.0.5
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 10.0.0.1
C:\>ping 13.0.0.5
Pinging 13.0.0.5 with 32 bytes of data:
Reply from 13.0.0.5: bytes=32 time=61ms TTL=126
Reply from 13.0.0.5: bytes=32 time=19ms TTL=126
Reply from 13.0.0.5: bytes=32 time=15ms TTL=126
Reply from 13.0.0.5: bytes=32 time=13ms TTL=126
Ping statistics for 13.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 13ms, Maximum = 61ms, Average = 27ms
C:\>

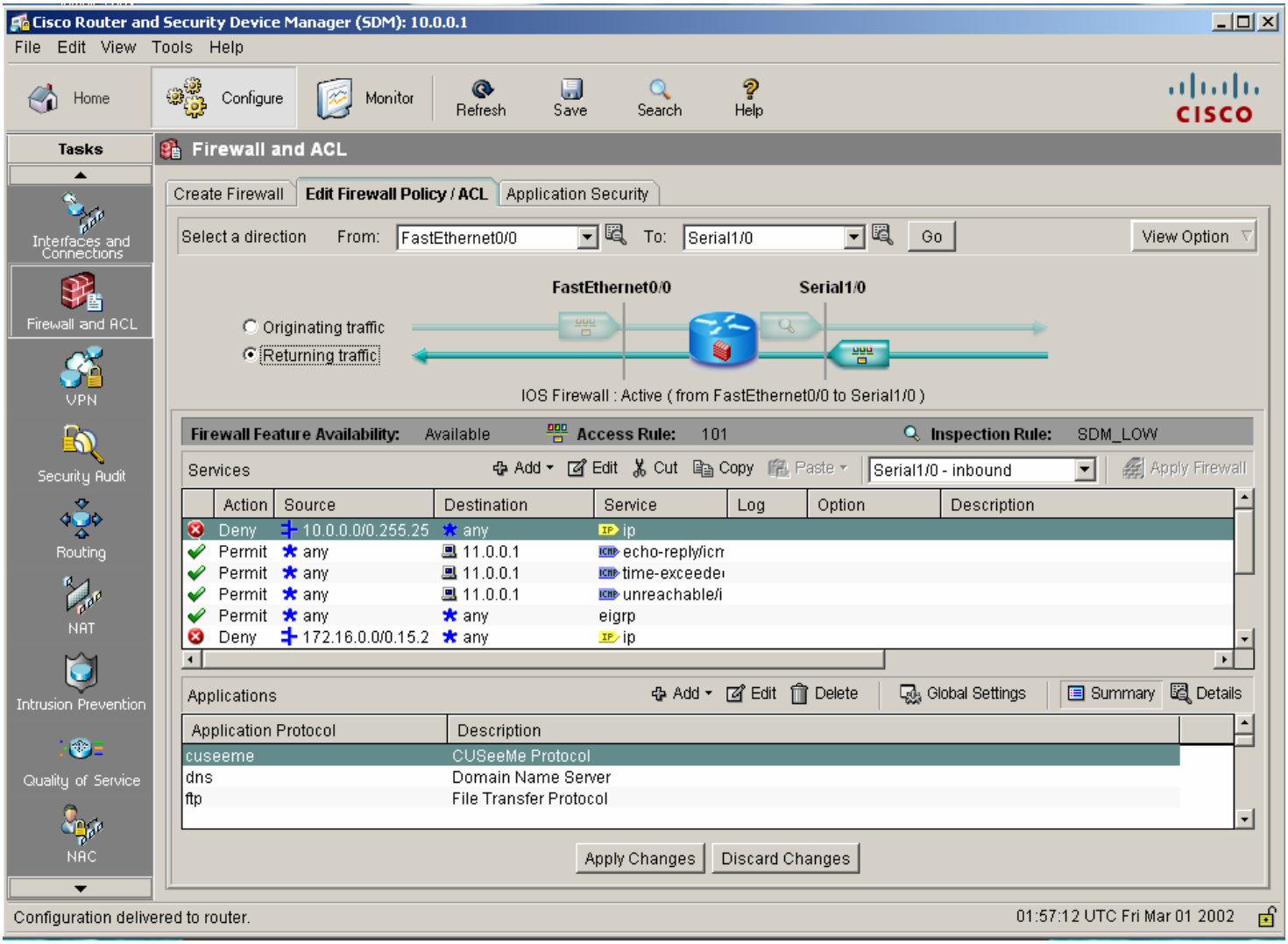

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 13.0.0.5
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 13.0.0.1
C:\>ping 10.0.0.5
Pinging 10.0.0.5 with 32 bytes of data:
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Ping statistics for 10.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

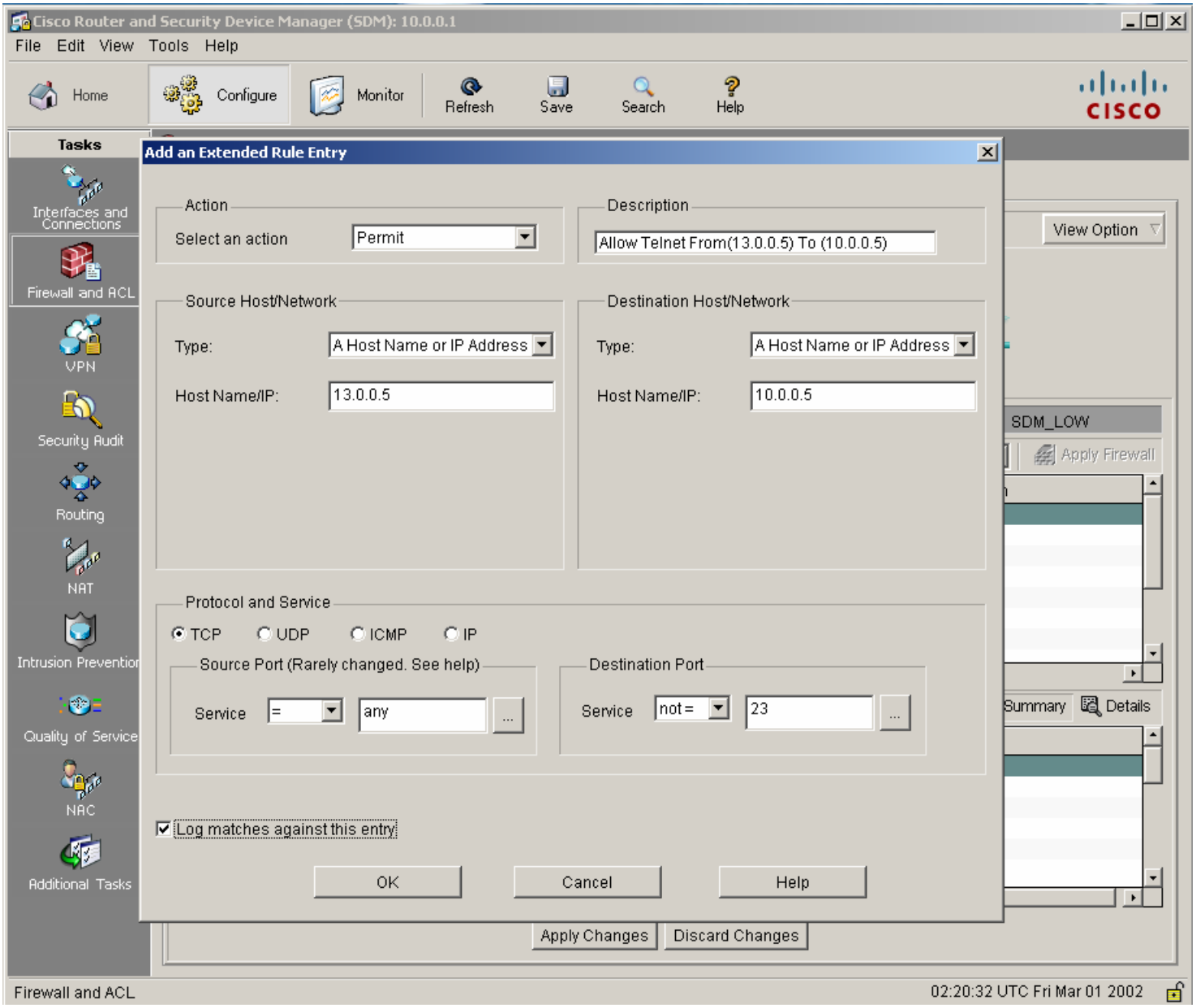

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 13.0.0.5
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 13.0.0.1
C:\>telnet 10.0.0.5
Connecting To 10.0.0.5...Could not open connection to the host, on port 23: Connect failed
C:\>

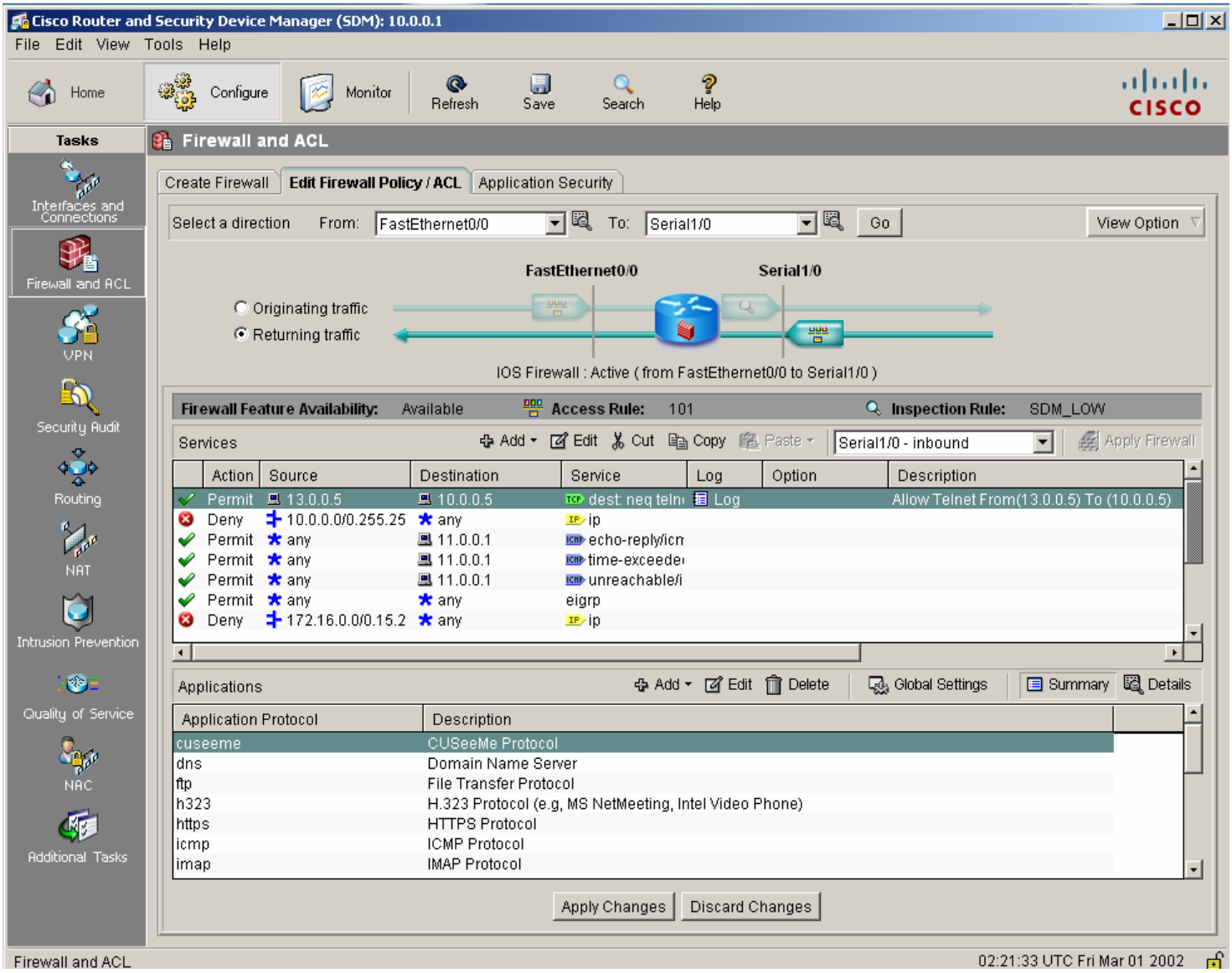

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 1
Select a Logging level to view debugging
Each row represent one log entry.
Update
Clear
Search...
Severity
Time
Description
information: Mar 1 02:10:03.071 list 101 denied tcp 13.0.0.5(3300) -> 10.0.0.5(23), 2 packets
Done.
02:10:10 UTC Fri Mar 01 2002

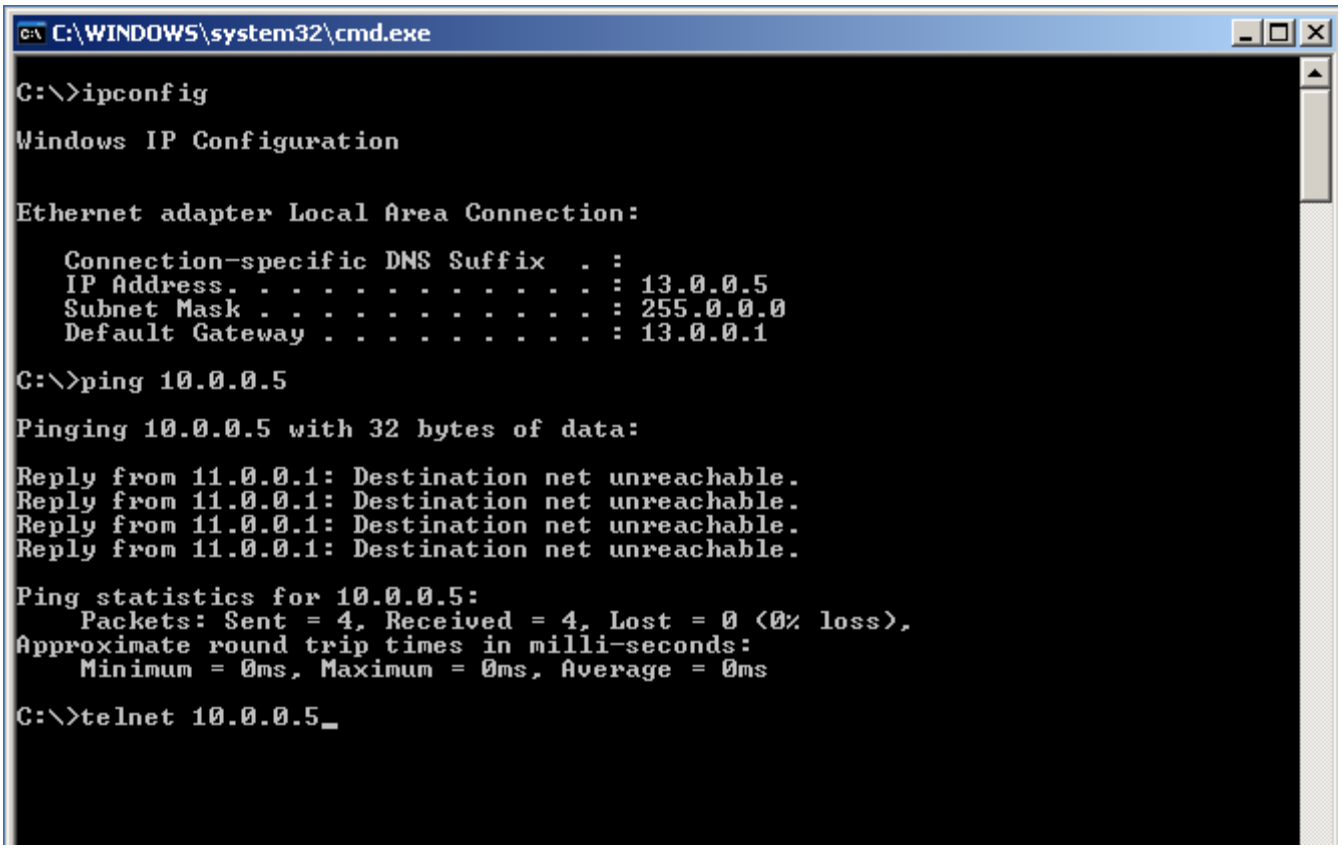

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Firewall Log: Configured
Number of attempts denied by firewall: 3
The table below shows the log of attempts denied by firewall
Update
Search...
Time
Description
Mar 1 02:10:03.0 list 101 denied tcp 13.0.0.5(3300) -> 10.0.0.5(23), 2 packets
Mar 1 02:11:03.1 list 101 denied tcp 13.0.0.5(3323) -> 10.0.0.5(23), 2 packets
Mar 1 02:11:29.0 list 101 denied tcp 13.0.0.5(3438) -> 10.0.0.5(23), 1 packet
View Details
View: Top Attackers
Attackers IP Address
Number of Attacks
Number of Packets denied
13.0.0.5
3
5
Done.
02:12:20 UTC Fri Mar 01 2002

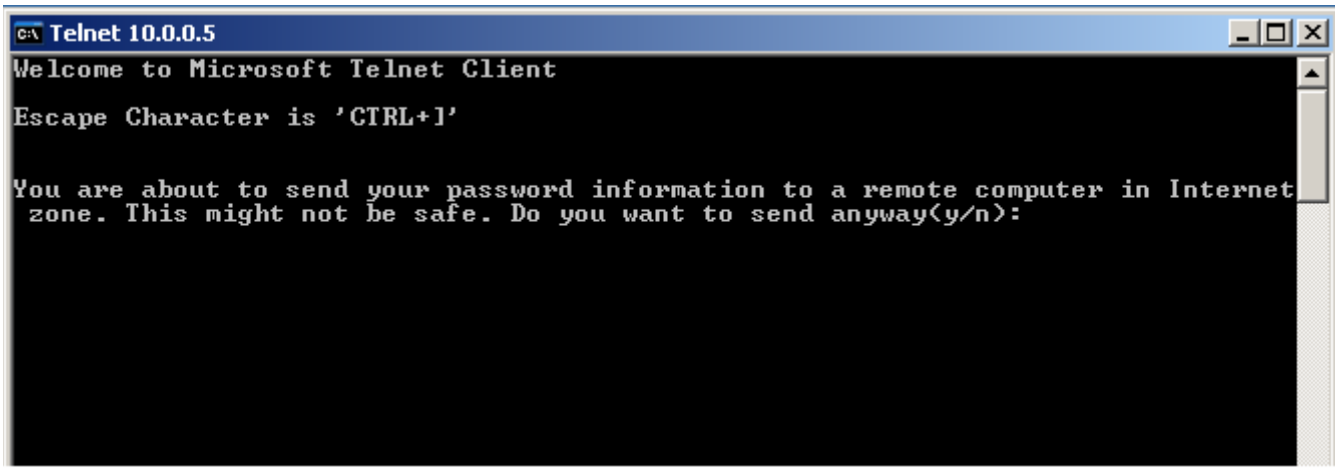

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
About Your Router
Host Name: R1
Cisco 3725
Hardware
More ...
Model Type: Cisco 3725
Available / Total Memory(MB): 66/128 MB
Total Flash Capacity: 16 MB
Software
More ...
IOS Version: 12.4(25a)
SDM Version: 2.4
Feature Availability: IP Firewall VPN IPS NAC
Configuration Overview
View Running Config
Interfaces and Connections
Up (2)
Down (4)
Total Supported LAN: 2
Configured LAN Interface: 1
DHCP Server: Not Configured
Total Supported WAN: 4(Serial)
Total WAN Connections: 1(HDLC)
Firewall Policies
Active
Trusted (1) Untrusted (1) DMZ (0)
Interface
NAT
Inspection Rule
Inbound
Outbound
Access Rule
Inbound
Outbound
FastEthernet0/0 -inside 100
Serial1/0 -outside SDM_LOW 101
VPN
Up (0)
IPSec (Site-to-Site): 0
Xauth Login Required: 0
No. of DMVPN Clients: 0
GRE over IPSec: 0
Easy VPN Remote: 0
No. of Active VPN Clients: 0
Routing
No. of Static Route: 0
Dynamic Routing Protocols: EIGRP
Intrusion Prevention
Active Signatures: 0
No. of IPS-enabled Interfaces: 0
SDF Version:
Security Dashboard
View home page
02:15:02 UTC Fri Mar 01 2002

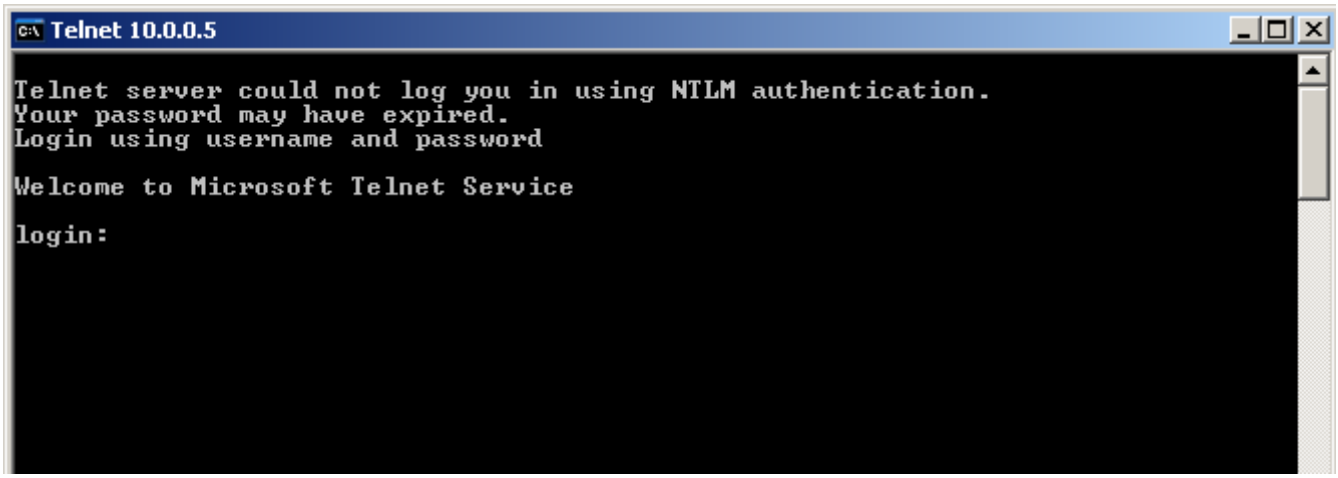

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial1/0
Go
View Option
FastEthernet0/0
Serial1/0
Originating traffic
Returning traffic
IOS Firewall : Active (from FastEthernet0/0 to Serial1/0)
Firewall Feature Availability: Available
Access Rule: 101
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Paste
Serial1/0 - inbound
Apply Firewall
Action
Source
Destination
Service
Log
Option
Description
Deny 10.0.0.0/0.255.25 any ip
Permit any 11.0.0.1 echo-reply/icm
Permit any 11.0.0.1 time-exceede
Permit any 11.0.0.1 unreachable/i
Permit any any eigrp
Deny 172.16.0.0/0.15.2 any ip
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Description
cuseeme CUSeeMe Protocol
dns Domain Name Server
ftp File Transfer Protocol
Apply Changes
Discard Changes
Configuration delivered to router.
01:57:12 UTC Fri Mar 01 2002

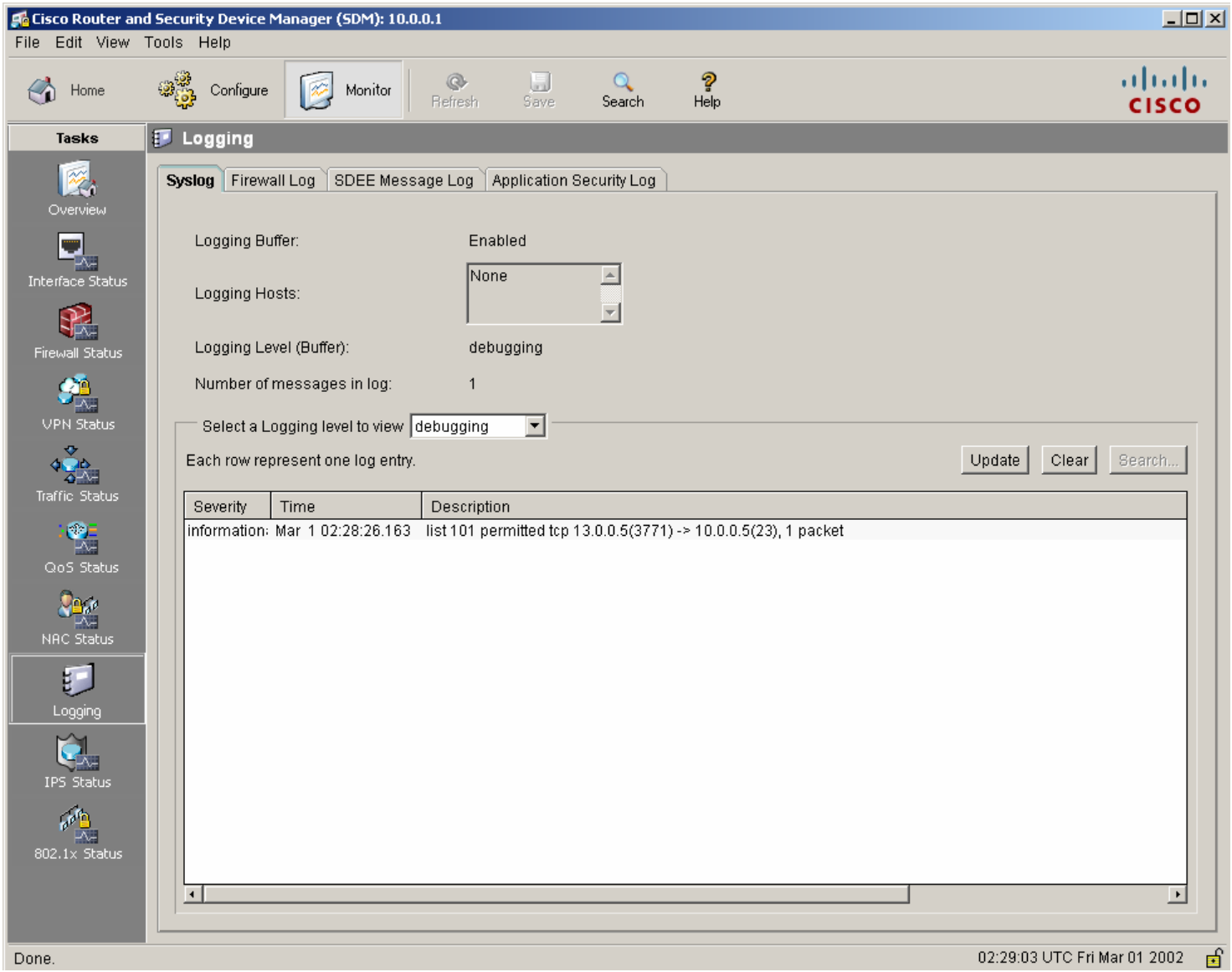

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Add an Extended Rule Entry
Action
Select an action
Permit
Description
Allow Telnet From(13.0.0.5) To (10.0.0.5)
Source Host/Network
Type:
A Host Name or IP Address
Host Name/IP:
13.0.0.5
Destination Host/Network
Type:
A Host Name or IP Address
Host Name/IP:
10.0.0.5
Protocol and Service
TCP
UDP
ICMP
IP
Source Port (Rarely changed. See help)
Service
=
any
Destination Port
Service
not =
23
Log matches against this entry
OK
Cancel
Help
View Option
SDM_LOW
Apply Firewall
Summary
Details
Apply Changes
Discard Changes
Firewall and ACL
02:20:32 UTC Fri Mar 01 2002

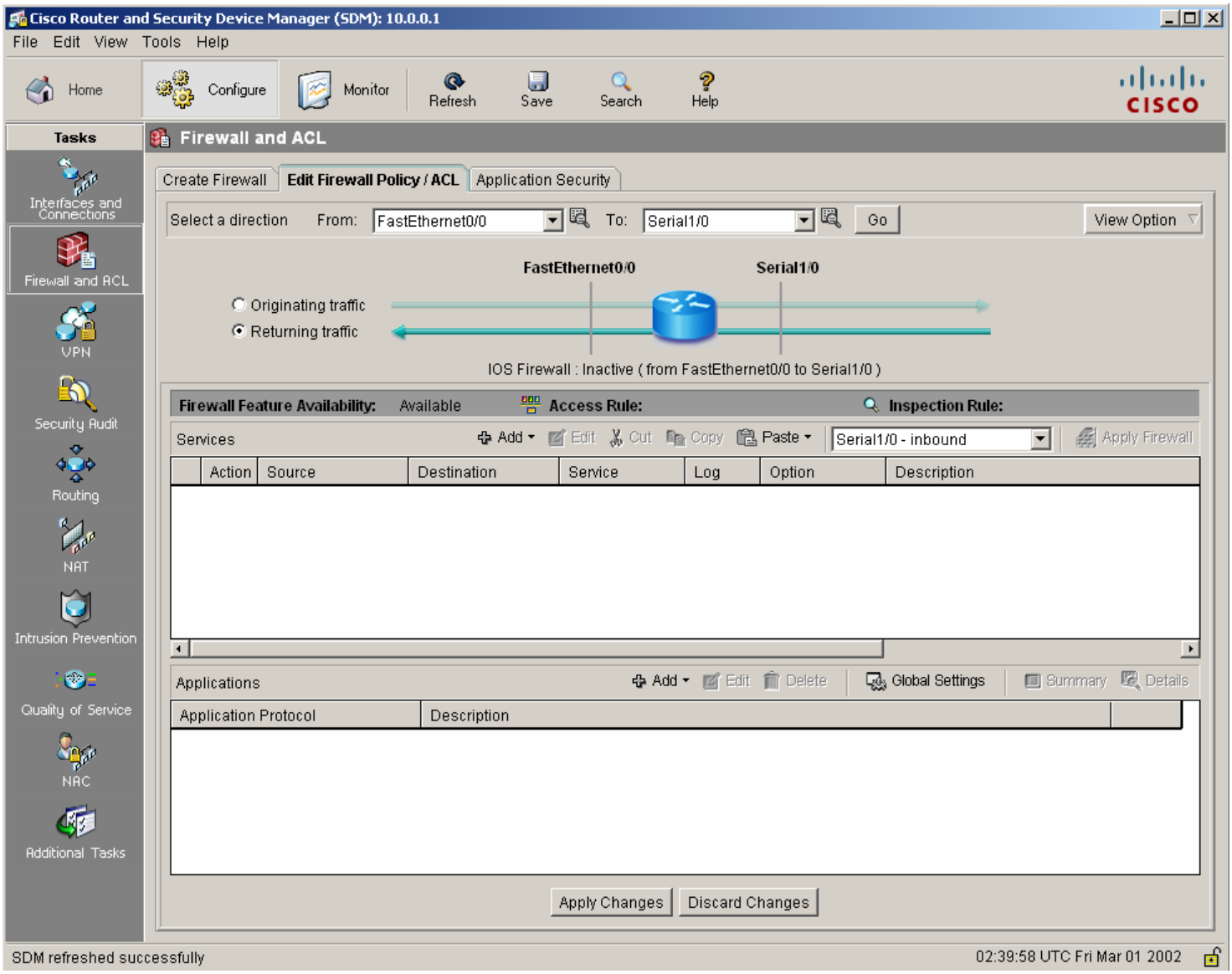

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial1/0
Go
View Option
FastEthernet0/0
Serial1/0
Originating traffic
Returning traffic
IOS Firewall : Active (from FastEthernet0/0 to Serial1/0)
Firewall Feature Availability: Available
Access Rule: 101
Inspection Rule: SDM_LOW
Services
Add
Edit
Cut
Copy
Paste
Serial1/0 - inbound
Apply Firewall
Action
Source
Destination
Service
Log
Option
Description
Permit 13.0.0.5 10.0.0.5 dest: neq teln Log Allow Telnet From(13.0.0.5) To (10.0.0.5)
Deny 10.0.0.0/0.255.25 any ip
Permit any 11.0.0.1 echo-reply/icn
Permit any 11.0.0.1 time-exceede
Permit any 11.0.0.1 unreachable/i
Permit any any eigrp
Deny 172.16.0.0/0.15.2 any ip
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Description
cuseeme CUSeeMe Protocol
dns Domain Name Server
ftp File Transfer Protocol
h323 H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
https HTTPS Protocol
icmp ICMP Protocol
imap IMAP Protocol
Apply Changes
Discard Changes
Firewall and ACL
02:21:33 UTC Fri Mar 01 2002


C:\WINDOWS\system32\cmd.exe
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 13.0.0.5
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 13.0.0.1
C:\>ping 10.0.0.5
Pinging 10.0.0.5 with 32 bytes of data:
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Reply from 11.0.0.1: Destination net unreachable.
Ping statistics for 10.0.0.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>telnet 10.0.0.5


Telnet 10.0.0.5
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'
You are about to send your password information to a remote computer in Internet zone. This might not be safe. Do you want to send anyway(y/n):


Telnet 10.0.0.5
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password
Welcome to Microsoft Telnet Service
login:


Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
Tasks
Overview
Interface Status
Firewall Status
VPN Status
Traffic Status
QoS Status
NAC Status
Logging
IPS Status
802.1x Status
Logging
Syslog
Firewall Log
SDEE Message Log
Application Security Log
Logging Buffer: Enabled
Logging Hosts: None
Logging Level (Buffer): debugging
Number of messages in log: 1
Select a Logging level to view debugging
Each row represent one log entry.
Update
Clear
Search...
Severity
Time
Description
information: Mar 1 02:28:26.163 list 101 permitted tcp 13.0.0.5(3771) -> 10.0.0.5(23), 1 packet
Done.
02:29:03 UTC Fri Mar 01 2002

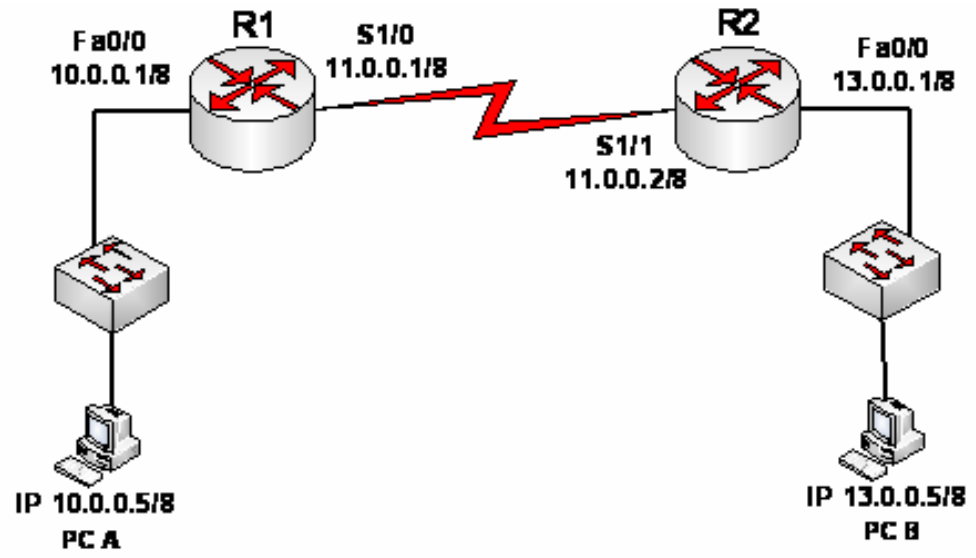

Cisco Router and Security Device Manager (SDM): 10.0.0.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
Tasks
Interfaces and Connections
Firewall and ACL
VPN
Security Audit
Routing
NAT
Intrusion Prevention
Quality of Service
NAC
Additional Tasks
Firewall and ACL
Create Firewall
Edit Firewall Policy / ACL
Application Security
Select a direction
From: FastEthernet0/0
To: Serial1/0
Go
View Option
FastEthernet0/0
Serial1/0
Originating traffic
Returning traffic
IOS Firewall : Inactive (from FastEthernet0/0 to Serial1/0)
Firewall Feature Availability: Available
Access Rule:
Inspection Rule:
Services
Add
Edit
Cut
Copy
Paste
Serial1/0 - inbound
Apply Firewall
Action
Source
Destination
Service
Log
Option
Description
Applications
Add
Edit
Delete
Global Settings
Summary
Details
Application Protocol
Description
Apply Changes
Discard Changes
SDM refreshed successfully
02:39:58 UTC Fri Mar 01 2002

LAB # 11

Site-to-Site VPN using CLI

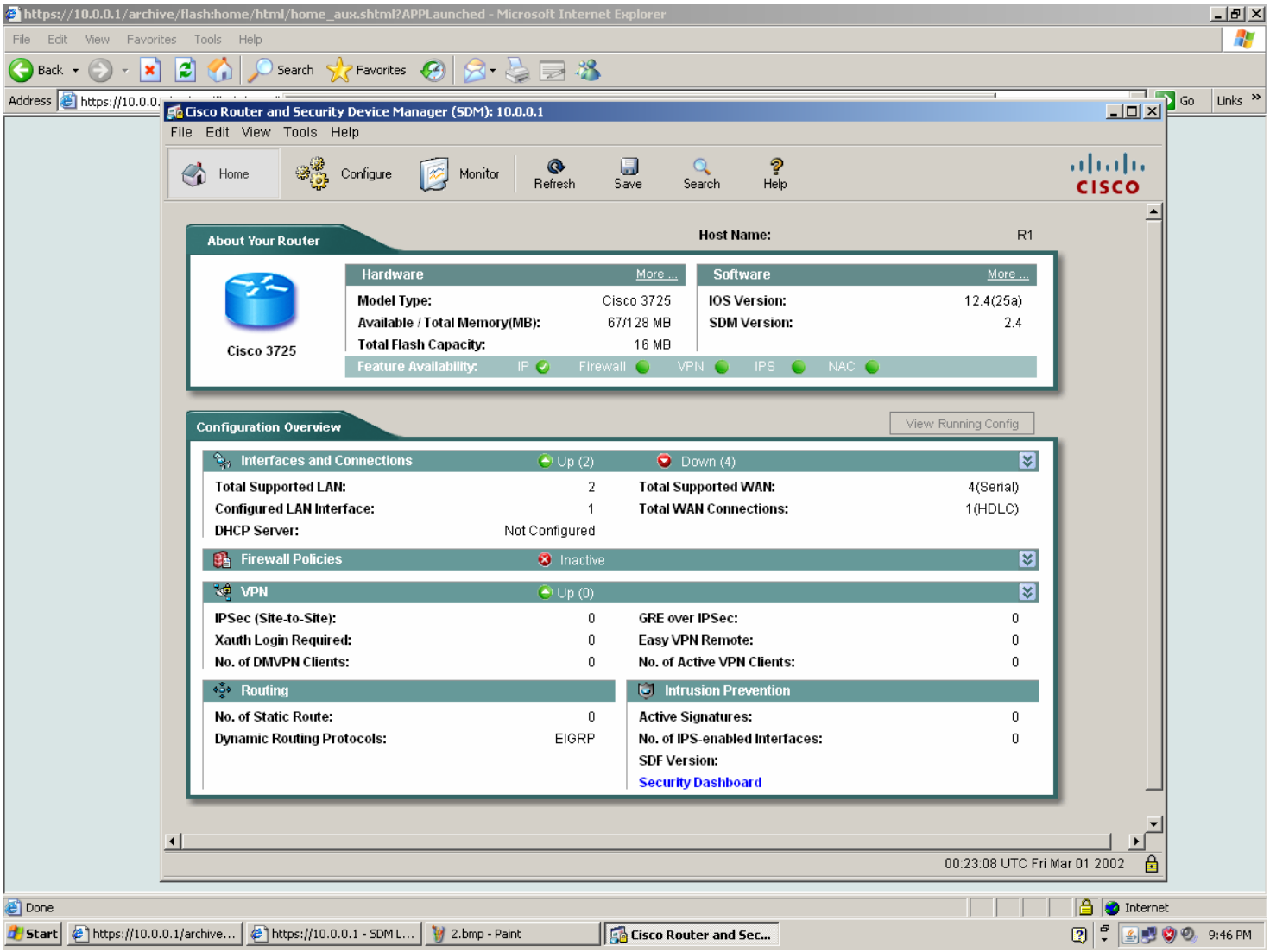
Objective

Establish Site-to-Site VPN between 2 VPN Gateways i.e Router 1 and Router 2 using PRE-SHARED KEYS for authentication.

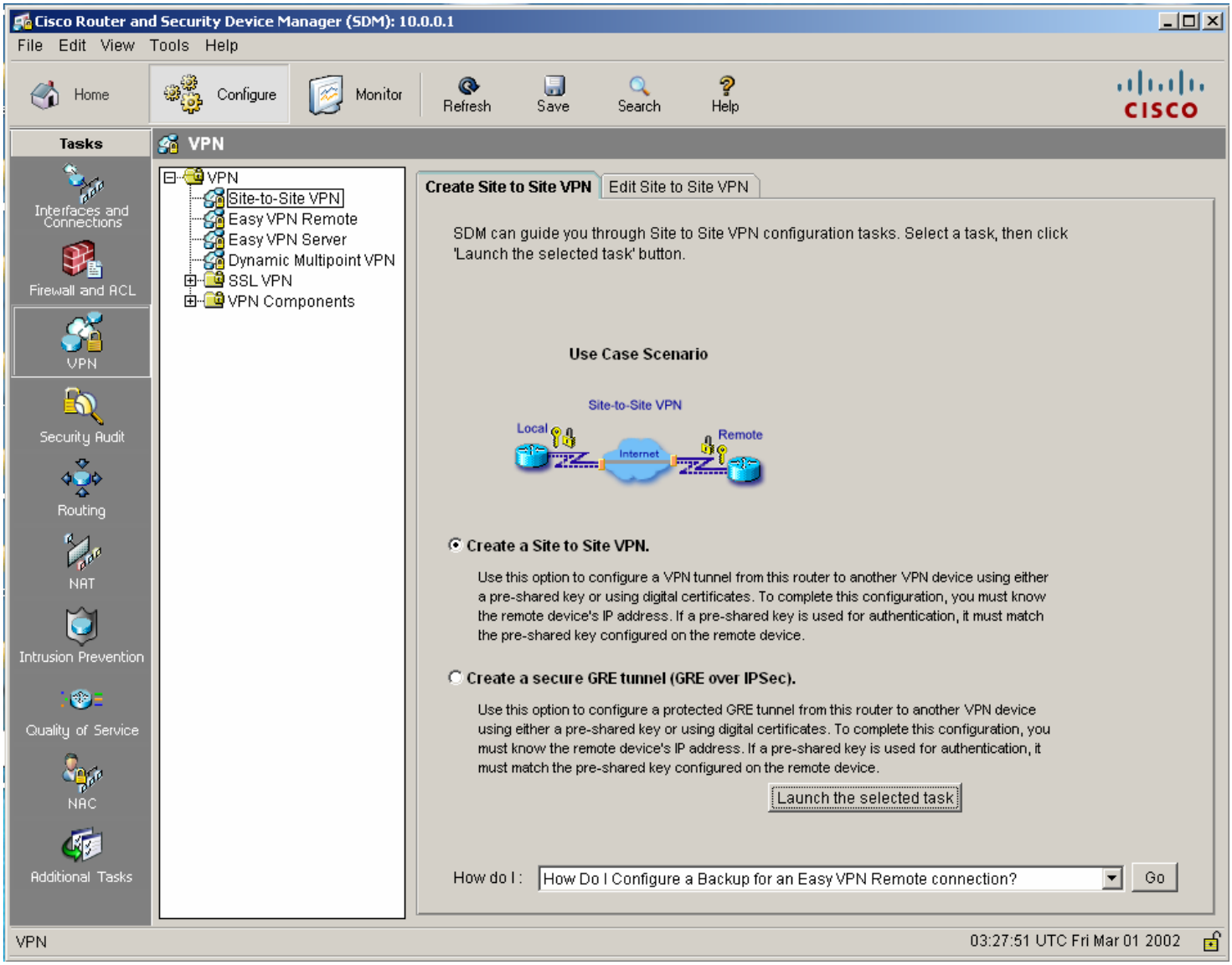


1) Bring up the connections and ping end to end.
2) From PC-A opens the browser and issues this command.
   http://10.0.0.1

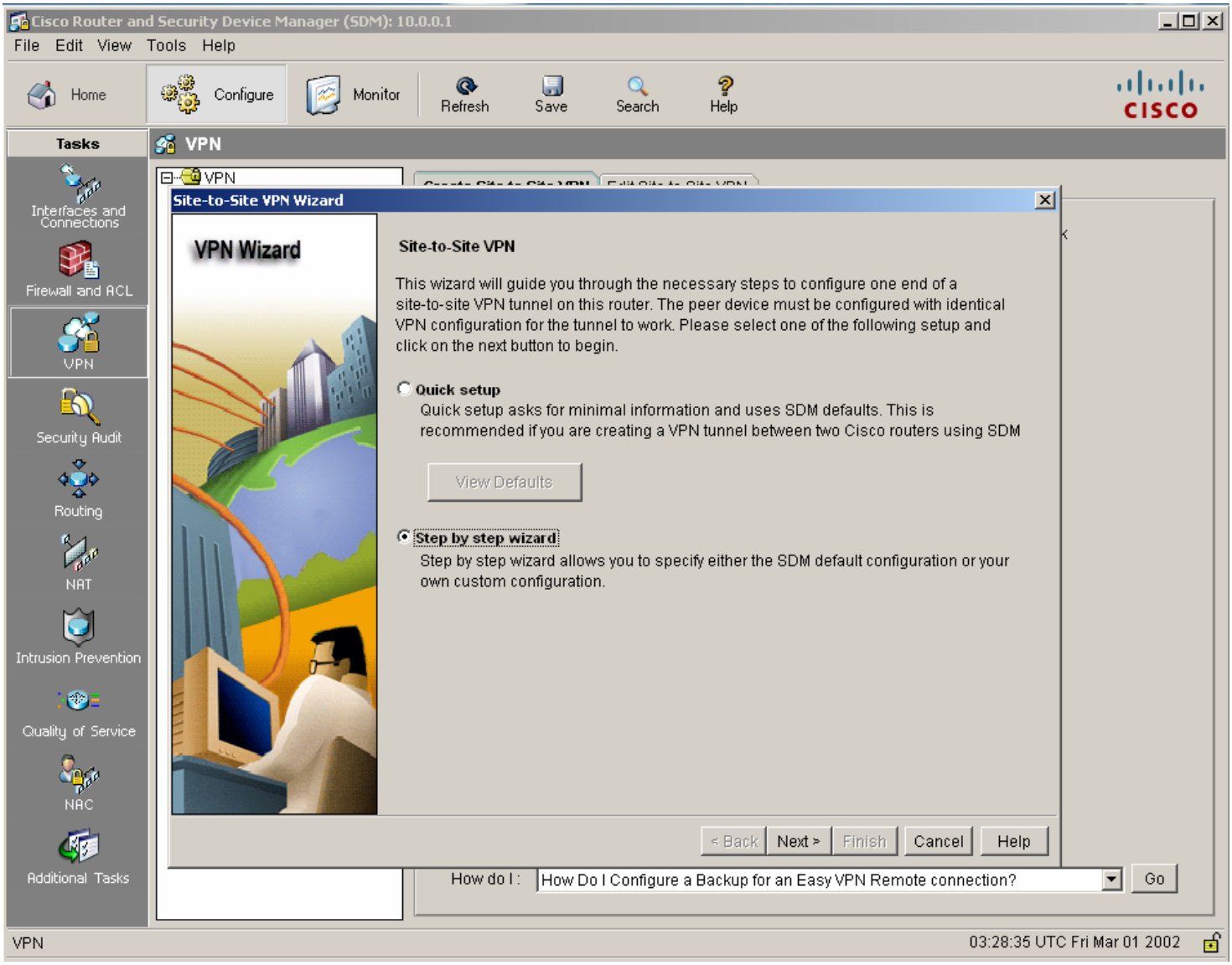
3) Now the following windows appears, Click on the configure tab above



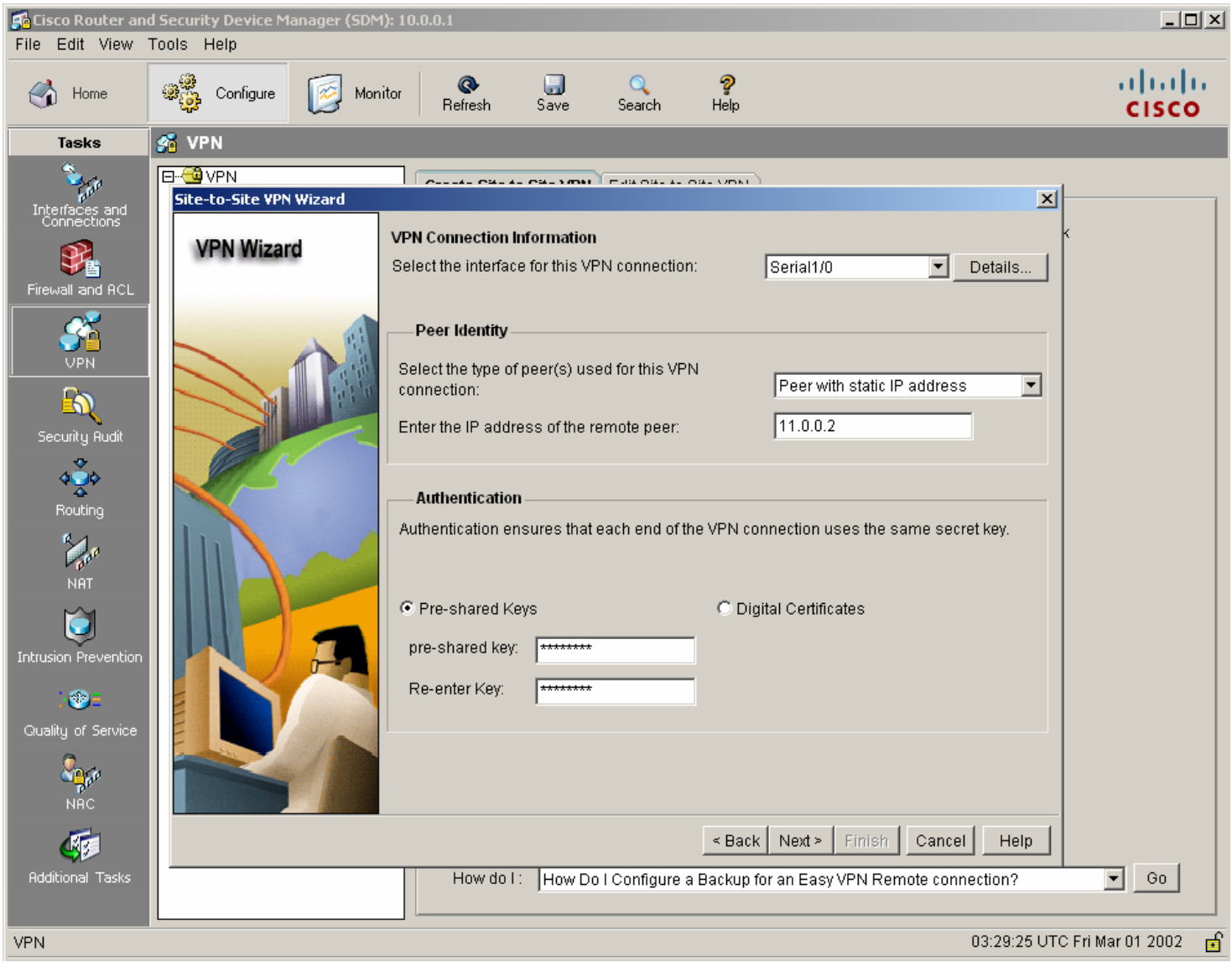
4) Clicking on Configure tab opens the list of configuration options available, select VPN from the left menu, now at left click on Create site to site vpn radio button and then click on the launch the selected task button to launch the wizard…



5) Now the wizard will start, click on the step by step wizard radio button and then click next



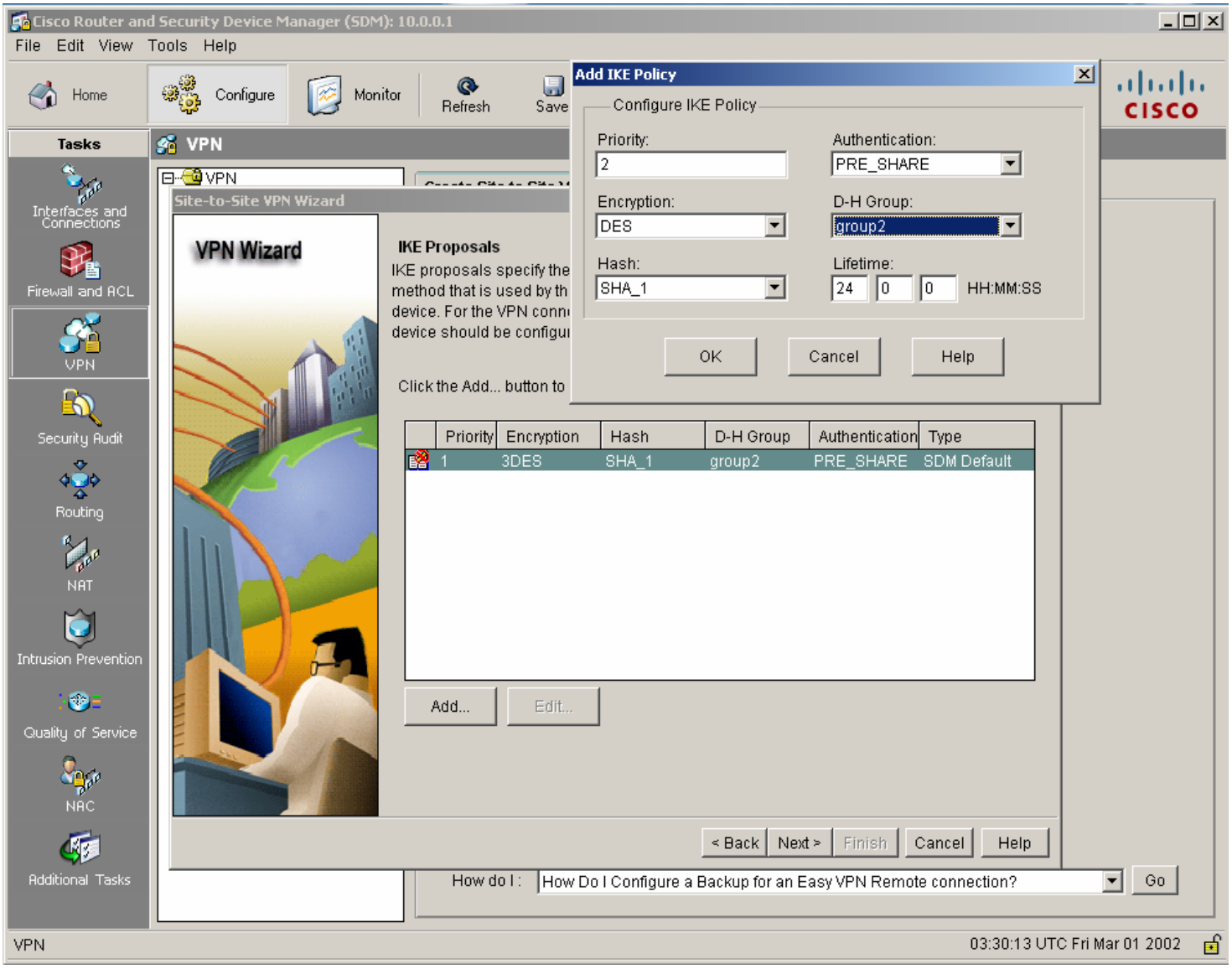
6) Now from the following window,
    1. Select the interface that is connected to Router 2.
    2. Specify that the peer is using the static ip address.
    3. Enter the ip address.
    4. Enter the preshared key for authentication used in ISAKMP phase 1



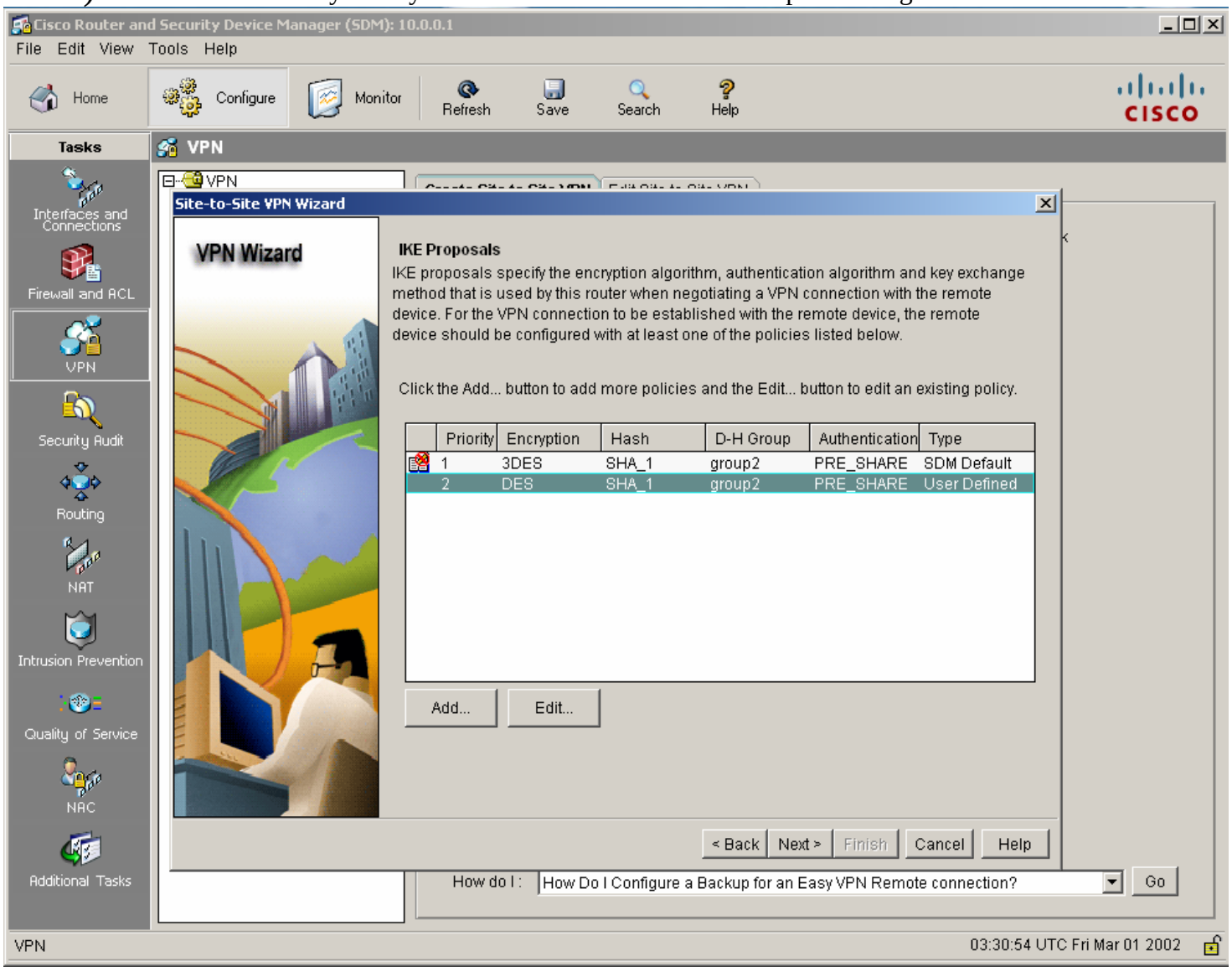
7). In this window, we have to define transform set for phase 1, click on the Add button to define our own transform set.

8). In this window, define your own parameters for the transform set and then click OK.

9). Now click Next

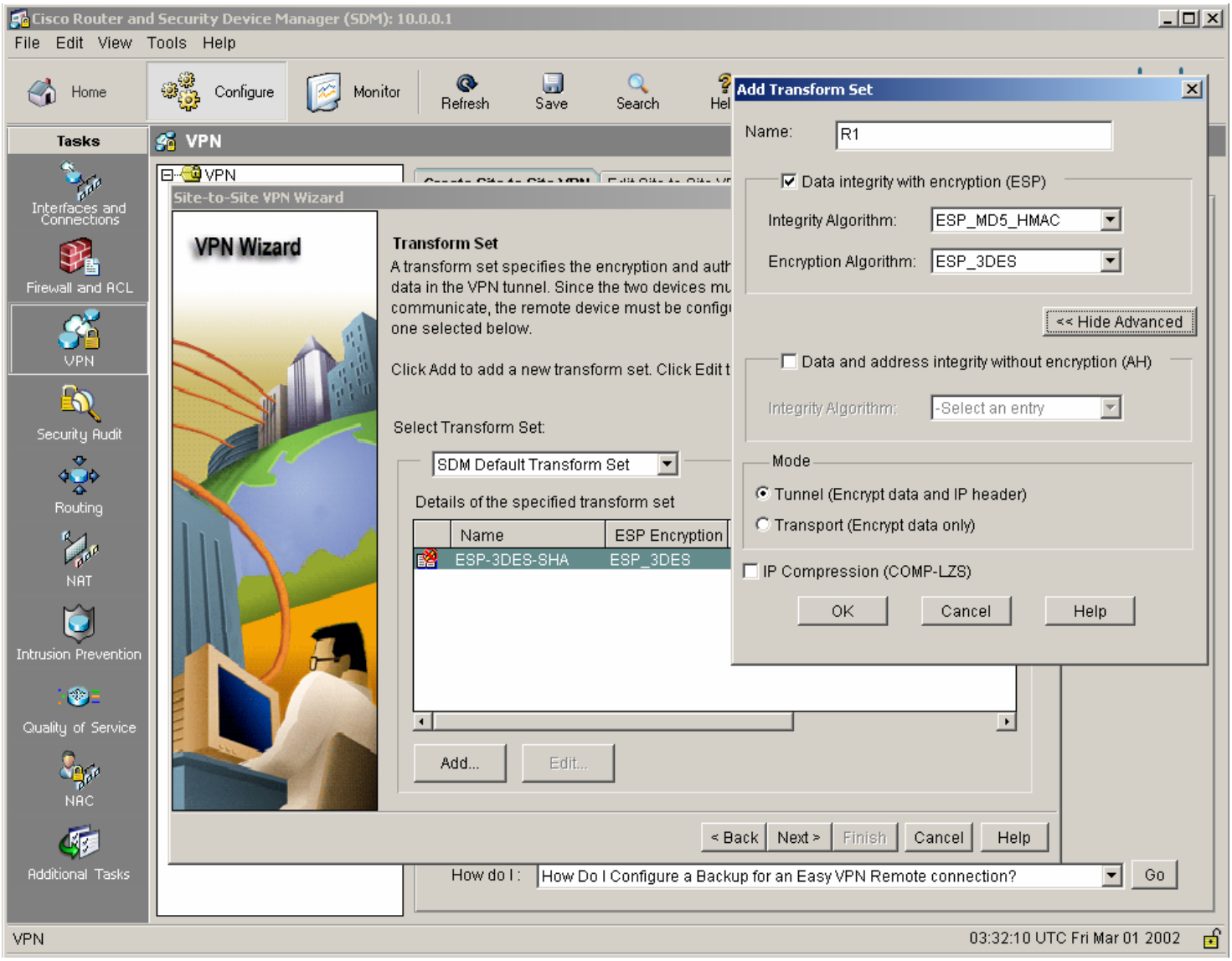


10).Now in this window you may define transform set for IPSec or phase 2 negotiation…

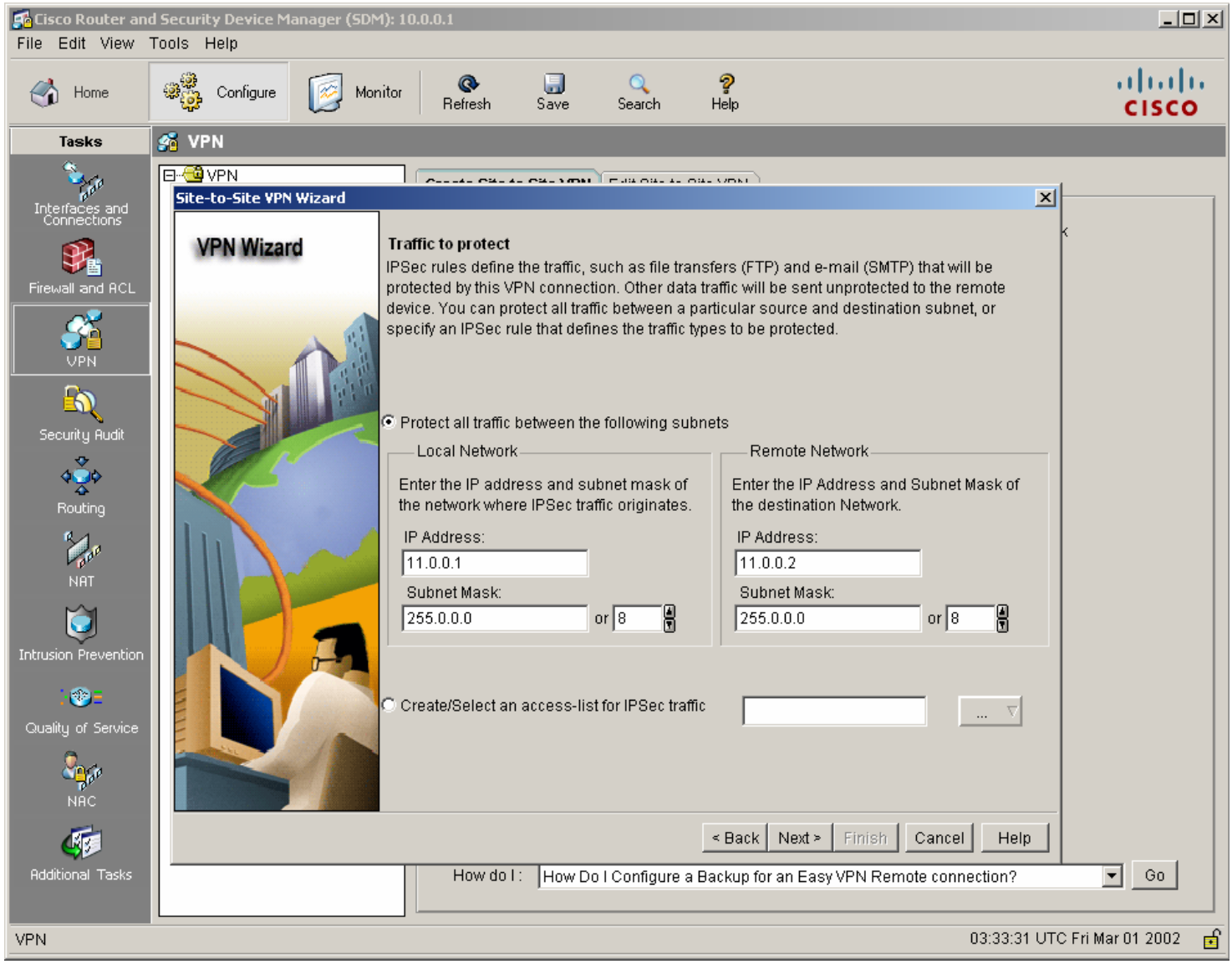


11). Now define the required parameters and click Ok.

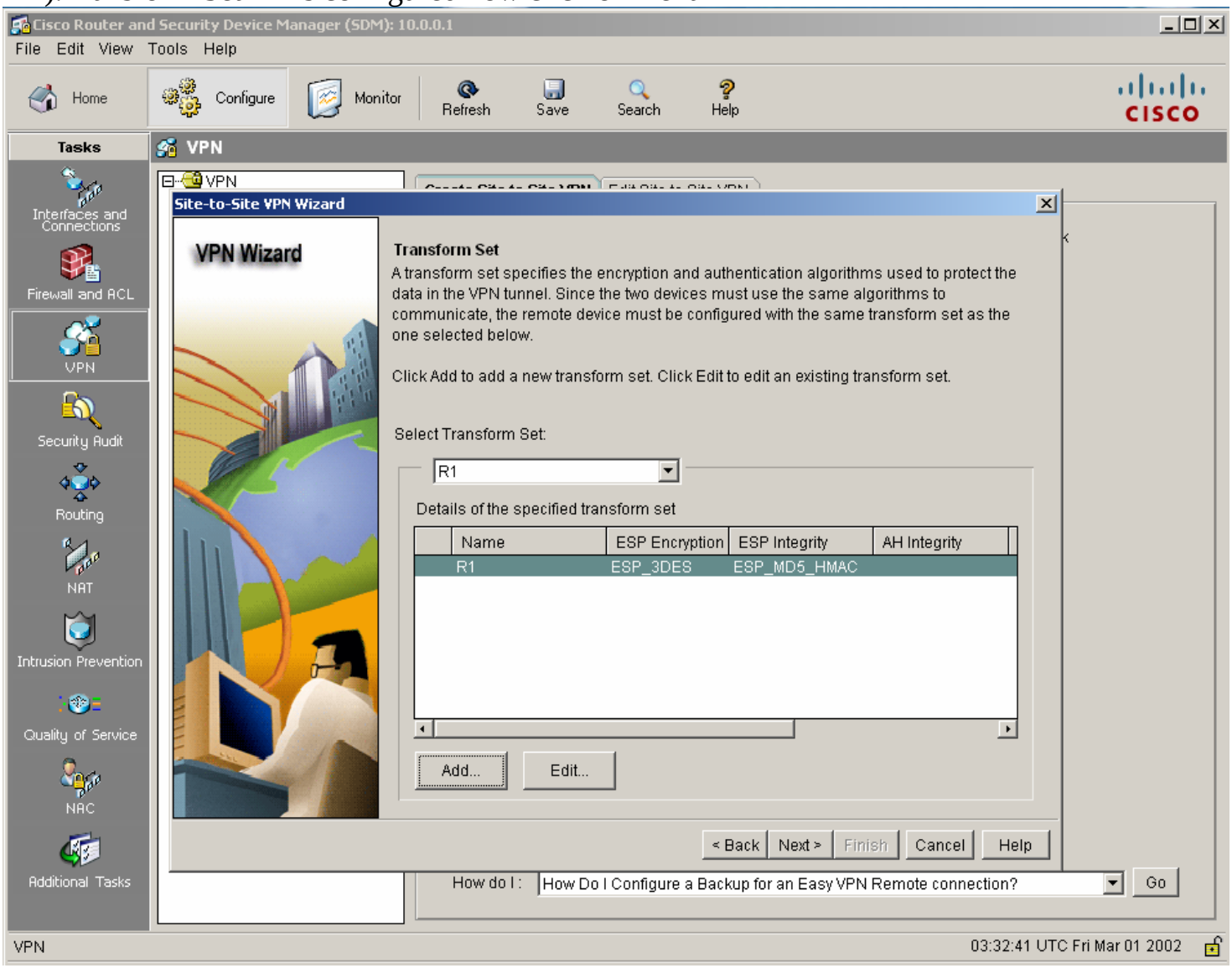
12). Now we can see that user defined Transform set is now listed. Click Next to continue.



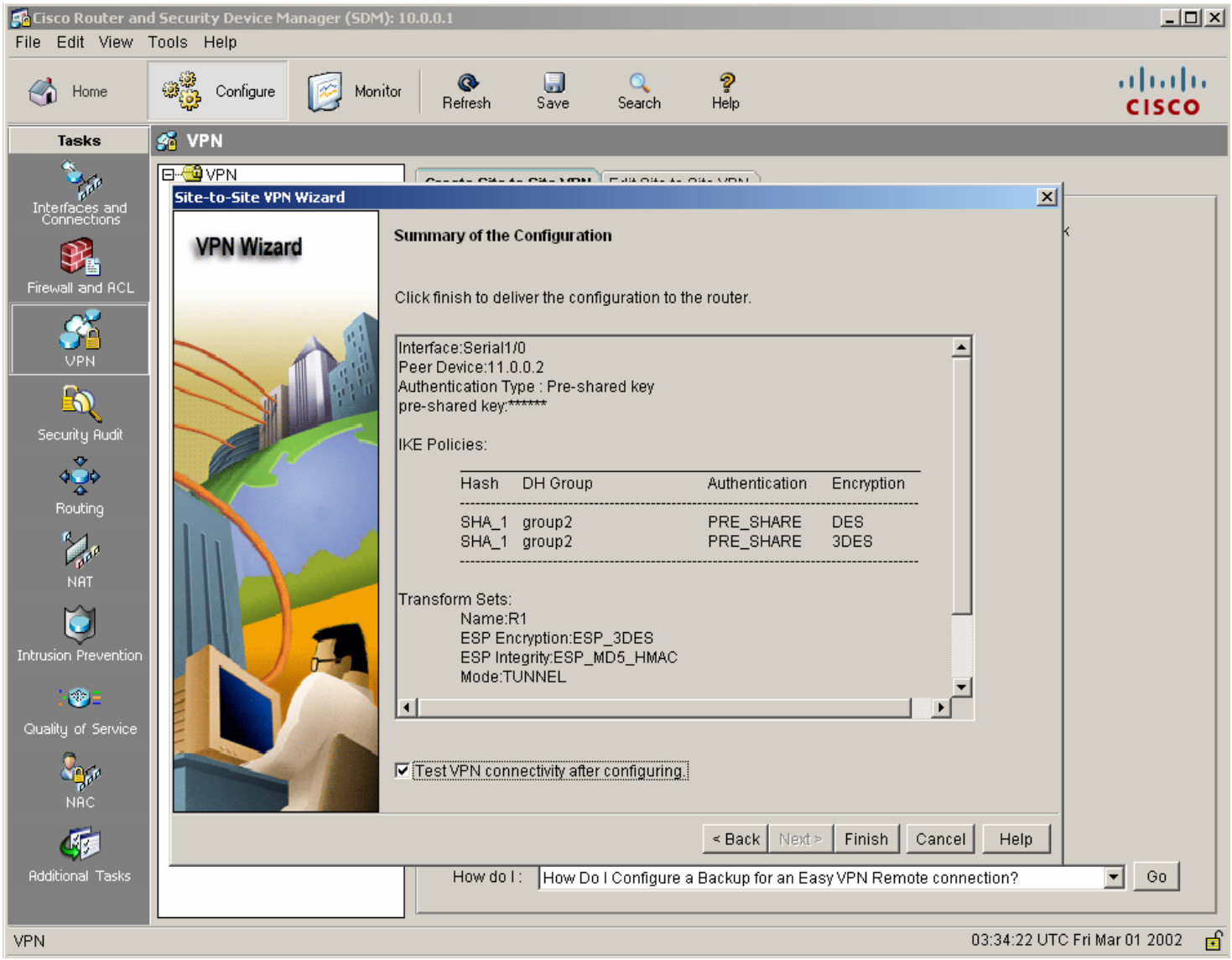
13) Now define the traffic to be protected



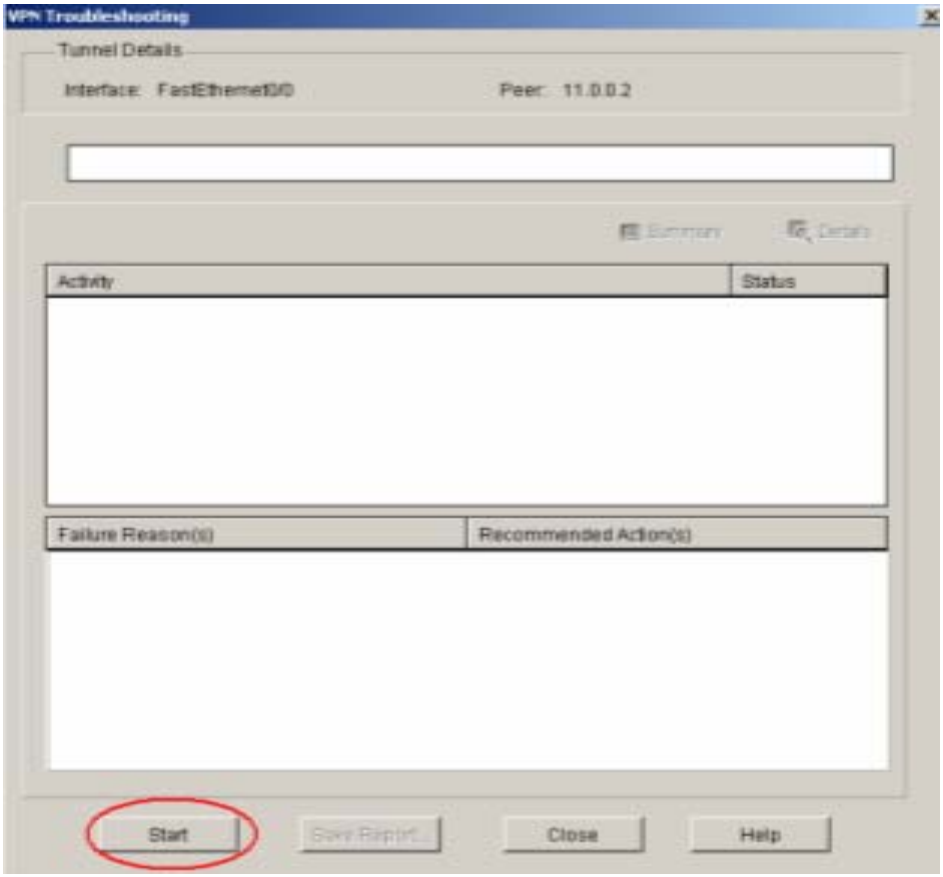
14).Transform Set R1 is configured now click on Next



15). Now the following window appears indicating that the wizard is complete

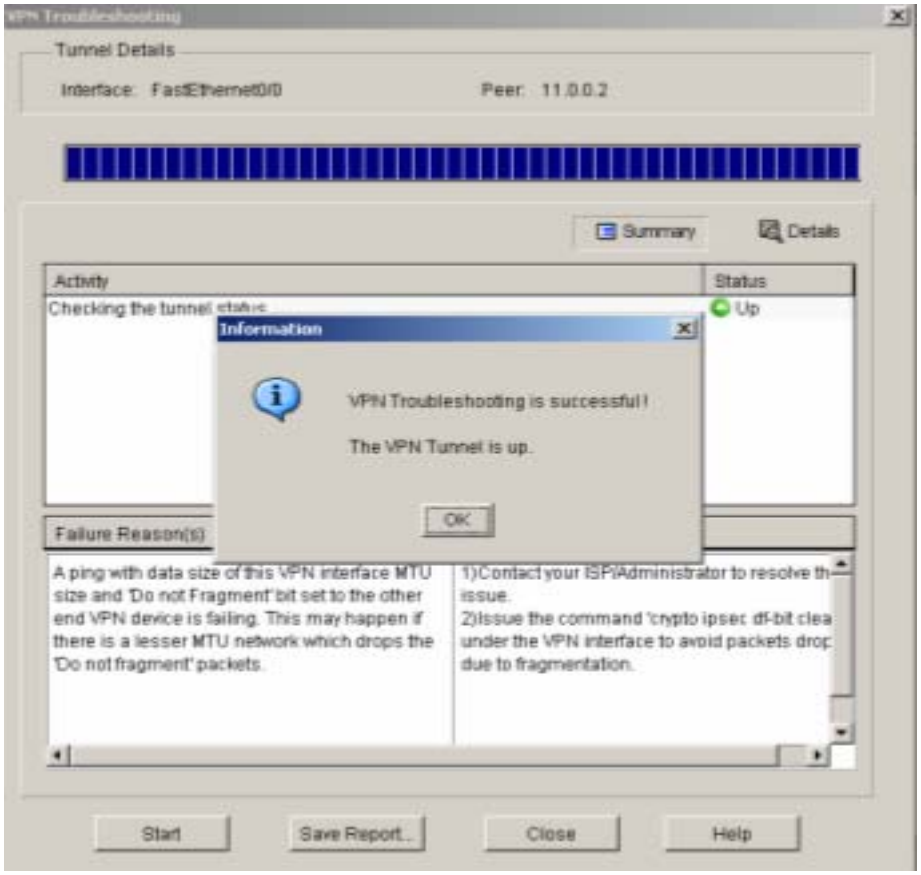


16). Click on the start button to test the tunnel connectivity.



17) If all configuration goes well then u should see the following screen..

Note: test the tunnl connectivity after u have configured Router 2 for IPSec !!!!



Configure Router 2 with CLI as show below.

first enable isakmp

Router2(config)# crypto isakmp enable (*optional*)

Configure isakmp policy set for negotiation

```
Router2(config)# crypto isakmp policy 10
Router2(config-isakmp)# authentication pre-share
Router2(config-isakmp)# encryption des
Router2(config-isakmp)# hash SHA_1
Router2(config-isakmp)# group 2
```

Configure pre-shared authentication key

Router2(config)# crypto isakmp key *cisco123* address 11.0.0.1

Configure cryto ACL to define which traffic to protect

Router2(config)# access-list 111 permit ip host 13.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255

Configure IPSec transform-set

Router2(config)# crypto ipsec transform-set R2 esp-3des esp-md5-hmac

Configure Crypto-map

```
Router2(config)# crypto map mymap 10 ipsec-isakmp
Router2(config-crypto-map)# match address 111
Router2(config-crypto-map)# set peer 11.0.0.1
Router2(config-crypto-map)# set transform-set R2
```

Apply the crypto map to the WAN interface

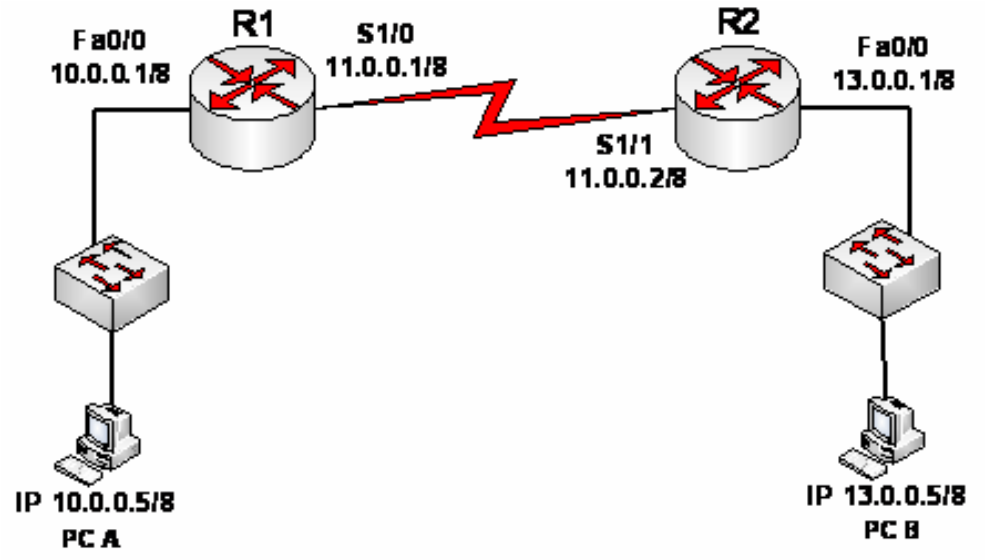
```
Router2(config)# int s 1/1
Router2(config-if)# crypto map mymap
```

LAB # 11

AAA Server Configuration

Objective

Configure AAA server to perform user authentication and accounting.

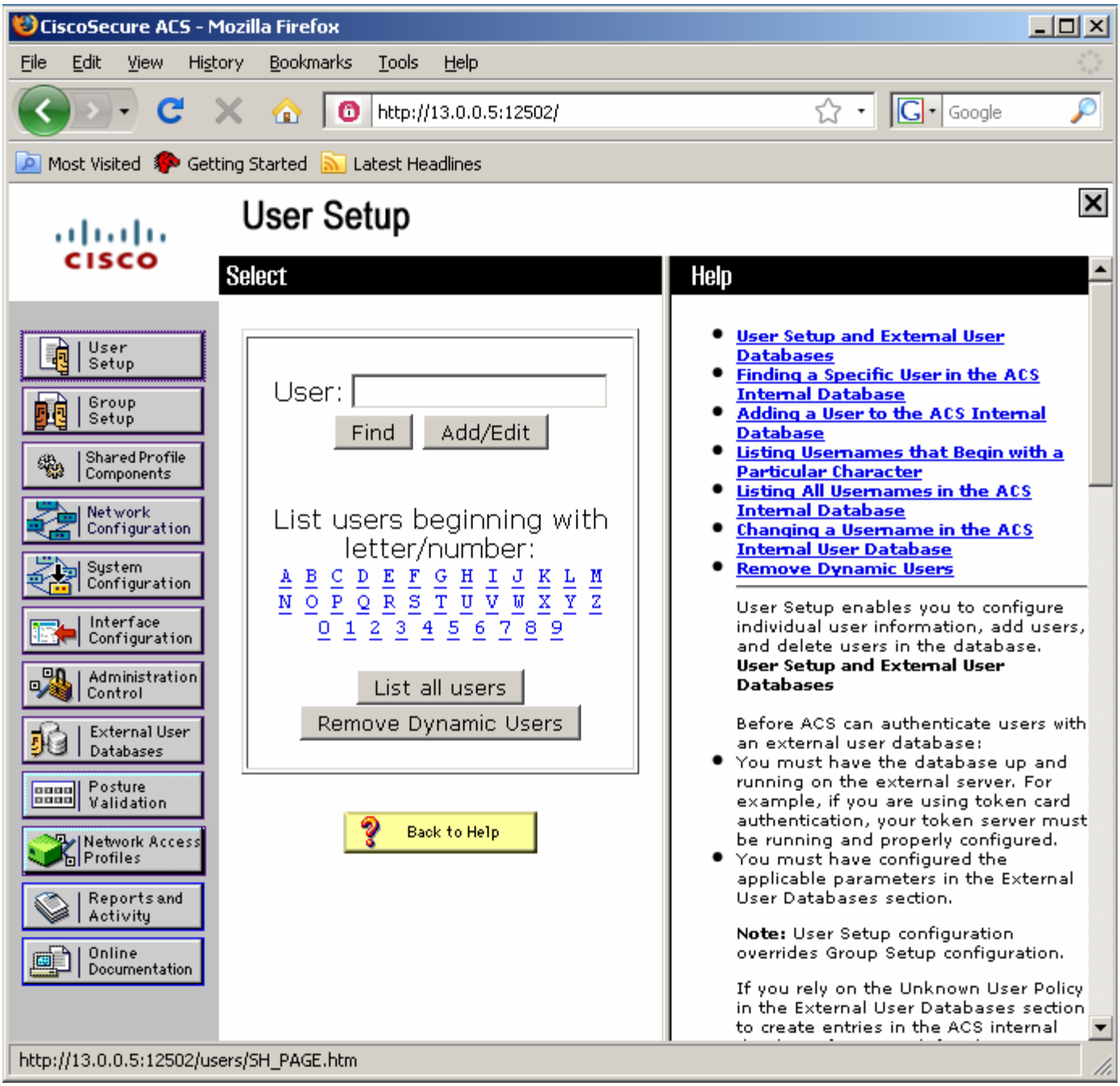


Configuration

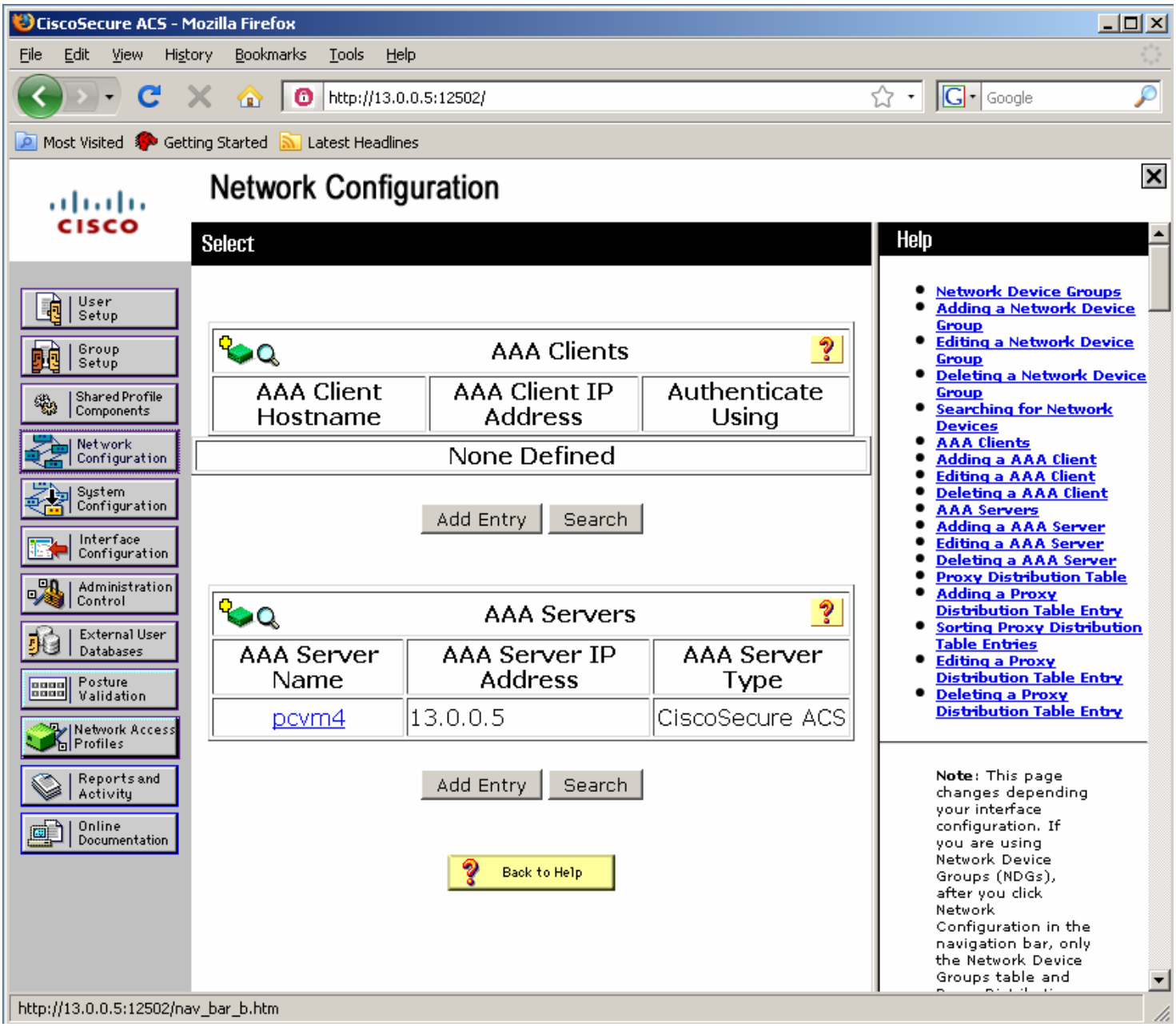
Configuraion on R2

R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#aaa accounting commands 15 default start-stop group tacacs+
R2(config)#aaa accounting exec default start-stop group tacacs+

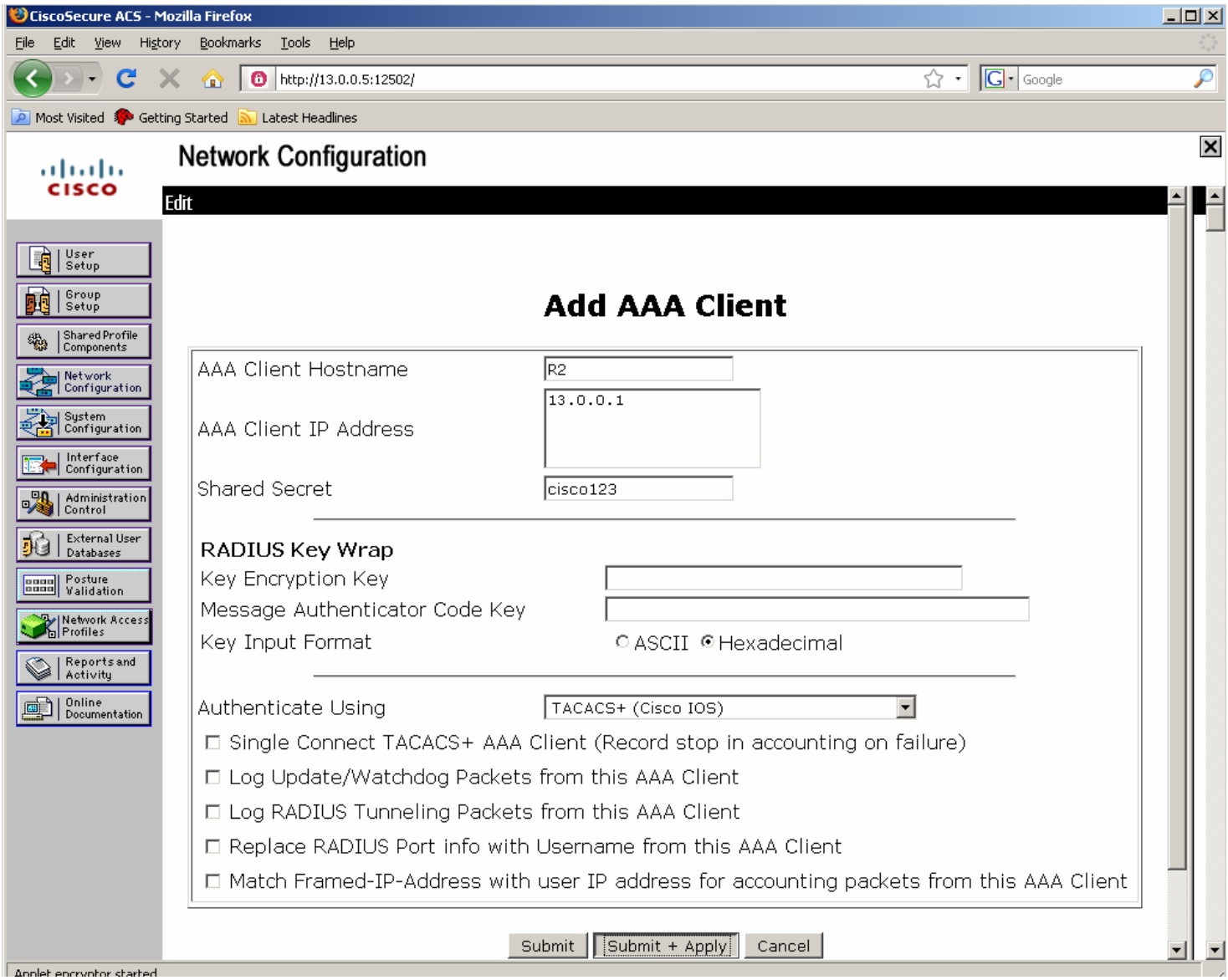
1) Bring up the connections and ping end to end.
2) Install ACS for windows.
3) Configure ACS as follows
4) Enter the user setup and enter the username. Click on Add/Edit to define the Password

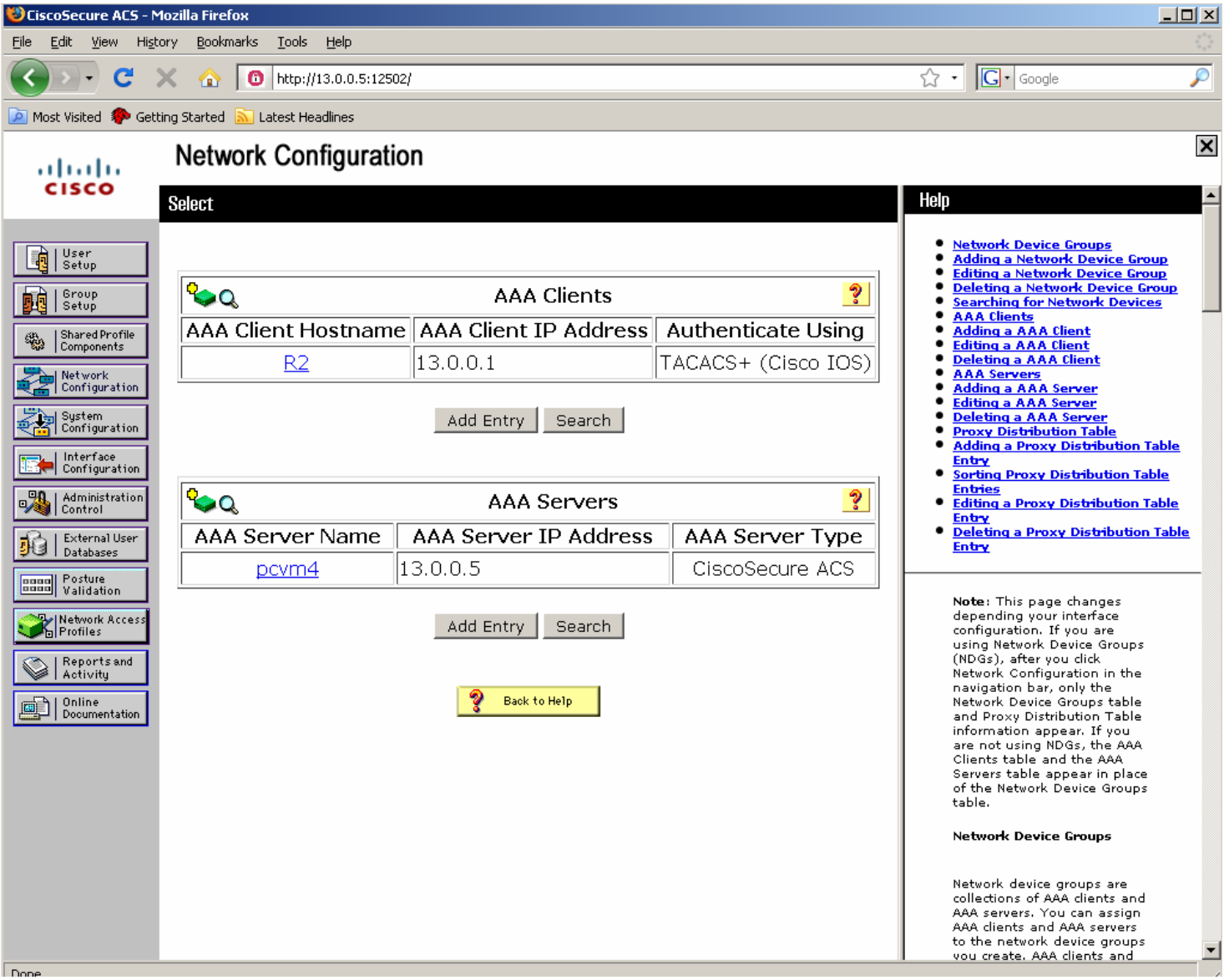


Configure Network Configuration click on **Network Congfiguration.**
Then click on AAA Client **Add Entry**

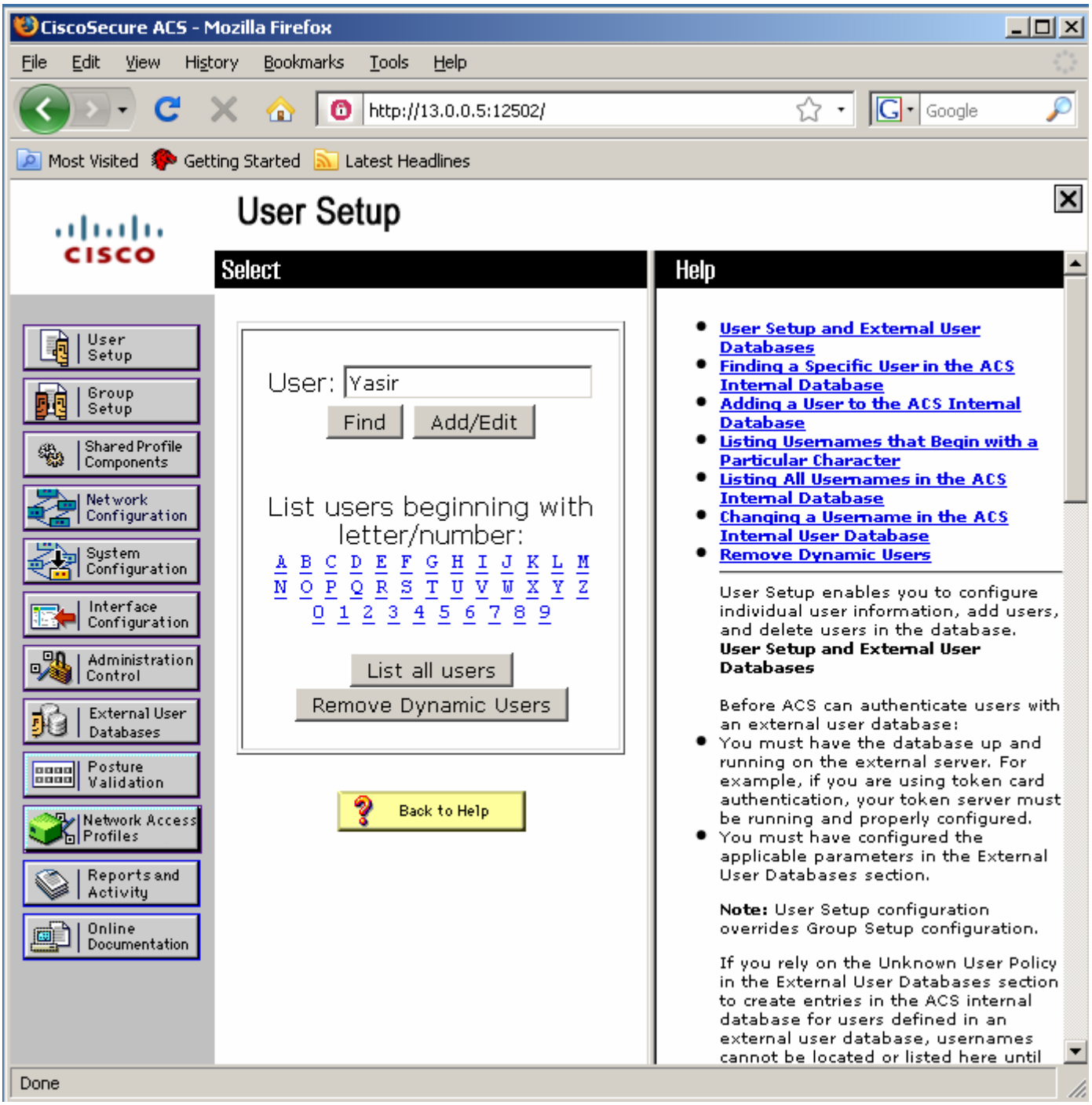


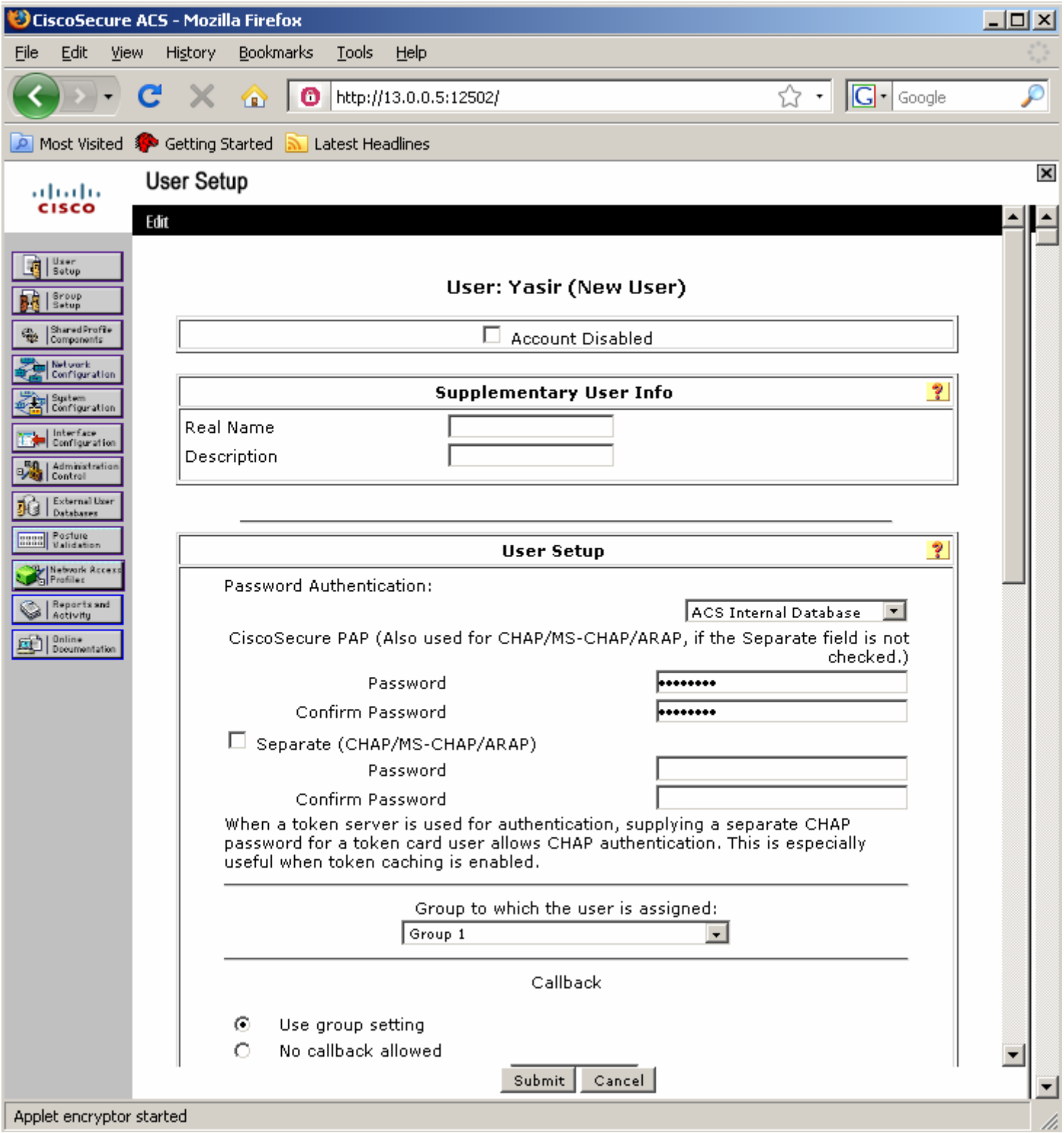
Configure Ip Address of the Client, Here Router 1 is your client Set Shared Secret Key.
Then click on **Submit + Apply**

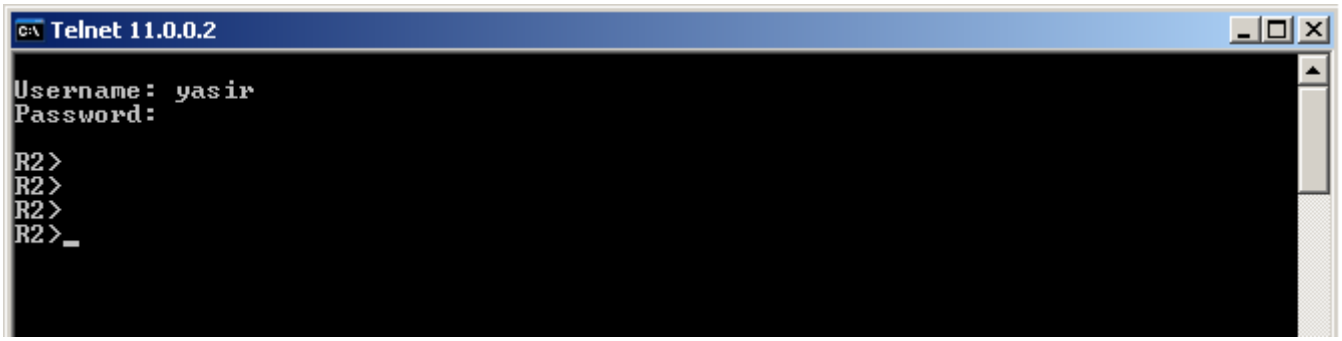



CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
Network Configuration
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
AAA Clients
AAA Client Hostname
AAA Client IP Address
Authenticate Using
R2
13.0.0.1
TACACS+ (Cisco IOS)
Add Entry
Search
AAA Servers
AAA Server Name
AAA Server IP Address
AAA Server Type
pcvm4
13.0.0.5
CiscoSecure ACS
Add Entry
Search
Back to Help
Help
Network Device Groups
Adding a Network Device Group
Editing a Network Device Group
Deleting a Network Device Group
Searching for Network Devices
AAA Clients
Adding a AAA Client
Editing a AAA Client
Deleting a AAA Client
AAA Servers
Adding a AAA Server
Editing a AAA Server
Deleting a AAA Server
Proxy Distribution Table
Adding a Proxy Distribution Table Entry
Sorting Proxy Distribution Table Entries
Editing a Proxy Distribution Table Entry
Deleting a Proxy Distribution Table Entry
Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.
Network Device Groups
Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and
Done

Add User Database in the ACS server.
Click on **User Step, Add user name and then click**




CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
User Setup
Edit
User Setup
Group Setup
SharedProfile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: Yasir (New User)
Account Disabled
Supplementary User Info
Real Name
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
Confirm Password
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Group 1
Callback
Use group setting
No callback allowed
Submit
Cancel
Applet encryptor started



CiscoSecure ACS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://13.0.0.5:12502/

Most Visited Getting Started Latest Headlines

Reports and Activity

Select

TACACS+ Accounting active.csv Refresh Download

Regular Expression | Start Date & Time | End Date & Time | Rows per Page

mm/dd/yyyy,hh:mm:ss | mm/dd/yyyy,hh:mm:ss | 50

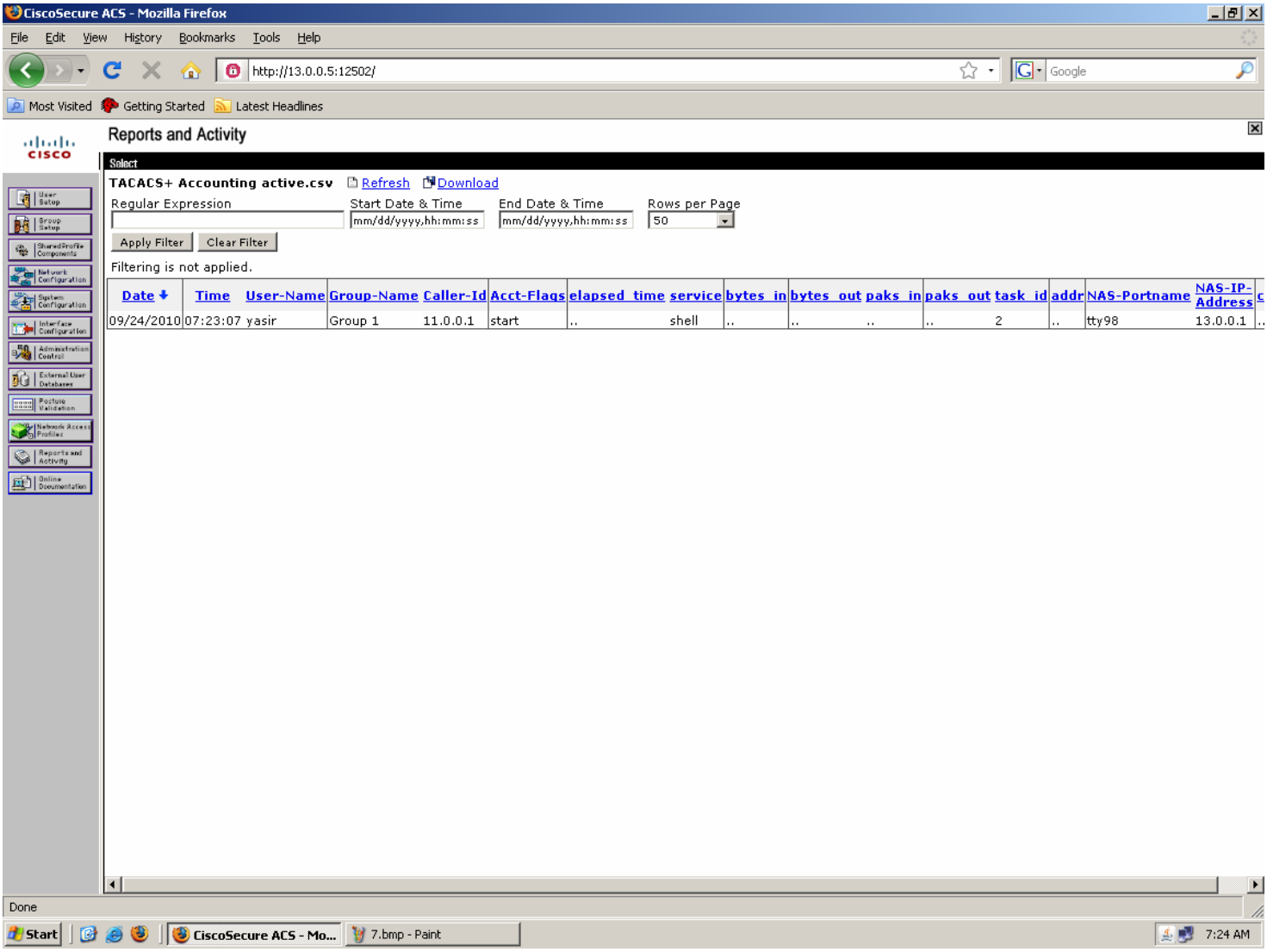
Apply Filter Clear Filter

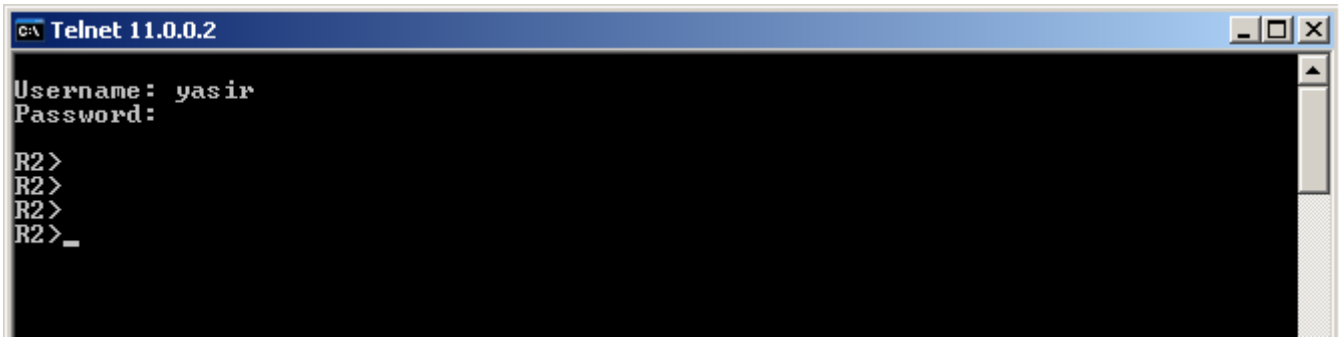
Filtering is not applied.

Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in	bytes_out	paks_in	paks_out	task_id	addr	NAS-Portname	NAS-IP-Address	c
09/24/2010	07:23:07	yasir	Group 1	11.0.0.1	start	..	shell	..	..	..	..	2	..	tty98	13.0.0.1	..

Done

Start | CiscoSecure ACS - Mo... | 7.bmp - Paint | 7:24 AM


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
Reports and Activity
Select
TACACS+ Accounting active.csv Refresh Download
Regular Expression
Start Date & Time
End Date & Time
Rows per Page
mm/dd/yyyy,hh:mm:ss
mm/dd/yyyy,hh:mm:ss
50
Apply Filter Clear Filter
Filtering is not applied.
Date Time User-Name Group-Name Caller-Id Acct-Flags elapsed_time service bytes_in bytes_out paks_in paks_out task_id addr NAS-Portname NAS-IP-Address
09/24/2010 07:23:07 yasir Group 1 11.0.0.1 start .. shell .. .. 2 .. tty98 13.0.0.1
Done
Start
CiscoSecure ACS - Mo...
7.bmp - Paint
7:24 AM



CiscoSecure ACS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://13.0.0.5:12502/

Most Visited Getting Started Latest Headlines

Reports and Activity

Select

TACACS+ Accounting active.csv Refresh Download

Regular Expression | Start Date & Time | End Date & Time | Rows per Page

Regular Expression	Start Date & Time	End Date & Time	Rows per Page
	mm/dd/yyyy,hh:mm:ss	mm/dd/yyyy,hh:mm:ss	50

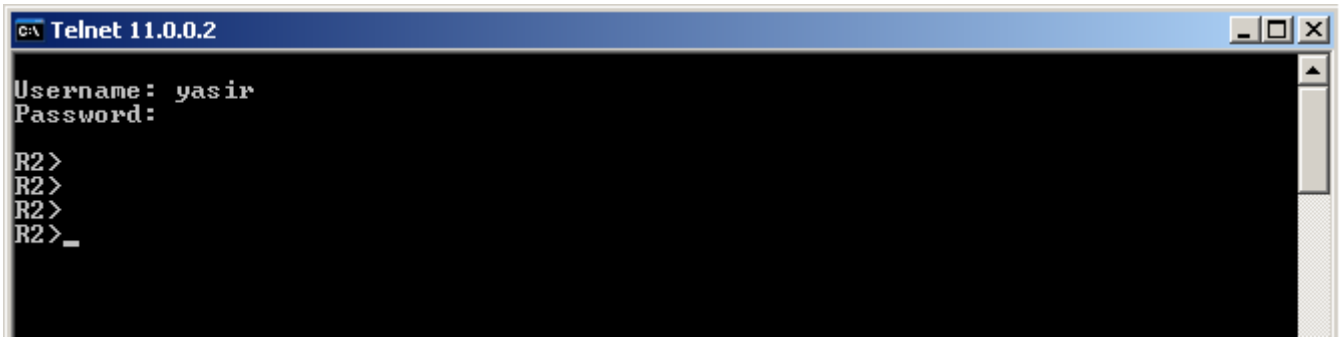
Apply Filter Clear Filter

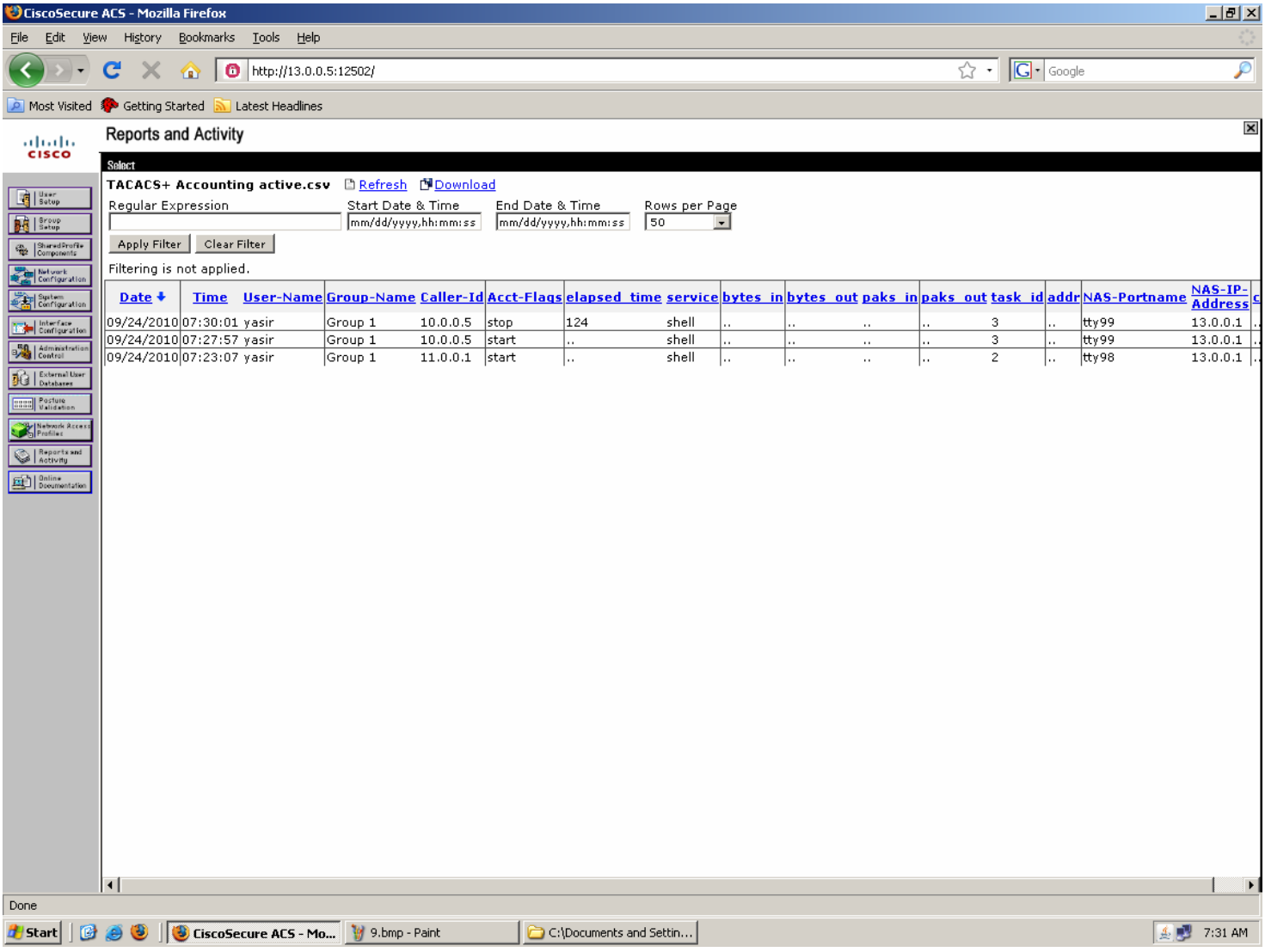
Filtering is not applied.

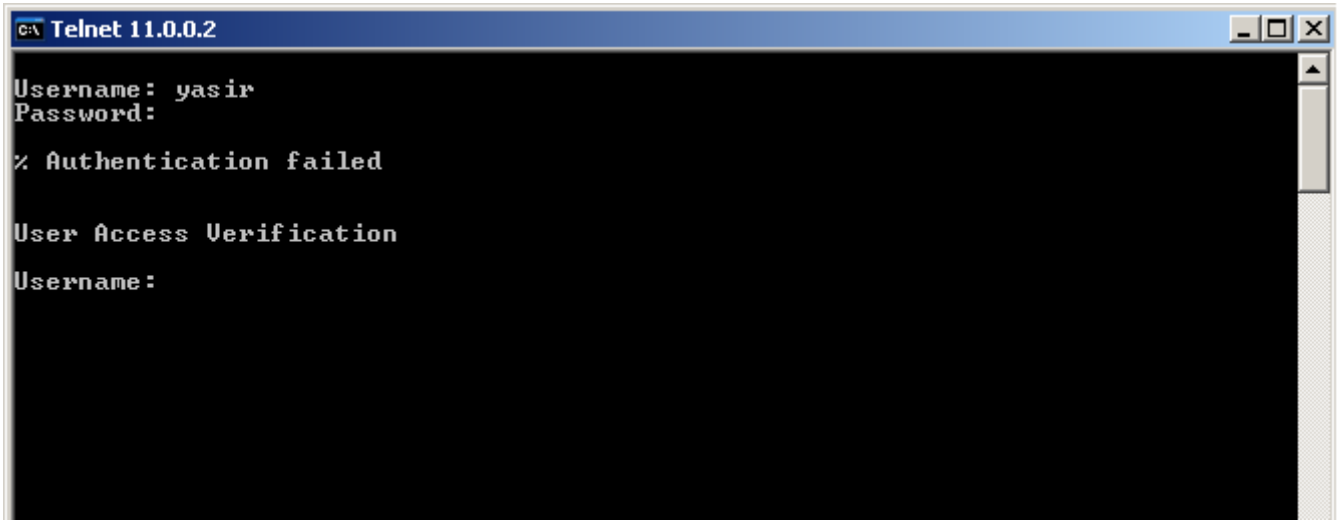
Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in	bytes_out	paks_in	paks_out	task_id	addr	NAS-Portname	NAS-IP-Address
09/24/2010	07:27:57	yasir	Group 1	10.0.0.5	start	..	shell	..	..	..	..	3	..	tty99	13.0.0.1
09/24/2010	07:23:07	yasir	Group 1	11.0.0.1	start	..	shell	..	..	..	..	2	..	tty98	13.0.0.1

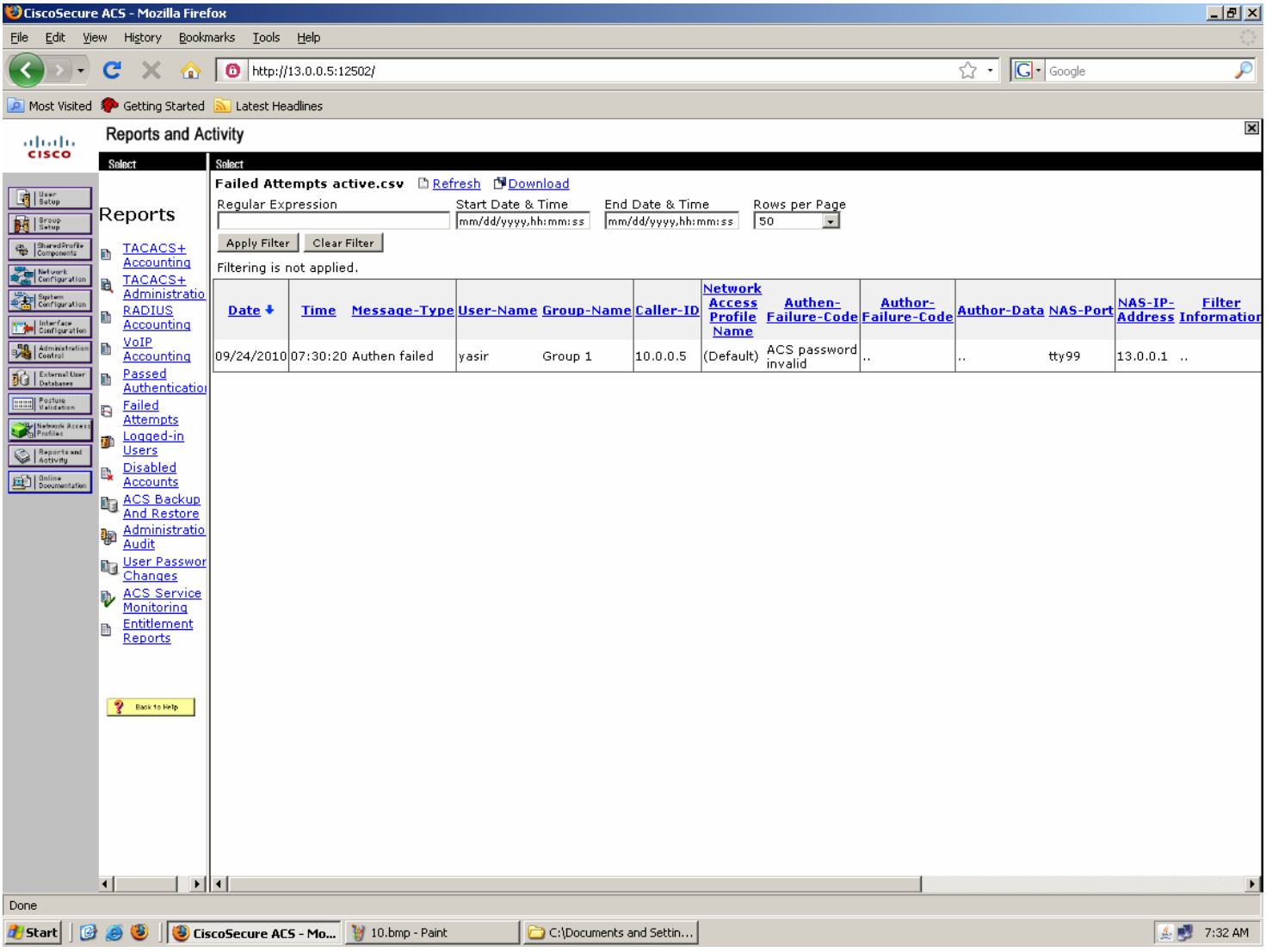
Done

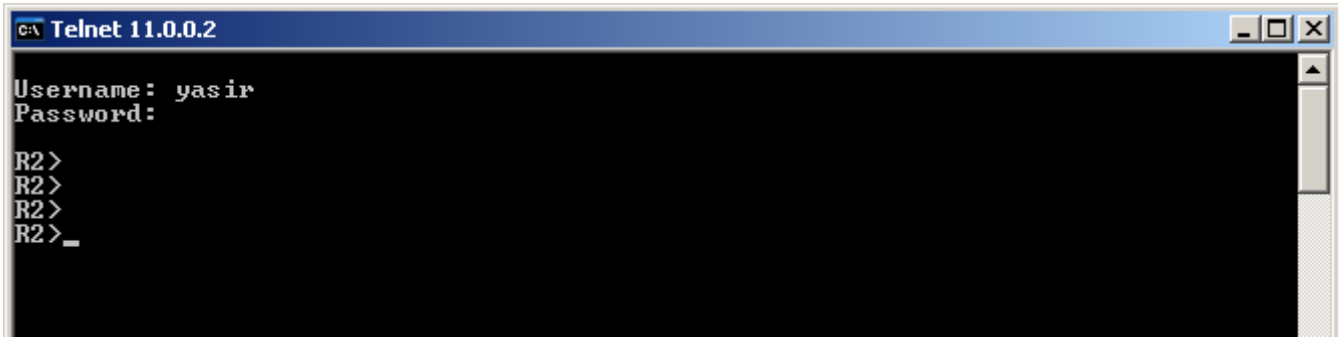
Start | CiscoSecure ACS - Mo... | 6.bmp - Paint | C:\Documents and Settin... | 7:28 AM

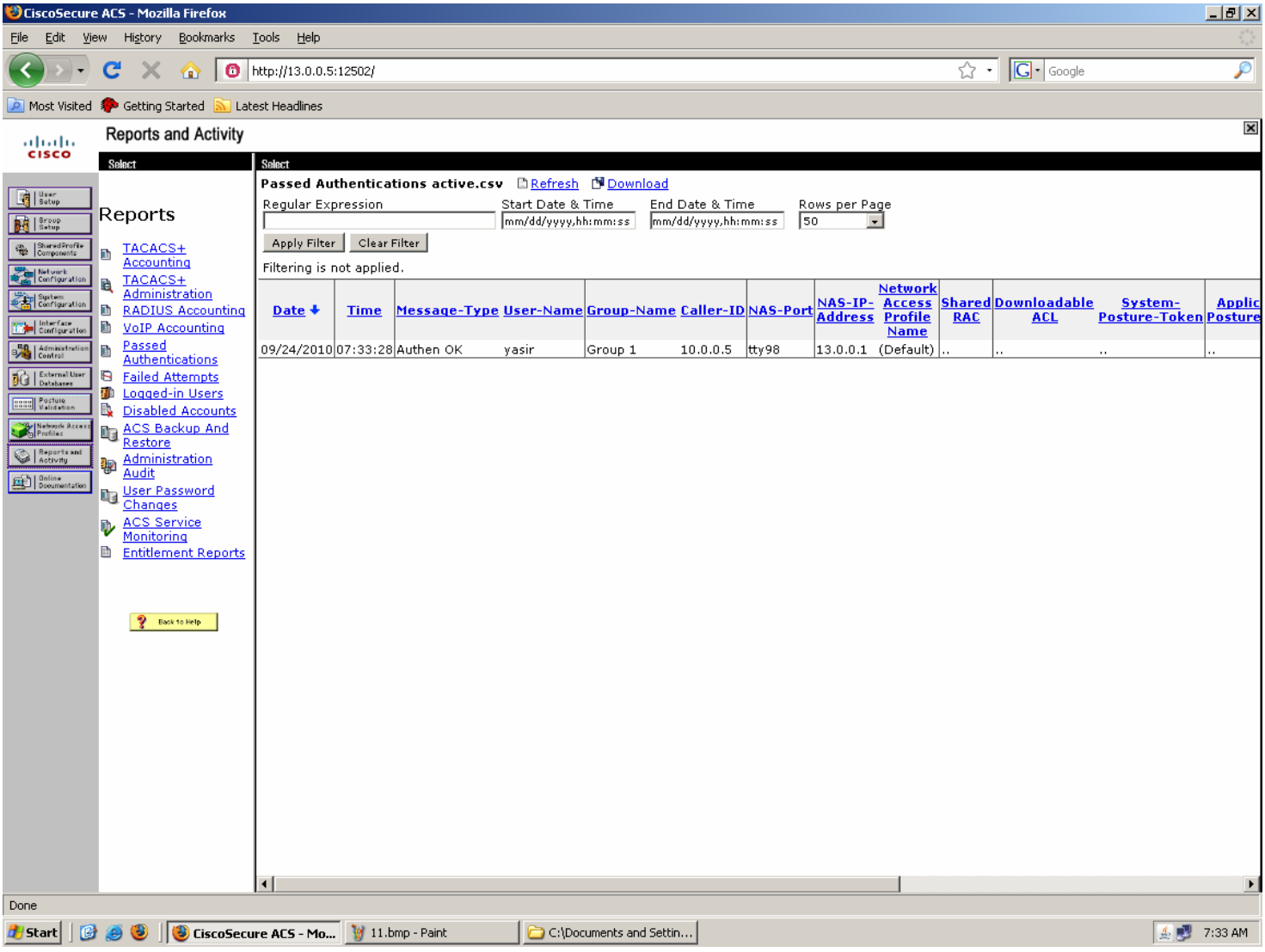

Telnet 11.0.0.2
Username: yasir
Password:
R2>
R2>
R2>
R2>_

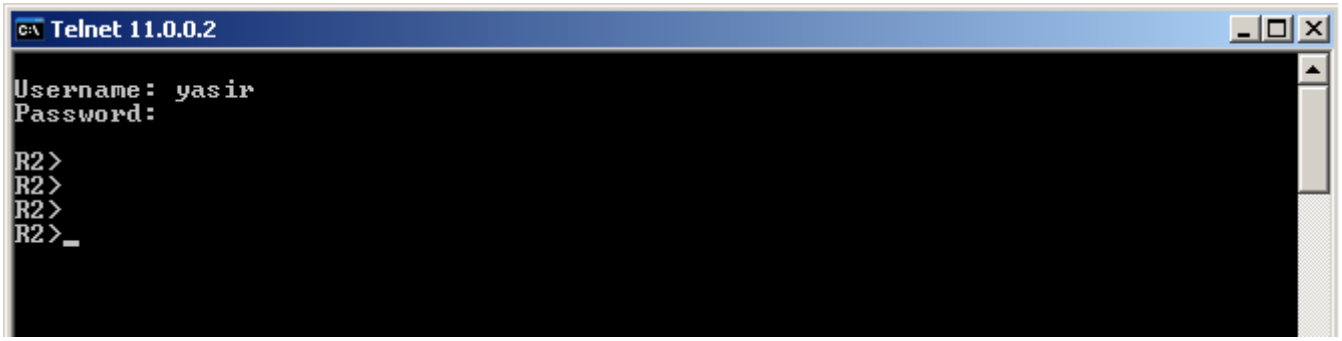

CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Most Visited Getting Started Latest Headlines
Reports and Activity
Select
TACACS+ Accounting active.csv Refresh Download
Regular Expression
Start Date & Time
End Date & Time
Rows per Page
mm/dd/yyyy,hh:mm:ss
mm/dd/yyyy,hh:mm:ss
50
Apply Filter
Clear Filter
Filtering is not applied.
Date Time User-Name Group-Name Caller-Id Acct-Flags elapsed_time service bytes_in bytes_out paks_in paks_out task_id addr NAS-Portname NAS-IP-Address
09/24/2010 07:30:01 yasir Group 1 10.0.0.5 stop 124 shell .. .. 3 .. tty99 13.0.0.1
09/24/2010 07:27:57 yasir Group 1 10.0.0.5 start .. shell .. .. 3 .. tty99 13.0.0.1
09/24/2010 07:23:07 yasir Group 1 11.0.0.1 start .. shell .. .. 2 .. tty98 13.0.0.1
Done
Start
CiscoSecure ACS - Mo...
9.bmp - Paint
C:\Documents and Settin...
7:31 AM


Telnet 11.0.0.2
Username: yasir
Password:
% Authentication failed
User Access Verification
Username:


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Most Visited Getting Started Latest Headlines
Reports and Activity
Reports
TACACS+ Accounting
TACACS+ Administratio
RADIUS Accounting
VoIP Accounting
Passed Authenticatio
Failed Attempts
Logged-in Users
Disabled Accounts
ACS Backup And Restore
Administratio Audit
User Passwor Changes
ACS Service Monitoring
Entitlement Reports
Failed Attempts active.csv
Refresh
Download
Regular Expression
Start Date & Time
End Date & Time
Rows per Page
mm/dd/yyyy,hh:mm:ss
50
Apply Filter
Clear Filter
Filtering is not applied.
Date
Time
Message-Type
User-Name
Group-Name
Caller-ID
Network Access Profile Name
Authen-Failure-Code
Author-Failure-Code
Author-Data
NAS-Port
NAS-IP-Address
Filter Information
09/24/2010 07:30:20 Authen failed yasir Group 1 10.0.0.5 (Default) ACS password invalid .. .. tty99 13.0.0.1 ..
Done
Start
CiscoSecure ACS - Mo...
10.bmp - Paint
C:\Documents and Settin...
7:32 AM


Telnet 11.0.0.2
Username: yasir
Password:
R2>
R2>
R2>
R2>_


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Most Visited Getting Started Latest Headlines
Reports and Activity
Select
Reports
TACACS+ Accounting
TACACS+ Administration
RADIUS Accounting
VoIP Accounting
Passed Authentications
Failed Attempts
Logged-in Users
Disabled Accounts
ACS Backup And Restore
Administration Audit
User Password Changes
ACS Service Monitoring
Entitlement Reports
Back to Help
Passed Authentications active.csv Refresh Download
Regular Expression
Start Date & Time
End Date & Time
Rows per Page
mm/dd/yyyy,hh:mm:ss
50
Apply Filter Clear Filter
Filtering is not applied.
Date Time Message-Type User-Name Group-Name Caller-ID NAS-Port NAS-IP-Address Network Access Profile Name Shared RAC Downloadable ACL System-Posture-Token Applic Posture
09/24/2010 07:33:28 Authen OK yasir Group 1 10.0.0.5 tty98 13.0.0.1 (Default) .. .. ..
Done
Start
CiscoSecure ACS - Mo...
11.bmp - Paint
C:\Documents and Settin...
7:33 AM



CiscoSecure ACS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://13.0.0.5:12502/

Most Visited Getting Started Latest Headlines

Reports and Activity

Select

Reports

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

Back to Help

Select

TACACS+ Accounting active.csv Refresh Download

Regular Expression | Start Date & Time (mm/dd/yyyy,hh:mm:ss) | End Date & Time (mm/dd/yyyy,hh:mm:ss) | Rows per Page (50)

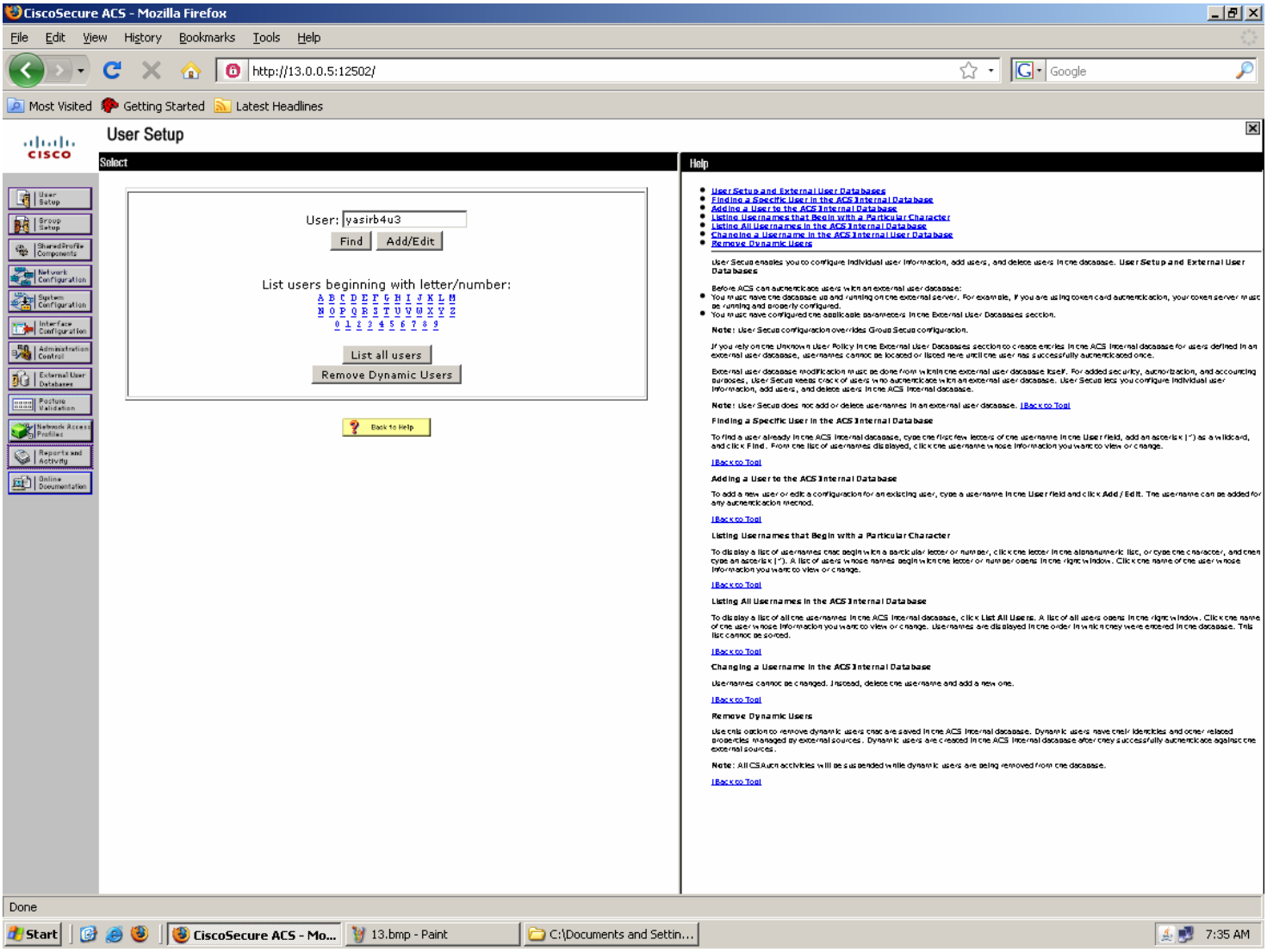
Apply Filter Clear Filter

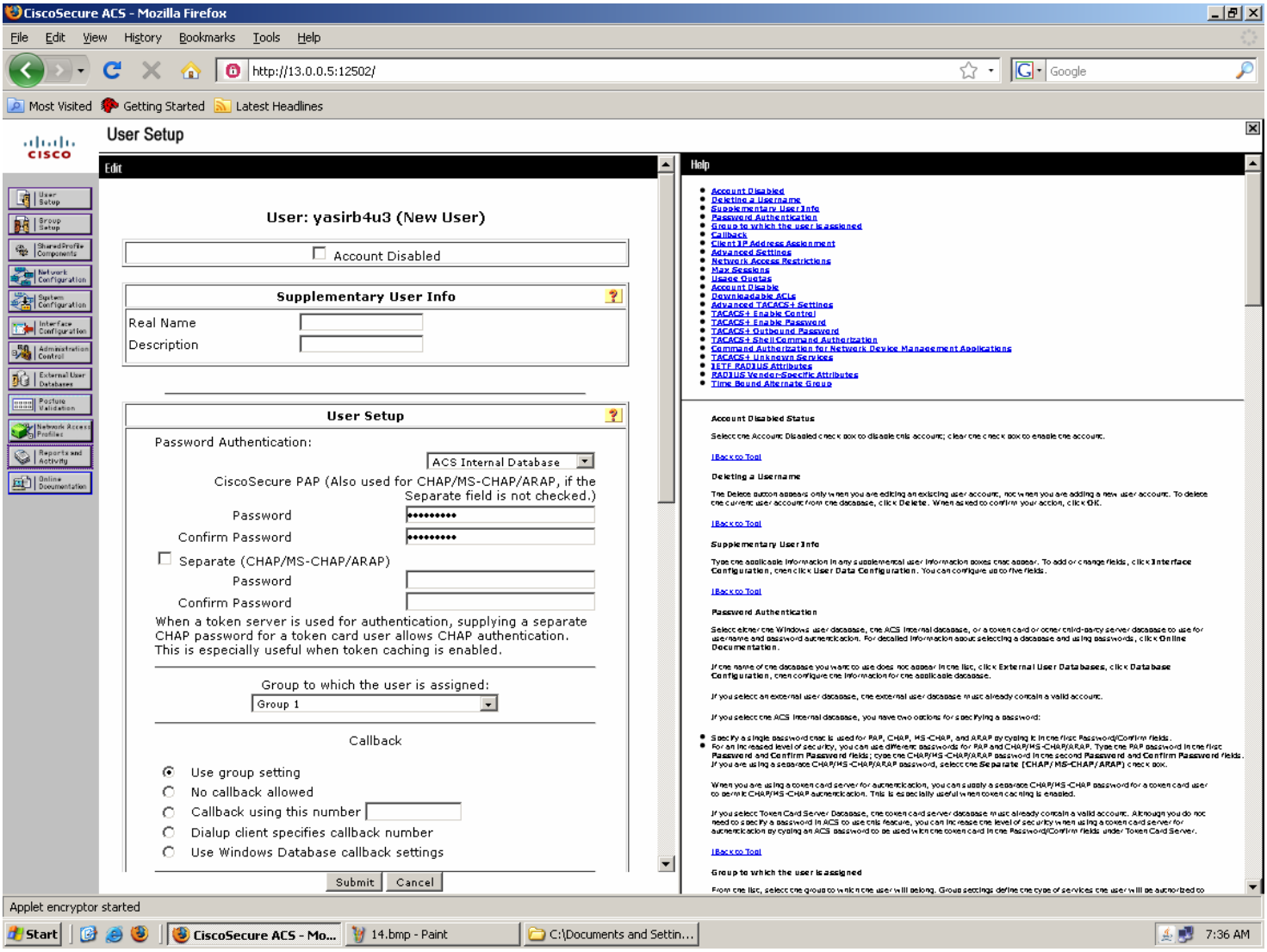
Filtering is not applied.

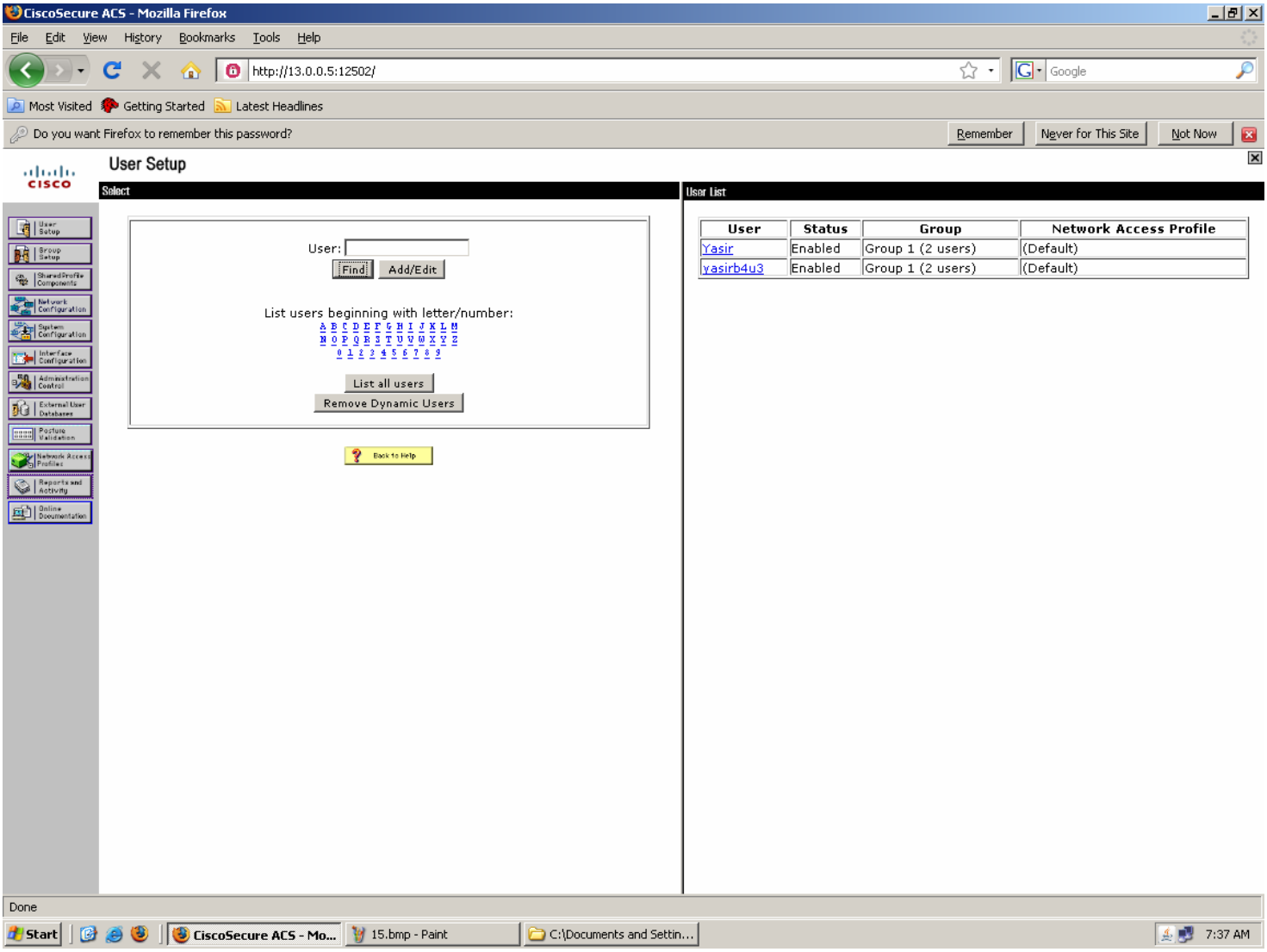
Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in	bytes_out	paks_in	paks_out	task_id	addr	NAS
09/24/2010	07:33:28	yasir	Group 1	10.0.0.5	start	..	shell	..	..	..	..	5	..	tty9
09/24/2010	07:33:14	yasir	Group 1	11.0.0.1	stop	607	shell	..	..	..	..	2	..	tty9
09/24/2010	07:30:01	yasir	Group 1	10.0.0.5	stop	124	shell	..	..	..	..	3	..	tty9
09/24/2010	07:27:57	yasir	Group 1	10.0.0.5	start	..	shell	..	..	..	..	3	..	tty9
09/24/2010	07:23:07	yasir	Group 1	11.0.0.1	start	..	shell	..	..	..	..	2	..	tty9

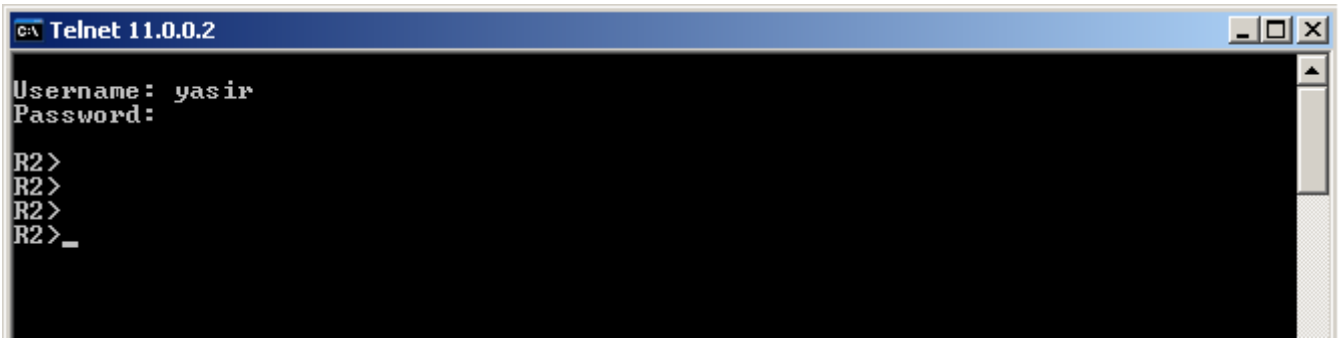
Done

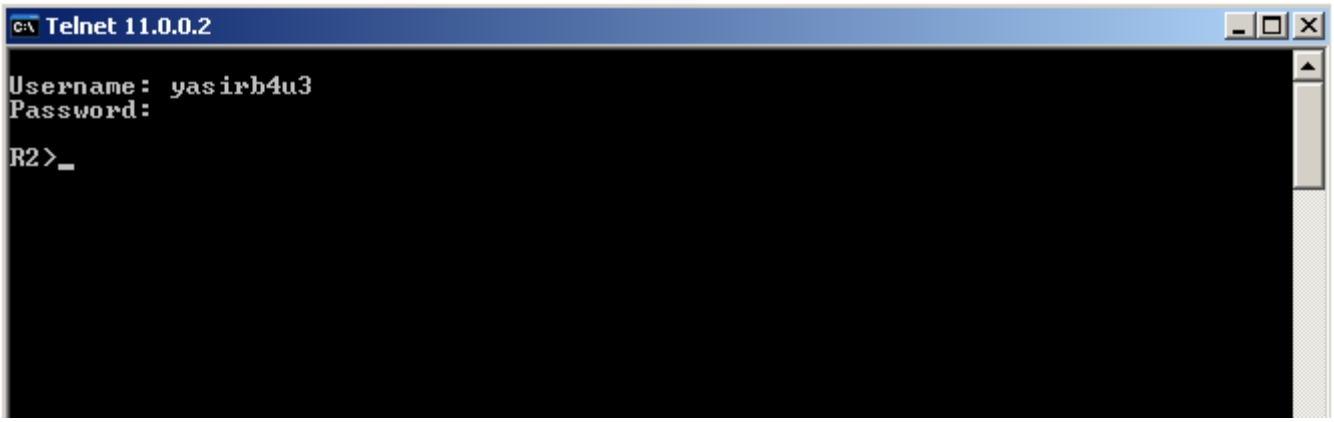
Start | CiscoSecure ACS - Mo... | 12.bmp - Paint | C:\Documents and Settin... | 7:34 AM

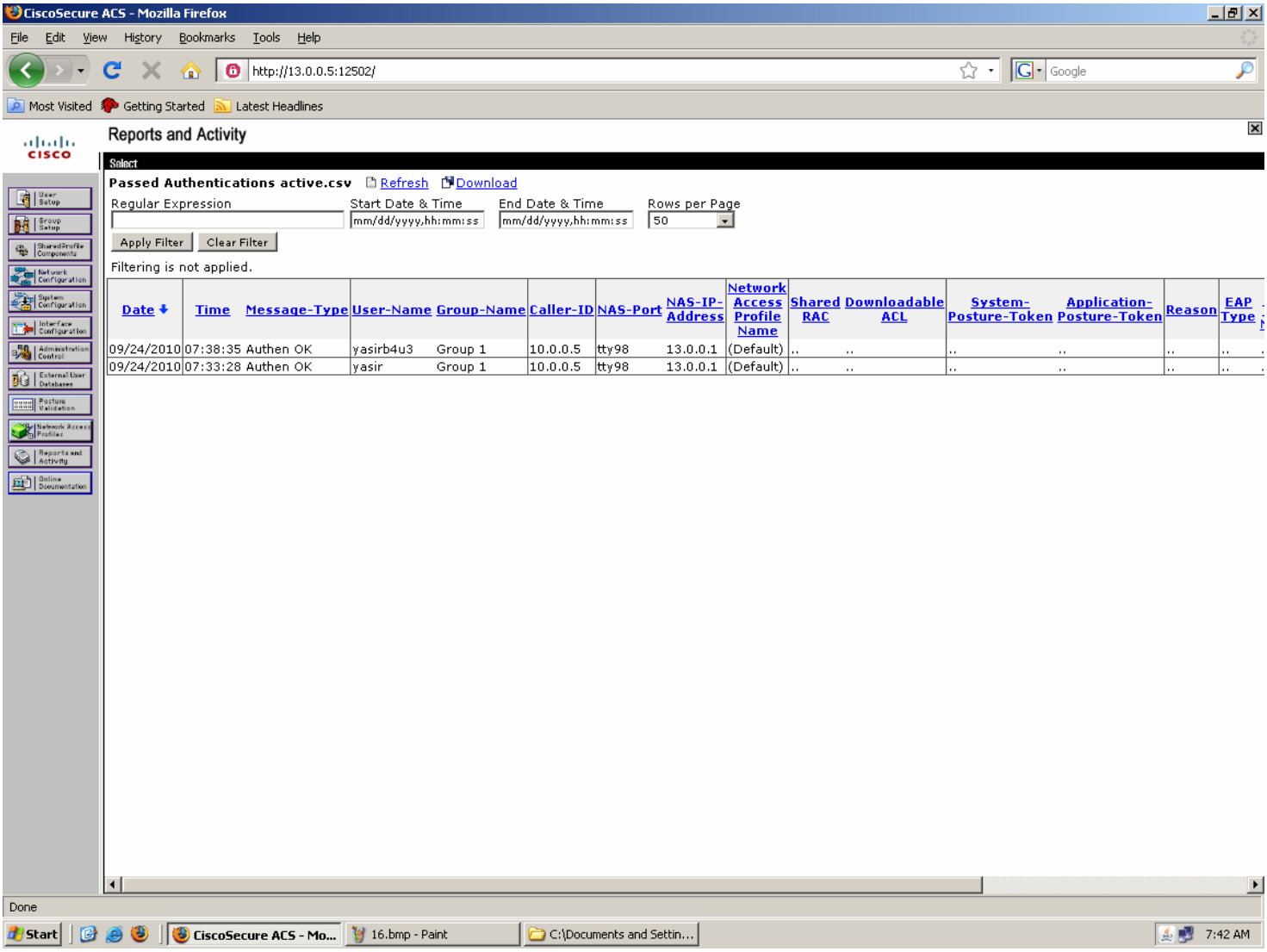

CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
cisco
User Setup
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: yasirb4u3
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
User Setup enables you to configure individual user information, add users, and delete users in the database.
User Setup and External User Databases
Before ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.
External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.
Note: User Setup does not add or delete usernames in an external user database. [Back to Top]
Finding a Specific User in the ACS Internal Database
To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.
[Back to Top]
Adding a User to the ACS Internal Database
To add a new user or edit a configuration for an existing user, type a username in the User field and click Add / Edit. The username can be added for any authentication method.
[Back to Top]
Listing Usernames that Begin with a Particular Character
To display a list of usernames that begin with a particular letter or number, click the letter in the alphanumeric list, or type the character, and then type an asterisk (*). A list of users whose names begin with the letter or number opens in the right window. Click the name of the user whose information you want to view or change.
[Back to Top]
Listing All Usernames in the ACS Internal Database
To display a list of all the usernames in the ACS internal database, click List All Users. A list of all users opens in the right window. Click the name of the user whose information you want to view or change. Usernames are displayed in the order in which they were entered in the database. This list cannot be sorted.
[Back to Top]
Changing a Username in the ACS Internal Database
Usernames cannot be changed. Instead, delete the username and add a new one.
[Back to Top]
Remove Dynamic Users
Use this option to remove dynamic users that are saved in the ACS internal database. Dynamic users have their identities and other related properties managed by external sources. Dynamic users are created in the ACS internal database after they successfully authenticate against the external sources.
Note: All CSAuth activities will be suspended while dynamic users are being removed from the database.
[Back to Top]
Done
Start
CiscoSecure ACS - Mo...
13.bmp - Paint
C:\Documents and Settin...
7:35 AM


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Most Visited Getting Started Latest Headlines
User Setup
Edit
User: yasirb4u3 (New User)
Account Disabled
Supplementary User Info
Real Name
Description
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
Confirm Password
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Group 1
Callback
Use group setting
No callback allowed
Callback using this number
Dialup client specifies callback number
Use Windows Database callback settings
Submit
Cancel
Help
Account Disabled
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Callback
Client IP Address Assignment
Advanced Settings
Network Access Restrictions
Max Sessions
Usage Quotas
Account Disable
Downloadable ACLs
Advanced TACACS+ Settings
TACACS+ Enable Control
TACACS+ Enable Password
TACACS+ Outbound Password
TACACS+ Shell Command Authorization
Command Authorization for Network Device Management Applications
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Time Bound Alternate Group
Account Disabled Status
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Applet encryptor started
Start
CiscoSecure ACS - Mo...
14.bmp - Paint
C:\Documents and Settin...
7:36 AM


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
Do you want Firefox to remember this password?
Remember
Never for This Site
Not Now
cisco
User Setup
Select
User:
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User List
User
Status
Group
Network Access Profile
Yasir
Enabled
Group 1 (2 users)
(Default)
yasirb4u3
Enabled
Group 1 (2 users)
(Default)
Done
Start
CiscoSecure ACS - Mo...
15.bmp - Paint
C:\Documents and Settin...
7:37 AM


Telnet 11.0.0.2
Username: yasir
Password:
R2>
R2>
R2>
R2>


Telnet 11.0.0.2
Username: yasirb4u3
Password:
R2>


CiscoSecure ACS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://13.0.0.5:12502/
Google
Most Visited Getting Started Latest Headlines
Reports and Activity
Select
Passed Authentications active.csv
Refresh
Download
Regular Expression
Start Date & Time
End Date & Time
Rows per Page
mm/dd/yyyy,hh:mm:ss
mm/dd/yyyy,hh:mm:ss
50
Apply Filter
Clear Filter
Filtering is not applied.
Date
Time
Message-Type
User-Name
Group-Name
Caller-ID
NAS-Port
NAS-IP-Address
Network Access Profile Name
Shared RAC
Downloadable ACL
System-Posture-Token
Application-Posture-Token
Reason
EAP Type
09/24/2010 07:38:35 Authen OK yasirb4u3 Group 1 10.0.0.5 tty98 13.0.0.1 (Default)
09/24/2010 07:33:28 Authen OK yasir Group 1 10.0.0.5 tty98 13.0.0.1 (Default)
Done
Start
CiscoSecure ACS - Mo...
16.bmp - Paint
C:\Documents and Settin...
7:42 AM