CCNA Security 2.0 Study Material – Chapter 10: Advanced Cisco Adaptive Security Appliance

itexamanswers.net/ccna-security-2-0-study-material-chapter-10-advanced-cisco-adaptive-security-appliance.html

October 9, 2017

Chapter Outline:

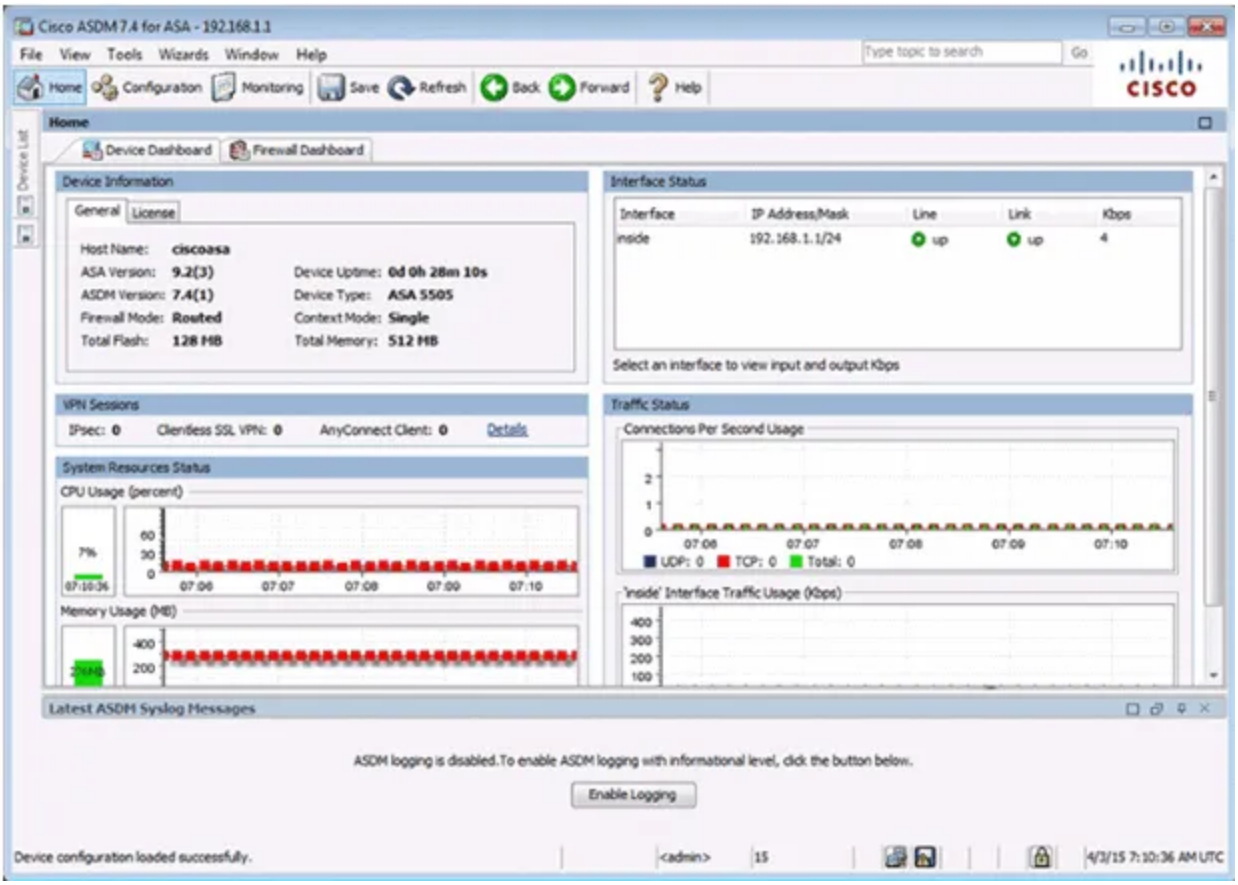
Section 10.1: ASA Security Device Manager

Upon completion of this section, you should be able to:

- Configure an ASA to provide basic firewall services using ASDM.
- Configure an ASA to provide additional firewall services using ASDM wizards.
- Configure management settings and services in an ASA using ASDM.
- Configure object groups on an ASA.

Topic 10.1.1: Introduction to ASDM

Overview of ASDM

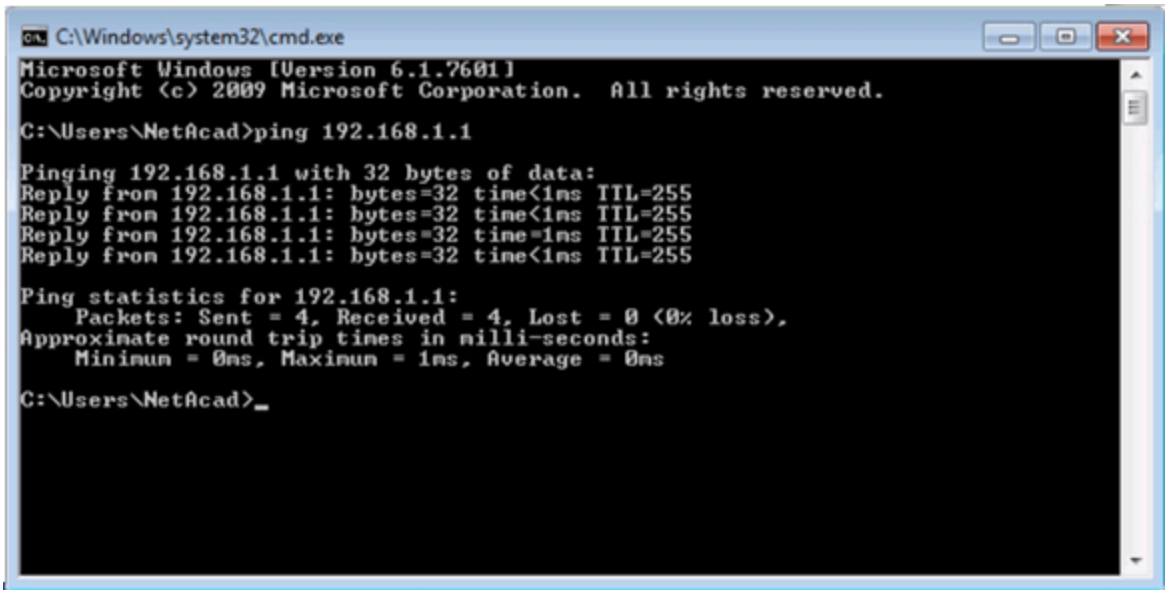


Preparing for ASDM

Preparing the ASA 5505

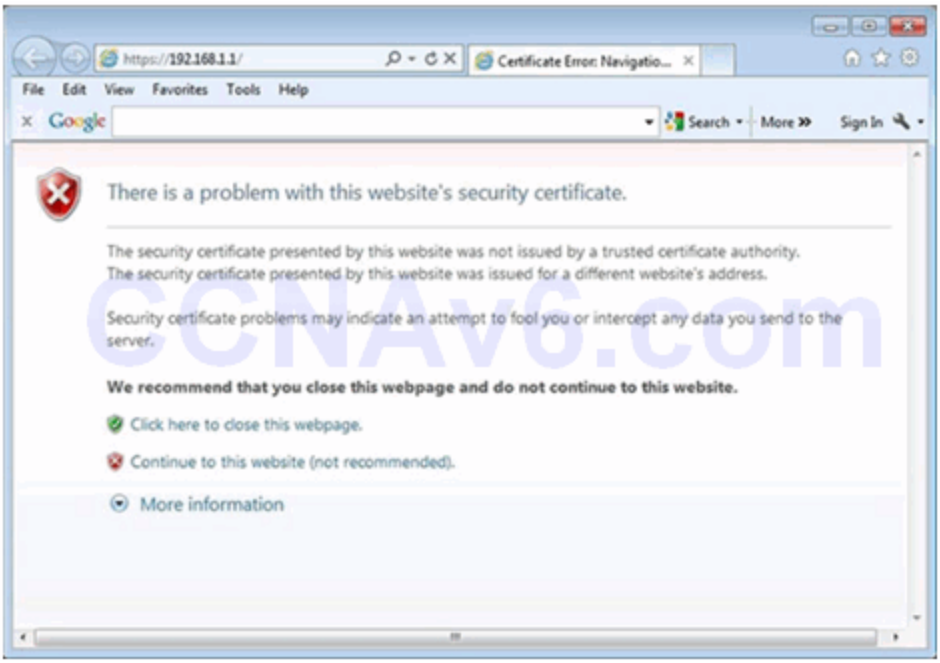
```
ciscoasa# conf t
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit
ciscoasa(config)#
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.3 255.255.255.255 inside
ciscoasa(config)#
```

Verify Connectivity to the ASA



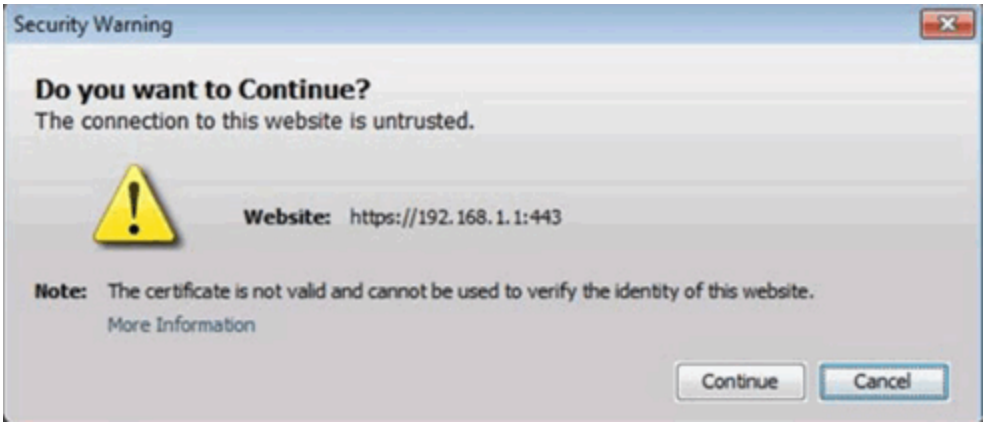
Starting ASDM

ASDM Security Certificate

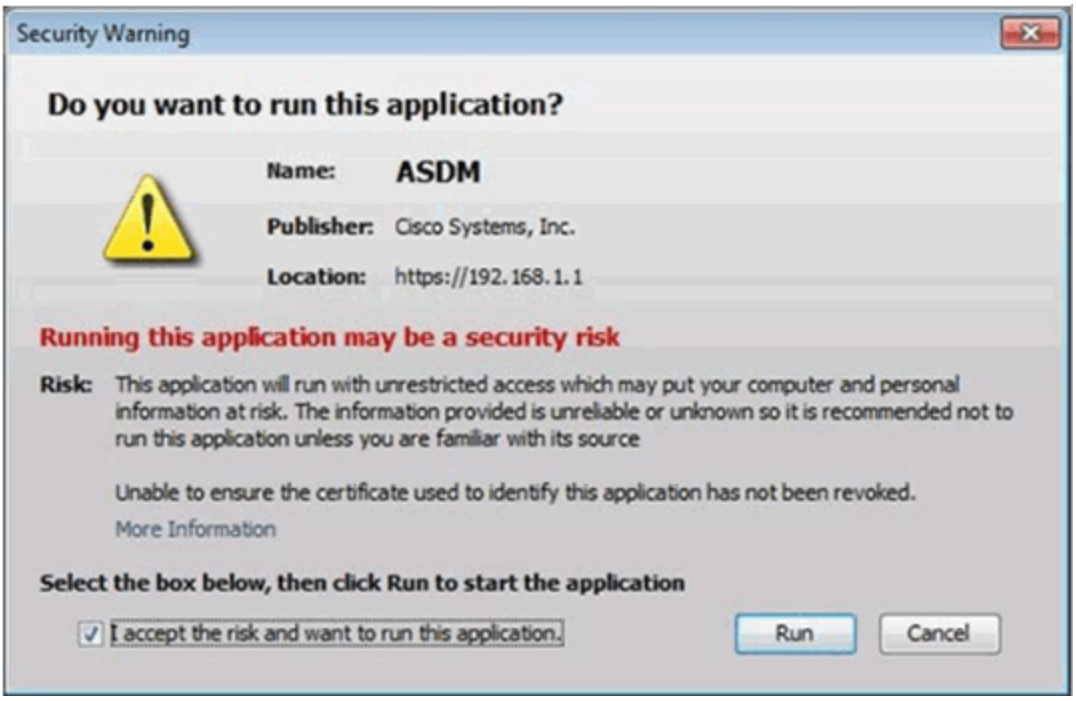


ASDM Launch Window

ASDM Security Warning – 1

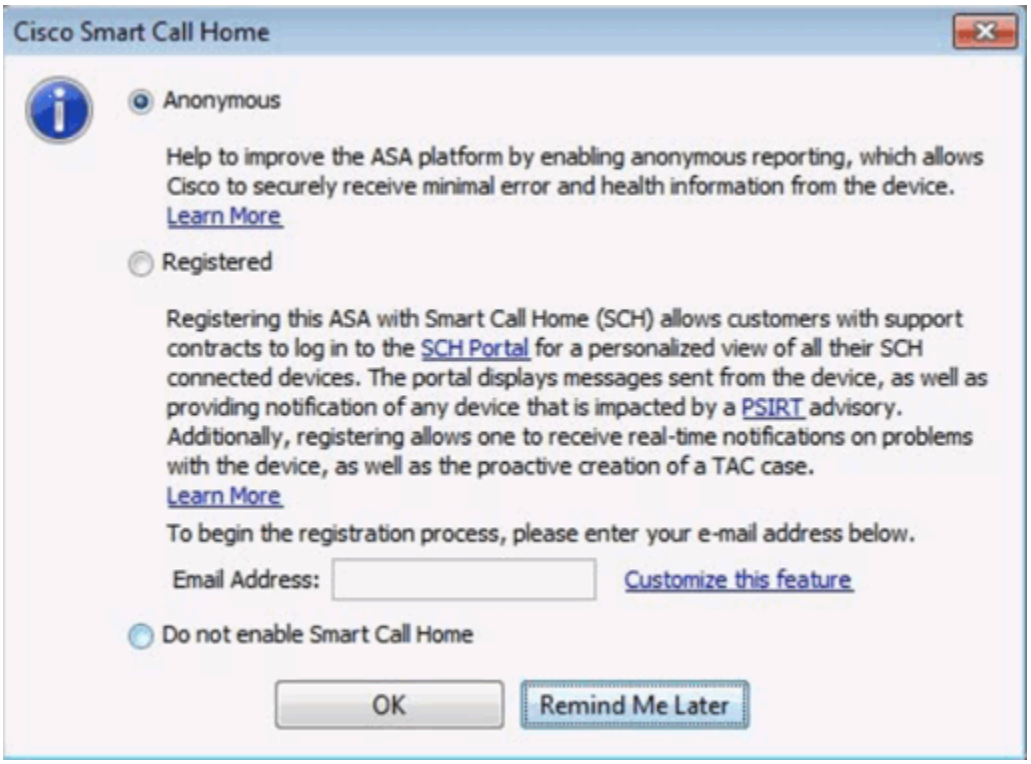


ASDM Security Warning – 2



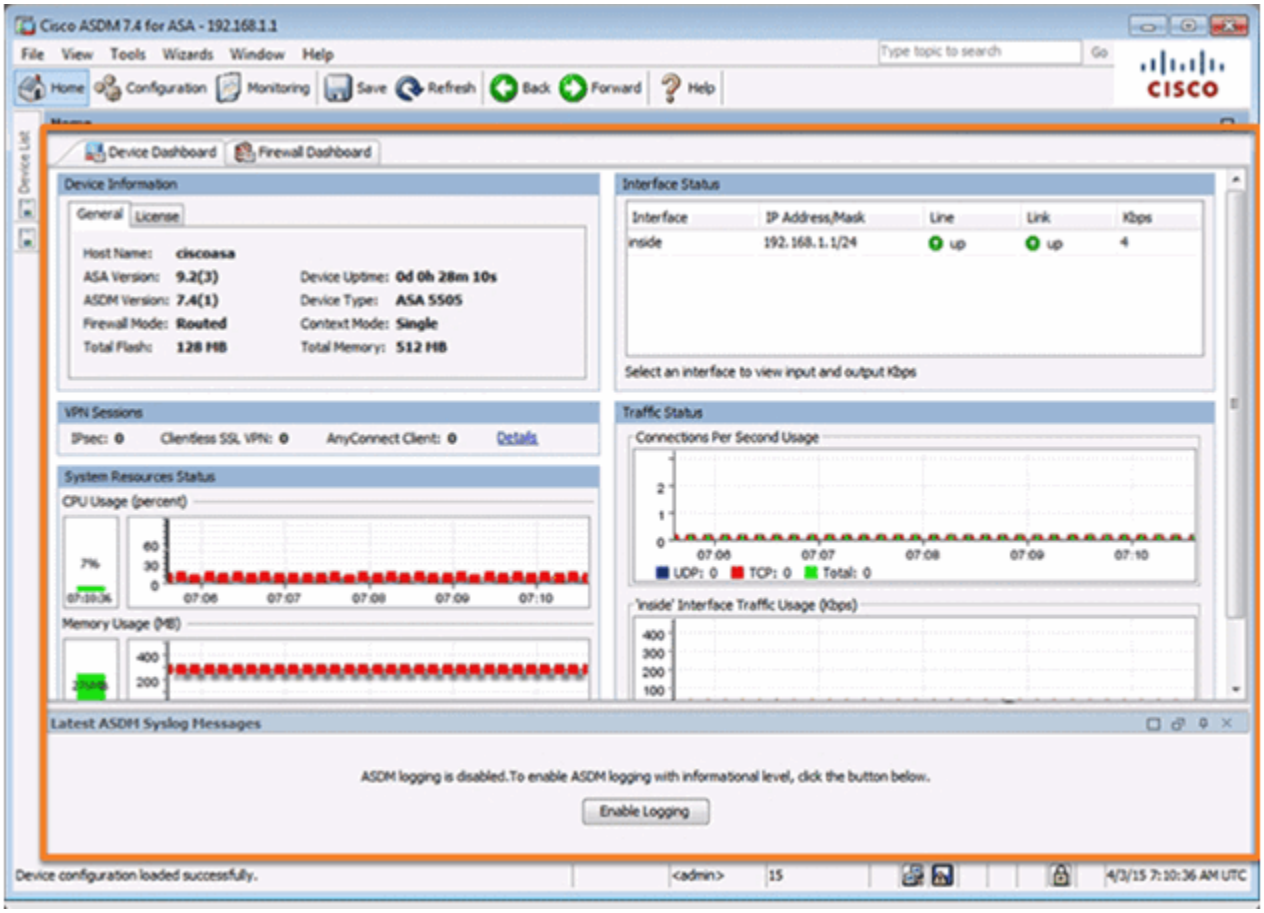
Authenticate to Use ASDM

Smart Call Home Window

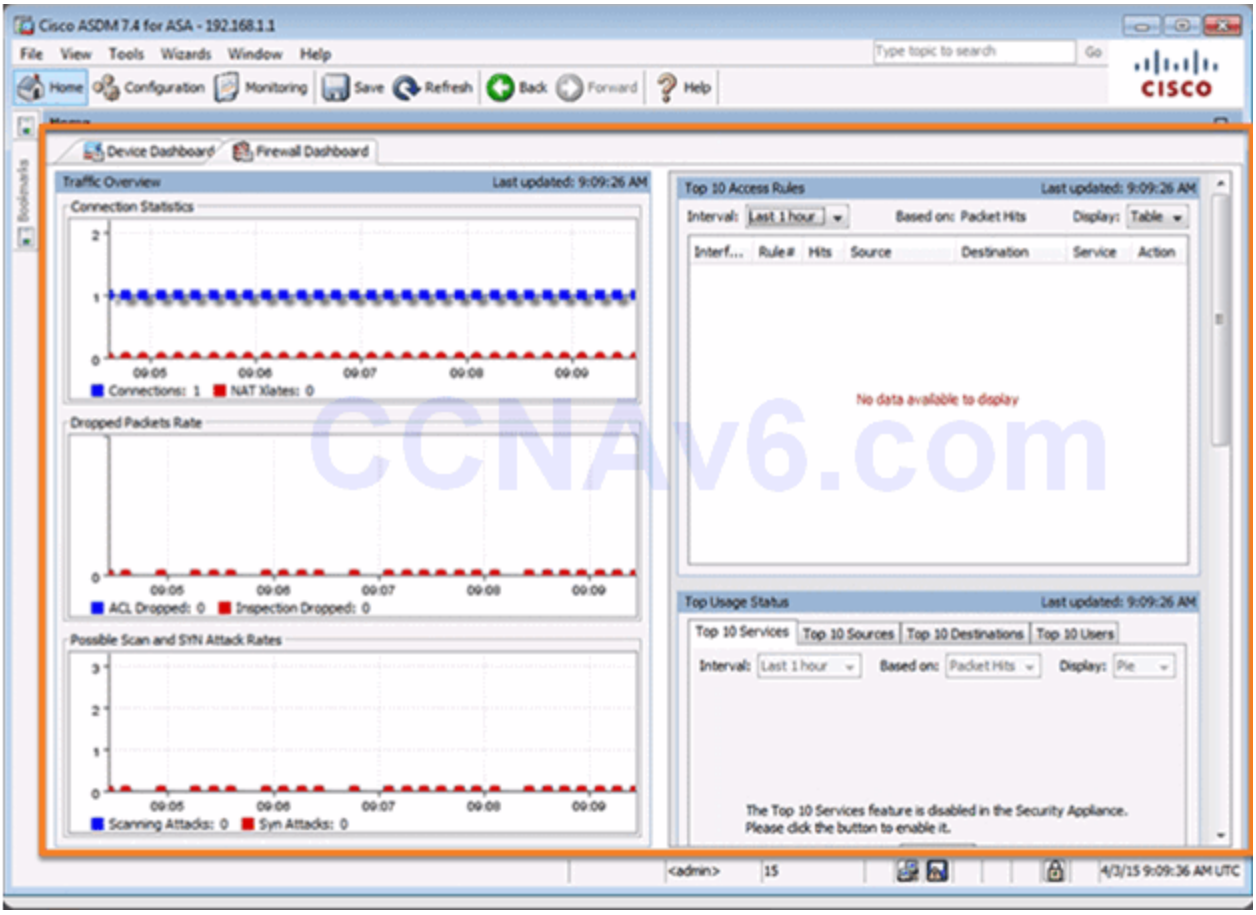


ASDM Home Page Dashboards

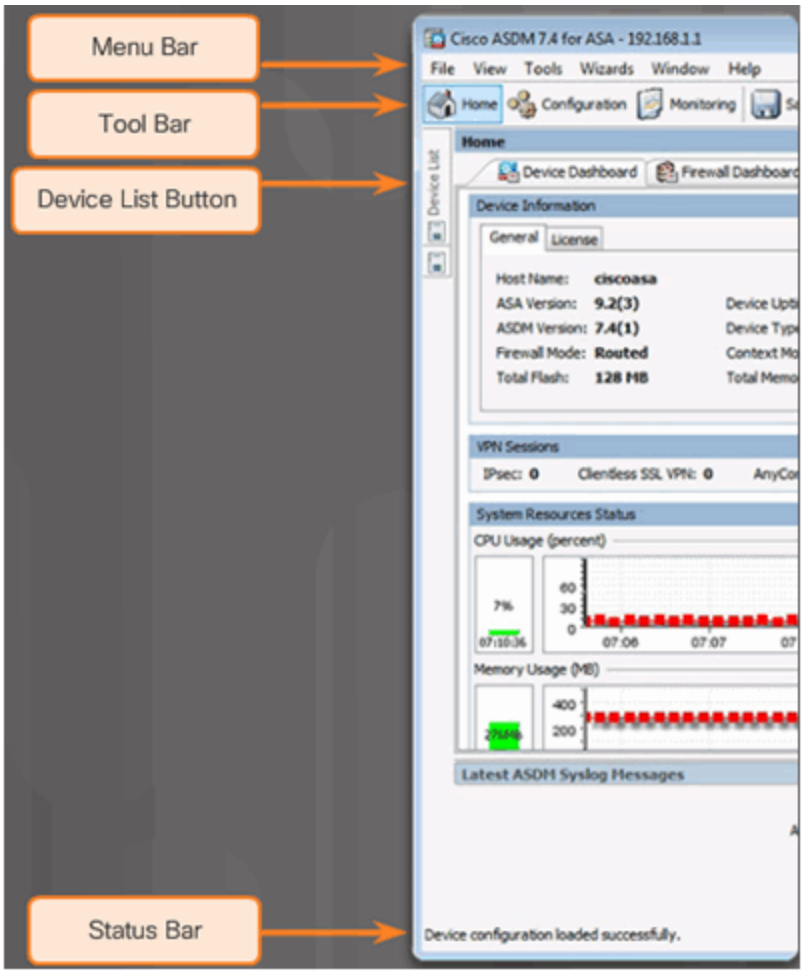
ASDM Device Dashboard Page



ASDM Firewall Dashboard Page

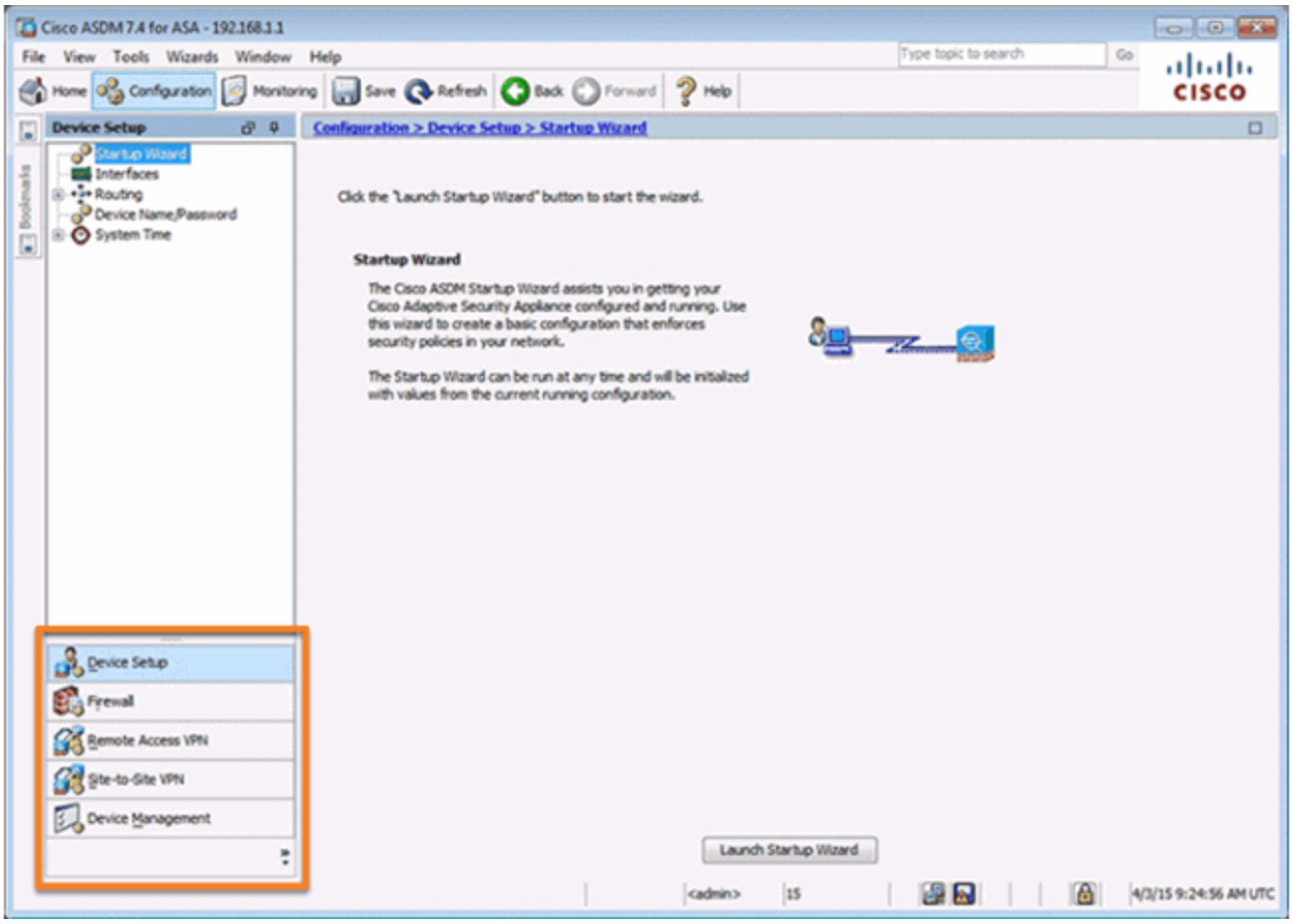


ASDM Page Elements

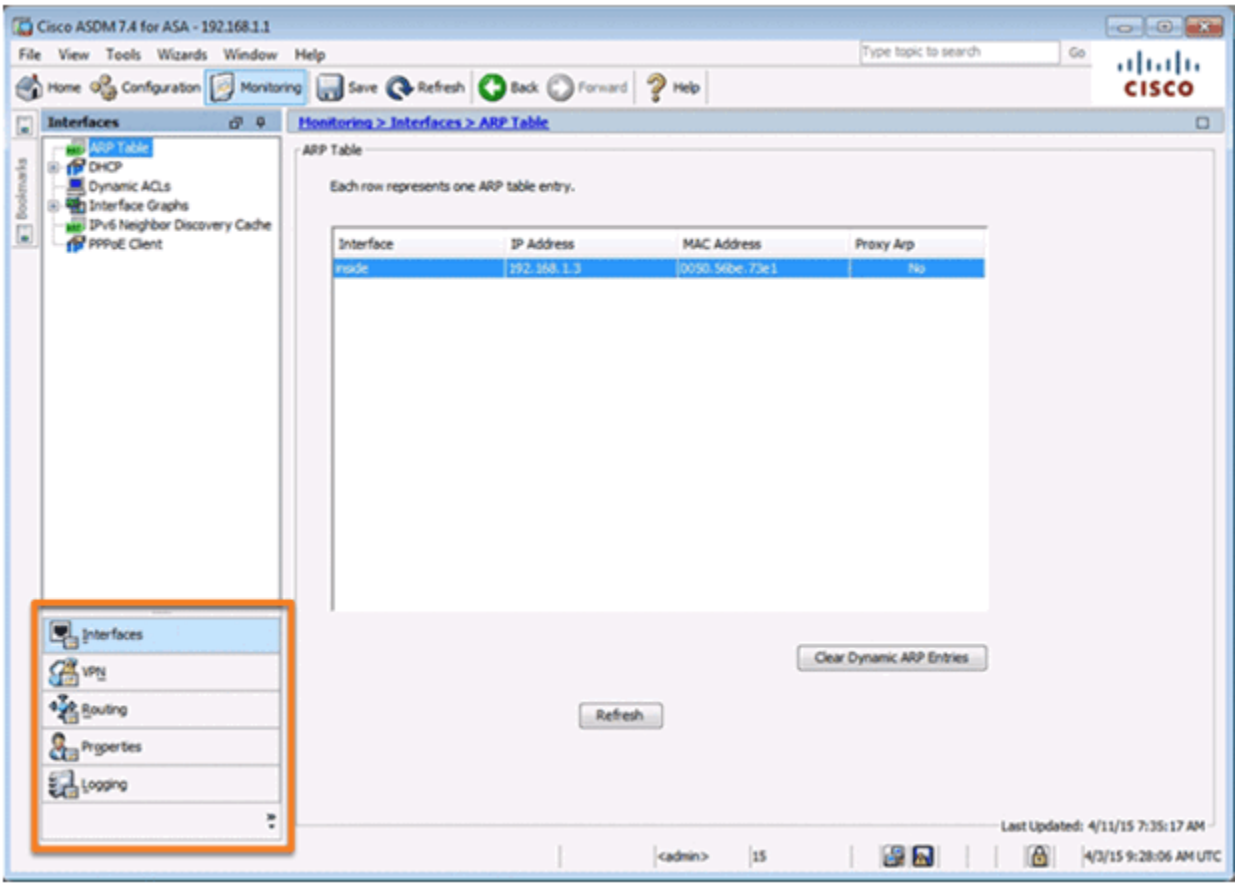


ASDM Configuration and Monitoring Views

Configuration View



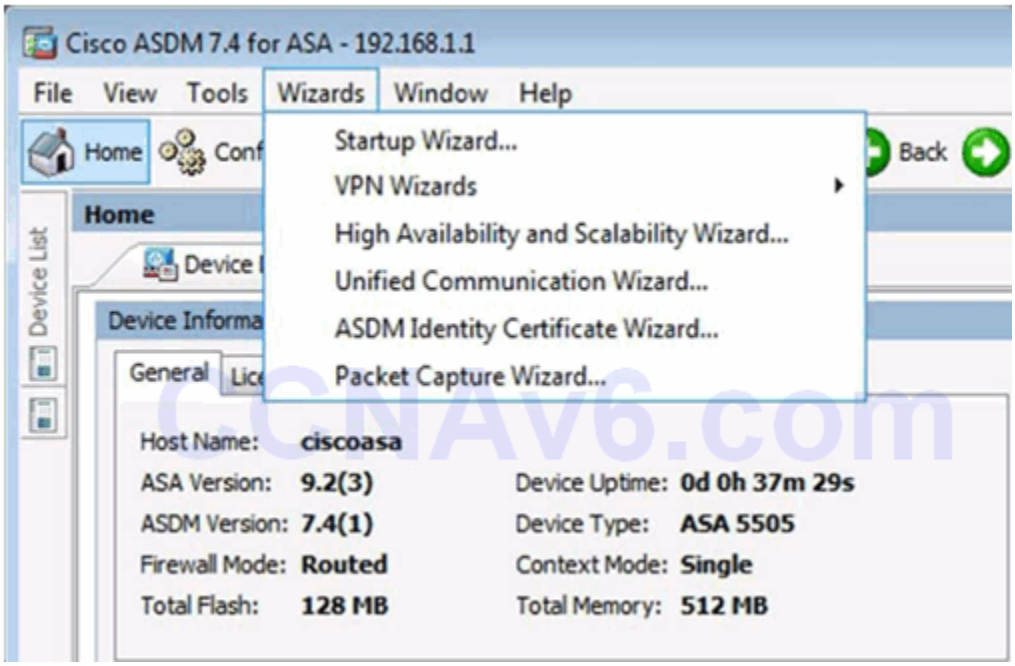
Monitoring View



Configure and Access on an ASA5505

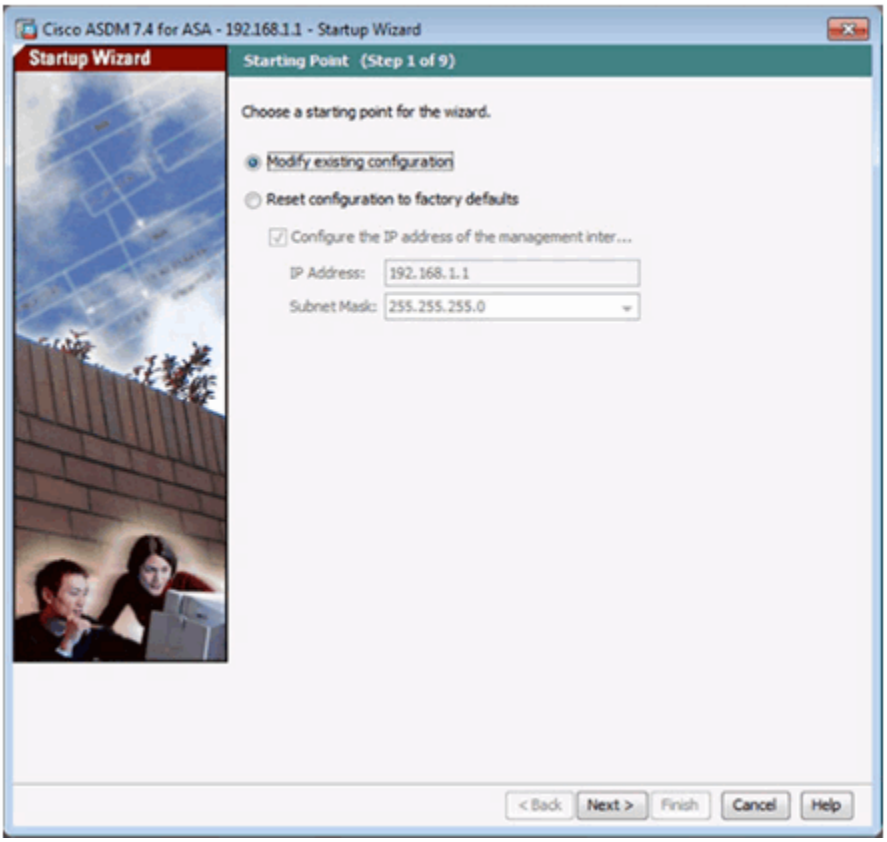
Topic 10.1.2: ASDM Wizard Menu

ASDM Wizards

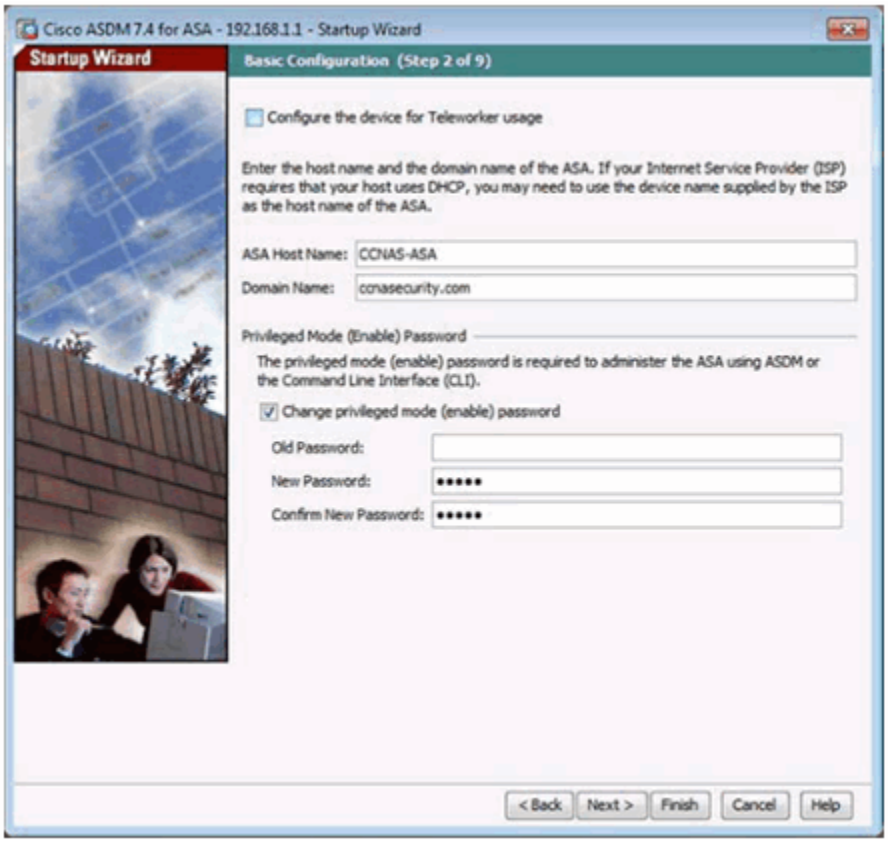


The Startup Wizard

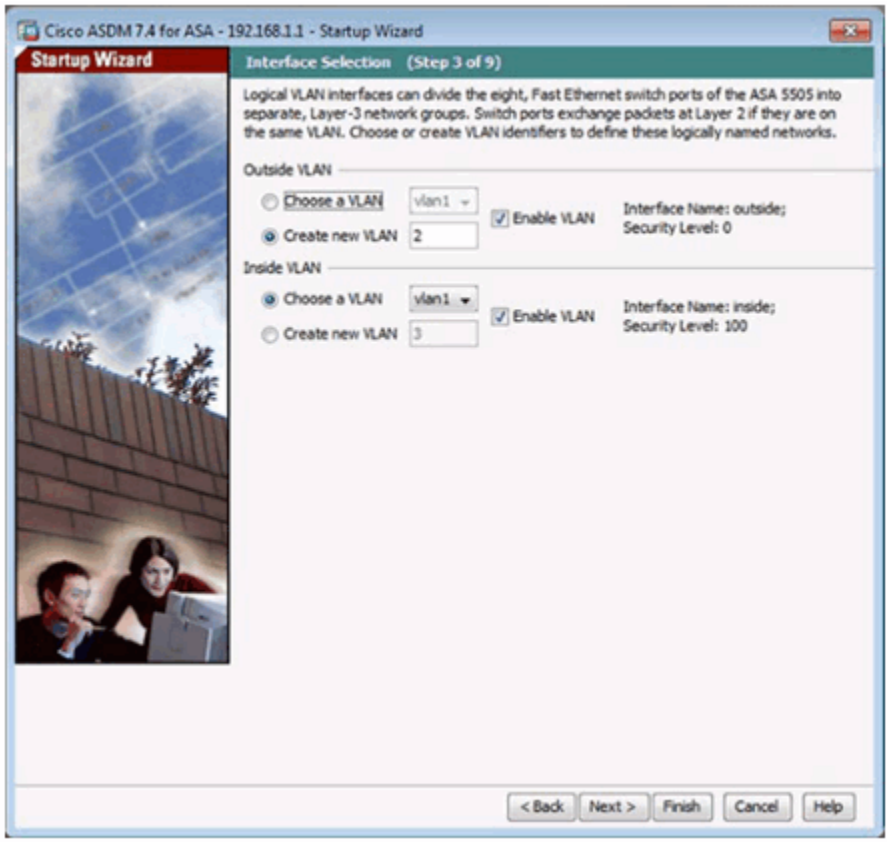
Startup Wizard Starting Point Window



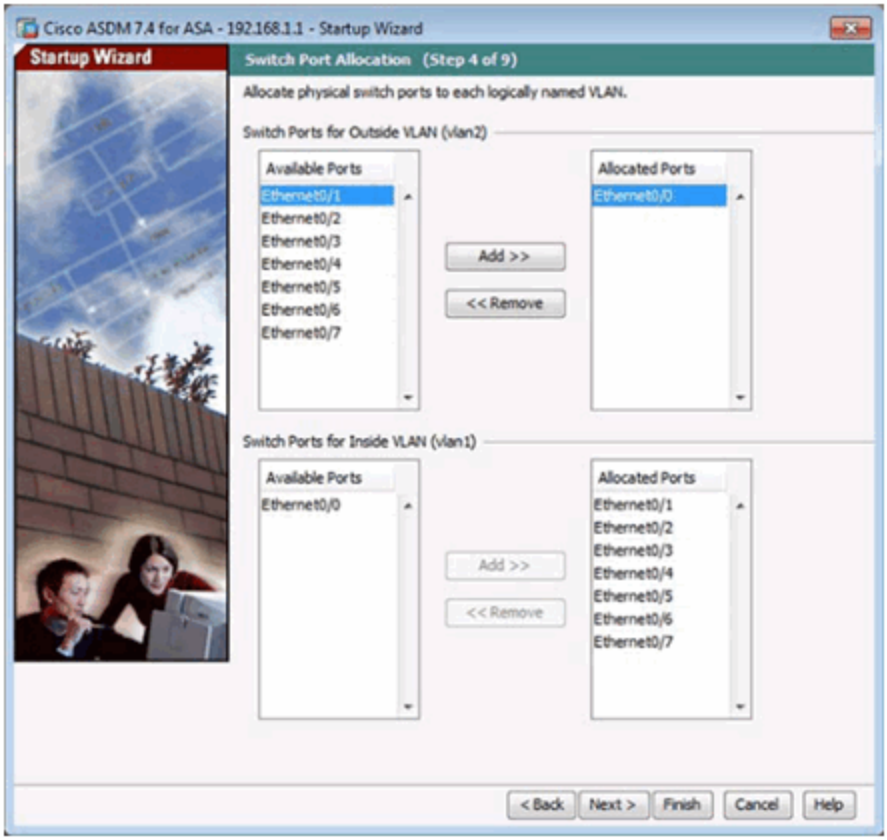
Startup Wizard Basic Configuration Window



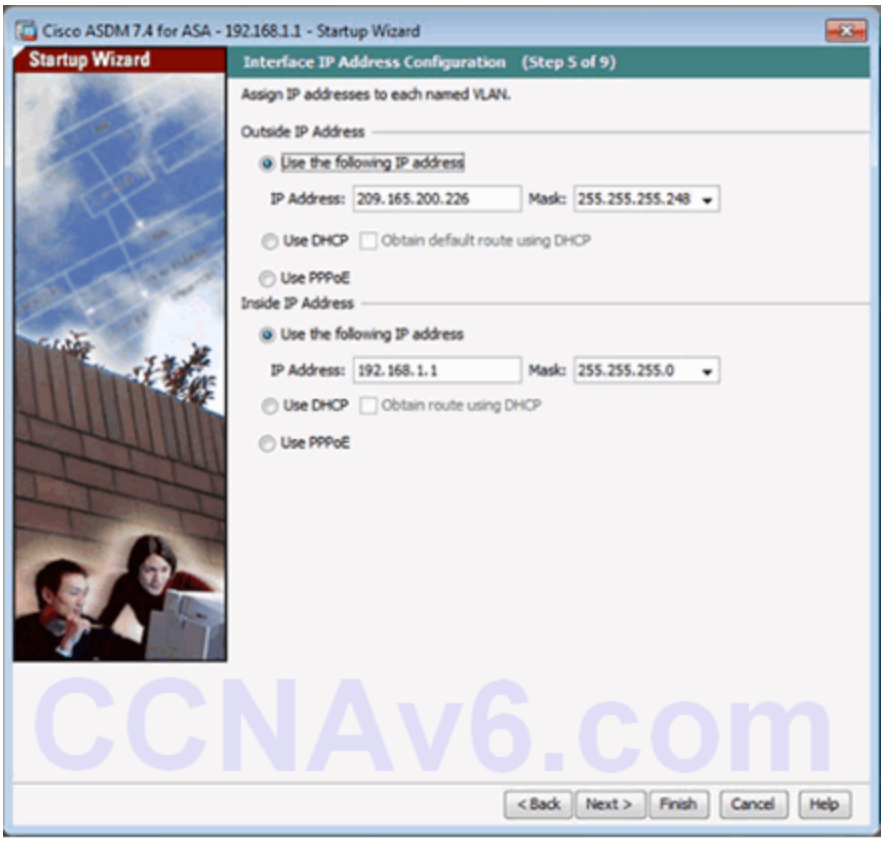
Startup Wizard Interface Selection Window



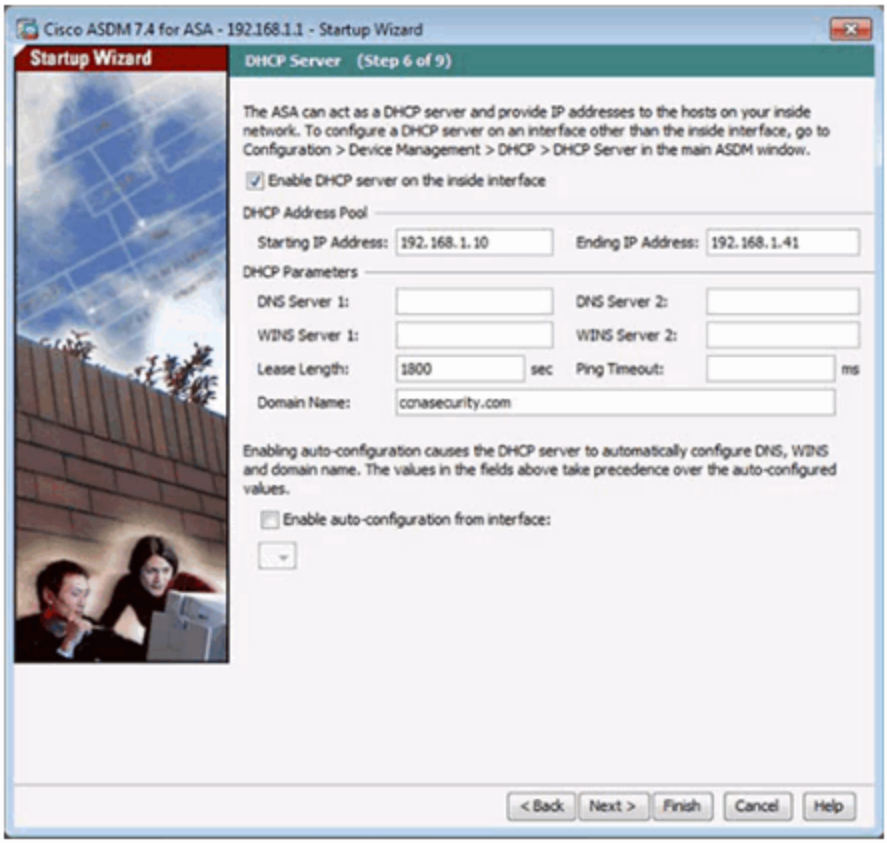
Startup Wizard Switch Port Allocation Window



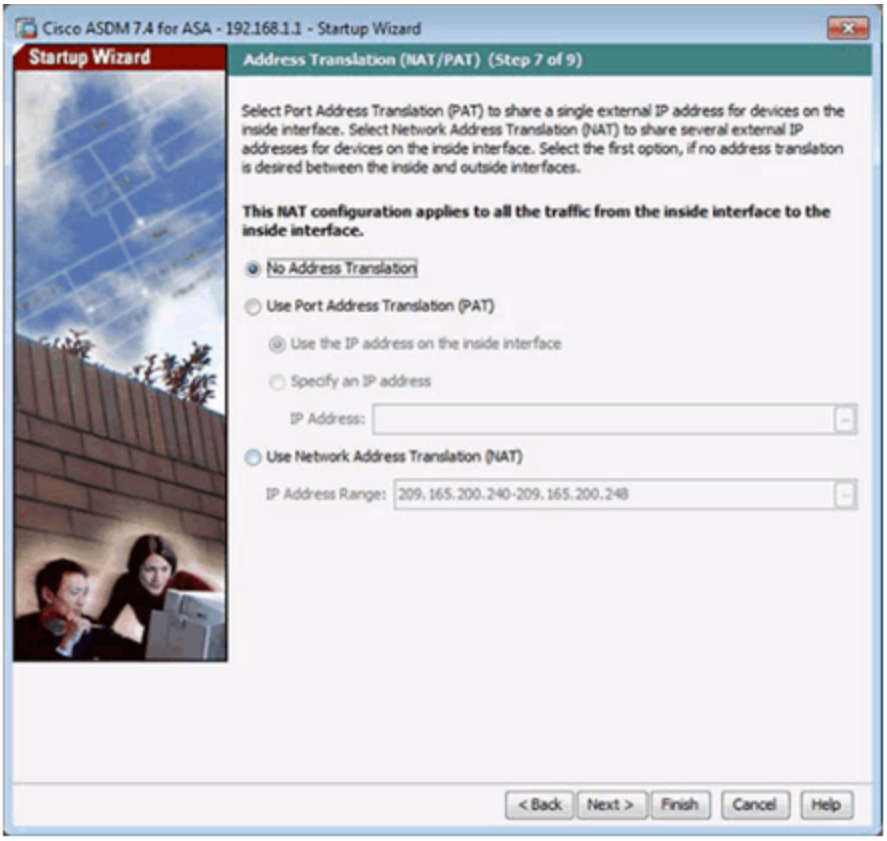
Startup Wizard Interface IP Address Configuration Window



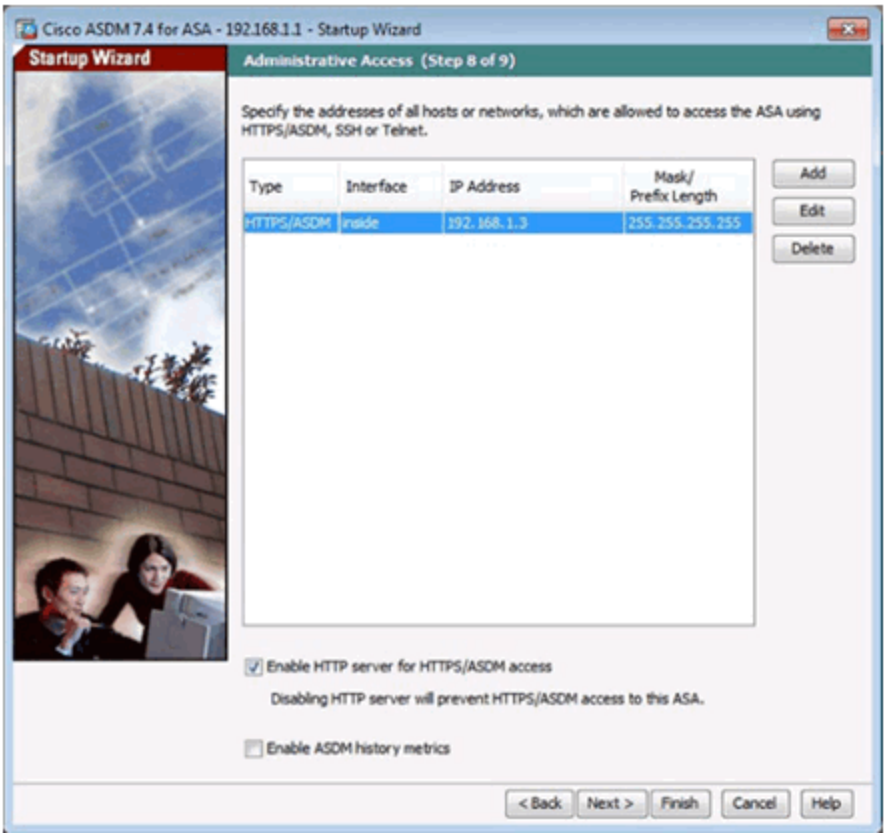
Startup Wizard DHCP Server Window



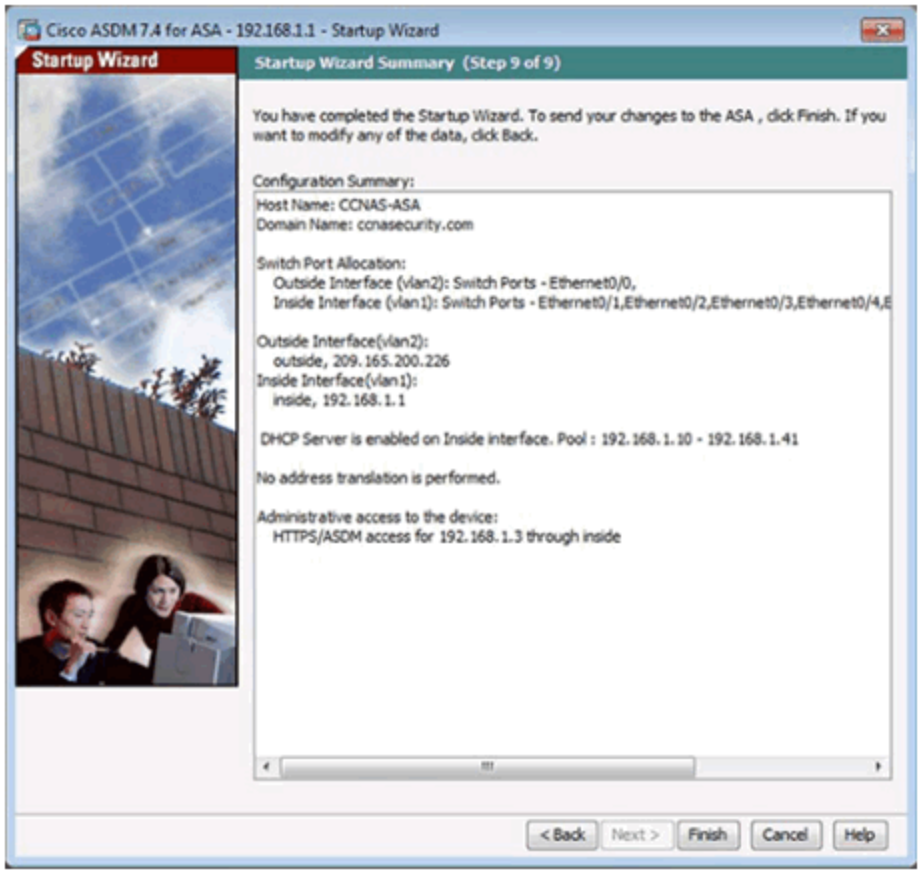
Startup Wizard Address Translation (NAT/PAT) Window



Startup Wizard Administrative Access Window

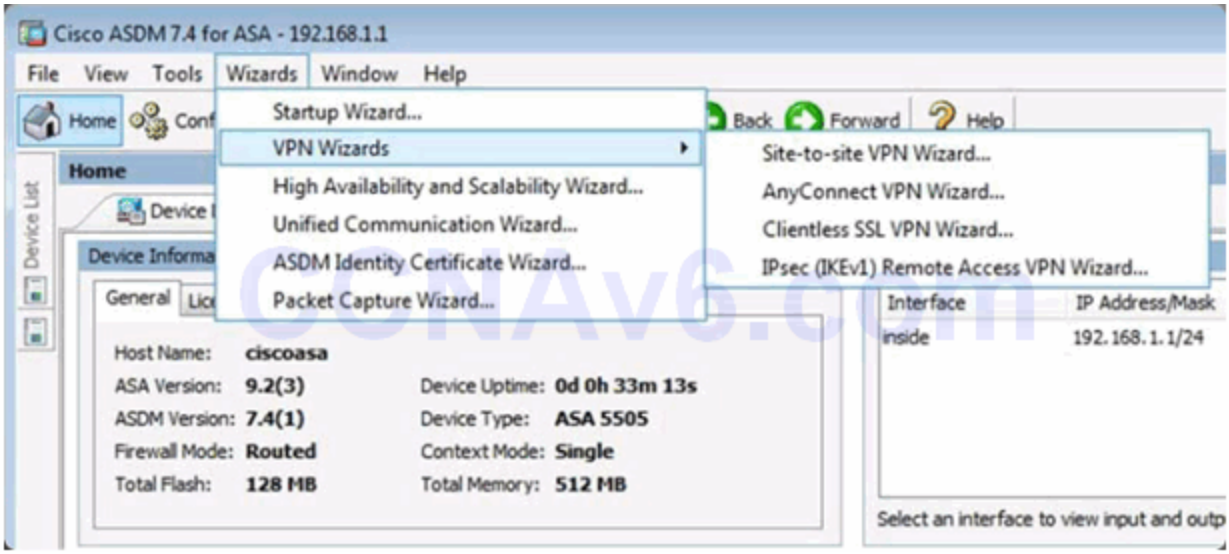


Startup Wizard Summary Window



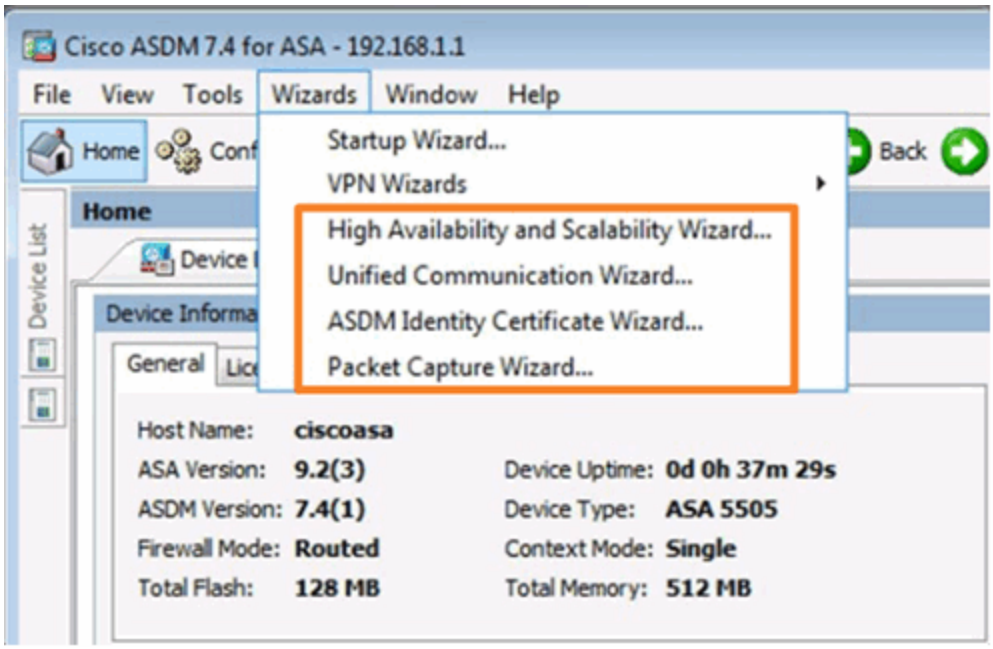
Different Types of VPN Wizards

ASDM VPN Wizards



ASDM Remote Access VPN Assistant

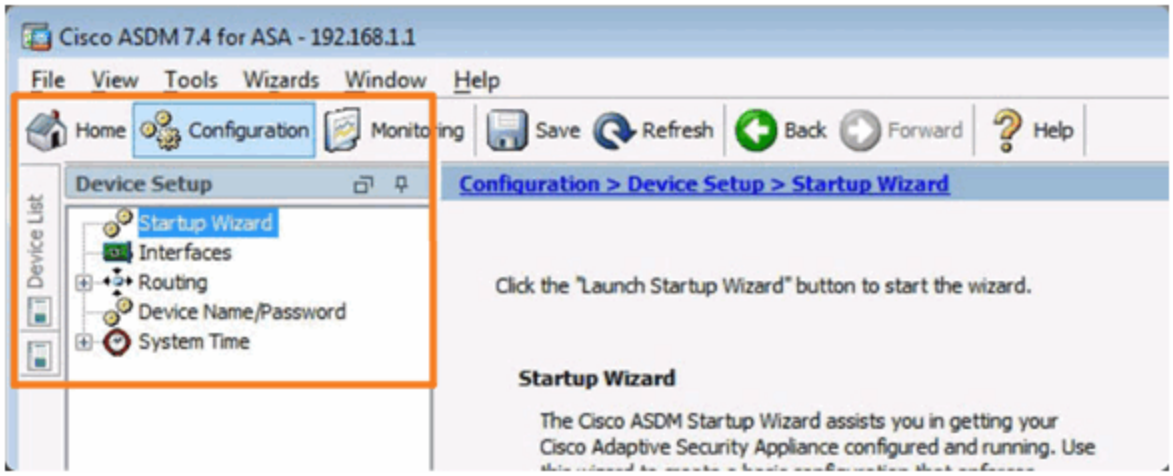
Other Wizards



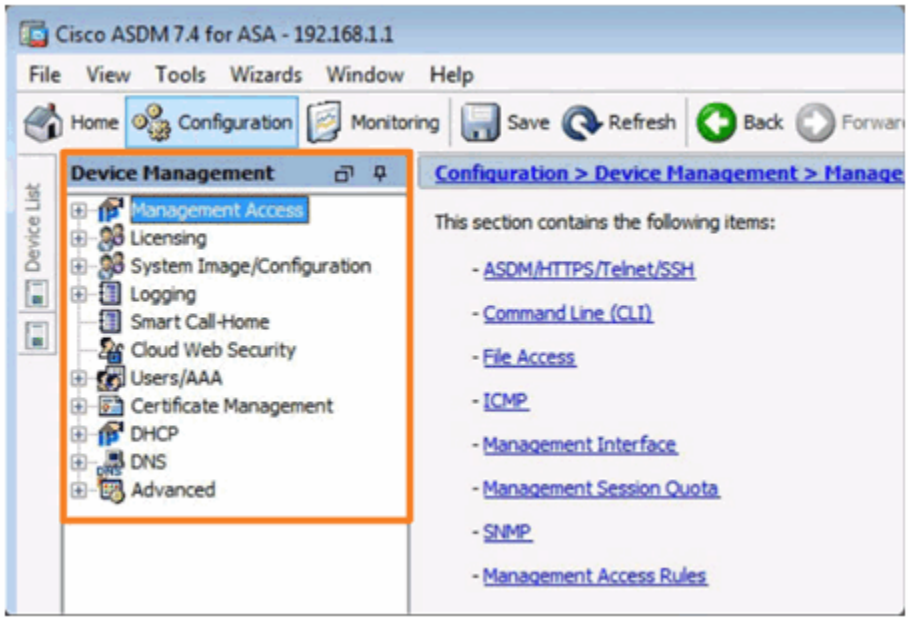
Topic 10.1.3: Configuring Management Settings and Services

Configuring Settings in ASDM

Configuration Device Setup Tab

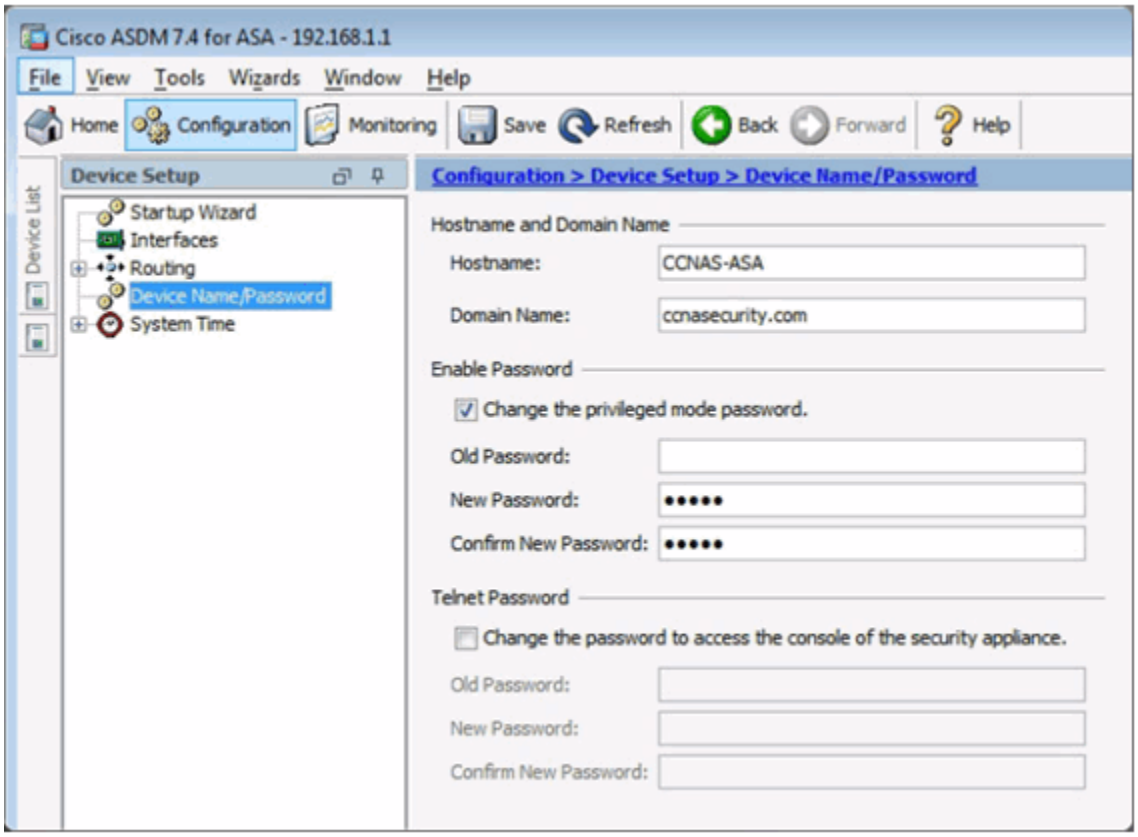


Configuration Device Management Tab

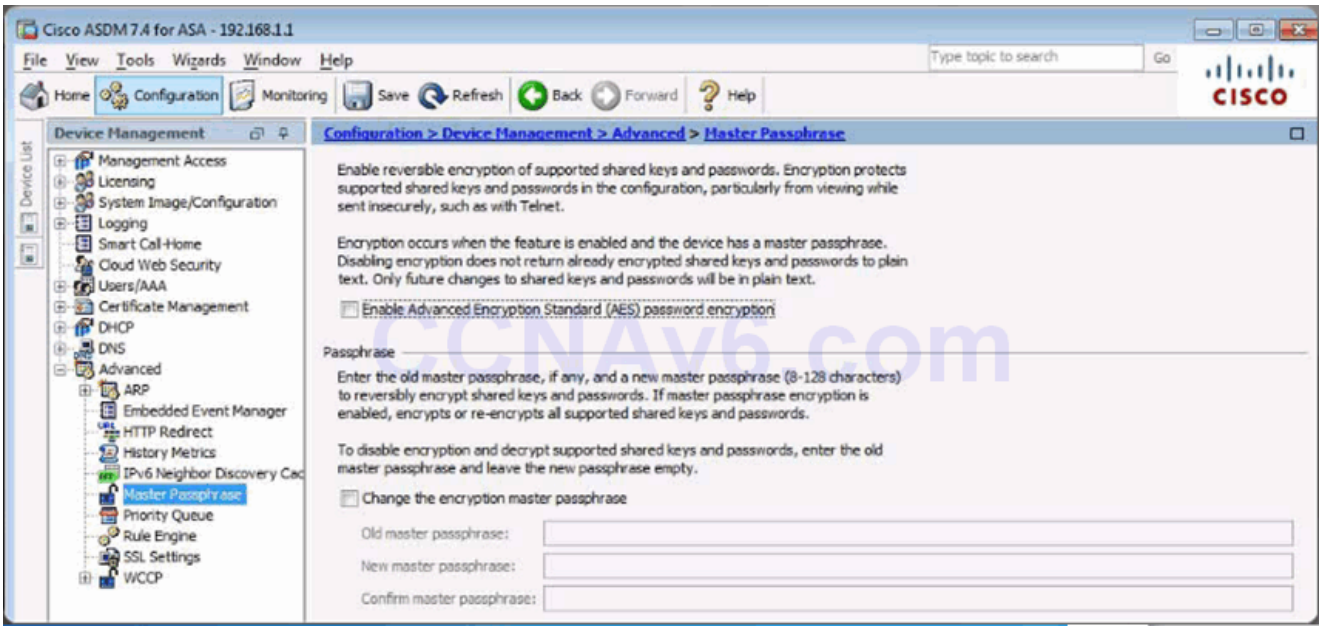


Configuring Basic Settings in ASDM

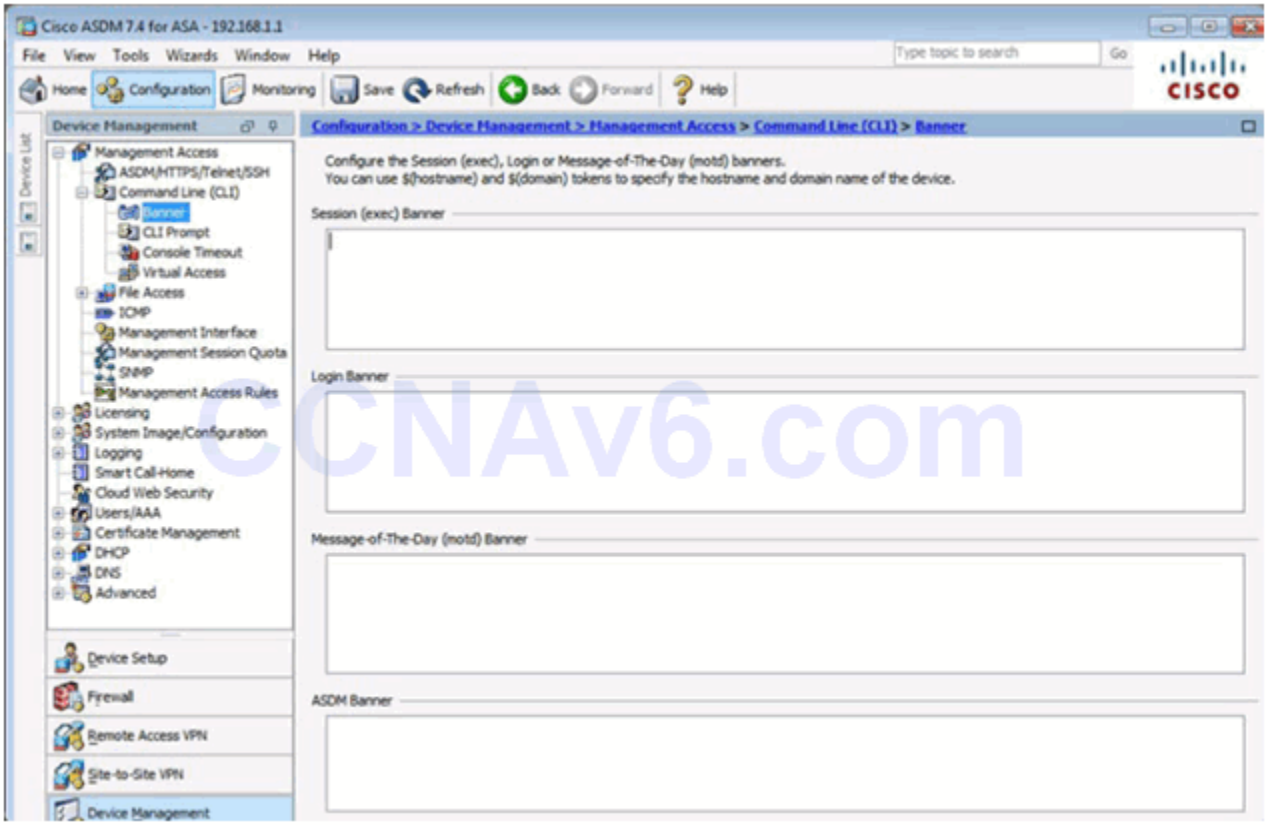
Configuring Hostname, Domain Name, and Enable Password



Configuring a Master Passphrase

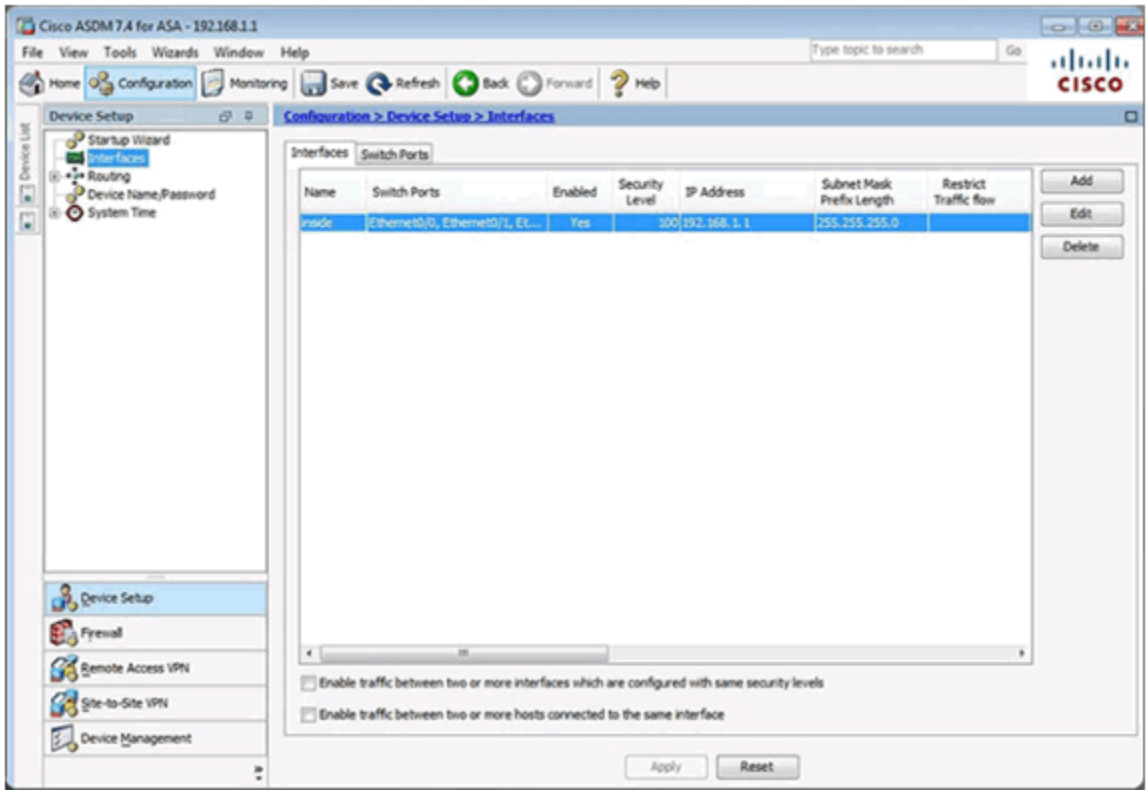


Configuring Legal Notification

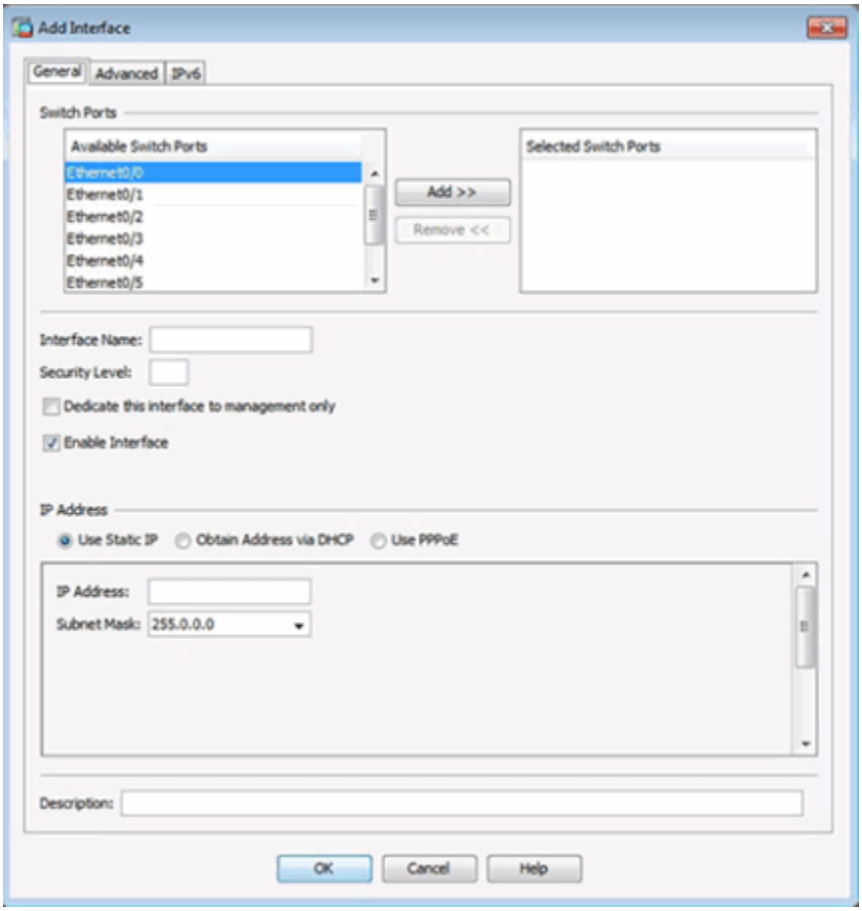


Configuring Interfaces in ASDM

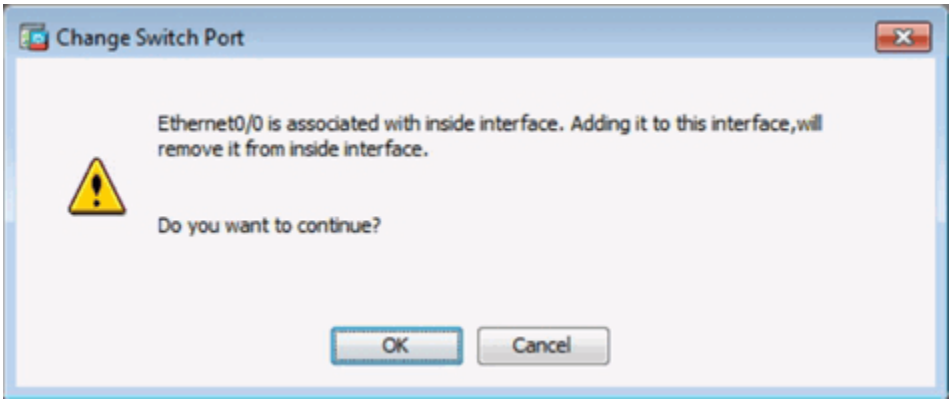
Configuring Interfaces



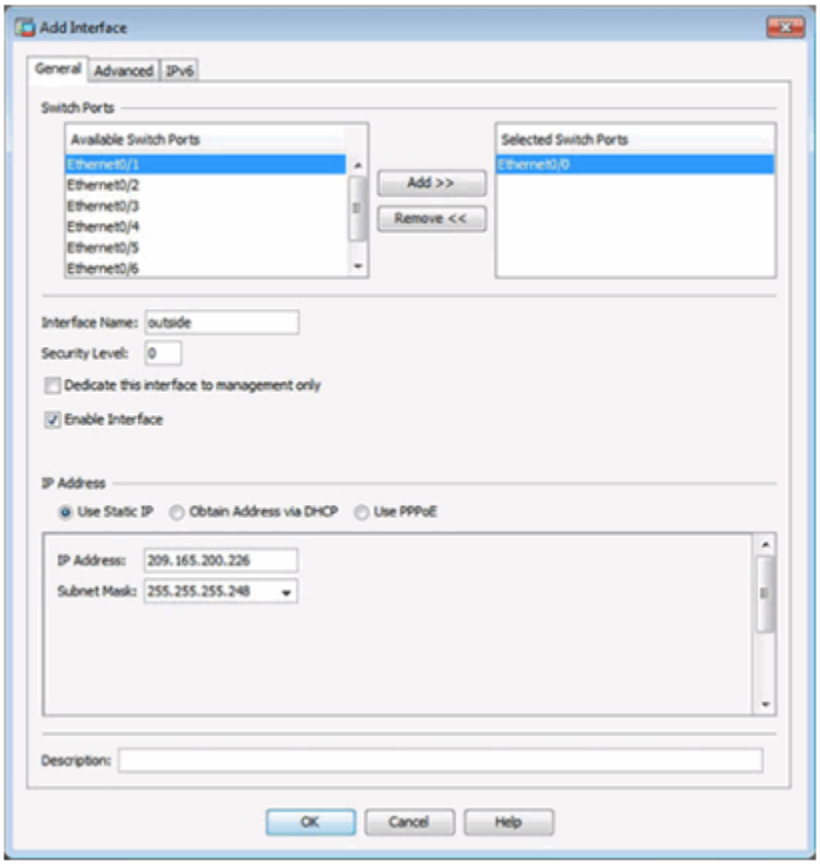
Adding an Outside Interface



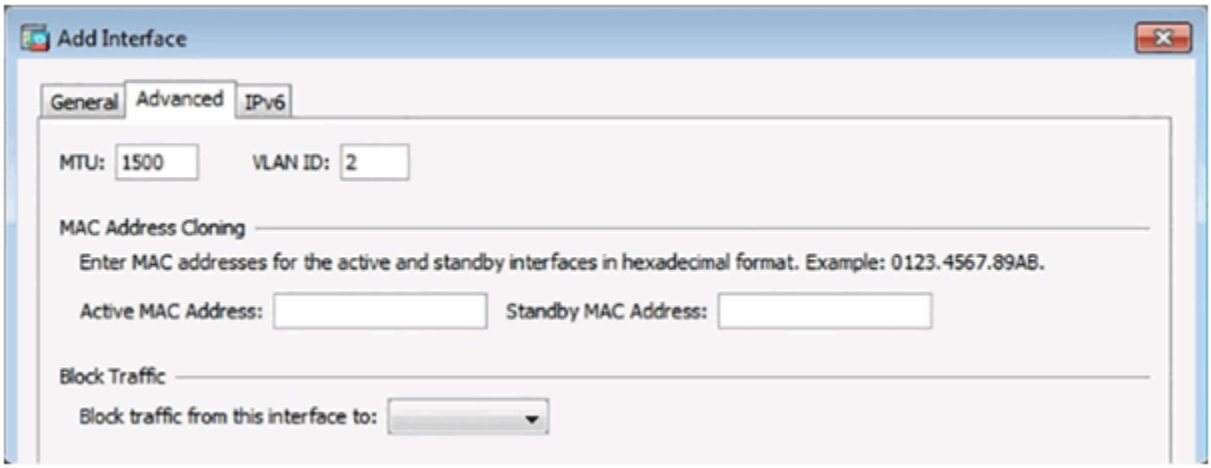
Change Switch Port Window



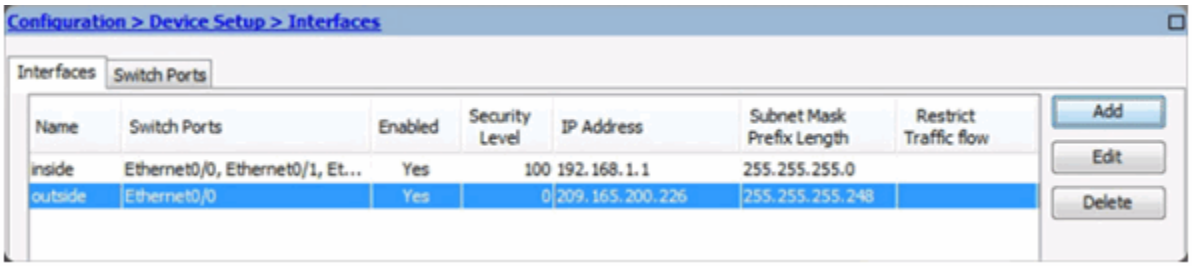
Adding an Outside Interface



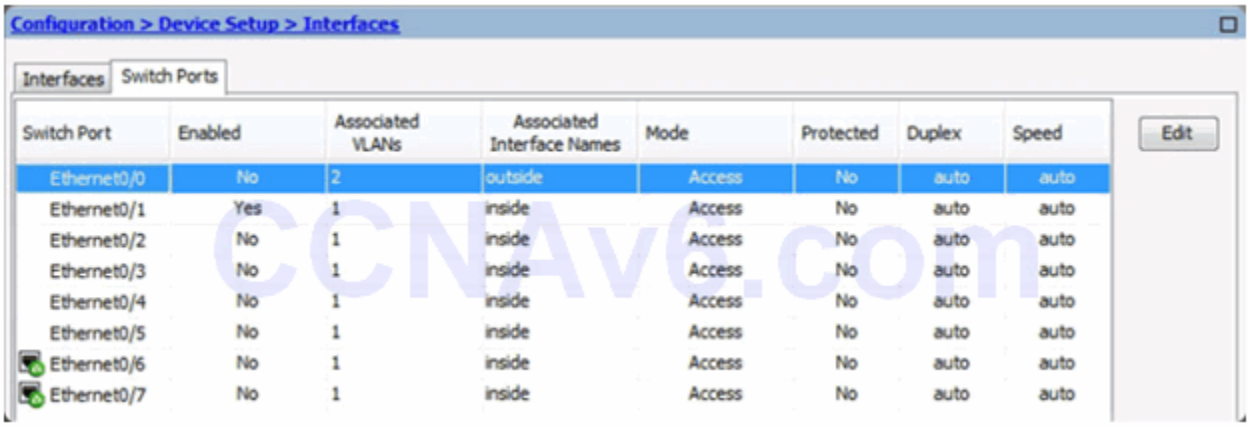
Advanced Outside Interface Settings



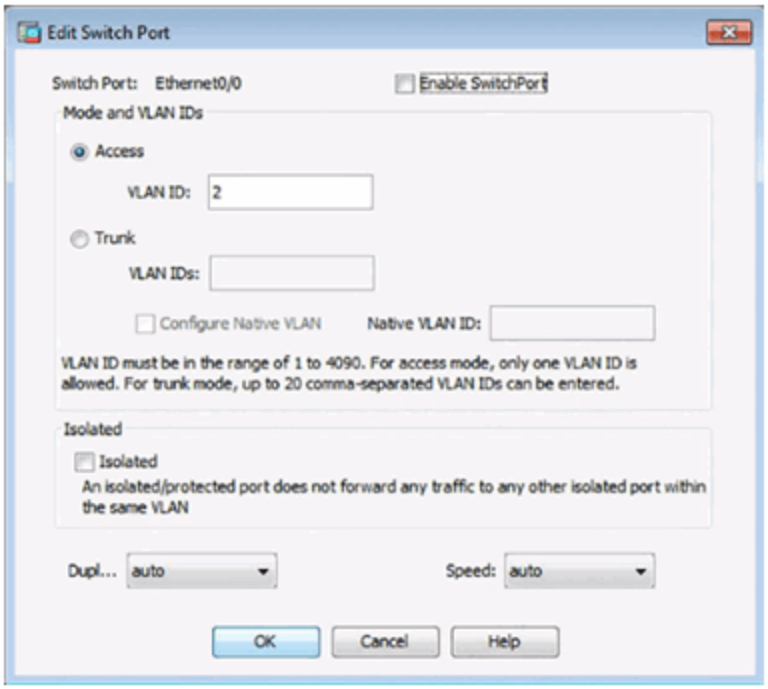
Updated Interface Page



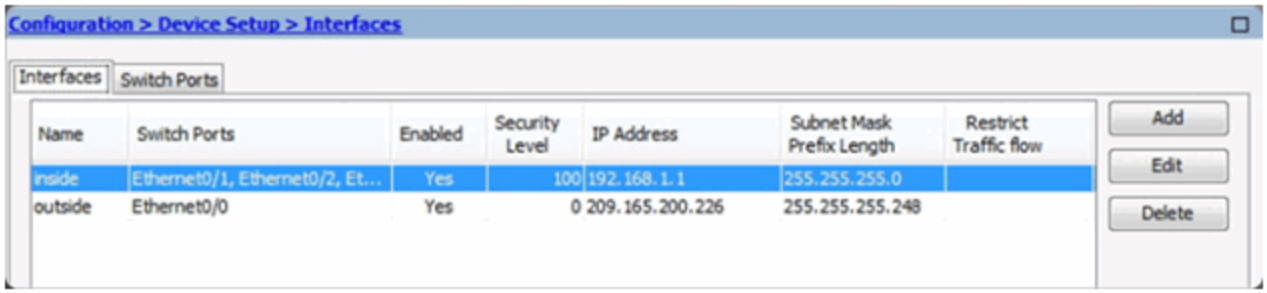
Verifying Interfaces



Enable Switch Ports

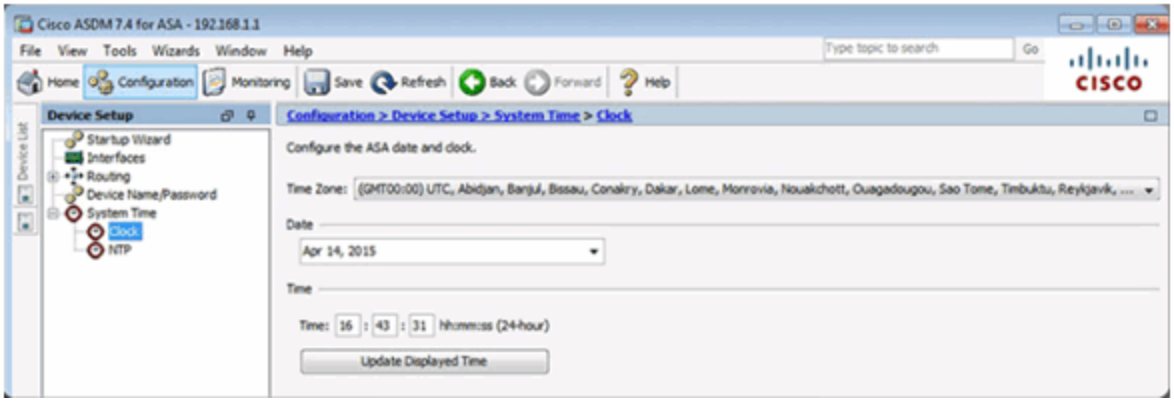


Apply Configuration

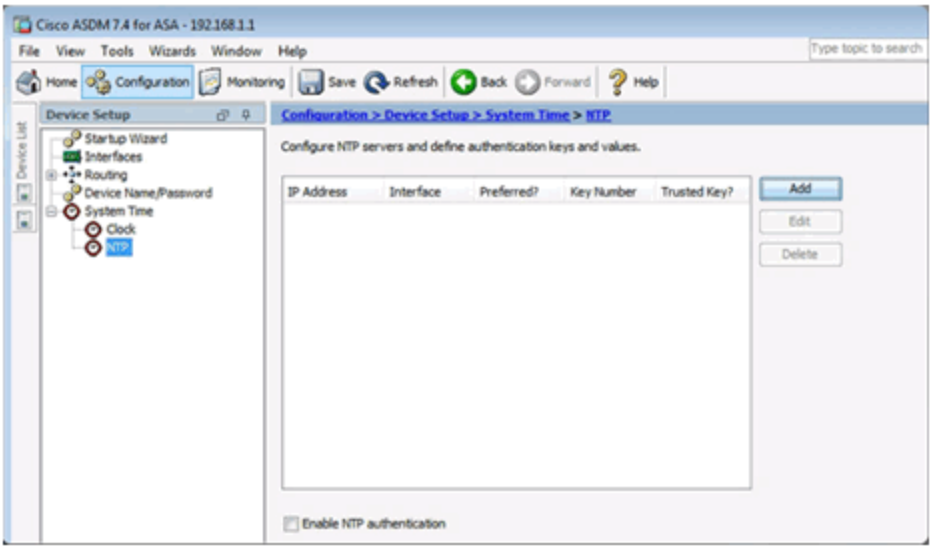


Configuring the System Time in ASDM

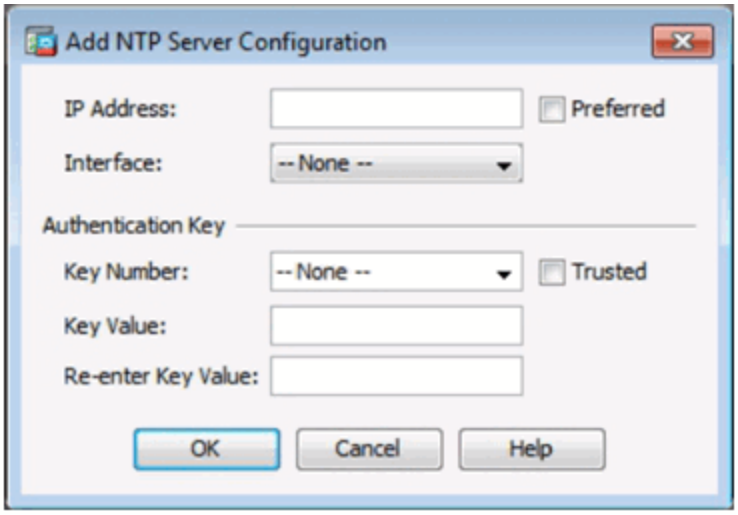
Manually Change the System Time



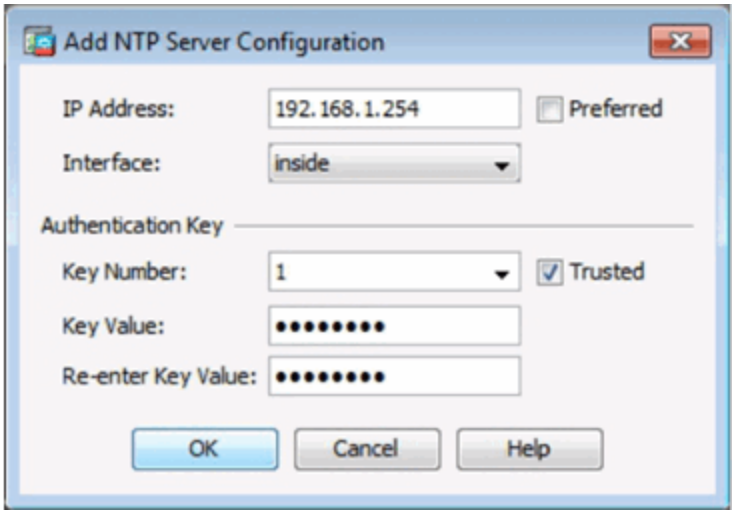
Use NTP to Change the System Time



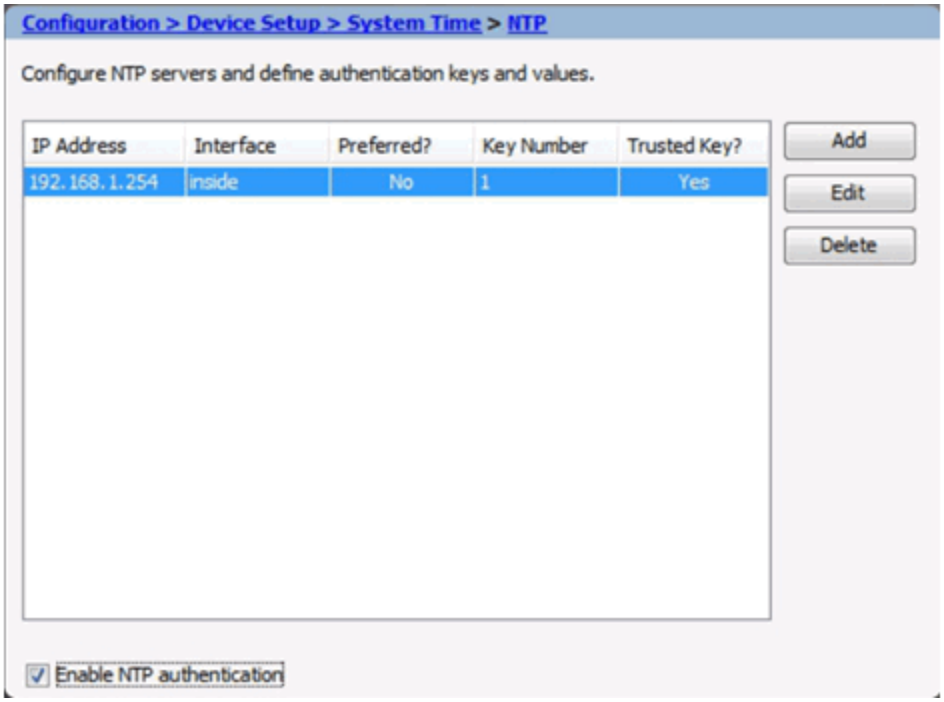
Add an NTP Server



Configure an NTP Server

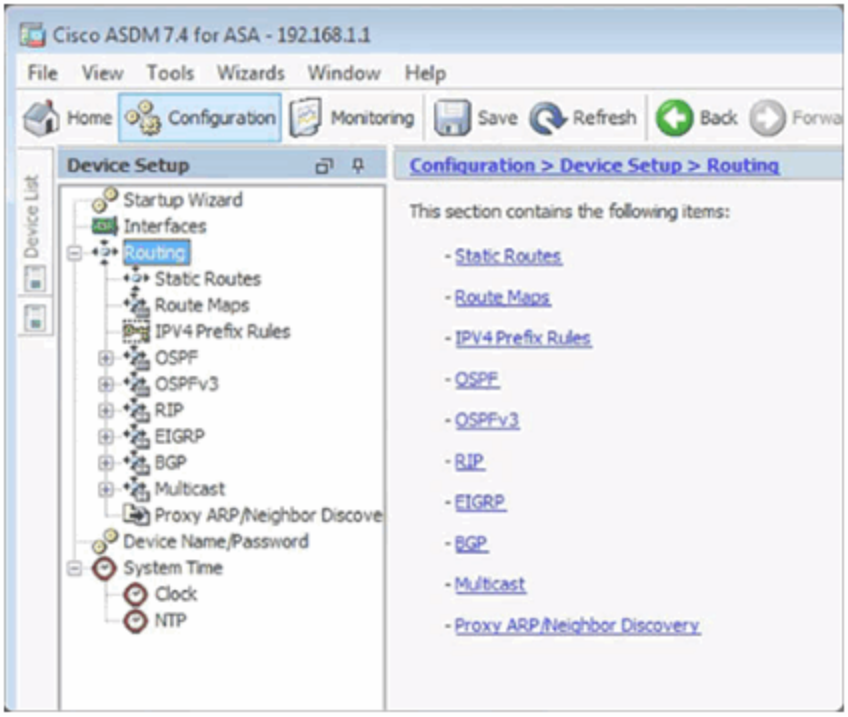


Apply the Configuration

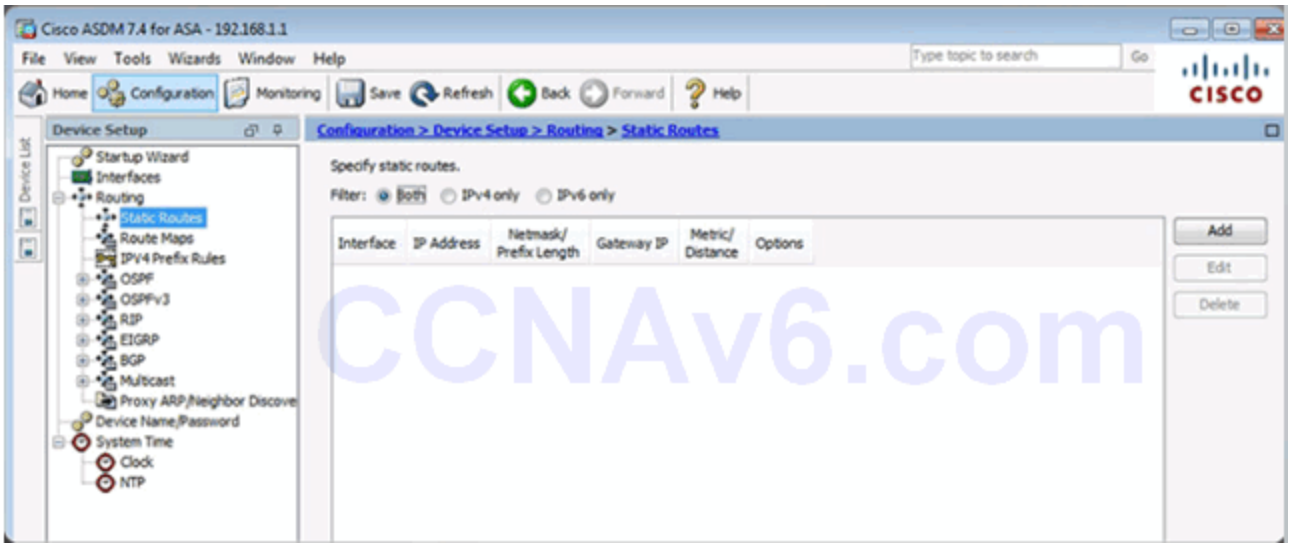


Configuring Routing in ASDM

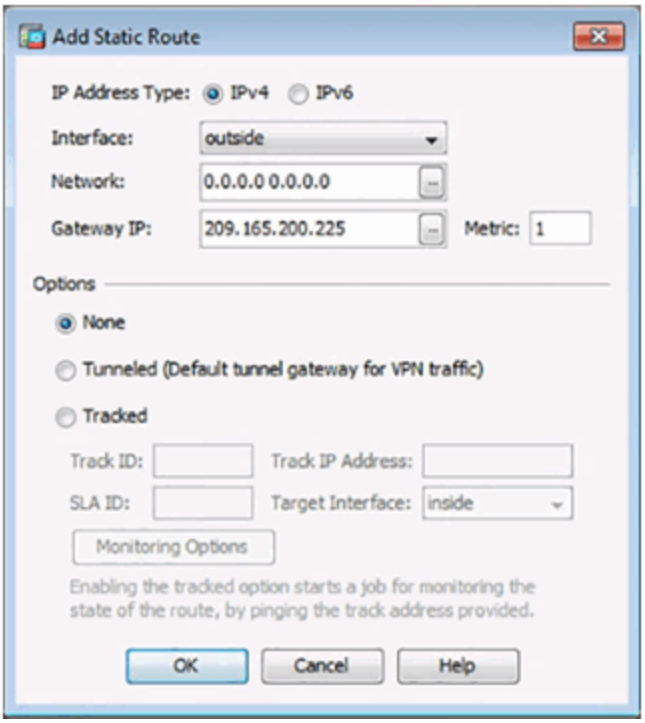
Configuring Routing



Configuring a Default Static Route

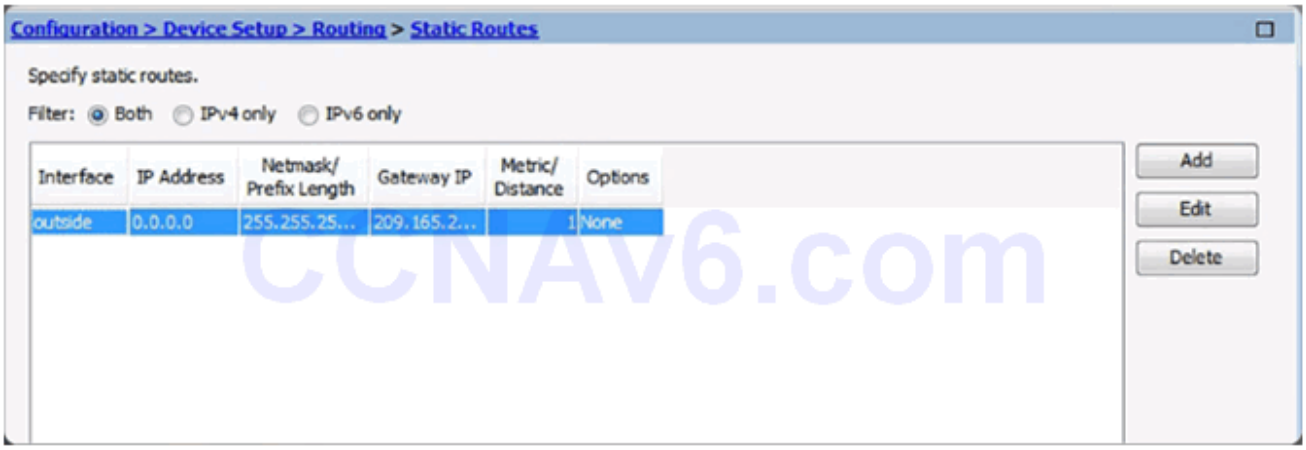


Add or Edit Route Window



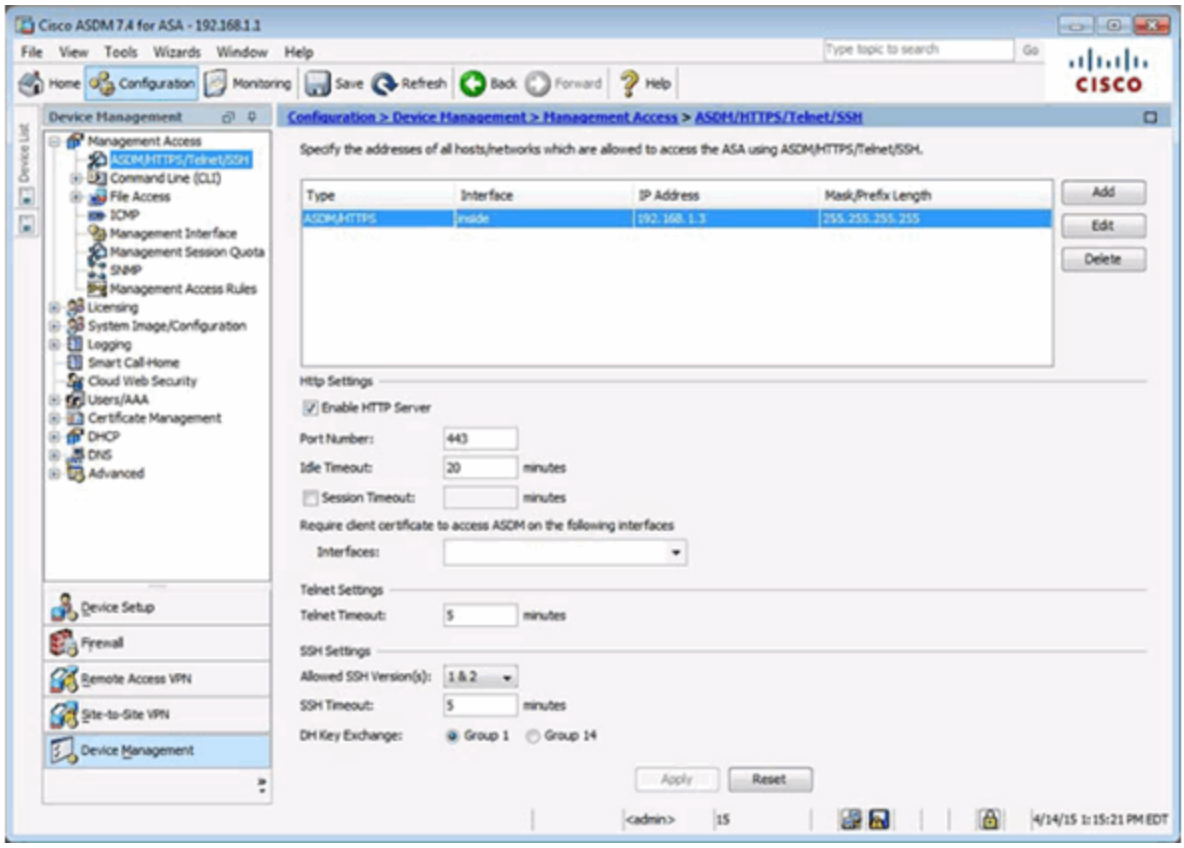
Add Static Route Details

Apply the Configuration

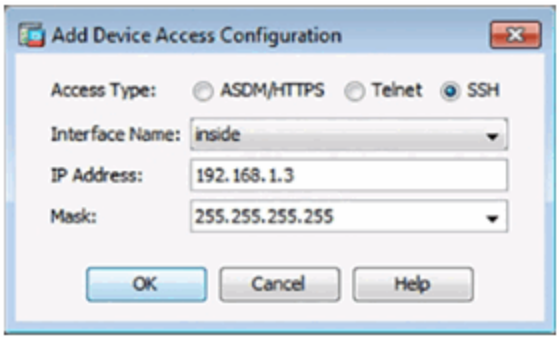


Configuring Device Management Access in ASDM

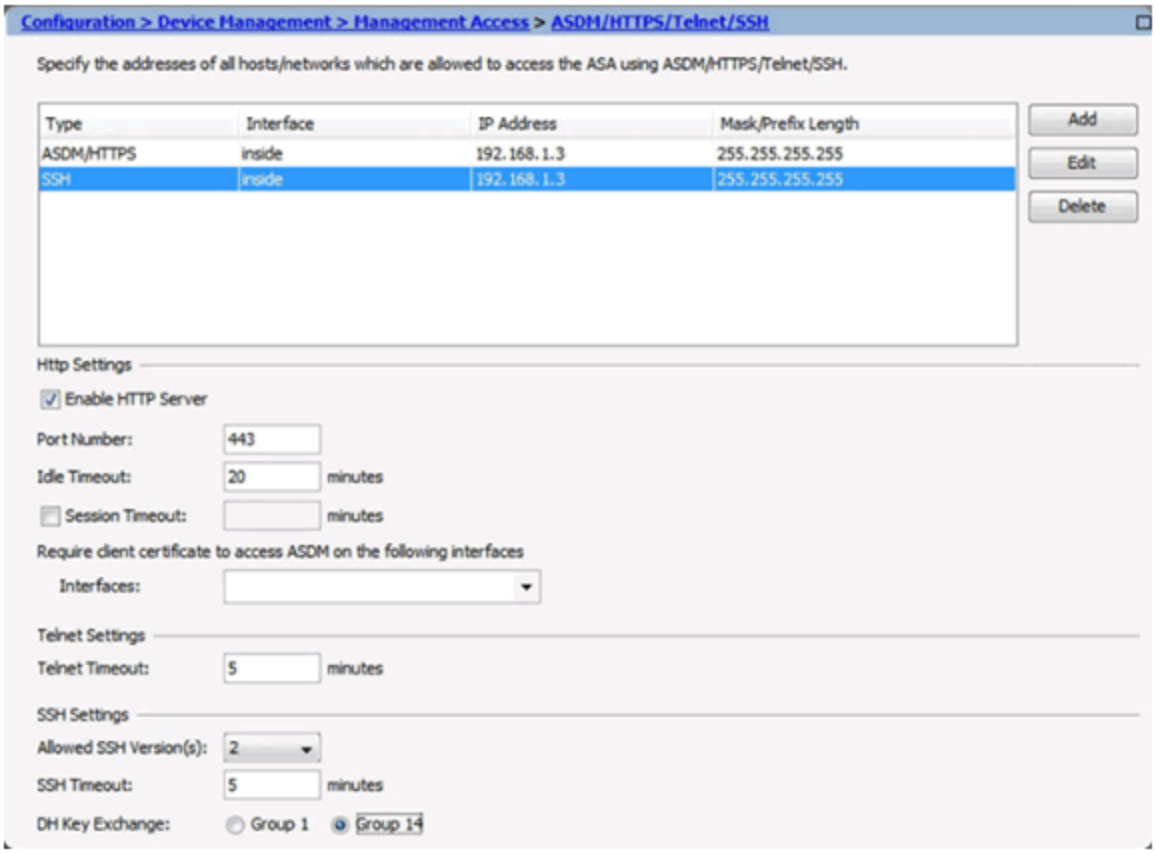
Configure ASDM/HTTPS/Telnet/SSH Access



Add Device Access Configuration Window

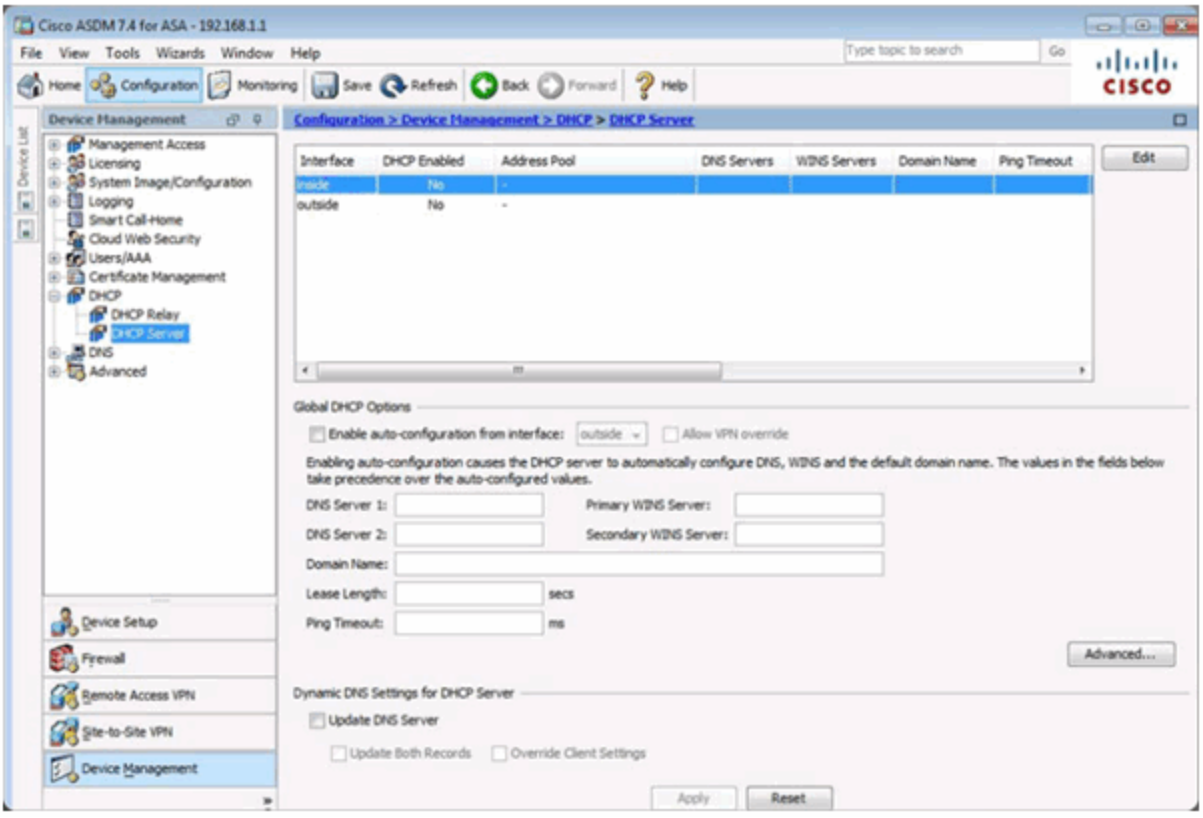


Configure SSH Settings

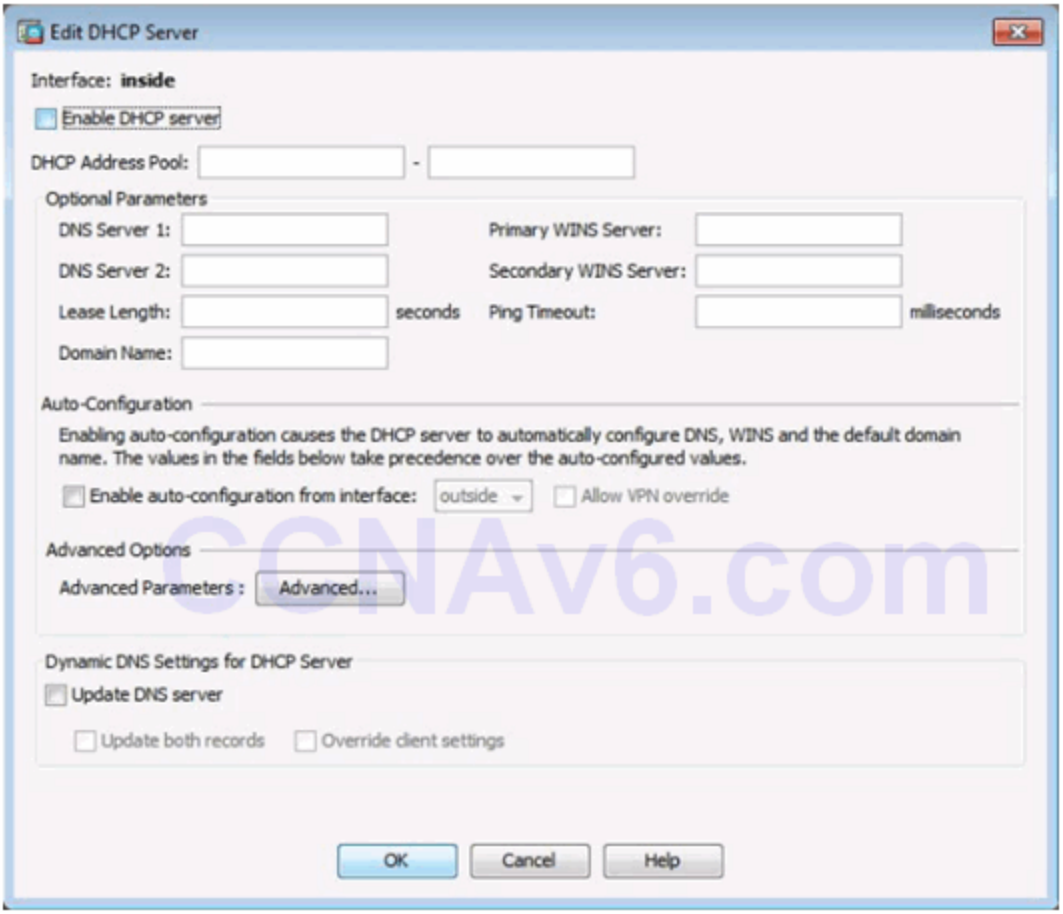


Configuring DHCP Services in ASDM

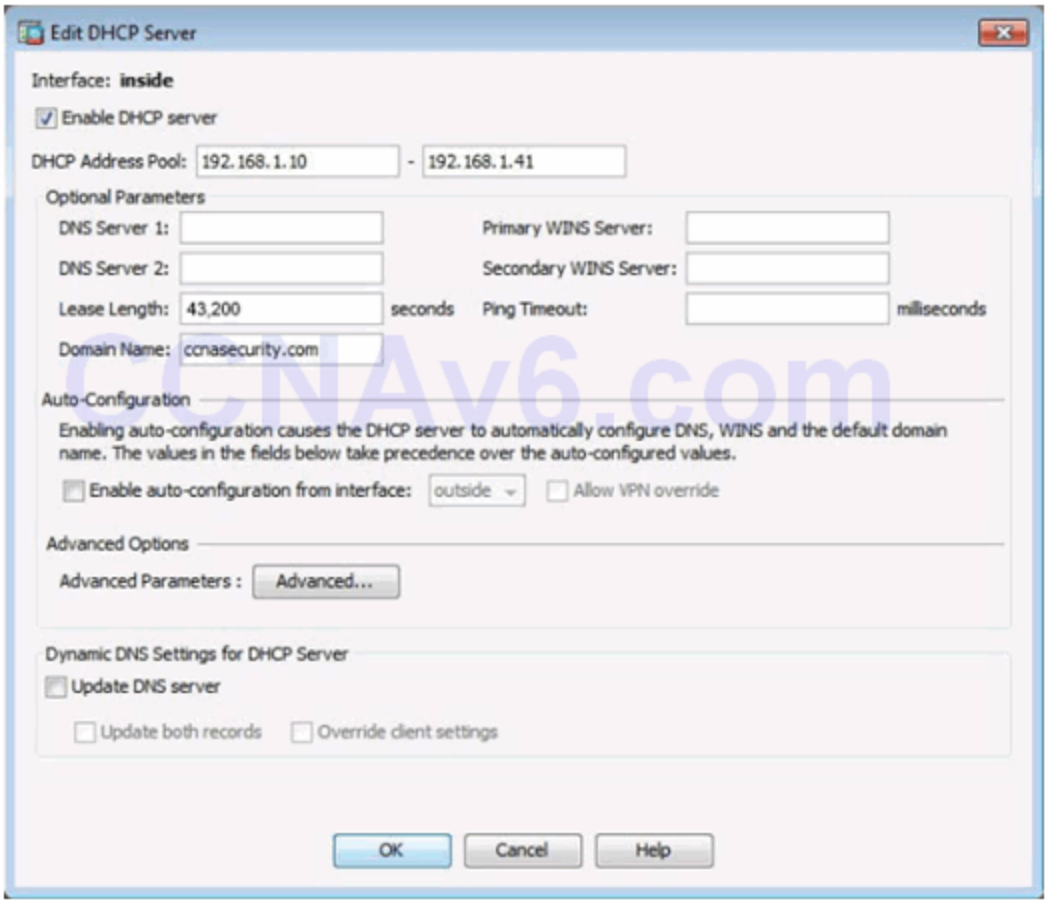
DHCP Server Page



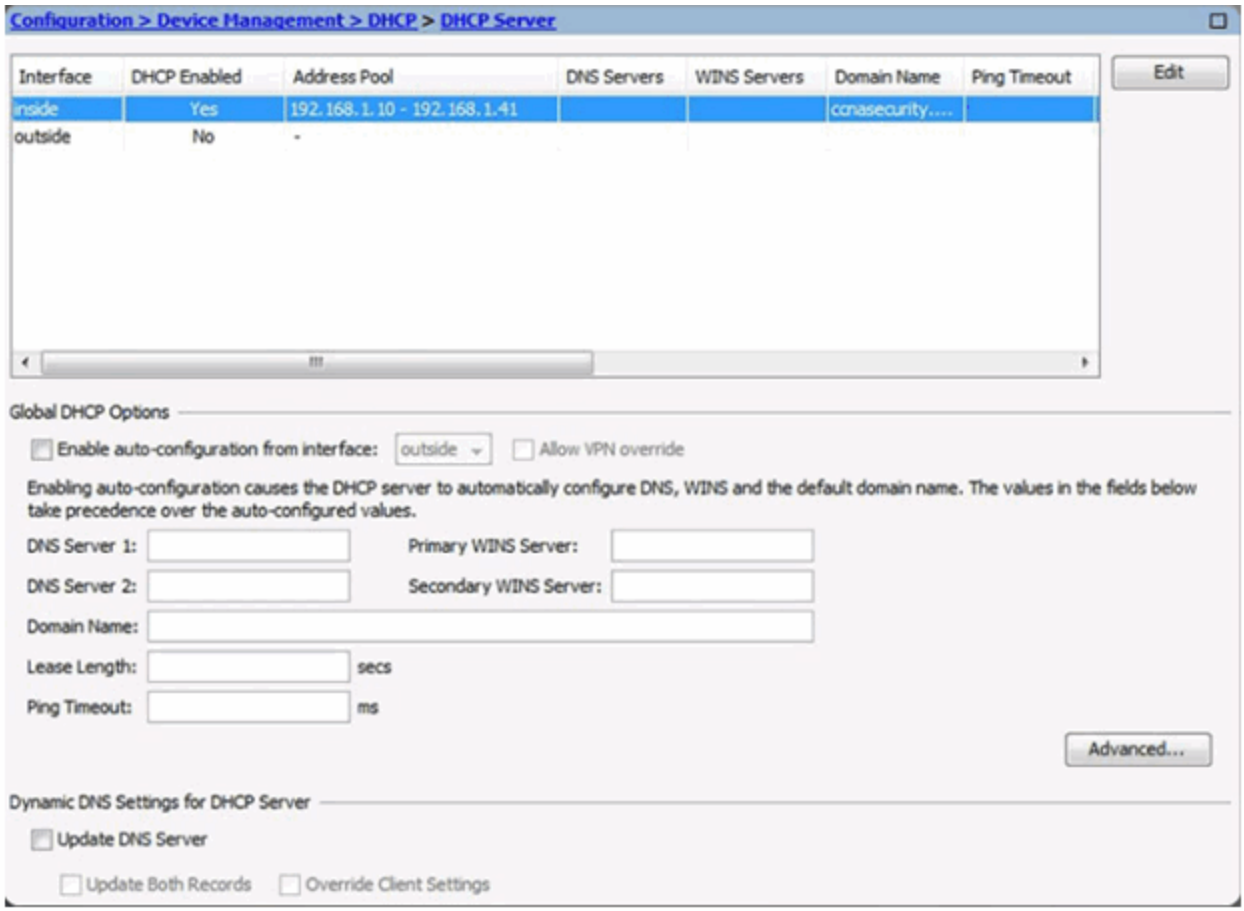
Edit DHCP Server Window



Configuring DHCP Server Services



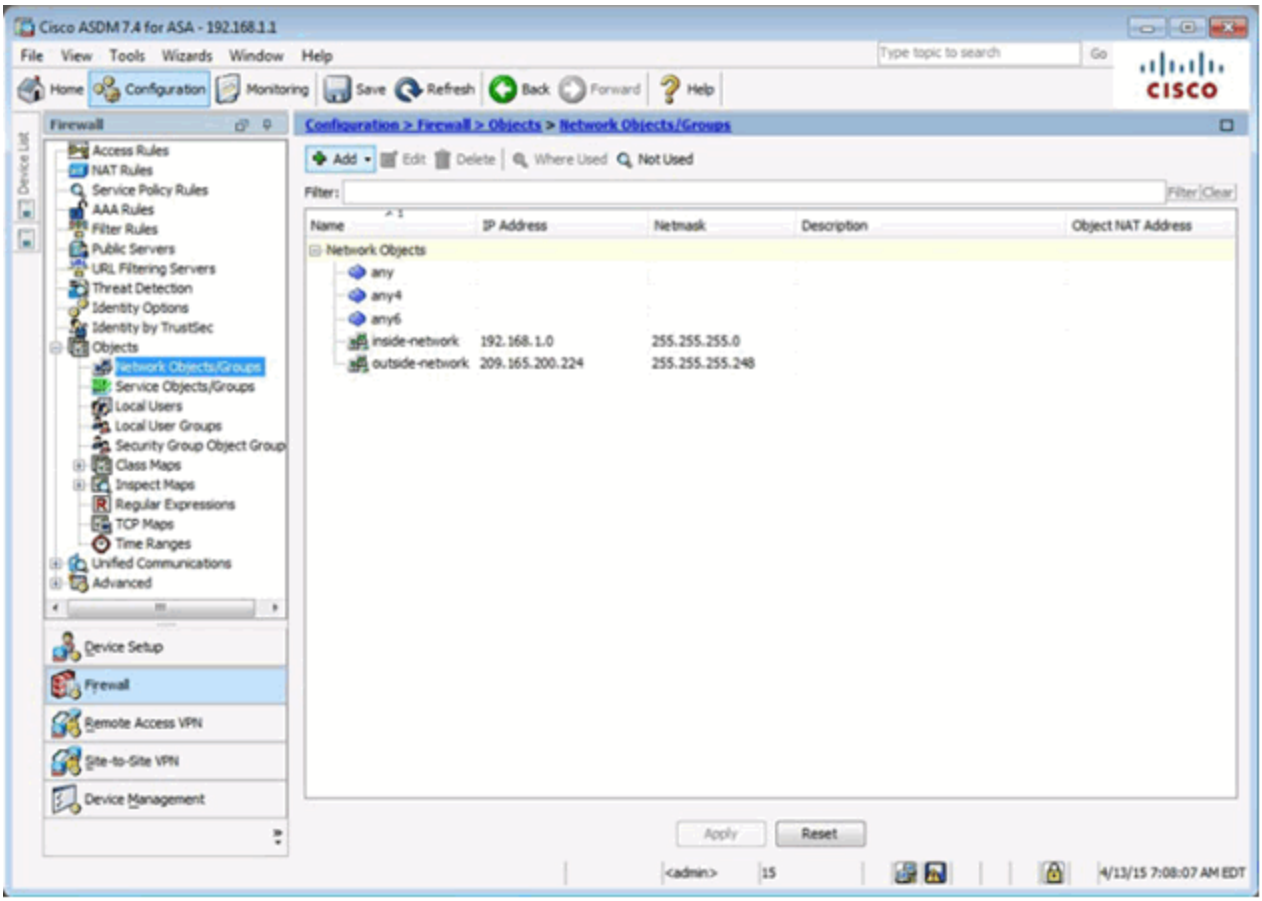
Verifying DHCP Server Services



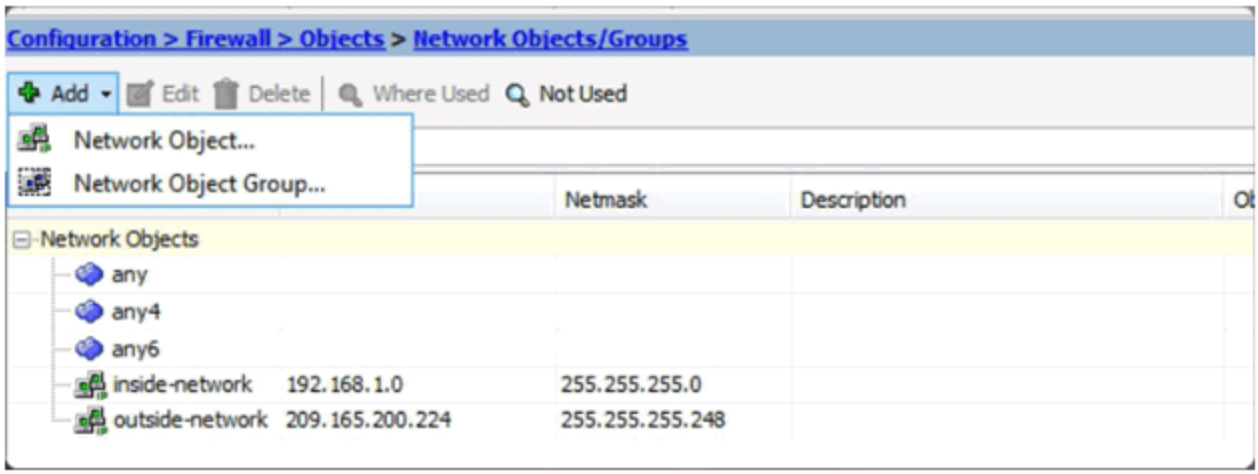
Topic 10.1.4: Configuring Advanced ASDM Features

Objects in ASDM

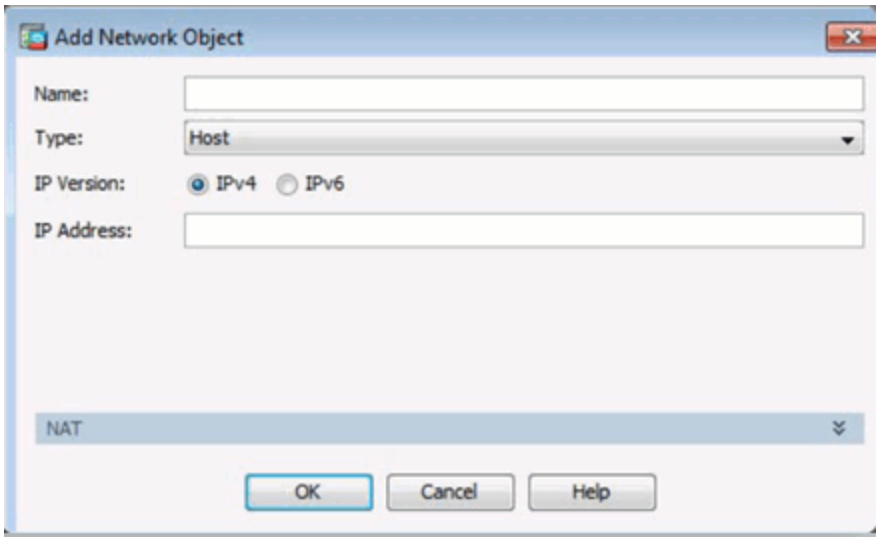
Network Objects/Groups Page



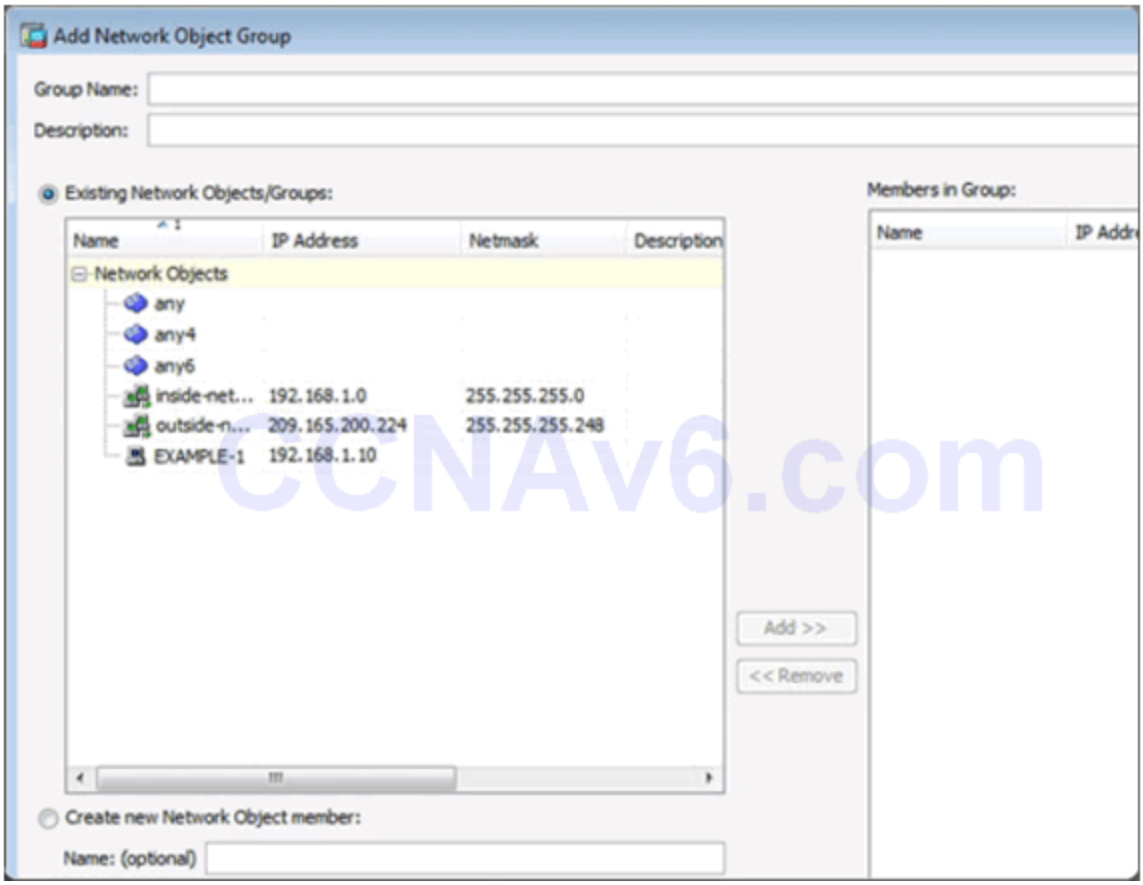
Adding a Network Object/Group



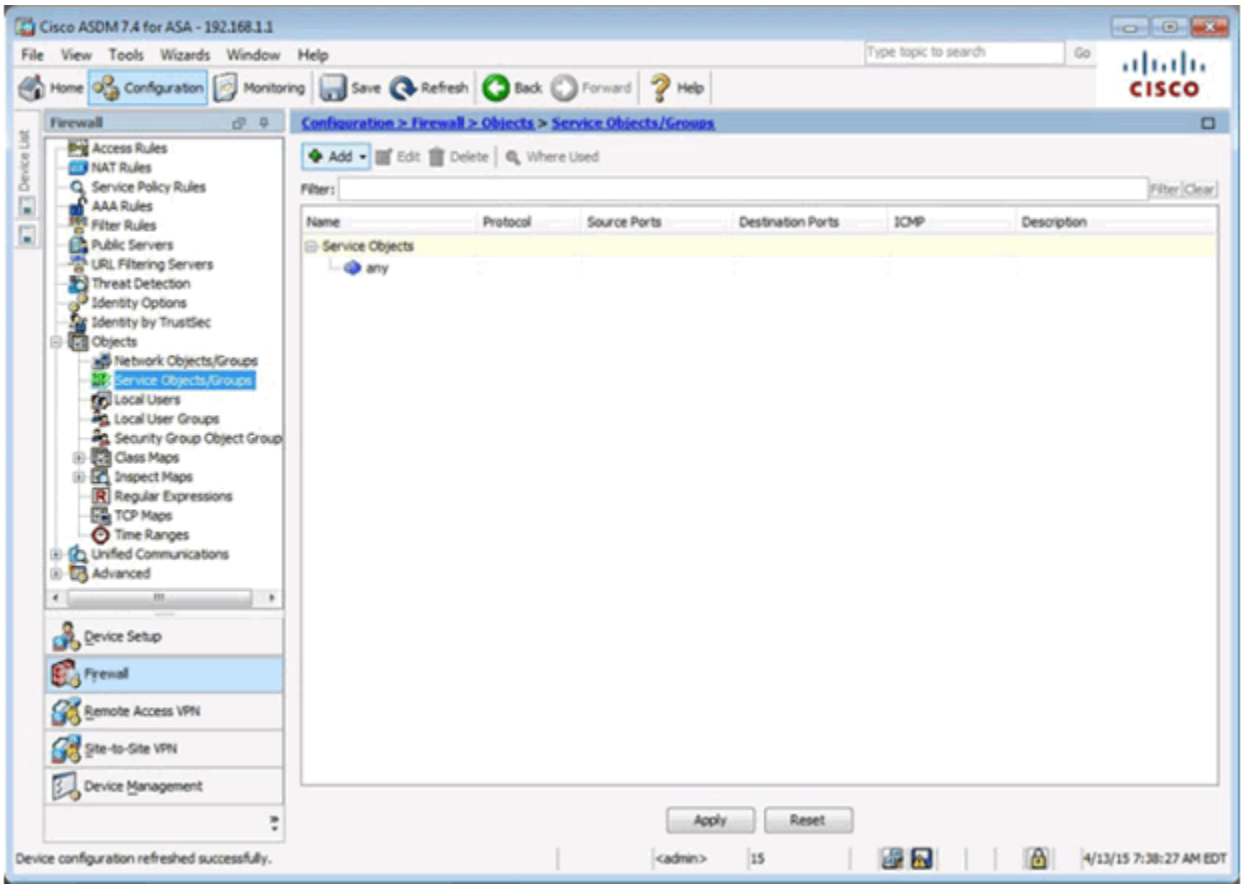
Add Network Object Window



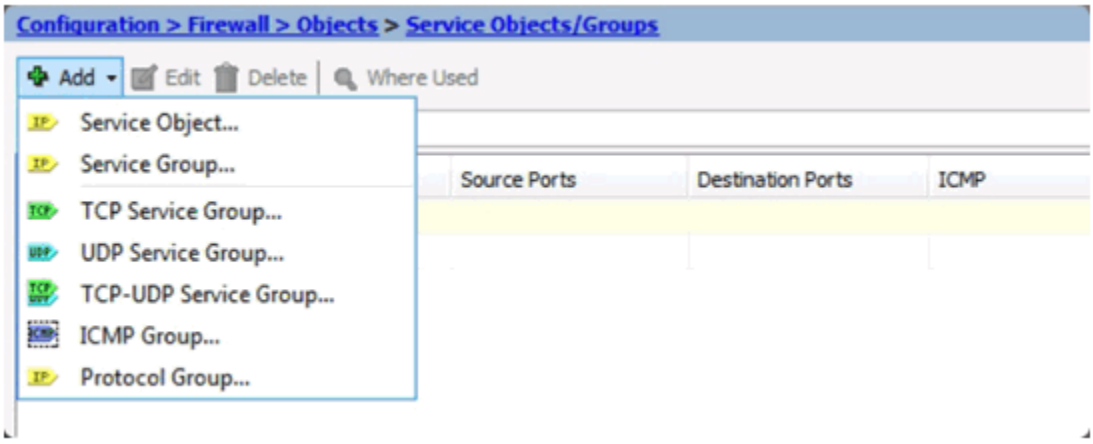
Add Network Object Group Window



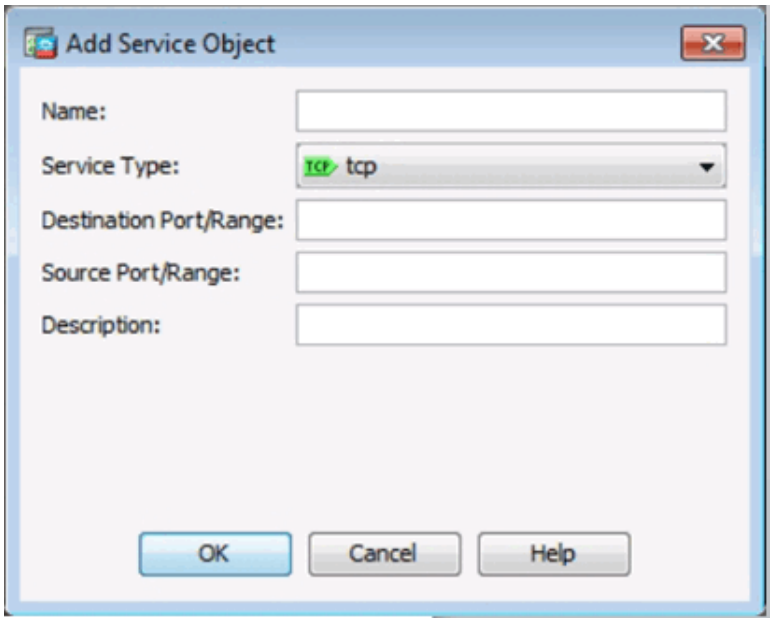
Service Objects/Group Page



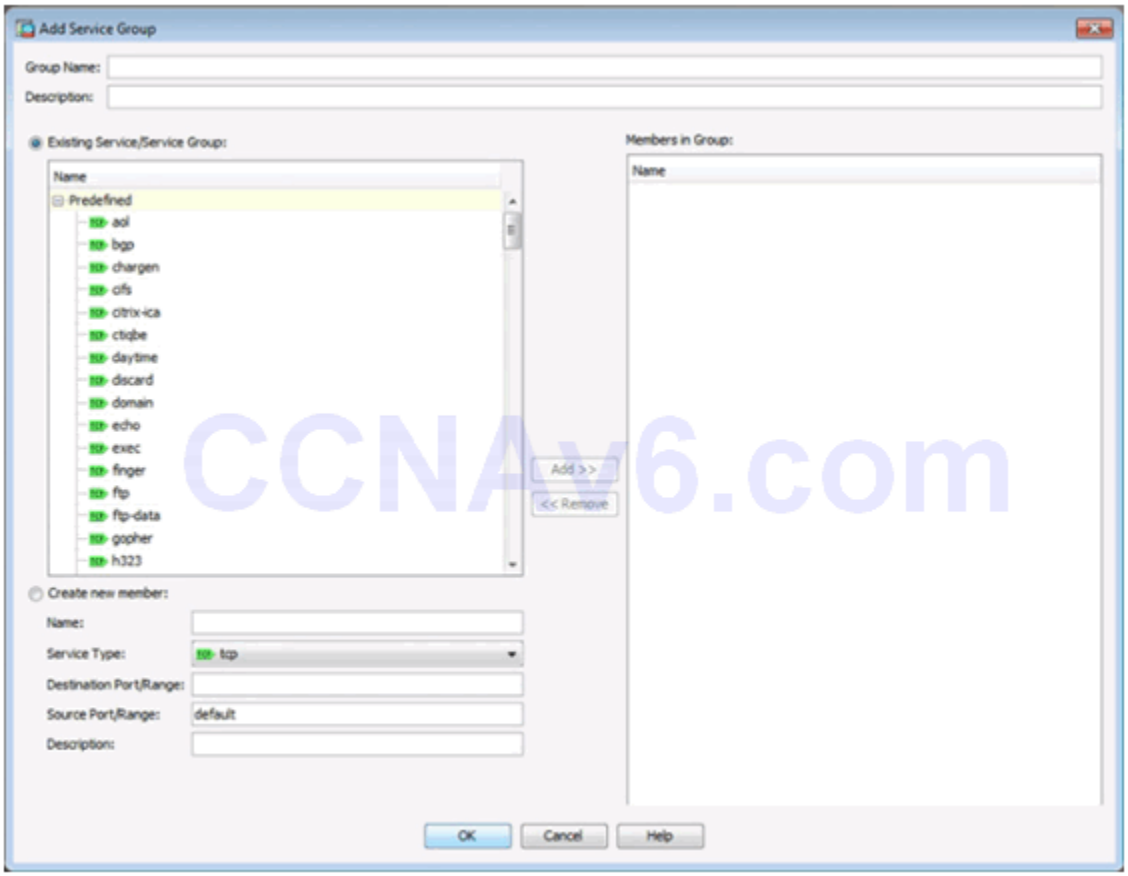
Adding a Service Object/Group



Add Service Object Window

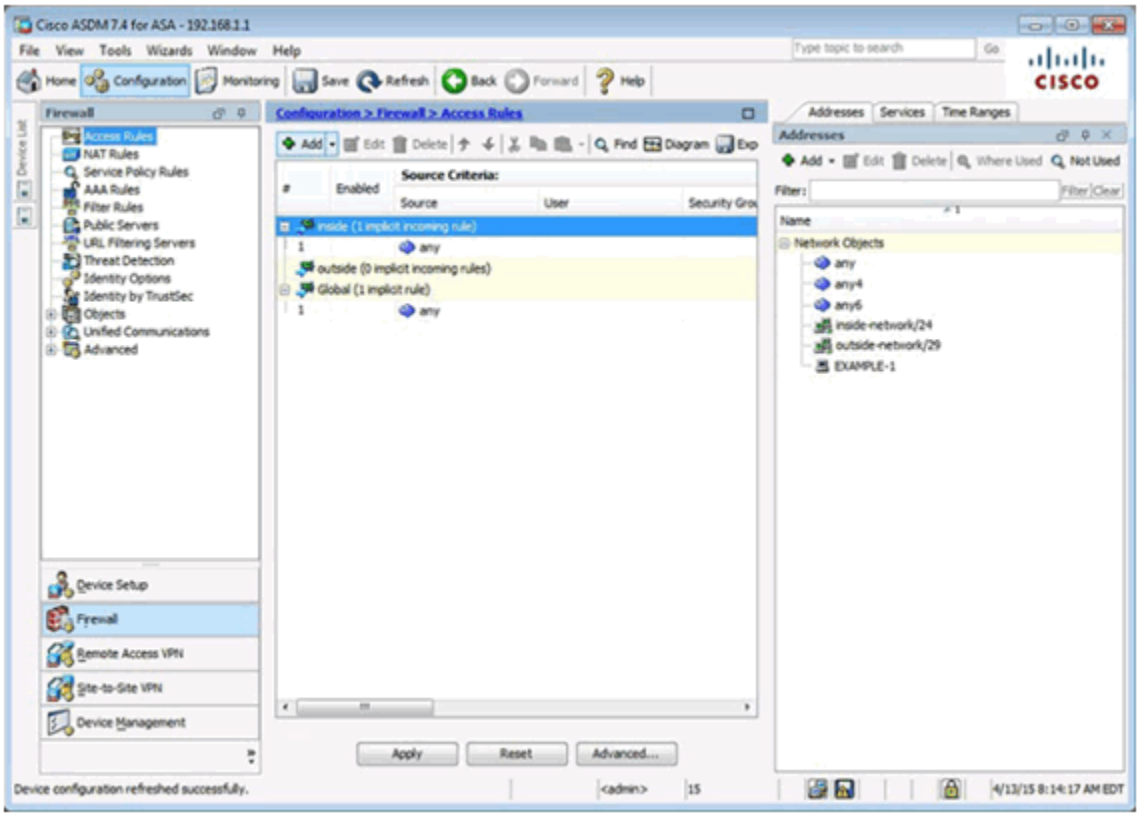


Add Service Object Group Window

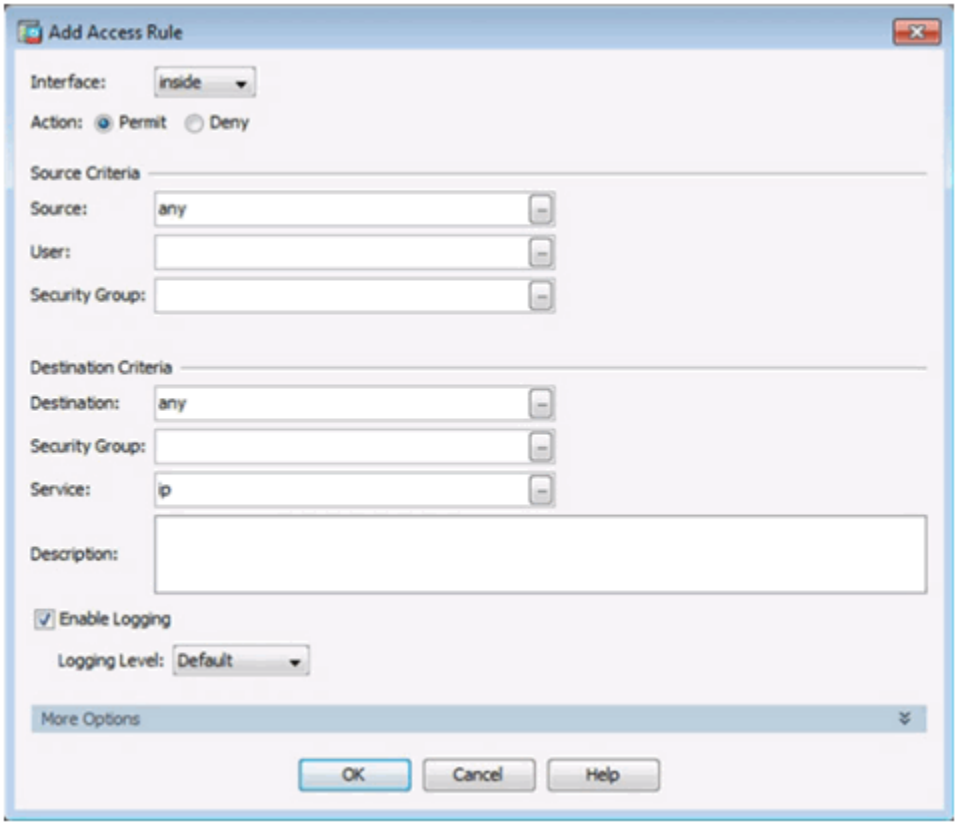


Configuring ACLs Using ASDM

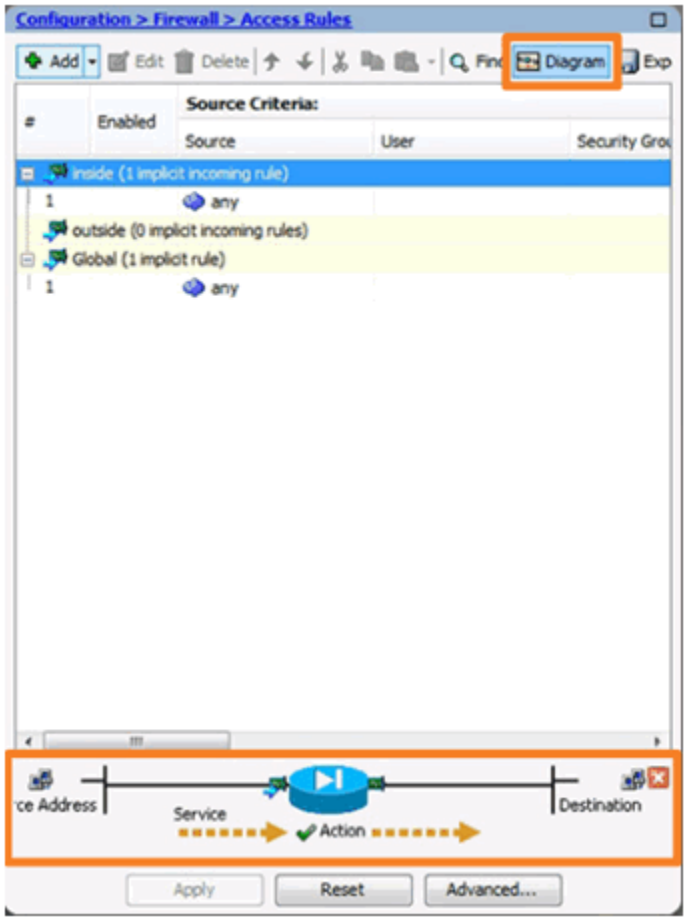
ACLs in ASDM



Add Access Rule Window

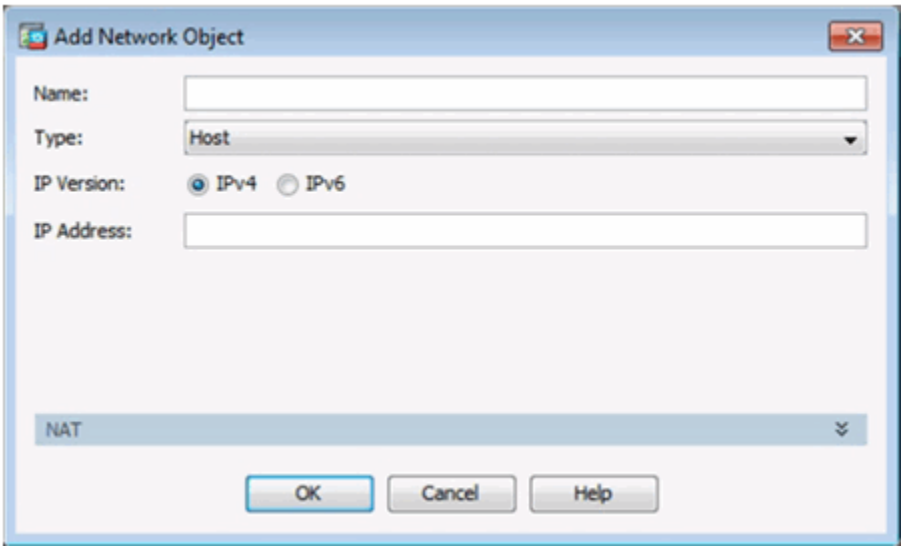


Diagramming Access Rules

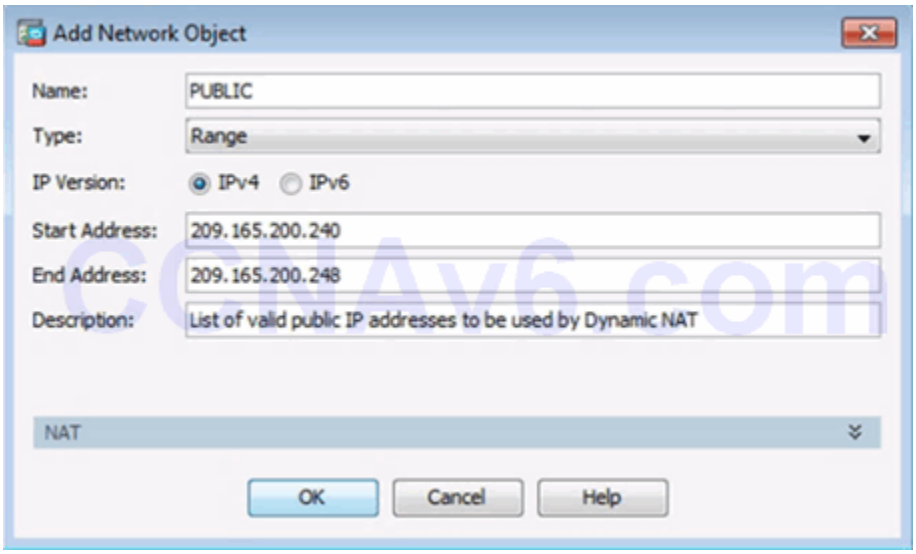


Configuring Dynamic NAT in ASDM

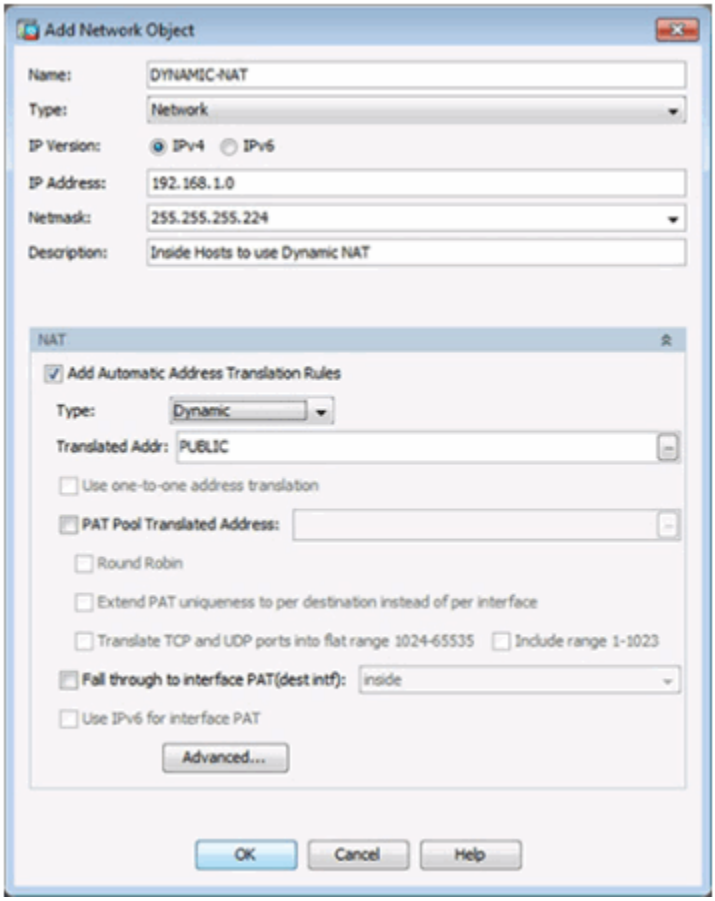
Add Network Object Window



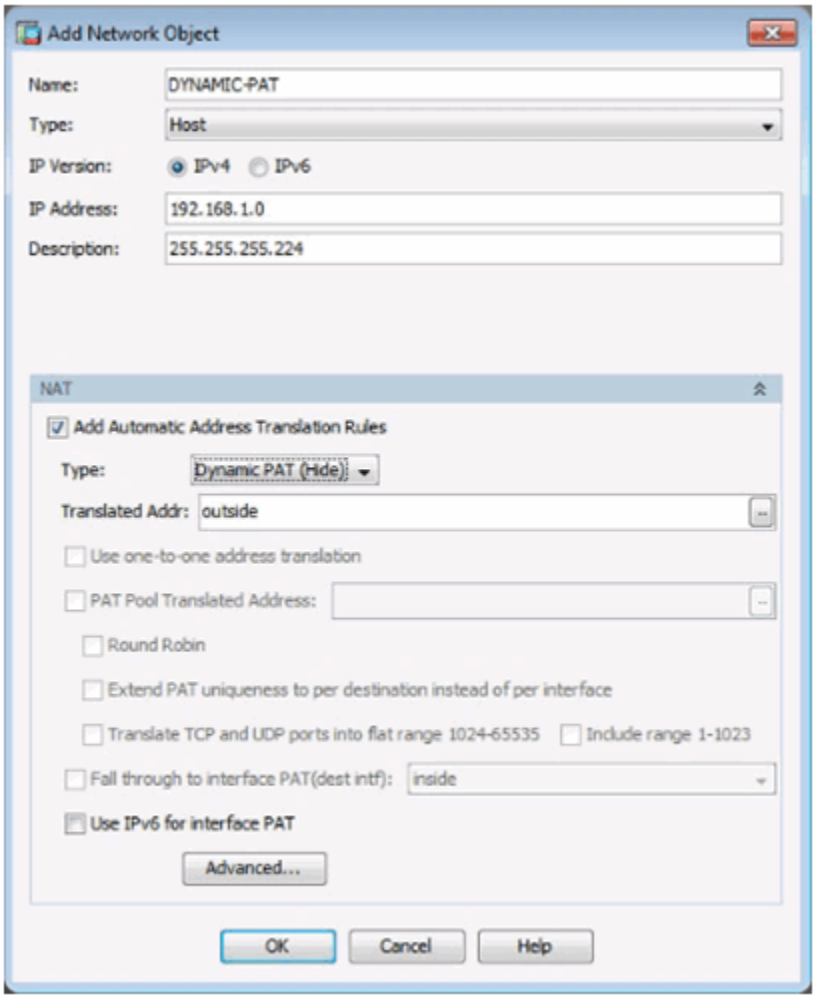
Creating a Network Object for Public Addresses



Creating a Network Object for Dynamic NAT

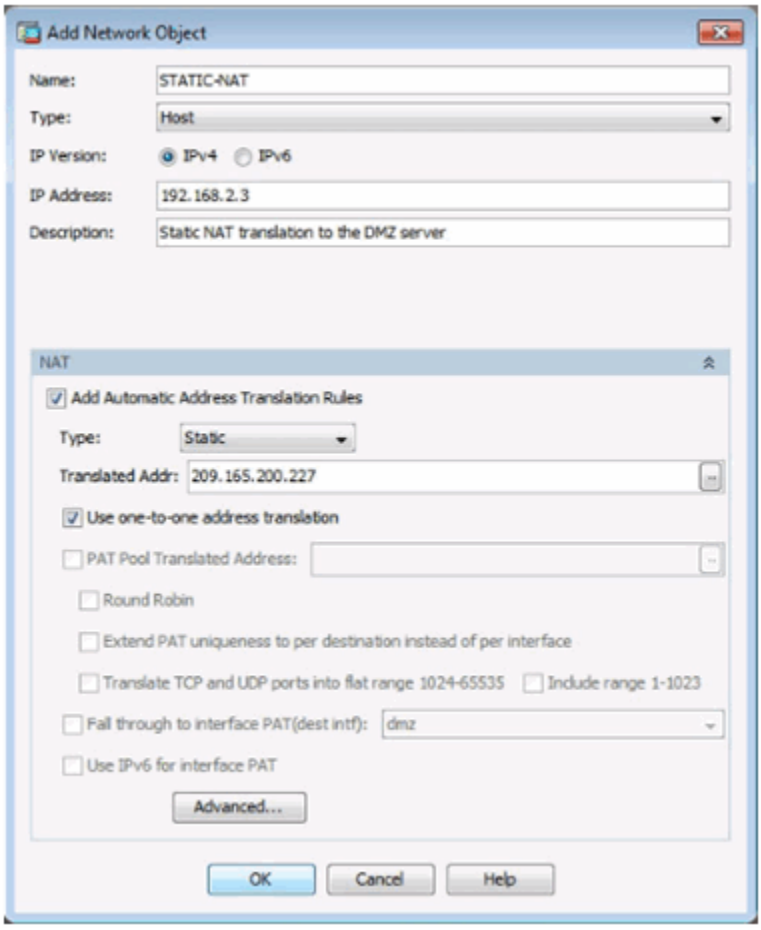


Configuring Dynamic PAT in ASDM

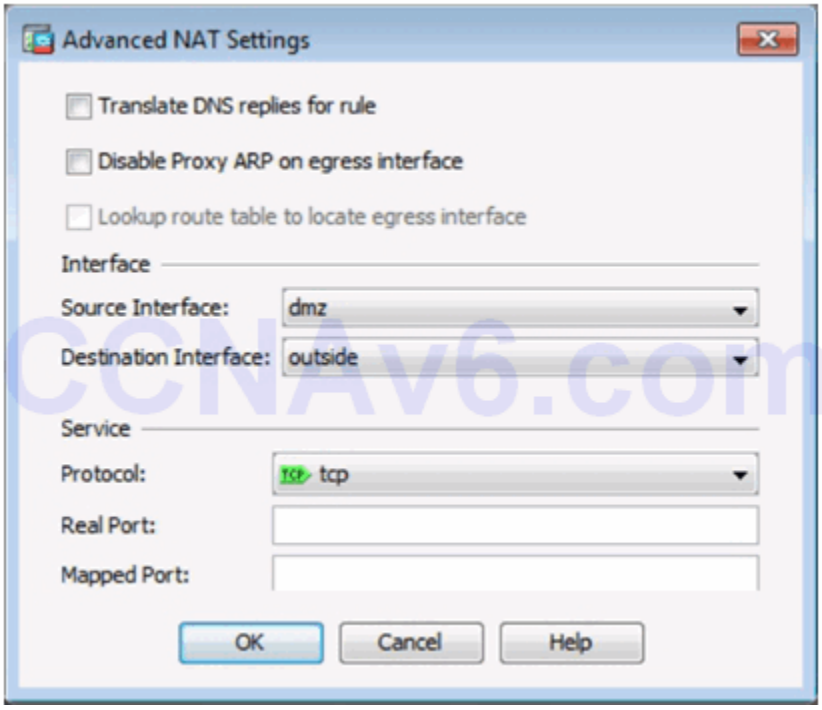


Configuring Static NAT in ASDM

Static NAT in ASDM

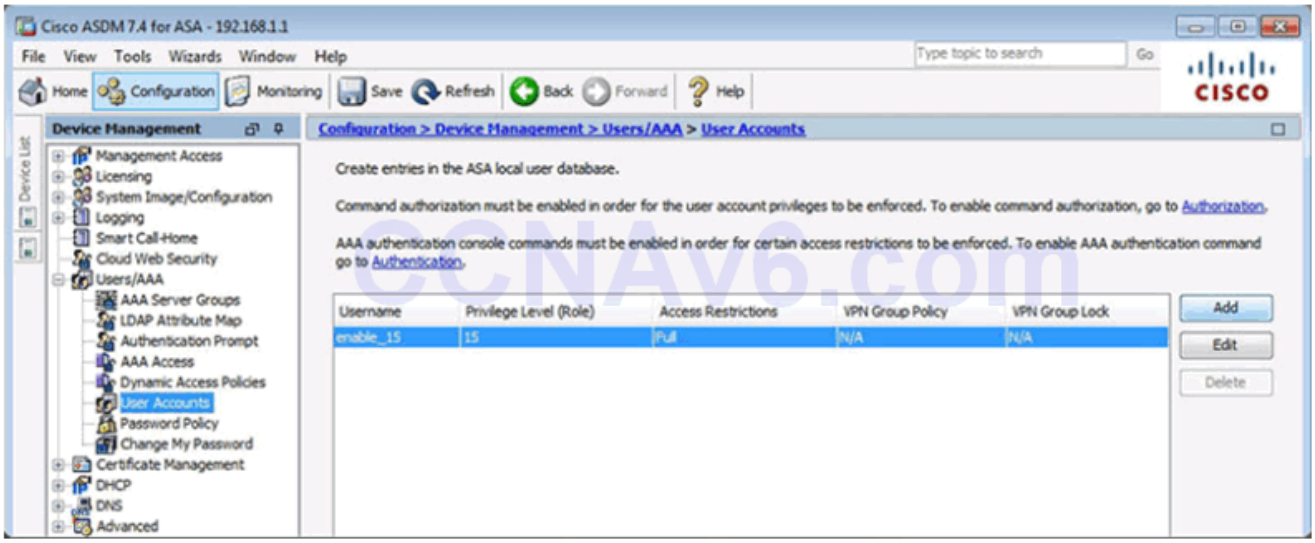


Advanced Static NAT Settings in ASDM

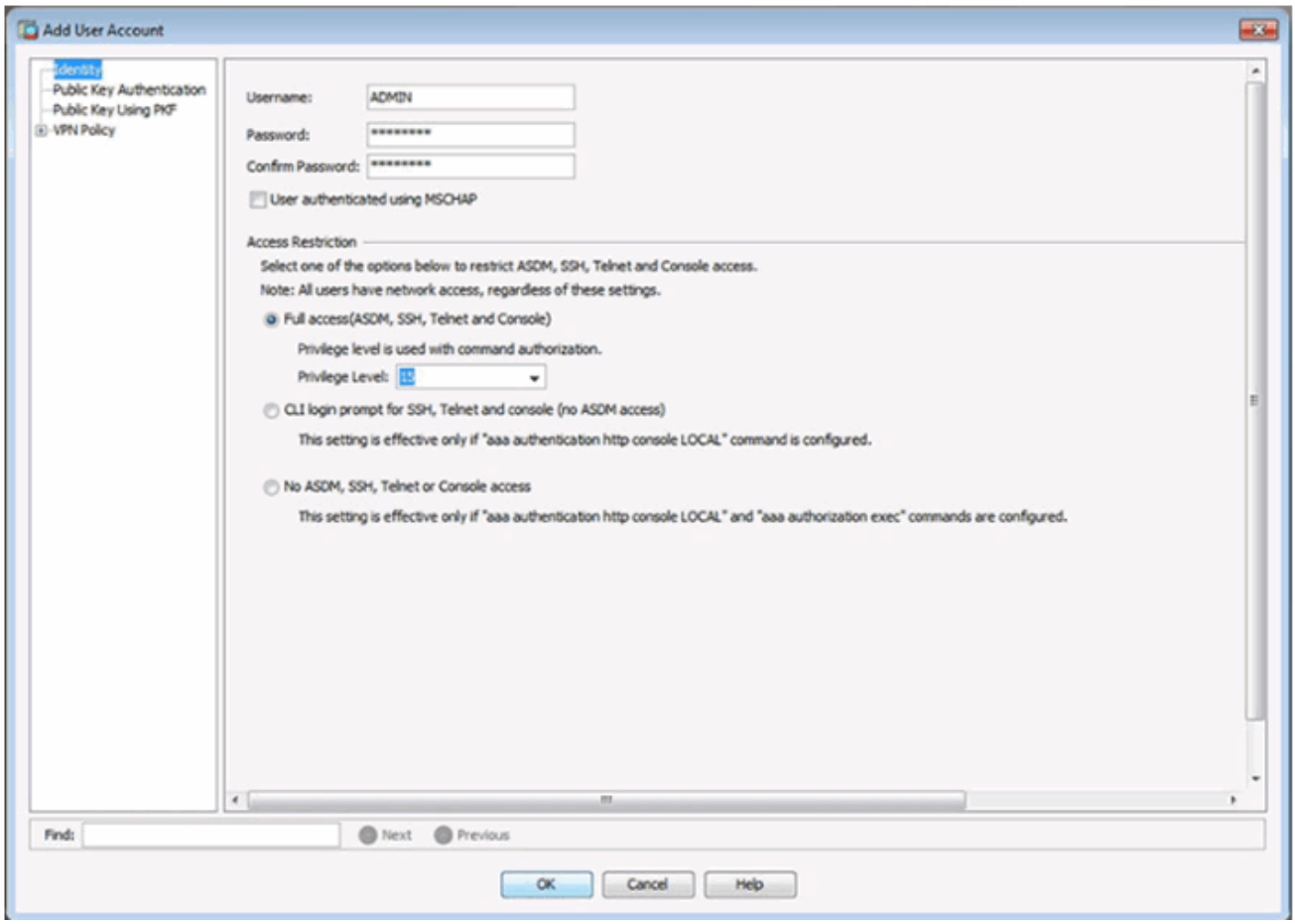


Configuring AAA Authentication

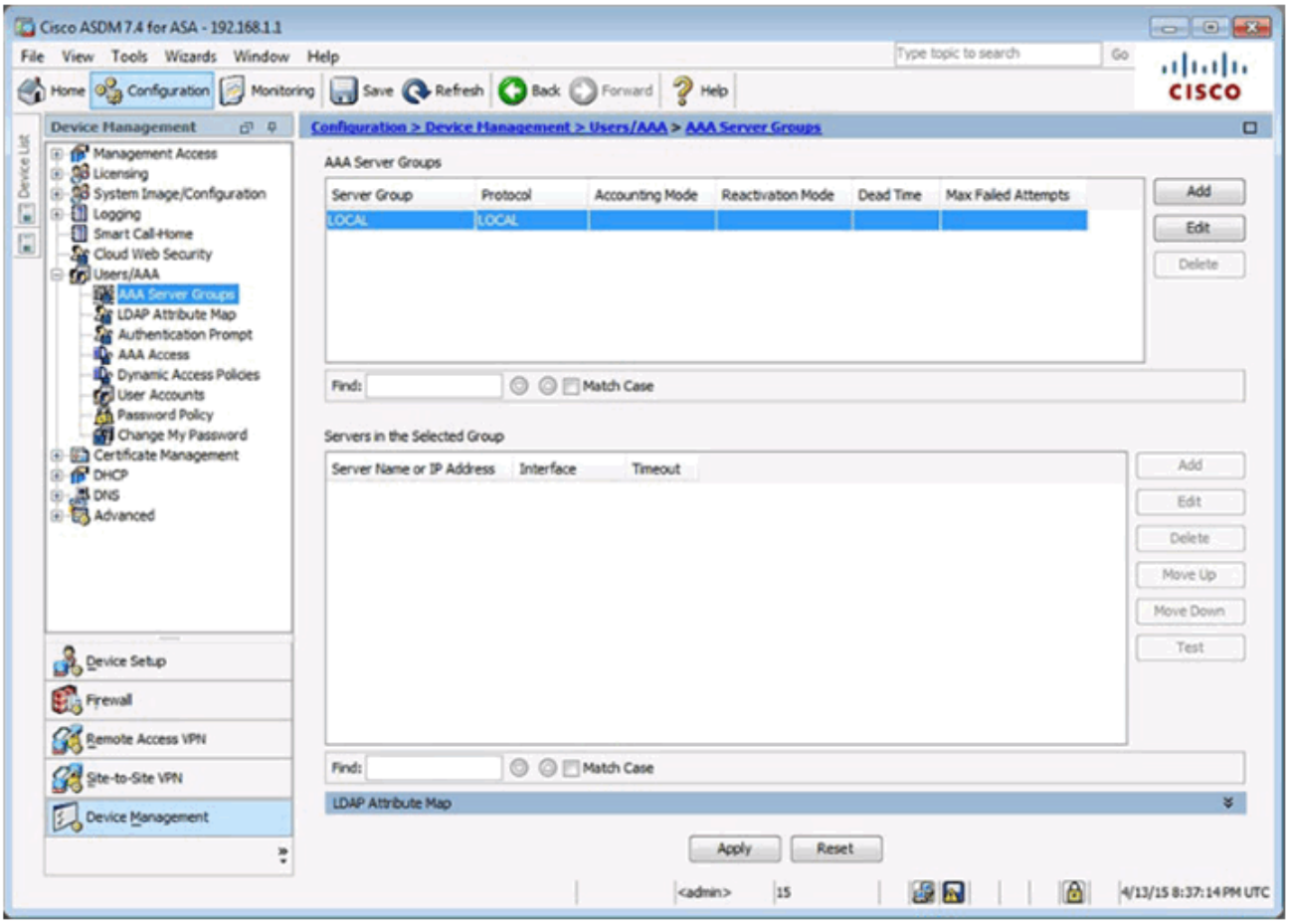
User Accounts Page



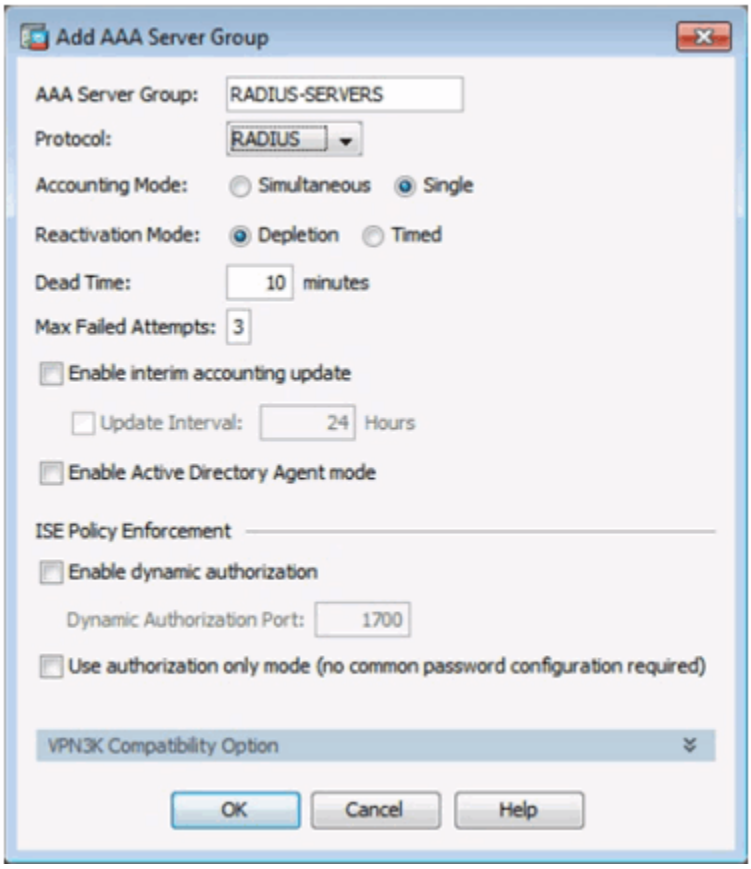
Add User Account Window



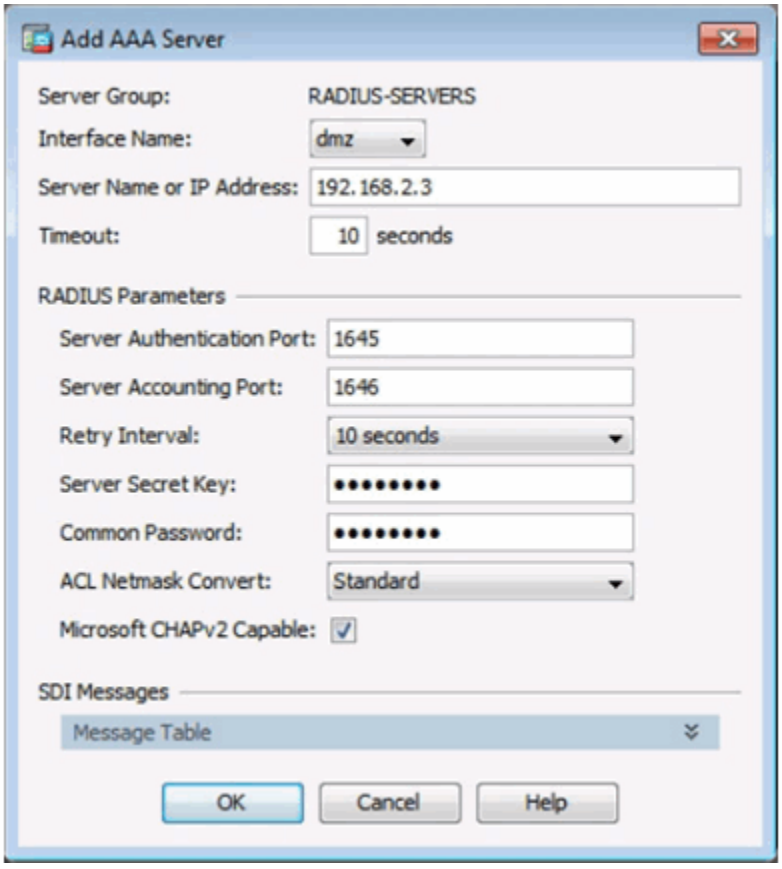
AAA Server Groups Page



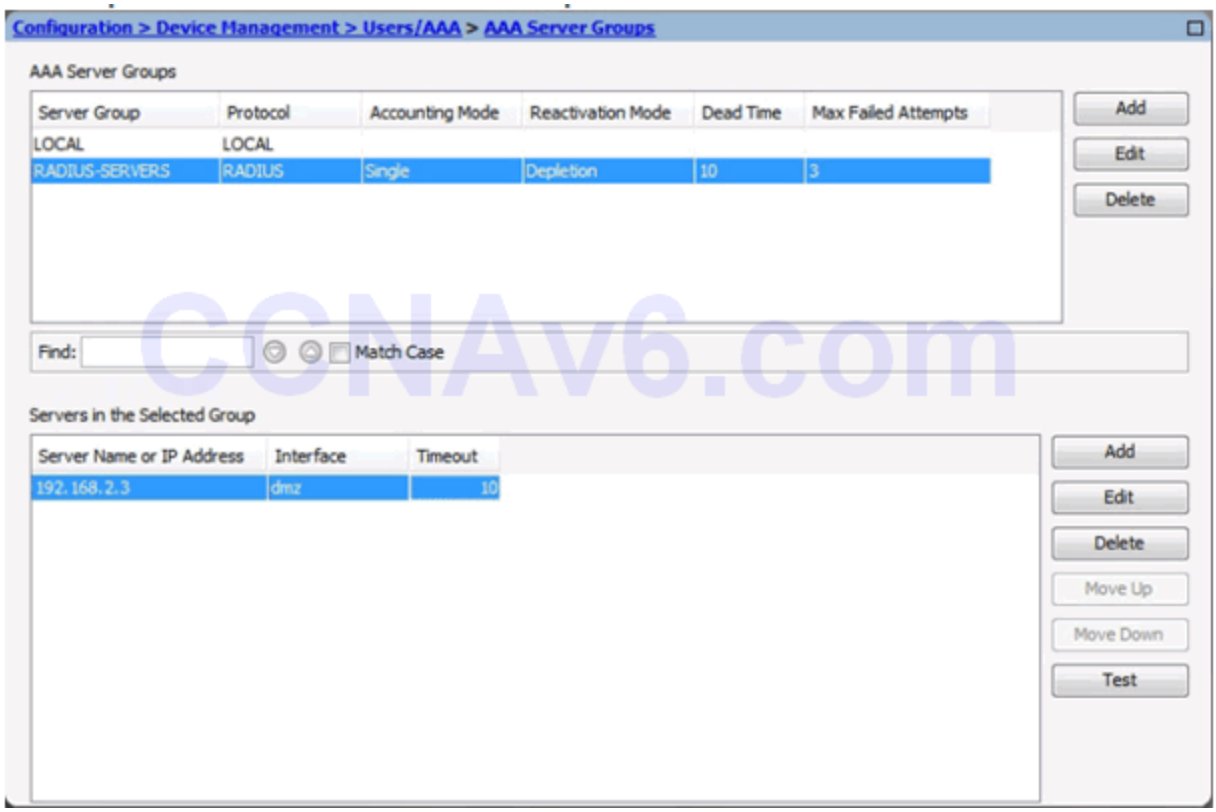
Add AAA Server Group Window



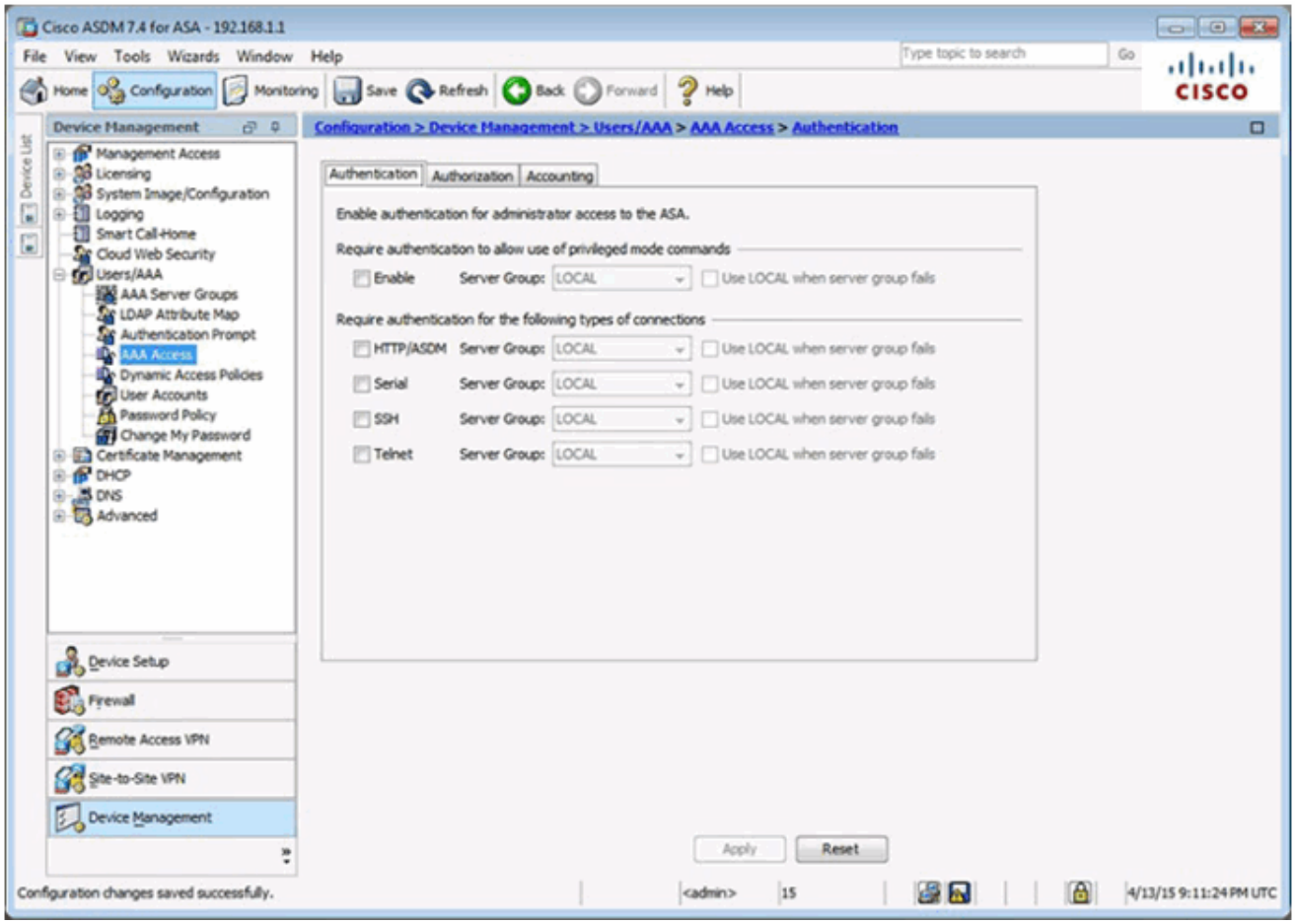
Add AAA Server Window



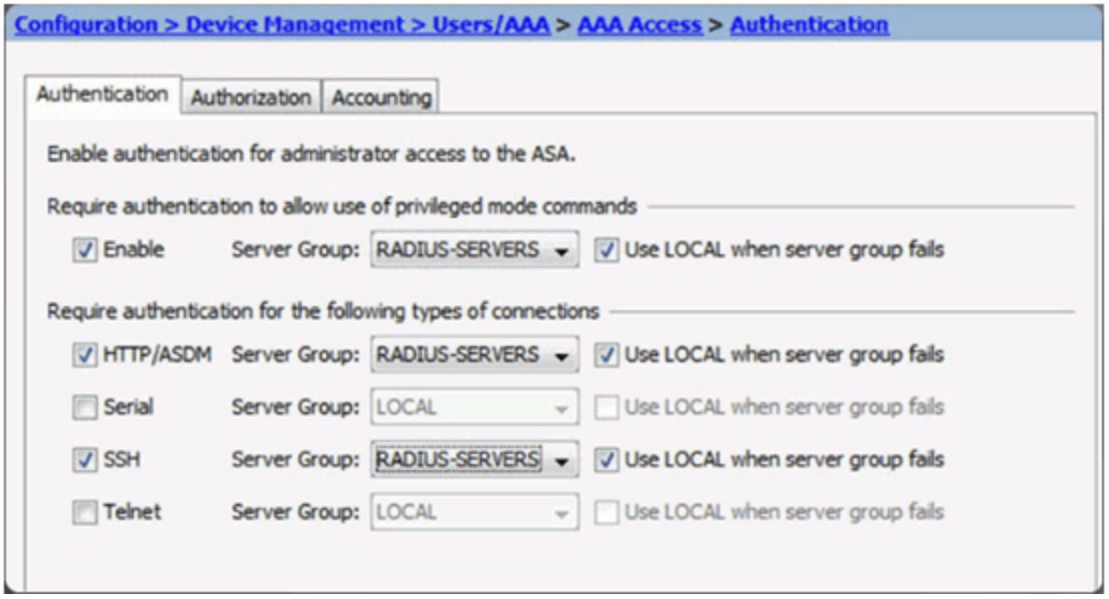
Completed AAA Server Groups Window



AAA Access Page

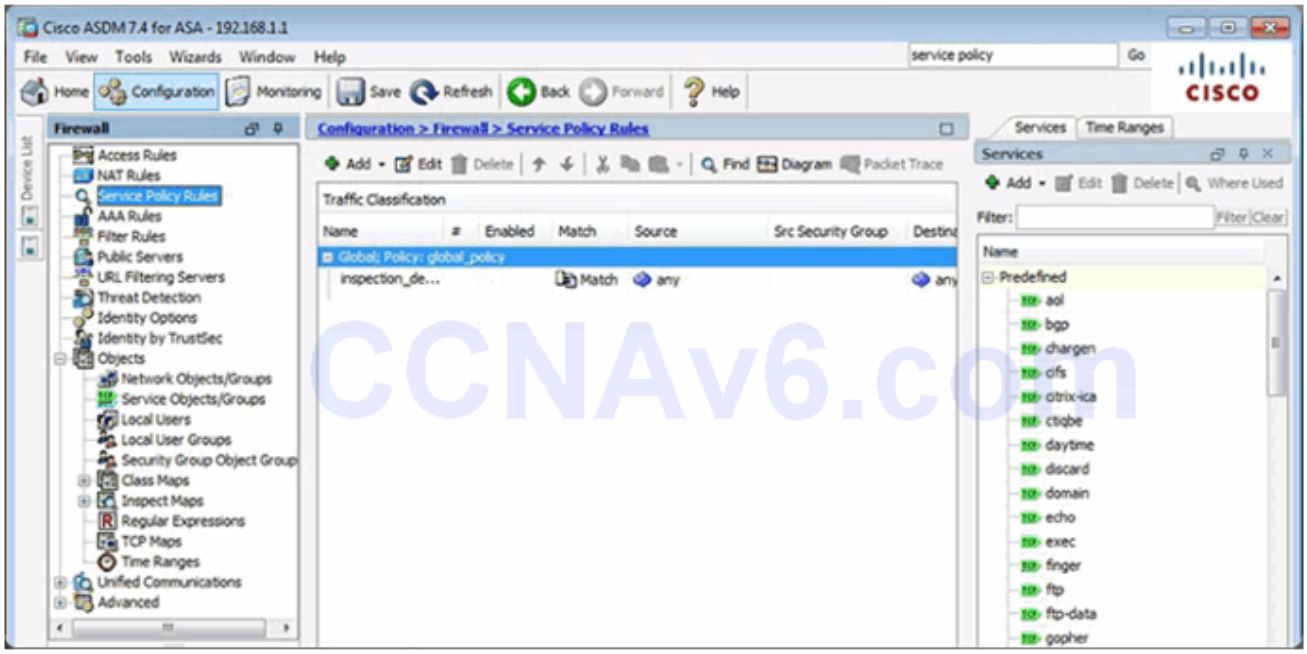


AAA Access > Authentication Window

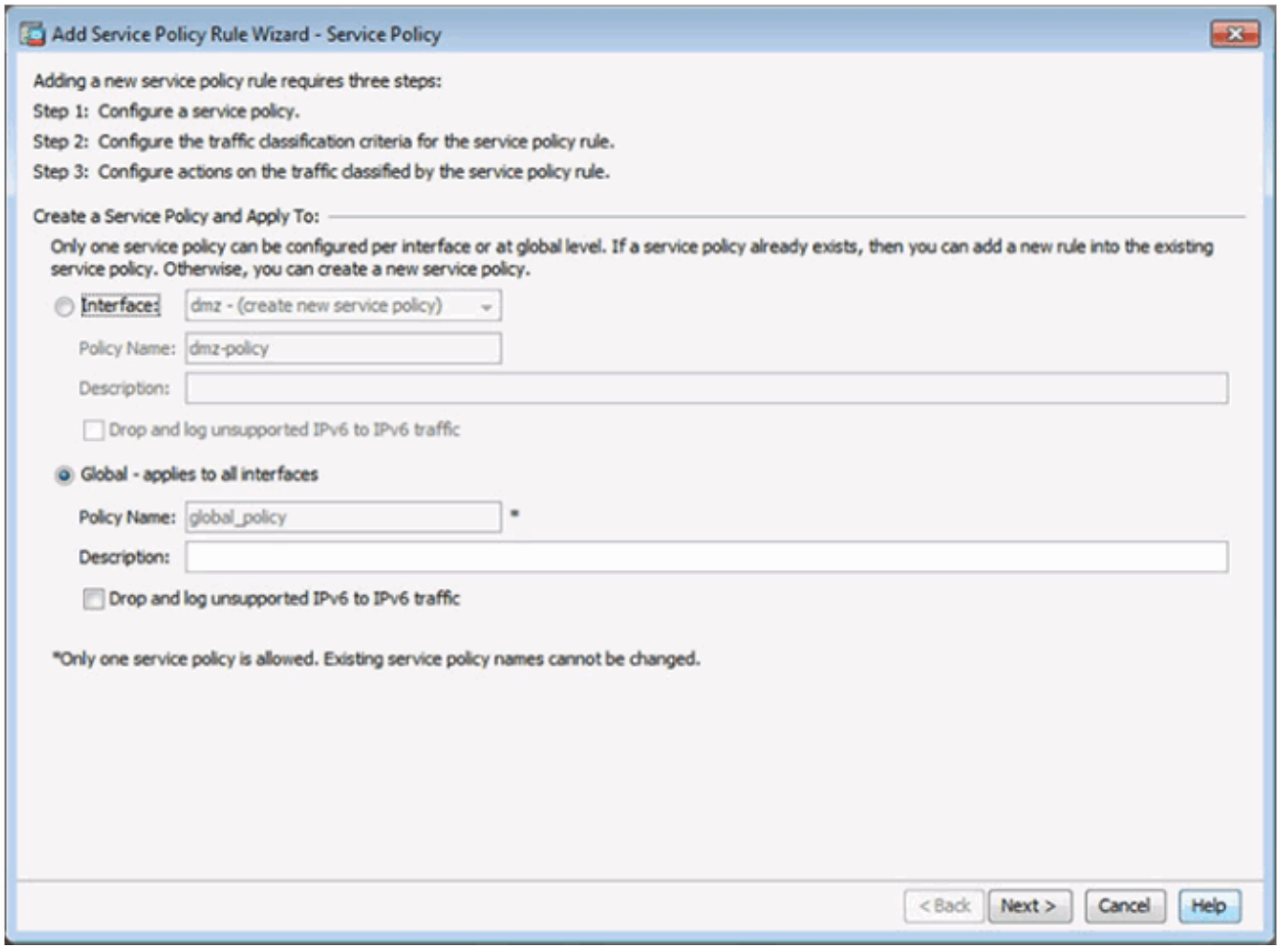


Configuring a Service Policy Using ASDM

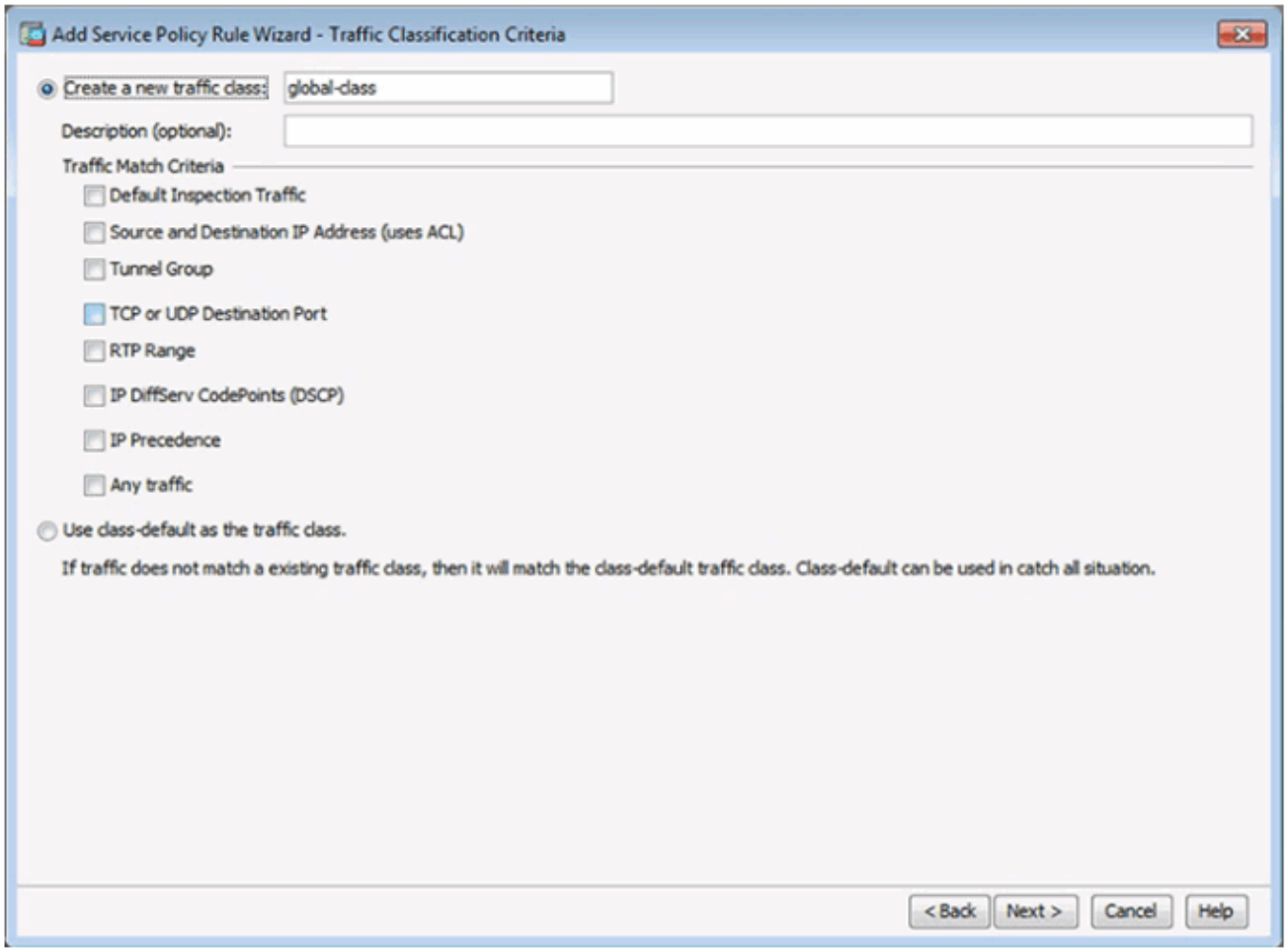
Service Policy in ASDM



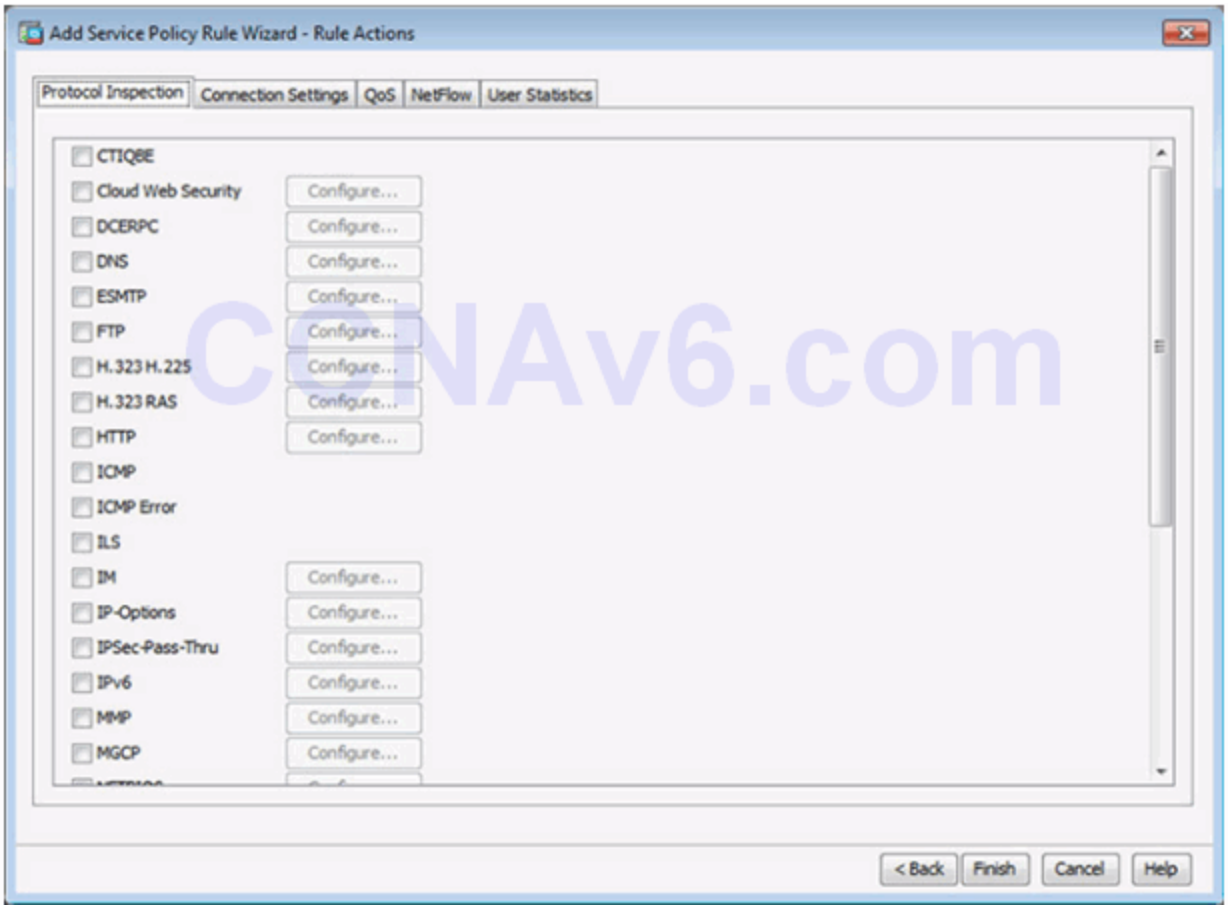
Configure a Service Policy



Configure Traffic Classification Criteria



Configure Actions



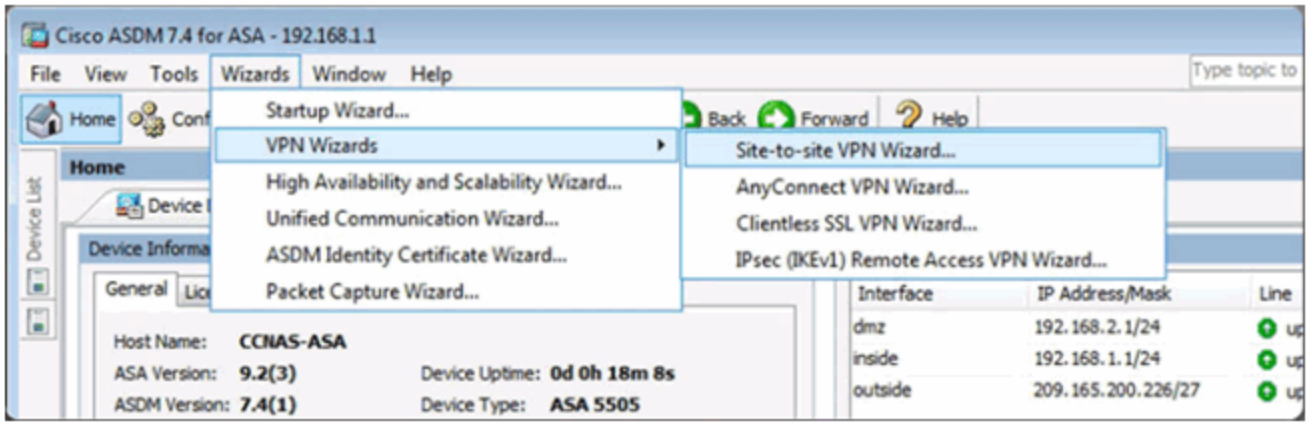
Section 10.2: ASA VPN Configuration

Upon completion of this section, you should be able to:

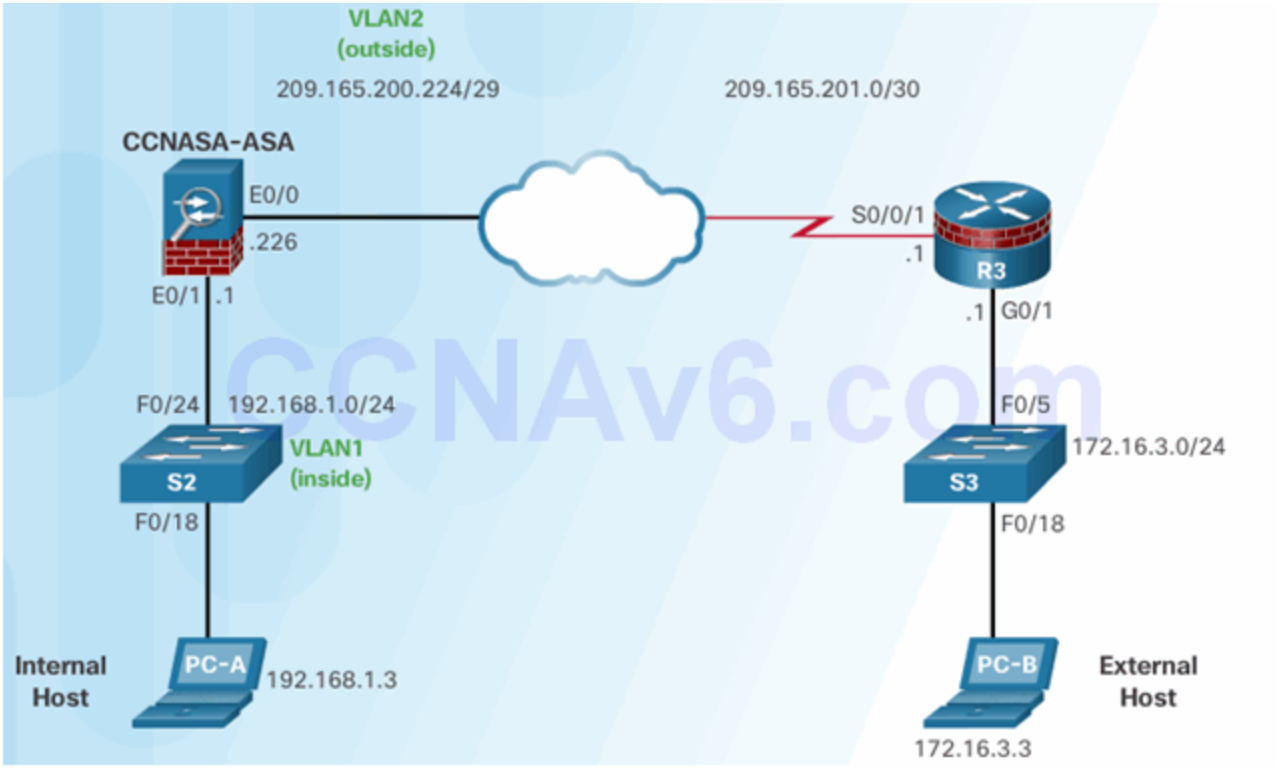
- Explain how the ASA supports site-to-site VPNs.
- Configure remote-access VPNs on an ASA.
- Configure remote-access VPN support using a clientless SSL VPN.
- Configure remote-access VPN support using Cisco AnyConnect.

Topic 10.2.1: Site-to-Site VPNs

ASA Support for Site-to-Site VPNs



ASA Site-to-Site VPNs Using ASDM



Configuring the ISR Site-to-Site VPNs Using the CLI

Basic ISR Configuration

```
R3(config)# interface GigabitEthernet0/1
R3(config-if)# description R3 LAN
R3(config-if)# ip address 172.16.3.1 255.255.255.0
R3(config-if)# exit
R3(config)#
R3(config)# interface Serial0/0/1
R3(config-if)# description WAN Connected to the Internet
R3(config-if)# ip address 209.165.201.1 255.255.255.252
R3(config-if)# exit
R3(config)#
R3(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1
R3(config)#
```

Configure the ISAKMP Policy

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# hash sha
R3(config-isakmp)# group 2
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)#
R3(config-isakmp)# crypto isakmp key SECRET-KEY address 209.165.200.226
R3(config)#
```

Configure the IPsec and VPN ACL

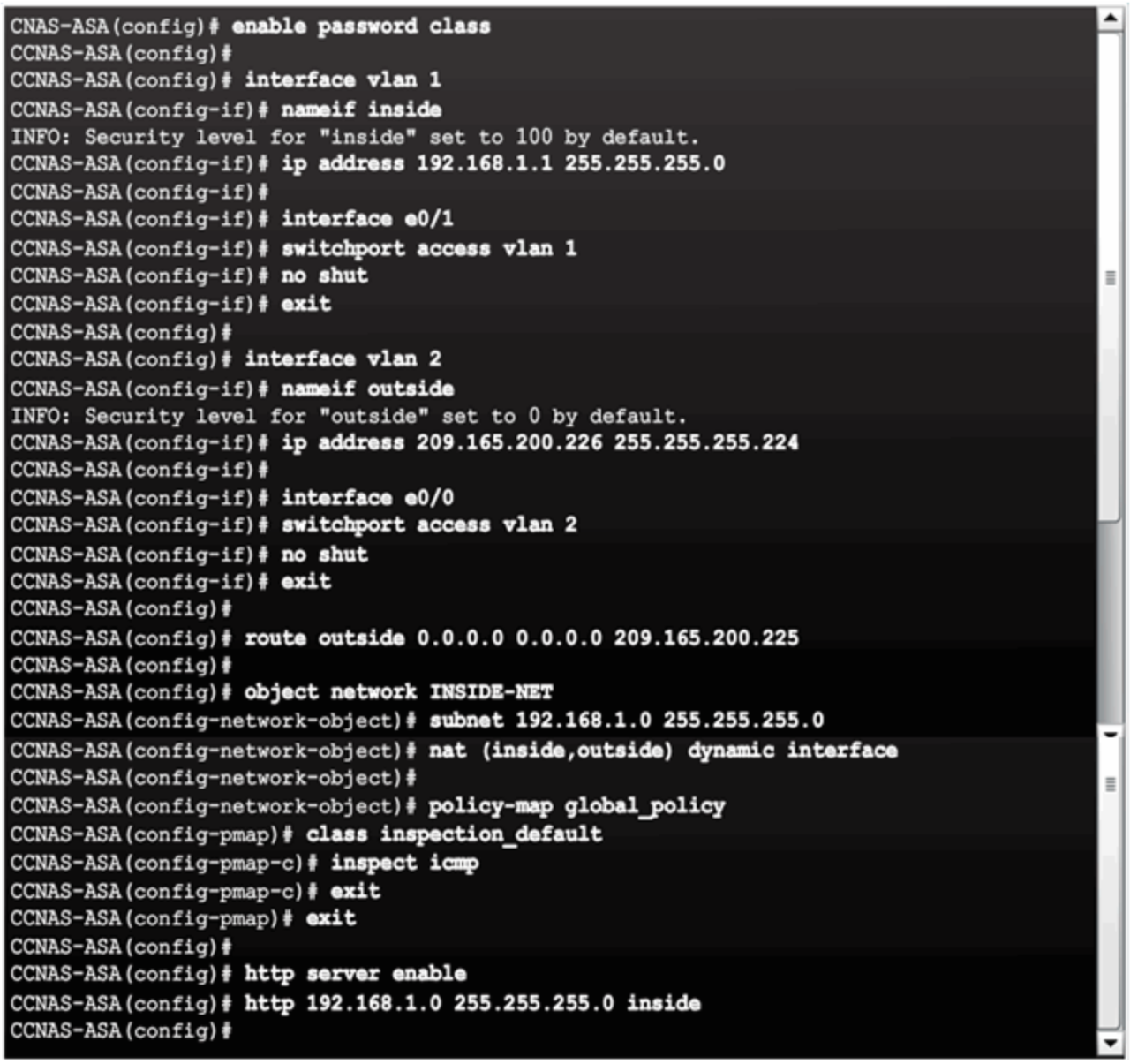
```
R3(config)# crypto ipsec transform-set ESP-TUNNEL esp-3des esp-sha-hmac
R3(cfg-crypto-trans)# mode tunnel
R3(cfg-crypto-trans)# exit
R3(config)#
R3(config)# ip access-list extended VPN-ACL
R3(config-ext-nacl)# remark VPN ACL defining interesting traffic
R3(config-ext-nacl)# permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config-ext-nacl)# exit
R3(config)#
```

Configure and Apply the Crypto Map

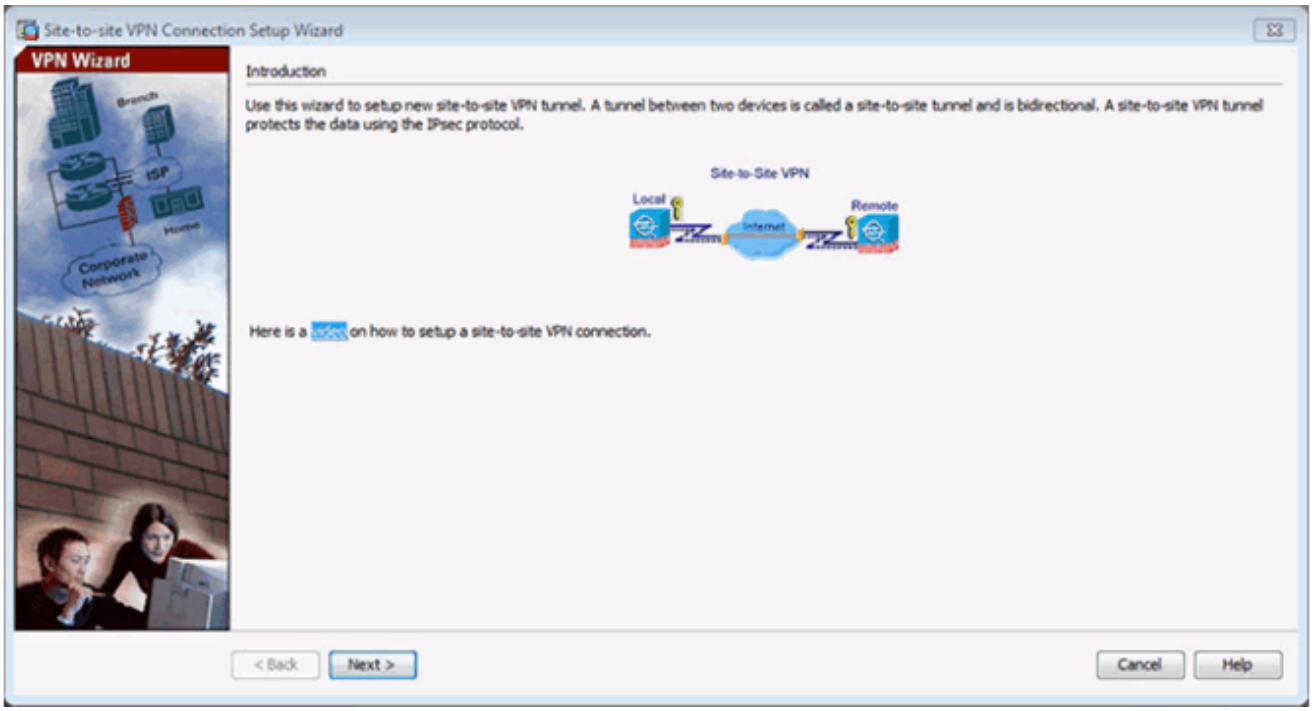
```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)# set peer 209.165.200.226
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# match address VPN-ACL
R3(config-crypto-map)# exit
R3(config)#
R3(config)# interface Serial0/0/1
R3(config-if)# crypto map S2S-MAP
R3(config-if)#
```

Configuring the ASA Site-to-Site VPNs Using ASDM

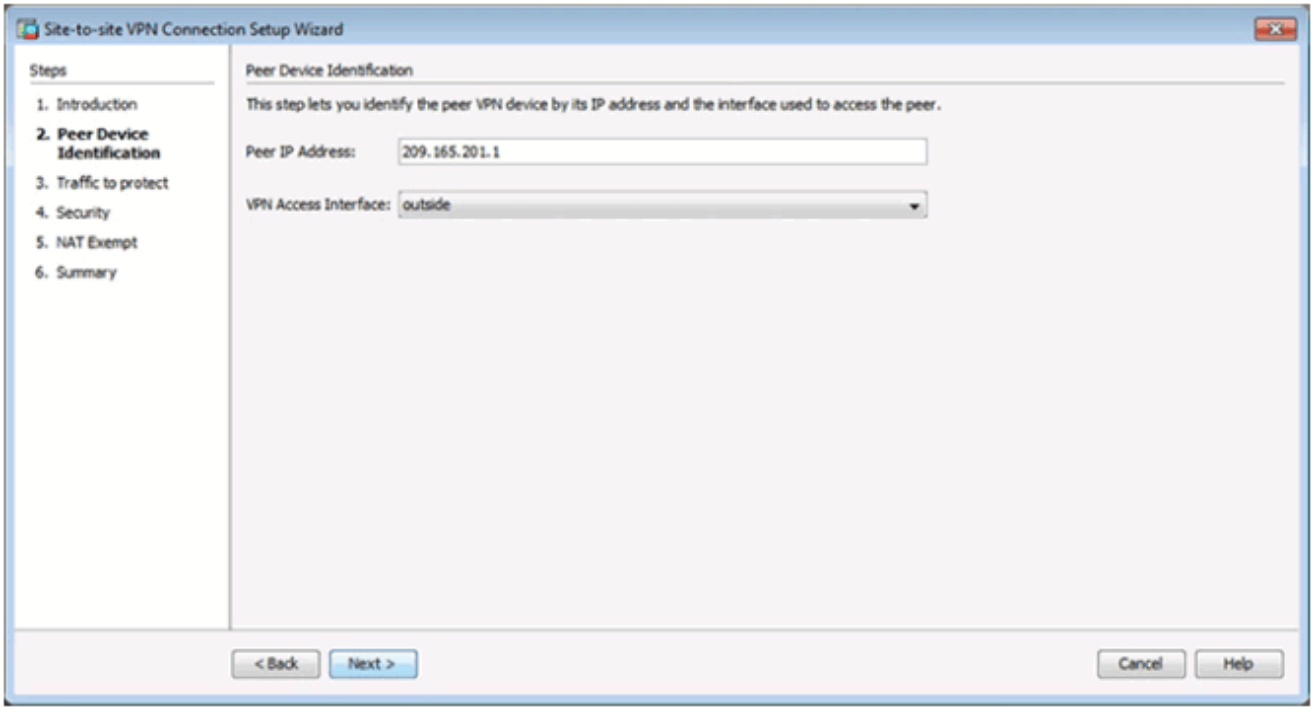
Basic ISR Configuration



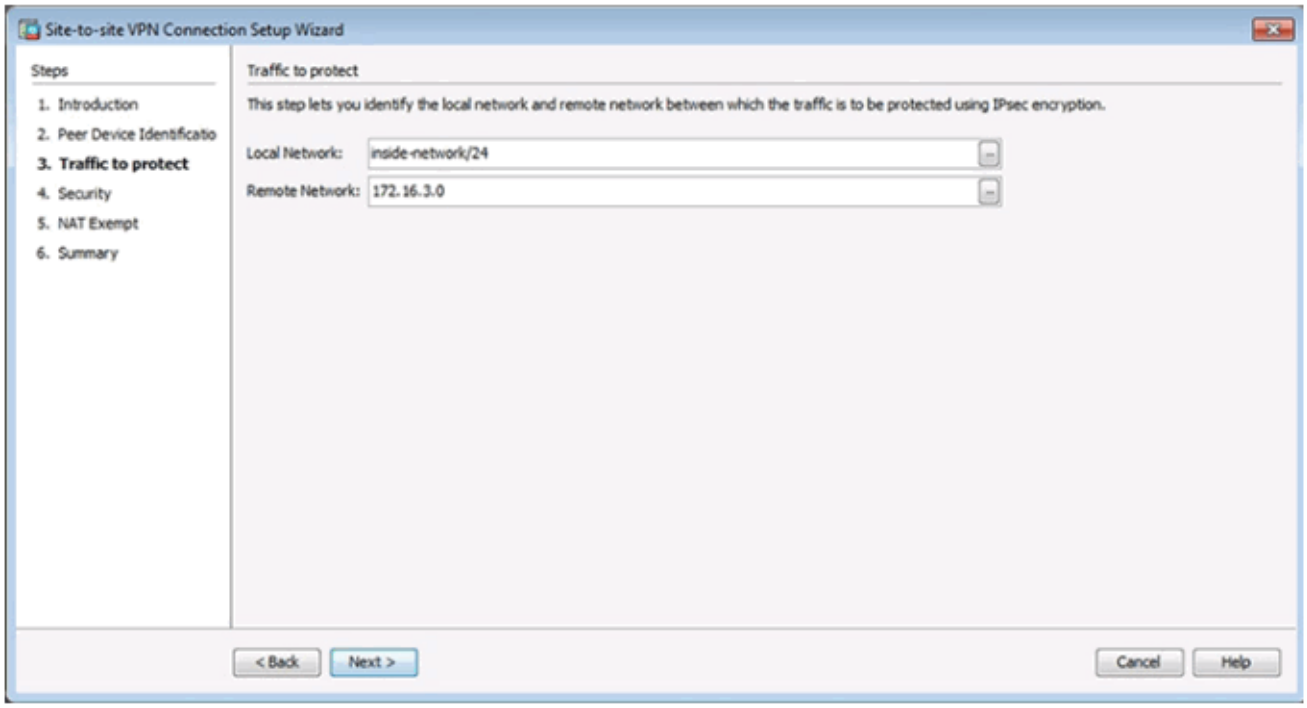
Introduction Window



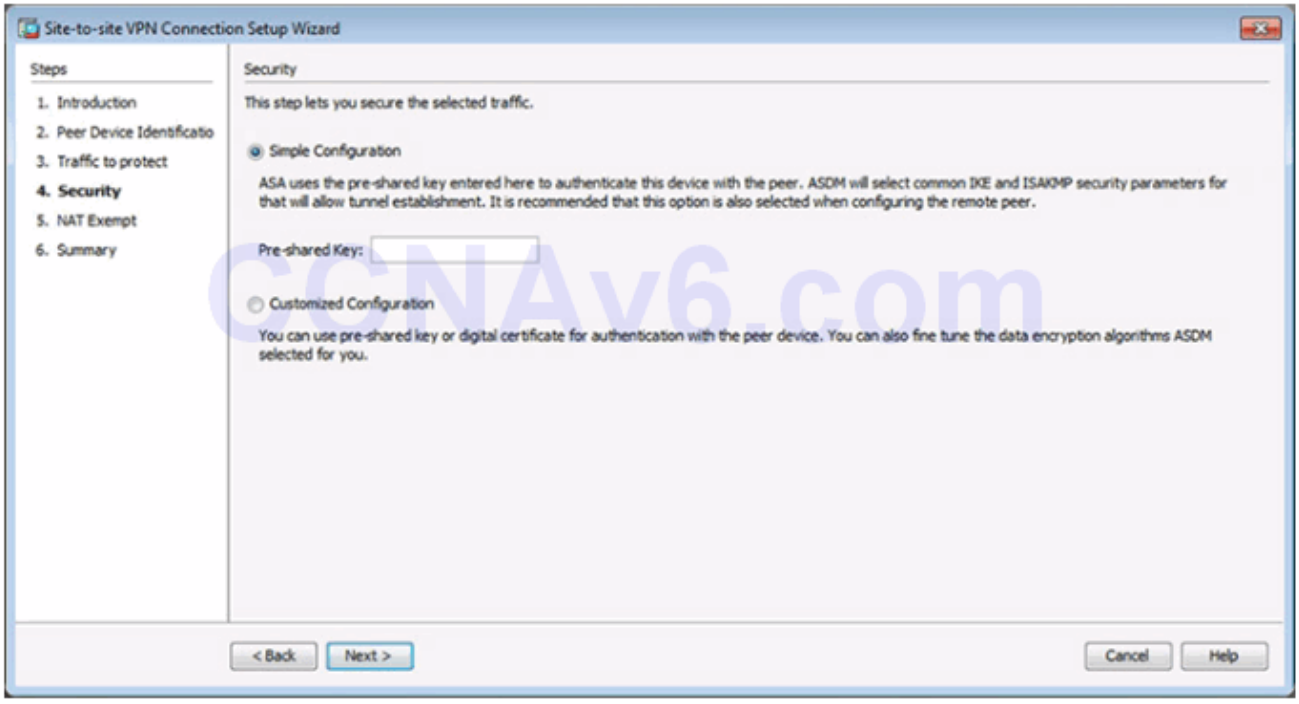
Peer Device Identification Window



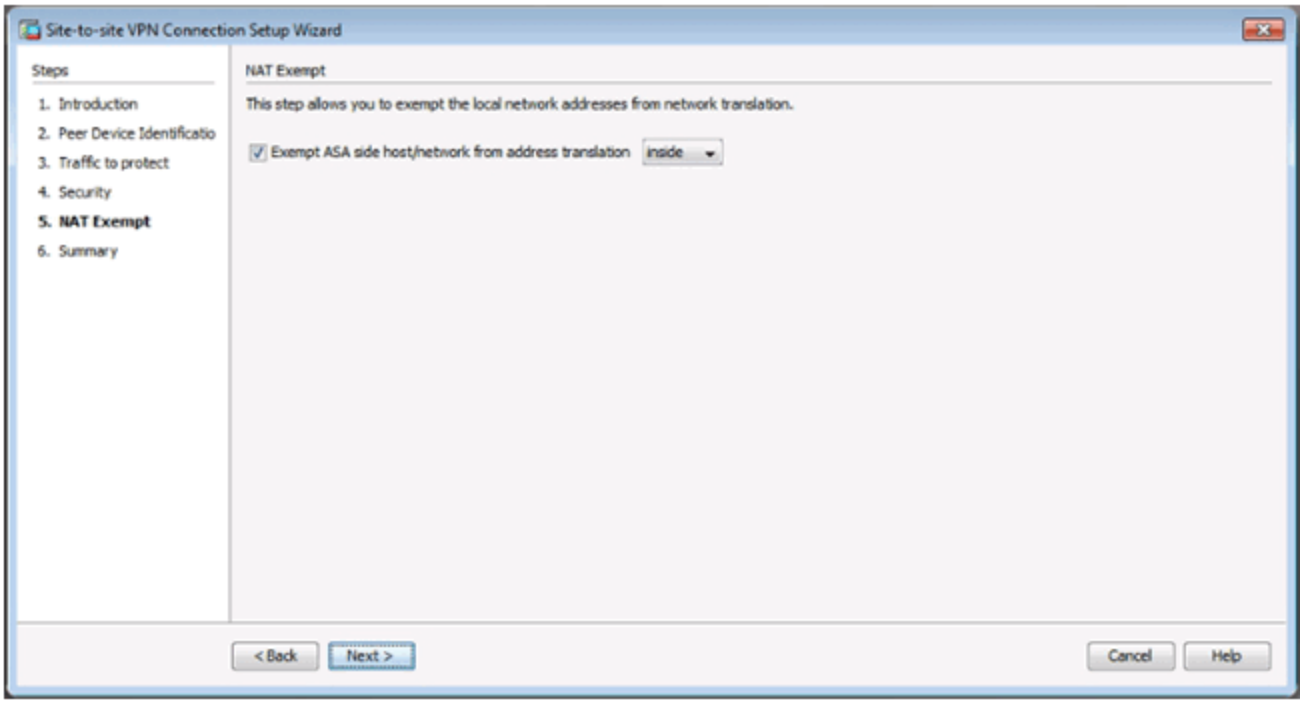
Traffic to Protect Window



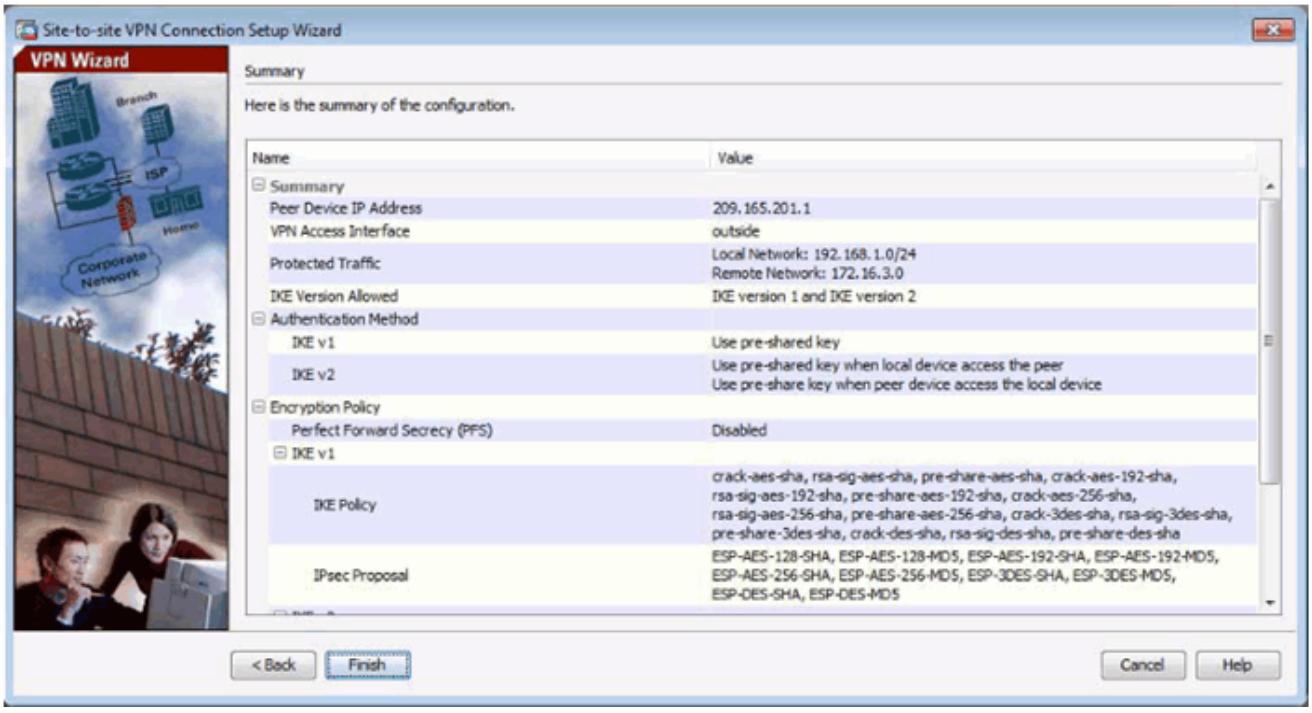
Security Window



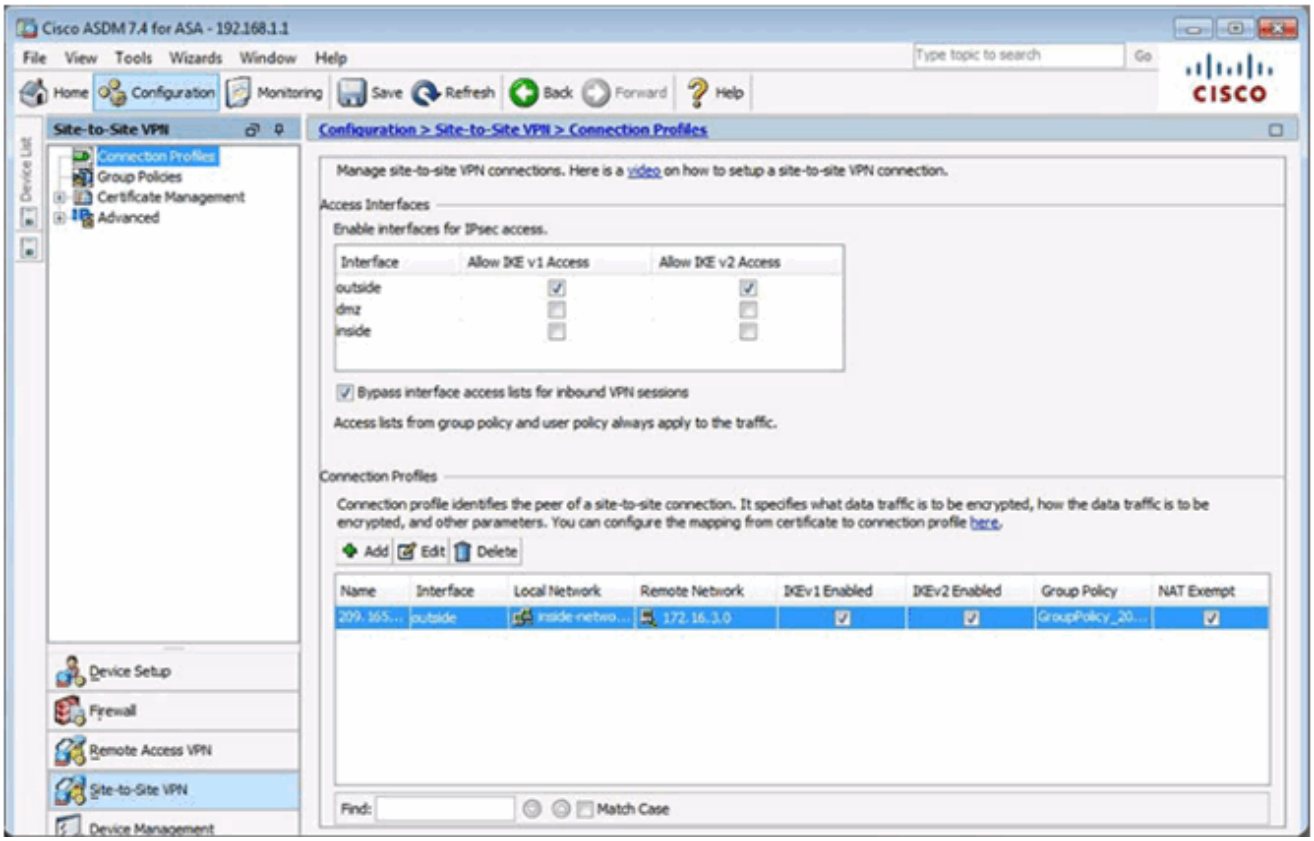
NAT Exempt Window



Summary Window

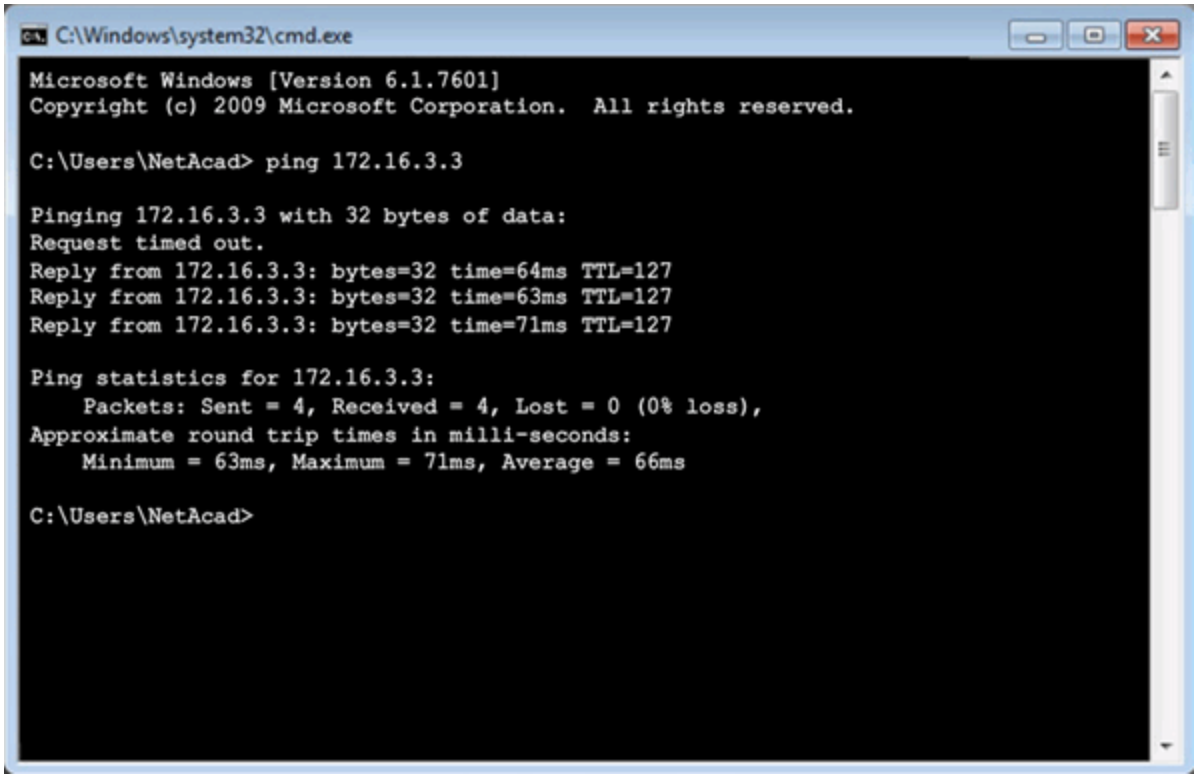


Verifying Site-to-Site VPNs Using ASDM

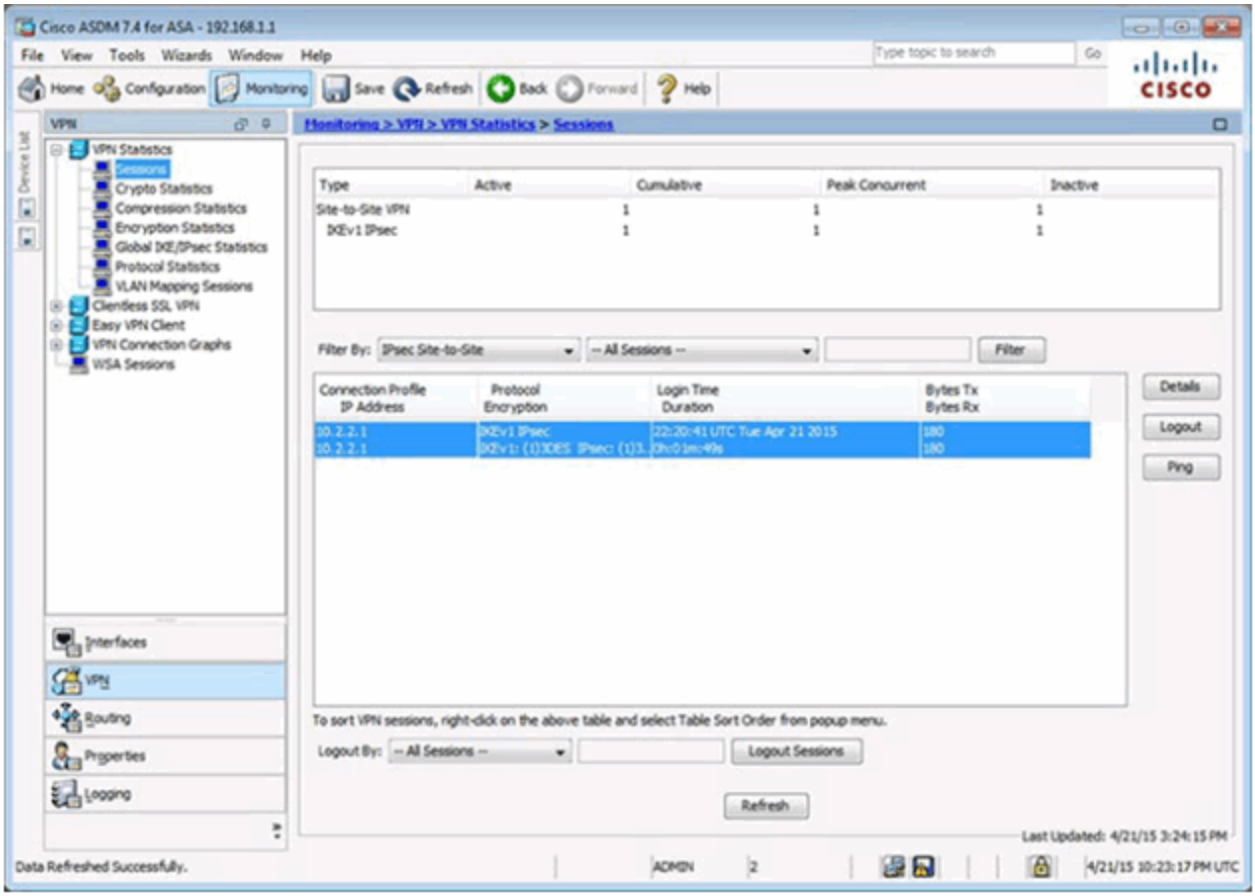


Test the Site-to-Site VPNs Using ASDM

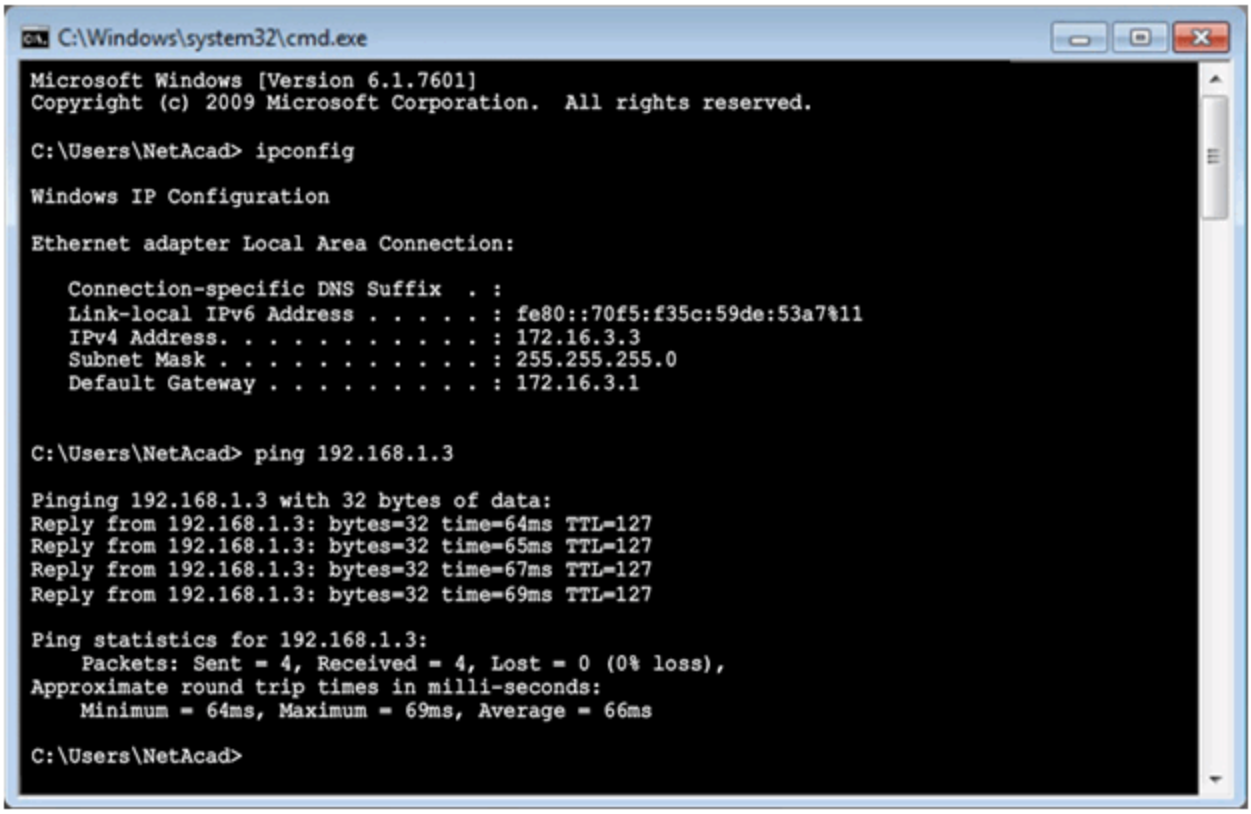
Establish the VPN Tunnel Connection to the Remote Network



Monitoring the VPN Tunnel

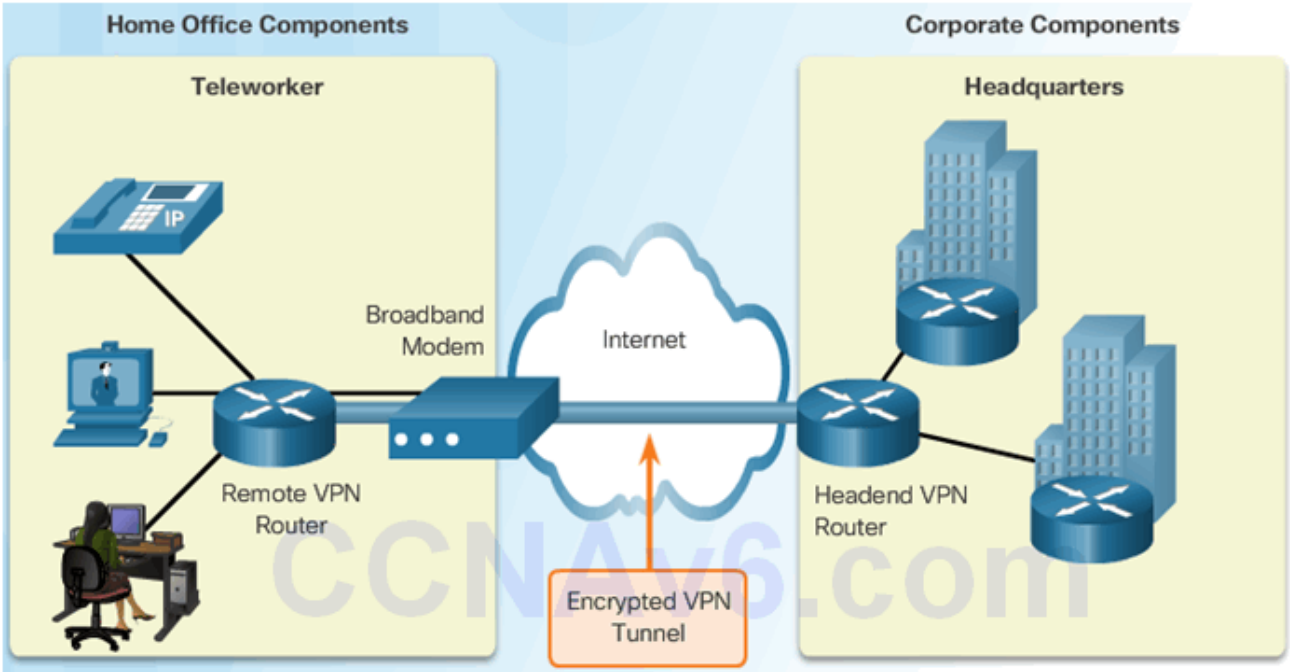


Verify VPN Tunnel Connectivity from the External Host

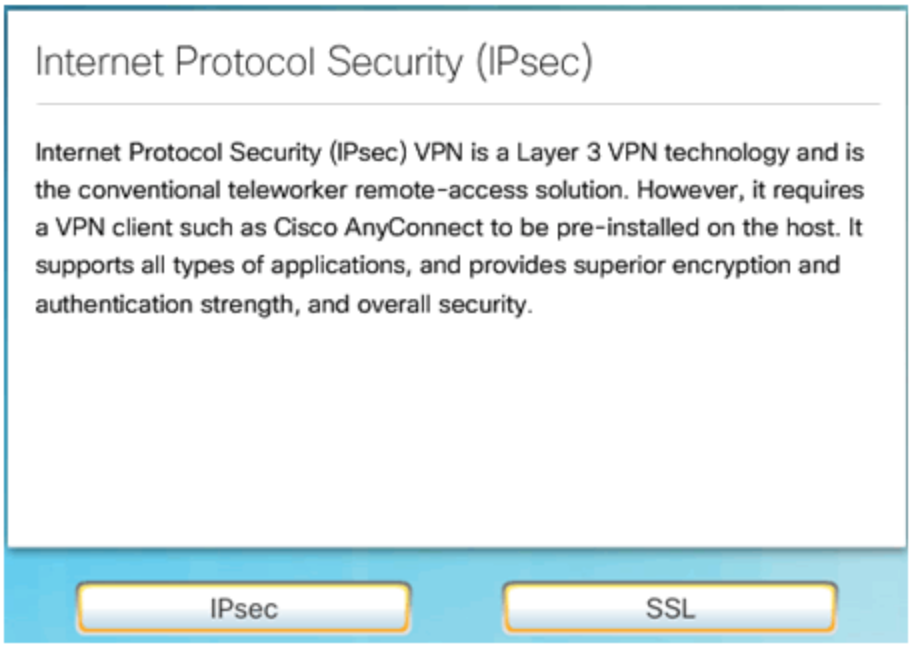


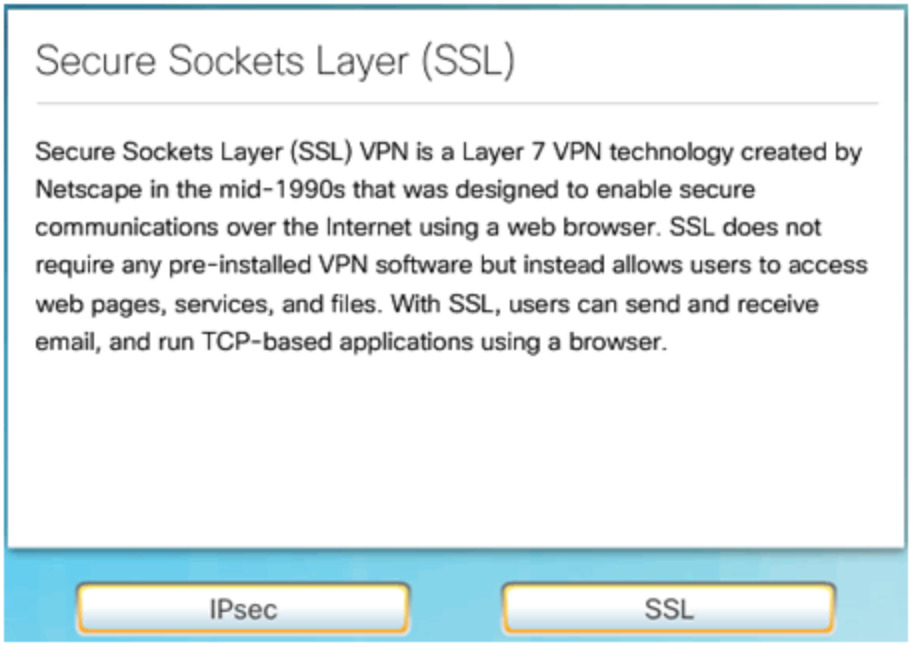
Topic 10.2.2: Remote-Access VPNs

Remote-Access VPN Options



IPsec Versus SSL



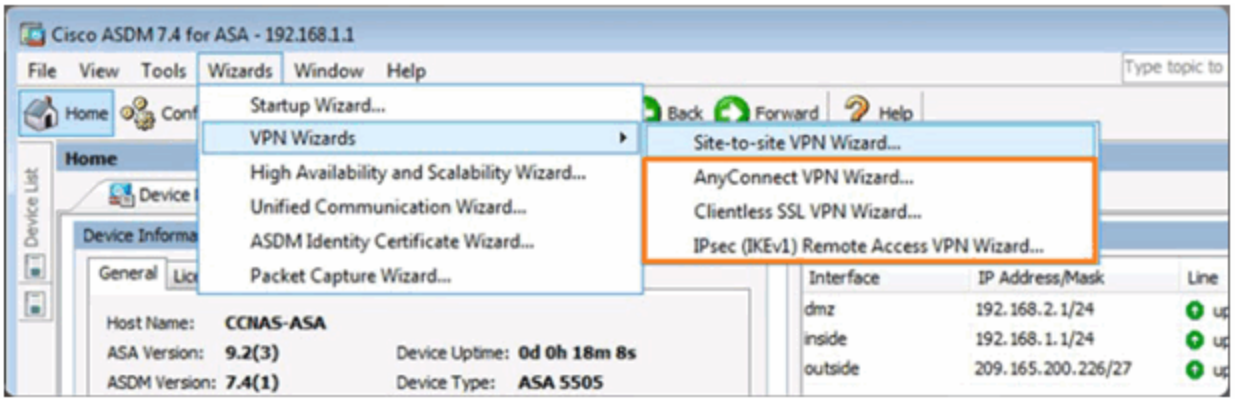


Comparing IPsec and SSL

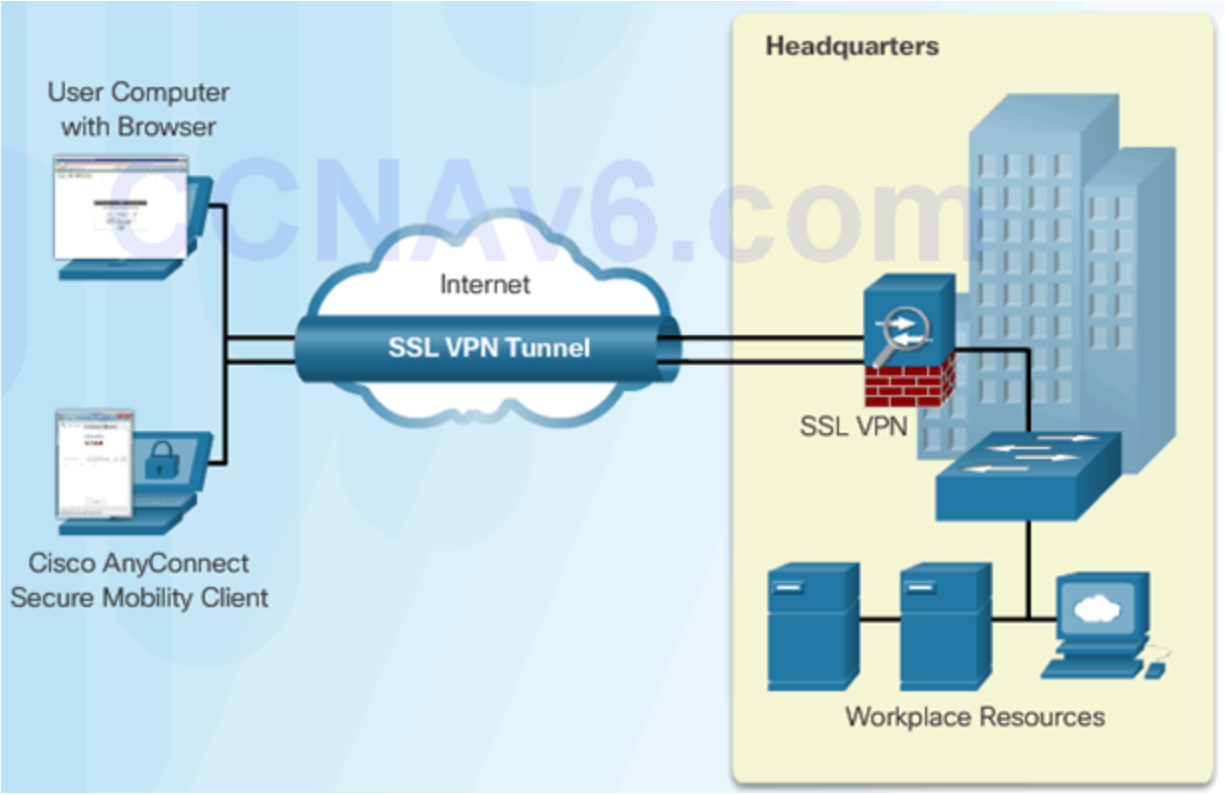
	IPSec	SSL
Applications supported	**Extensive**- all IP-based applications are supported.	**Limited**- only web-based applications and file sharing are supported.
Authentication strength	**Strong**- using two-way authentication with shared keys or digital certificates.	**Moderate**- using one-way or two-way authentication.
Encryption strength	**Strong**- with key lengths from 56 bits to 256 bits.	**Moderate to strong**- with key lengths from 40 bits to 256 bits.
Connection complexity	**Medium**- because it requires a VPN client pre-installed on a host.	**Low**- it only requires a web browser on a host.
Connection option	**Limited**- only specific devices with specific configurations can connect.	**Extensive**- any device with a web browser can connect.

ASA SSL VPNs

Remote Access VPN Wizards

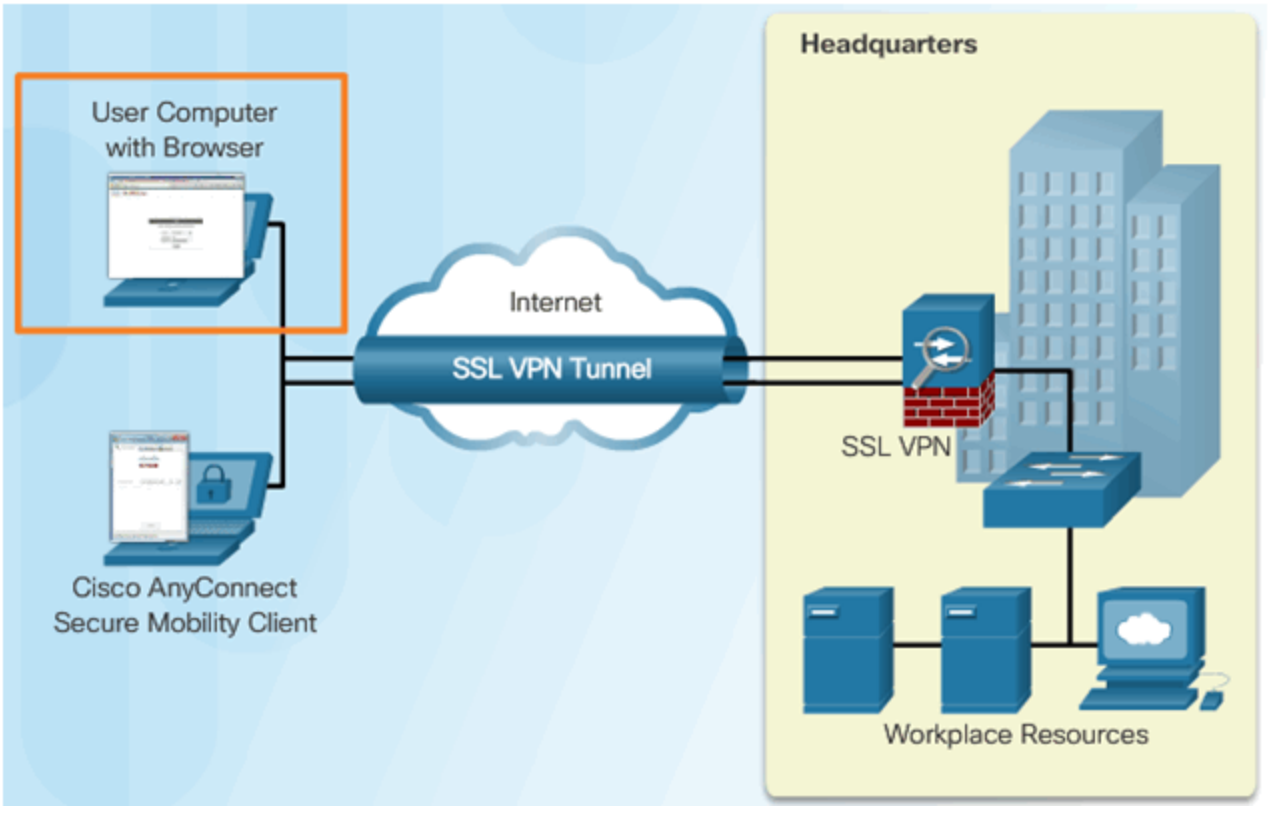


Cisco ASA SSL Remote Access VPN Solutions

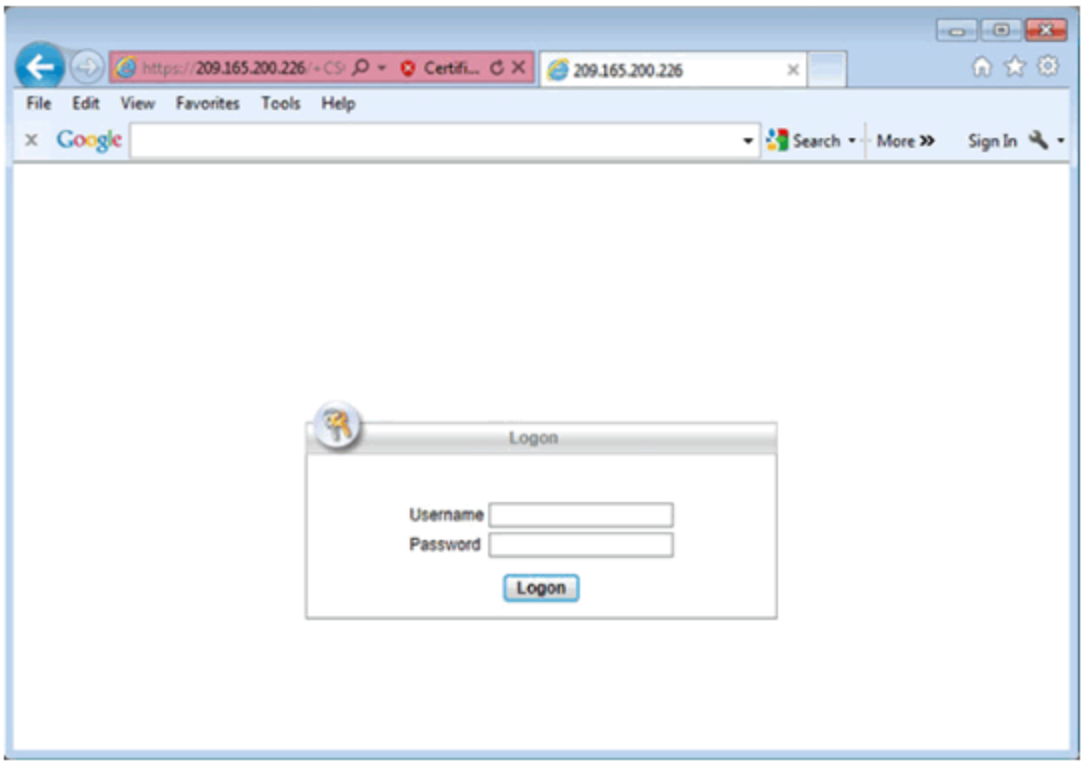


Clientless SSL VPN Solution

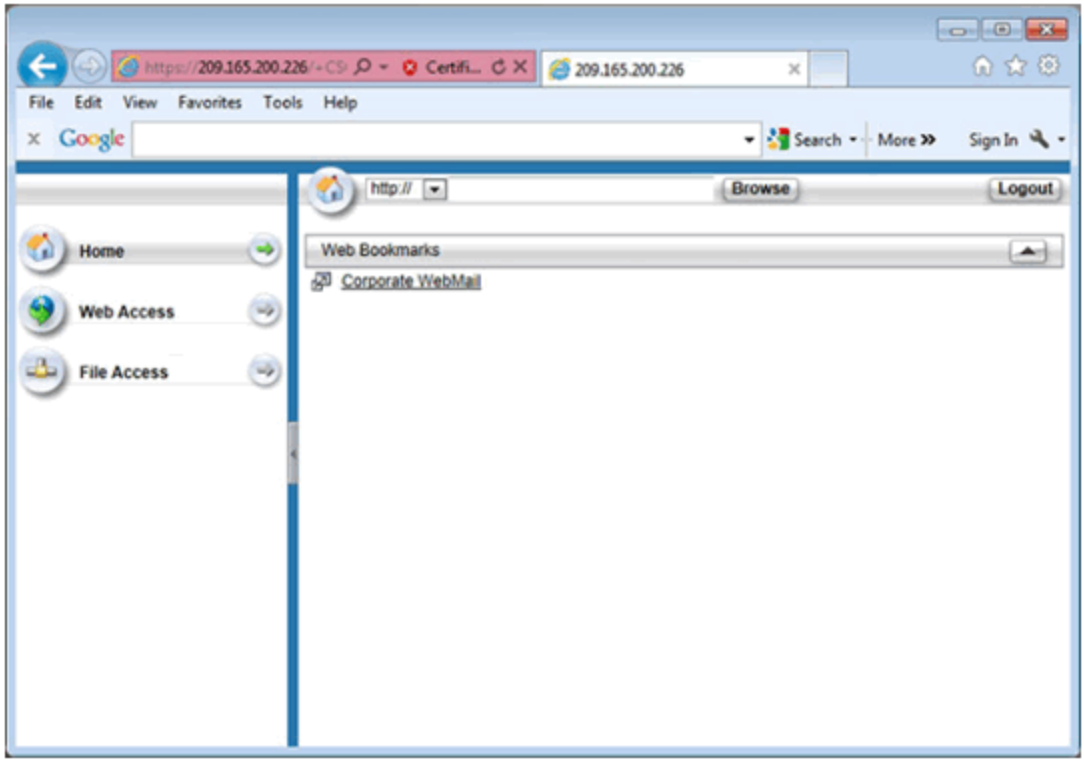
Cisco ASA Clientless SSL VPN Deployment



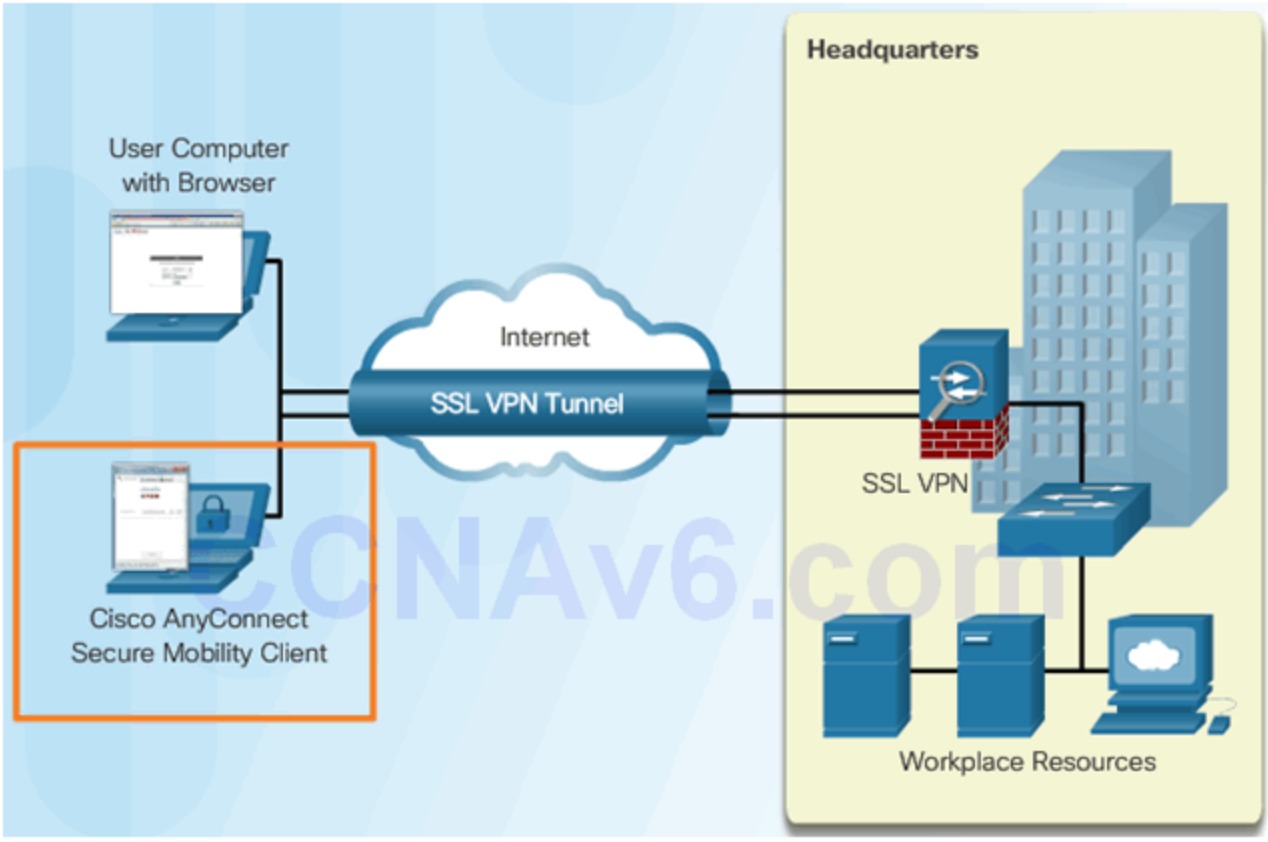
Clientless Login Web page



Web Portal Home Page

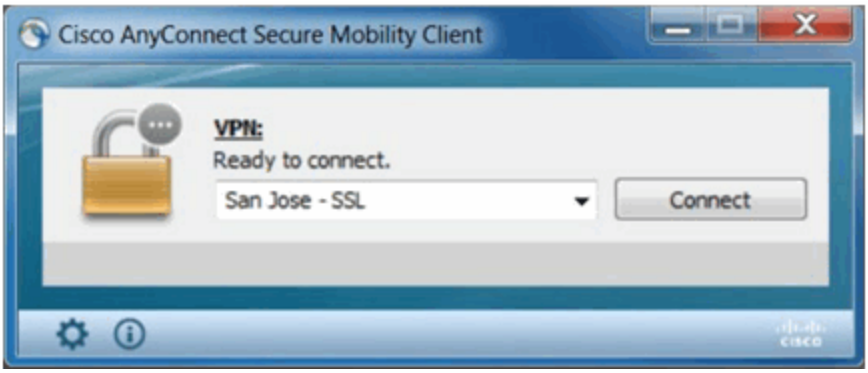


Client-Based SSL VPN Solution

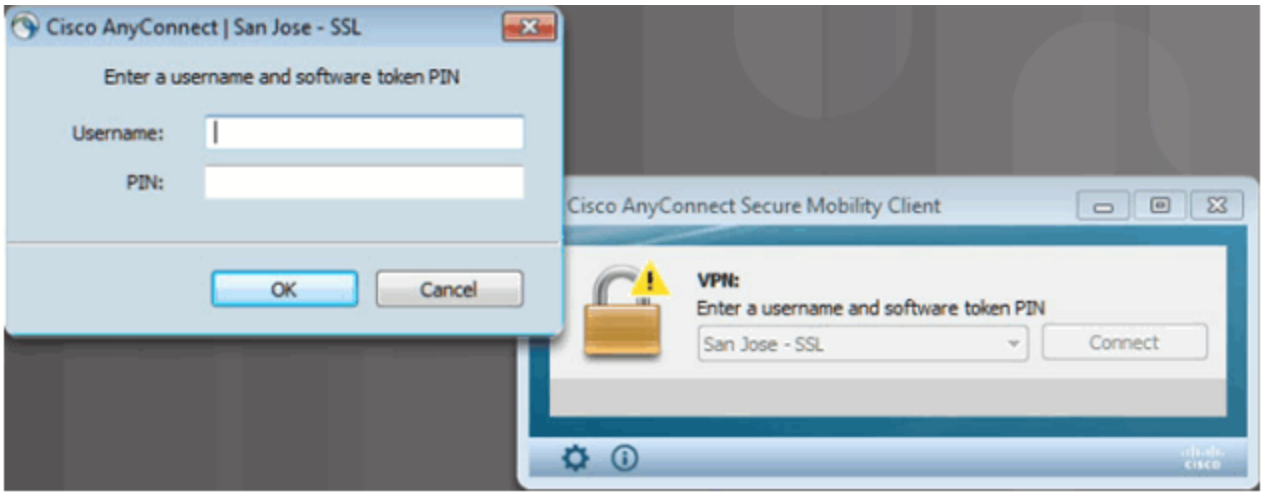


Cisco AnyConnect Secure Mobility Client

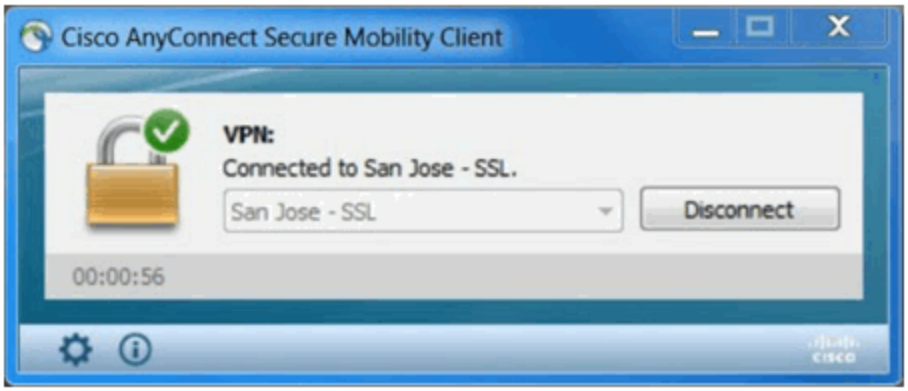
AnyConnect Connection Window



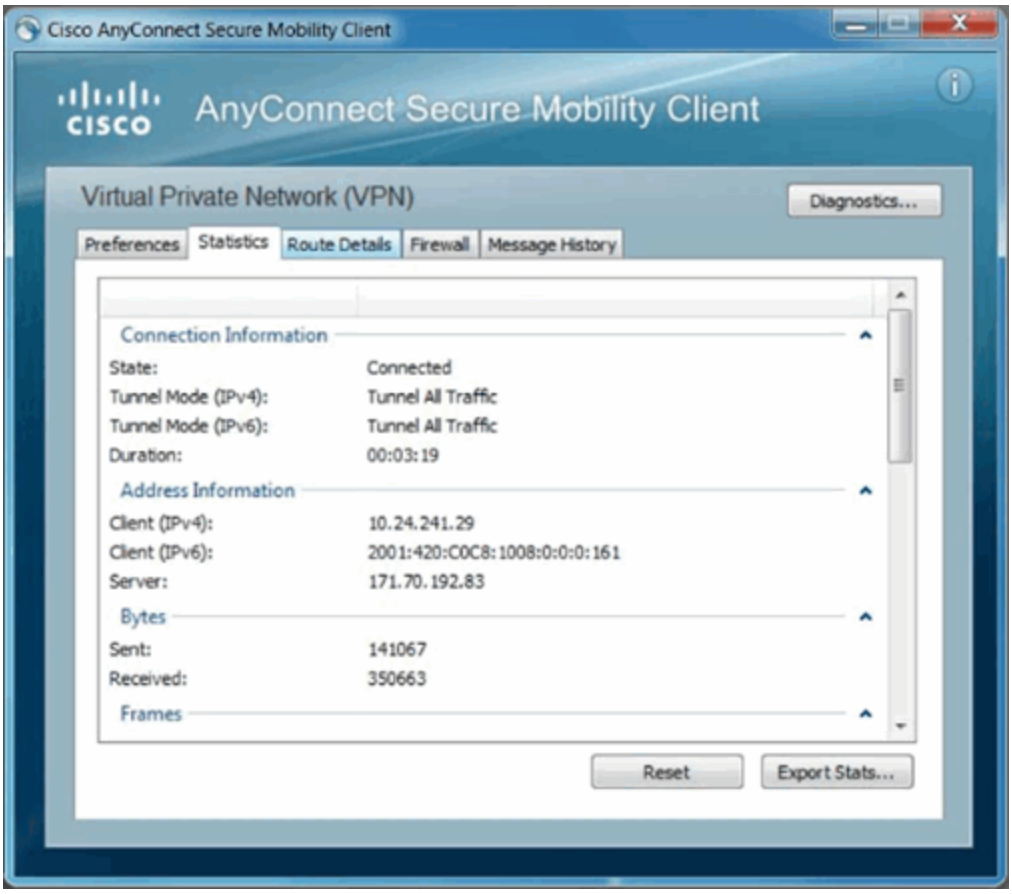
AnyConnect Authenticate Window



AnyConnect Authenticated Window



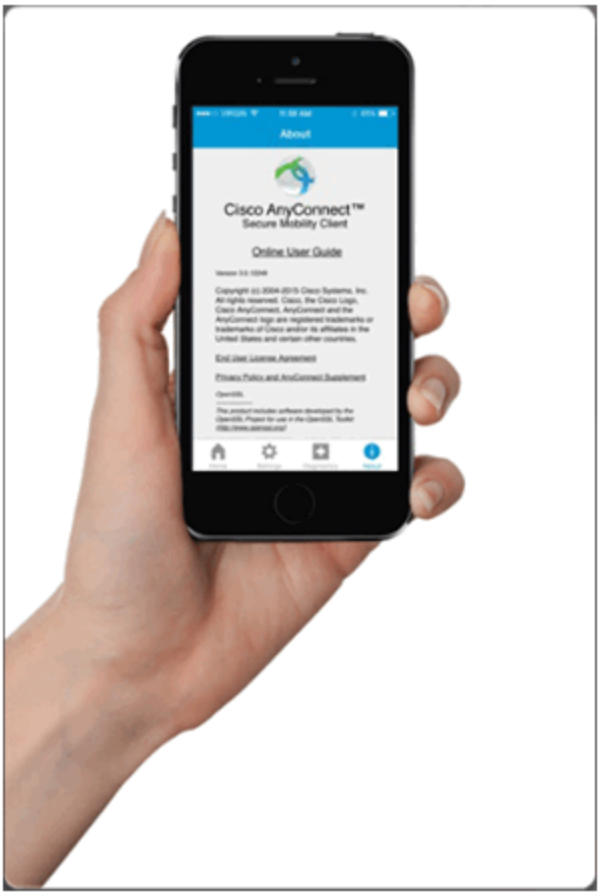
AnyConnect Statistics Window



AnyConnect for Mobile Devices

Cisco AnyConnect Secure Mobility Client is available on the following platforms:

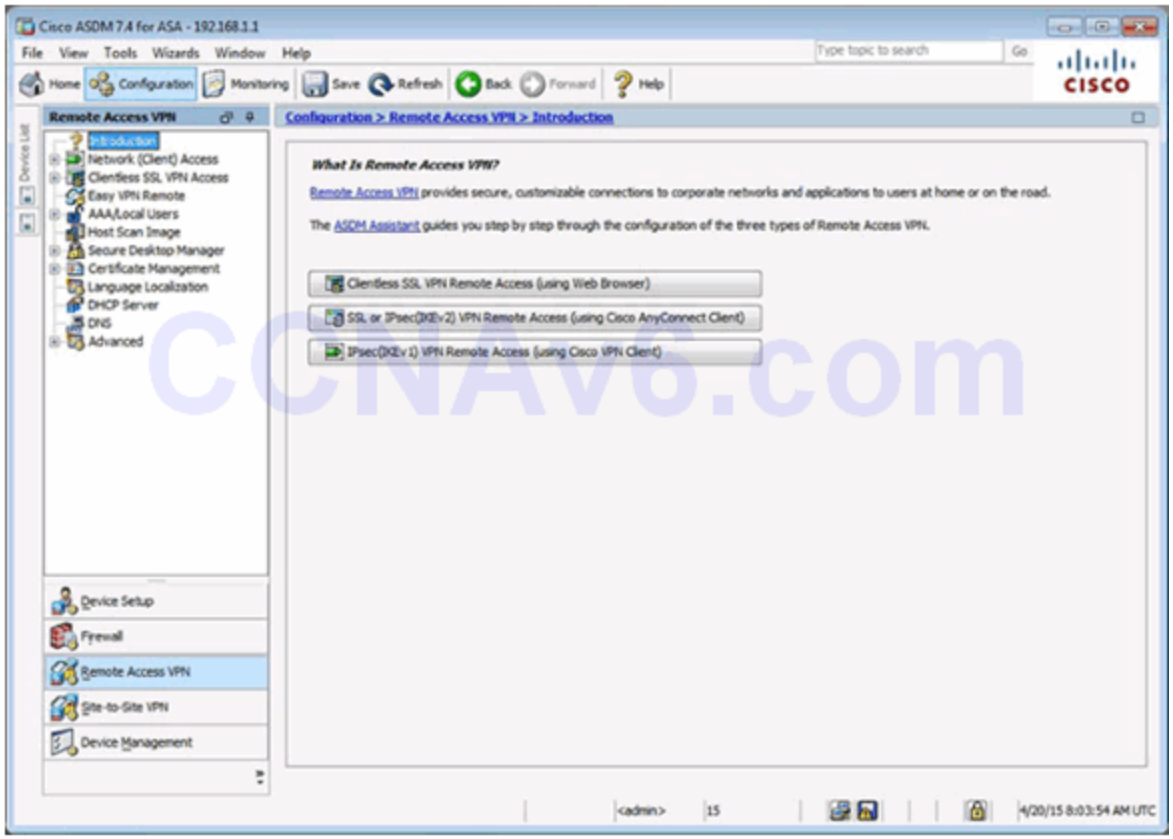
- iOS
- Android
- BlackBerry
- Windows Mobile



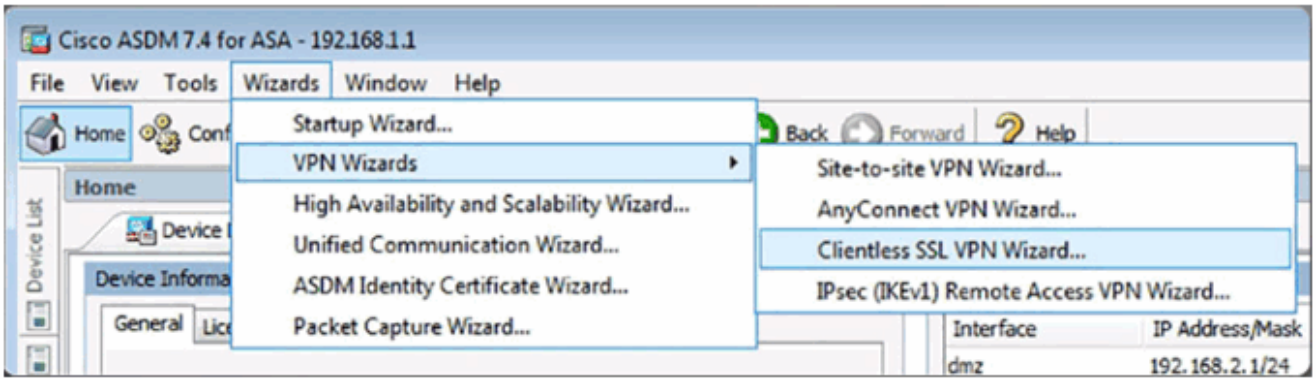
Topic 10.2.3: Configuring Clientless SSL VPN

Configuring Clientless SSL VPN on an ASA

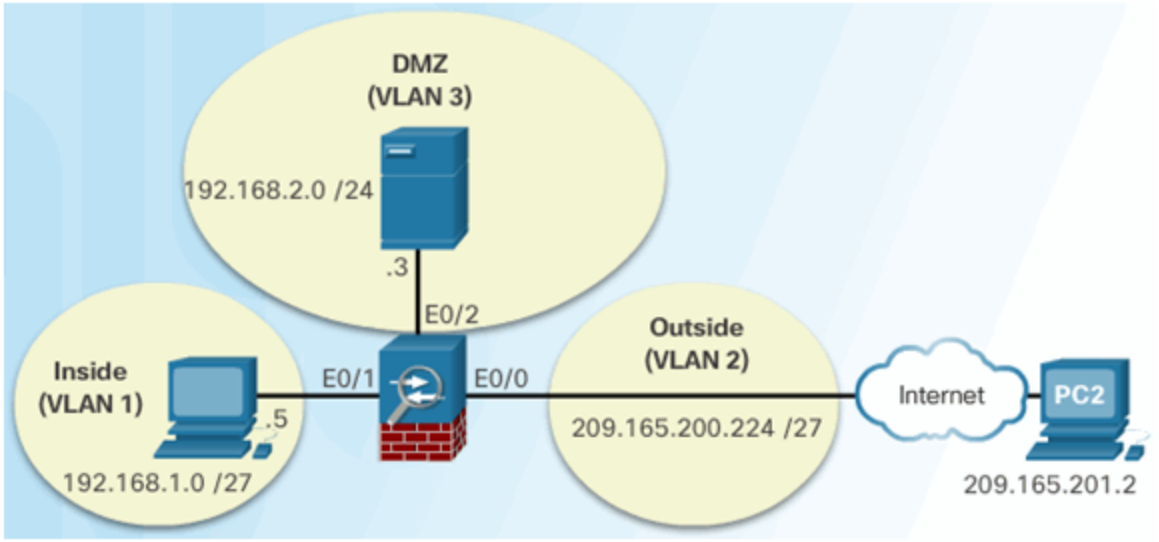
ASDM Assistant



Clientless VPN Wizard

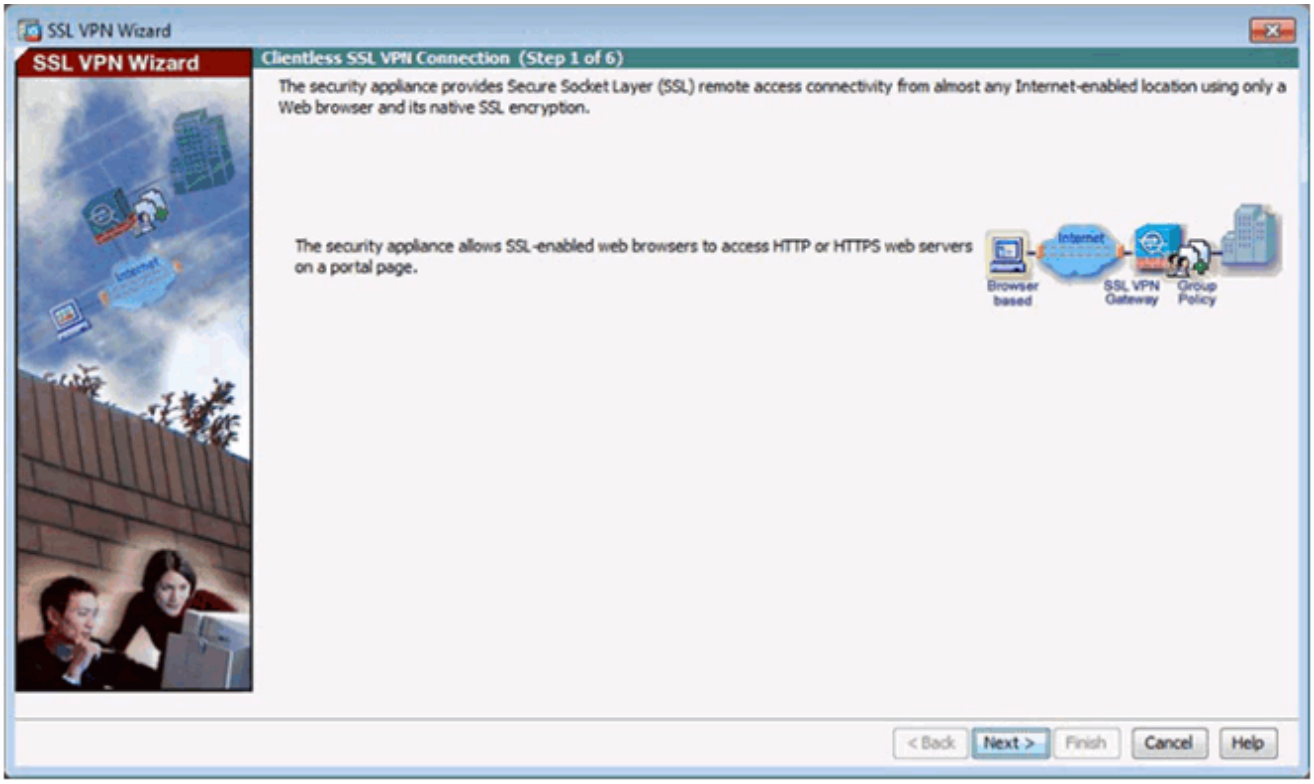


Sample Clientless VPN Topology

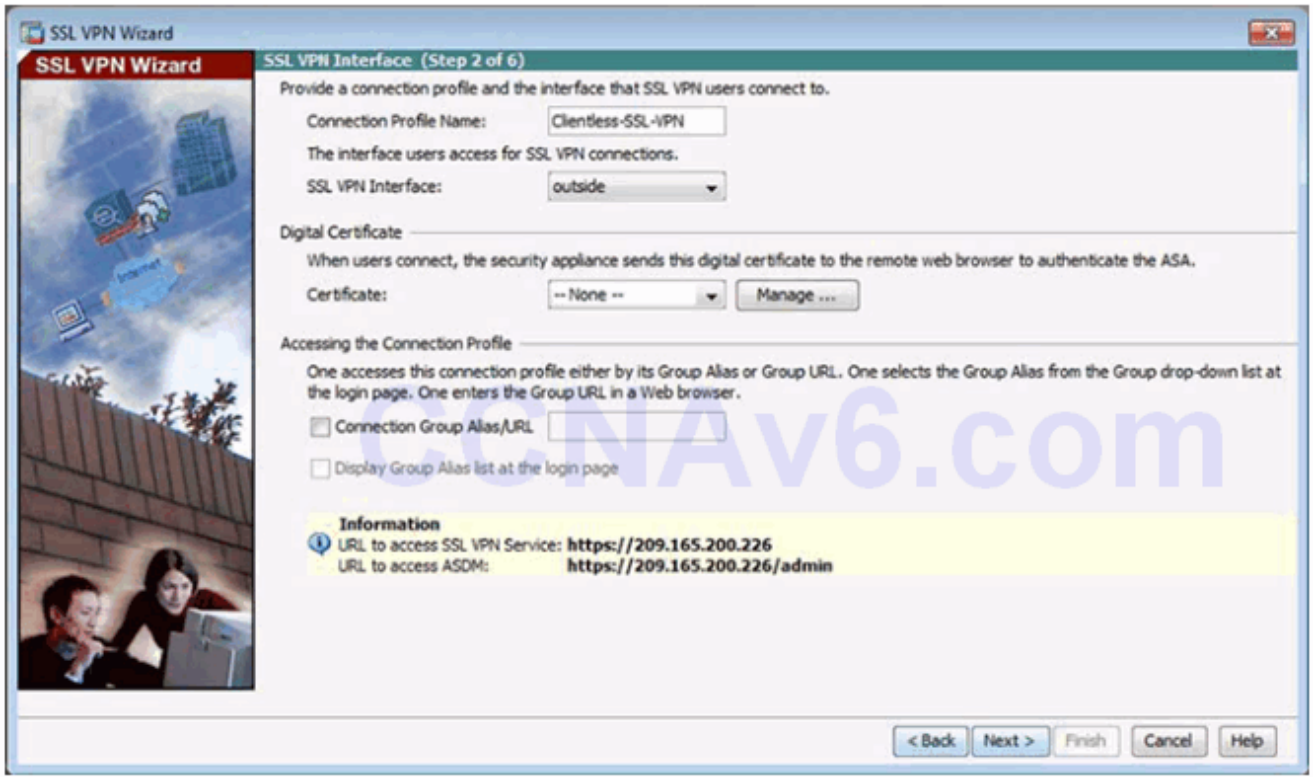


Clientless SSL VPN

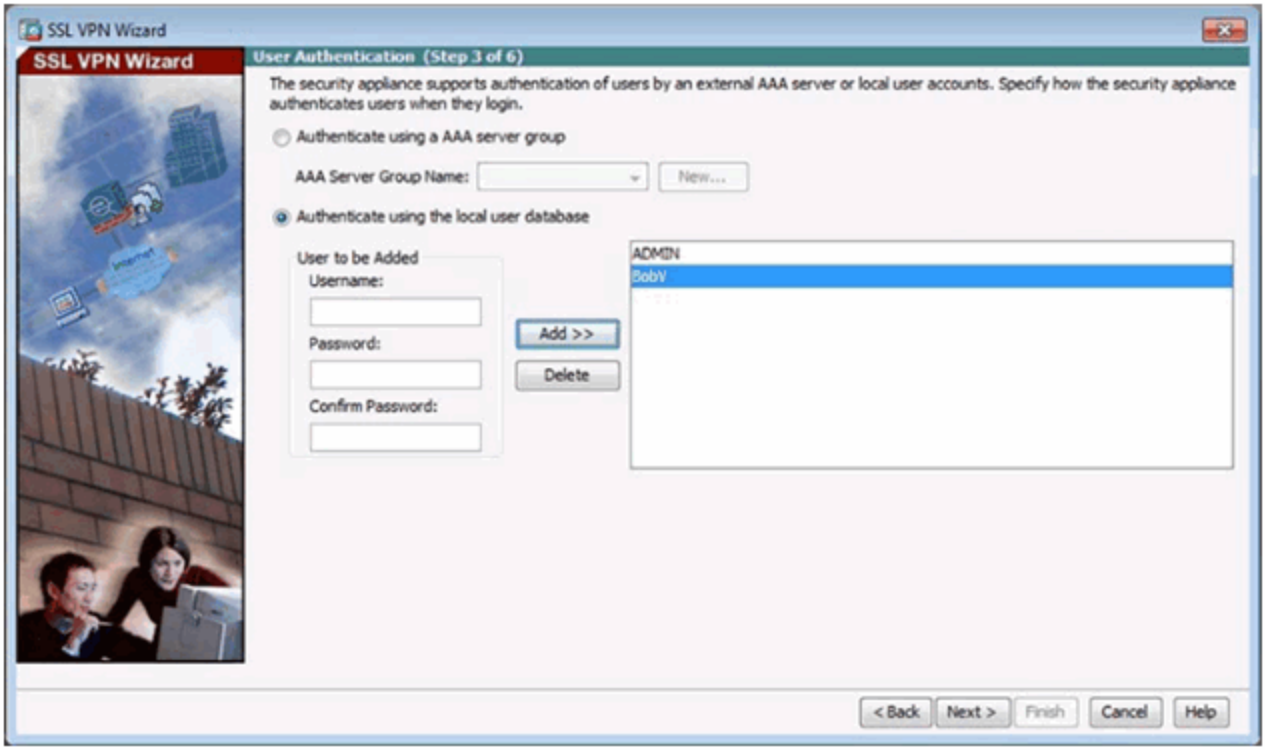
Clientless SSL VPN Introduction Window



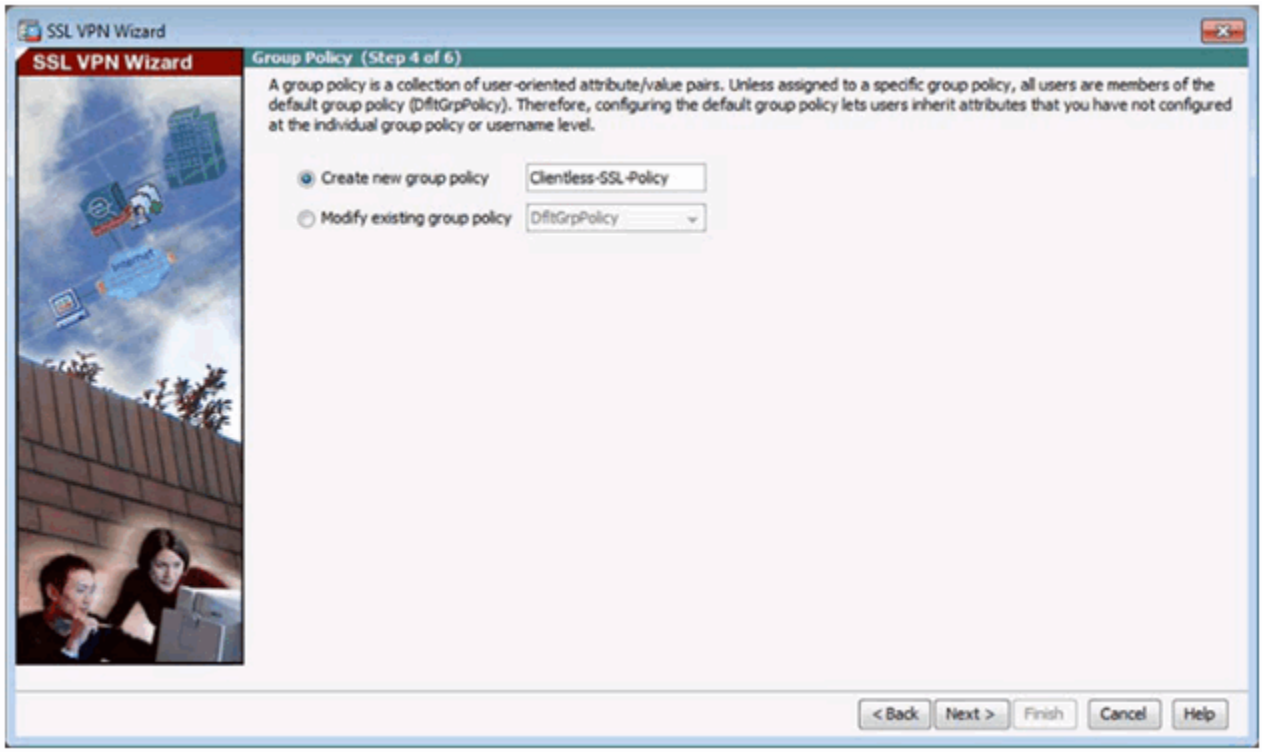
SSL VPN Interface Window



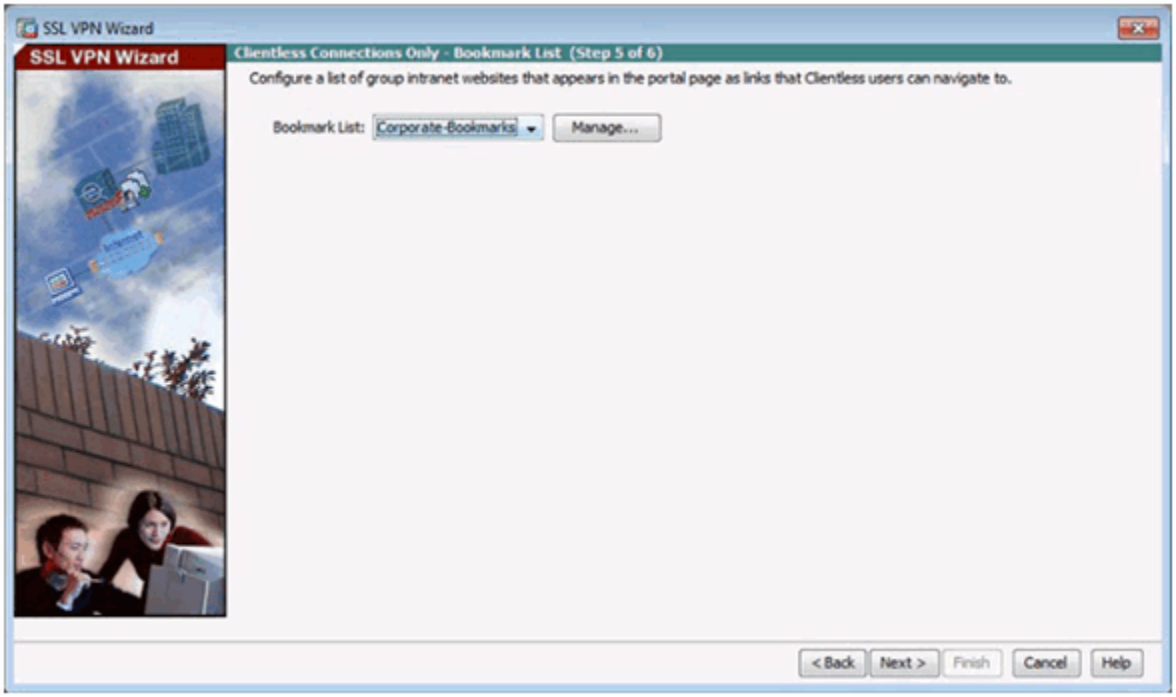
User Authentication Window



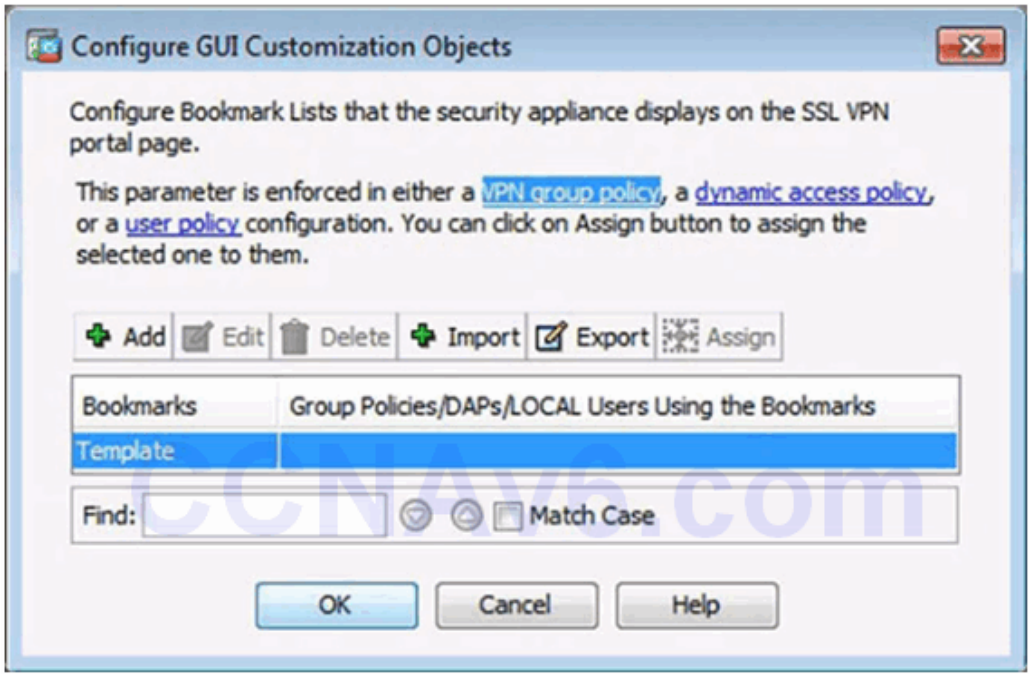
Group Policy Window



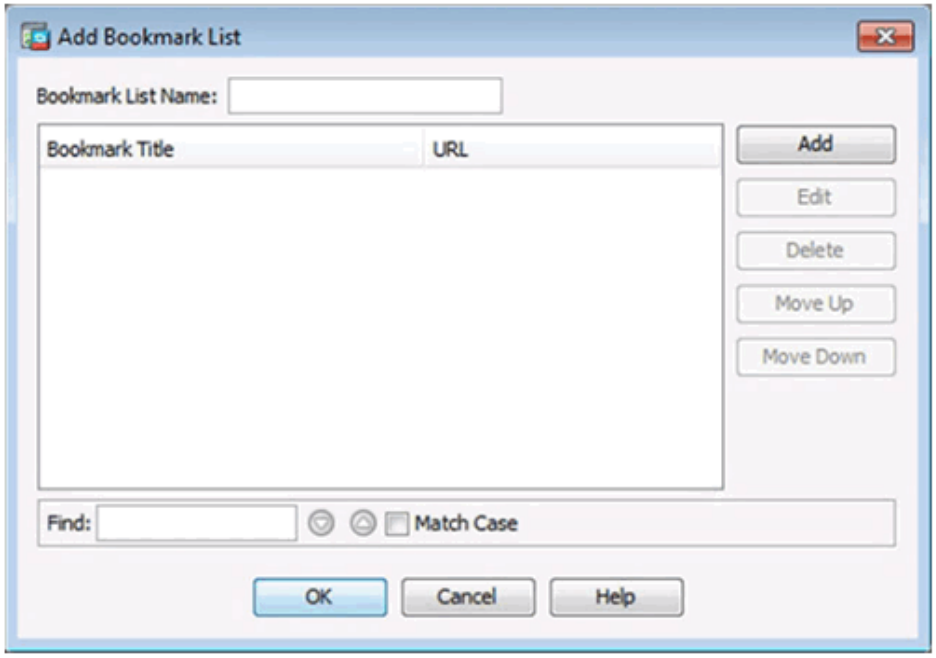
Bookmark List Window



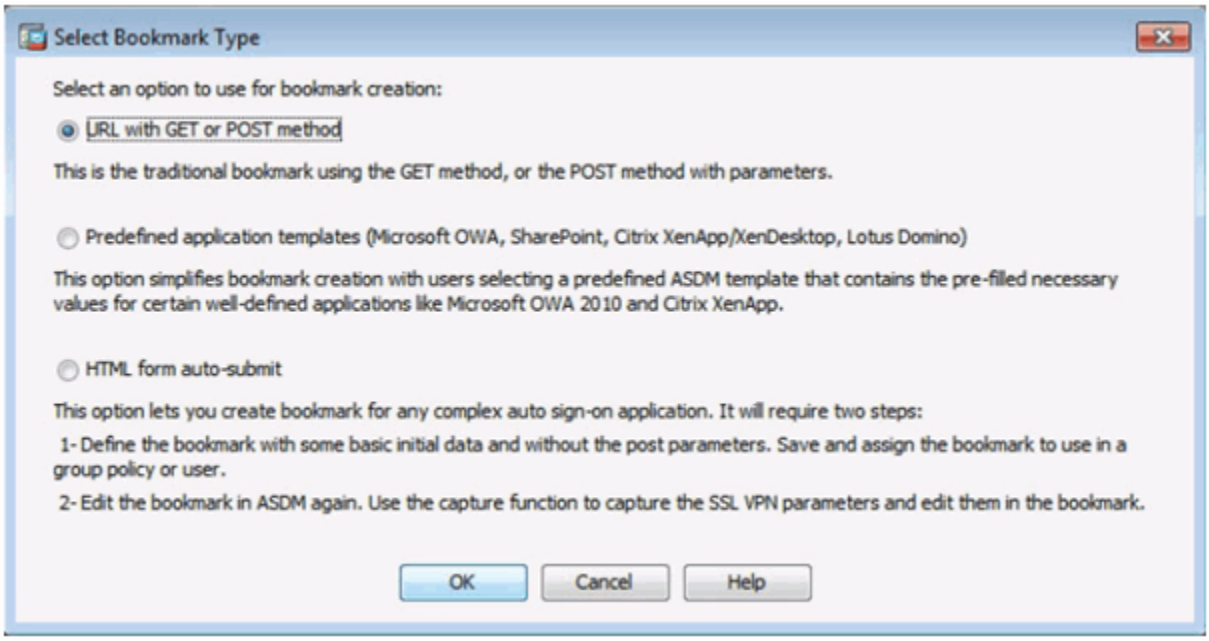
Configure GUI Customization Objects Window



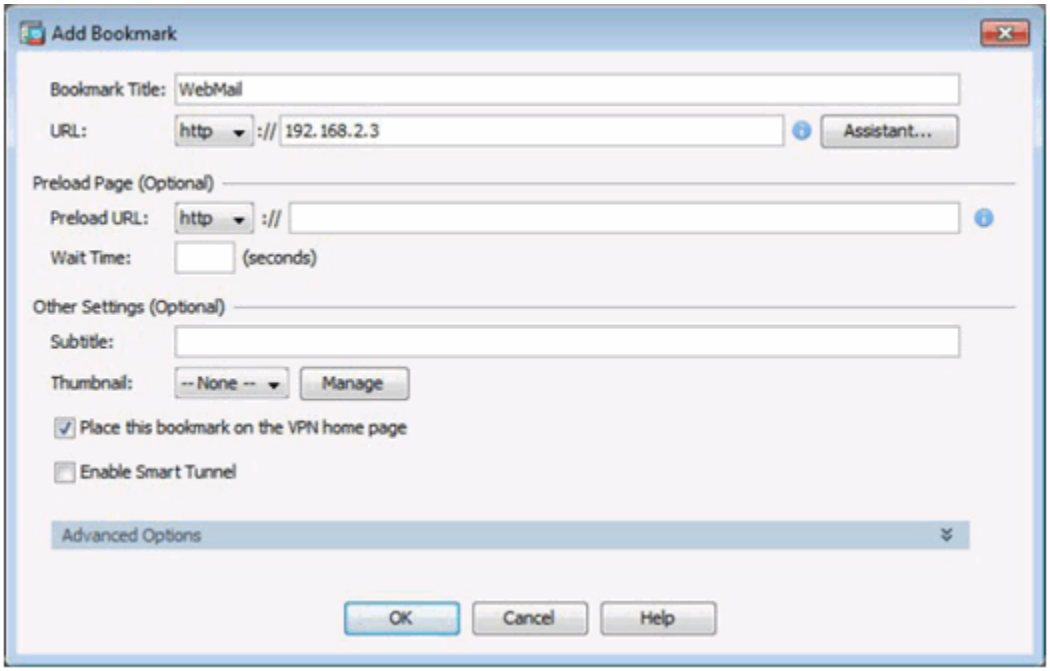
Add Bookmark List Window



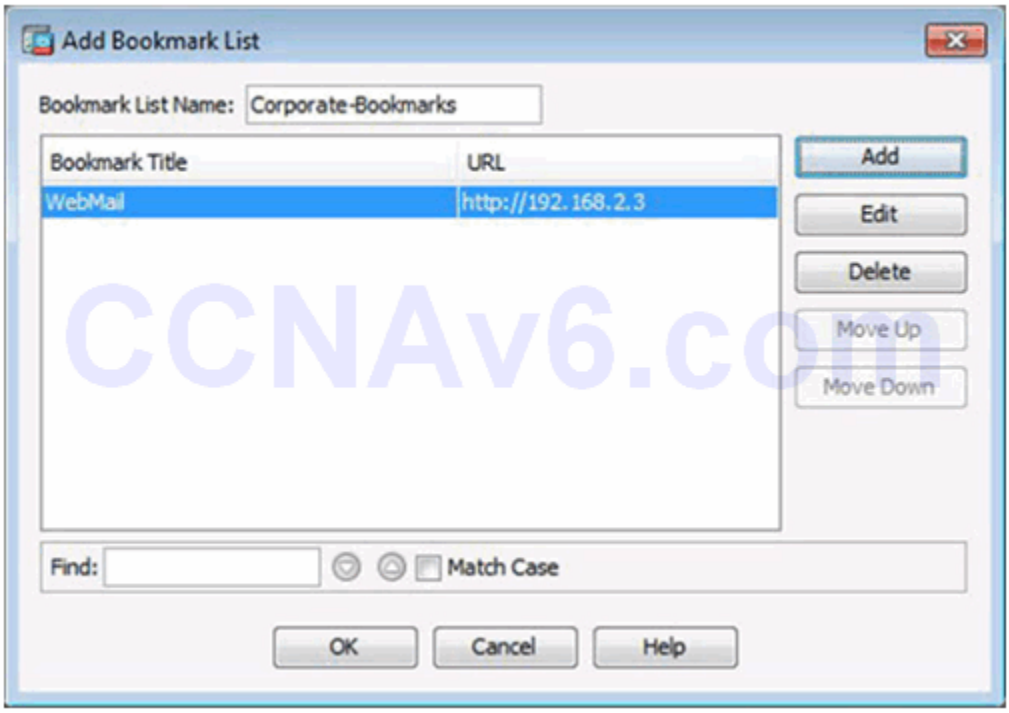
Select Bookmark Type Window



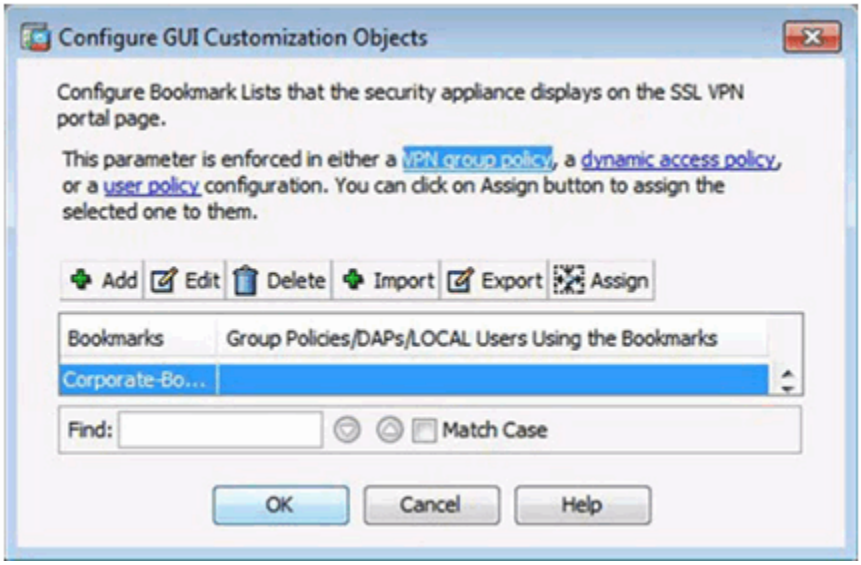
Add Bookmark Window



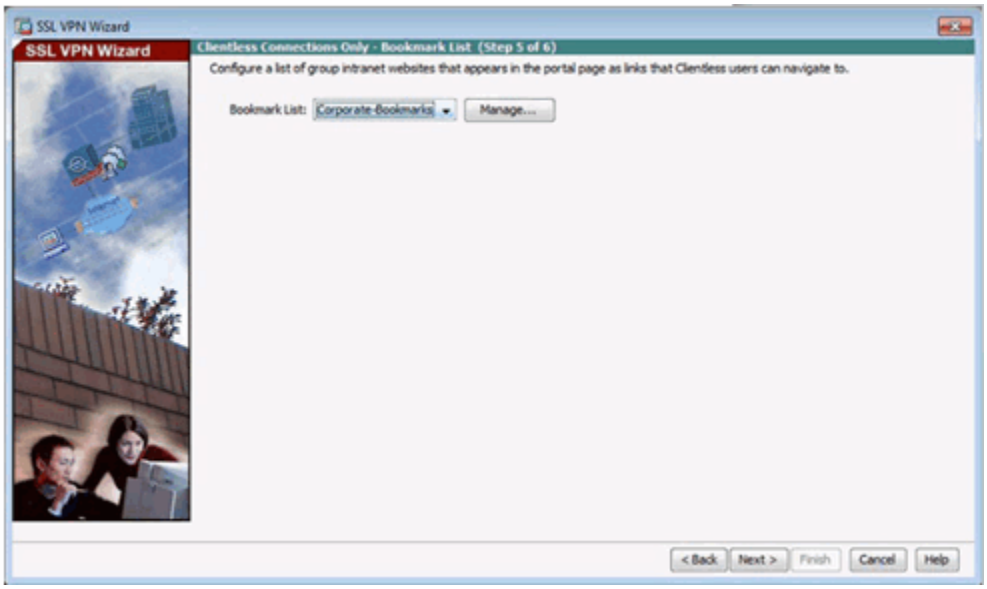
Revised Add Bookmark List Window



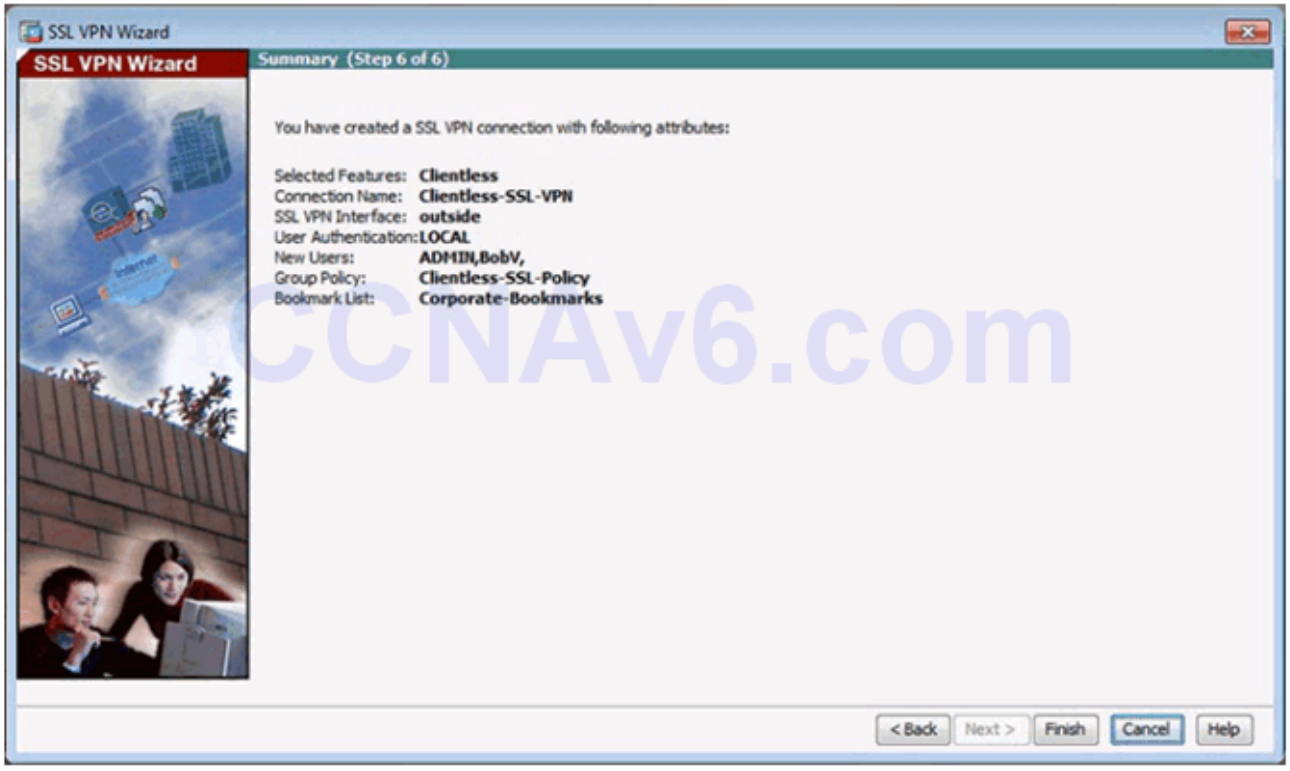
Revised Configure GUI Customization Objects Window



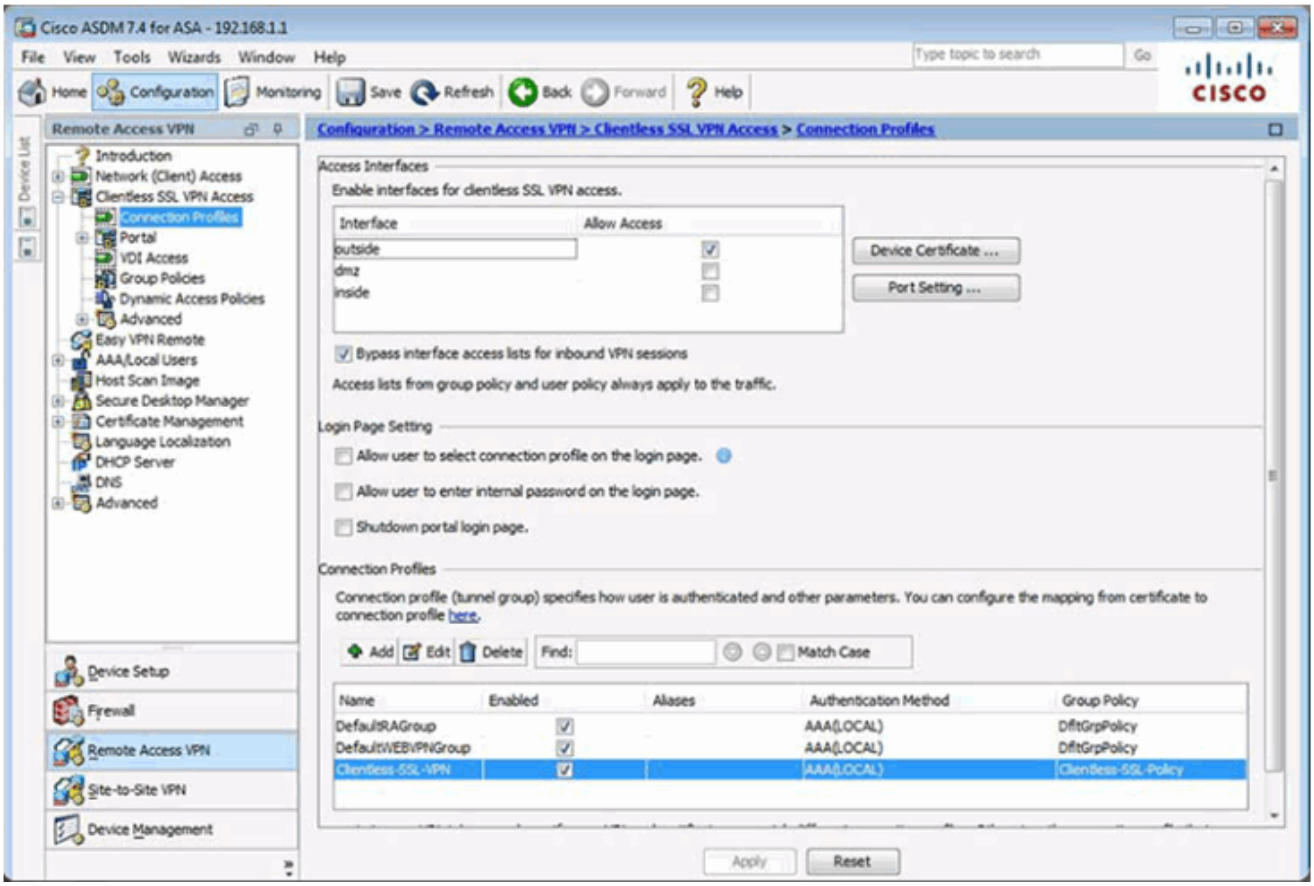
Revised Bookmark List Window



Summary Window

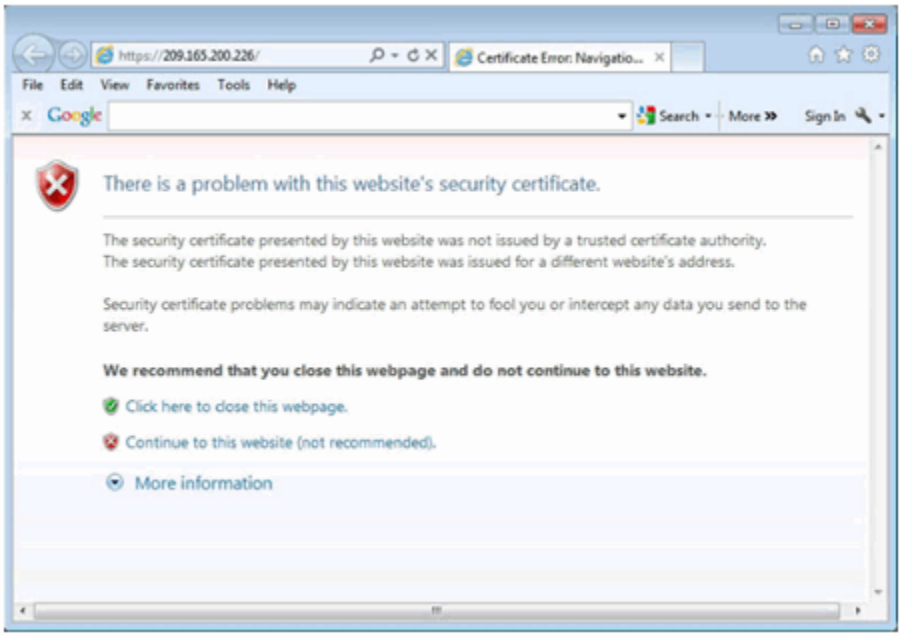


Verifying Clientless SSL VPN

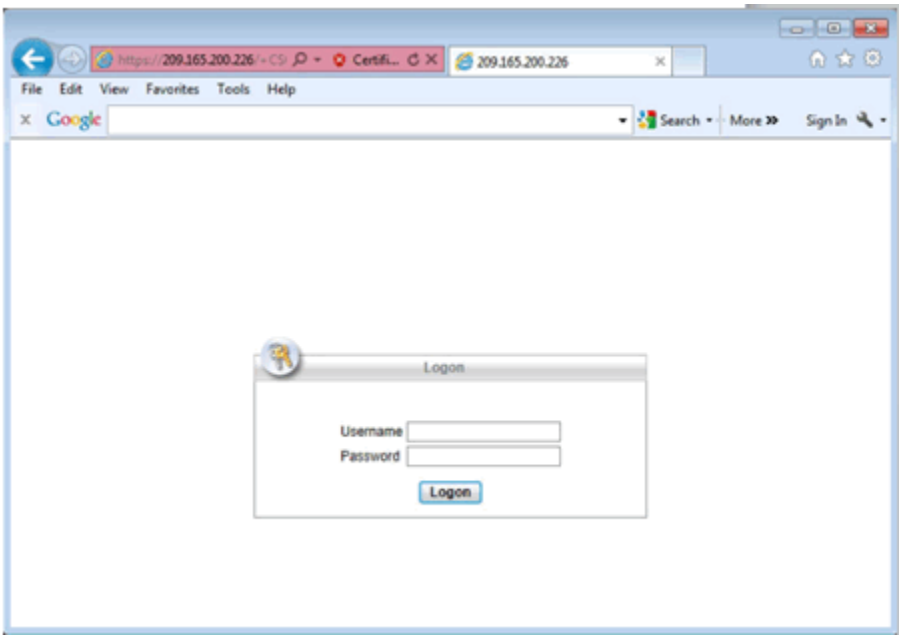


Testing the Clientless SSL VPN Connection

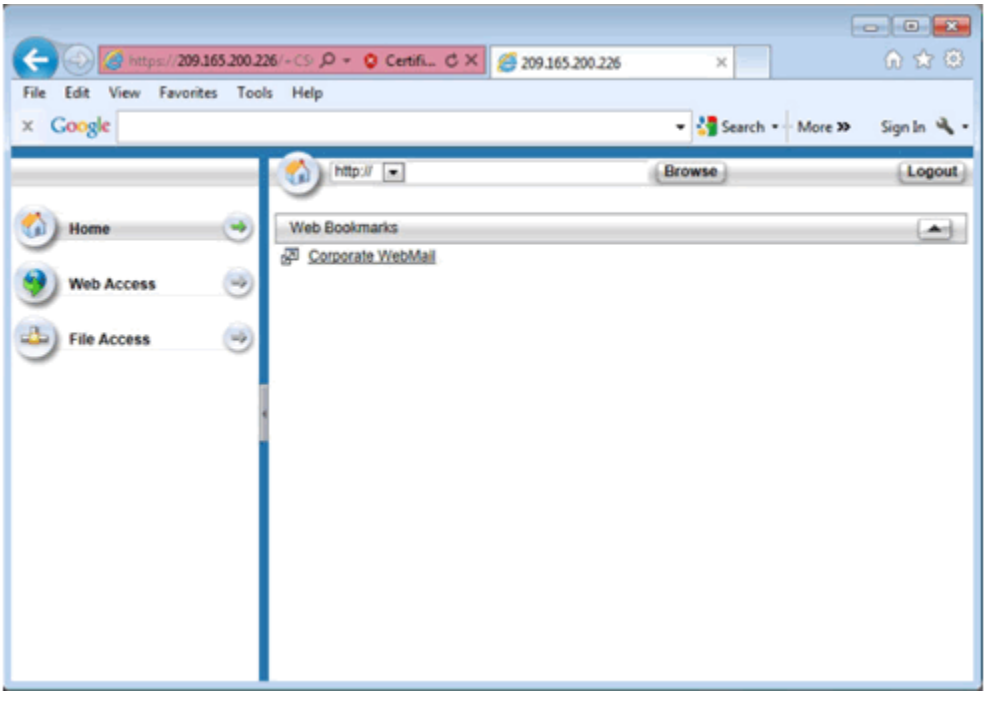
Security Certificate Window



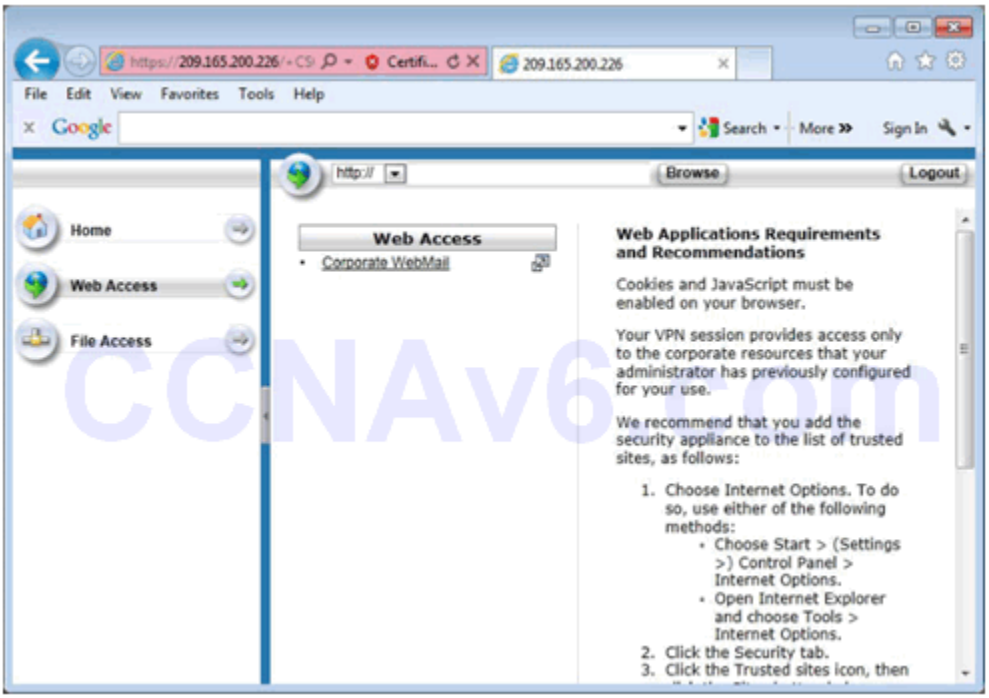
Logon Window



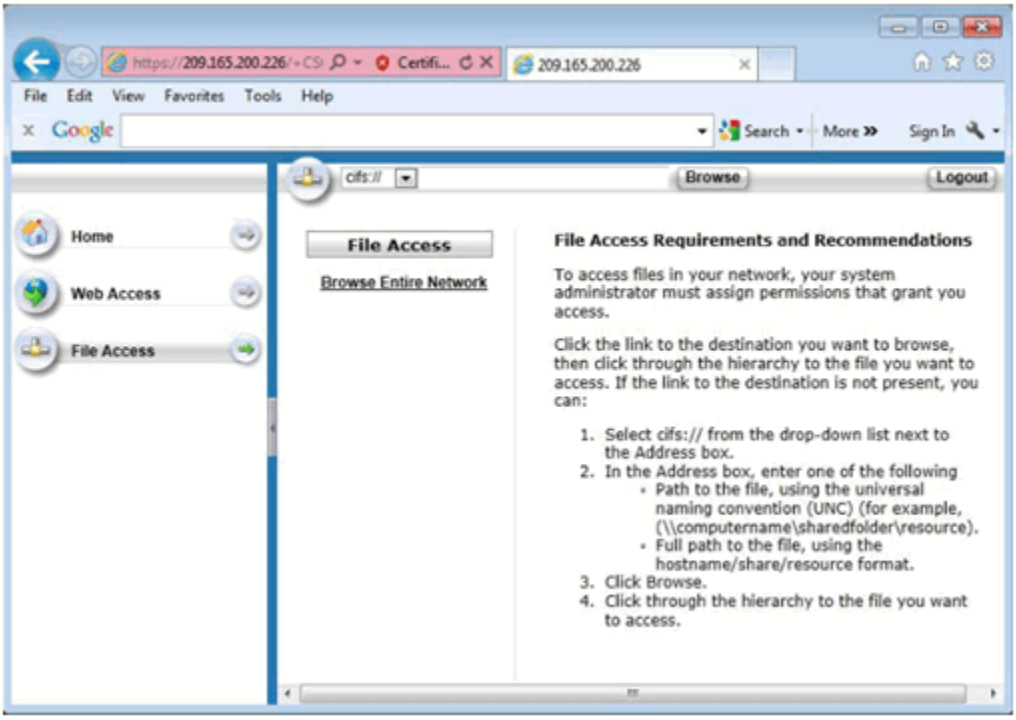
Web Portal Home Page



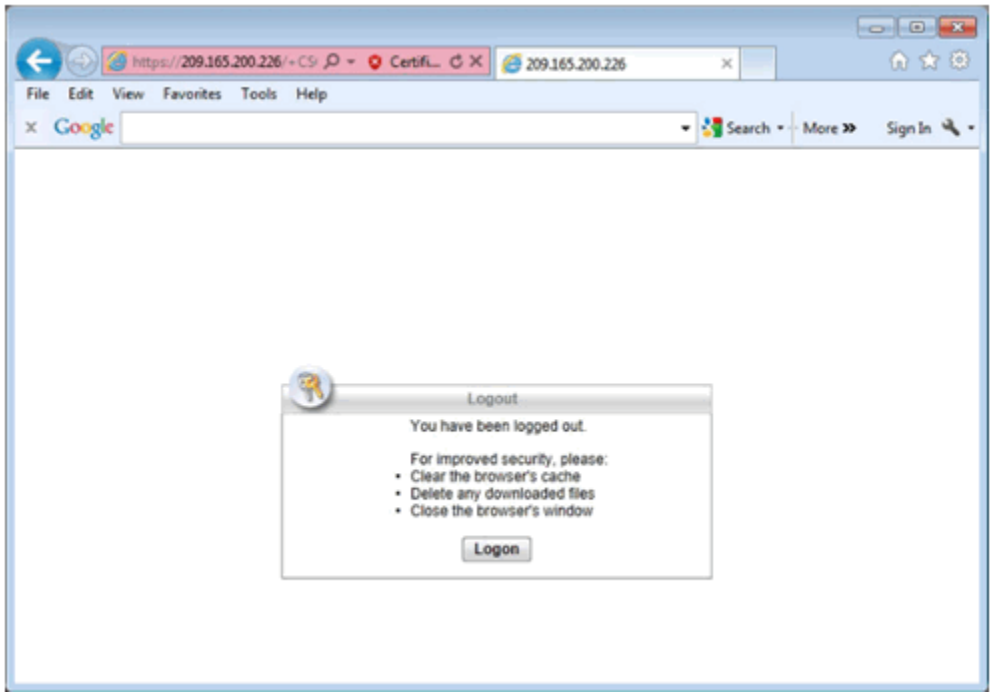
Web Portal Web Access Page



Web Portal File Access Page



Log Out of the Web Portal



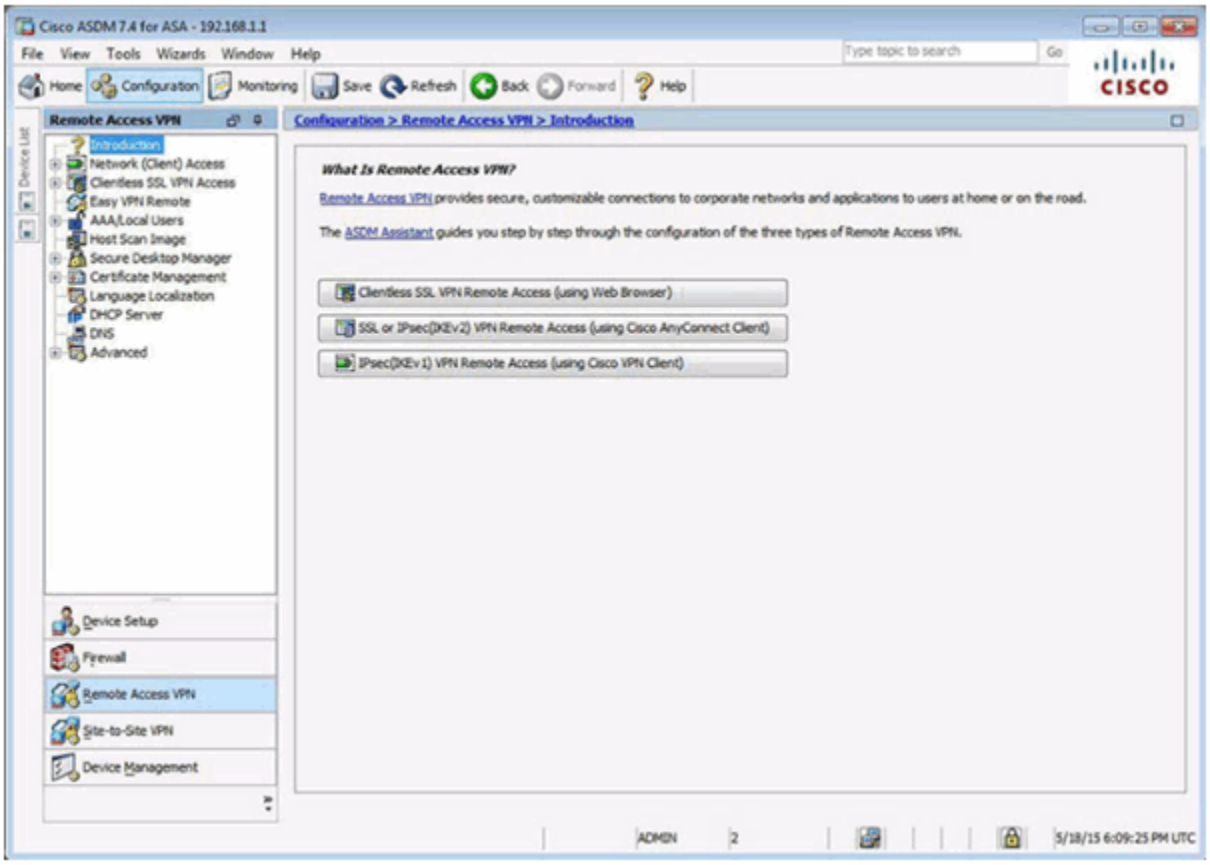
Viewing the Generated CLI Config

```
webvpn
 enable outside

group-policy Clientless-SSL-Policy internal
group-policy Clientless-SSL-Policy attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list value Corporate-Bookmarks

username ADMIN password 3MBOT/Mpbpc4KbOv encrypted privilege 0
username ADMIN attributes
 vpn-group-policy Clientless-SSL-Policy
username BobV password AOv1eG/KWkzEwhtN encrypted privilege 0
username BobV attributes
 vpn-group-policy Clientless-SSL-Policy

tunnel-group Clientless-SSL-VPN type remote-access
tunnel-group Clientless-SSL-VPN general-attributes
 default-group-policy Clientless-SSL-Policy
```

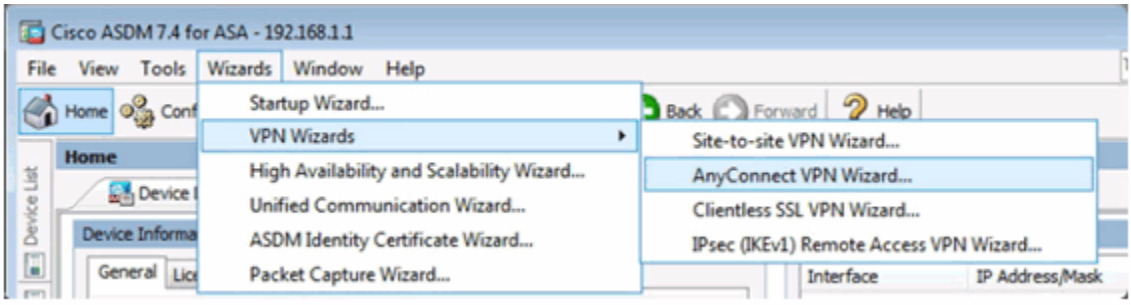
Topic 10.2.4: Configuring AnyConnect SSL VPN

Configuring SSL VPN AnyConnect

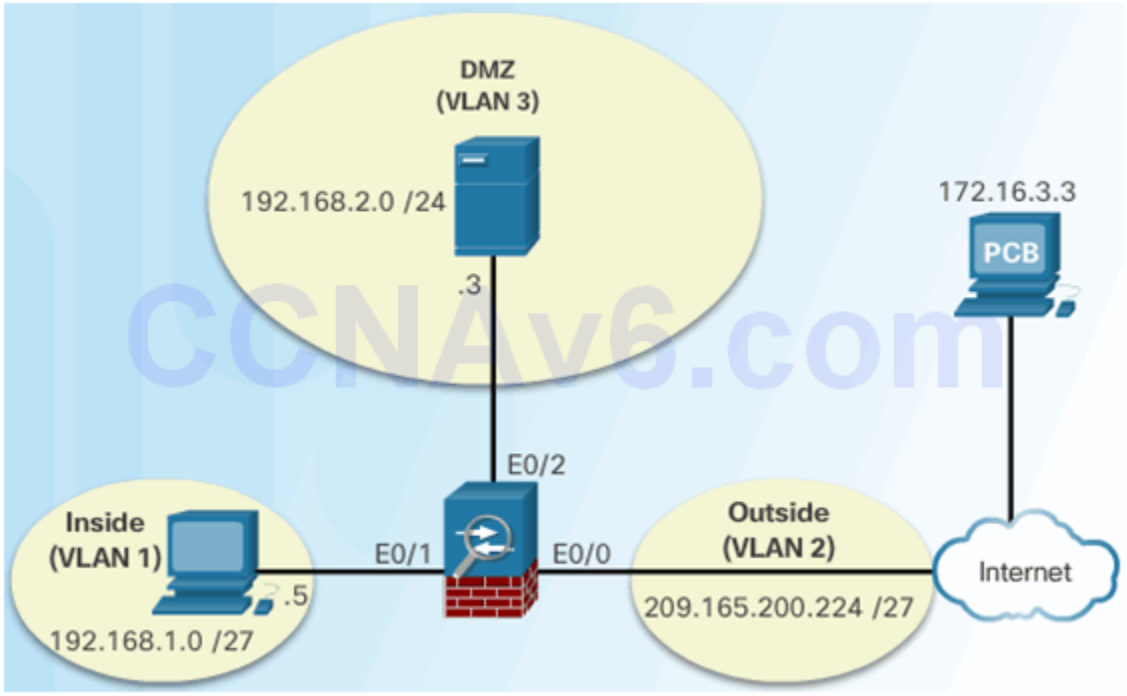
ASDM Assistant



Client-Based VPN Wizard

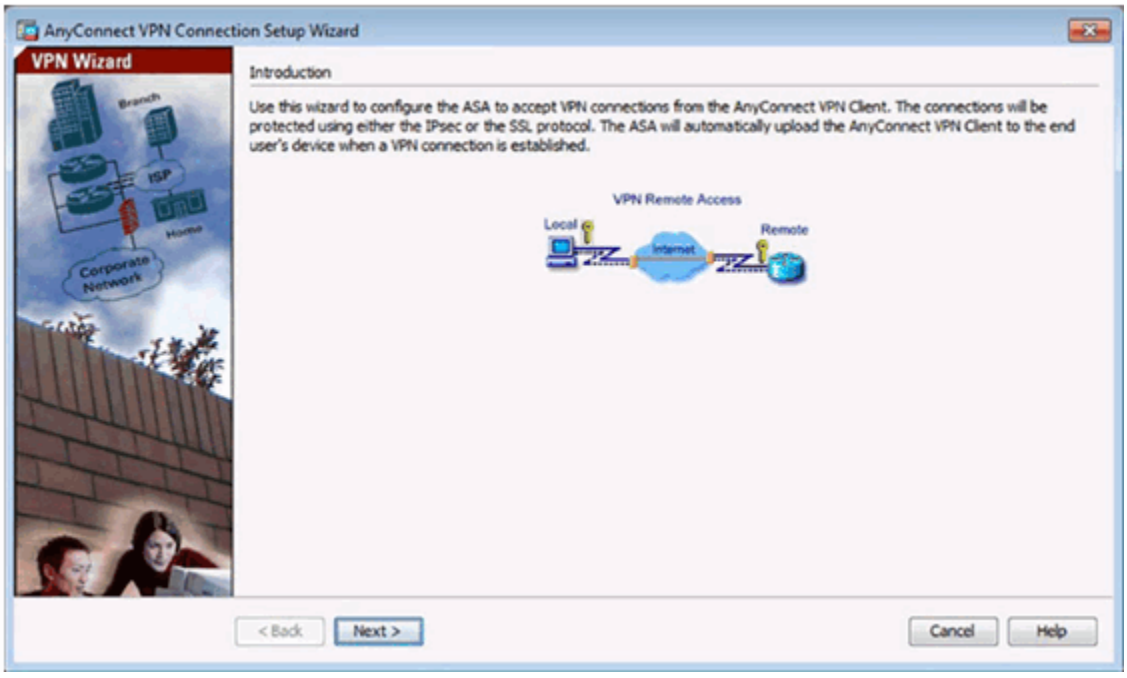


Sample SSL VPN Topology

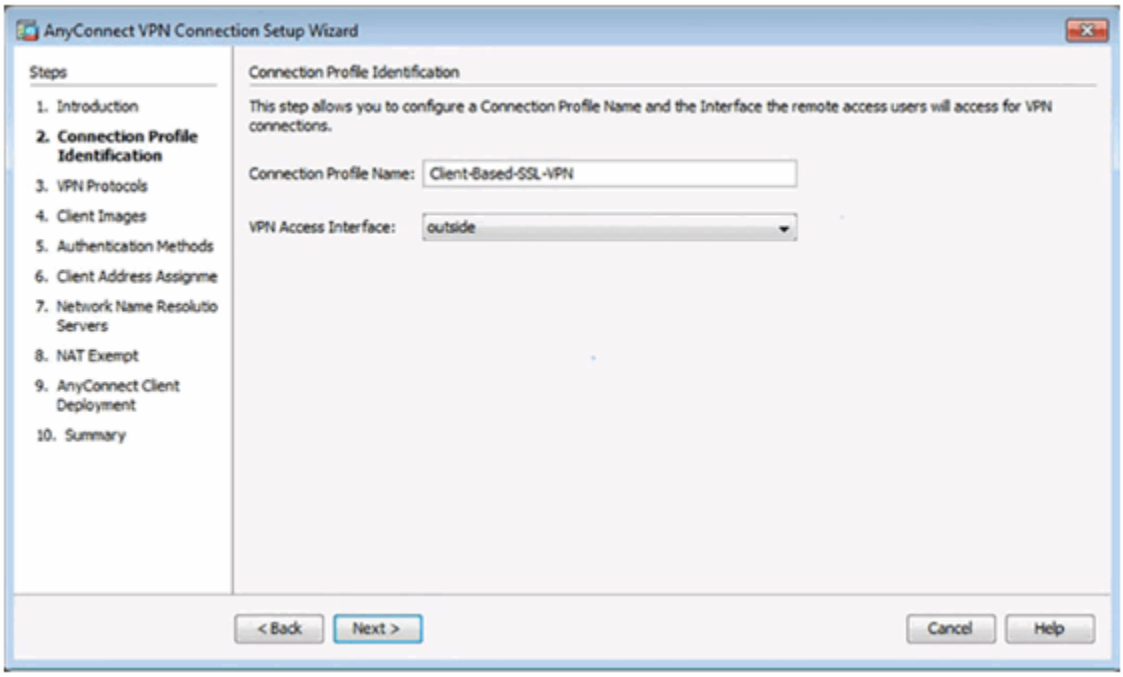


AnyConnect SSL VPN

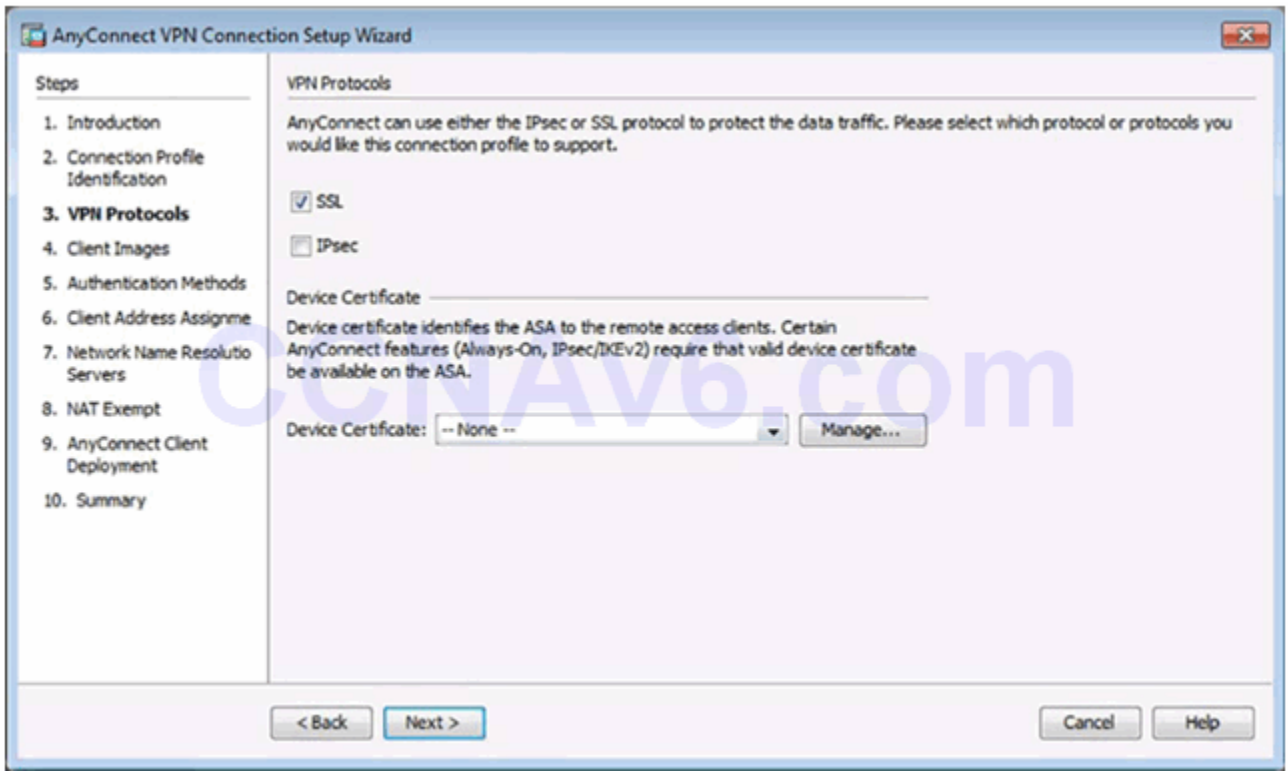
AnyConnect VPN Wizard Introduction Window



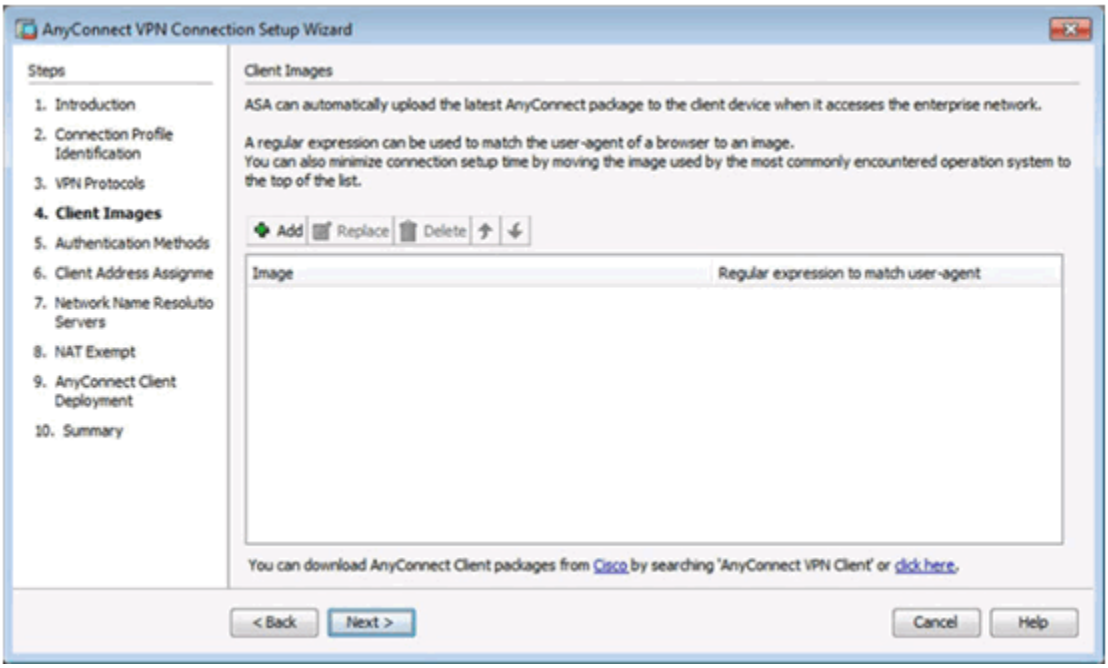
Connection Profile Identification Window



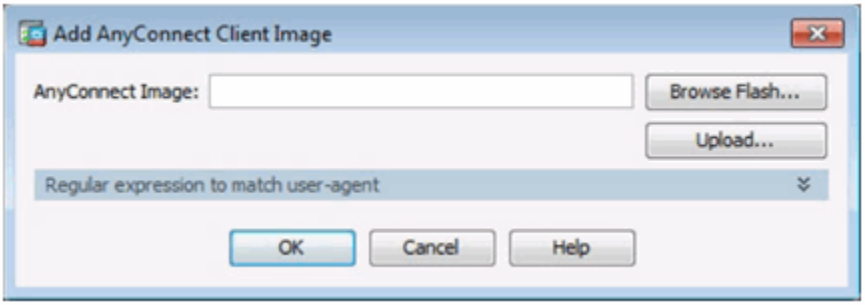
VPN Protocols Window



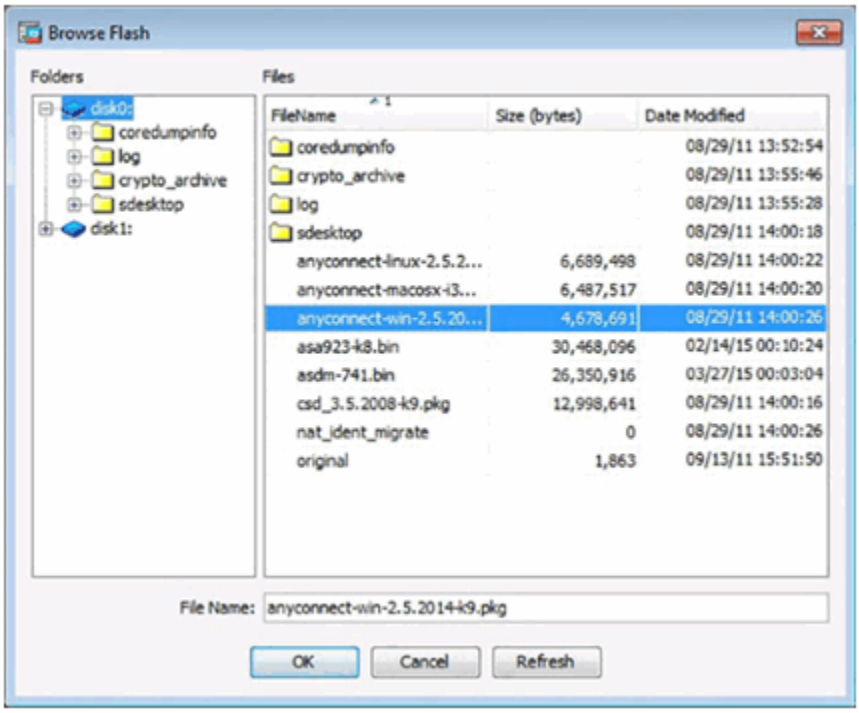
Client Images Window



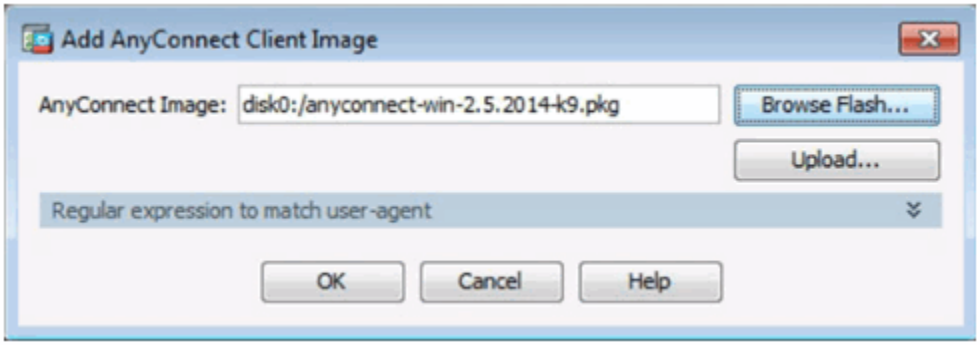
Add AnyConnect Client Image Window



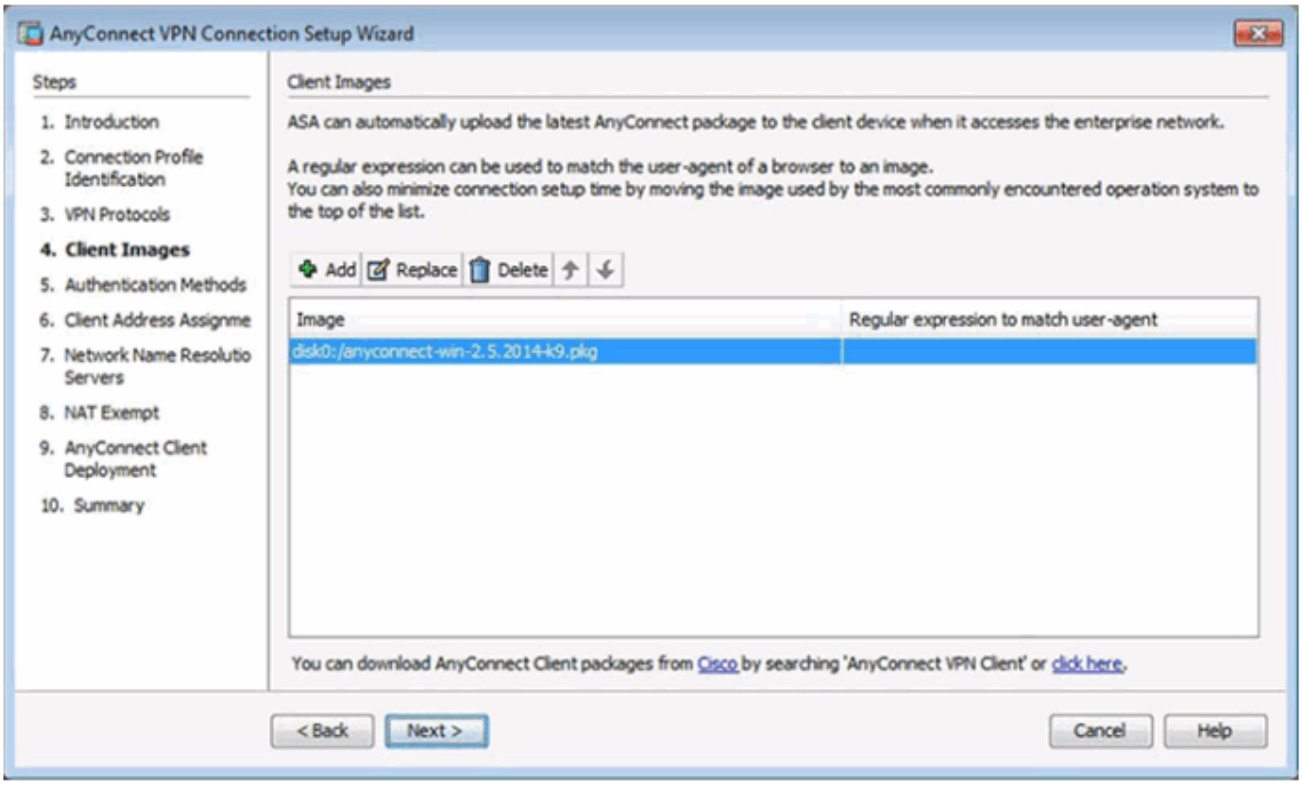
Browse Flash Window



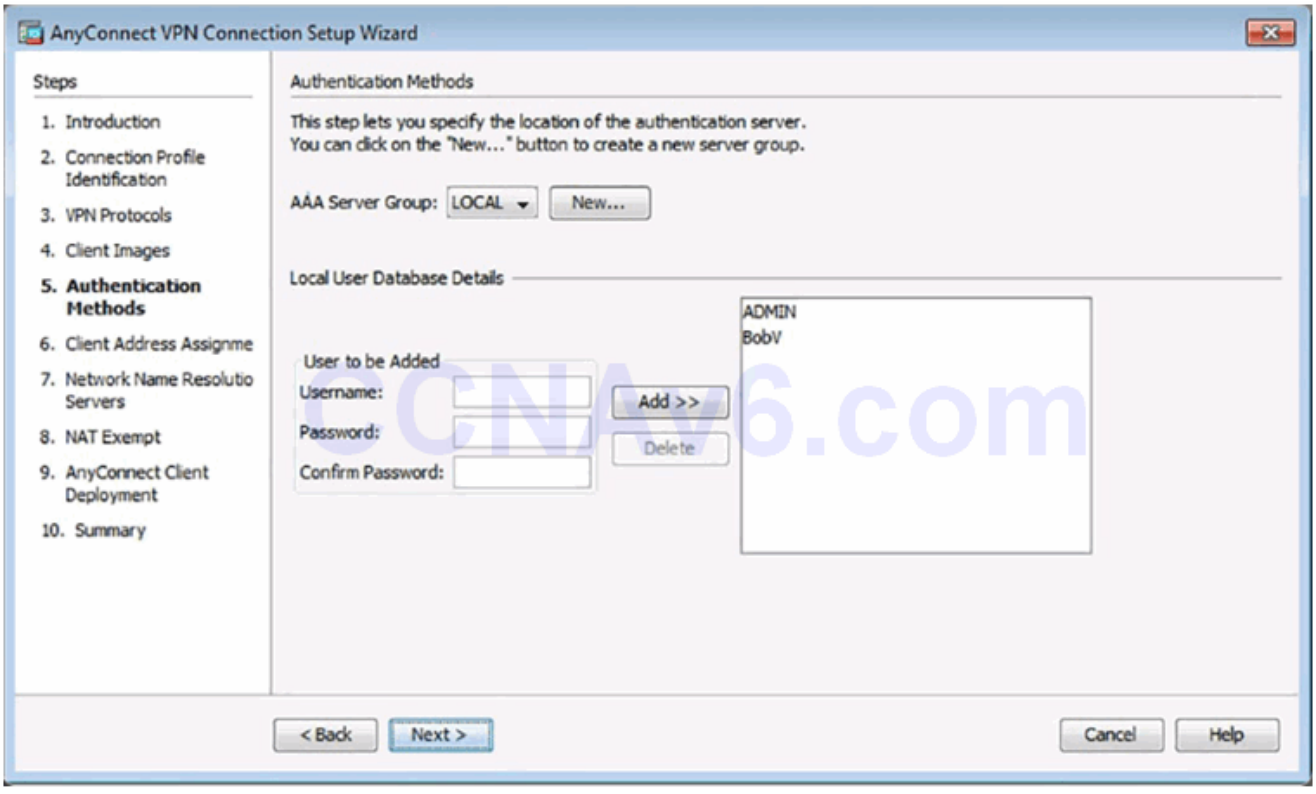
Add AnyConnect Client Image Window



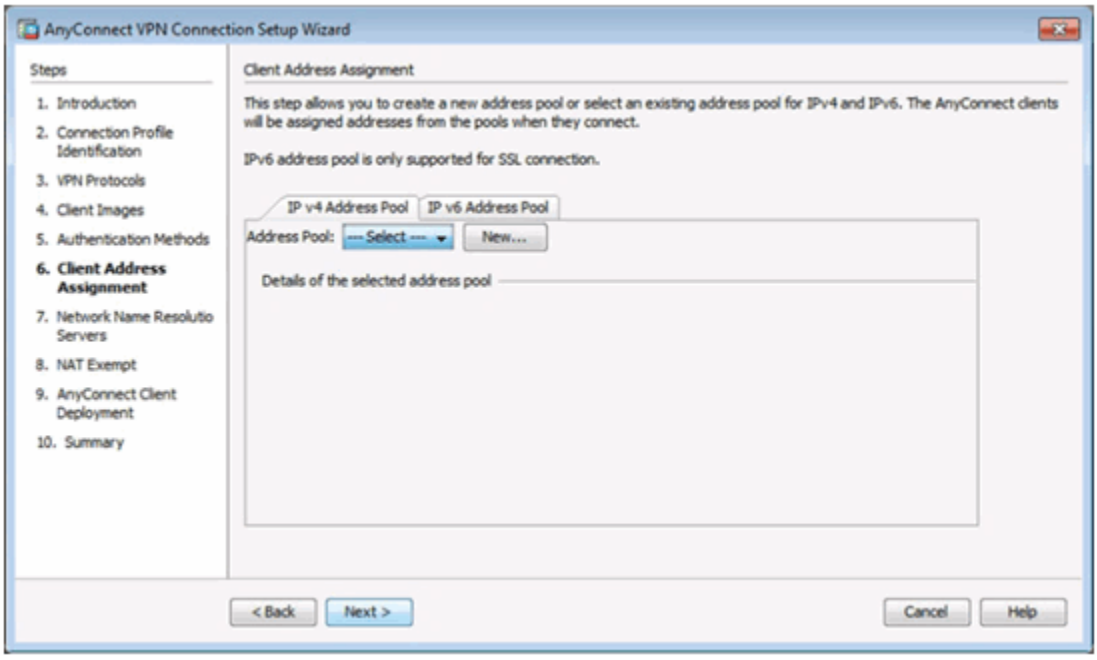
Completed Client Images Window



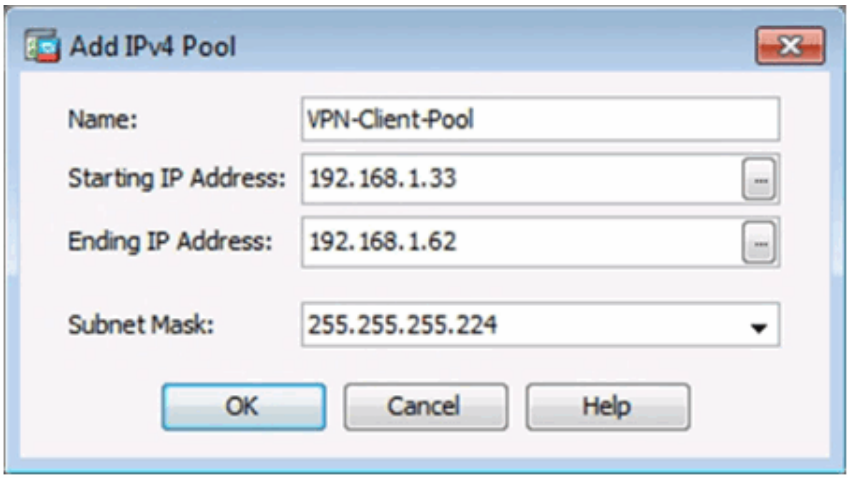
Authentication Methods Window



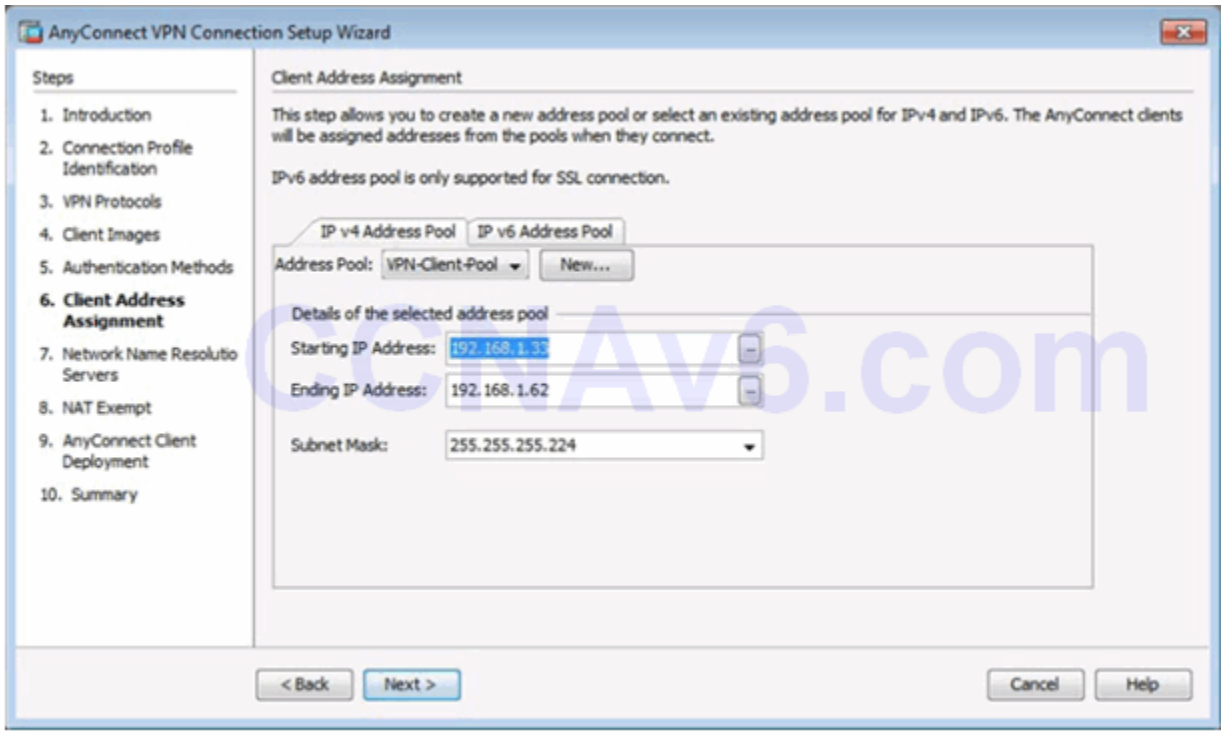
Client Address Management Window



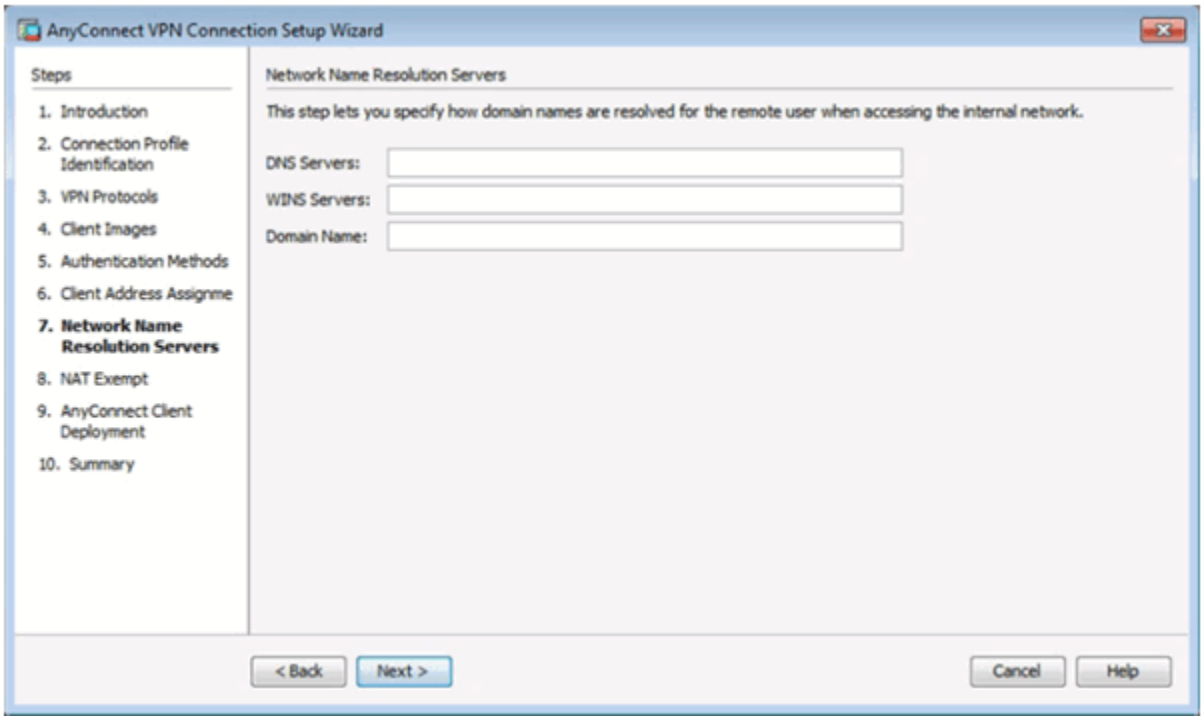
Add IPv4 Window



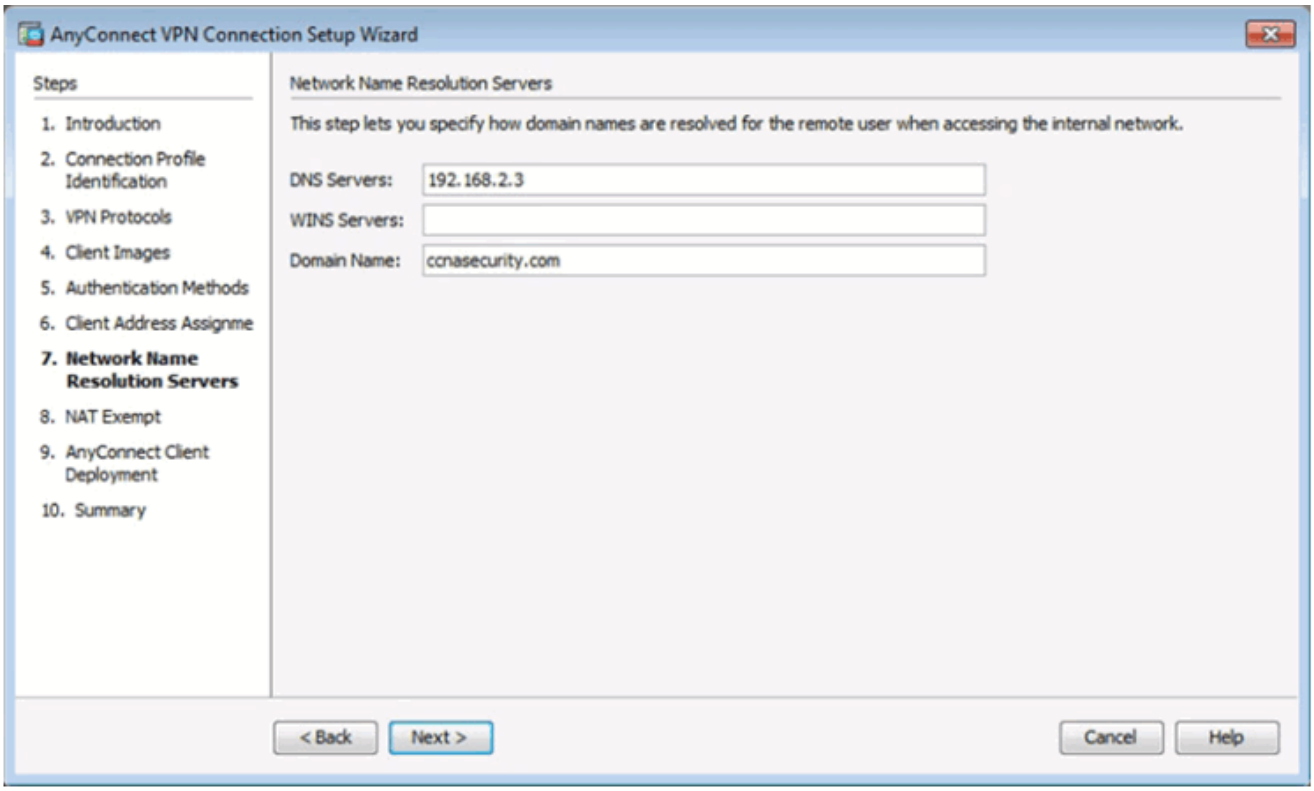
Completed Client Address Management Window



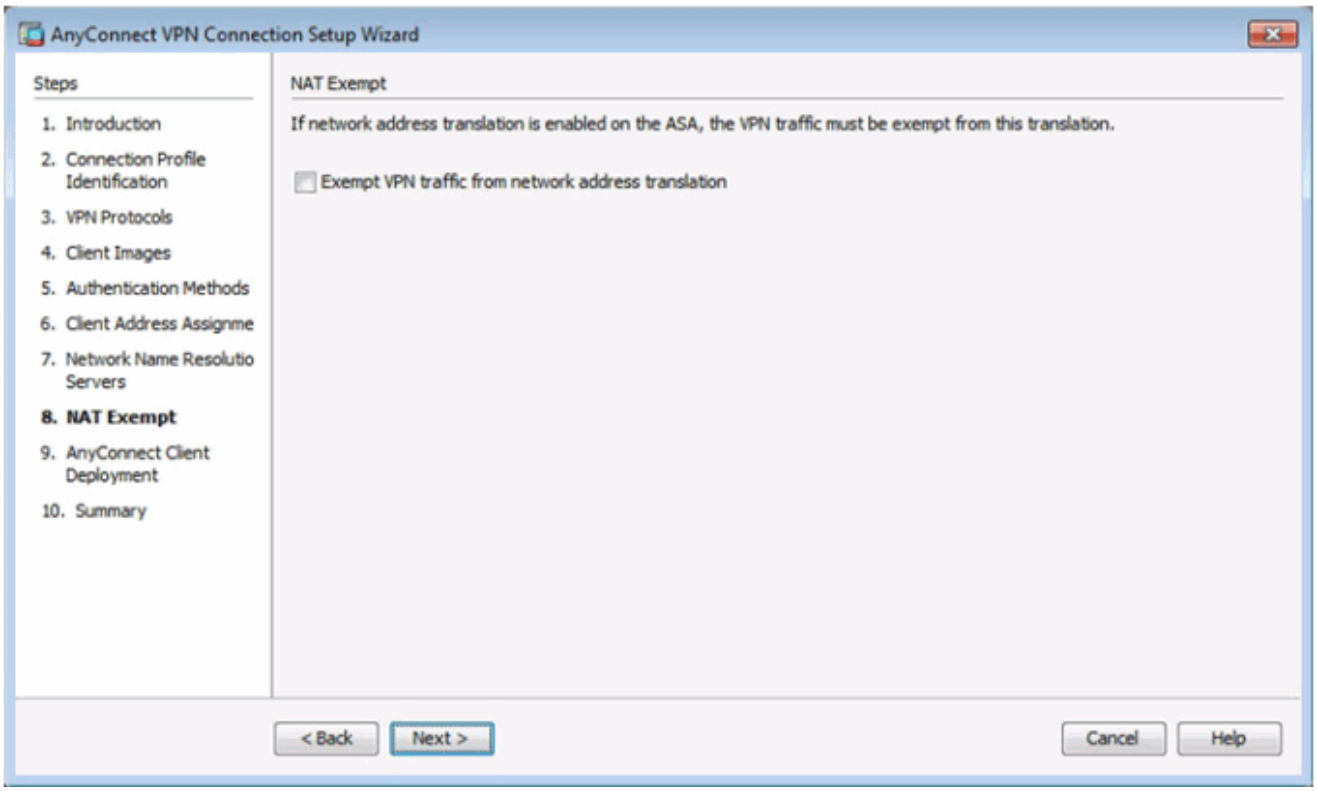
Network Name Resolution Servers Window



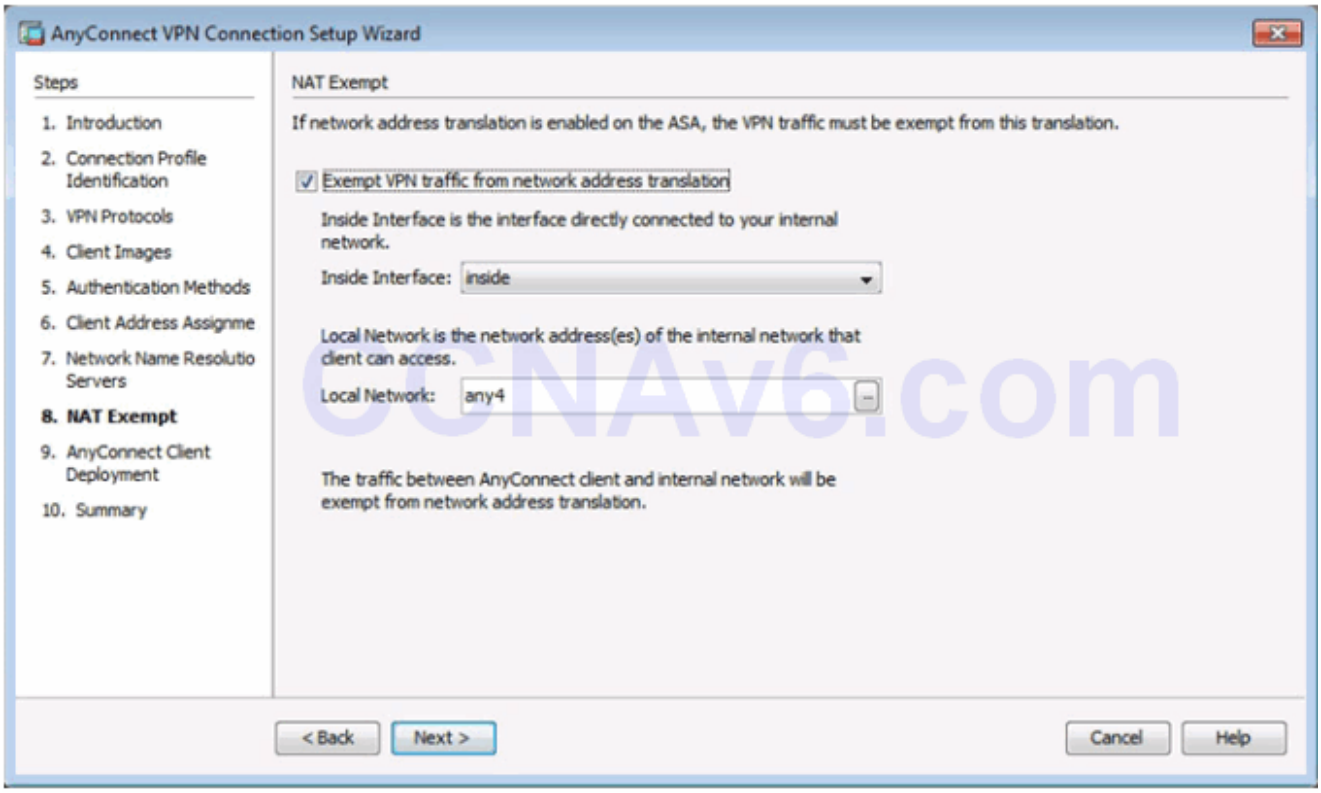
Completed Network Name Resolution Servers Window



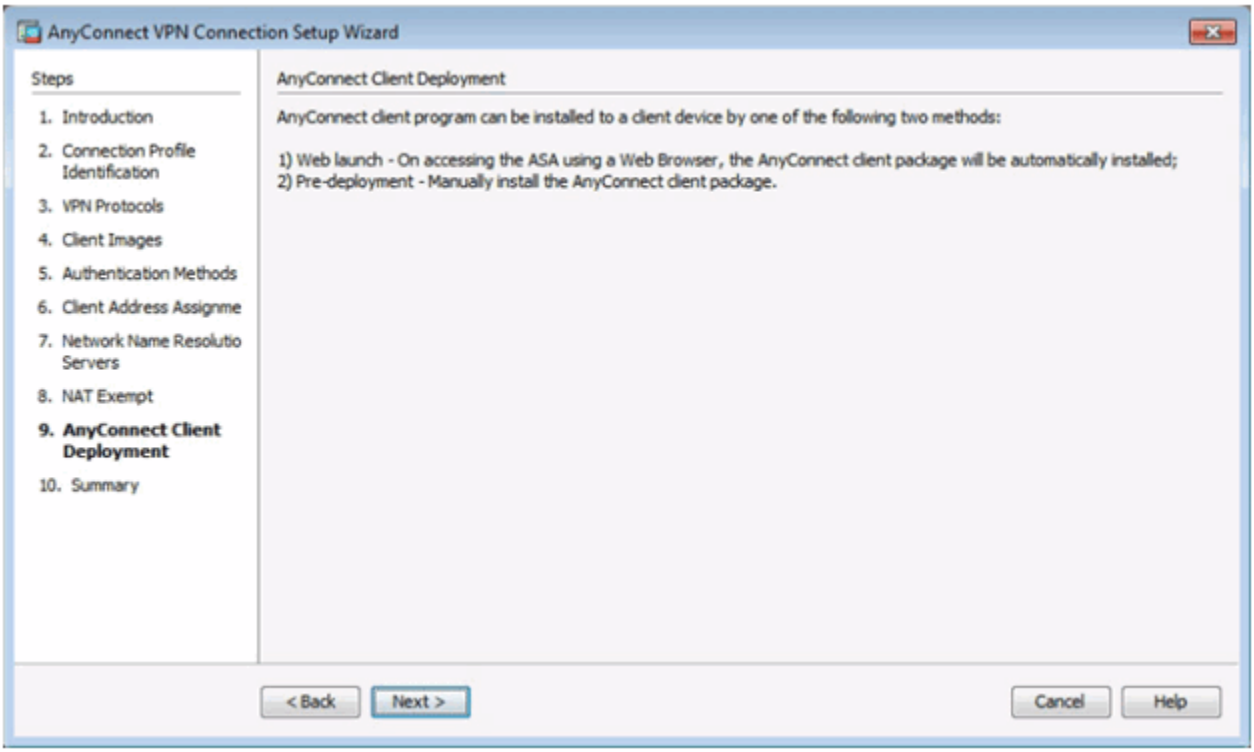
NAT Exempt Window



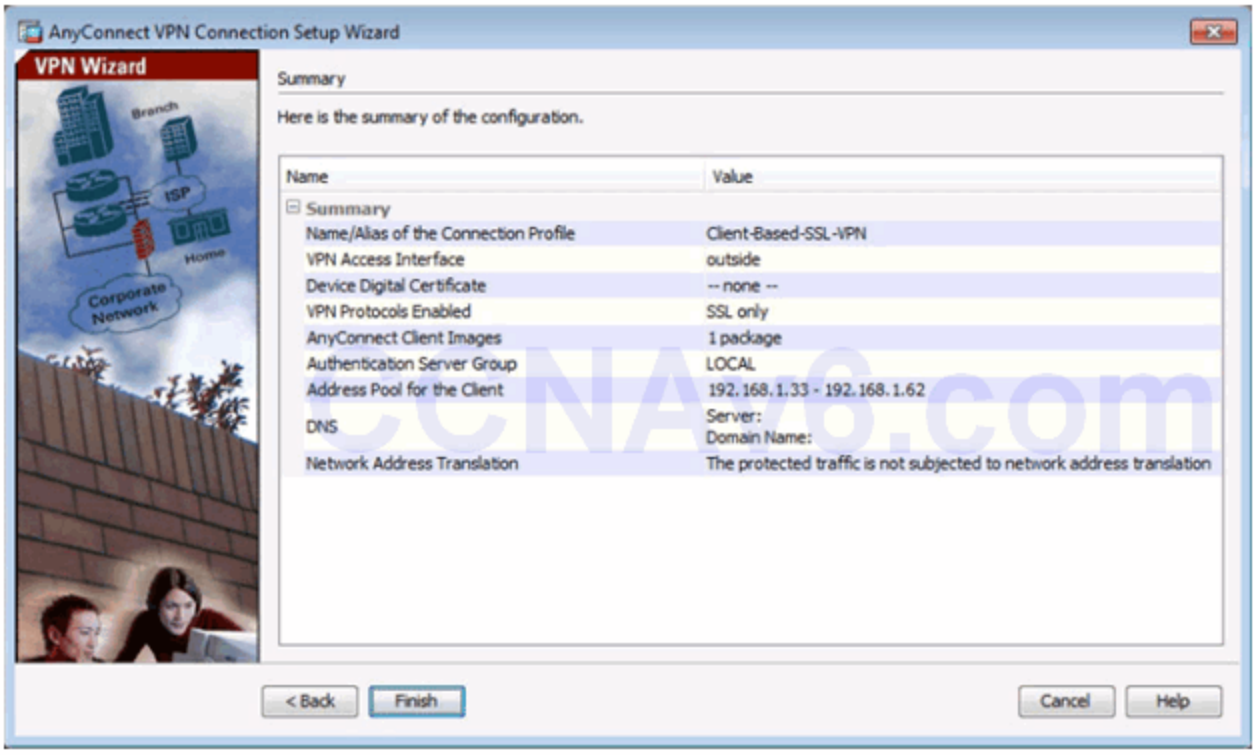
Completed NAT Exempt Window



AnyConnect Client Deployment

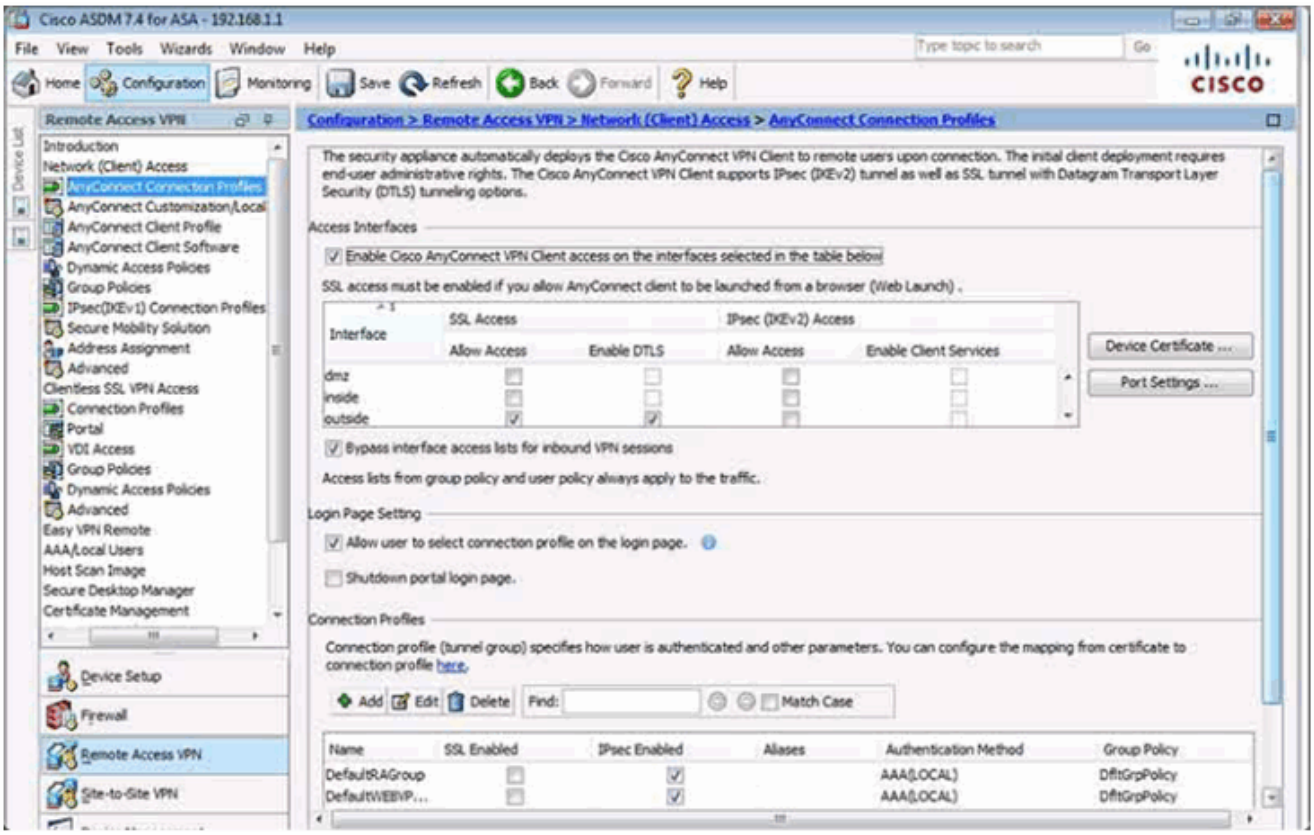


Summary Window

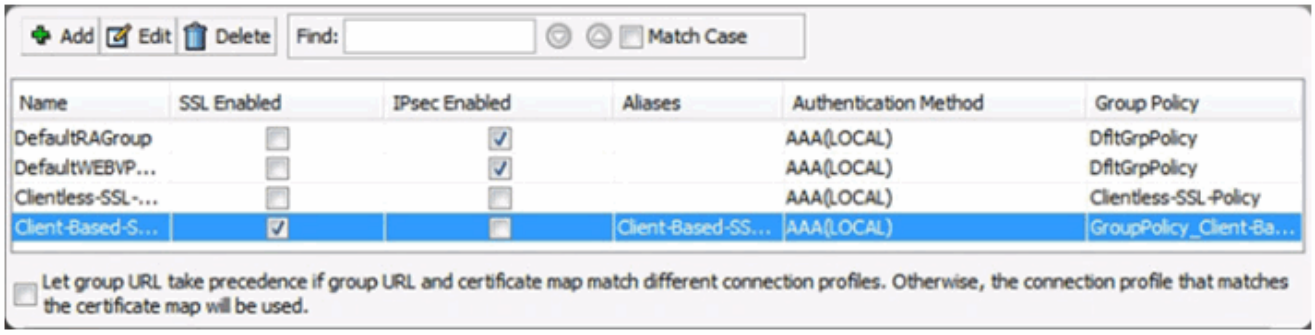


Verifying AnyConnect Connection

AnyConnect Connection Profiles Page

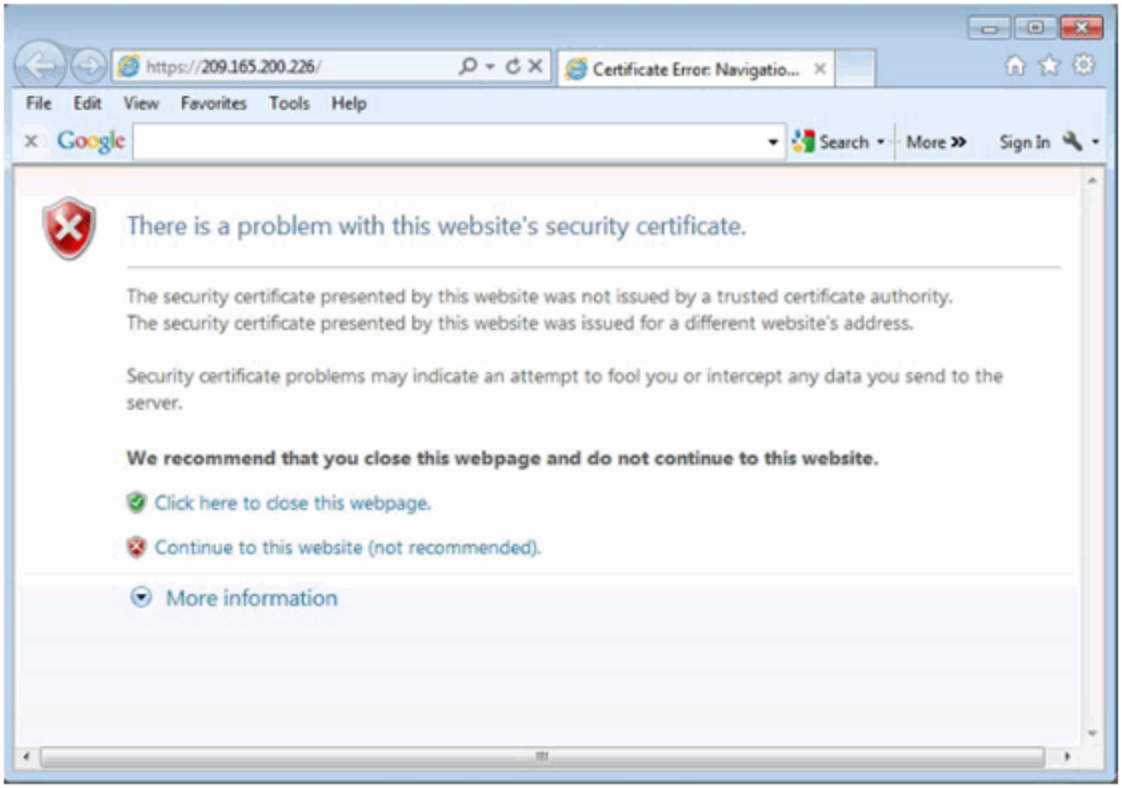


Verifying the Client-Based Configuration

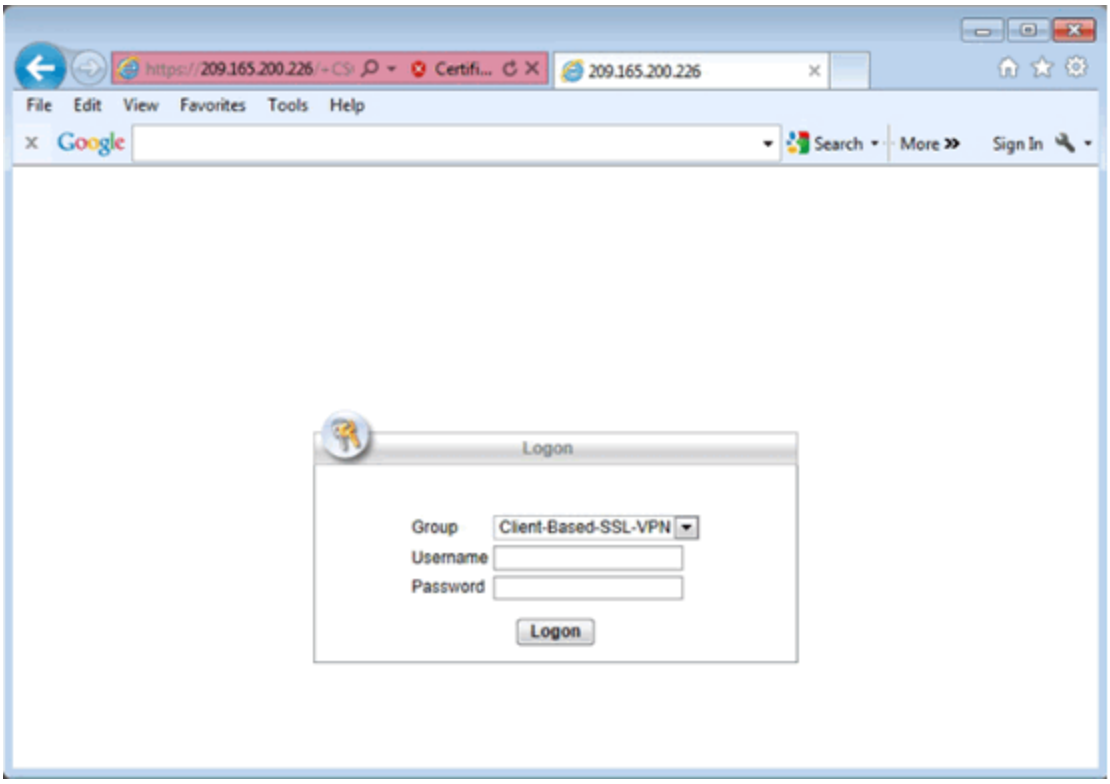


Install the AnyConnect Client

Security Certificate Window

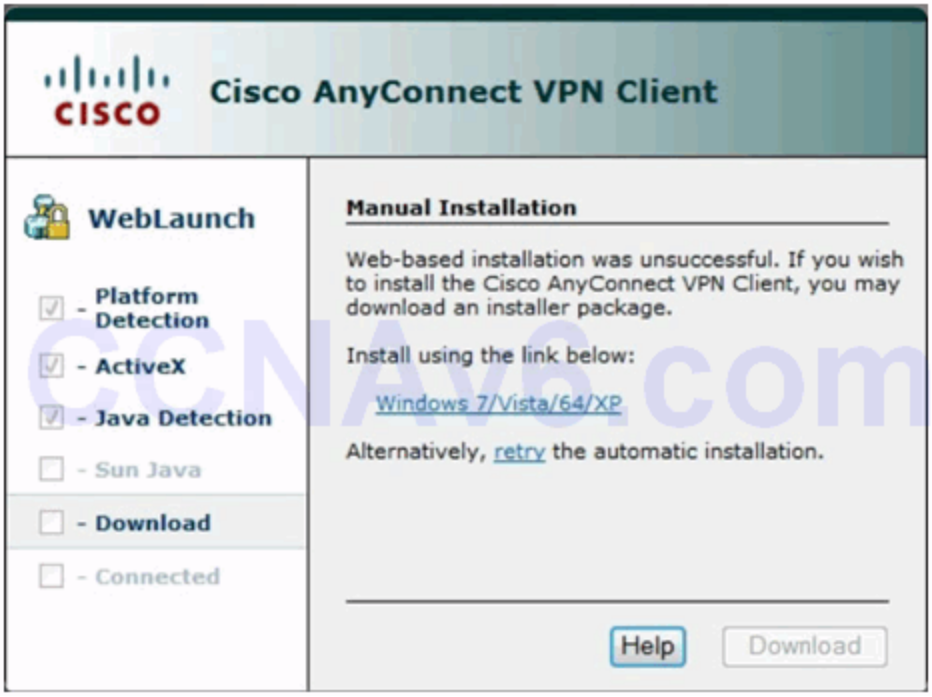


Logon Window



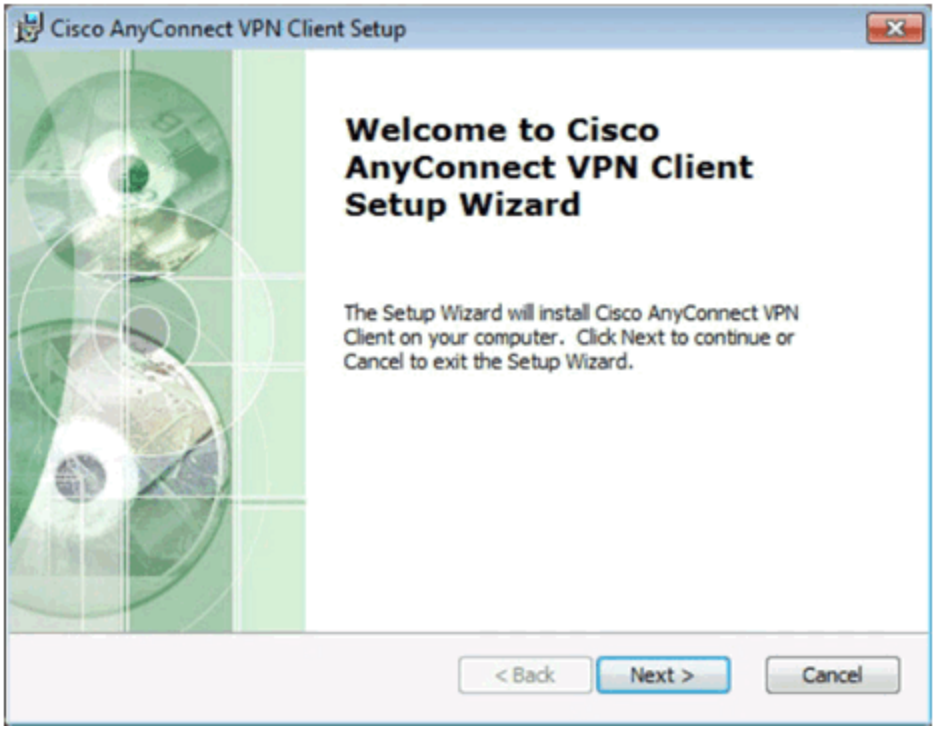
Cisco AnyConnect VPN Client Window

Manual Installation Window

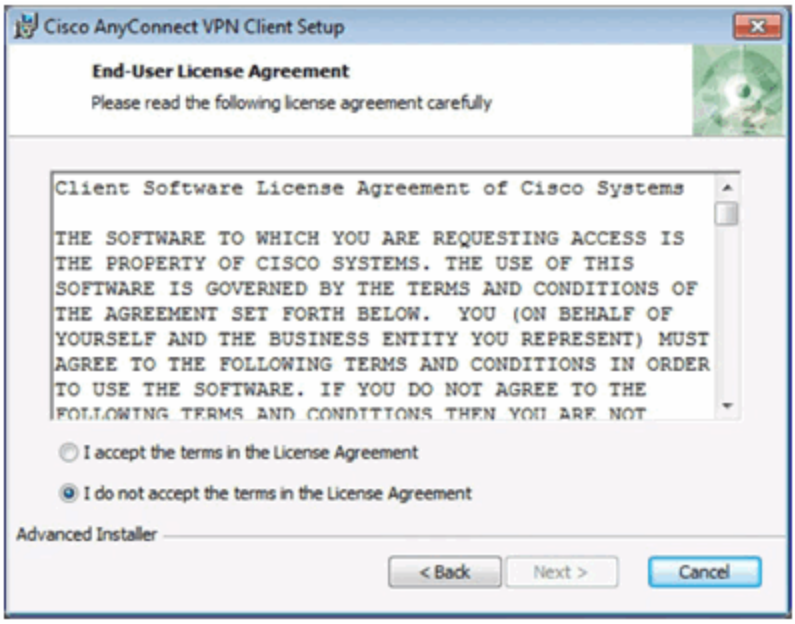


Run Installer Window

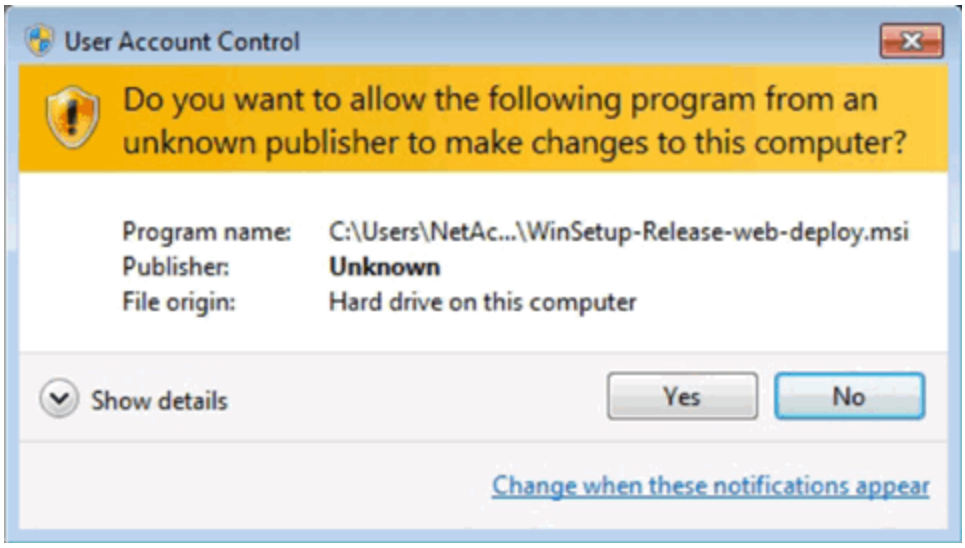
Cisco AnyConnect VPN Client Setup Window



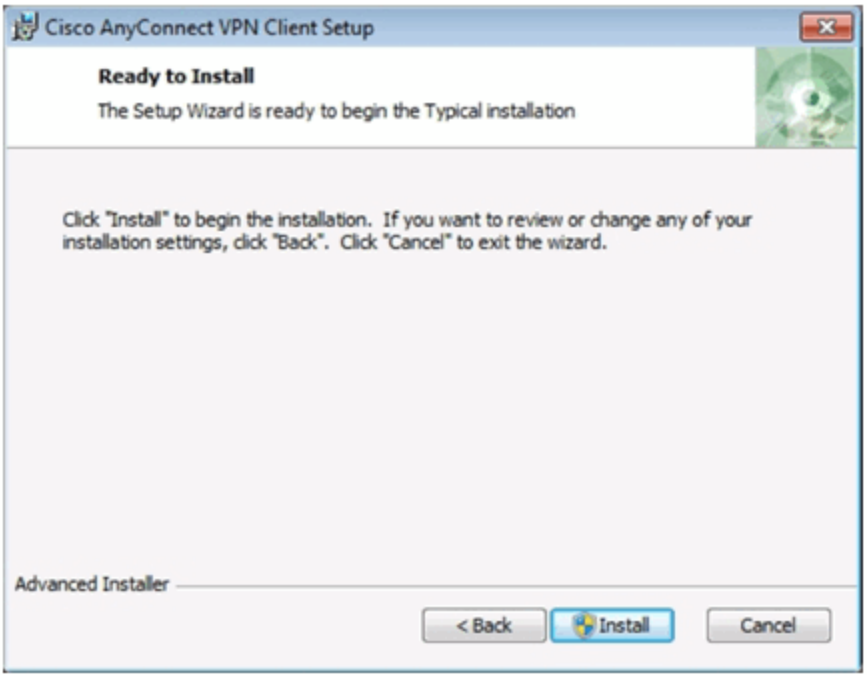
End-User Agreement Window



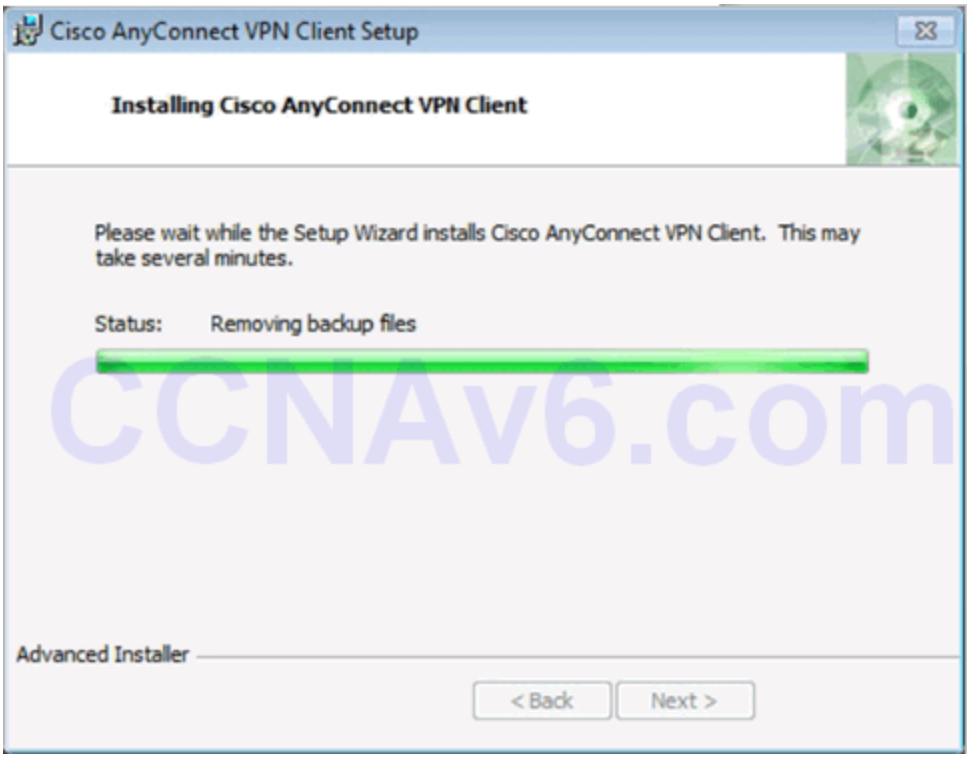
User Account Control Security Window



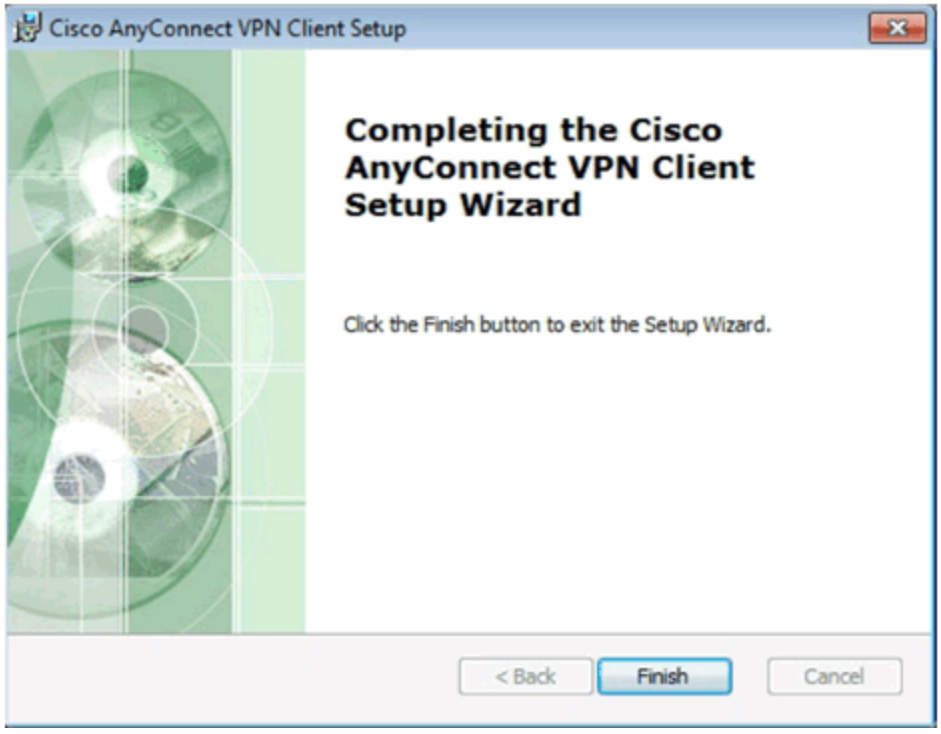
Ready to Install AnyConnect Client



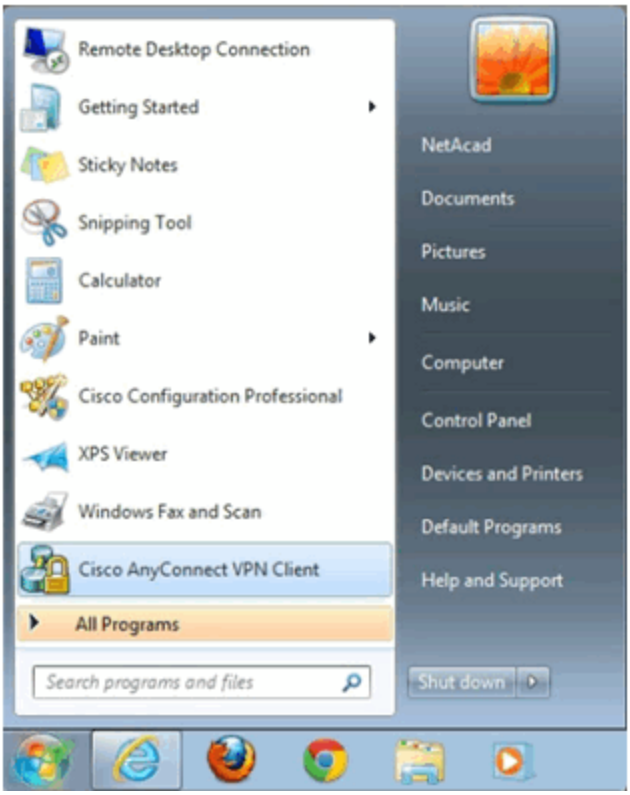
Installing the AnyConnect Client



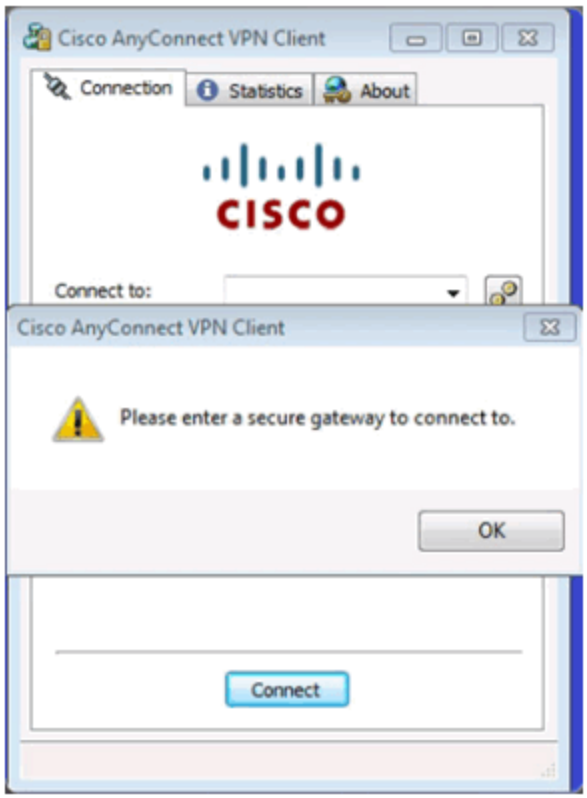
Complete Cisco AnyConnect VPN Installation



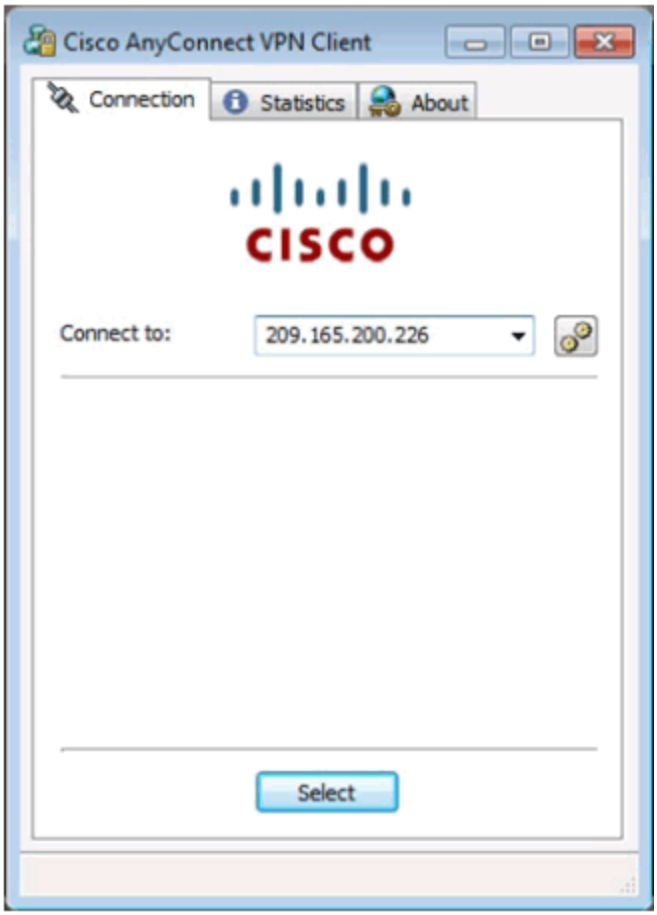
Start the Cisco AnyConnect VPN Cisco



Cisco AnyConnect VPN Client Window



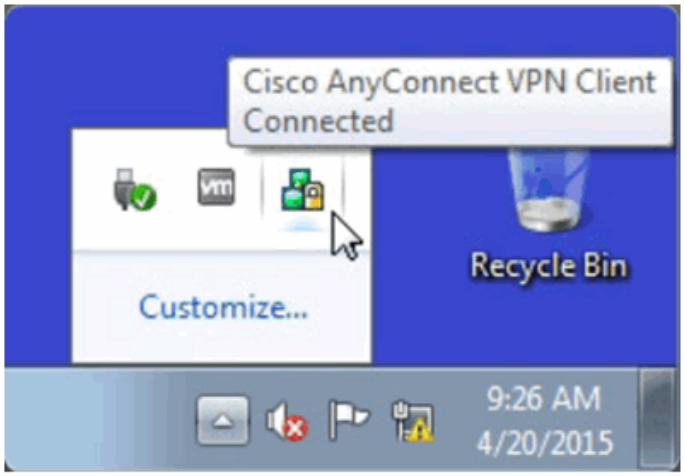
Cisco AnyConnect VPN Connect Window



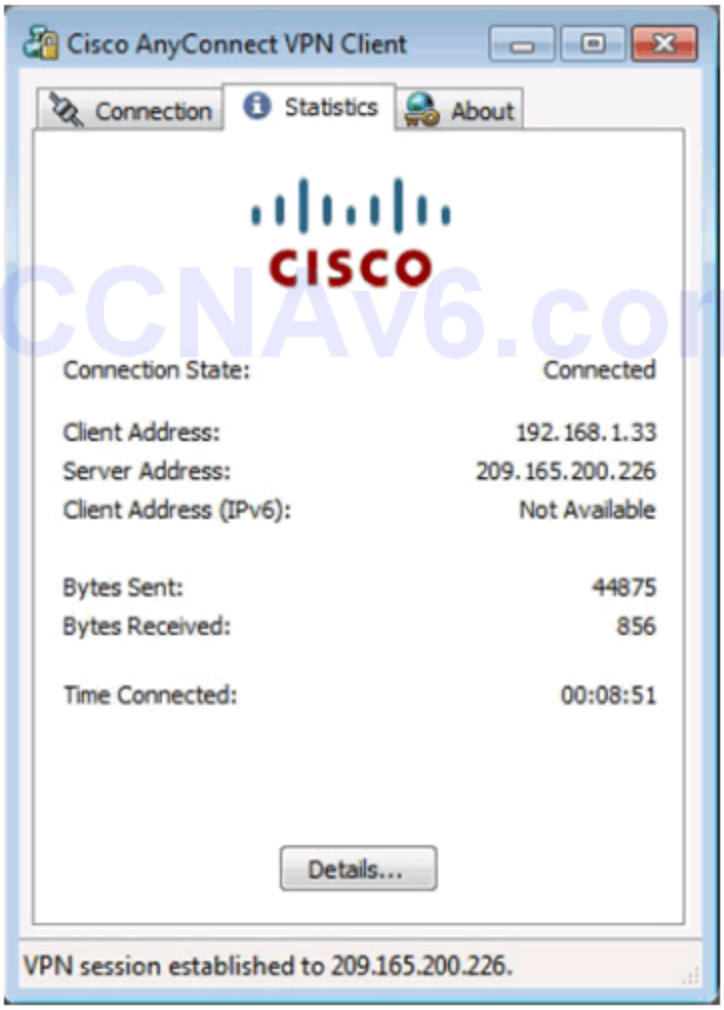
Certificate Security Warning Window

Cisco AnyConnect VPN Authentication Window

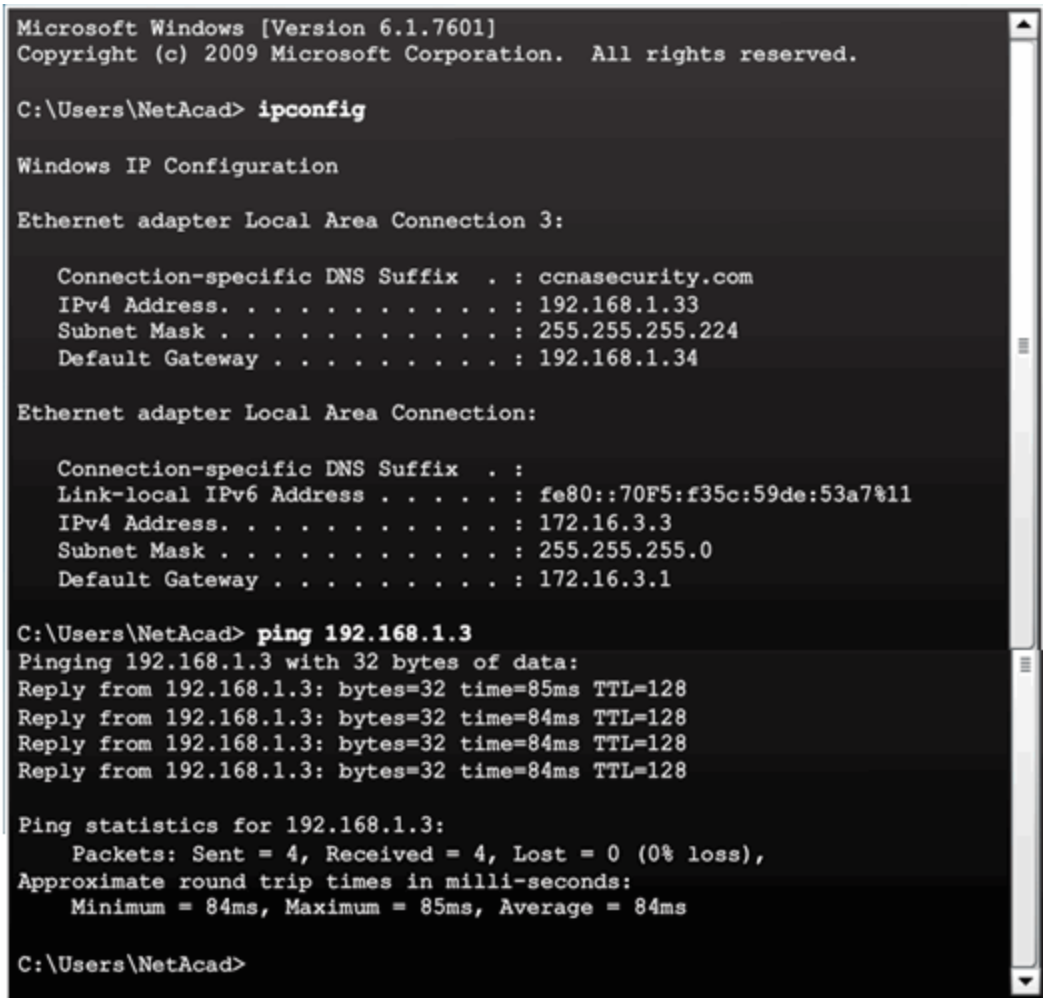
Cisco AnyConnect VPN Icon in System Tray



Cisco AnyConnect VPN Client Status



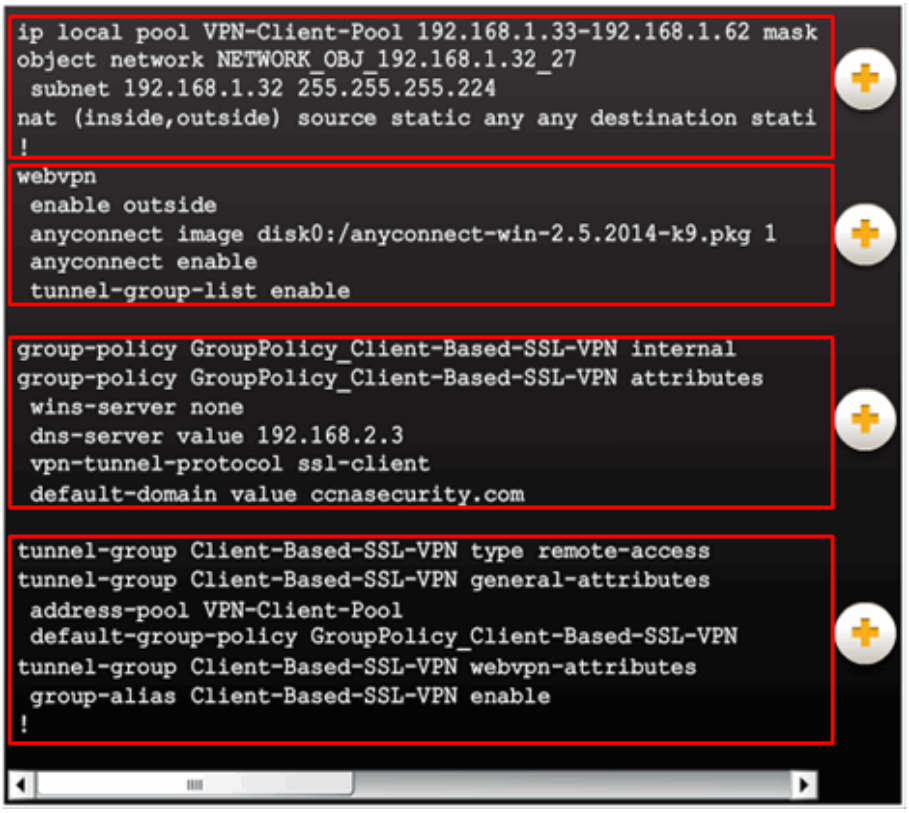
Verifying Connectivity to Internal Network



Viewing the Generated CLI Config

AnyConnect SSL VPN Configuration settings:

- NAT
- WebVPN
- Group policy
- Tunnel group



Section 10.3: Summary

Chapter Objectives:

- Implement an ASA firewall configuration.
- Configure remote-access VPNs on an ASA.

Download Slide PowerPoint (pptx):

[sociallocker id=”54558″]Click here[/sociallocker]