

Chapter 10: Advanced Cisco Adaptive Security Appliance

CCNA Security v2.0



Chapter Outline

10.0 Introduction

10.1 ASA Security Device
Manager

10.2 ASA VPN Configuration

10.3 Summary

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

The screenshot displays the Cisco ASDM 7.4 for ASA web interface. The browser window title is "Cisco ASDM 7.4 for ASA - 192.168.1.1". The interface includes a menu bar (File, View, Tools, Wizards, Window, Help) and a navigation bar with buttons for Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help. The main content area is divided into several sections:

- Device Information:** Shows general and license details for the device. Host Name: ciscoasa, ASA Version: 9.2(3), ASDM Version: 7.4(1), Firewall Mode: Routed, Total Flash: 128 MB, Device Uptime: 0d 0h 28m 10s, Device Type: ASA 5505, Context Mode: Single, Total Memory: 512 MB.
- Interface Status:** A table showing the status of the 'inside' interface. The IP Address/Mask is 192.168.1.1/24, the Line is 'up', the Link is 'up', and the Kbps is 4.
- VPN Sessions:** Shows 0 IPsec, 0 Clientless SSL VPN, and 0 AnyConnect Client sessions.
- System Resources Status:** Includes CPU Usage (79%) and Memory Usage (374 MB) graphs.
- Traffic Status:** Shows Connections Per Second Usage and 'inside' Interface Traffic Usage (Kbps) graphs.
- Latest ASDM Syslog Messages:** A section for viewing system logs, with a message indicating that ASDM logging is disabled and a button to "Enable Logging".

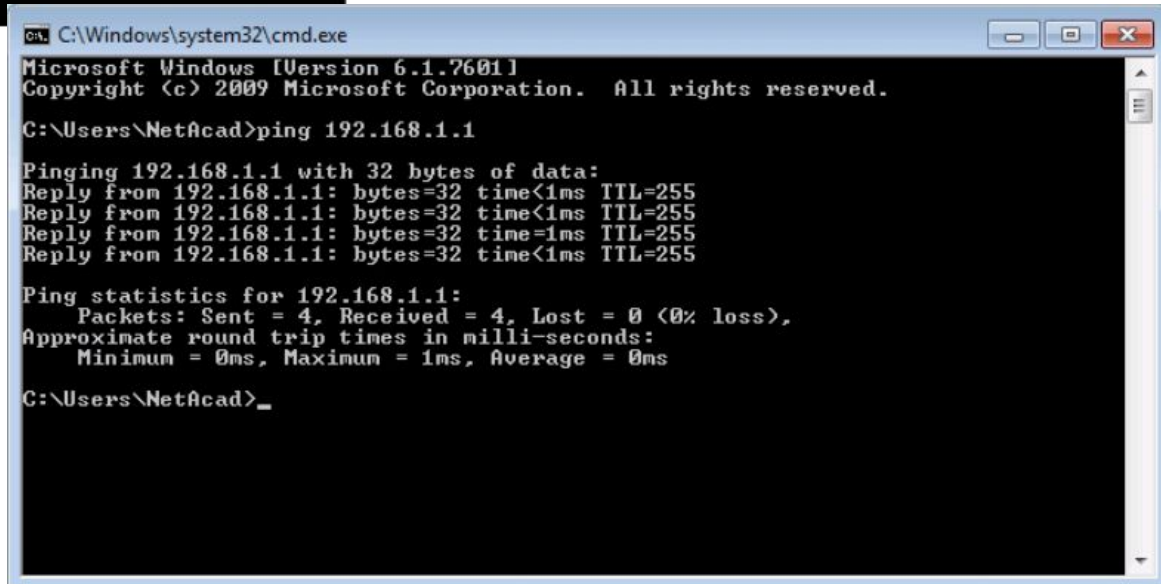
At the bottom of the interface, a status bar shows "Device configuration loaded successfully.", the user role "<admin>", the page number "15", and the timestamp "4/3/15 7:10:36 AM UTC".

Preparing for ASDM

```
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)#
```

Preparing the ASA
5505

Verify Connectivity to
the ASA



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>_
```

Starting ASDM



ASDM Security Certificate

ASDM Launch Window



Starting ASDM (Cont.)



ASDM Security
Warning - 1

ASDM Security
Warning - 2

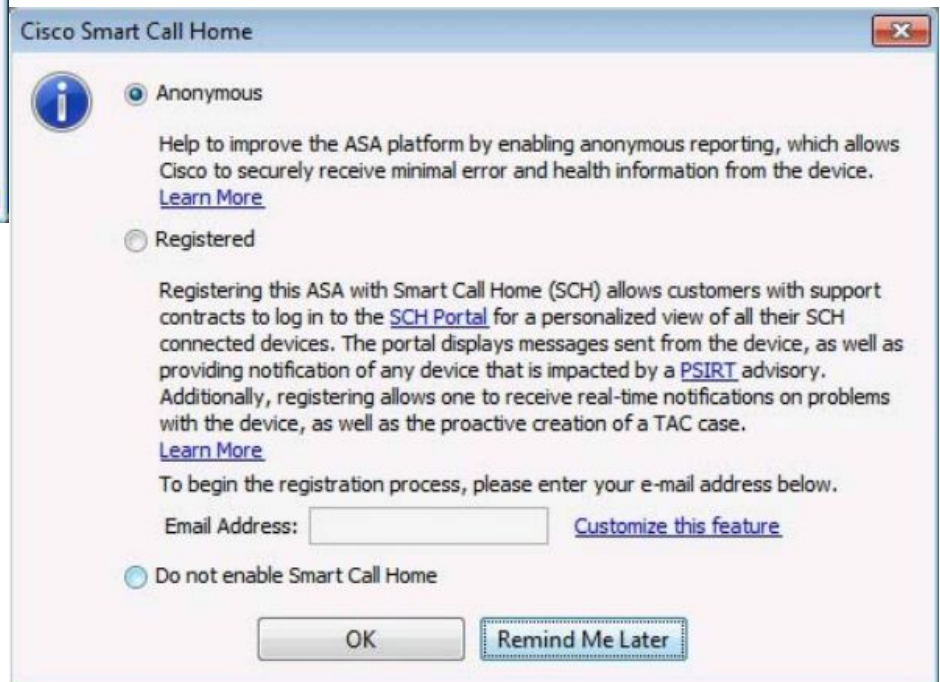


Starting ASDM (Cont.)



Smart Call Home Window

Authenticate to Use ASDM



ASDM Home Page Dashboards

ASDM Device Dashboard Page

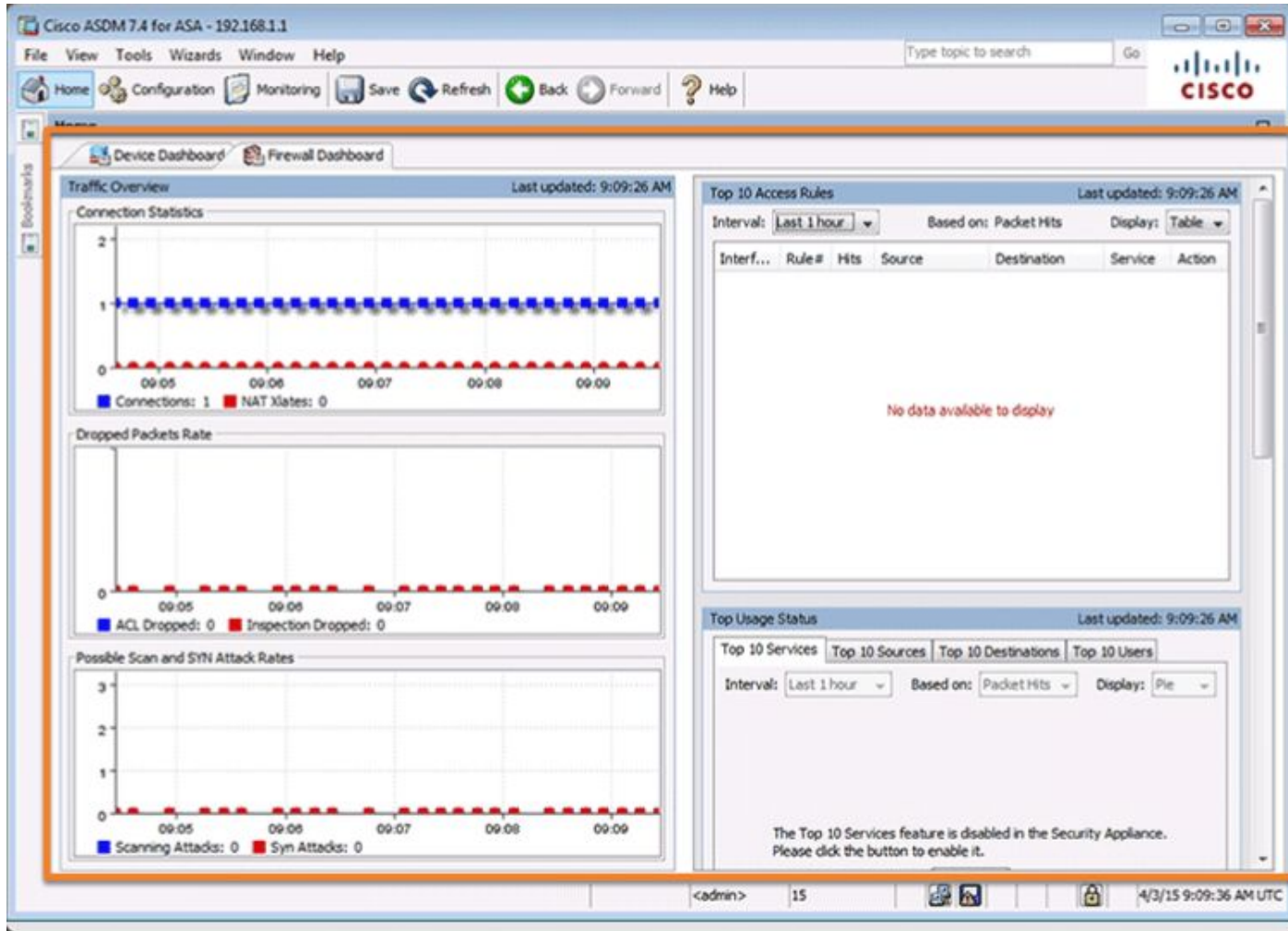
The screenshot shows the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The dashboard is divided into several sections:

- Device Information:** General tab selected. Host Name: ciscoasa, ASA Version: 9.2(3), ASDM Version: 7.4(1), Firewall Mode: Routed, Total Flash: 128 MB, Device Uptime: 0d 0h 28m 10s, Device Type: ASA 5505, Context Mode: Single, Total Memory: 512 MB.
- Interface Status:** Table showing interface 'inside' with IP Address/Mask 192.168.1.1/24, Line up, Link up, and Kbps 4.
- VPN Sessions:** IPsec: 0, Clientless SSL VPN: 0, AnyConnect Client: 0.
- System Resources Status:** CPU Usage (percent) graph showing 7% usage. Memory Usage (MB) graph showing 256 MB usage.
- Traffic Status:** Connections Per Second Usage graph showing 0 connections. 'inside' Interface Traffic Usage (Kbps) graph showing 0 Kbps.
- Latest ASDM Syslog Messages:** ASDM logging is disabled. To enable ASDM logging with informational level, click the button below. [Enable Logging]

Device configuration loaded successfully. <admin> 15 4/3/15 7:10:36 AM UTC

ASDM Home Page Dashboards (Cont.)

ASDM Firewall Dashboard Page



ASDM Page Elements

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The interface is annotated with four callout boxes on the left side, each with an orange arrow pointing to a specific element:

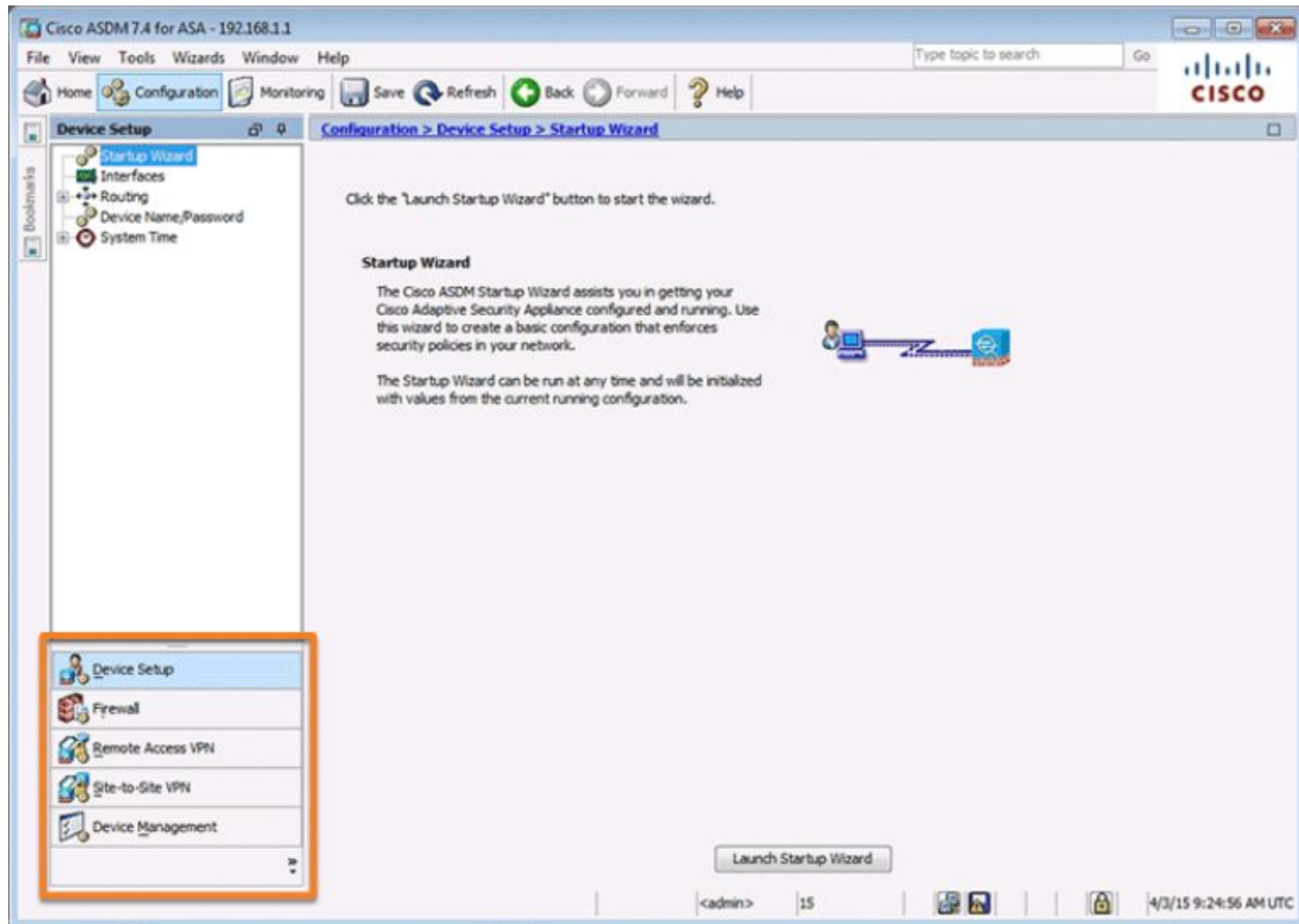
- Menu Bar:** Points to the top menu bar containing File, View, Tools, Wizards, Window, and Help.
- Tool Bar:** Points to the toolbar below the menu bar, featuring icons for Home, Configuration, Monitoring, and Security.
- Device List Button:** Points to the 'Device List' button located on the left sidebar.
- Status Bar:** Points to the status bar at the bottom of the window, which displays the message 'Device configuration loaded successfully.'

The main content area of the interface includes the following sections:

- Home:** Contains 'Device Dashboard' and 'Firewall Dashboard' buttons.
- Device Information:** A tabbed interface with 'General' and 'License' tabs. The 'General' tab shows:
 - Host Name: **ciscoasa**
 - ASA Version: **9.2(3)**
 - ASDM Version: **7.4(1)**
 - Firewall Mode: **Routed**
 - Total Flash: **128 MB**
- VPN Sessions:** Shows 'IPsec: 0', 'Clientless SSL VPN: 0', and 'AnyConnect: 0'.
- System Resources Status:** Includes two graphs:
 - CPU Usage (percent):** A bar chart showing 7% usage at 07:10:36.
 - Memory Usage (MB):** A bar chart showing 214MB usage.
- Latest ASDM Syslog Messages:** A section for viewing system logs.

ASDM Configuration and Monitoring Views

Configuration View



ASDM Configuration and Monitoring Views (Cont.)

Monitoring View

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The main window shows the 'Monitoring > Interfaces > ARP Table' view. The ARP Table contains one entry for the 'inside' interface.

Interface	IP Address	MAC Address	Proxy Arp
inside	192.168.1.3	0050.50be.73e1	No

Each row represents one ARP table entry.

Buttons: Refresh, Clear Dynamic ARP Entries

Bottom status bar: Last Updated: 4/11/15 7:35:17 AM, <admin> | 15, 4/3/15 9:28:06 AM UTC

Configure and Access on an ASA5505



Video | Configure and Access ASDM on an ASA5505

Topic 10.1.2: ASDM Wizard Menu



ASDM Wizards

The screenshot displays the Cisco ASDM 7.4 for ASA interface. The title bar reads "Cisco ASDM 7.4 for ASA - 192.168.1.1". The menu bar includes "File", "View", "Tools", "Wizards", "Window", and "Help". The "Wizards" menu is open, showing the following options:

- Startup Wizard...
- VPN Wizards
- High Availability and Scalability Wizard...
- Unified Communication Wizard...
- ASDM Identity Certificate Wizard...
- Packet Capture Wizard...

The interface also shows a "Home" button, a "Device List" sidebar, and a "Device Information" section with the following details:

Host Name:	ciscoasa	Device Uptime:	0d 0h 37m 29s
ASA Version:	9.2(3)	Device Type:	ASA 5505
ASDM Version:	7.4(1)	Context Mode:	Single
Firewall Mode:	Routed	Total Memory:	512 MB
Total Flash:	128 MB		

The Startup Wizard

Cisco ASDM 7.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard Starting Point (Step 1 of 9)

Choose a starting point for the wizard.

- Modify existing configuration
- Reset configuration to factory defaults

Configure the IP address of the management inter...

IP Address:

Subnet Mask:

< Back Next > Finish Cancel Help

Startup Wizard Basic Configuration Window

Startup Wizard Starting Point Window

Cisco ASDM 7.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard Basic Configuration (Step 2 of 9)

Configure the device for Teleworker usage

Enter the host name and the domain name of the ASA. If your Internet Service Provider (ISP) requires that your host uses DHCP, you may need to use the device name supplied by the ISP as the host name of the ASA.

ASA Host Name:

Domain Name:

Privileged Mode (Enable) Password

The privileged mode (enable) password is required to administer the ASA using ASDM or the Command Line Interface (CLI).

Change privileged mode (enable) password

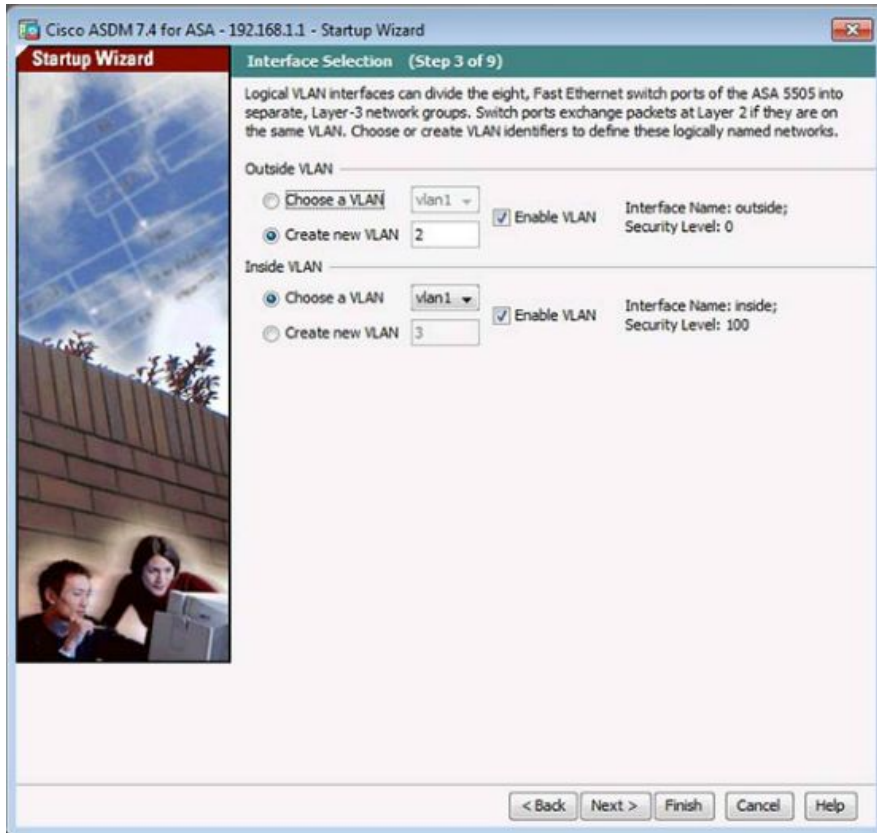
Old Password:

New Password:

Confirm New Password:

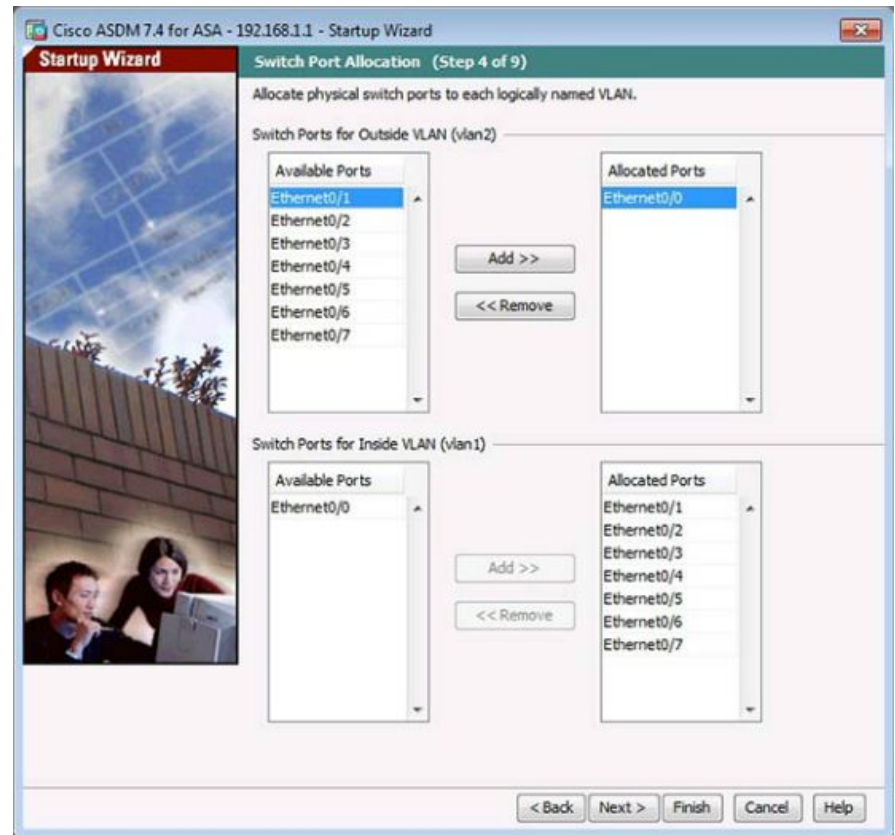
< Back Next > Finish Cancel Help

The Startup Wizard (Cont.)



Startup Wizard Switch Port Allocation Window

Startup Wizard Interface Selection Window



The Startup Wizard (Cont.)

Cisco ASDM 7.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Interface IP Address Configuration (Step 5 of 9)

Assign IP addresses to each named VLAN.

Outside IP Address

Use the following IP address

IP Address: 209.165.200.226 Mask: 255.255.255.248

Use DHCP Obtain default route using DHCP

Use PPPoE

Inside IP Address

Use the following IP address

IP Address: 192.168.1.1 Mask: 255.255.255.0

Use DHCP Obtain route using DHCP

Use PPPoE

< Back Next > Finish Cancel Help

Startup Wizard DHCP Server Window

Startup Wizard Interface IP Address Configuration Window

Cisco ASDM 7.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

DHCP Server (Step 6 of 9)

The ASA can act as a DHCP server and provide IP addresses to the hosts on your inside network. To configure a DHCP server on an interface other than the inside interface, go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.

Enable DHCP server on the inside interface

DHCP Address Pool

Starting IP Address: 192.168.1.10 Ending IP Address: 192.168.1.41

DHCP Parameters

DNS Server 1: DNS Server 2:

WINS Server 1: WINS Server 2:

Lease Length: 1800 sec Ping Timeout: ms

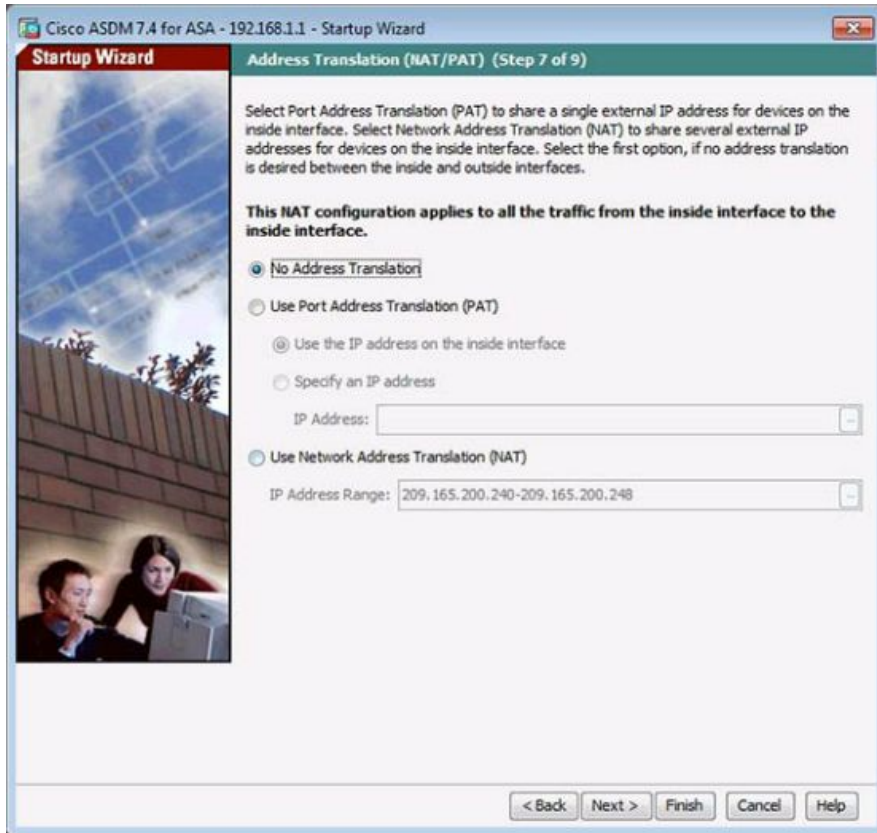
Domain Name: cnasecurity.com

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.

Enable auto-configuration from interface:

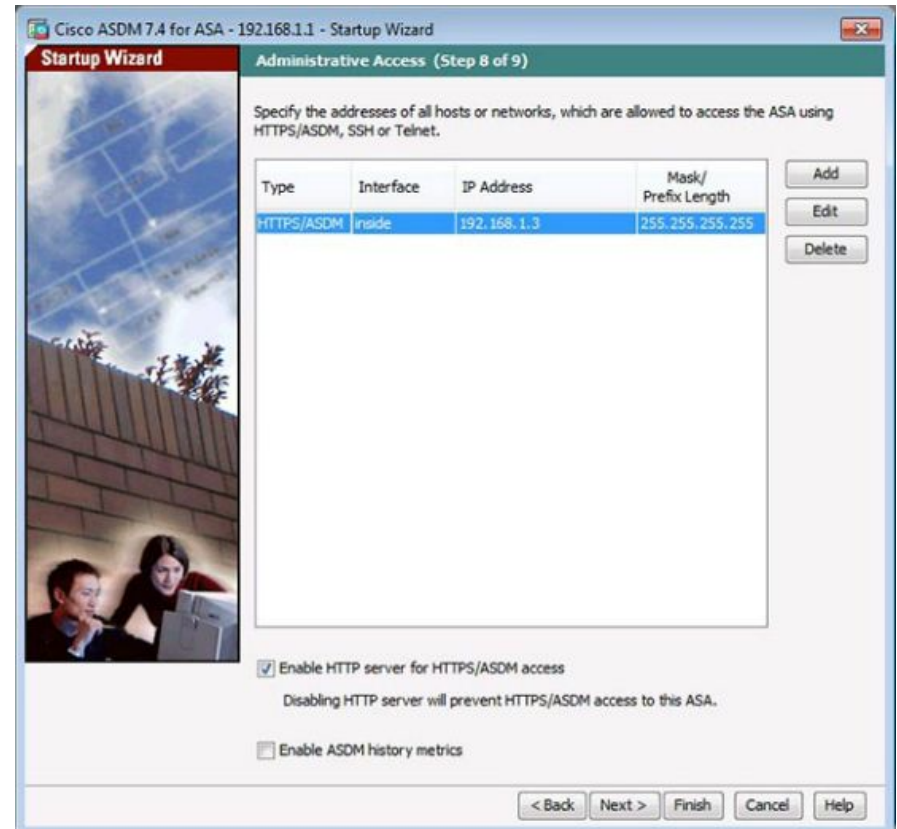
< Back Next > Finish Cancel Help

The Startup Wizard (Cont.)



Startup Wizard Administrative Access Window

Startup Wizard Address Translation (NAT/PAT) Window

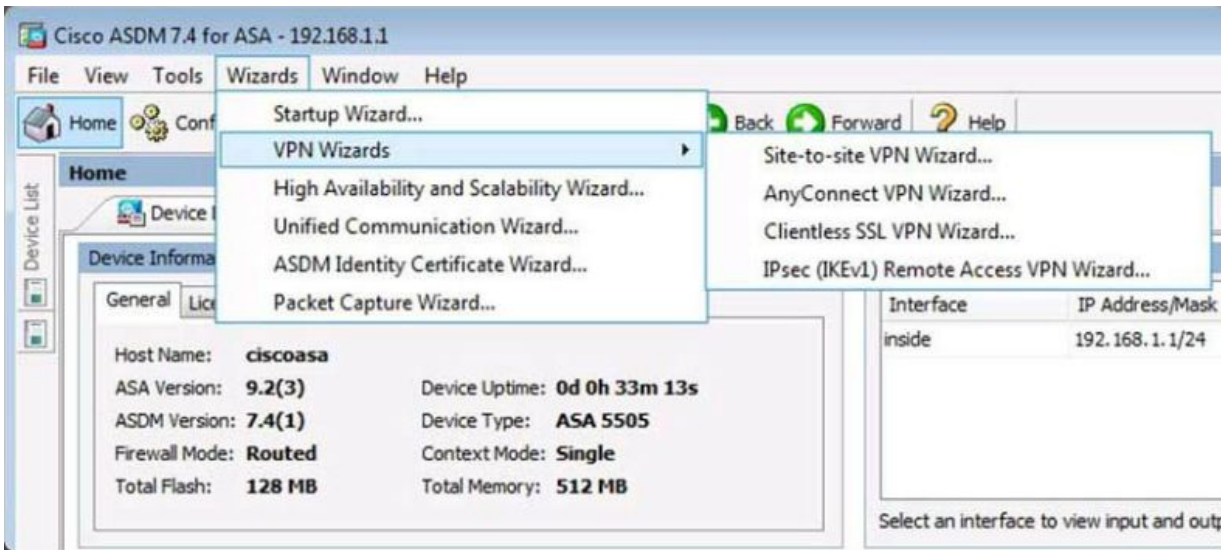


The Startup Wizard (Cont.)

Startup Wizard Summary Window



Different Types of VPN Wizards

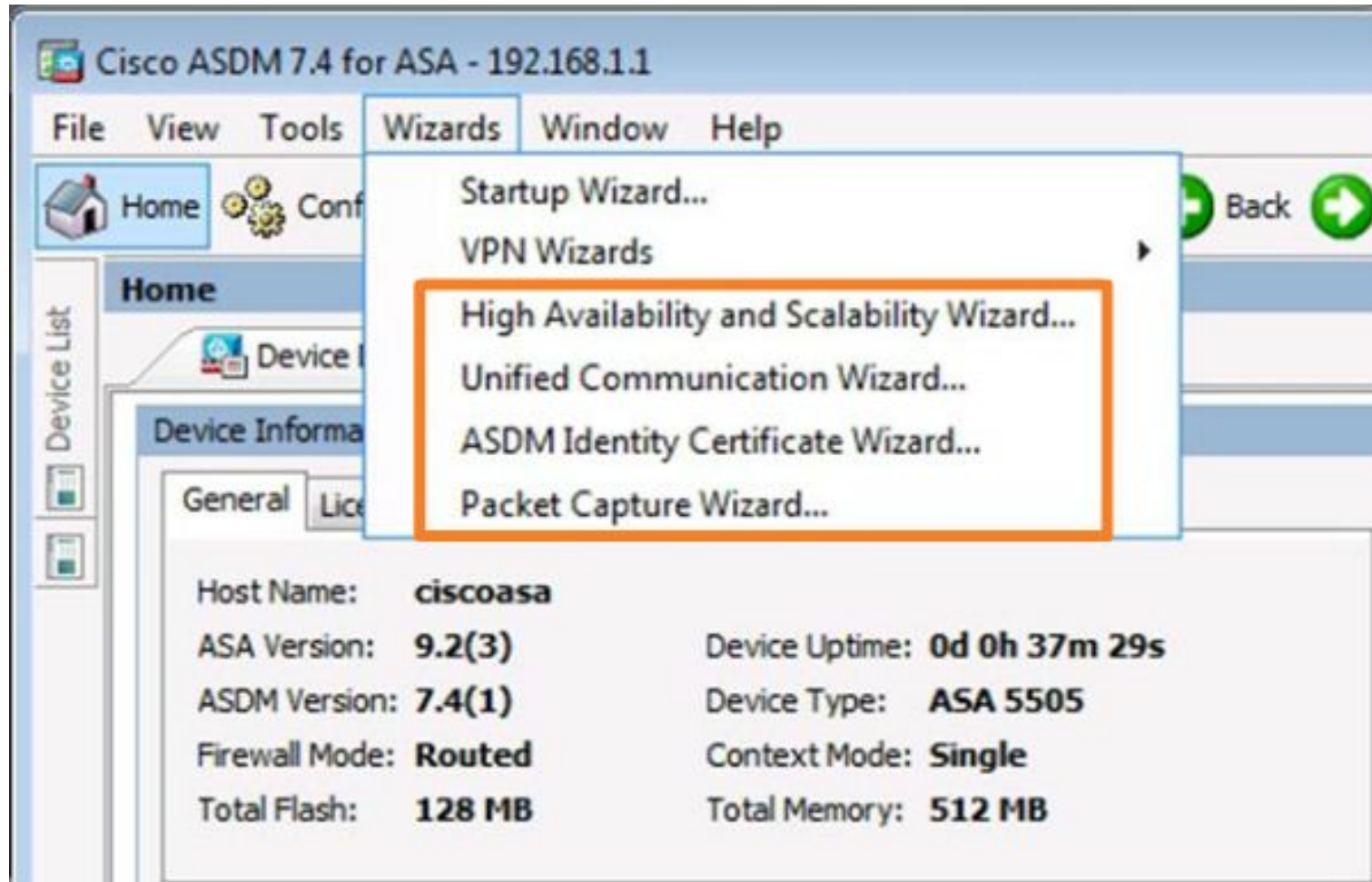


ASDM VPN Wizards

ASDM Remote Access VPN Assistant



Other Wizards



Topic 10.1.3: Configuring Management Settings and Services



Configuring Settings in ASDM

Configuration Device Setup Tab

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The top menu bar includes File, View, Tools, Wizards, Window, and Help. Below the menu bar is a navigation bar with icons for Home, Configuration, and Monitoring, along with buttons for Save, Refresh, Back, Forward, and Help. The Configuration tab is highlighted with an orange box. The left sidebar shows the Device List with the following items: Startup Wizard (highlighted with a blue box), Interfaces, Routing, Device Name/Password, and System Time. The main content area shows the breadcrumb path Configuration > Device Setup > Startup Wizard and the instruction: Click the "Launch Startup Wizard" button to start the wizard. Below this is the heading "Startup Wizard" and the text: The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that performs...

Configuring Settings in ASDM (Cont.)

Configuration Device Management Tab

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward

Device Management

Device List

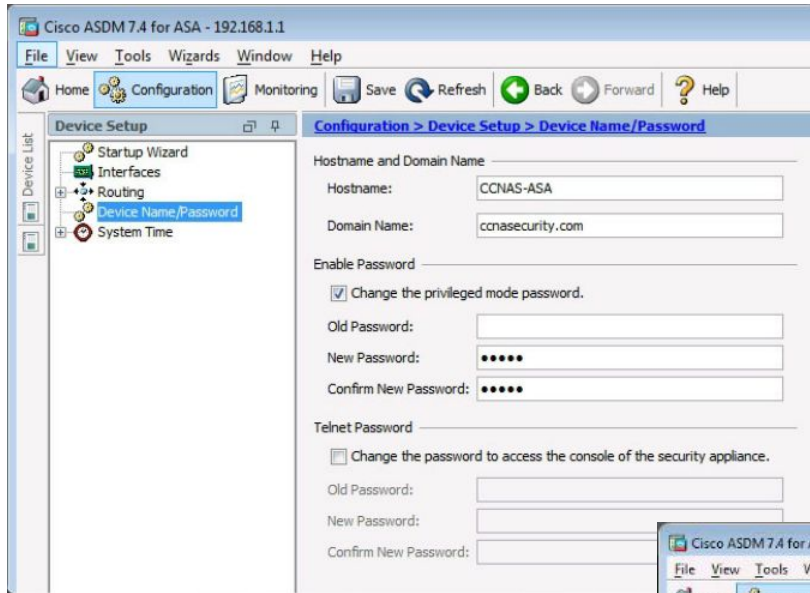
- Management Access
- Licensing
- System Image/Configuration
- Logging
- Smart Call-Home
- Cloud Web Security
- Users/AAA
- Certificate Management
- DHCP
- DNS
- Advanced

Configuration > Device Management > Manage

This section contains the following items:

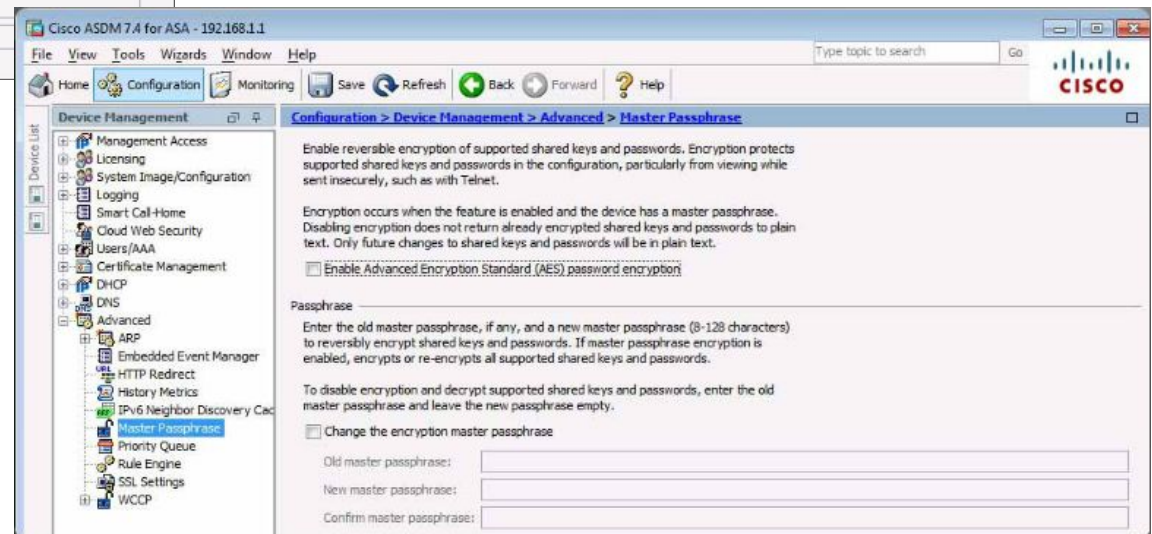
- [ASDM/HTTPS/Telnet/SSH](#)
- [Command Line \(CLI\)](#)
- [File Access](#)
- [ICMP](#)
- [Management Interface](#)
- [Management Session Quota](#)
- [SNMP](#)
- [Management Access Rules](#)

Configuring Basic Settings in ASDM



Configuring Hostname, Domain Name, and Enable Password

Configuring a Master Passphrase



Configuring Basic Settings in ASDM (Cont.)

Configuring Legal Notification

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Device Management > Management Access > Command Line (CLI) > Banner. The main content area contains the following text: "Configure the Session (exec), Login or Message-of-The-Day (motd) banners. You can use \$(hostname) and \$(domain) tokens to specify the hostname and domain name of the device." Below this text are four large text input fields for configuring the banners: "Session (exec) Banner", "Login Banner", "Message-of-The-Day (motd) Banner", and "ASDM Banner". The left sidebar shows a tree view of configuration categories, with "Banner" selected under "Command Line (CLI)".

Configuring Interfaces in ASDM

Configuring Interfaces

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Device Setup > Interfaces". The left sidebar shows the "Device Setup" tree with "Interfaces" selected. The main content area shows a table of interfaces with the following data:

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/0, Ethernet0/1, Et...	Yes	100	192.168.1.1	255.255.255.0	

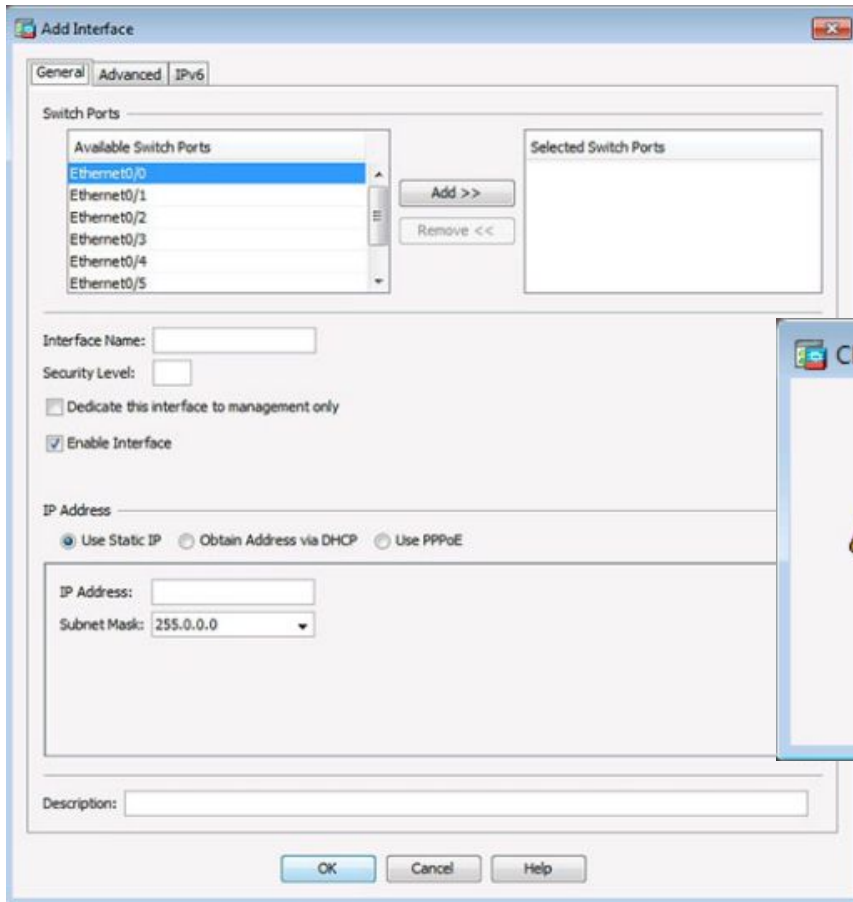
Below the table, there are two checkboxes:

- Enable traffic between two or more interfaces which are configured with same security levels
- Enable traffic between two or more hosts connected to the same interface

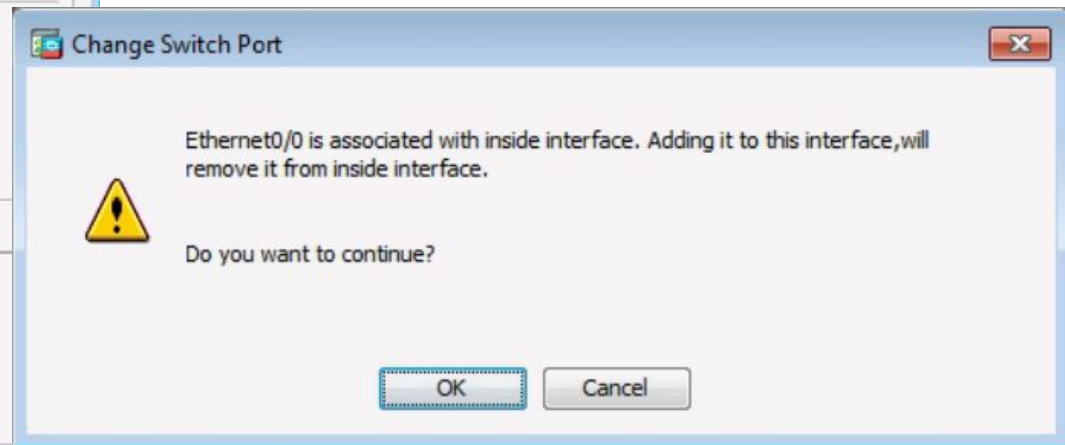
At the bottom of the window, there are "Apply" and "Reset" buttons.

Configuring Interfaces in ASDM (Cont.)

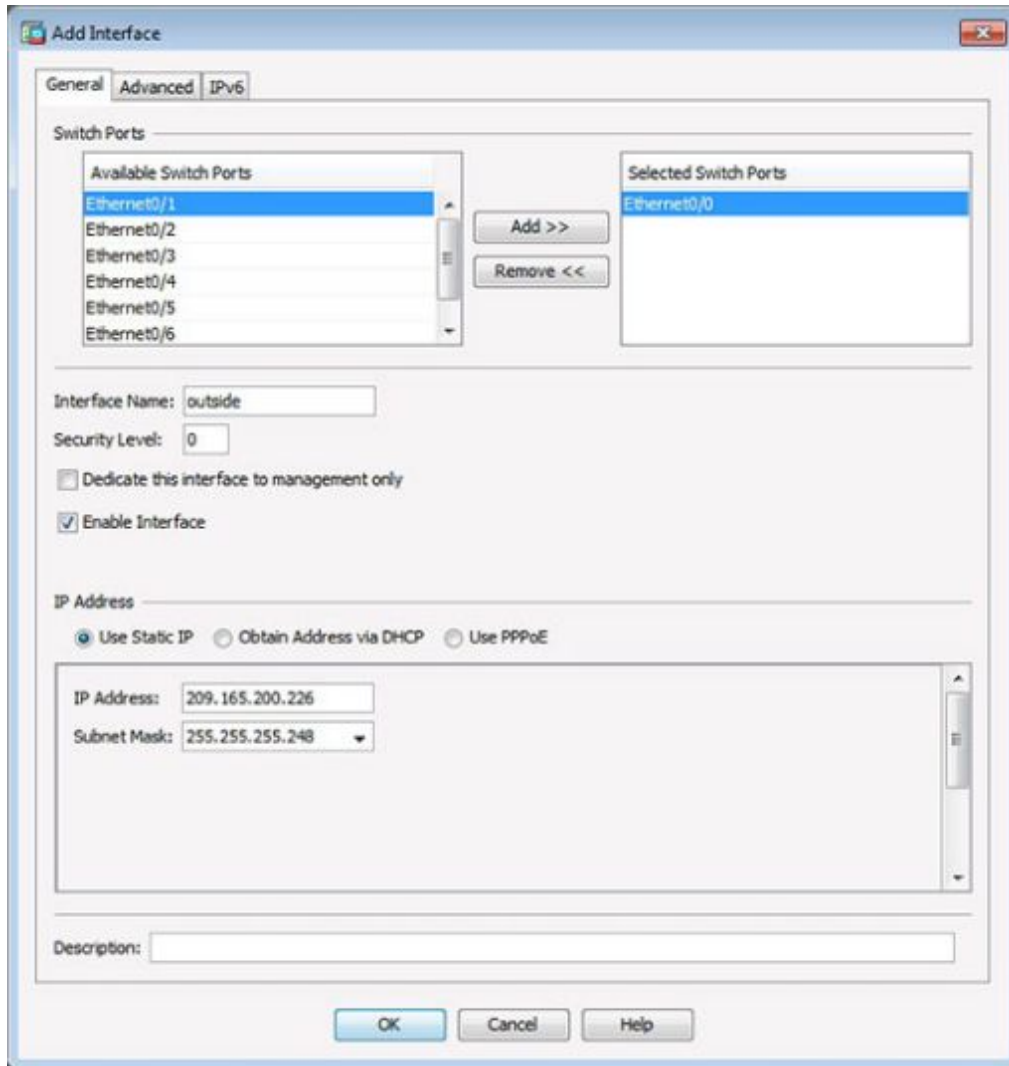
Adding an Outside Interface



Change Switch Port Window



Configuring Interfaces in ASDM (Cont.)



Adding an Outside Interface

Configuring Interfaces in ASDM (Cont.)

Advanced Outside Interface Settings

Add Interface

General | **Advanced** | IPv6

MTU: VLAN ID:

MAC Address Cloning _____
Enter MAC addresses for the active and standby interfaces in hexadecimal format. Example: 0123.4567.89AB.

Active MAC Address: Standby MAC Address:

Block Traffic _____
Block traffic from this interface to:

Updated Interface Page

Configuration > Device Setup > Interfaces

Interfaces | **Switch Ports**



Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/0, Ethernet0/1, Et...	Yes	100	192.168.1.1	255.255.255.0	
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248	

Configuring Interfaces in ASDM (Cont.)

Verifying Interfaces

Configuration > Device Setup > Interfaces

Interfaces Switch Ports

Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed	Edit
Ethernet0/0	No	2	outside	Access	No	auto	auto	
Ethernet0/1	Yes	1	inside	Access	No	auto	auto	
Ethernet0/2	No	1	inside	Access	No	auto	auto	
Ethernet0/3	No	1	inside	Access	No	auto	auto	
Ethernet0/4	No	1	inside	Access	No	auto	auto	
Ethernet0/5	No	1	inside	Access	No	auto	auto	
 Ethernet0/6	No	1	inside	Access	No	auto	auto	
 Ethernet0/7	No	1	inside	Access	No	auto	auto	

Configuring Interfaces in ASDM (Cont.)

Switch Port: Ethernet0/0 Enable SwitchPort

Mode and VLAN IDs

Access
VLAN ID: 2

Trunk
VLAN IDs:

Configure Native VLAN Native VLAN ID:

VLAN ID must be in the range of 1 to 4090. For access mode, only one VLAN ID is allowed. For trunk mode, up to 20 comma-separated VLAN IDs can be entered.

Isolated

Isolated
An isolated/protected port does not forward any traffic to any other isolated port within the same VLAN

Dupl... auto Speed: auto

OK Cancel Help

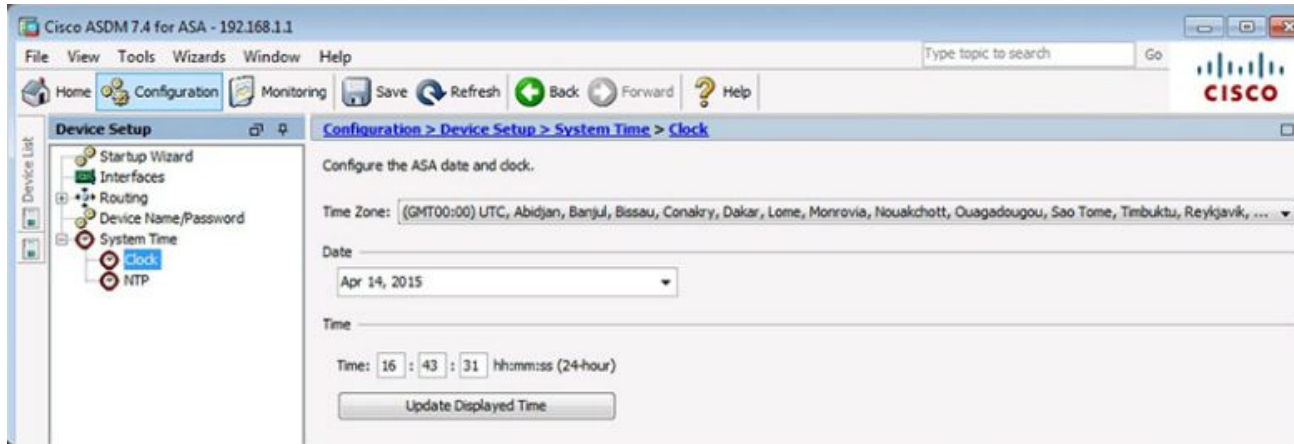
Enable Switch Ports

Apply Configuration

Name	Switch Ports	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Restrict Traffic flow
inside	Ethernet0/1, Ethernet0/2, Et...	Yes	100	192.168.1.1	255.255.255.0	
outside	Ethernet0/0	Yes	0	209.165.200.226	255.255.255.248	

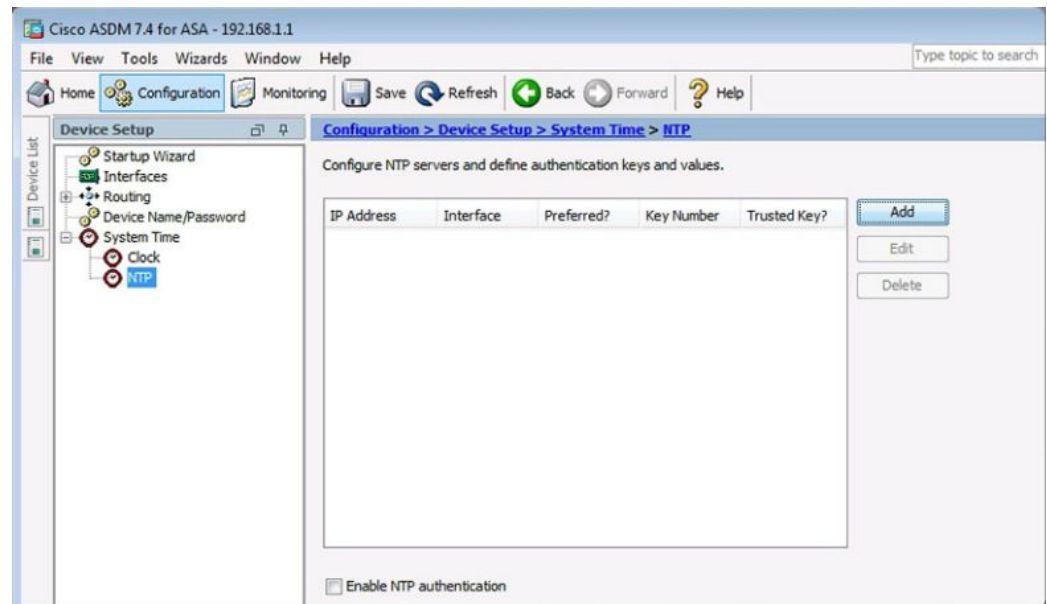
Add Edit Delete

Configuring the System Time in ASDM

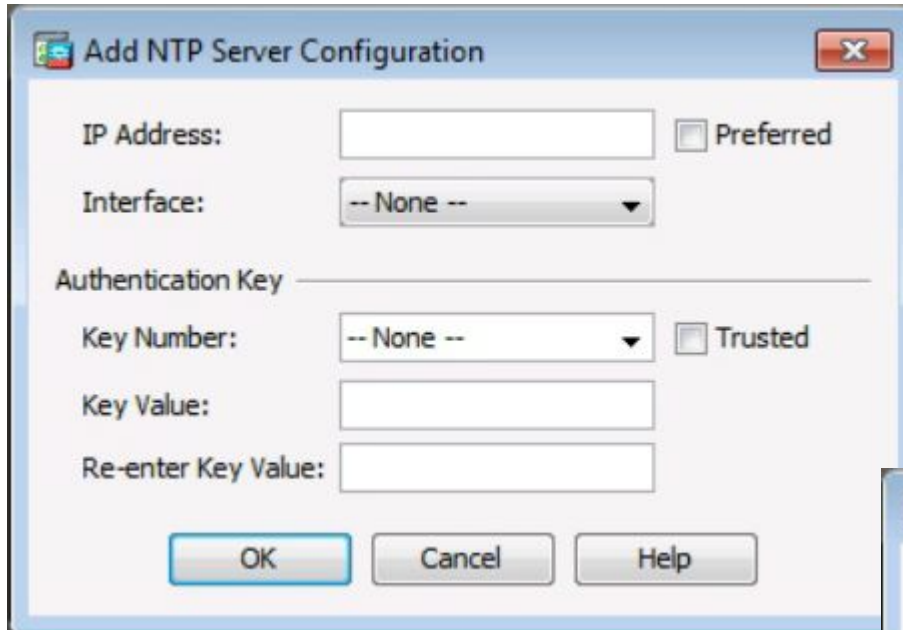


Manually Change the System Time

Use NTP to Change the System Time



Configuring the System Time in ASDM (Cont.)



Add NTP Server Configuration

IP Address: Preferred

Interface:

Authentication Key

Key Number: Trusted

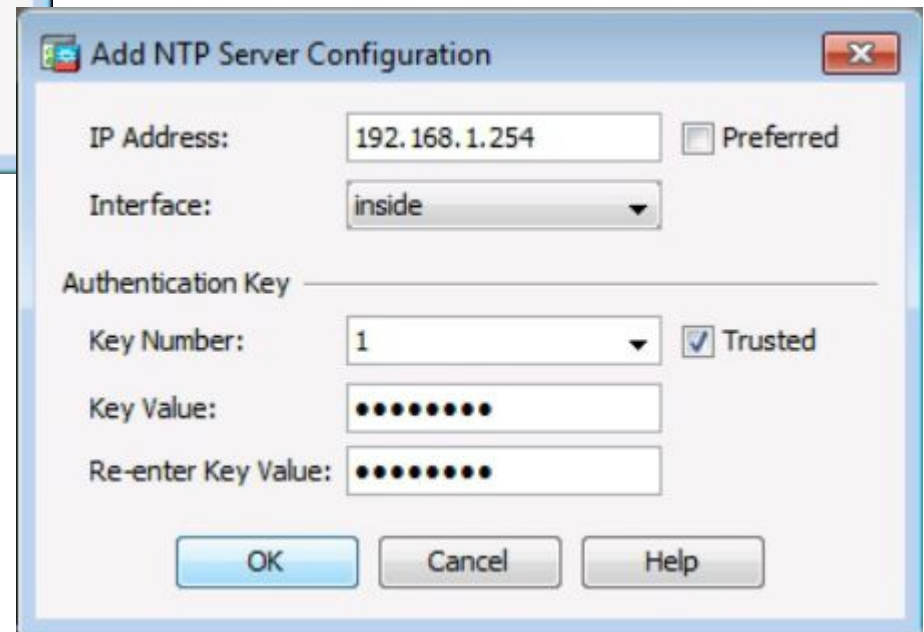
Key Value:

Re-enter Key Value:

OK Cancel Help

Configure an NTP Server

Add an NTP Server



Add NTP Server Configuration

IP Address: Preferred

Interface:

Authentication Key

Key Number: Trusted

Key Value:

Re-enter Key Value:

OK Cancel Help

Configuring the System Time in ASDM (Cont.)

Apply the Configuration

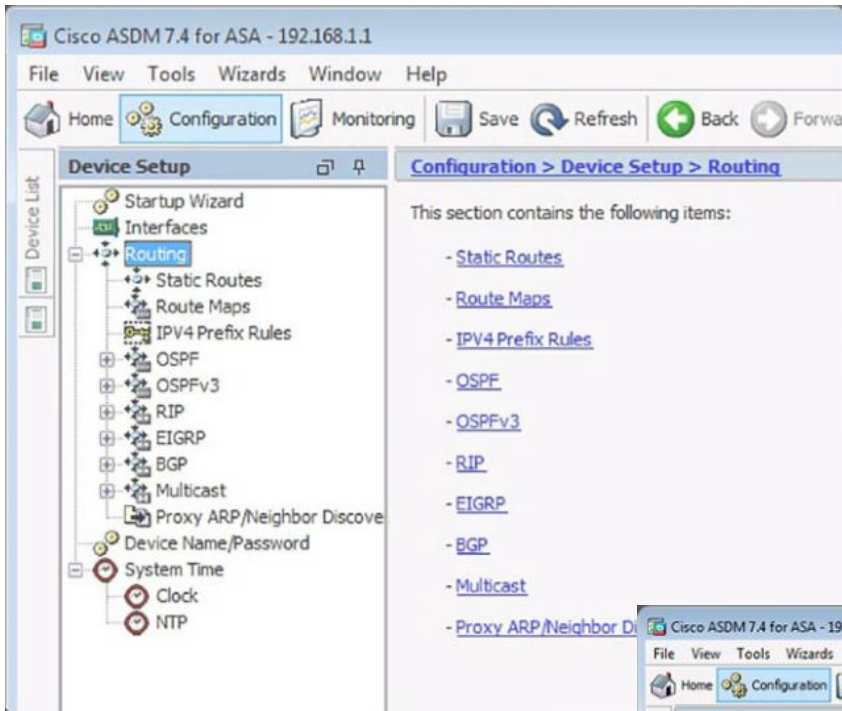
[Configuration](#) > [Device Setup](#) > [System Time](#) > [NTP](#)

Configure NTP servers and define authentication keys and values.

IP Address	Interface	Preferred?	Key Number	Trusted Key?
192.168.1.254	inside	No	1	Yes

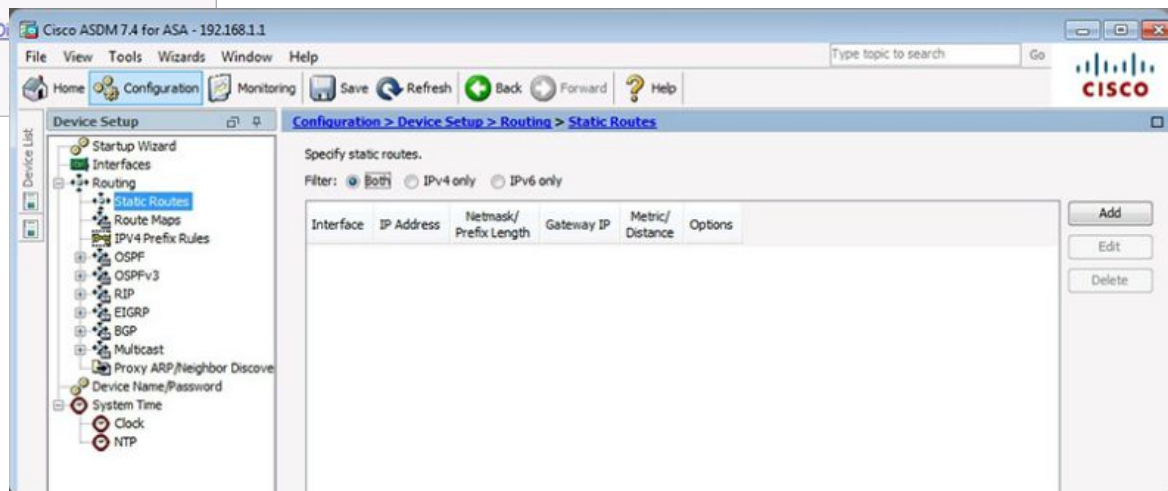
Enable NTP authentication

Configuring Routing in ASDM



Configuring Routing

Configuring a Default Static Route



Configuring Routing in ASDM (Cont.)

Add or Edit Route Window

Add Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID: Track IP Address:

SLA ID: Target Interface:

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Add Static Route Details

Add Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID: Track IP Address:

SLA ID: Target Interface:

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

Configuring Routing in ASDM (Cont.)

Apply the Configuration

Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: Both IPv4 only IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside	0.0.0.0	255.255.25...	209.165.2...	1	None

Add
Edit
Delete

Configuring Device Management Access in ASDM

Configure ASDM/HTTPS/Telnet/SSH Access

The screenshot shows the Cisco ASDM 7.4 for ASA configuration interface. The breadcrumb navigation is Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH. The main content area is titled "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." It contains a table with the following data:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.1.3	255.255.255.255

Below the table are sections for "Http Settings", "Telnet Settings", and "SSH Settings".

Http Settings

- Enable HTTP Server
- Port Number: 443
- Idle Timeout: 20 minutes
- Session Timeout: [] minutes
- Require client certificate to access ASDM on the following interfaces: []

Telnet Settings

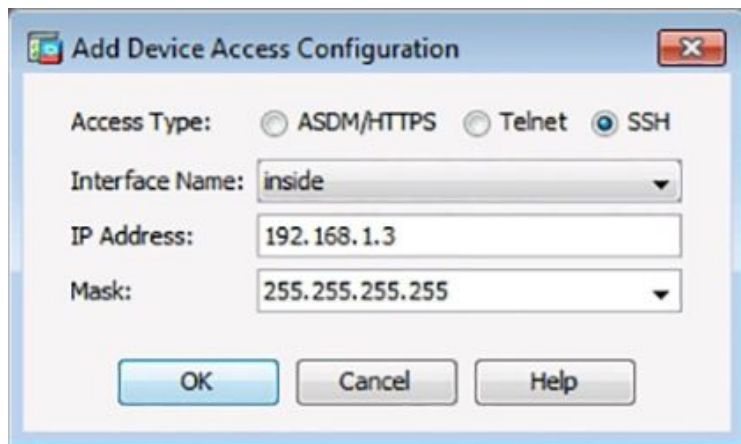
- Telnet Timeout: 5 minutes

SSH Settings

- Allowed SSH Version(s): 1 & 2
- SSH Timeout: 5 minutes
- DH Key Exchange: Group 1 Group 14

Buttons for "Add", "Edit", and "Delete" are located to the right of the table. "Apply" and "Reset" buttons are at the bottom of the configuration area. The status bar at the bottom shows "<admin> 15" and the date/time "4/14/15 1:15:21 PM EDT".

Configuring Device Management Access in ASDM (Cont.)

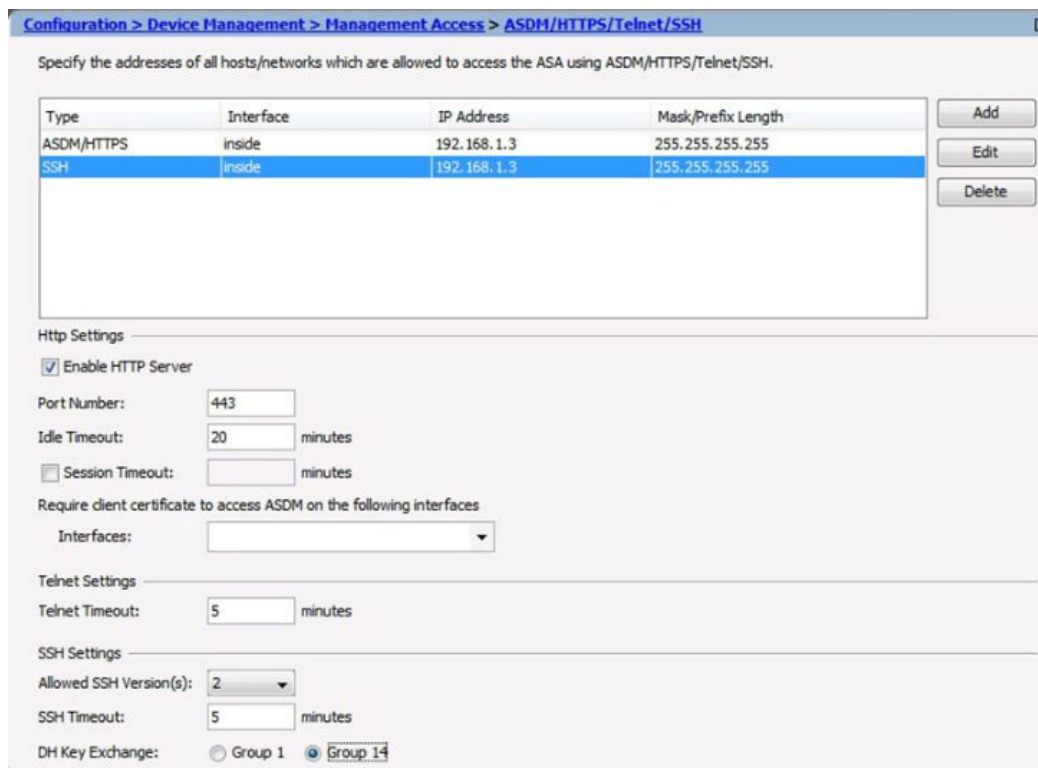


The dialog box titled "Add Device Access Configuration" has a close button (X) in the top right corner. It contains the following fields and controls:

- Access Type: Three radio buttons labeled "ASDM/HTTPS", "Telnet", and "SSH". The "SSH" radio button is selected.
- Interface Name: A dropdown menu with "inside" selected.
- IP Address: A text input field containing "192.168.1.3".
- Mask: A dropdown menu with "255.255.255.255" selected.
- Buttons: "OK", "Cancel", and "Help" buttons at the bottom.

Configure SSH Settings

Add Device Access Configuration Window



The configuration window shows the path: Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH. Below the path is a description: "Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH." Below this is a table with columns: Type, Interface, IP Address, and Mask/Prefix Length. The table contains two rows, both highlighted in blue. To the right of the table are "Add", "Edit", and "Delete" buttons. Below the table are sections for "Http Settings", "Telnet Settings", and "SSH Settings".

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	inside	192.168.1.3	255.255.255.255
SSH	inside	192.168.1.3	255.255.255.255

Http Settings

- Enable HTTP Server
- Port Number: 443
- Idle Timeout: 20 minutes
- Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces: dropdown menu

Telnet Settings

- Telnet Timeout: 5 minutes

SSH Settings

- Allowed SSH Version(s): 2
- SSH Timeout: 5 minutes
- DH Key Exchange: Group 1 Group 14

Configuring DHCP Services in ASDM

DHCP Server Page

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management

Configuration > Device Management > DHCP > DHCP Server

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout	Edit
inside	No	-					
outside	No	-					

Global DHCP Options

Enable auto-configuration from interface: outside Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Domain Name:

Lease Length: secs

Ping Timeout: ms

Dynamic DNS Settings for DHCP Server

Update DNS Server

Update Both Records Override Client Settings

Configuring DHCP Services in ASDM (Cont.)

Edit DHCP Server Window

Interface: **inside**

Enable DHCP server

DHCP Address Pool: -

Optional Parameters

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Lease Length: seconds Ping Timeout: milliseconds

Domain Name:

Auto-Configuration

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

Enable auto-configuration from interface: Allow VPN override

Advanced Options

Advanced Parameters :

Dynamic DNS Settings for DHCP Server

Update DNS server

Update both records Override client settings

Configuring DHCP Services in ASDM (Cont.)

Configuring DHCP Server Services

The screenshot shows the 'Edit DHCP Server' configuration window. The interface is set to 'inside'. The 'Enable DHCP server' checkbox is checked. The DHCP Address Pool is configured as 192.168.1.10 to 192.168.1.41. Under 'Optional Parameters', the DNS Server 1 and 2 fields are empty, the Primary and Secondary WINS Servers are empty, the Lease Length is 43,200 seconds, and the Ping Timeout is empty milliseconds. The Domain Name is set to ccnasecurity.com. The 'Auto-Configuration' section is disabled, with 'Enable auto-configuration from interface' set to 'outside' and 'Allow VPN override' unchecked. The 'Advanced Options' section has an 'Advanced...' button. The 'Dynamic DNS Settings for DHCP Server' section is also disabled, with 'Update DNS server', 'Update both records', and 'Override client settings' all unchecked. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Interface: **inside**

Enable DHCP server

DHCP Address Pool: 192.168.1.10 - 192.168.1.41

Optional Parameters

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Lease Length: 43,200 seconds Ping Timeout: milliseconds

Domain Name:

Auto-Configuration

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

Enable auto-configuration from interface: Allow VPN override

Advanced Options

Advanced Parameters :

Dynamic DNS Settings for DHCP Server

Update DNS server

Update both records Override client settings

Configuring DHCP Services in ASDM (Cont.)

Verifying DHCP Server Services

The screenshot shows the ASDM configuration page for DHCP Server services. The breadcrumb navigation is Configuration > Device Management > DHCP > DHCP Server. A table lists the configuration for two interfaces: 'inside' and 'outside'. The 'inside' interface has DHCP Enabled set to 'Yes', an Address Pool of '192.168.1.10 - 192.168.1.41', and a Domain Name of 'cnasecurity....'. The 'outside' interface has DHCP Enabled set to 'No' and an empty Address Pool. Below the table, the 'Global DHCP Options' section includes a dropdown menu for 'Enable auto-configuration from interface' set to 'outside', and an unchecked checkbox for 'Allow VPN override'. A note states: 'Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.' Below this note are input fields for 'DNS Server 1', 'DNS Server 2', 'Primary WINS Server', 'Secondary WINS Server', 'Domain Name', 'Lease Length' (in seconds), and 'Ping Timeout' (in milliseconds). An 'Advanced...' button is located at the bottom right of this section. The 'Dynamic DNS Settings for DHCP Server' section at the bottom has an unchecked checkbox for 'Update DNS Server', and two unchecked checkboxes for 'Update Both Records' and 'Override Client Settings'.

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout
inside	Yes	192.168.1.10 - 192.168.1.41			cnasecurity....	
outside	No	-				

Global DHCP Options

Enable auto-configuration from interface: outside Allow VPN override

Enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and the default domain name. The values in the fields below take precedence over the auto-configured values.

DNS Server 1: Primary WINS Server:

DNS Server 2: Secondary WINS Server:

Domain Name:

Lease Length: secs

Ping Timeout: ms

Advanced...

Dynamic DNS Settings for DHCP Server

Update DNS Server

Update Both Records Override Client Settings

Topic 10.1.4: Configuring Advanced ASDM Features



Objects in ASDM

Network Objects/Groups Page

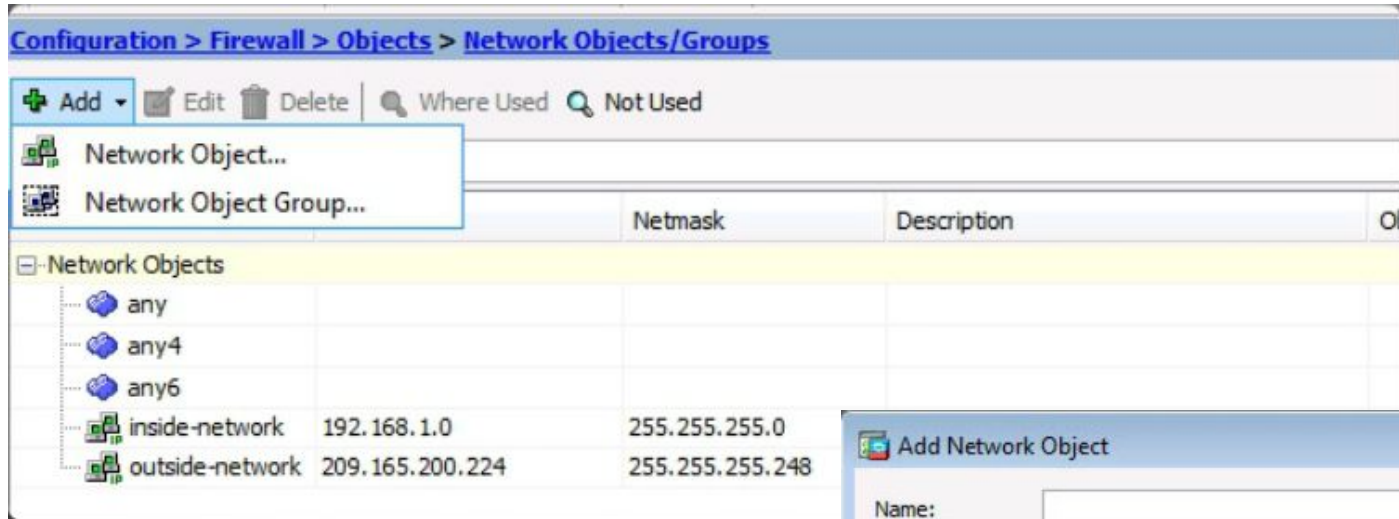
The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The main window shows the configuration page for Network Objects/Groups. The left-hand navigation pane is expanded to show the 'Objects' folder, with 'Network Objects/Groups' selected. The main area contains a table of network objects with the following data:

Name	IP Address	Netmask	Description	Object NAT Address
Network Objects				
any				
any4				
any6				
inside-network	192.168.1.0	255.255.255.0		
outside-network	209.165.200.224	255.255.255.248		

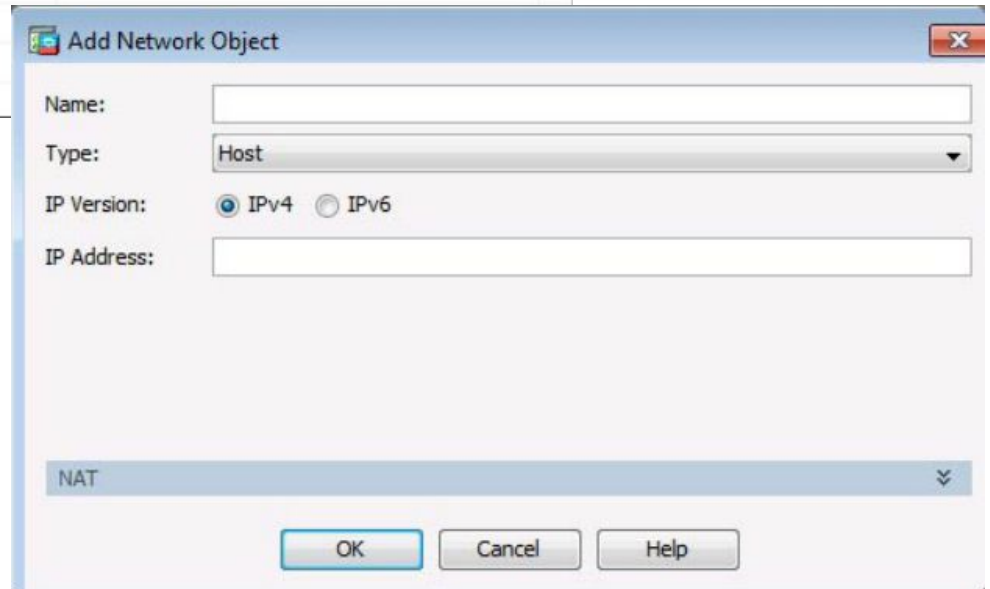
The interface also shows a status bar at the bottom with the user name '<admin>', the number '15', and the date/time '4/13/15 7:08:07 AM EDT'. The Cisco logo is visible in the top right corner of the application window.

Objects in ASDM (Cont.)

Adding a Network Object/Group

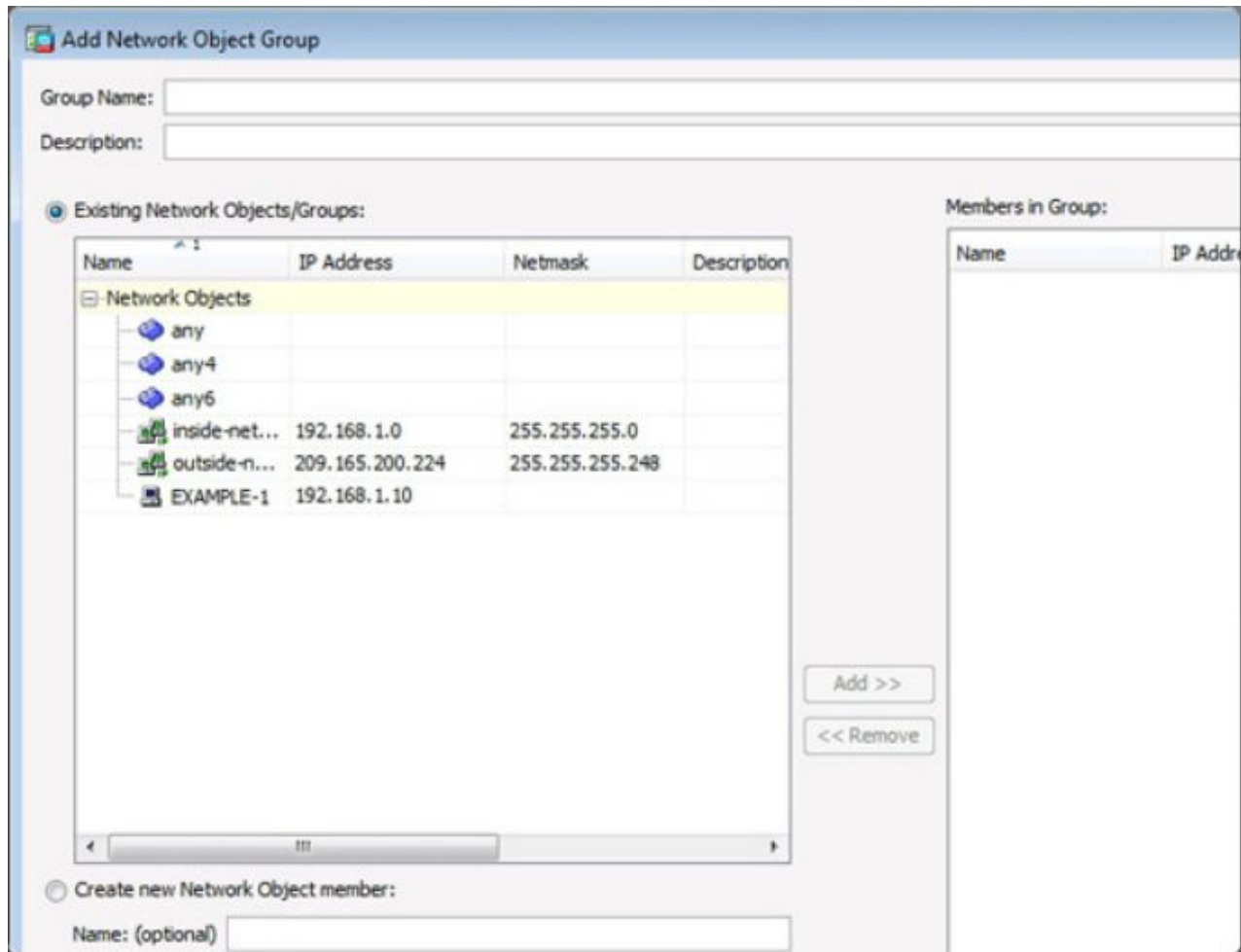


Add Network Object Window



Objects in ASDM (Cont.)

Add Network Object Group Window



Objects in ASDM (Cont.)

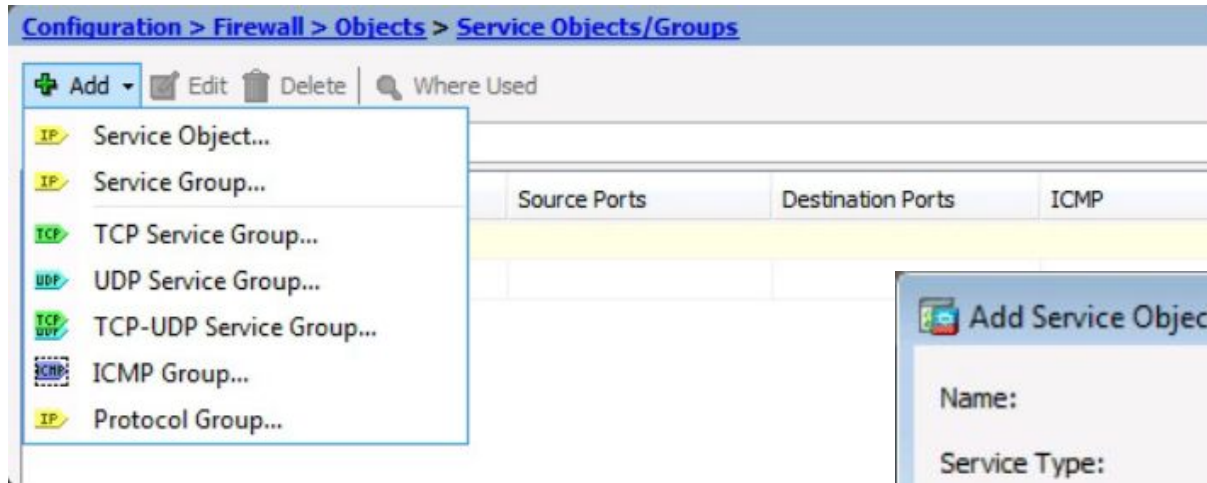
Service Objects/Group Page

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Firewall > Objects > Service Objects/Groups. The left-hand 'Device List' pane shows a tree view of configuration objects, with 'Service Objects/Groups' selected and highlighted in blue. Below the tree is a 'Device Setup' section with icons for Device Setup, Firewall, Remote Access VPN, Site-to-Site VPN, and Device Management. The main content area features a toolbar with 'Add', 'Edit', and 'Delete' buttons, and a search field labeled 'Where Used'. Below this is a table with the following columns: Name, Protocol, Source Ports, Destination Ports, ICMP, and Description. The table contains one entry: 'any' under the 'Name' column. At the bottom of the interface, there are 'Apply' and 'Reset' buttons, and a status bar showing 'Device configuration refreshed successfully.', the user 'admin', the ID '15', and the date/time '4/13/15 7:38:27 AM EDT'.

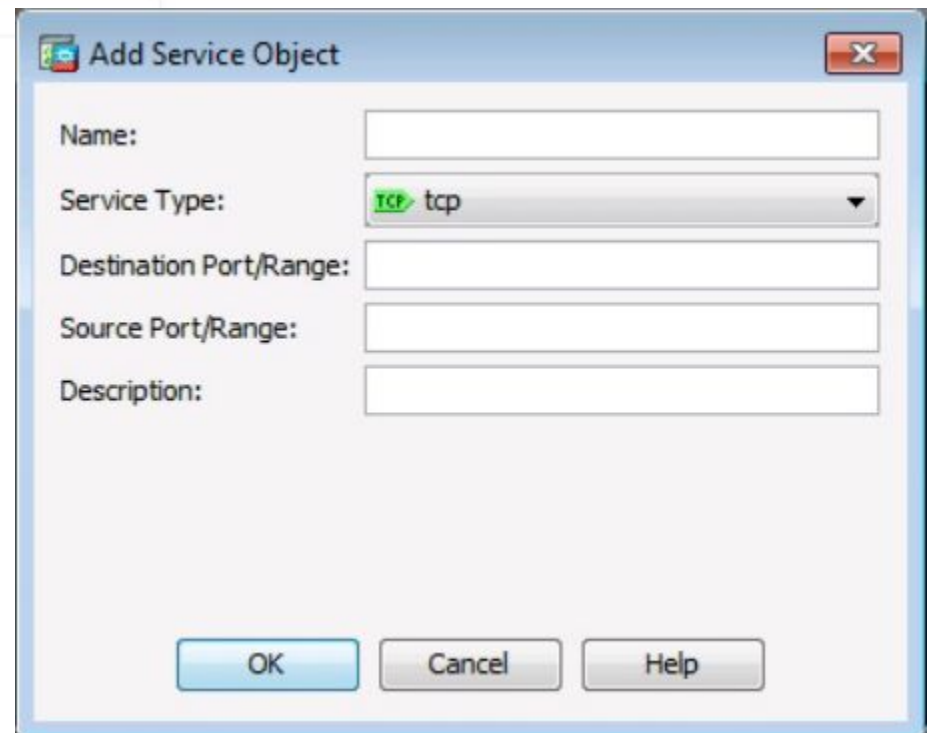
Name	Protocol	Source Ports	Destination Ports	ICMP	Description
any					

Objects in ASDM (Cont.)

Adding a Service Object/Group

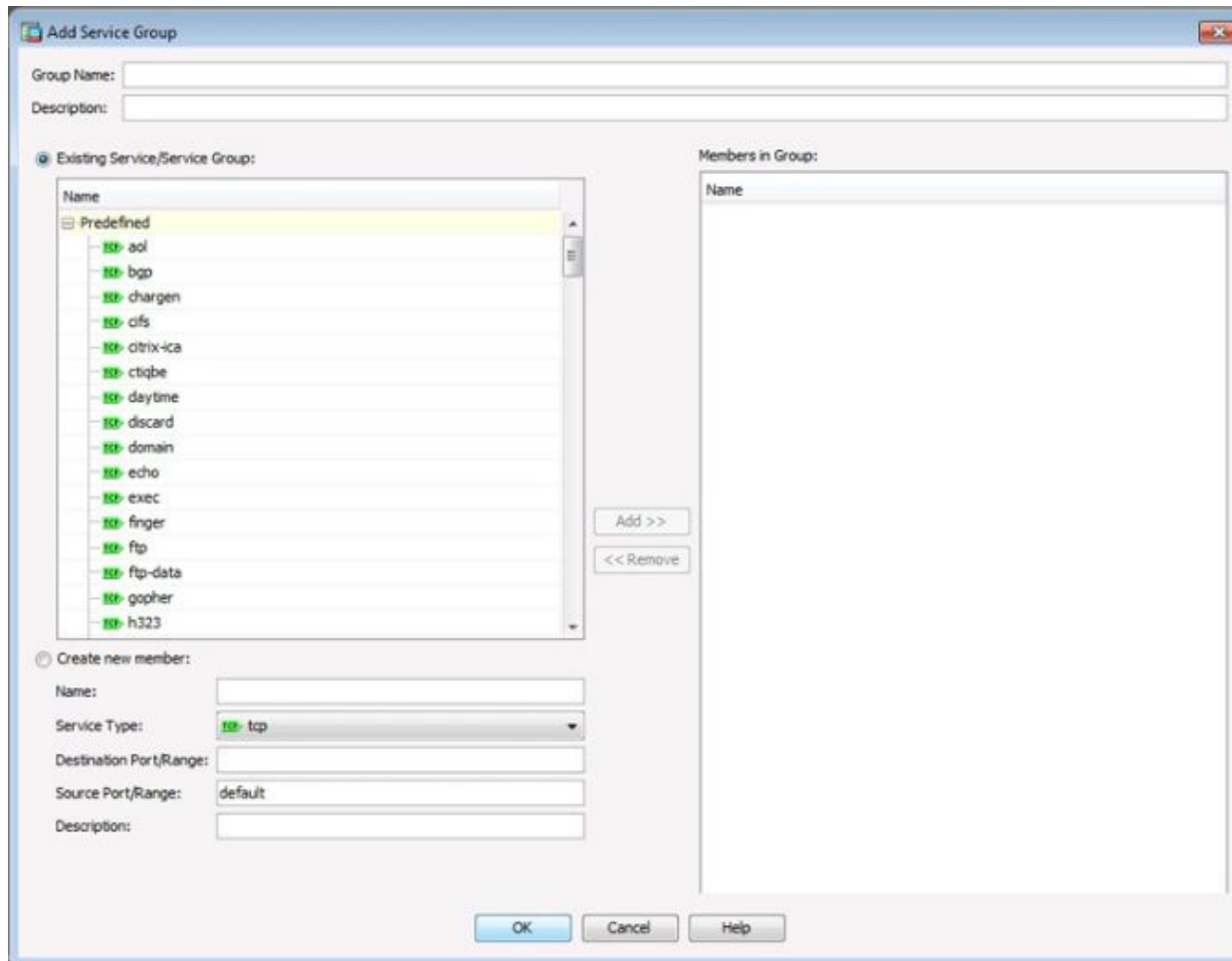


Add Service Object Window



Objects in ASDM (Cont.)

Add Service Object Group Window



Configuring ACLs Using ASDM

ACLs in ASDM

The screenshot displays the Cisco ASDM 7.4 for ASA interface. The main window is titled "Configuration > Firewall > Access Rules". The left sidebar shows the "Firewall" configuration tree with "Access Rules" selected. The central pane shows a table of source criteria for the selected rule:

#	Enabled	Source	User	Security Group
inside (1 implicit incoming rule)				
1		any		
outside (0 implicit incoming rules)				
Global (1 implicit rule)				
1		any		

The right pane shows the "Addresses" configuration, with a list of network objects:

- any
- any4
- any6
- inside-network/24
- outside-network/29
- EXAMPLE-1

At the bottom of the window, there are "Apply", "Reset", and "Advanced..." buttons. The status bar at the bottom indicates "Device configuration refreshed successfully.", the user is "", and the page number is "15". The system time is "4/13/15 8:14:17 AM EDT".

Configuring ACLs Using ASDM (Cont.)

Add Access Rule Window

Interface: inside

Action: Permit Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: any

Security Group:

Service: ip

Description:

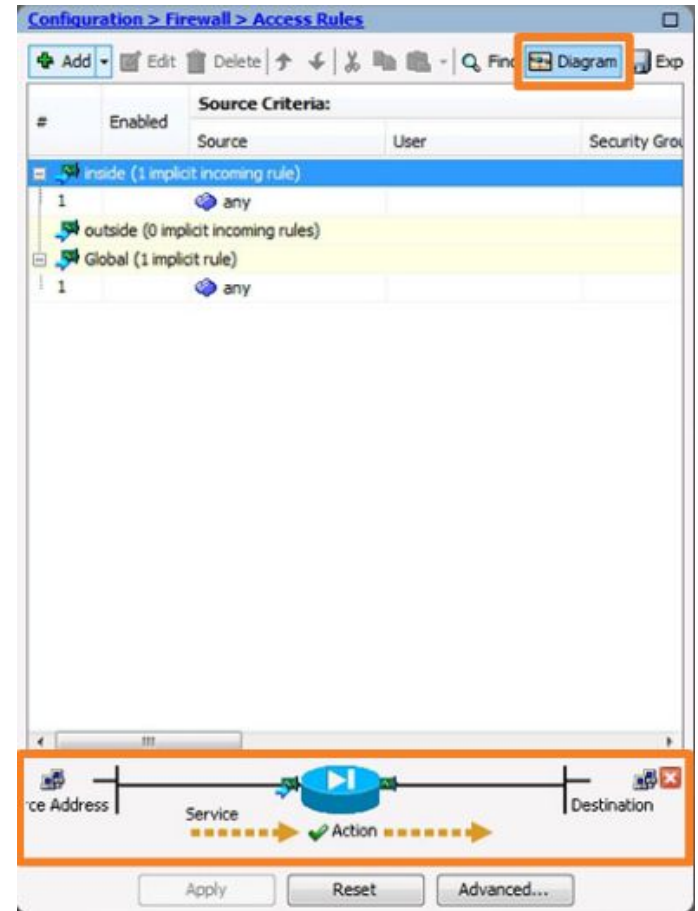
Enable Logging

Logging Level: Default

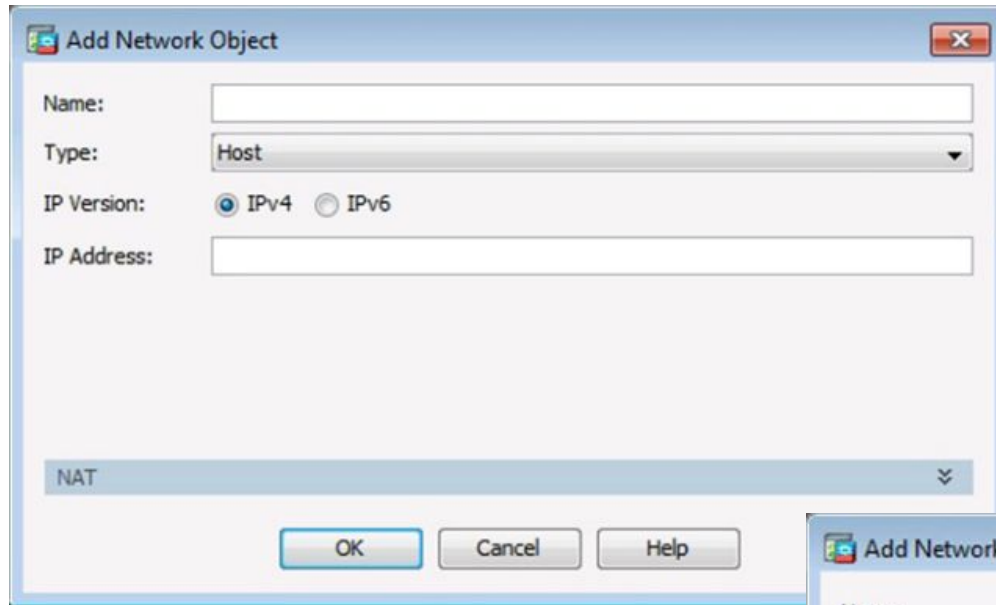
More Options

OK Cancel Help

Diagramming Access Rules



Configuring Dynamic NAT in ASDM



Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

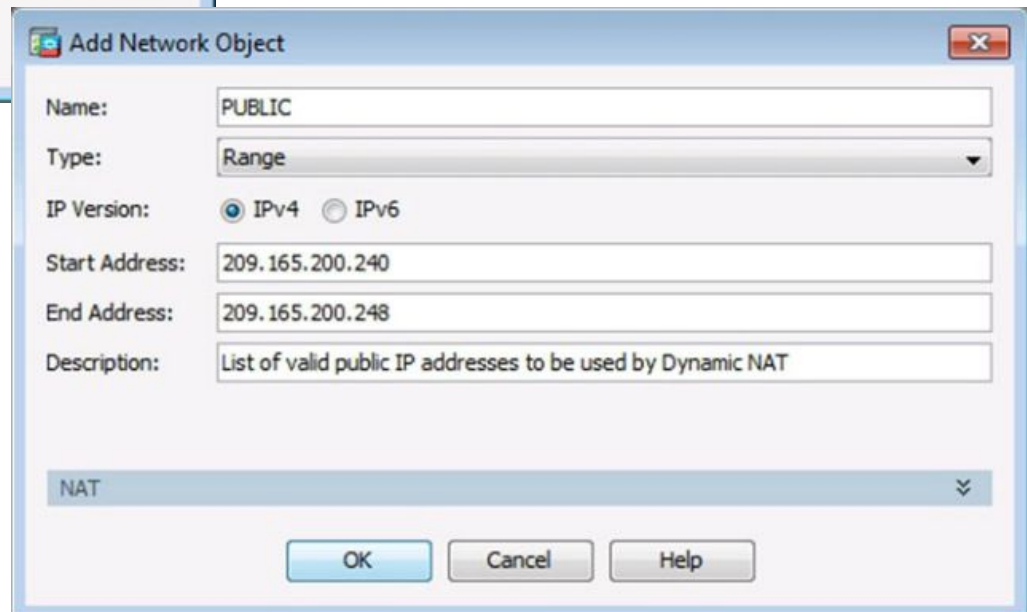
IP Address:

NAT

OK Cancel Help

Add Network Object Window

Creating a Network Object
for Public Addresses



Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

Start Address:

End Address:

Description:

NAT

OK Cancel Help

Configuring Dynamic NAT in ASDM (Cont.)

The screenshot shows the 'Add Network Object' dialog box in ASDM. The 'Name' field is 'DYNAMIC-NAT', 'Type' is 'Network', 'IP Version' is 'IPv4', 'IP Address' is '192.168.1.0', and 'Netmask' is '255.255.255.224'. The 'Description' is 'Inside Hosts to use Dynamic NAT'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Dynamic', and 'Translated Addr' set to 'PUBLIC'. Other options like 'Use one-to-one address translation', 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness to per destination instead of per interface', 'Translate TCP and UDP ports into flat range 1024-65535', 'Include range 1-1023', 'Fall through to interface PAT(dest intf): inside', and 'Use IPv6 for interface PAT' are all unchecked. An 'Advanced...' button is visible below the NAT options. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Creating a Network Object for Dynamic NAT

Configuring Dynamic PAT in ASDM

The screenshot shows the 'Add Network Object' dialog box in ASDM. The 'Name' field is 'DYNAMIC-PAT', 'Type' is 'Host', 'IP Version' is 'IPv4', 'IP Address' is '192.168.1.0', and 'Description' is '255.255.255.224'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Dynamic PAT (Hide)', and 'Translated Addr' set to 'outside'. Other options like 'Use one-to-one address translation', 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness to per destination instead of per interface', 'Translate TCP and UDP ports into flat range 1024-65535', 'Include range 1-1023', 'Fall through to interface PAT(dest intf): inside', and 'Use IPv6 for interface PAT' are unchecked. An 'Advanced...' button is visible below the NAT options. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Add Network Object

Name: DYNAMIC-PAT
Type: Host
IP Version: IPv4 IPv6
IP Address: 192.168.1.0
Description: 255.255.255.224

NAT

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide) ▾

Translated Addr: outside

Use one-to-one address translation

PAT Pool Translated Address: ..

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf): inside

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

Configuring Static NAT in ASDM

Static NAT in ASDM

Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

Advanced Static NAT Settings in ASDM

Advanced NAT Settings

Translate DNS replies for rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Interface

Source Interface:

Destination Interface:

Service

Protocol:

Real Port:

Mapped Port:

Configuring AAA Authentication

User Accounts Page

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Management Configuration > Device Management > Users/AAA > User Accounts

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [Authentication](#).

Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock
enable_15	15	Full	N/A	N/A

Add Edit Delete

Configuring AAA Authentication (Cont.)

Add User Account Window

Add User Account

Identity

- Public Key Authentication
- Public Key Using PKF
- VPN Policy

Username: ADMIN

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access (ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 15

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if "aaa authentication http console LOCAL" command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Find:

Next Previous

OK Cancel Help

Configuring AAA Authentication (Cont.)

AAA Server Groups Page

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Device Management > Users/AAA > AAA Server Groups. The left-hand navigation pane shows the 'Users/AAA' folder expanded, with 'AAA Server Groups' selected. The main content area is titled 'AAA Server Groups' and contains a table with the following columns: Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. A single entry is visible in the table:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				

Below the table is a search field labeled 'Find:' with a 'Match Case' checkbox. To the right of the table are buttons for 'Add', 'Edit', and 'Delete'. Below the search field is another section titled 'Servers in the Selected Group' with a table containing columns for Server Name or IP Address, Interface, and Timeout. This table is currently empty. To the right of this table are buttons for 'Add', 'Edit', 'Delete', 'Move Up', 'Move Down', and 'Test'. Below this table is another search field labeled 'Find:' with a 'Match Case' checkbox. At the bottom of the main content area, there is a dropdown menu currently set to 'LDAP Attribute Map' and buttons for 'Apply' and 'Reset'. The status bar at the bottom of the window shows '<admin>' on the left and '4/13/15 8:37:14 PM UTC' on the right.

Configuring AAA Authentication (Cont.)

Add AAA Server Group Window

The 'Add AAA Server Group' window is configured with the following settings:

- AAA Server Group: RADIUS-SERVERS
- Protocol: RADIUS
- Accounting Mode: Single (selected)
- Reactivation Mode: Depletion (selected)
- Dead Time: 10 minutes
- Max Failed Attempts: 3
- Enable interim accounting update
 - Update Interval: 24 Hours
- Enable Active Directory Agent mode
- ISE Policy Enforcement
 - Enable dynamic authorization
 - Dynamic Authorization Port: 1700
 - Use authorization only mode (no common password configuration required)
- VPN3K Compatibility Option

Buttons: OK, Cancel, Help

Add AAA Server Window

The 'Add AAA Server' window is configured with the following settings:

- Server Group: RADIUS-SERVERS
- Interface Name: dmz
- Server Name or IP Address: 192.168.2.3
- Timeout: 10 seconds
- RADIUS Parameters
 - Server Authentication Port: 1645
 - Server Accounting Port: 1646
 - Retry Interval: 10 seconds
 - Server Secret Key: [Redacted]
 - Common Password: [Redacted]
 - ACL Netmask Convert: Standard
 - Microsoft CHAPv2 Capable:
- SDI Messages
 - Message Table

Buttons: OK, Cancel, Help

Configuring AAA Authentication (Cont.)

Completed AAA Server Groups Window

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
RADIUS-SERVERS	RADIUS	Single	Depletion	10	3

Find: Match Case

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.2.3	dmz	10

Buttons: Add, Edit, Delete, Move Up, Move Down, Test

Configuring AAA Authentication (Cont.)

AAA Access Page

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation path is Configuration > Device Management > Users/AAA > AAA Access > Authentication. The left-hand 'Device List' pane shows the 'Users/AAA' folder expanded, with 'AAA Access' selected. The main configuration area is titled 'Authentication' and contains the following settings:

- Enable authentication for administrator access to the ASA.**
- Require authentication to allow use of privileged mode commands:**
 - Enable Server Group: LOCAL Use LOCAL when server group fails
- Require authentication for the following types of connections:**
 - HTTP/ASDM Server Group: LOCAL Use LOCAL when server group fails
 - Serial Server Group: LOCAL Use LOCAL when server group fails
 - SSH Server Group: LOCAL Use LOCAL when server group fails
 - Telnet Server Group: LOCAL Use LOCAL when server group fails

At the bottom of the configuration area are 'Apply' and 'Reset' buttons. A status bar at the very bottom indicates 'Configuration changes saved successfully.' and shows the user as '<admin>' with a session ID of '15' and a timestamp of '4/13/15 9:11:24 PM UTC'.

Configuring AAA Authentication (Cont.)

AAA Access > Authentication Window

[Configuration](#) > [Device Management](#) > [Users/AAA](#) > [AAA Access](#) > [Authentication](#)

Authentication | Authorization | Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands _____

Enable Server Group: Use LOCAL when server group fails

Require authentication for the following types of connections _____

<input checked="" type="checkbox"/> HTTP/ASDM	Server Group: <input type="text" value="RADIUS-SERVERS"/>	<input checked="" type="checkbox"/> Use LOCAL when server group fails
<input type="checkbox"/> Serial	Server Group: <input type="text" value="LOCAL"/>	<input type="checkbox"/> Use LOCAL when server group fails
<input checked="" type="checkbox"/> SSH	Server Group: <input type="text" value="RADIUS-SERVERS"/>	<input checked="" type="checkbox"/> Use LOCAL when server group fails
<input type="checkbox"/> Telnet	Server Group: <input type="text" value="LOCAL"/>	<input type="checkbox"/> Use LOCAL when server group fails

Configuring a Service Policy Using ASDM

Service Policy in ASDM

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Firewall > Service Policy Rules". The left sidebar shows the "Firewall" tree with "Service Policy Rules" selected. The main area shows a table of traffic classification rules. The selected rule is "Global; Policy: global_policy" with a match type of "Match" and a source of "any". The right sidebar shows the "Services" list, including predefined services like "aol", "bgp", "chargen", etc.

Configuration > Firewall > Service Policy Rules

Name	Enabled	Match	Source	Src Security Group	Destine
Global; Policy: global_policy		Match	any		any

Services

- Predefined
 - aol
 - bgp
 - chargen
 - cifs
 - citrix-ica
 - ctiqbe
 - daytime
 - discard
 - domain
 - echo
 - exec
 - finger
 - ftp
 - ftp-data
 - gopher

Configuring a Service Policy Using ASDM (Cont.)

Configure a Service Policy

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: dmz - (create new service policy)

Policy Name: dmz-policy

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Global - applies to all interfaces

Policy Name: global_policy *

Description:

Drop and log unsupported IPv6 to IPv6 traffic

*Only one service policy is allowed. Existing service policy names cannot be changed.

< Back Next > Cancel Help

Configuring a Service Policy Using ASDM (Cont.)

Configure Traffic Classification Criteria

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

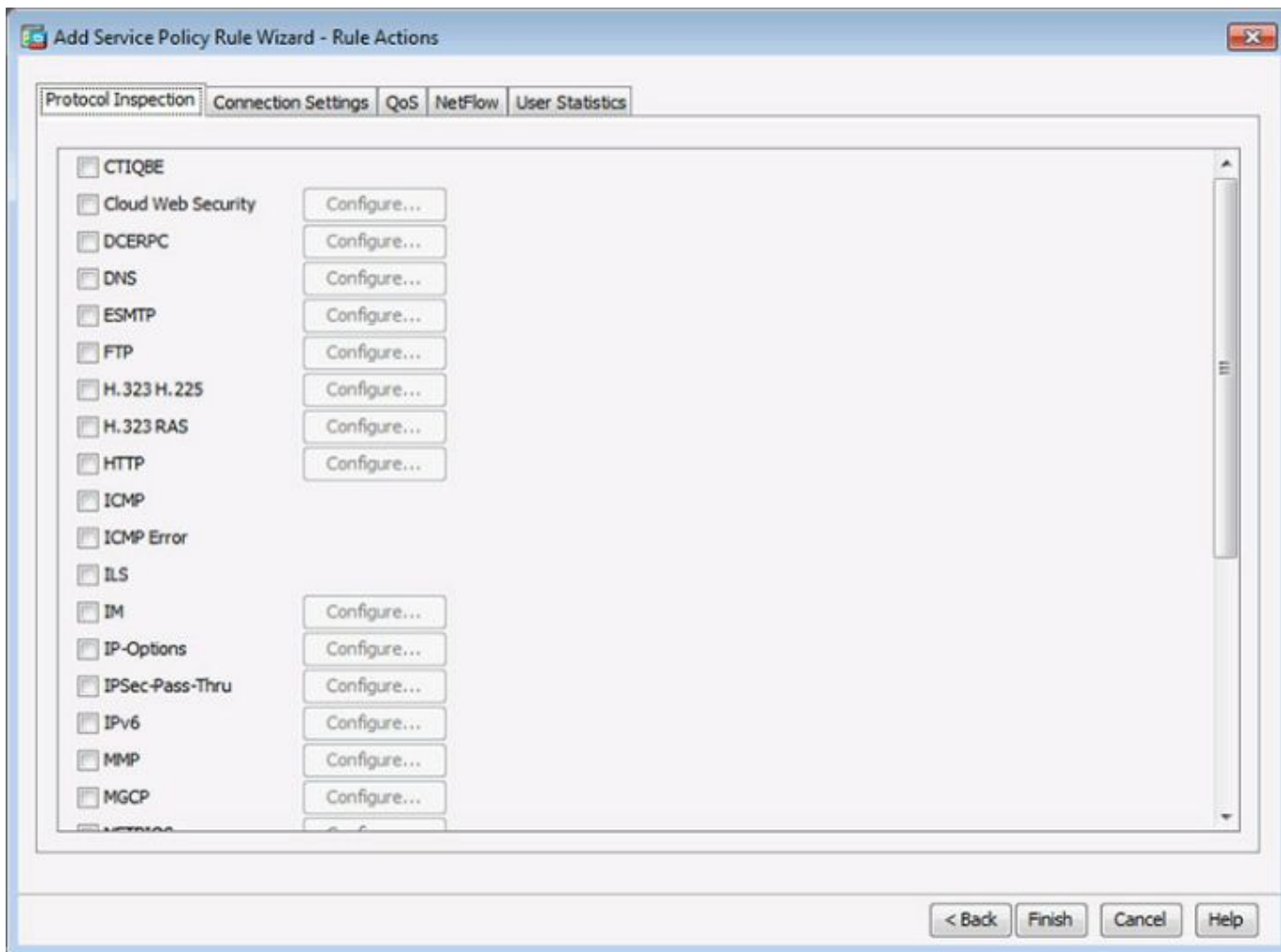
Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back Next > Cancel Help

Configuring a Service Policy Using ASDM (Cont.)

Configure Actions



Section 10.2: ASA VPN Configuration

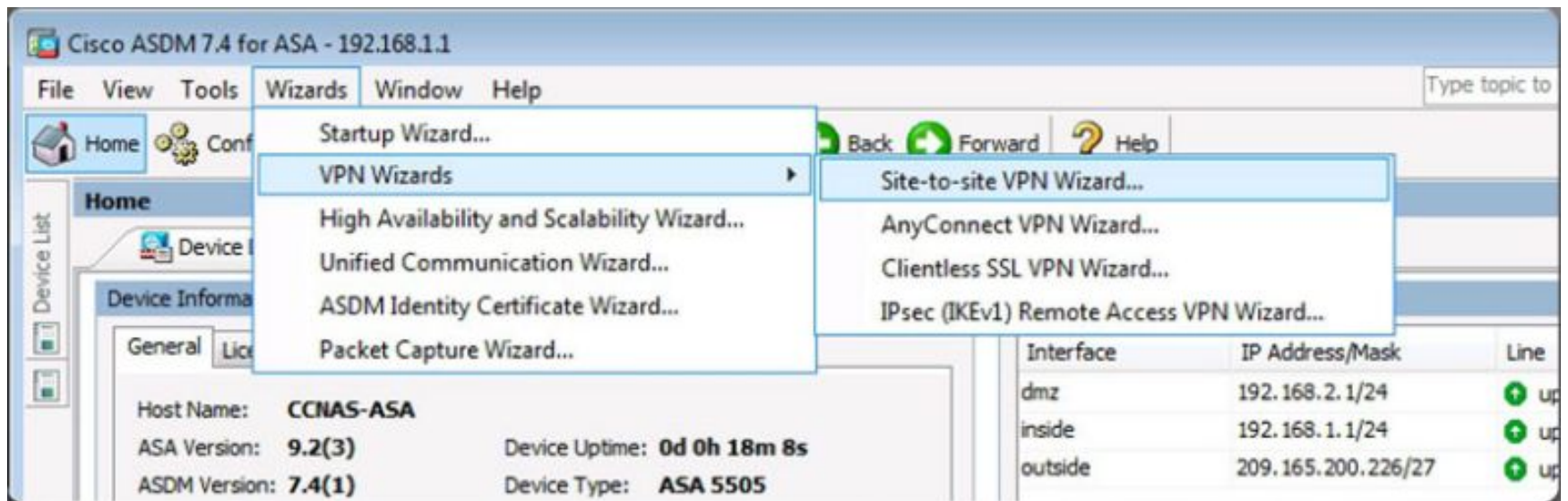
Upon completion of this section, you should be able to:

- 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.

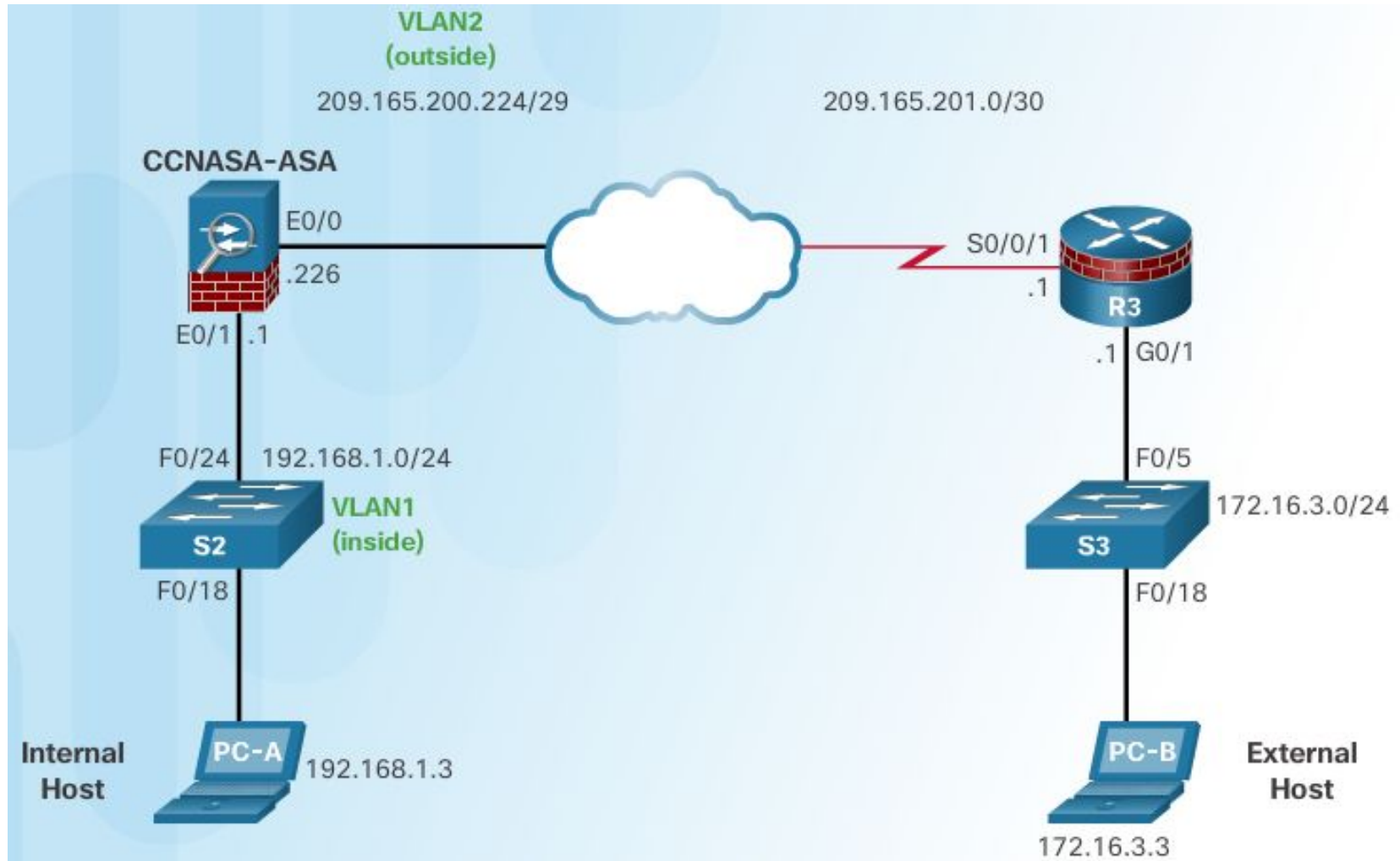
Topic 10.2.1: Site-to-Site VPNs



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)#
```

Configuring the ISR Site-to-Site VPNs Using the CLI (Cont.)

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

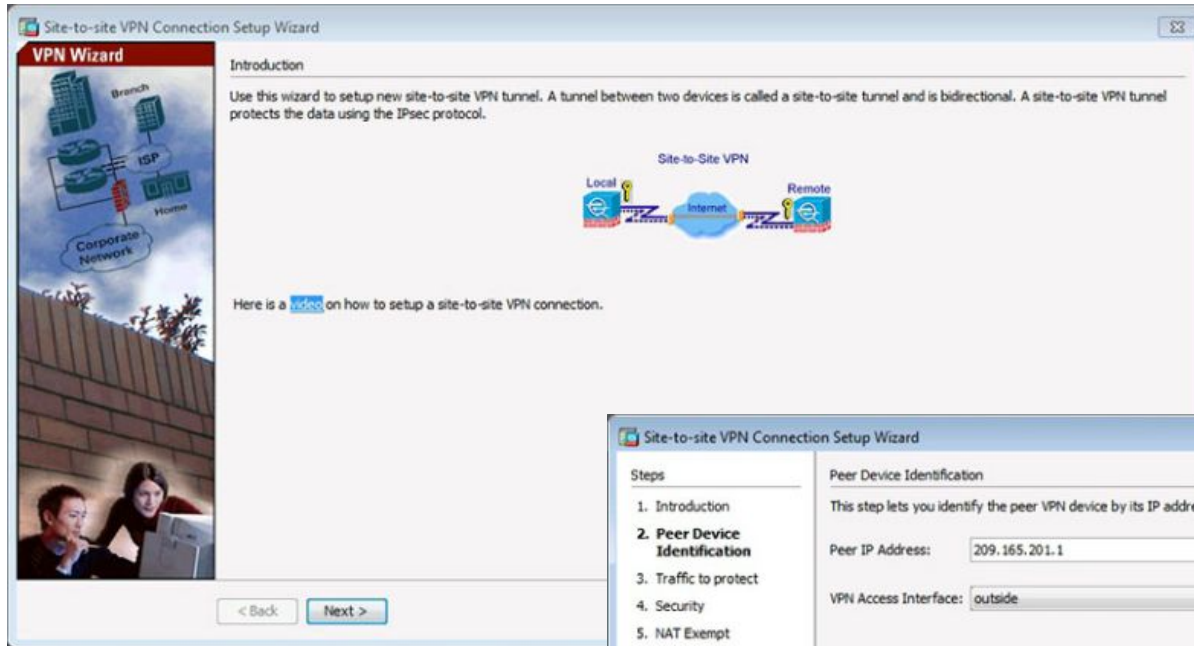
```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)# set peer 209.165.200.226
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# match address VPN-ACL
R3(config-crypto-map)# exit
R3(config)#
R3(config)# interface Serial10/0/1
R3(config-if)# crypto map S2S-MAP
R3(config-if)#
```

Configuring the ASA Site-to-Site VPNs Using ASDM

```
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.224
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)#
CCNAS-ASA(config-network-object)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# http server enable
CCNAS-ASA(config)# http 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)#
```

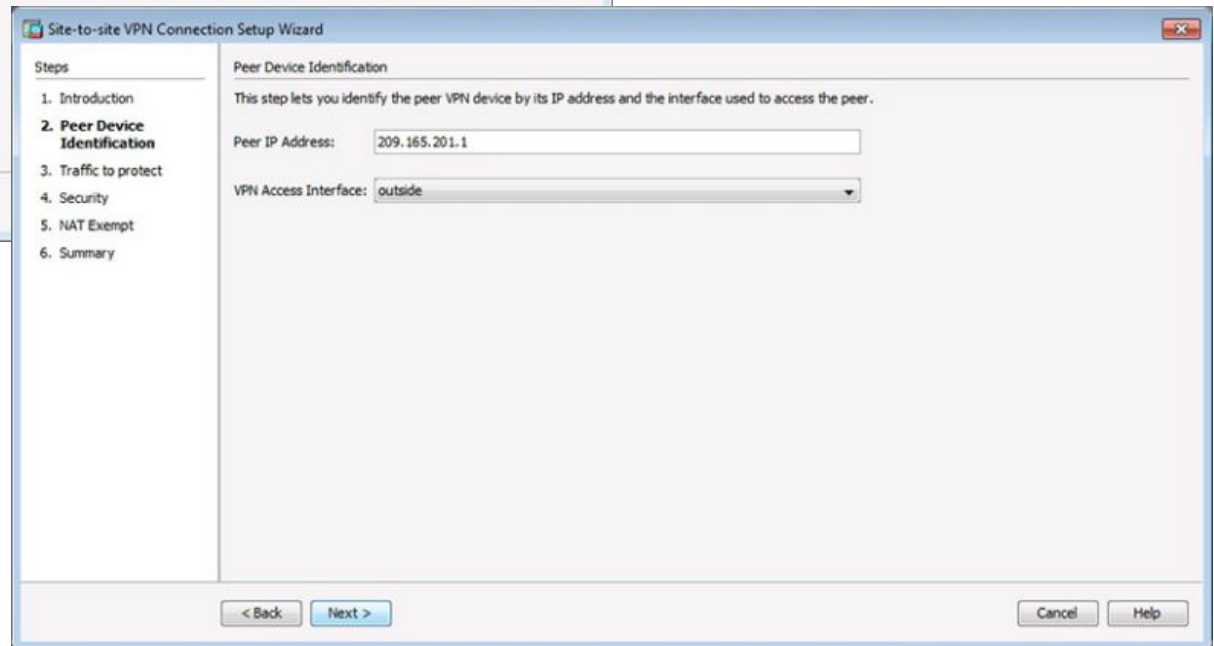
Basic ISR Configuration

Configuring the ASA Site-to-Site VPNs Using ASDM (Cont.)

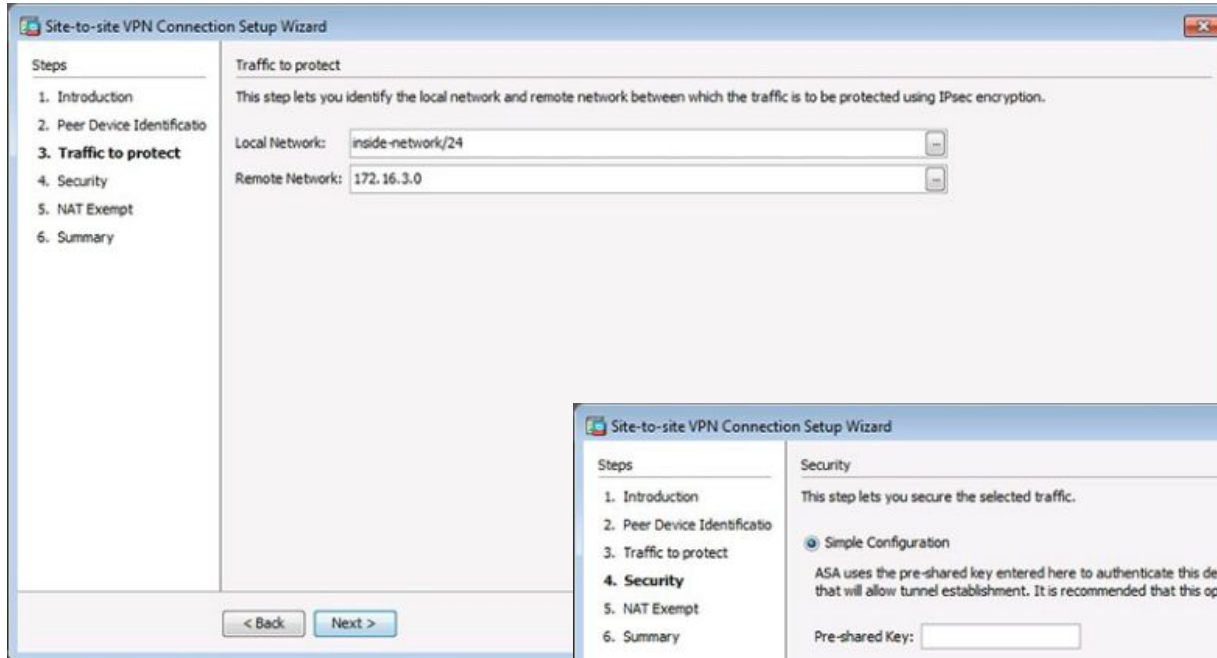


Introduction Window

Peer Device Identification Window

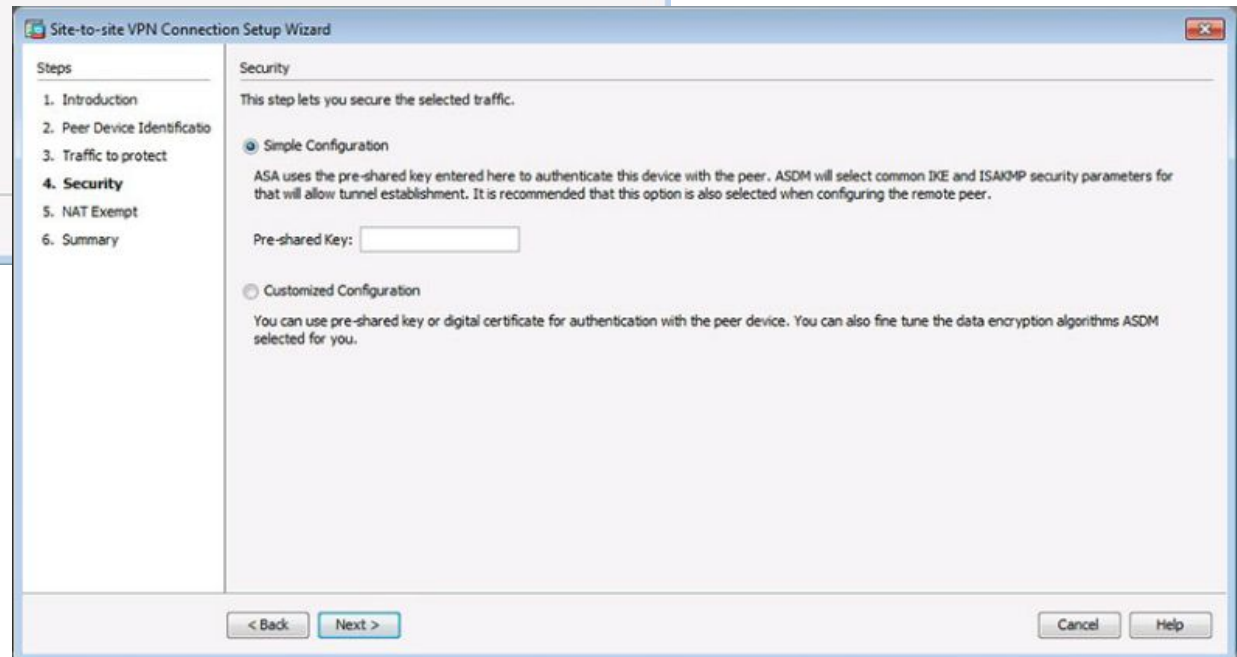


Configuring the ASA Site-to-Site VPNs Using ASDM (Cont.)

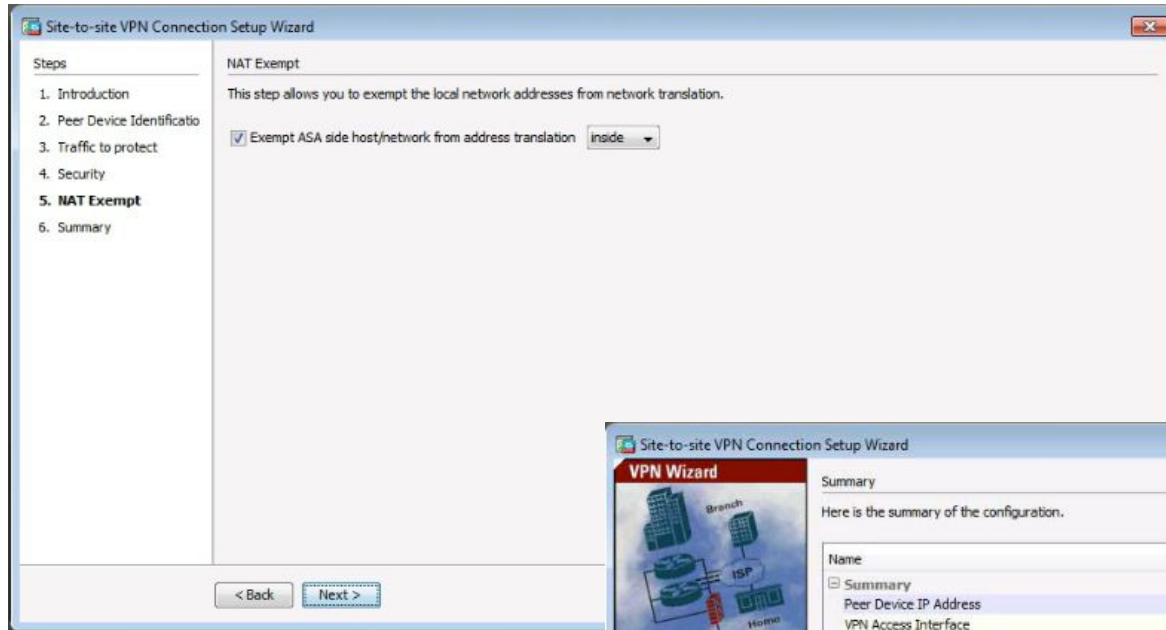


Traffic to Protect Window

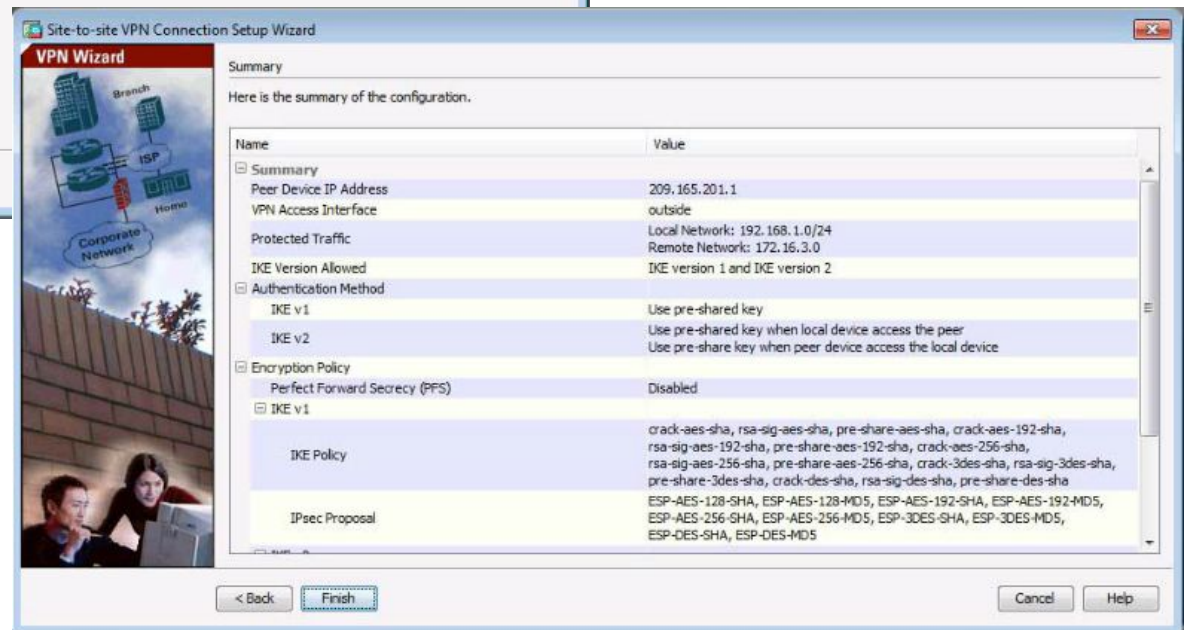
Security Window



Configuring the ASA Site-to-Site VPNs Using ASDM (Cont.)



NAT Exempt Window



Summary Window

Verifying Site-to-Site VPNs Using ASDM

The screenshot displays the Cisco ASDM 7.4 for ASA interface. The main window title is "Cisco ASDM 7.4 for ASA - 192.168.1.1". The navigation pane on the left shows "Site-to-Site VPN" selected, with sub-items: "Connection Profiles", "Group Policies", "Certificate Management", and "Advanced". The main content area is titled "Configuration > Site-to-Site VPN > Connection Profiles".

Manage site-to-site VPN connections. Here is a [video](#) on how to setup a site-to-site VPN connection.

Access Interfaces
Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Connection Profiles
Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile [here](#).

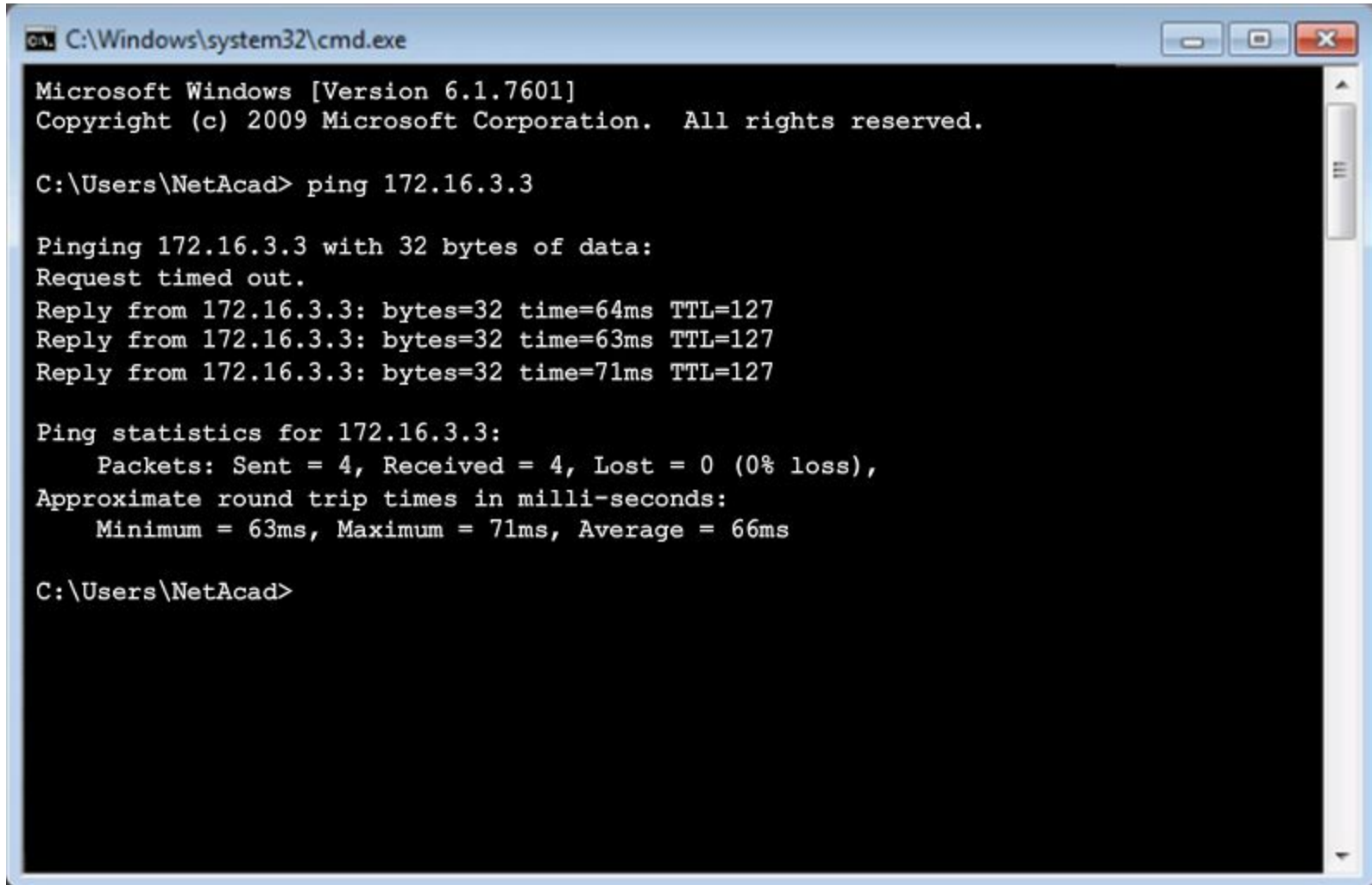
+ Add Edit Delete

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy	NAT Exempt
209.165...	outside	inside-netwo...	172.16.3.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	GroupPolicy_20...	<input checked="" type="checkbox"/>

Find: Match Case

Test the Site-to-Site VPNs Using ASDM

Establish the VPN Tunnel Connection to the Remote Network



```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ping 172.16.3.3

Pinging 172.16.3.3 with 32 bytes of data:
Request timed out.
Reply from 172.16.3.3: bytes=32 time=64ms TTL=127
Reply from 172.16.3.3: bytes=32 time=63ms TTL=127
Reply from 172.16.3.3: bytes=32 time=71ms TTL=127

Ping statistics for 172.16.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 71ms, Average = 66ms

C:\Users\NetAcad>
```

Test the Site-to-Site VPNs Using ASDM (Cont.)

Monitoring the VPN Tunnel

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The main window is titled "Monitoring > VPN > VPN Statistics > Sessions". The left sidebar shows a tree view of VPN statistics, with "Sessions" selected. The main content area features a summary table and a detailed session table.

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	1	1	1
IPsec	1	1	1	1

Filter By: IPsec Site-to-Site -- All Sessions -- Filter

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Details	Logout	Ping
10.2.2.1	IPsec	22:20:41 UTC Tue Apr 21 2015	180			
10.2.2.1	IPsec (1)AES	0h:03m:49s	180			

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

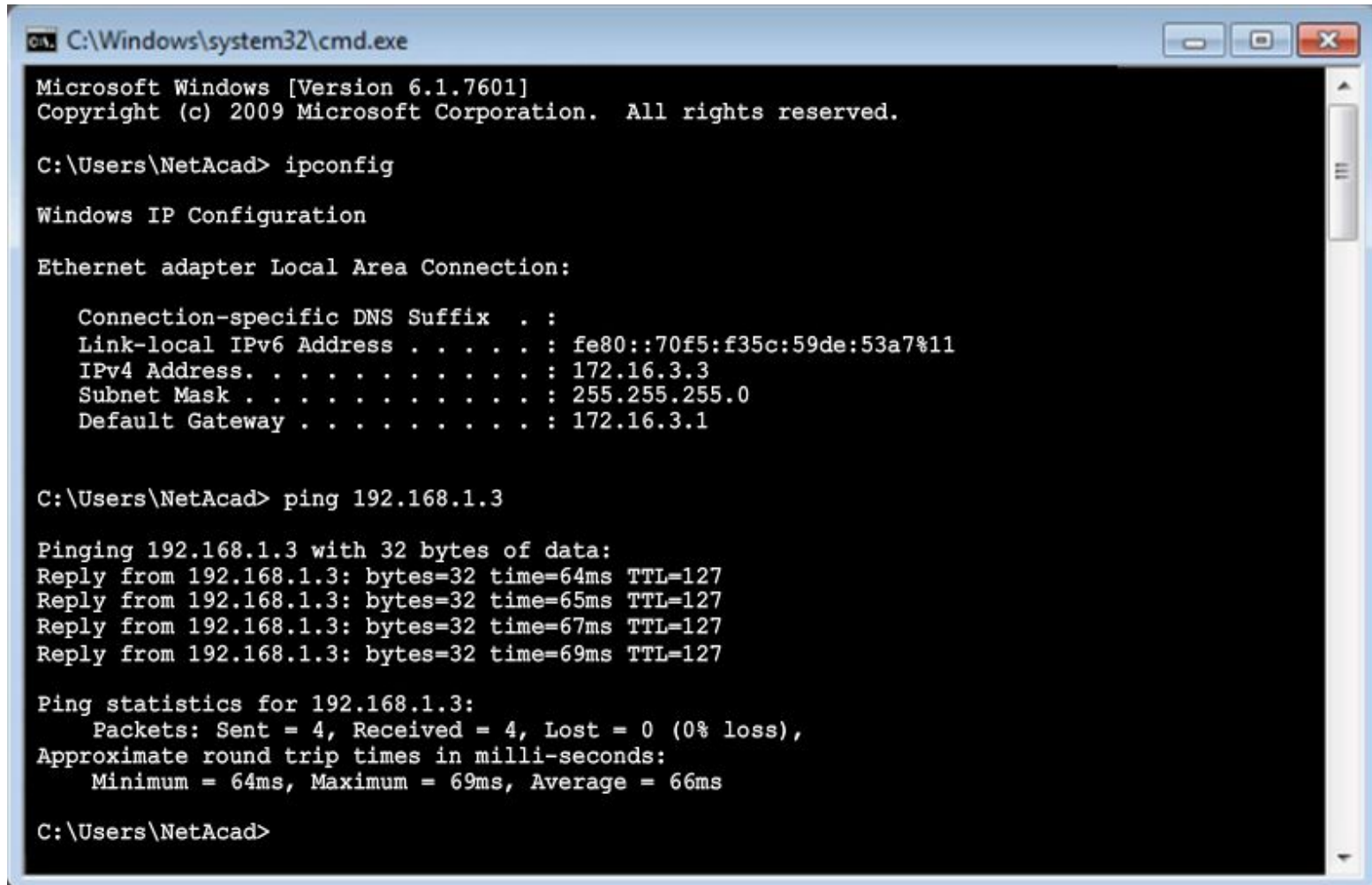
Logout By: -- All Sessions -- Logout Sessions Refresh

Last Updated: 4/21/15 3:24:15 PM

Data Refreshed Successfully. ADMIN 2 4/21/15 10:23:17 PM UTC

Test the Site-to-Site VPNs Using ASDM (Cont.)

Verify VPN Tunnel Connectivity from the External Host



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::70f5:f35c:59de:53a7%11
    IPv4 Address. . . . . : 172.16.3.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.3.1

C:\Users\NetAcad> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=64ms TTL=127
Reply from 192.168.1.3: bytes=32 time=65ms TTL=127
Reply from 192.168.1.3: bytes=32 time=67ms TTL=127
Reply from 192.168.1.3: bytes=32 time=69ms TTL=127

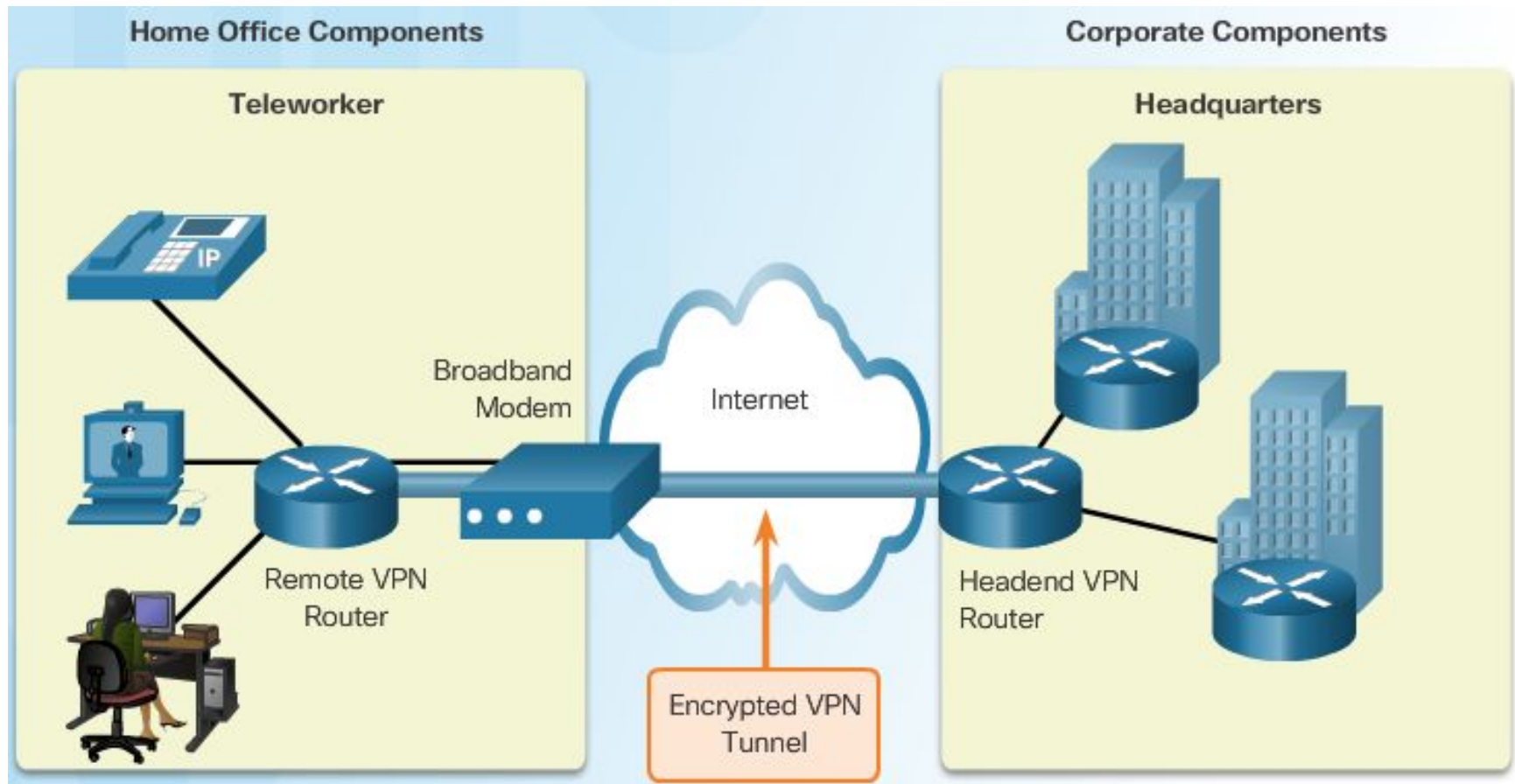
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 64ms, Maximum = 69ms, Average = 66ms

C:\Users\NetAcad>
```

Topic 10.2.2: Remote-Access VPNs



Remote-Access VPN Options



IPsec Versus SSL

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) VPN is a Layer 3 VPN technology and is the conventional teleworker remote-access solution. However, it requires a VPN client such as Cisco AnyConnect to be pre-installed on the host. It supports all types of applications, and provides superior encryption and authentication strength, and overall security.

IPsec

SSL

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) VPN is a Layer 7 VPN technology created by Netscape in the mid-1990s that was designed to enable secure communications over the Internet using a web browser. SSL does not require any pre-installed VPN software but instead allows users to access web pages, services, and files. With SSL, users can send and receive email, and run TCP-based applications using a browser.

IPsec

SSL

IPsec Versus SSL (Cont.)

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

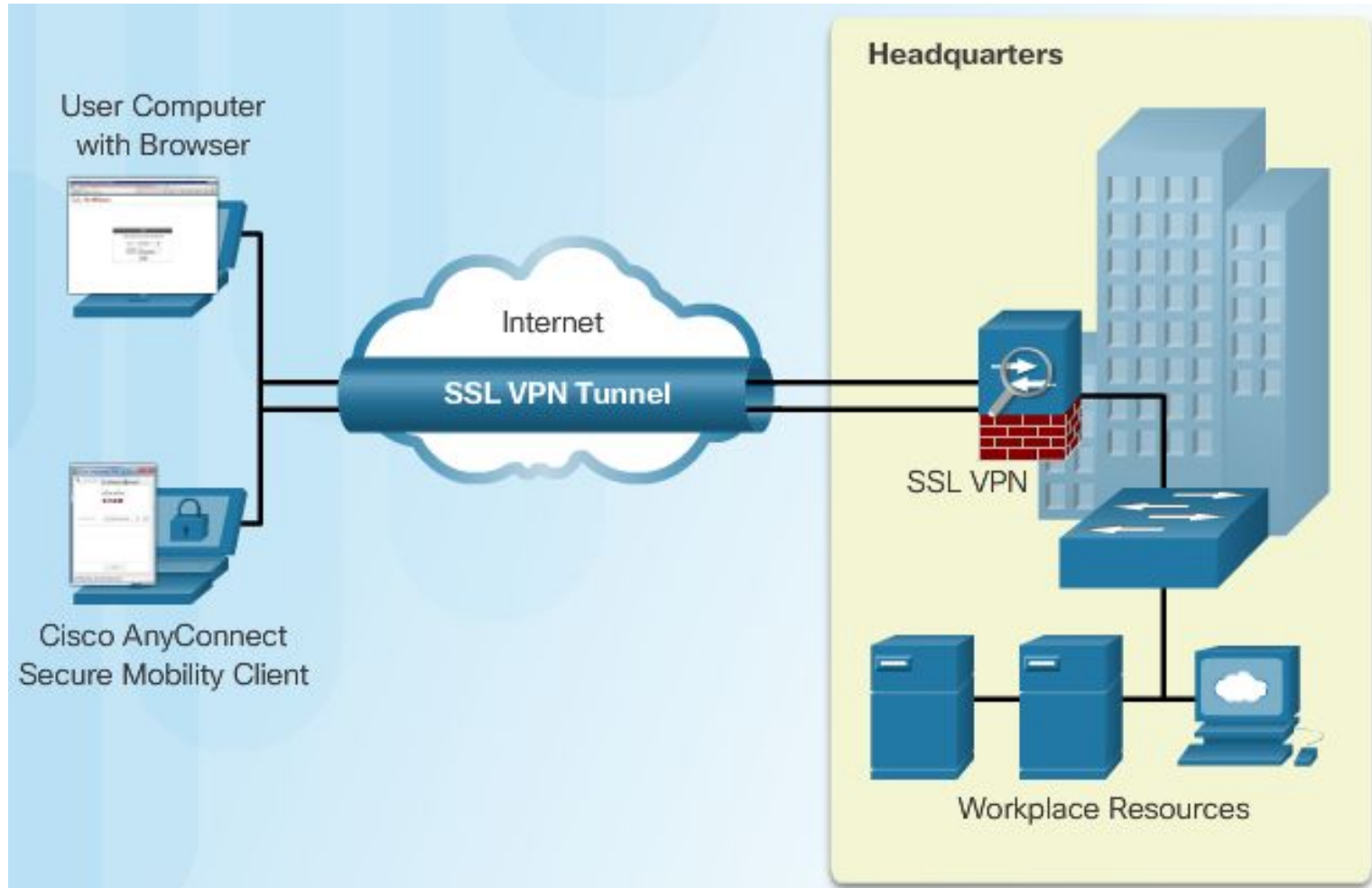
The screenshot shows the Cisco ASDM 7.4 for ASA interface. The 'Wizards' menu is open, and the 'VPN Wizards' option is selected. A sub-menu is displayed, listing several VPN wizard options. The 'IPsec (IKEv1) Remote Access VPN Wizard...' option is highlighted with an orange border.

Host Name: **CCNAS-ASA**
ASA Version: **9.2(3)** Device Uptime: **0d 0h 18m 8s**
ASDM Version: **7.4(1)** Device Type: **ASA 5505**

Interface	IP Address/Mask	Line
dmz	192.168.2.1/24	↑ up
inside	192.168.1.1/24	↑ up
outside	209.165.200.226/27	↑ up

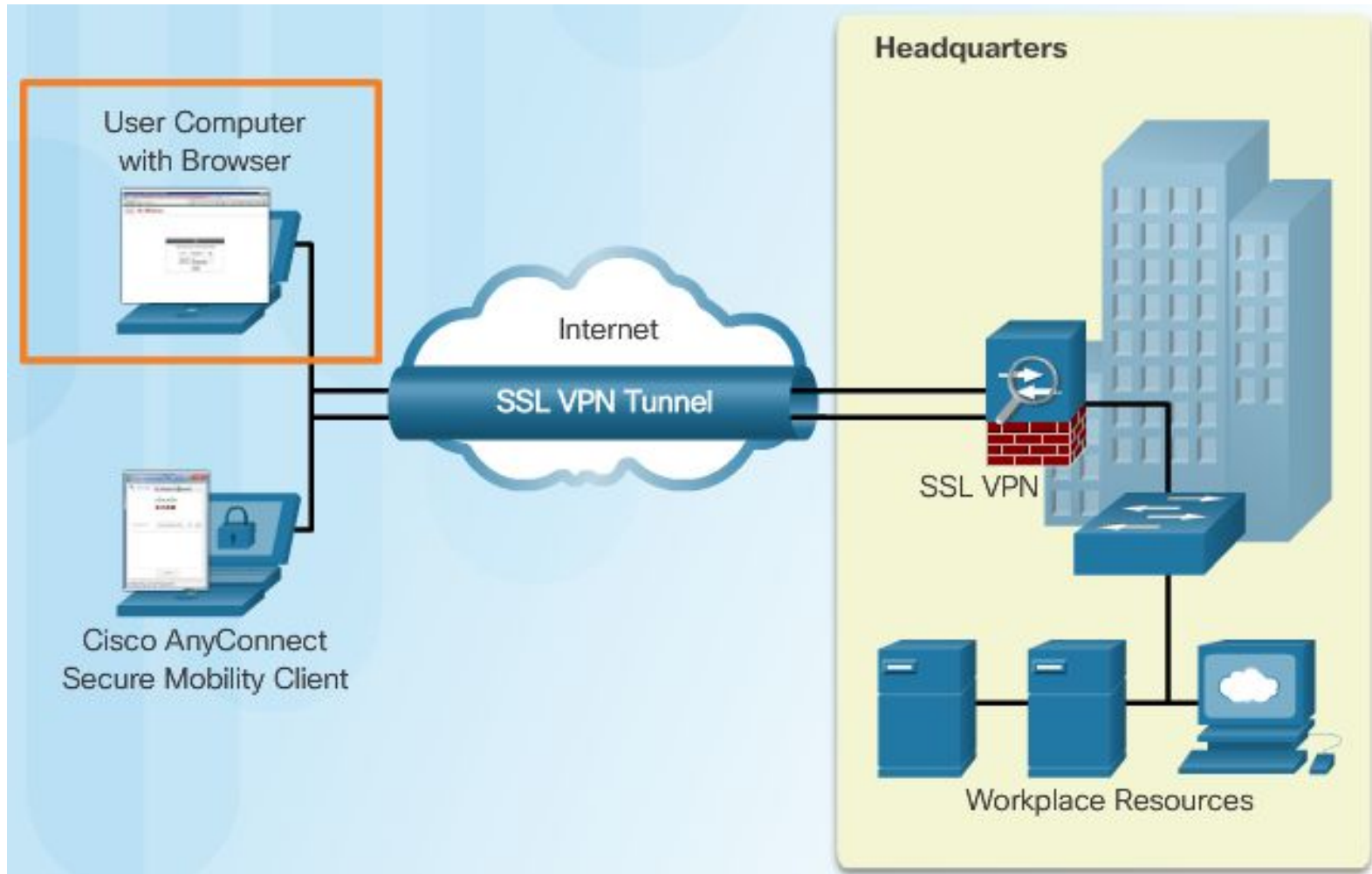
ASA SSL VPNs (Cont.)

Cisco ASA SSL Remote Access VPN Solutions

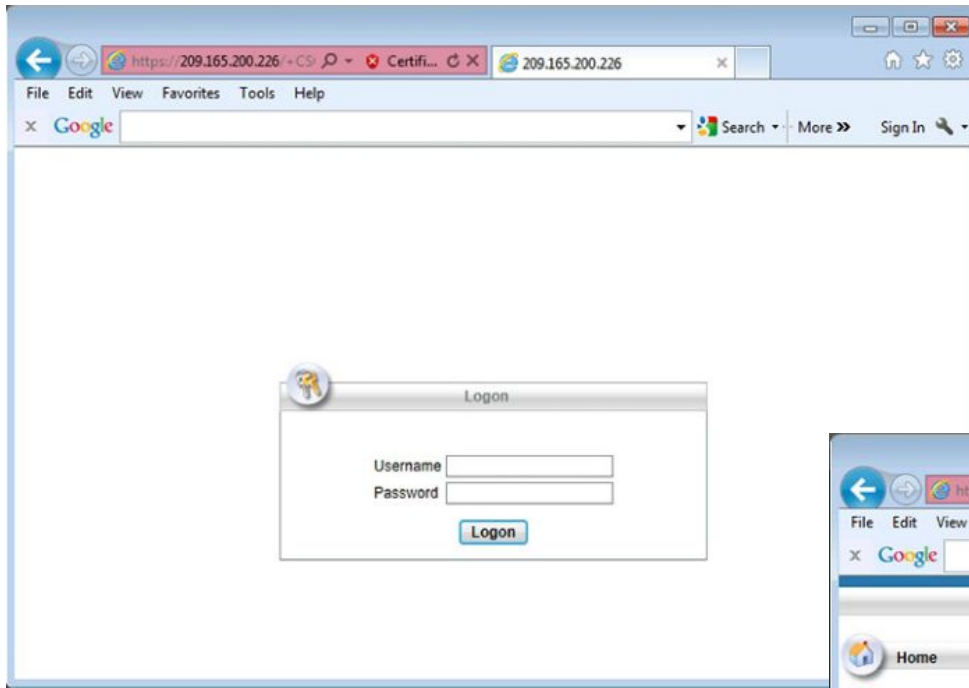


Clientless SSL VPN Solution

Cisco ASA Clientless SSL VPN Deployment

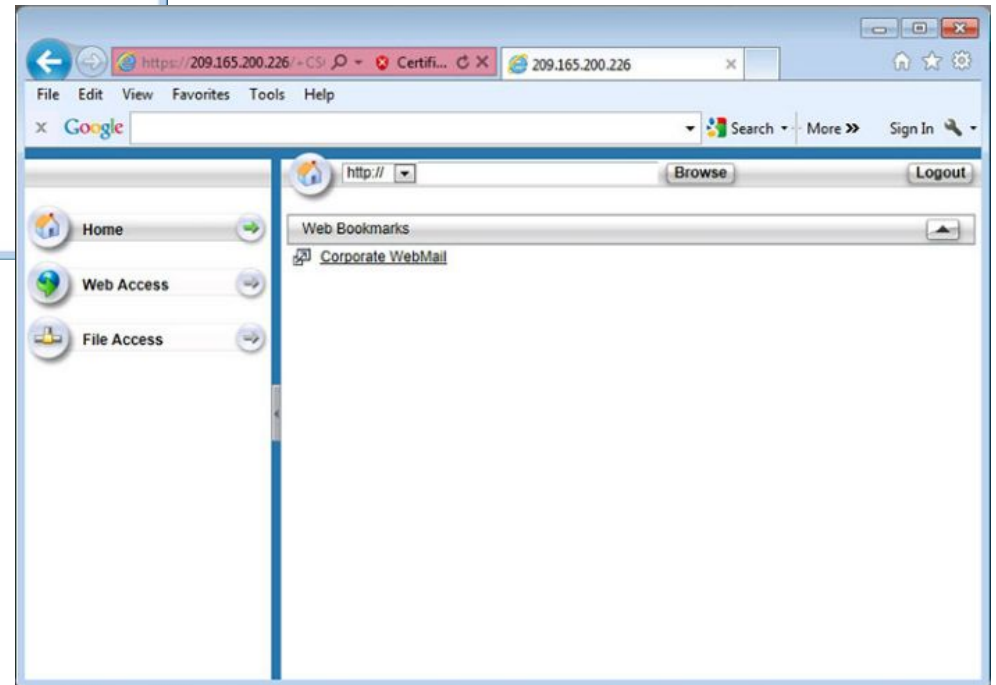


Clientless SSL VPN Solution (Cont.)

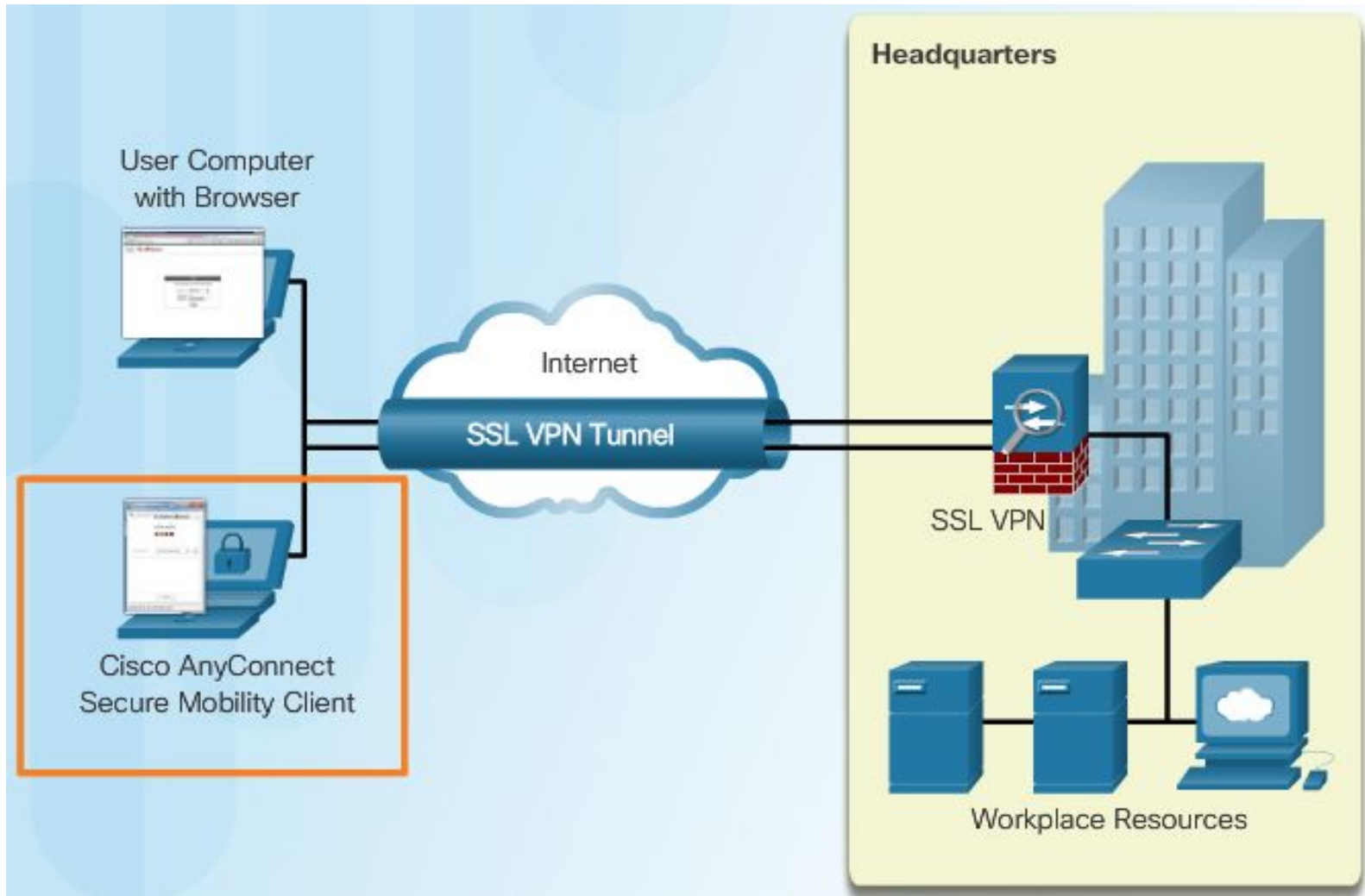


Clientless Login Web page

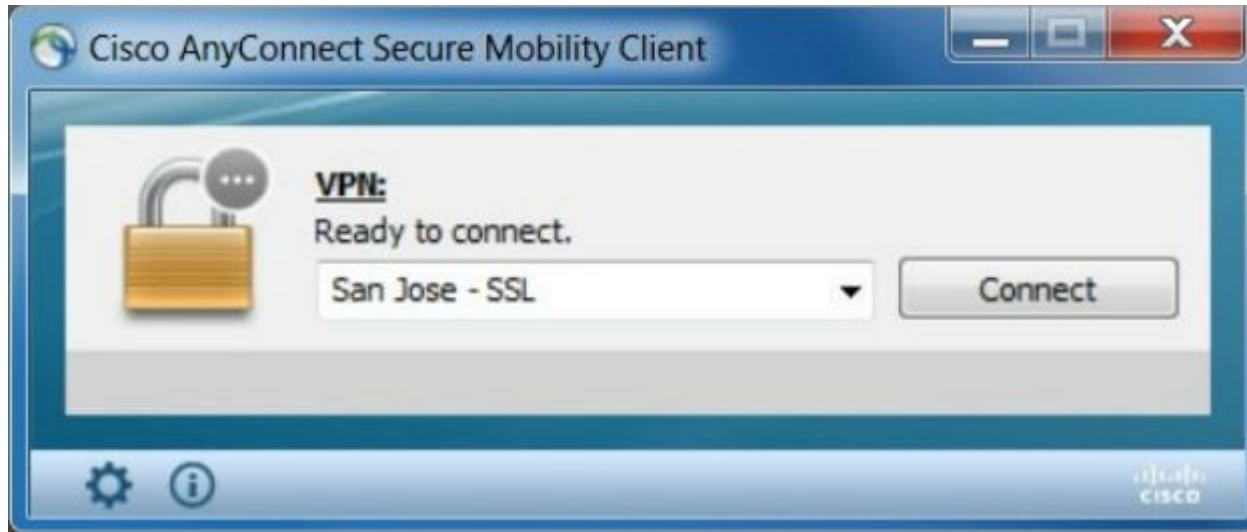
Web Portal Home Page



Client-Based SSL VPN Solution

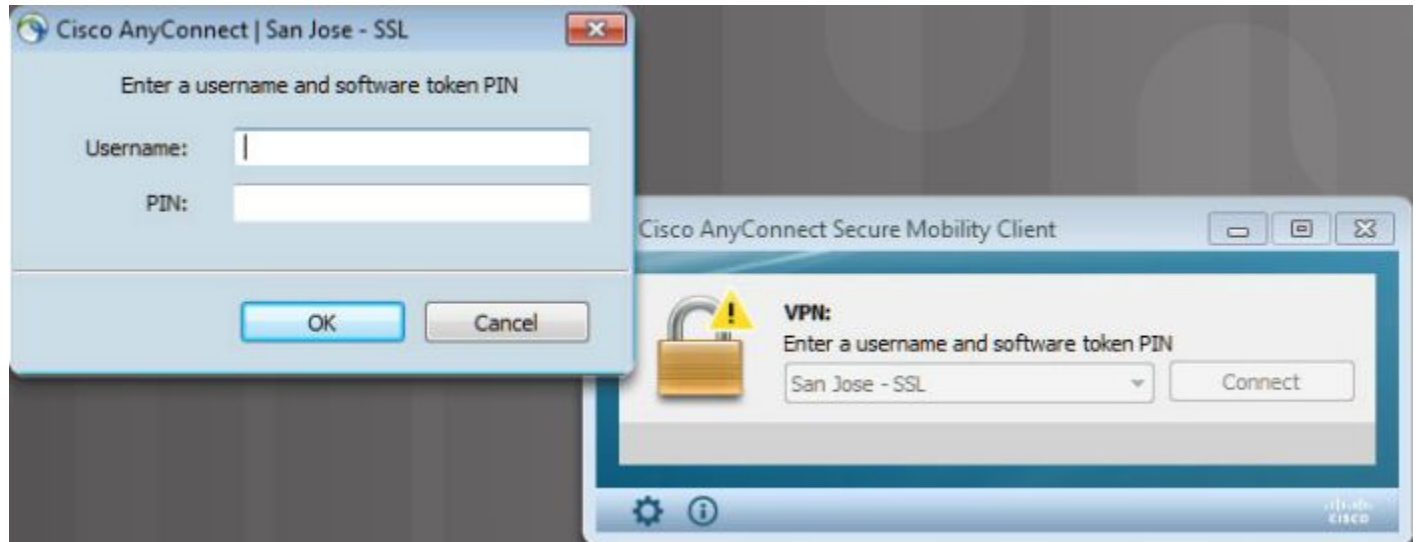


Cisco AnyConnect Secure Mobility Client



AnyConnect
Connection Window

AnyConnect
Authenticate
Window



Cisco AnyConnect Secure Mobility Client (Cont.)



AnyConnect
Authenticated Window

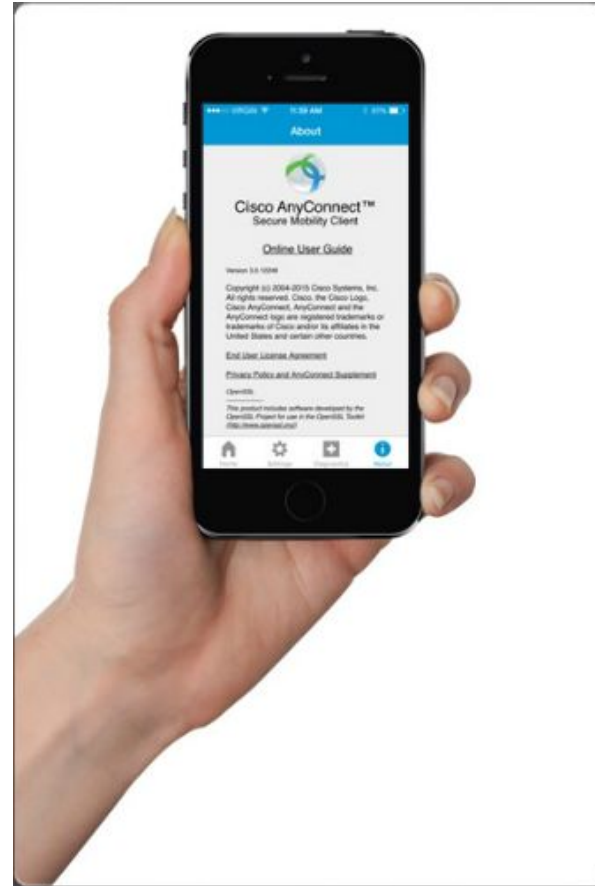
AnyConnect Statistics
Window



AnyConnect for Mobile Devices

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

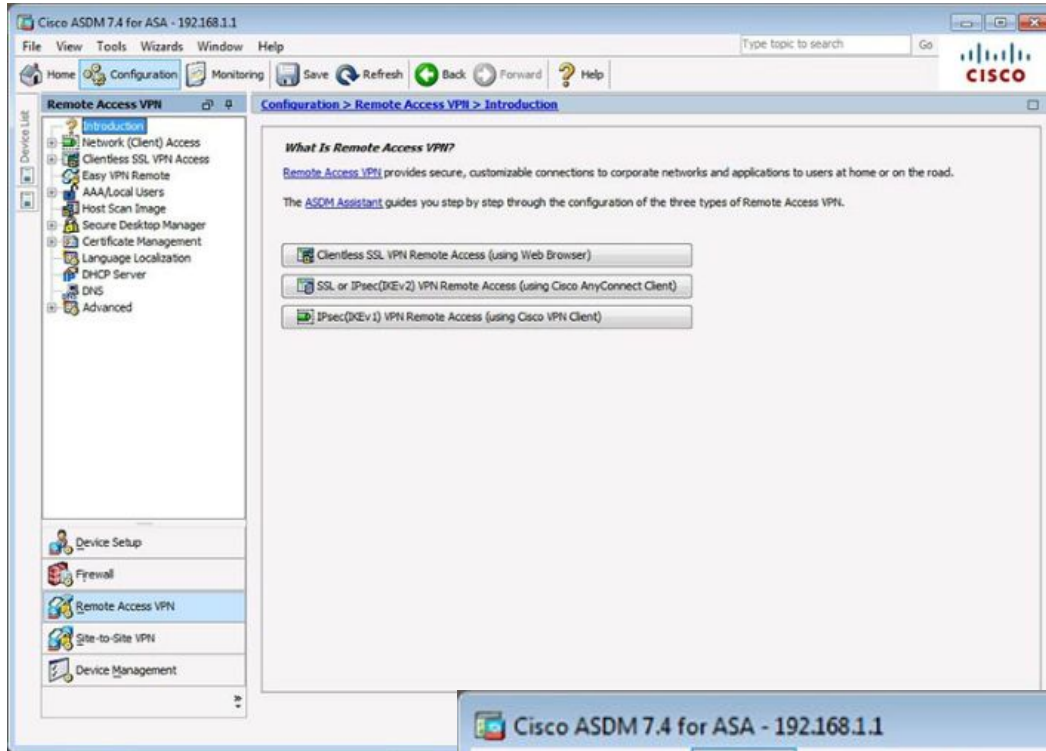
- iOS
- Android
- BlackBerry
- Windows Mobile



Topic 10.2.3: Configuring Clientless SSL VPN

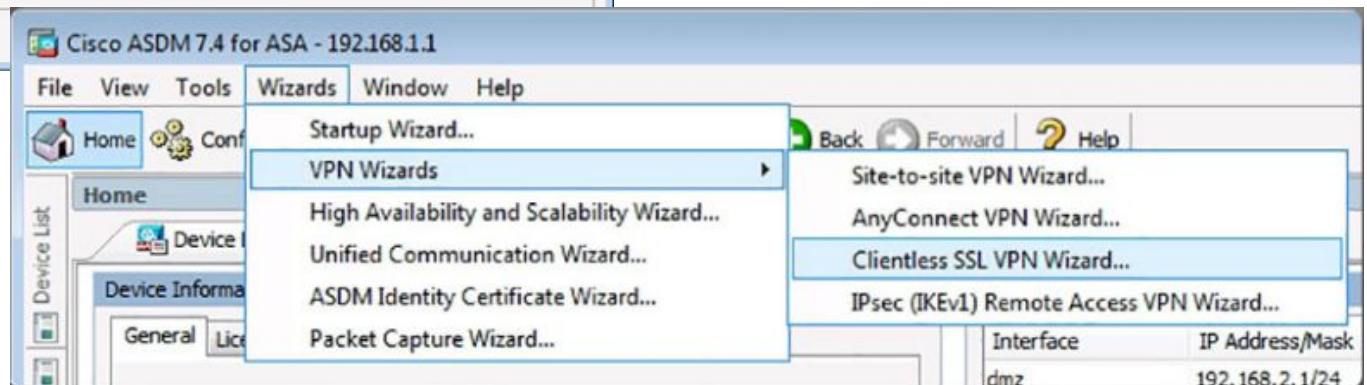


Configuring Clientless SSL VPN on an ASA

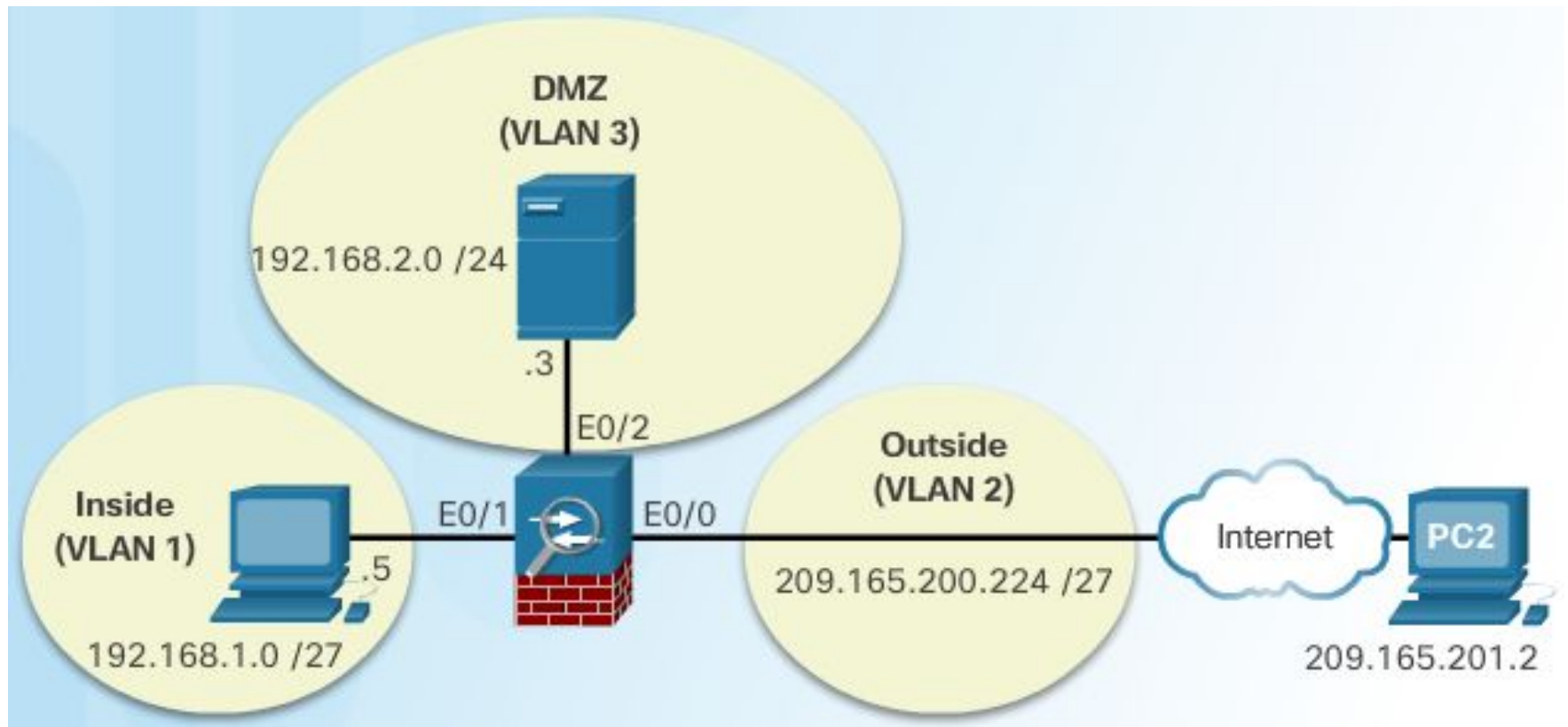


ASDM Assistant

Clientless VPN Wizard



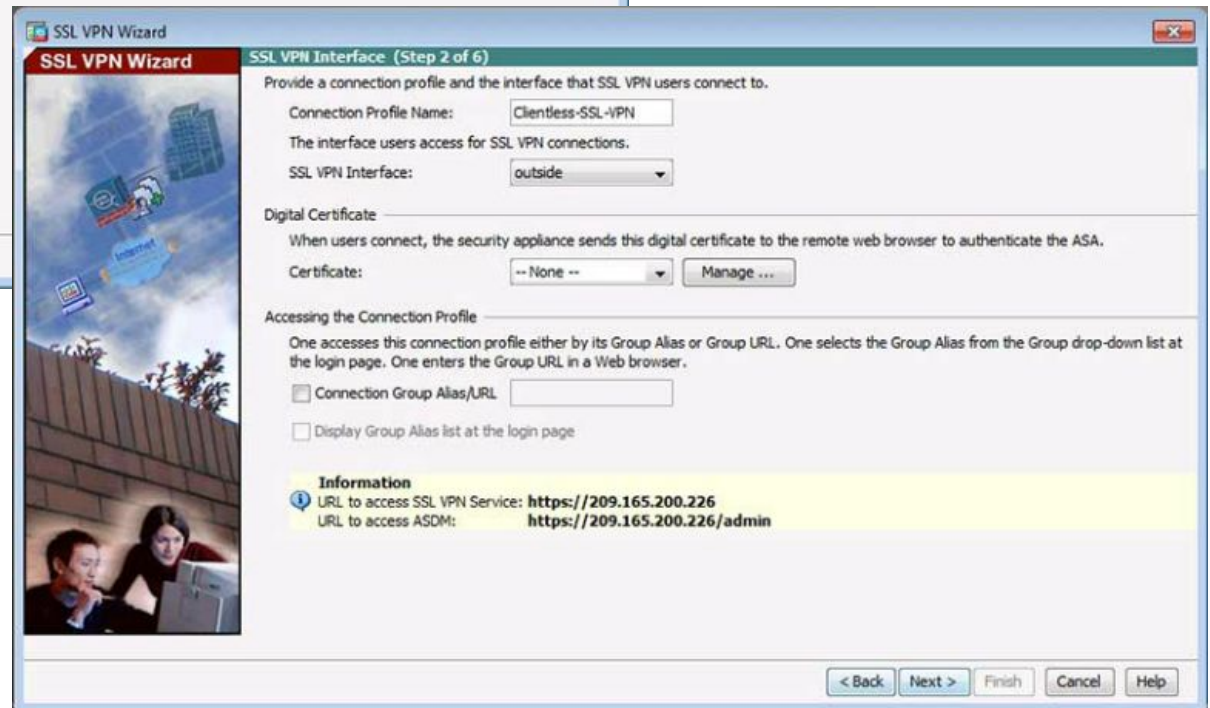
Sample Clientless VPN Topology



Clientless SSL VPN

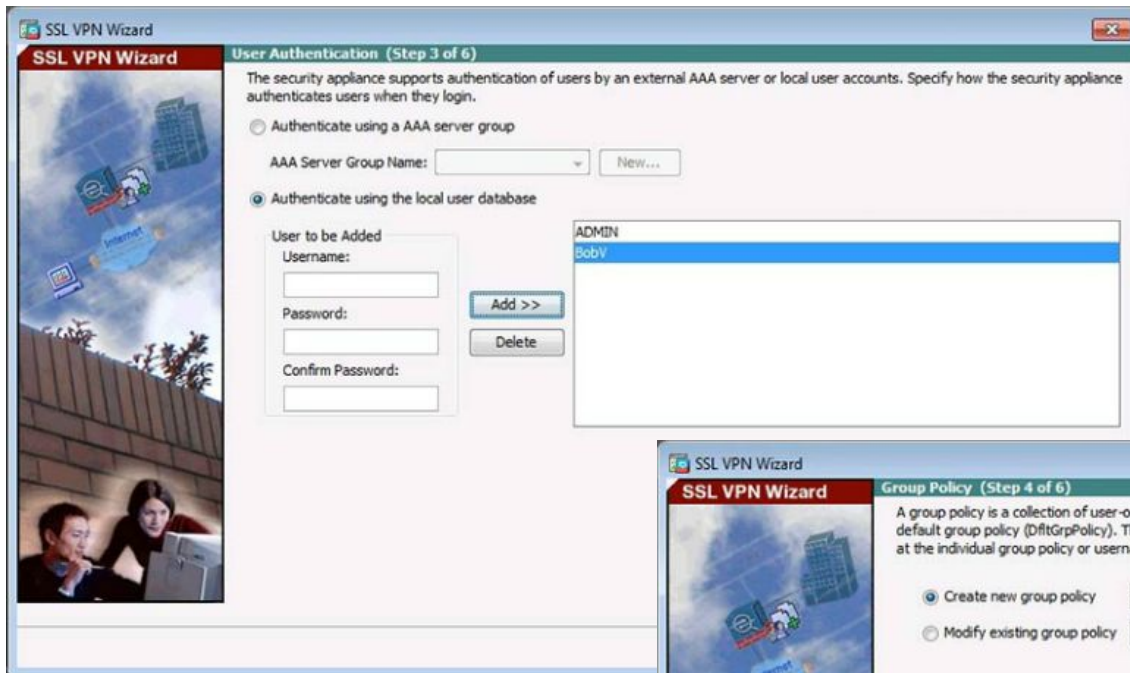


Clientless SSL VPN Introduction Window



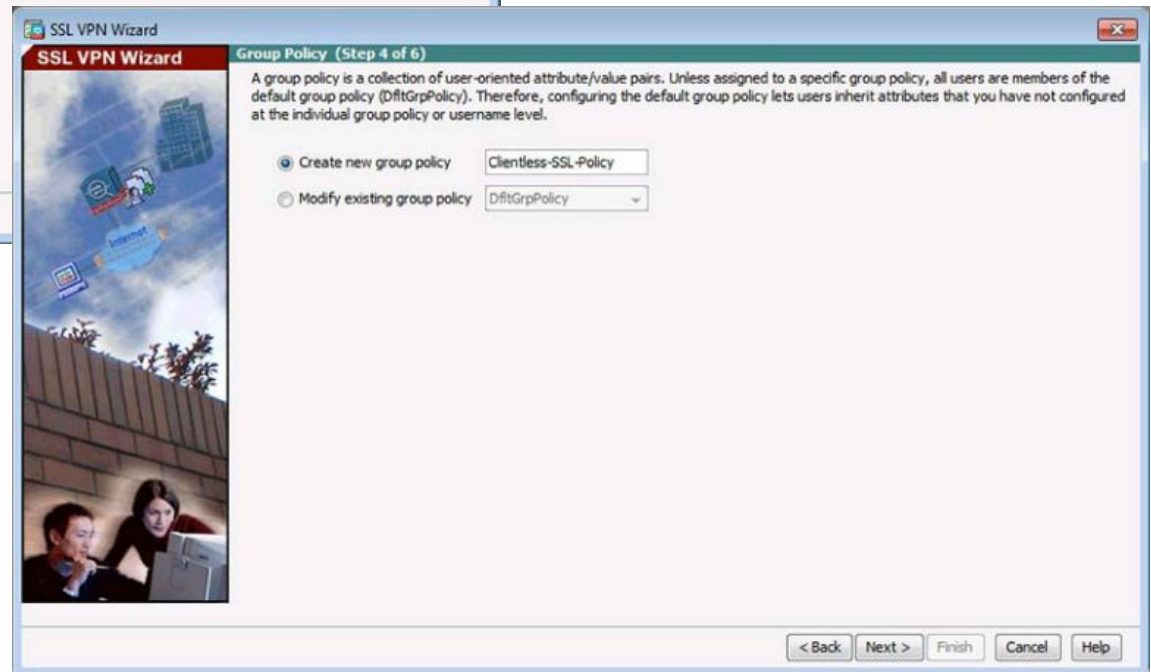
SSL VPN Interface Window

Clientless SSL VPN (Cont.)

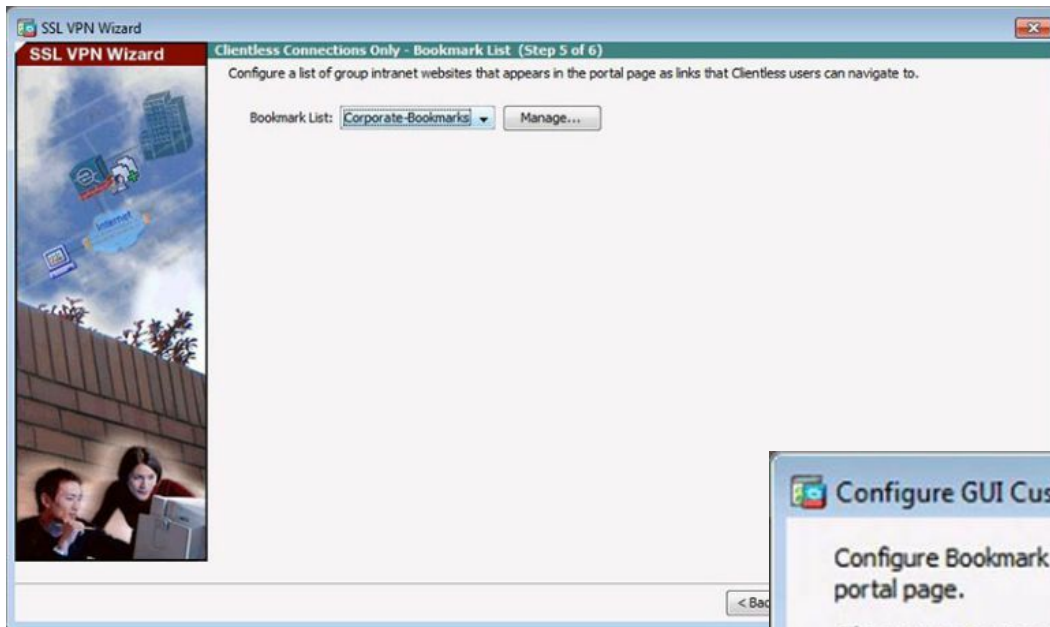


User Authentication Window

Group Policy Window

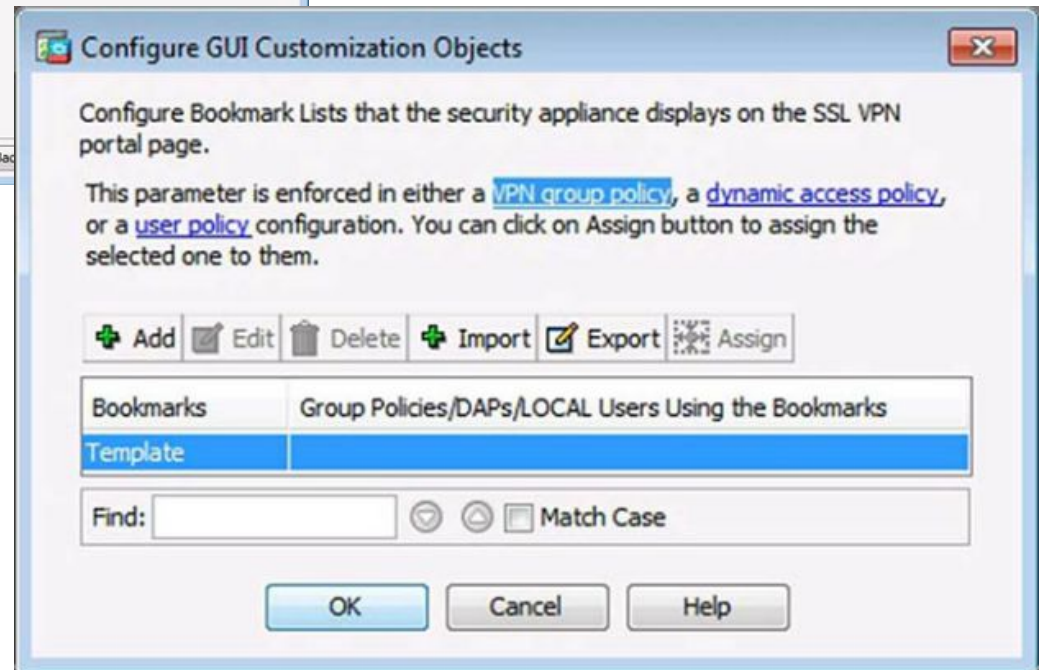


Clientless SSL VPN (Cont.)

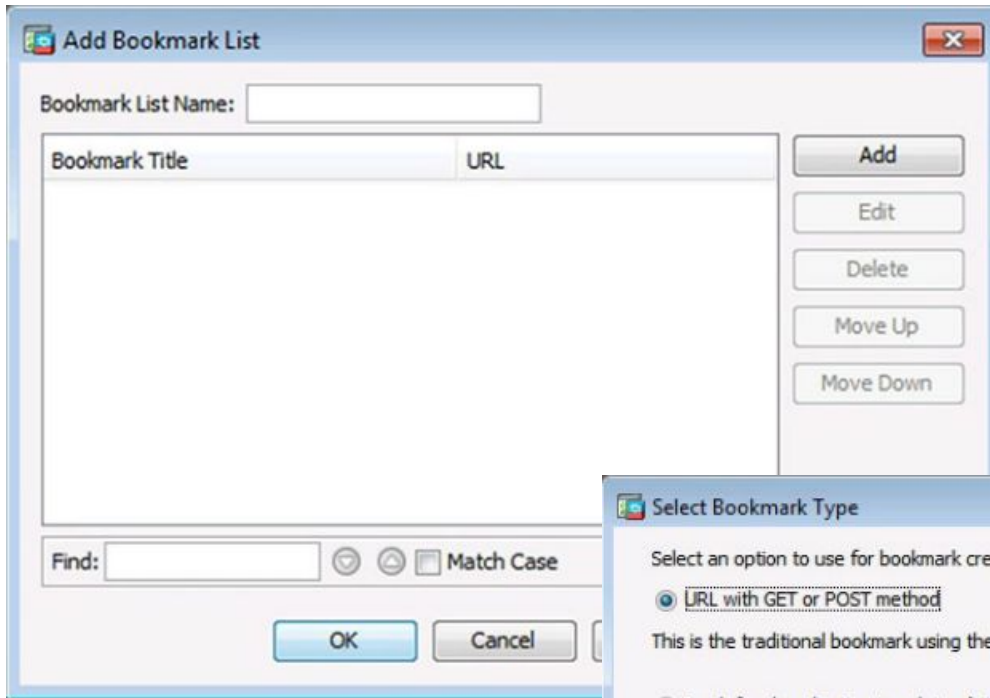


Bookmark List Window

Configure GUI Customization Objects Window

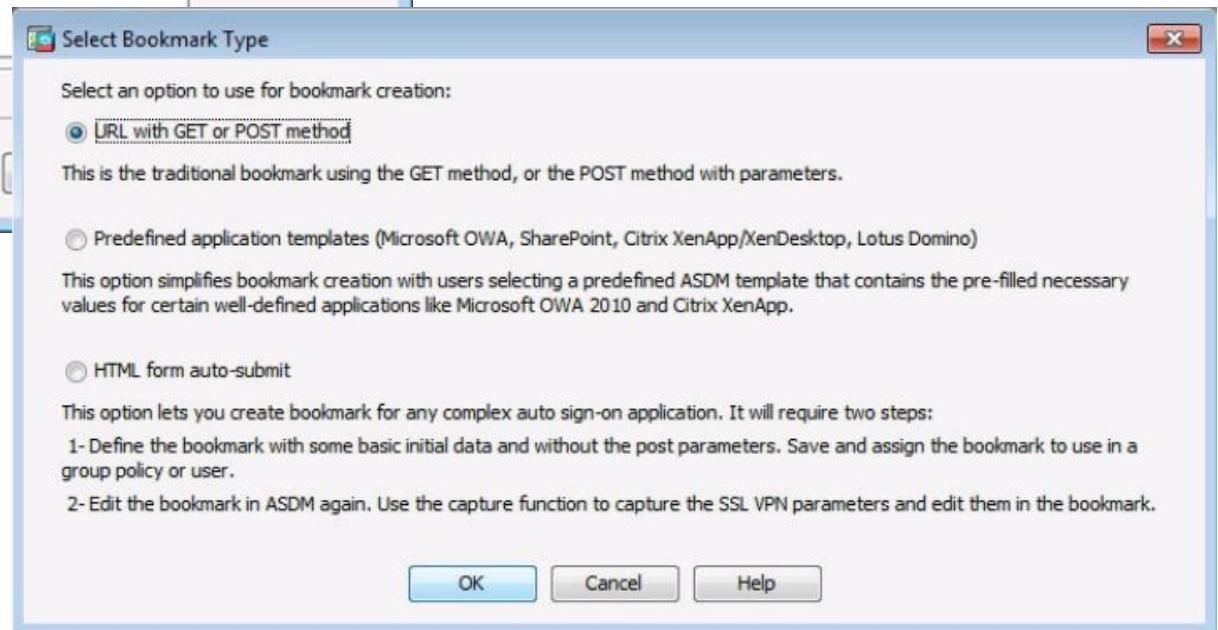


Clientless SSL VPN (Cont.)

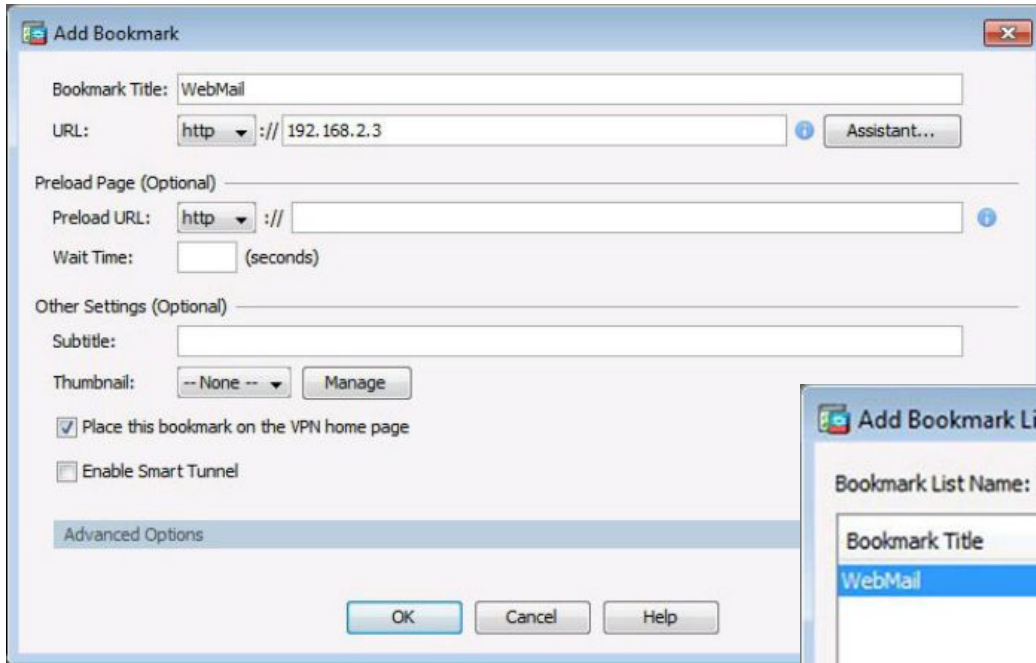


Add Bookmark List Window

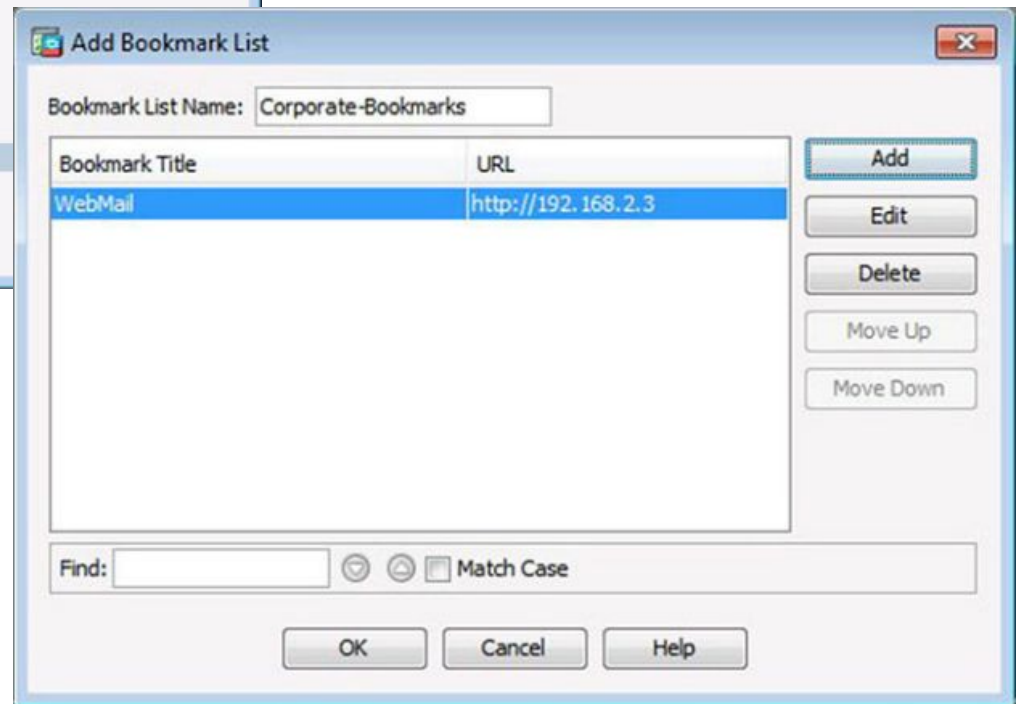
Select Bookmark Type Window



Clientless SSL VPN (Cont.)

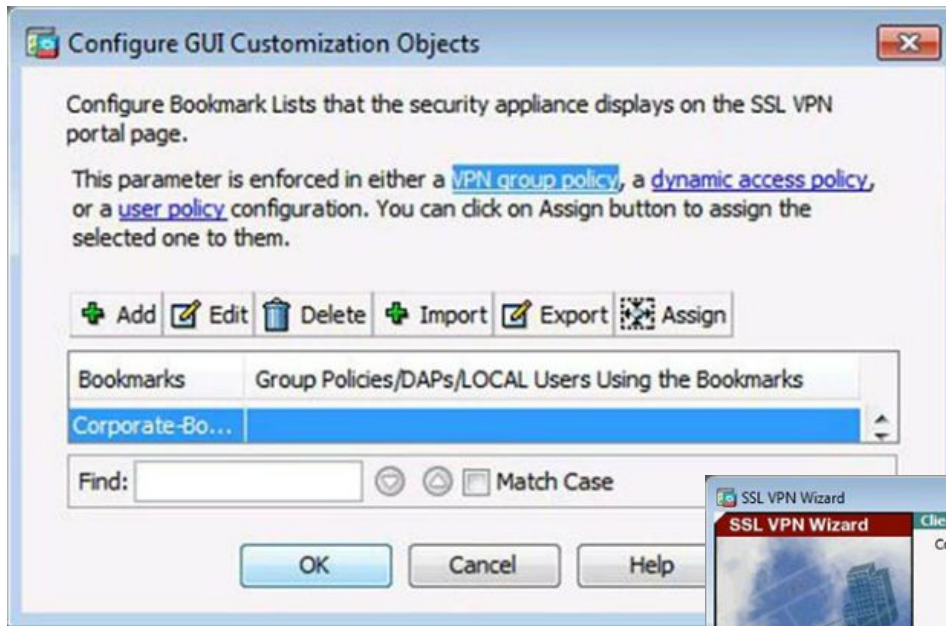


Add Bookmark Window



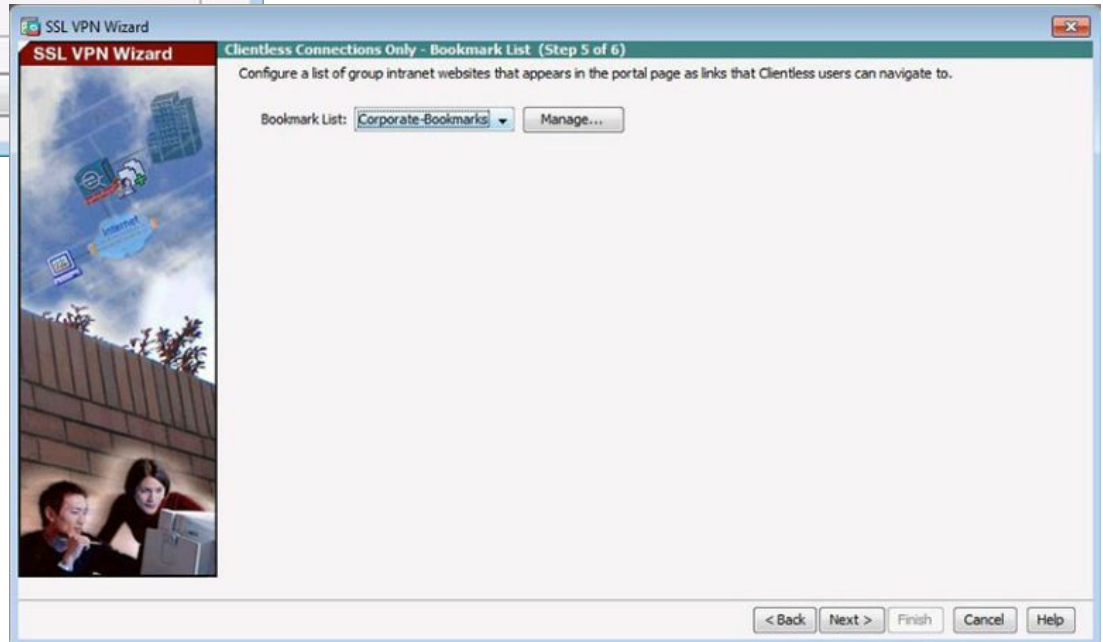
Revised Add Bookmark List Window

Clientless SSL VPN (Cont.)



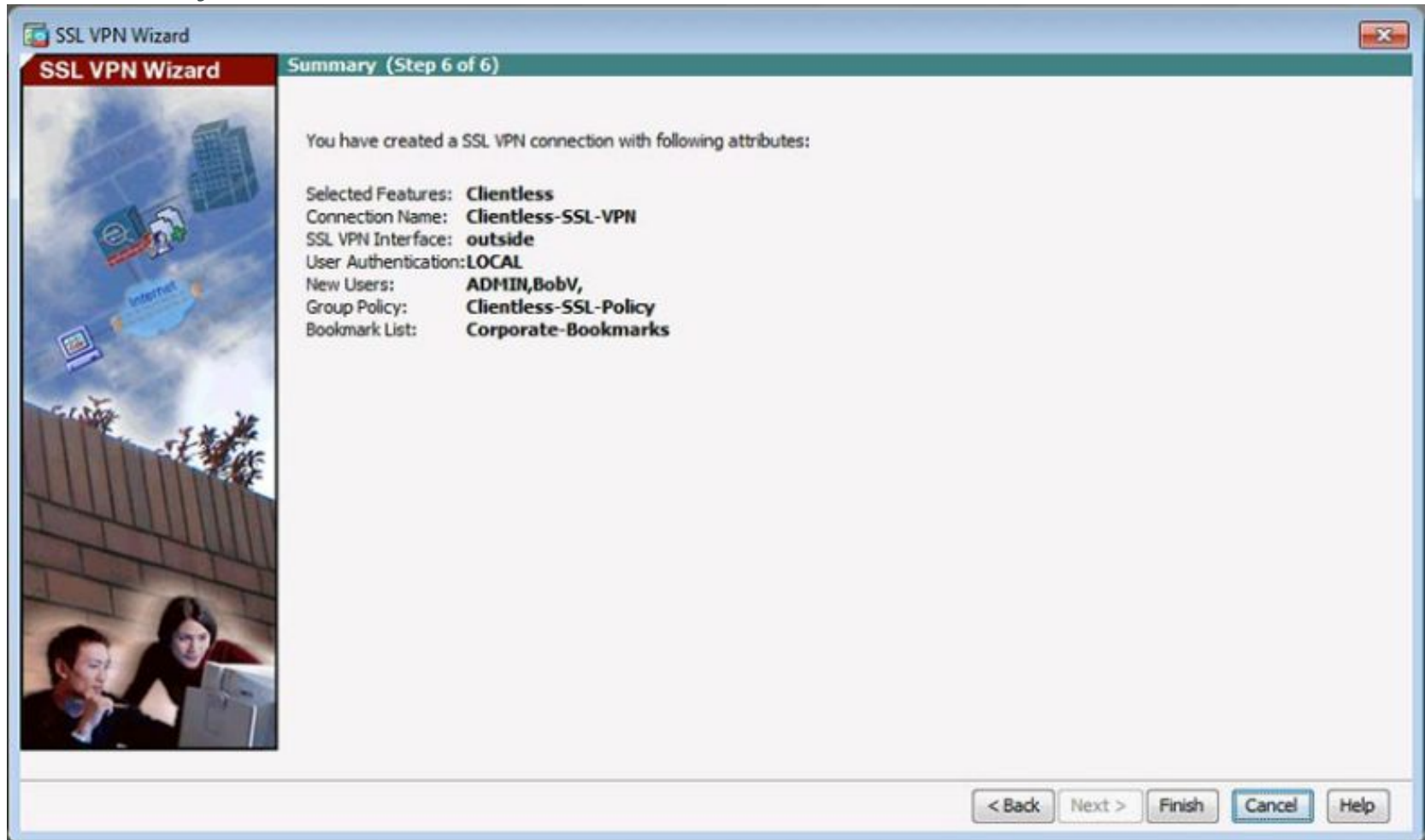
Revised Configure GUI Customization Objects Window

Revised Bookmark List Window



Clientless SSL VPN (Cont.)

Summary Window



Verifying Clientless SSL VPN

The screenshot shows the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles. The left sidebar shows a tree view with 'Connection Profiles' selected under 'Clientless SSL VPN Access'. The main content area is divided into sections: 'Access Interfaces', 'Login Page Setting', and 'Connection Profiles'.

Access Interfaces
Enable interfaces for clientless SSL VPN access.

Interface	Allow Access
outside	<input checked="" type="checkbox"/>
dmz	<input type="checkbox"/>
inside	<input type="checkbox"/>

Bypass interface access lists for inbound VPN sessions
Access lists from group policy and user policy always apply to the traffic.

Login Page Setting

- Allow user to select connection profile on the login page.
- Allow user to enter internal password on the login page.
- Shutdown portal login page.

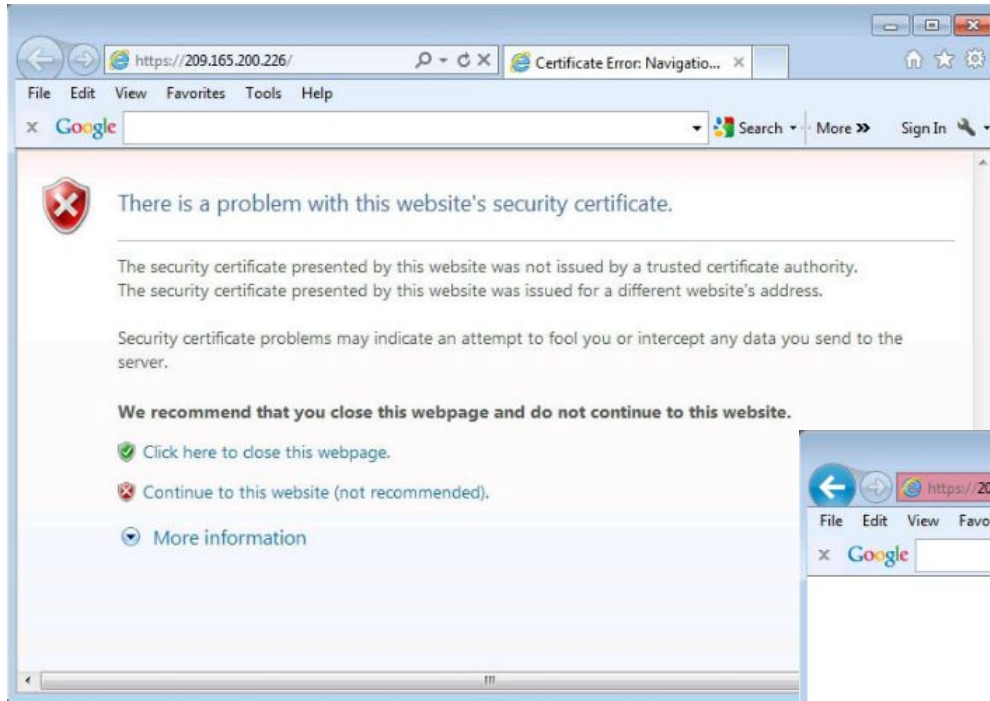
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Buttons: Add, Edit, Delete, Find: [text box], Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultIRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
Clientless-SSL-VPN	<input checked="" type="checkbox"/>		AAA(LOCAL)	Clientless-SSL-Policy

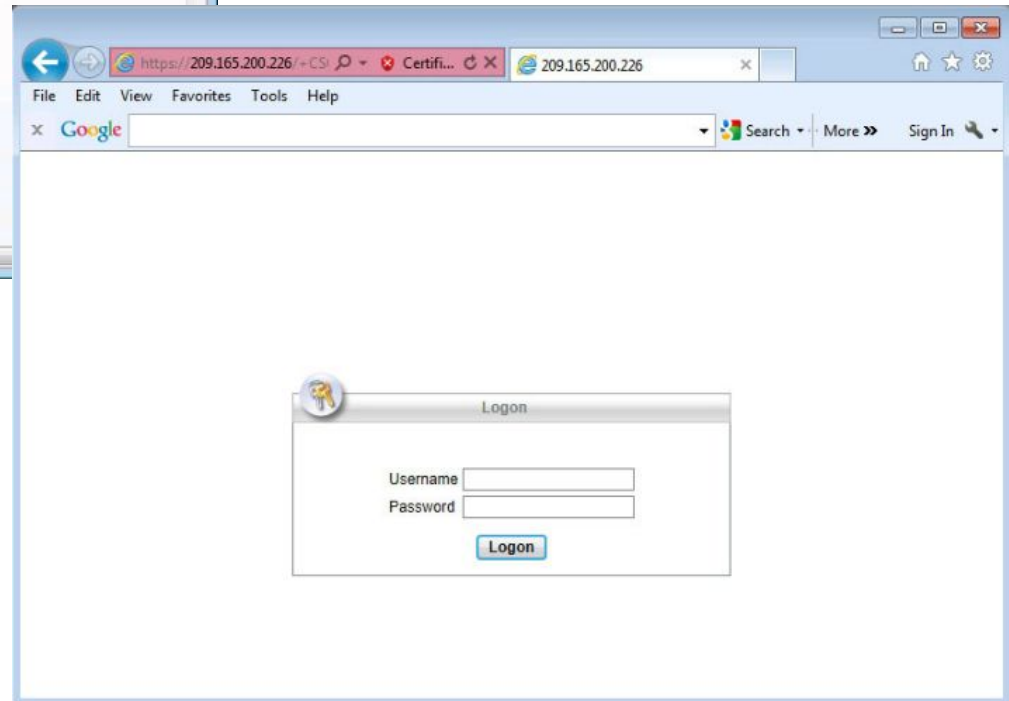
Buttons: Apply, Reset

Testing the Clientless SSL VPN Connection

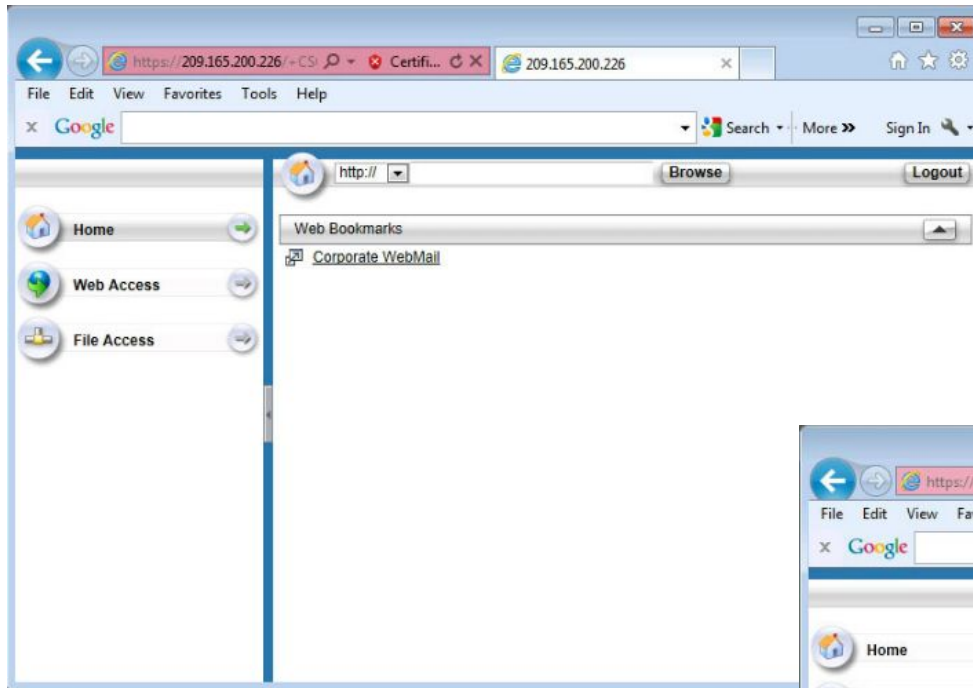


Security Certificate Window

Logon Window

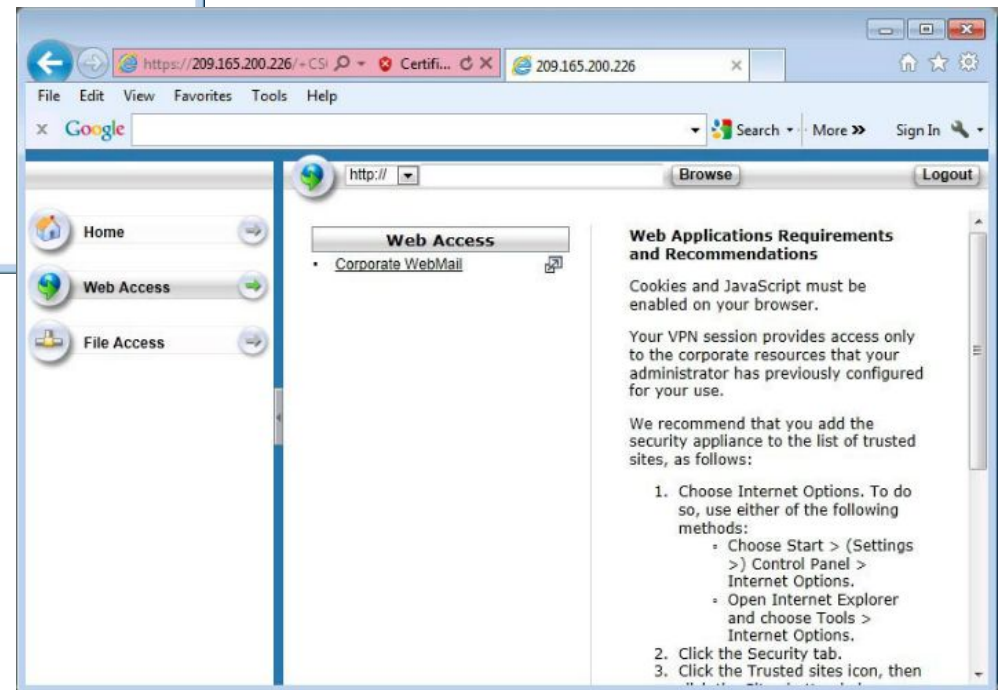


Testing the Clientless SSL VPN Connection (Cont.)

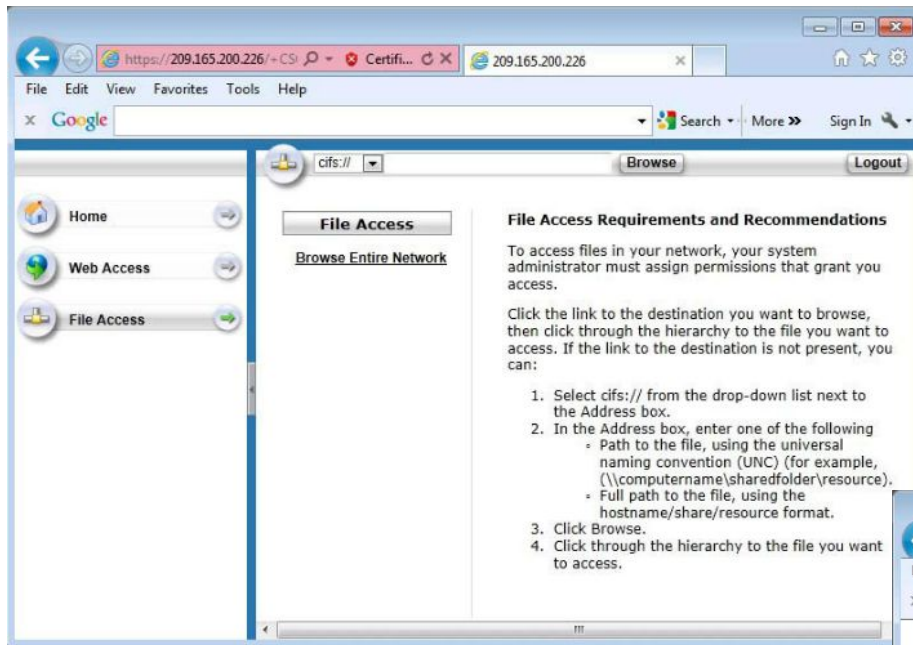


Web Portal Home Page

Web Portal Web Access Page

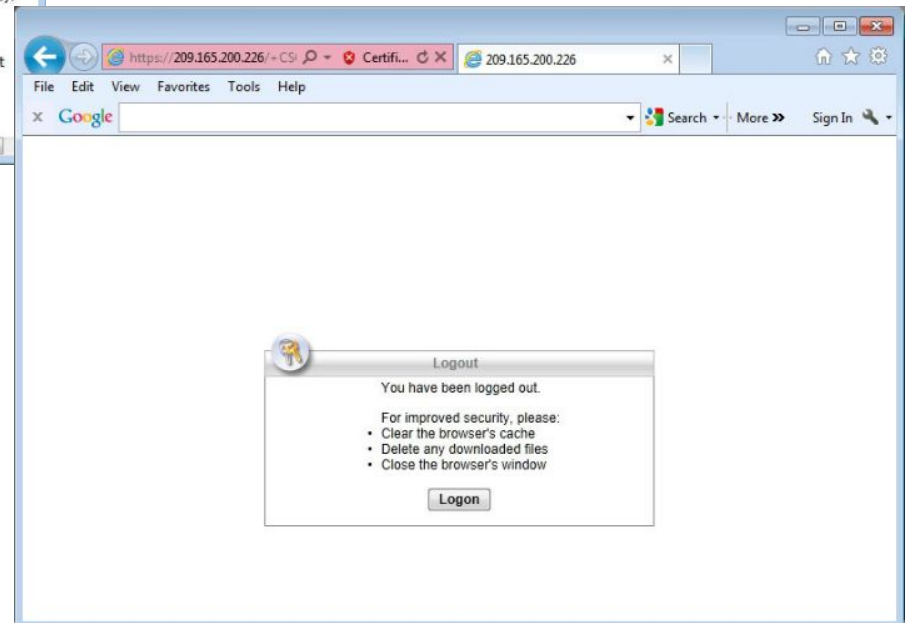


Testing the Clientless SSL VPN Connection (Cont.)



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

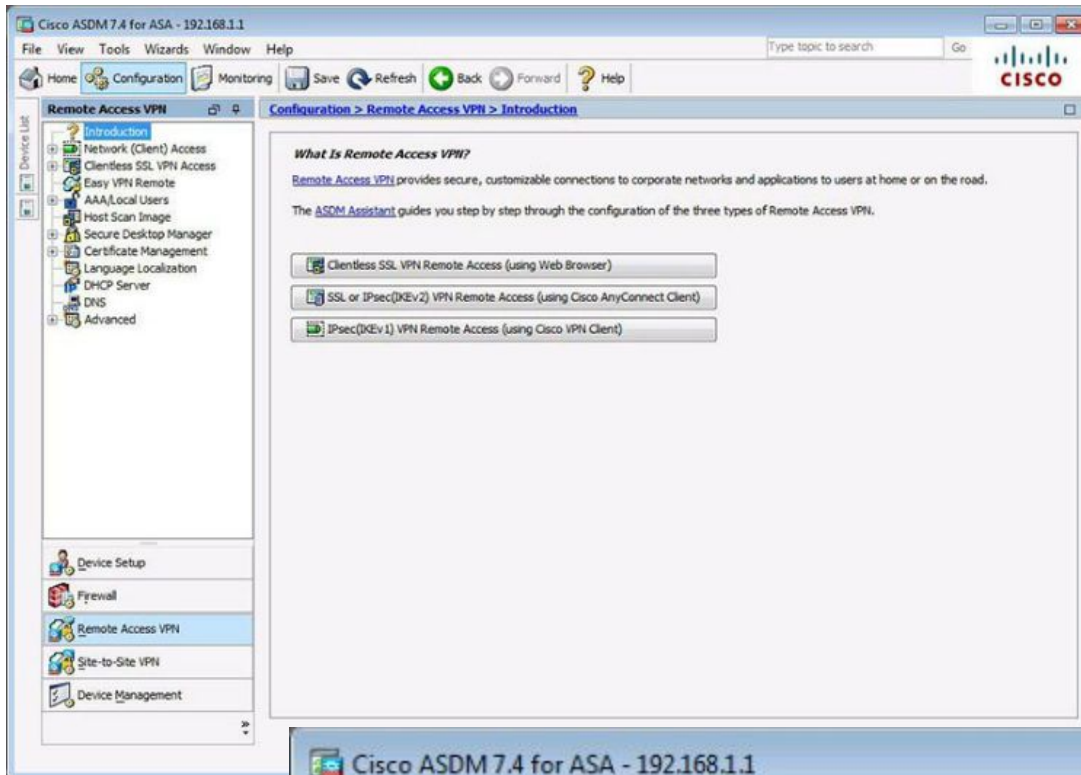
username ADMIN password 3MBOT/Mpbpc4KbOv encrypted privilege 0
username ADMIN attributes
  vpn-group-policy Clientless-SSL-Policy
username BobV password AOvleG/KWkzEwhtN encrypted privilege 0
username BobV attributes
  vpn-group-policy Clientless-SSL-Policy

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

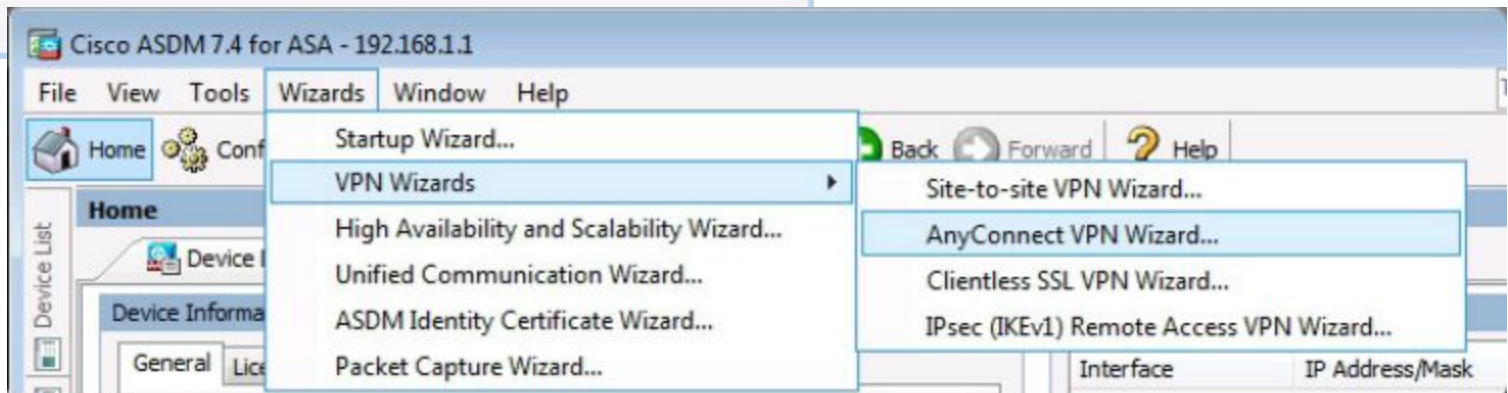


Configuring SSL VPN AnyConnect

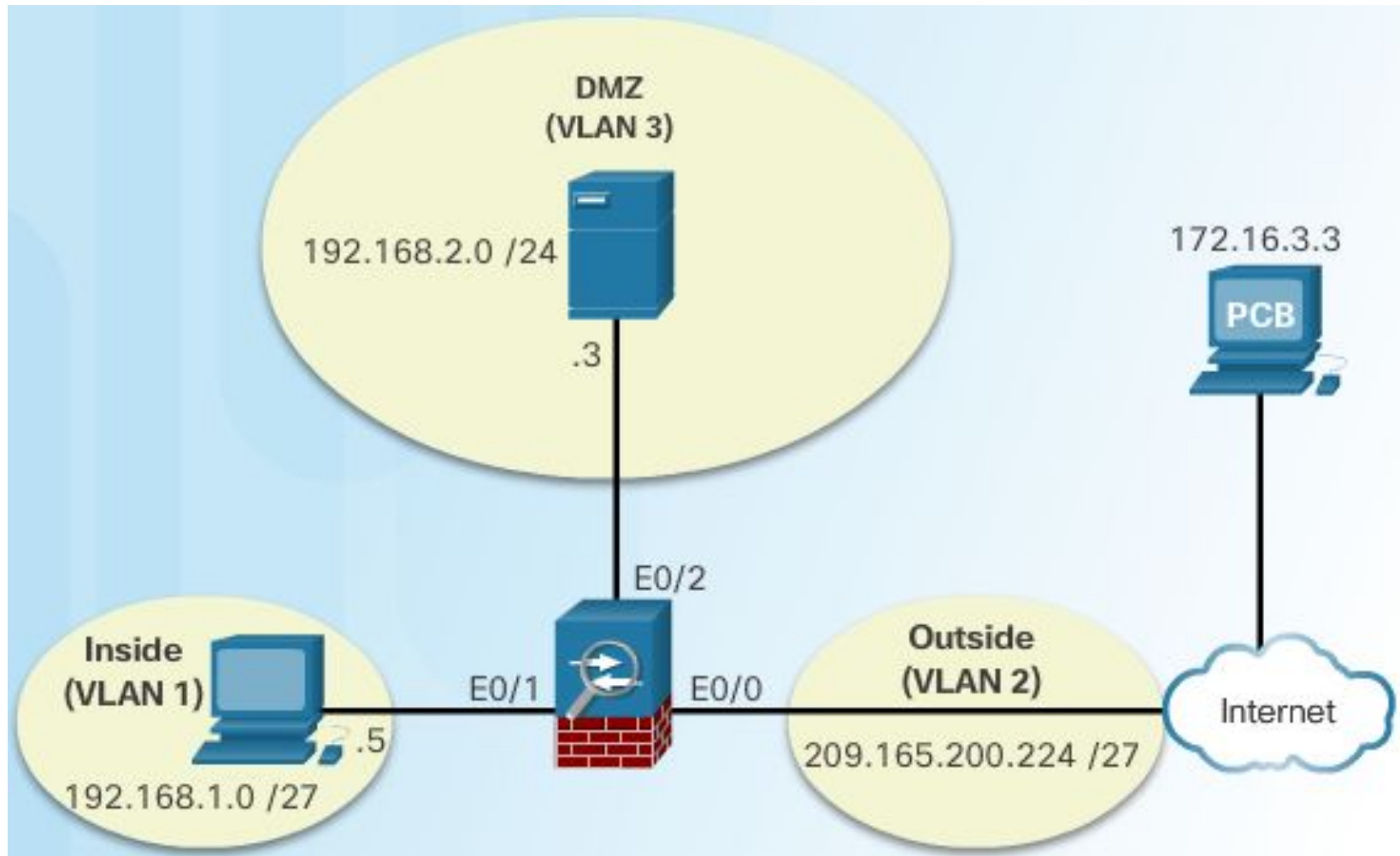


ASDM Assistant

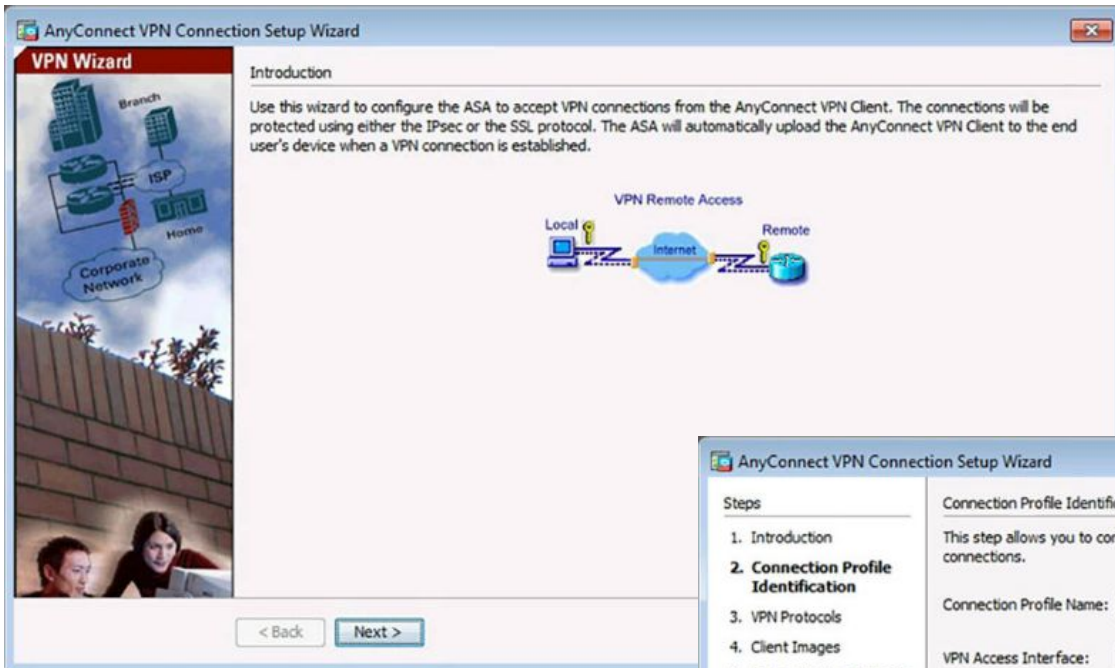
Client-Based VPN Wizard



Sample SSL VPN Topology

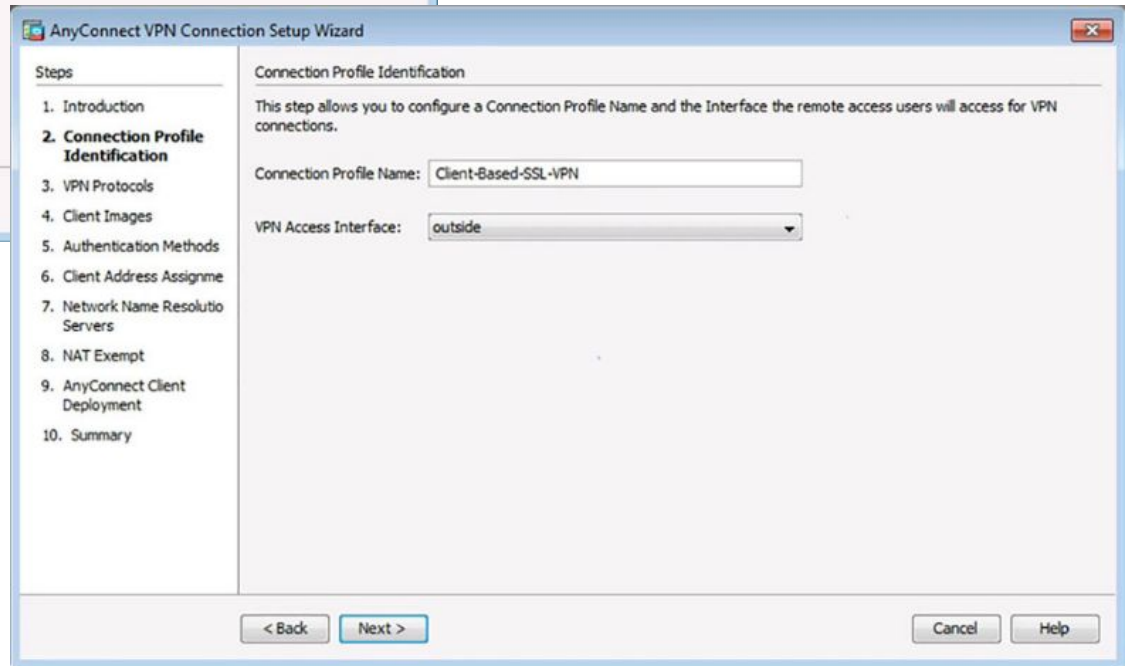


AnyConnect SSL VPN



AnyConnect VPN Wizard Introduction Window

Connection Profile Identification Window

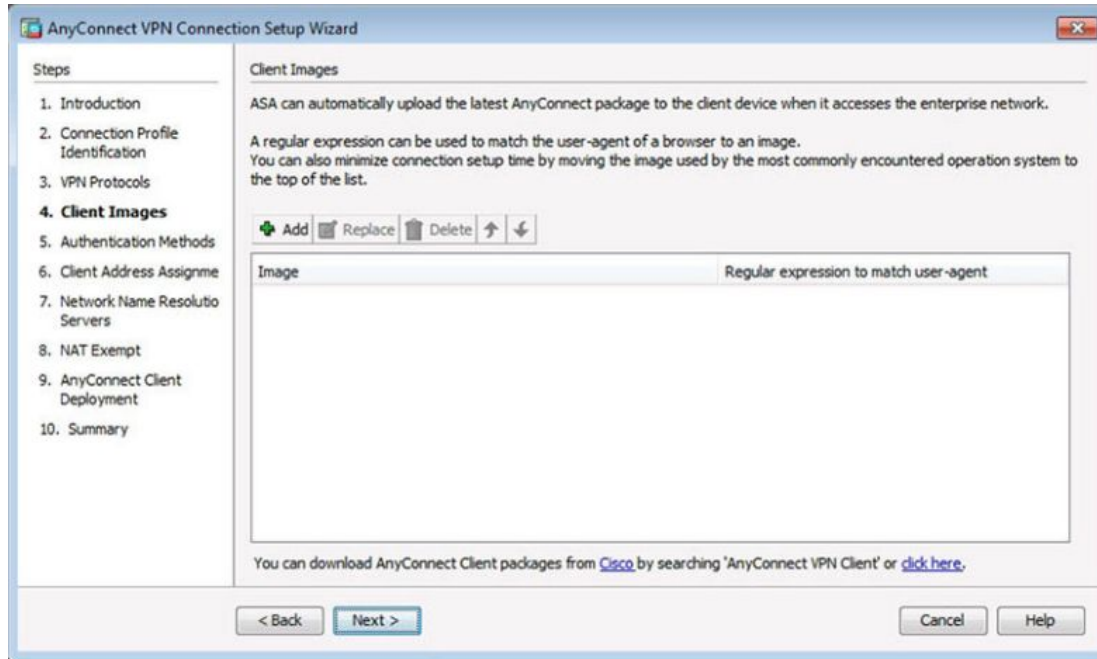


AnyConnect SSL VPN (Cont.)

VPN Protocols Window

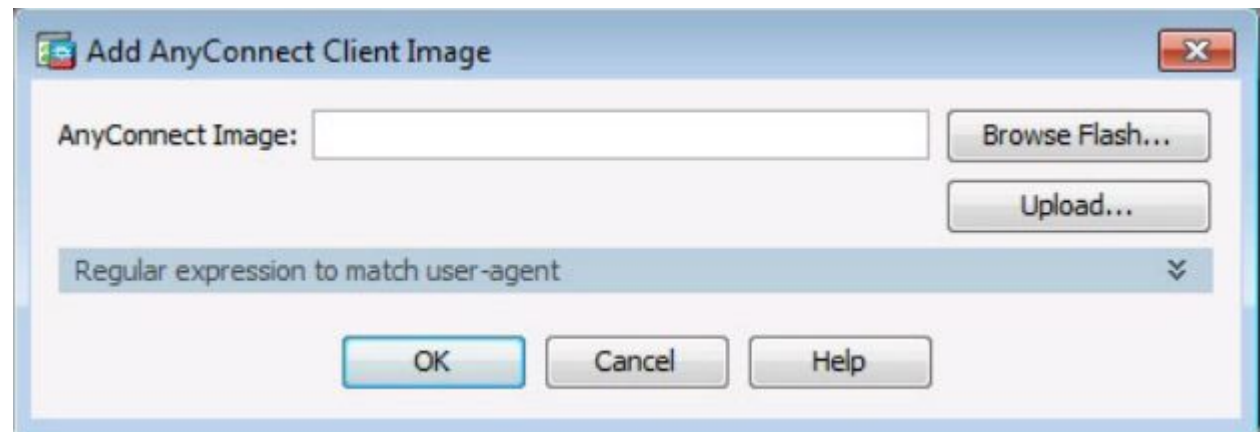
The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. The title bar reads 'AnyConnect VPN Connection Setup Wizard'. On the left, a 'Steps' pane lists 10 steps, with '3. VPN Protocols' selected and highlighted. The main area is titled 'VPN Protocols' and contains the following text: 'AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.' Below this text are two checkboxes: 'SSL' (checked) and 'IPsec' (unchecked). Further down, there is a 'Device Certificate' label followed by a text input field containing '-- None --' and a 'Manage...' button. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

AnyConnect SSL VPN (Cont.)

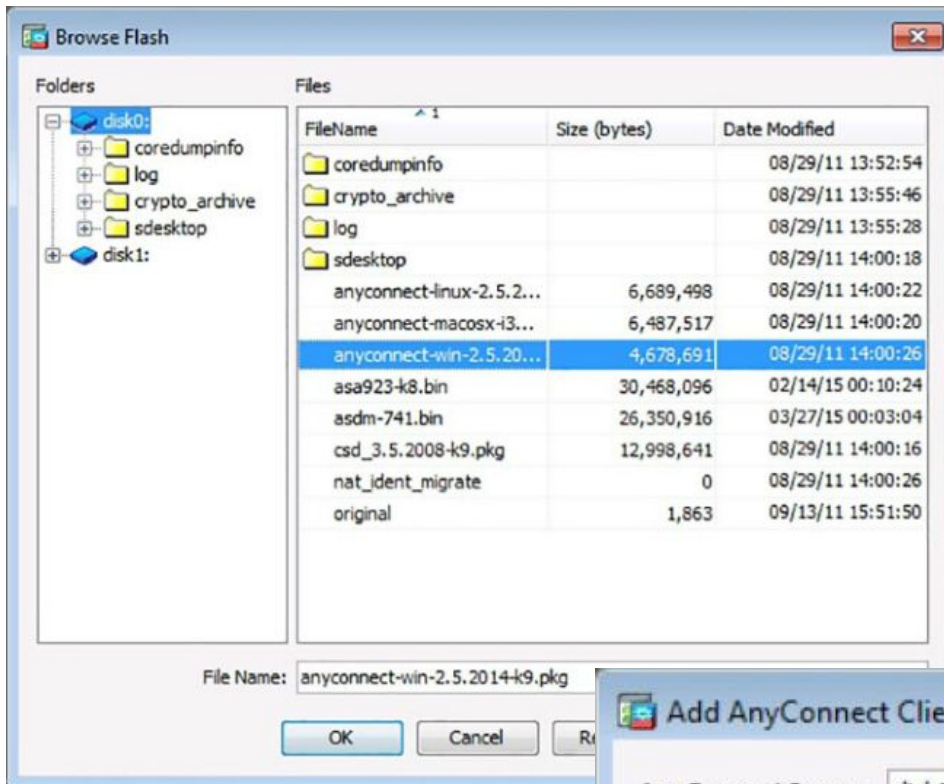


Client Images Window

Add AnyConnect Client Image Window

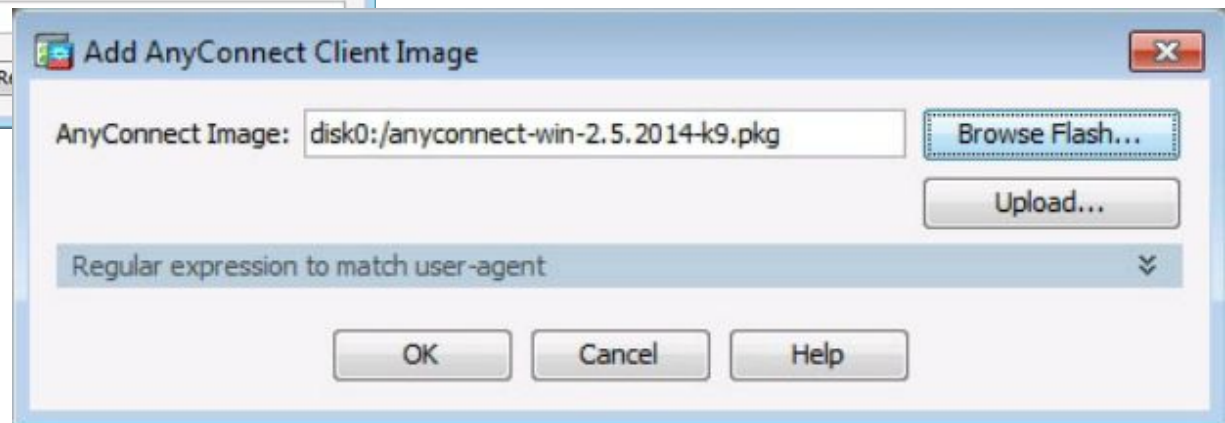


AnyConnect SSL VPN (Cont.)



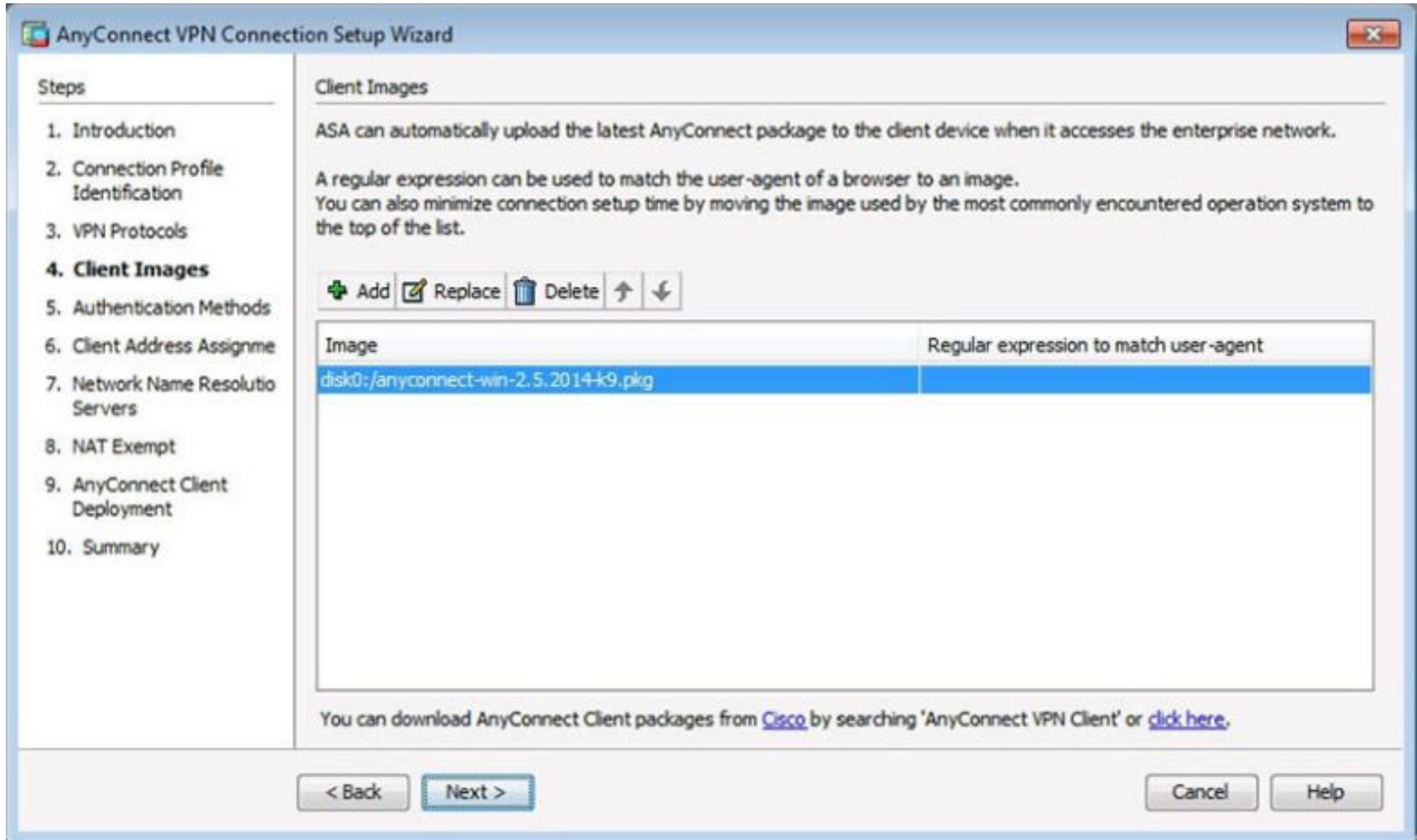
Browse Flash Window

Add AnyConnect Client Image Window



AnyConnect SSL VPN (Cont.)

Completed Client Images Window



AnyConnect SSL VPN (Cont.)

Authentication Methods Window

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window, specifically the 'Authentication Methods' step. The window title is 'AnyConnect VPN Connection Setup Wizard'. On the left, a 'Steps' pane lists 10 steps, with '5. Authentication Methods' highlighted. The main area is titled 'Authentication Methods' and contains the following text: 'This step lets you specify the location of the authentication server. You can click on the "New..." button to create a new server group.' Below this text is a label 'AAA Server Group:' followed by a dropdown menu showing 'LOCAL' and a 'New...' button. A horizontal line separates this section from the 'Local User Database Details' section. In the 'Local User Database Details' section, there is a 'User to be Added' area with three input fields: 'Username:', 'Password:', and 'Confirm Password:'. To the right of these fields are 'Add >>' and 'Delete' buttons. A list box on the right contains the text 'ADMIN' and 'BobV'. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
- 5. Authentication Methods**
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Authentication Methods

This step lets you specify the location of the authentication server. You can click on the "New..." button to create a new server group.

AAA Server Group: LOCAL New...

Local User Database Details

User to be Added

Username:

Password:

Confirm Password:

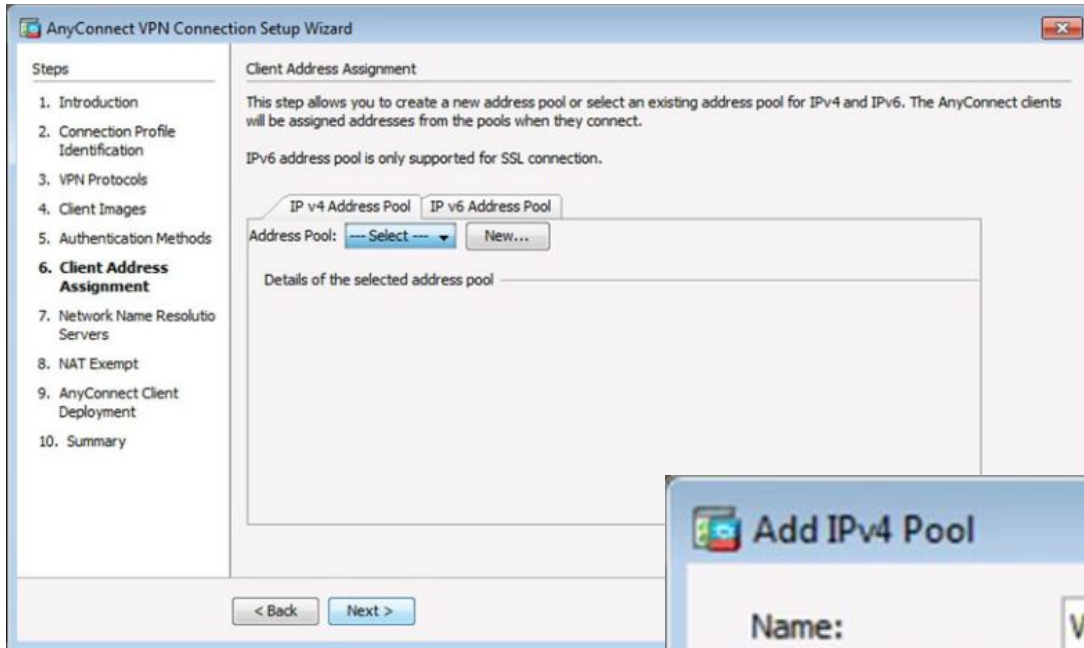
Add >>

Delete

ADMIN
BobV

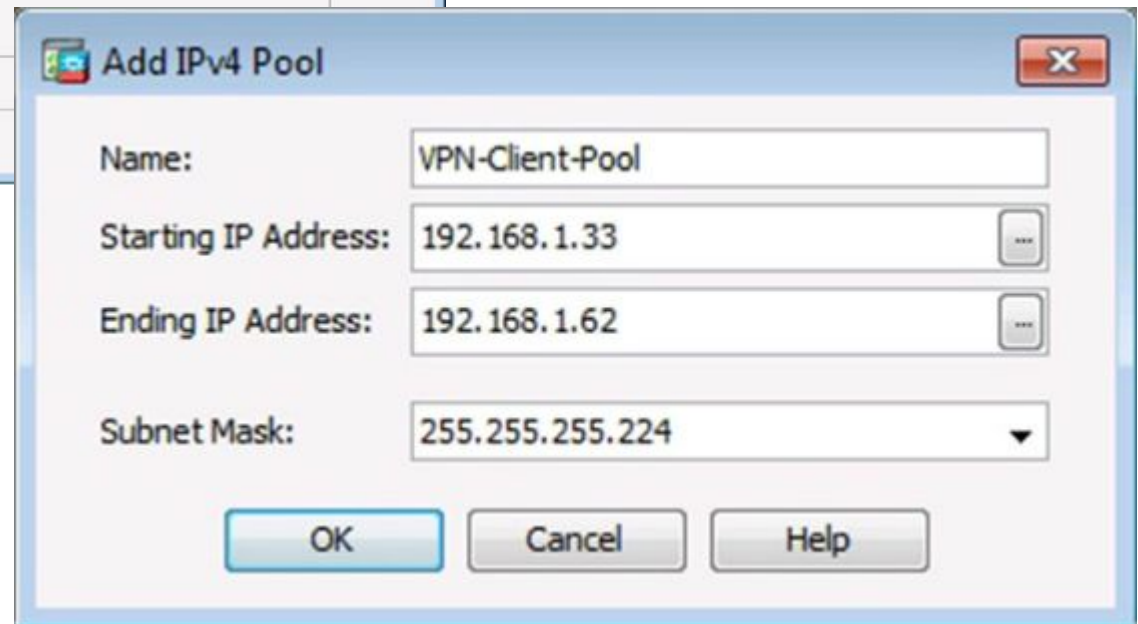
< Back Next > Cancel Help

AnyConnect SSL VPN (Cont.)

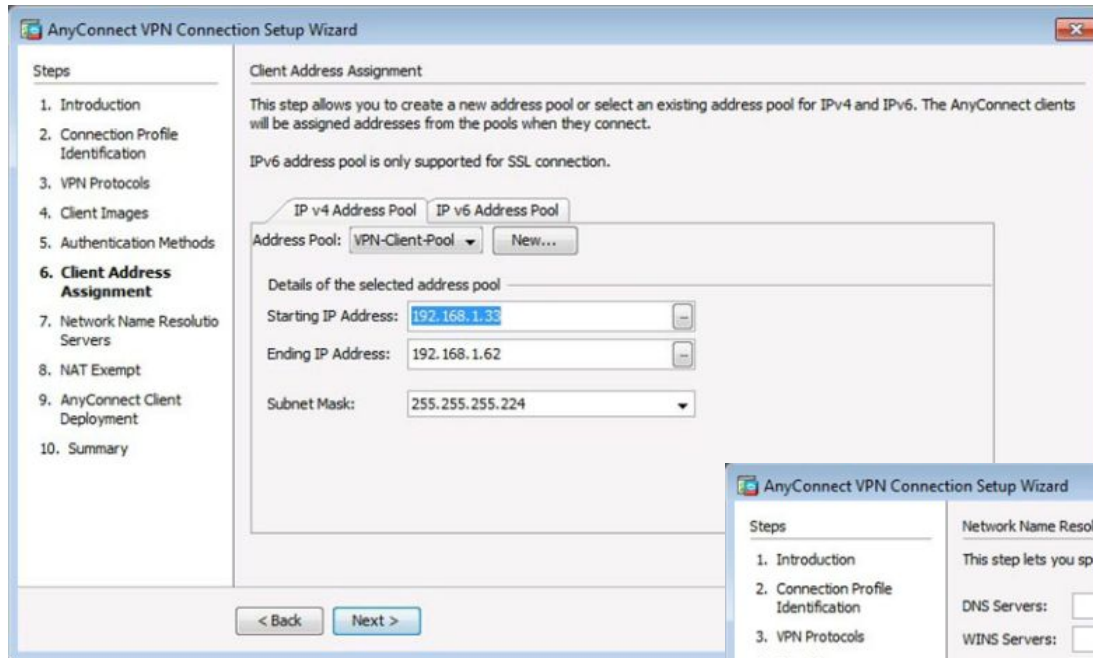


Client Address Management Window

Add IPv4 Window

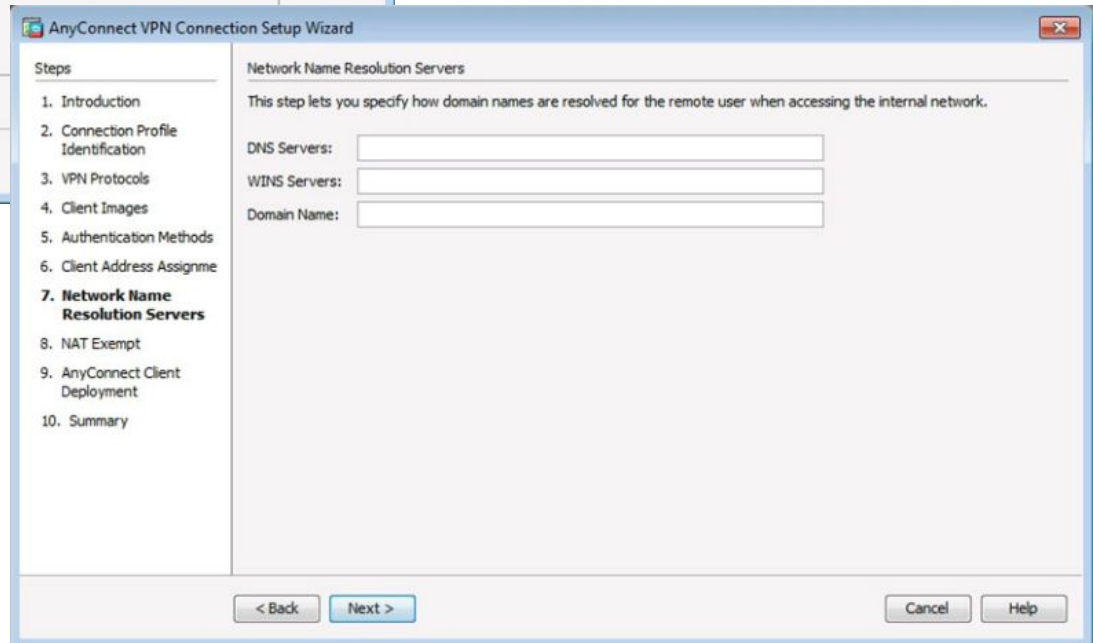


AnyConnect SSL VPN (Cont.)



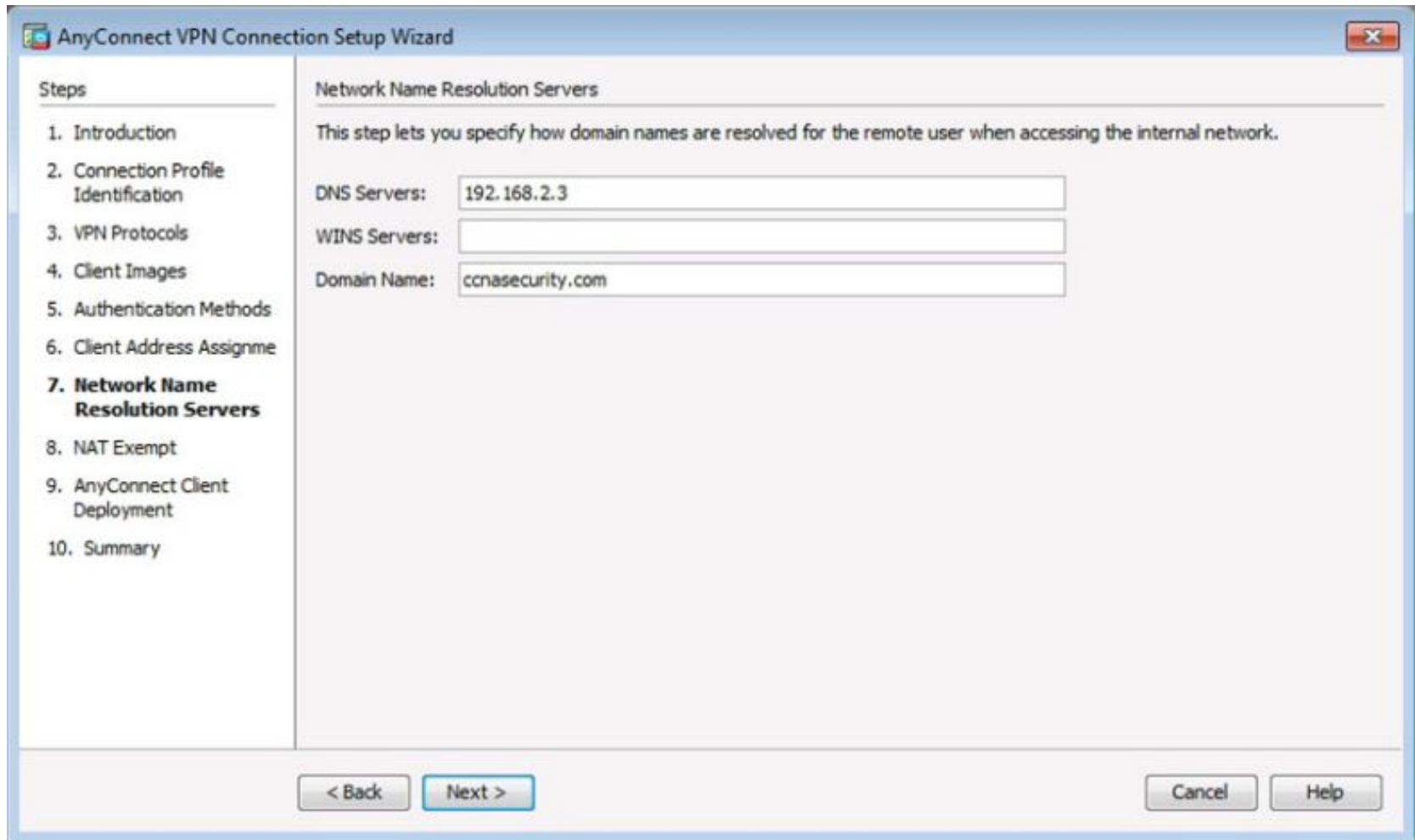
Completed Client Address Management Window

Network Name Resolution Servers Window



AnyConnect SSL VPN (Cont.)

Completed Network Name Resolution Servers Window



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window. The title bar reads 'AnyConnect VPN Connection Setup Wizard'. On the left, a 'Steps' sidebar lists 10 steps, with step 7, 'Network Name Resolution Servers', highlighted in bold. The main area is titled 'Network Name Resolution Servers' and contains the text: 'This step lets you specify how domain names are resolved for the remote user when accessing the internal network.' Below this text are three input fields: 'DNS Servers:' with the value '192.168.2.3', 'WINS Servers:' which is empty, and 'Domain Name:' with the value 'ccnasecurity.com'. At the bottom of the window are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
- 7. Network Name Resolution Servers**
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Network Name Resolution Servers

This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

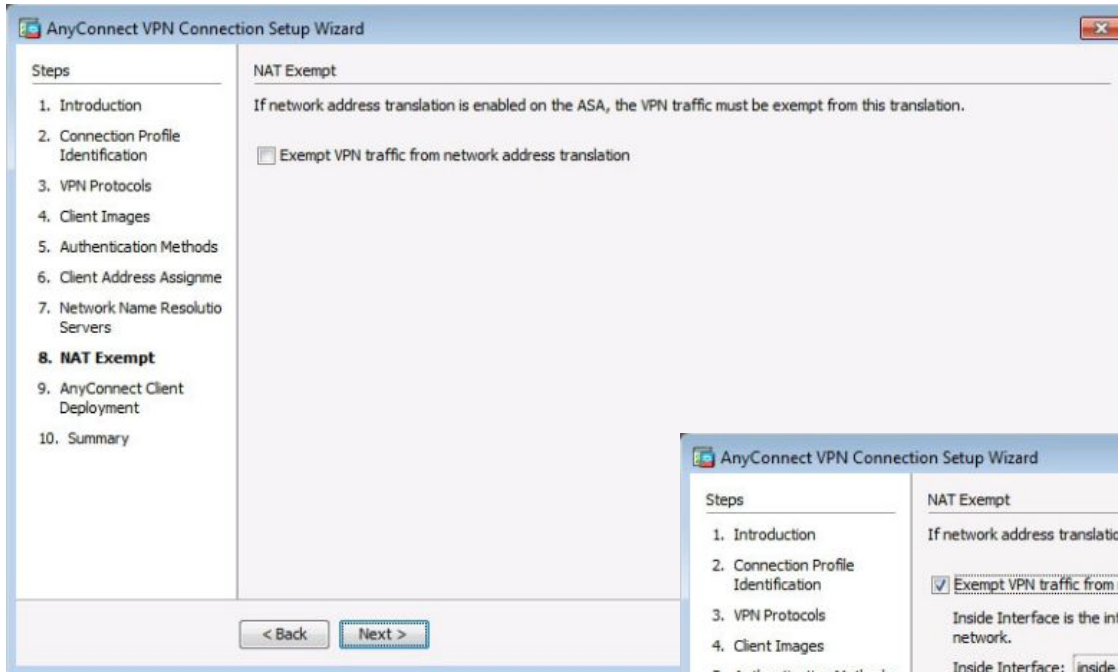
DNS Servers: 192.168.2.3

WINS Servers:

Domain Name: ccnasecurity.com

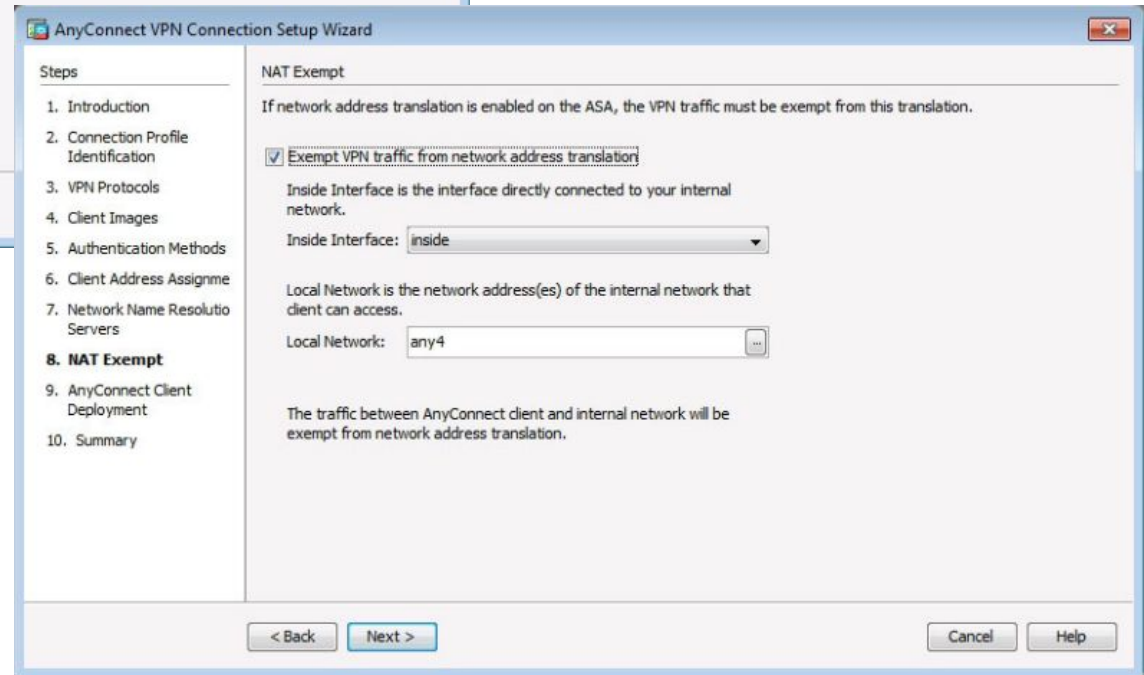
< Back Next > Cancel Help

AnyConnect SSL VPN (Cont.)

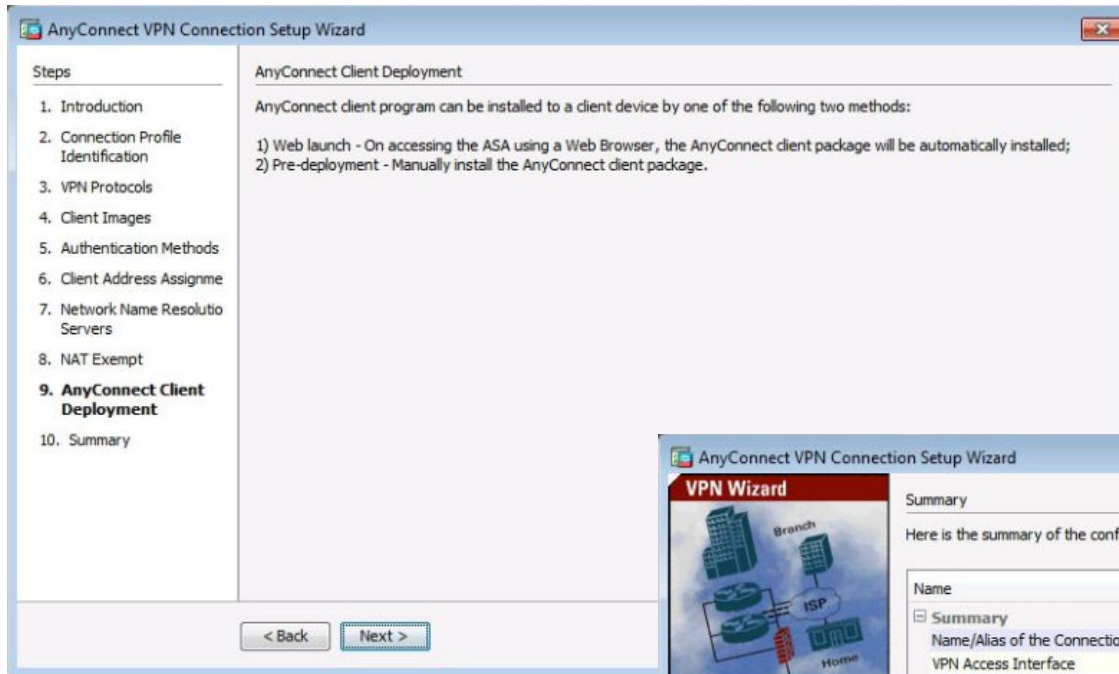


NAT Exempt Window

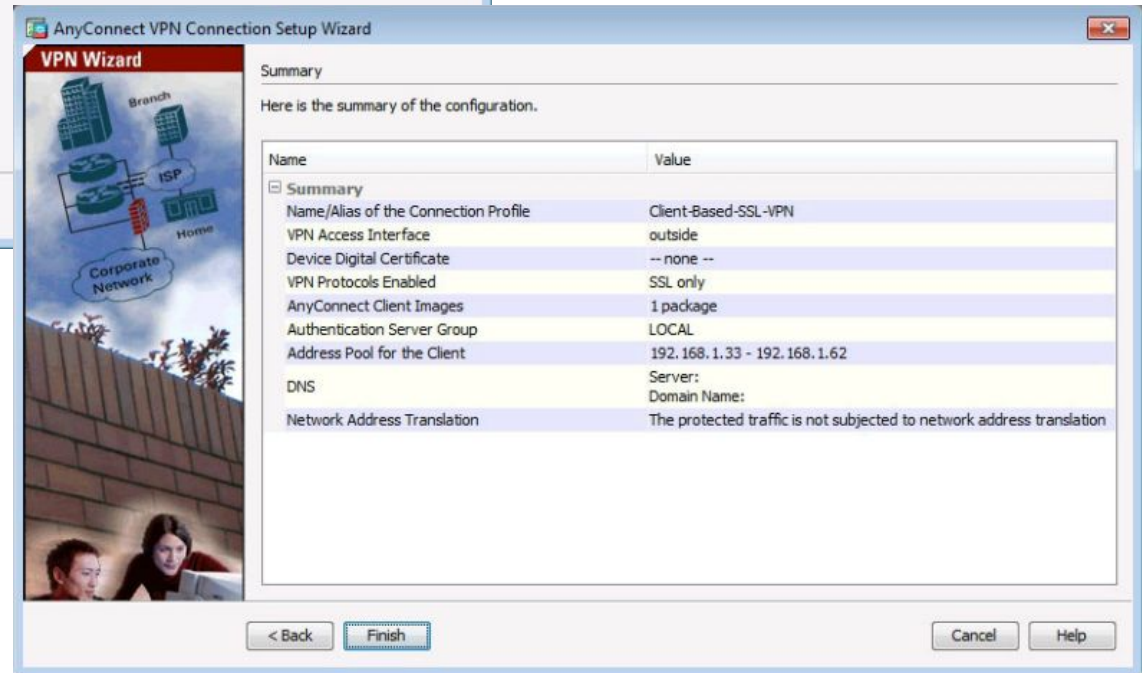
Completed NAT Exempt Window



AnyConnect SSL VPN (Cont.)



AnyConnect Client Deployment



Summary Window

Verifying AnyConnect Connection

AnyConnect Connection Profiles Page

The screenshot displays the Cisco ASDM 7.4 for ASA - 192.168.1.1 interface. The breadcrumb navigation is Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. The left sidebar shows the navigation tree with 'AnyConnect Connection Profiles' selected under 'Remote Access VPN'. The main content area contains the following sections:

- Introduction:** The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
- Access Interfaces:**
 - Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.
 - SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).
- Table:**

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

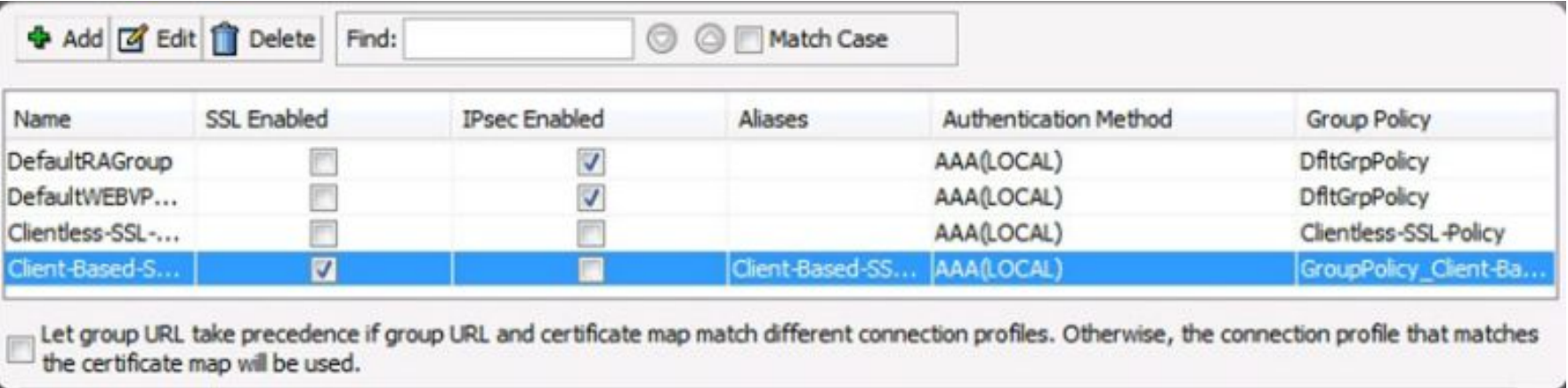
- Bypass interface access lists for inbound VPN sessions.
- Access lists from group policy and user policy always apply to the traffic.

- Login Page Setting:**
- Allow user to select connection profile on the login page.
- Shutdown portal login page.
- Connection Profiles:**
- Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).
- Buttons: Add, Edit, Delete, Find: [text input], Match Case.
- Table:**

Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy

Verifying AnyConnect Connection (Cont.)

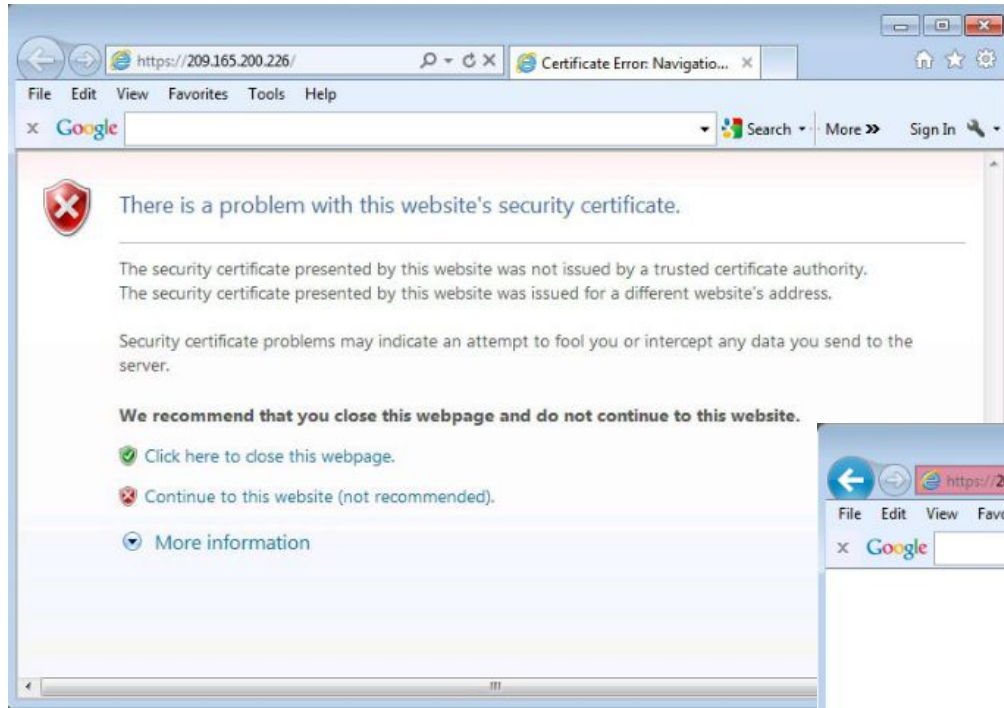
Verifying the Client-Based Configuration



Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfitGrpPolicy
DefaultWEBVP...	<input type="checkbox"/>	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfitGrpPolicy
Clientless-SSL-...	<input type="checkbox"/>	<input type="checkbox"/>		AAA(LOCAL)	Clientless-SSL-Policy
Client-Based-S...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Client-Based-SS...	AAA(LOCAL)	GroupPolicy_Client-Ba...

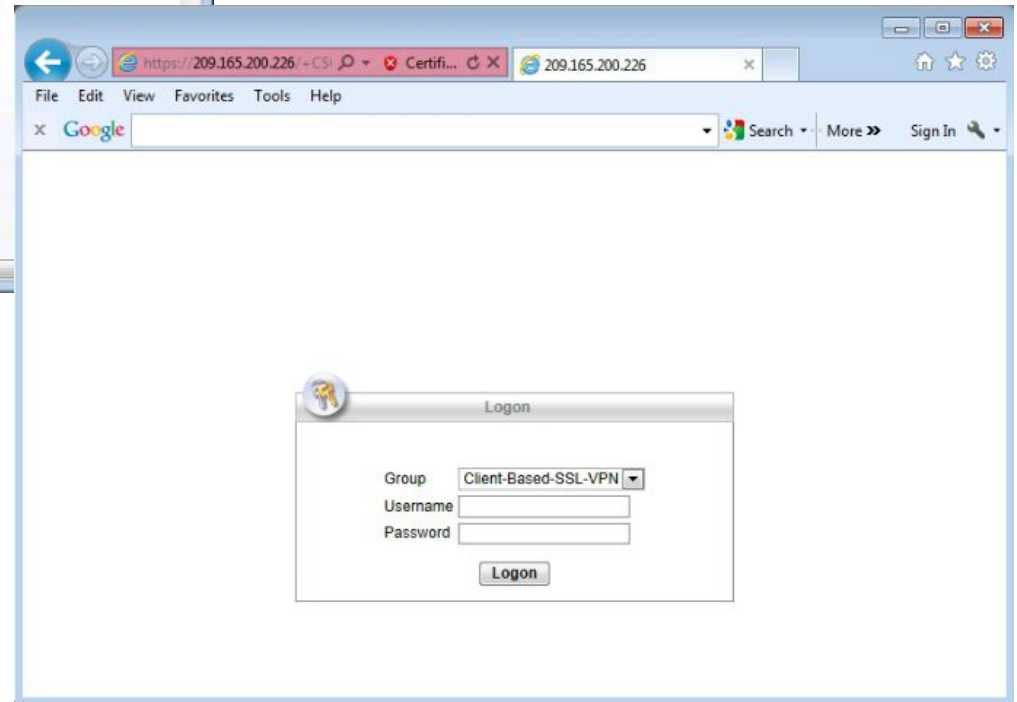
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

Install the AnyConnect Client



Logon Window

Security Certificate Window

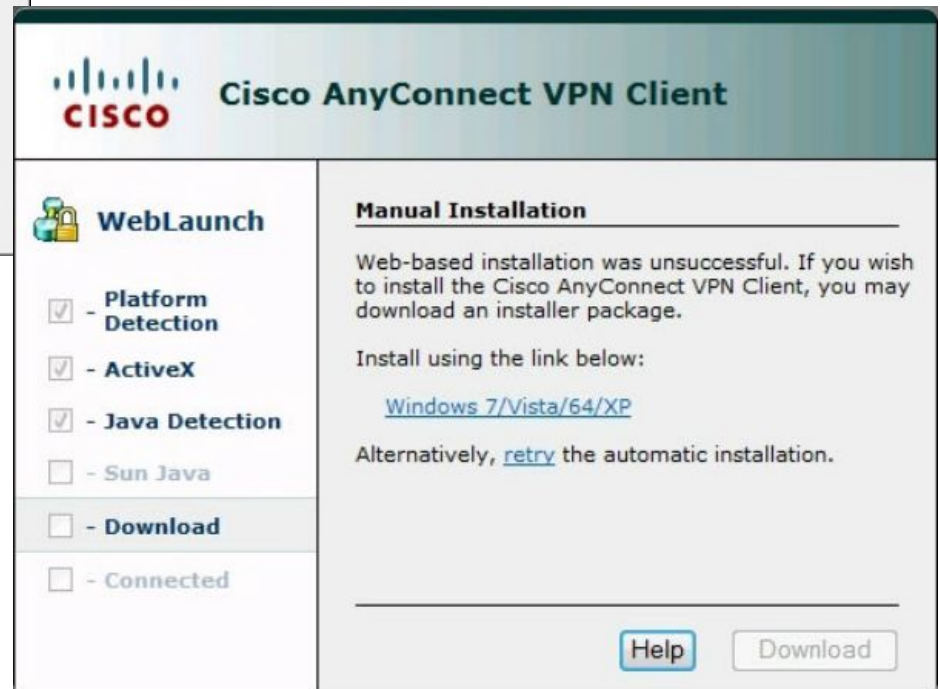


Install the AnyConnect Client (Cont.)



Cisco AnyConnect VPN Client Window

Manual Installation Window



Install the AnyConnect Client (Cont.)

Run Installer Window



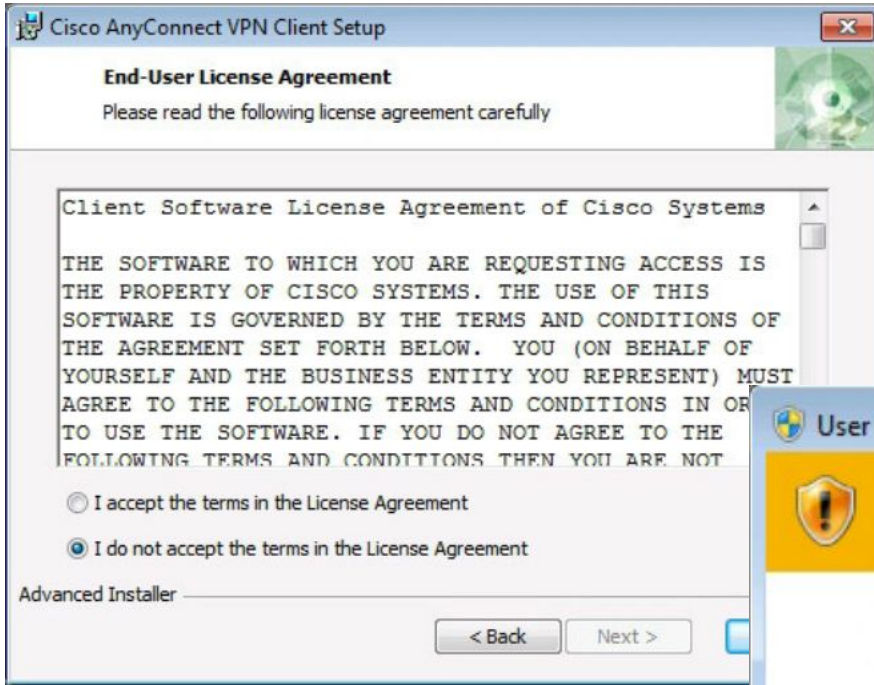
Install the AnyConnect Client (Cont.)

Cisco AnyConnect VPN Client Setup Window

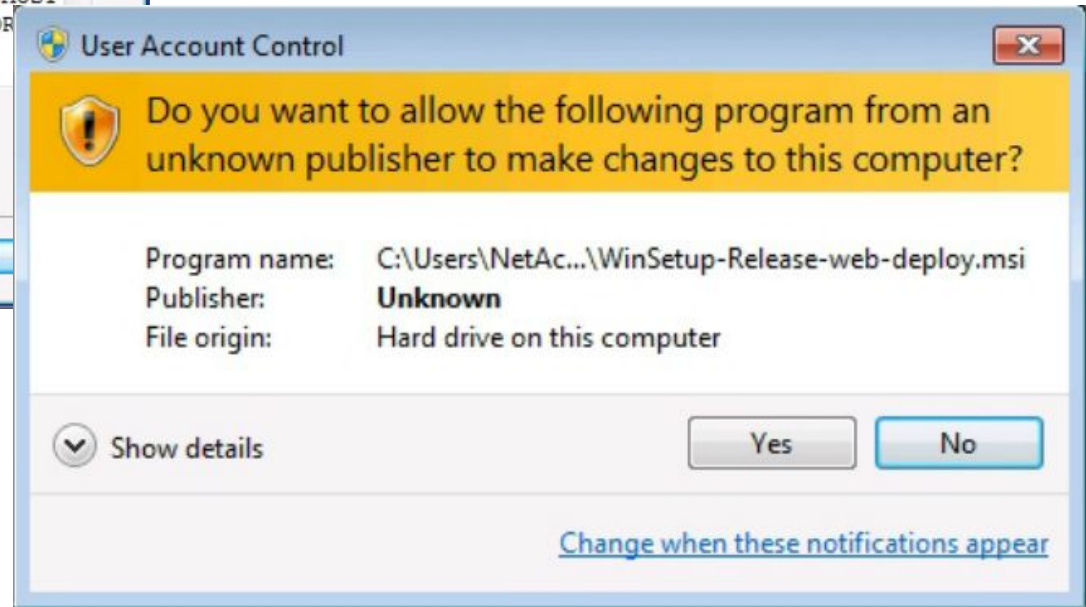


Install the AnyConnect Client (Cont.)

End-User Agreement Window

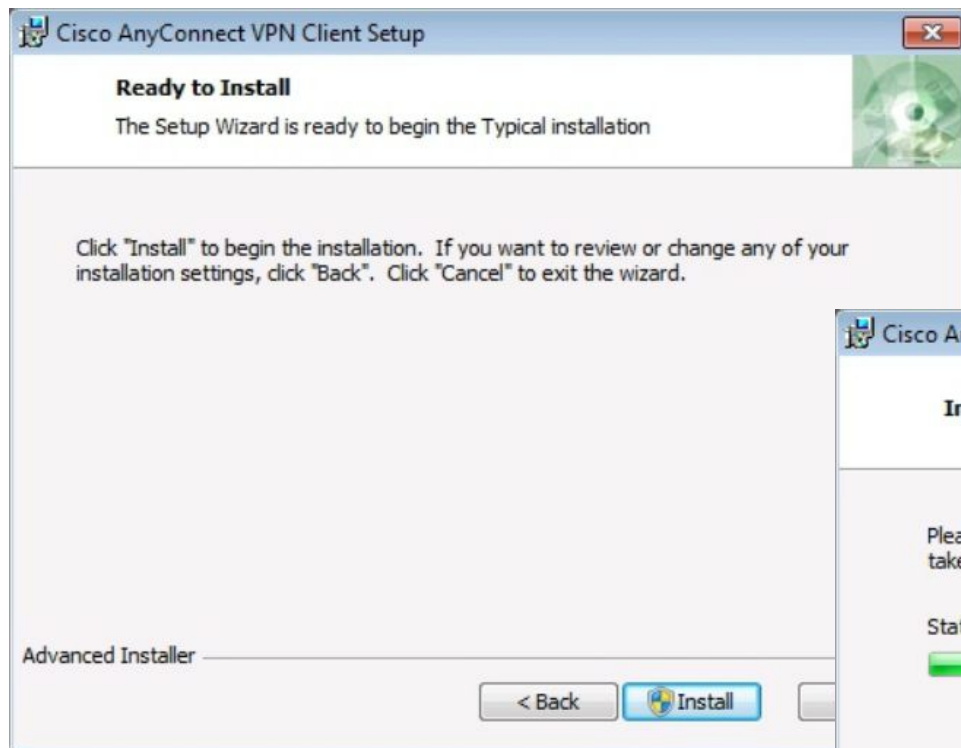


User Account Control Security Window

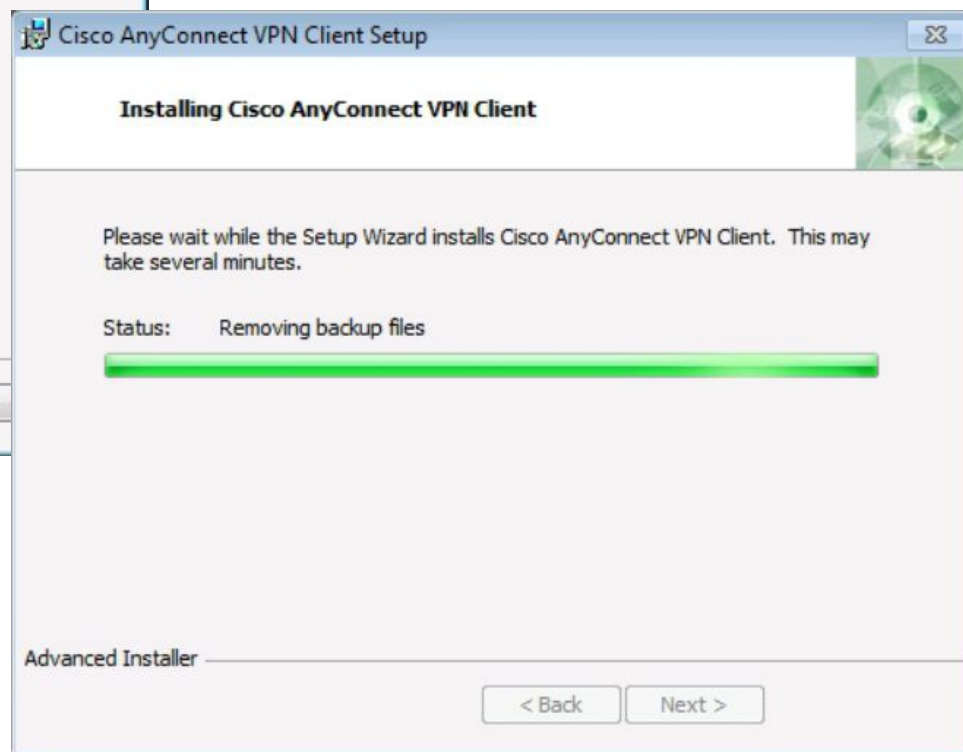


Install the AnyConnect Client (Cont.)

Ready to Install AnyConnect Client



Installing the AnyConnect Client



Install the AnyConnect Client (Cont.)

Complete Cisco AnyConnect VPN Client Installation



Install the AnyConnect Client (Cont.)

Start the Cisco AnyConnect VPN Client
Cisco

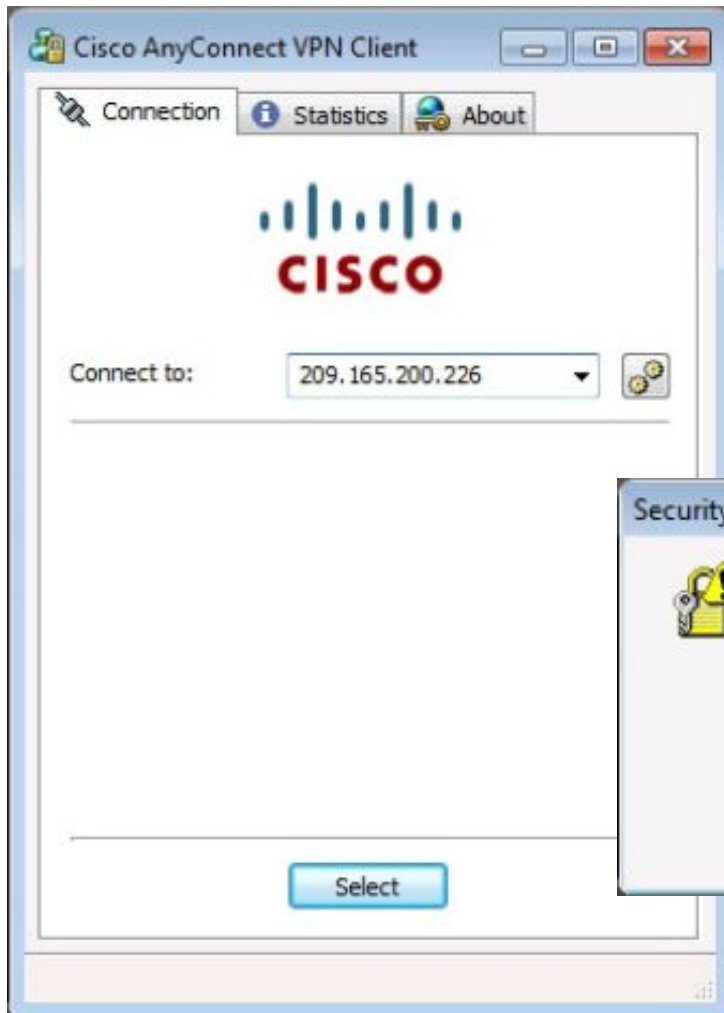


Cisco AnyConnect VPN Client
Window



Install the AnyConnect Client (Cont.)

Cisco AnyConnect VPN Connect Window



Certificate Security Warning Window



Install the AnyConnect Client (Cont.)

Cisco AnyConnect VPN Authentication Window



Cisco AnyConnect VPN Icon in System Tray

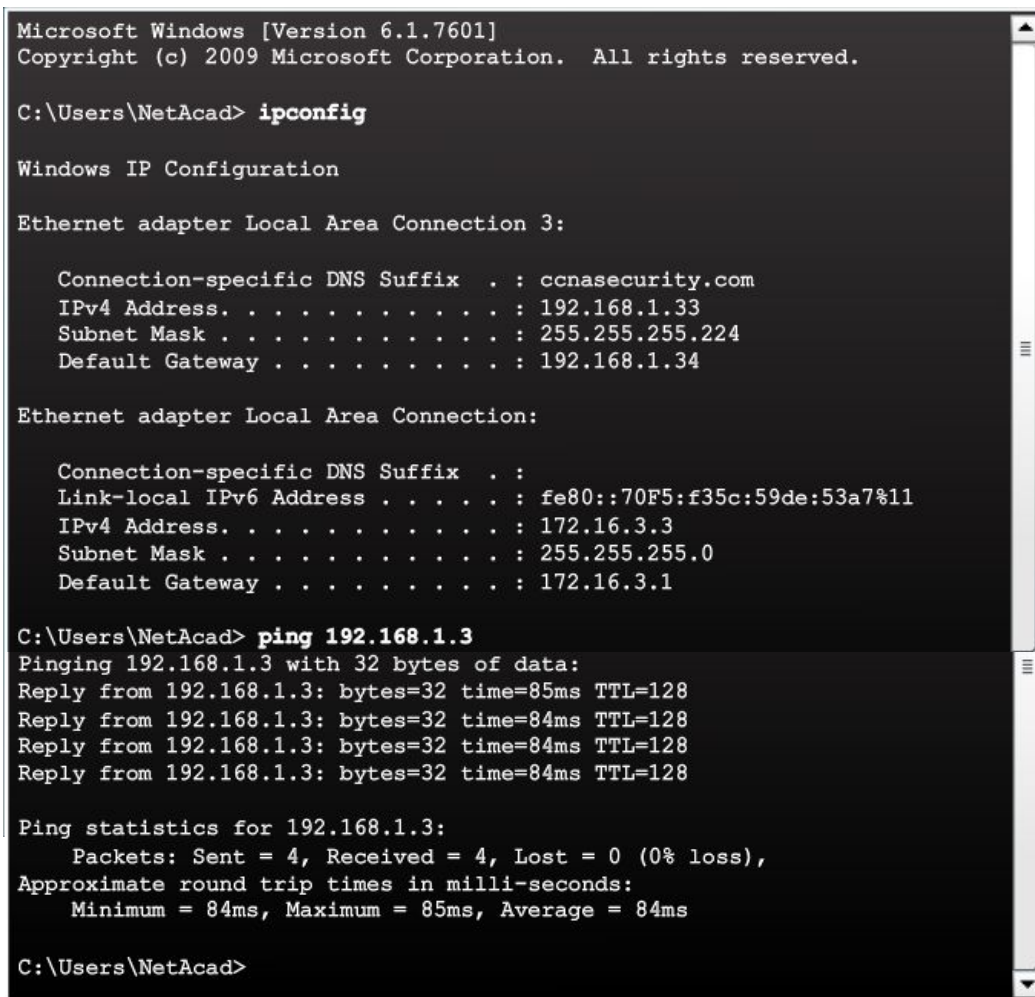


Install the AnyConnect Client (Cont.)

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

```
ip local pool VPN-Client-Pool 192.168.1.33-192.168.1.62 mask  
object network NETWORK_OBJ_192.168.1.32_27  
  subnet 192.168.1.32 255.255.255.224  
nat (inside,outside) source static any any destination stati  
!
```

```
webvpn  
  enable outside  
  anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1  
  anyconnect enable  
  tunnel-group-list enable
```

```
group-policy GroupPolicy_Client-Based-SSL-VPN internal  
group-policy GroupPolicy_Client-Based-SSL-VPN attributes  
  wins-server none  
  dns-server value 192.168.2.3  
  vpn-tunnel-protocol ssl-client  
  default-domain value ccnasecurity.com
```

```
tunnel-group Client-Based-SSL-VPN type remote-access  
tunnel-group Client-Based-SSL-VPN general-attributes  
  address-pool VPN-Client-Pool  
  default-group-policy GroupPolicy_Client-Based-SSL-VPN  
tunnel-group Client-Based-SSL-VPN webvpn-attributes  
  group-alias Client-Based-SSL-VPN enable  
!
```

Section 10.3: Summary

Chapter Objectives:

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

Thank you.



Cisco Networking Academy
Mind Wide Open

Instructor Resources

- **Remember**, there are helpful tutorials and user guides available via your NetSpace home page. (<https://www.netacad.com>)
- These resources cover a variety of topics including navigation, assessments, and assignments.
- A screenshot has been provided here highlighting the tutorials related to activating exams, managing assessments, and creating quizzes.

