

# **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](http://itexamanswers.net/ccna-security-2-0-study-material-chapter-10-advanced-cisco-adaptive-security-appliance.html)

October 9, 2017

## **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:**

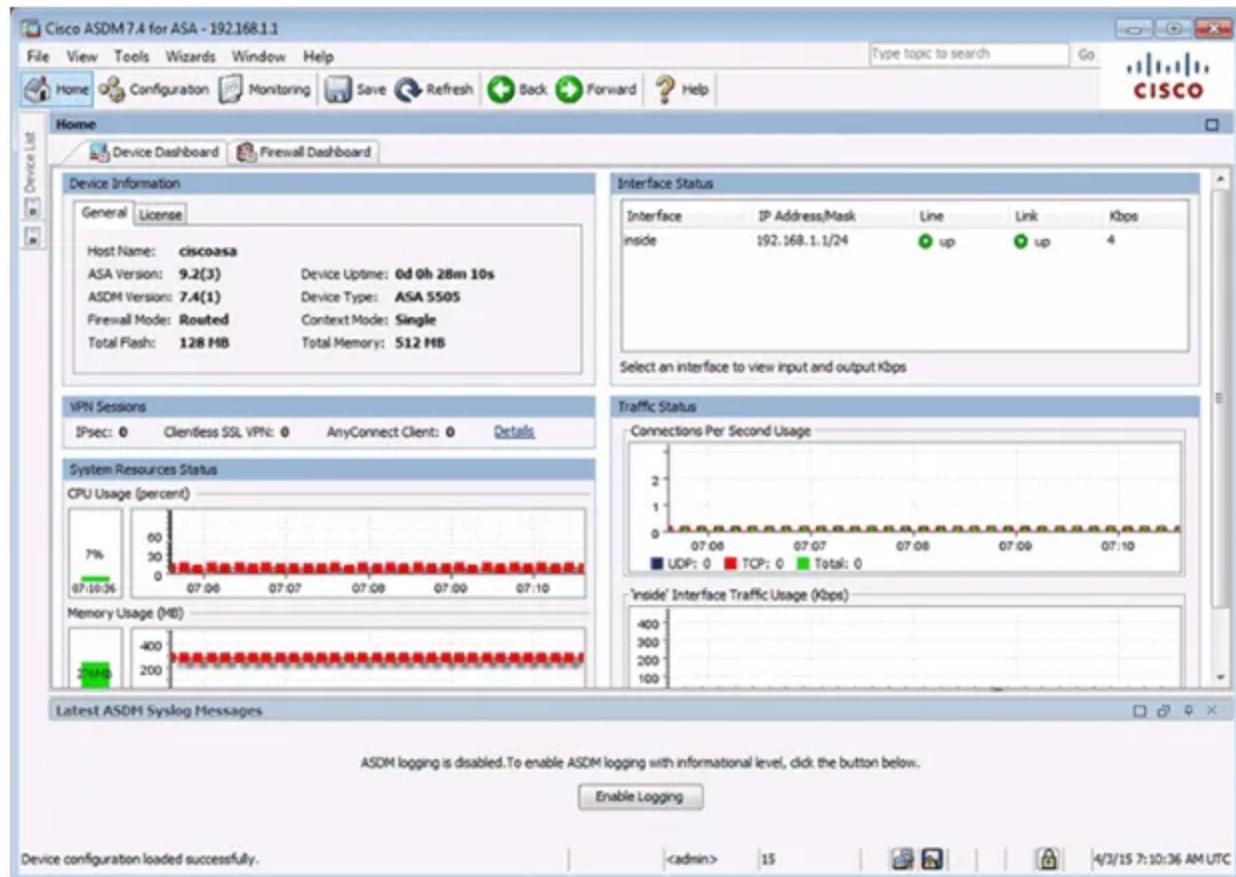
- Configure an ASA to provide basic firewall services using ASDM.
- Configure an ASA to provide additional firewall services using ASDM wizards.
- Configure management settings and services in an ASA using ASDM.
- Configure object groups on an ASA.

### **Topic 10.1.1: Introduction to ASDM**

---

#### **Overview of ASDM**

---



## 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

```
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

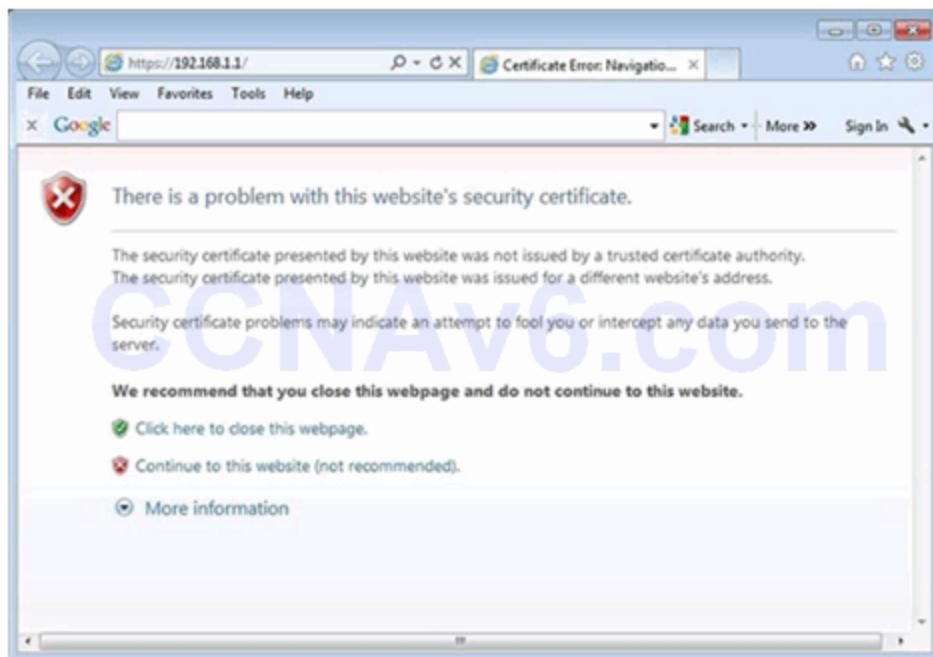
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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



## ASDM Security Warning – 1



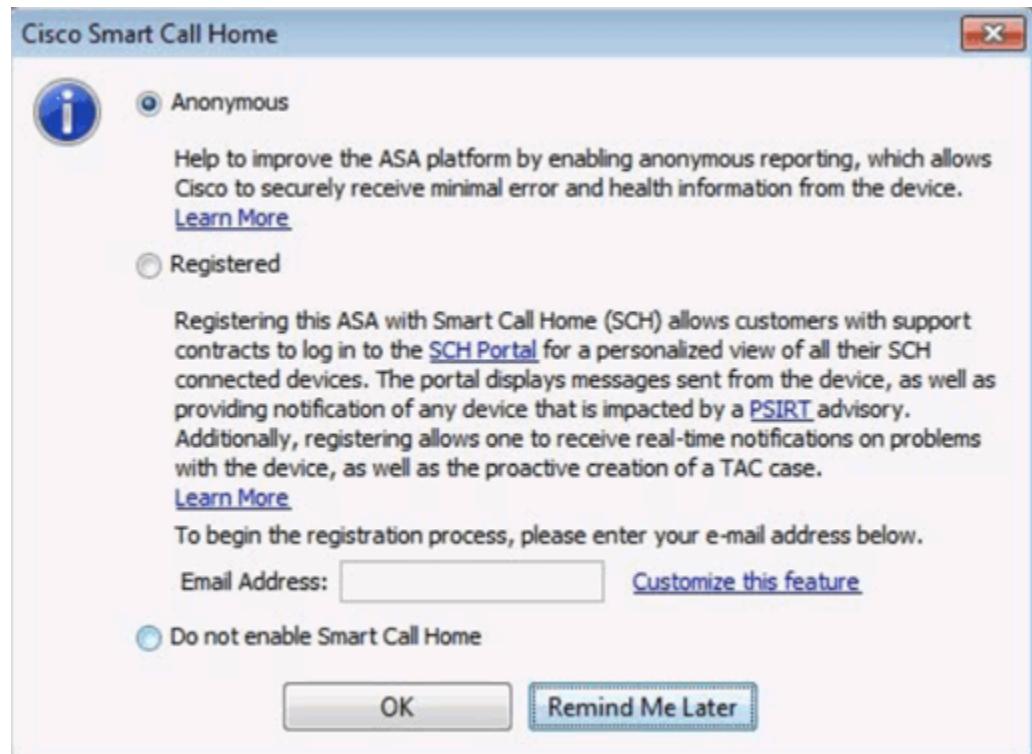
## ASDM Security Warning – 2



Authenticate to Use ASDM



Smart Call Home Window

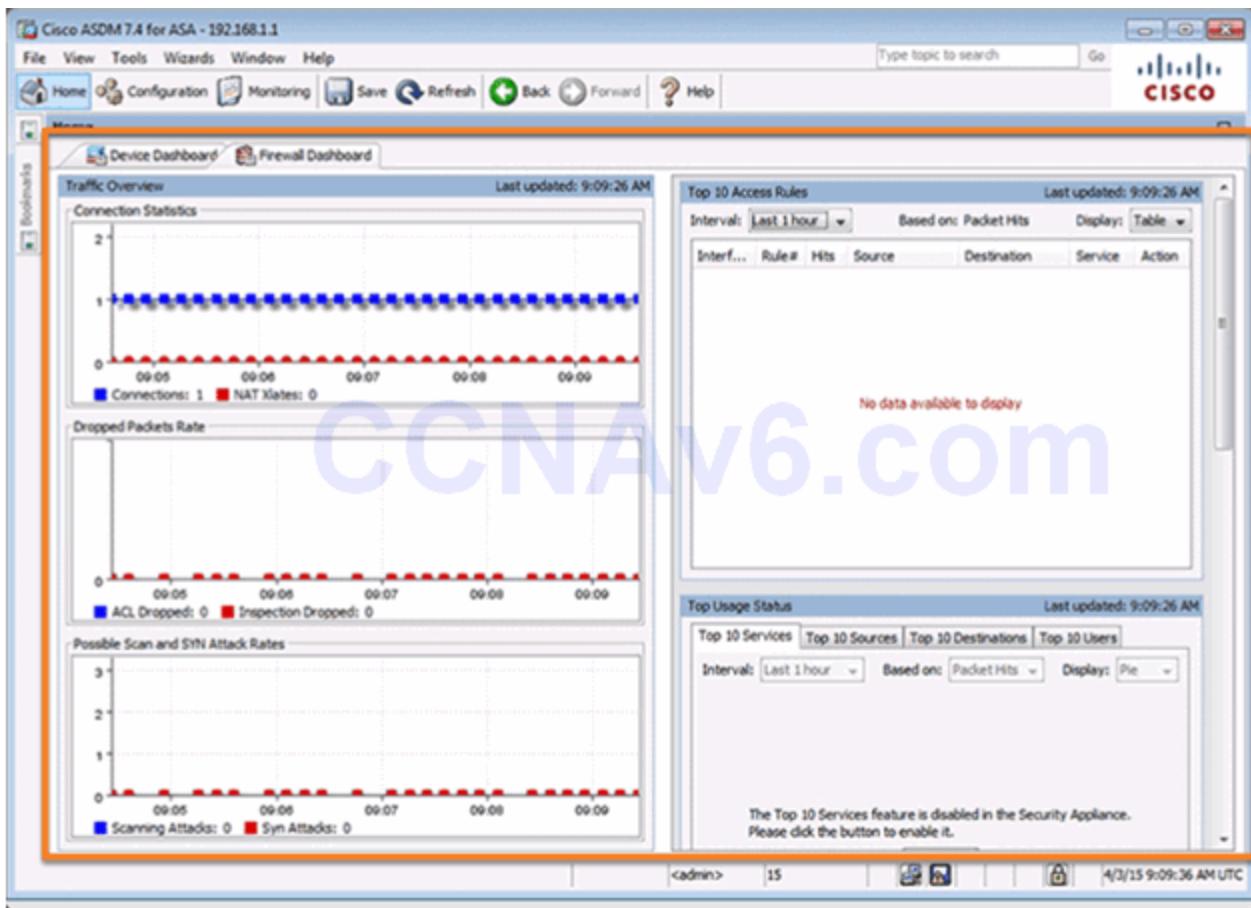


## ASDM Home Page Dashboards

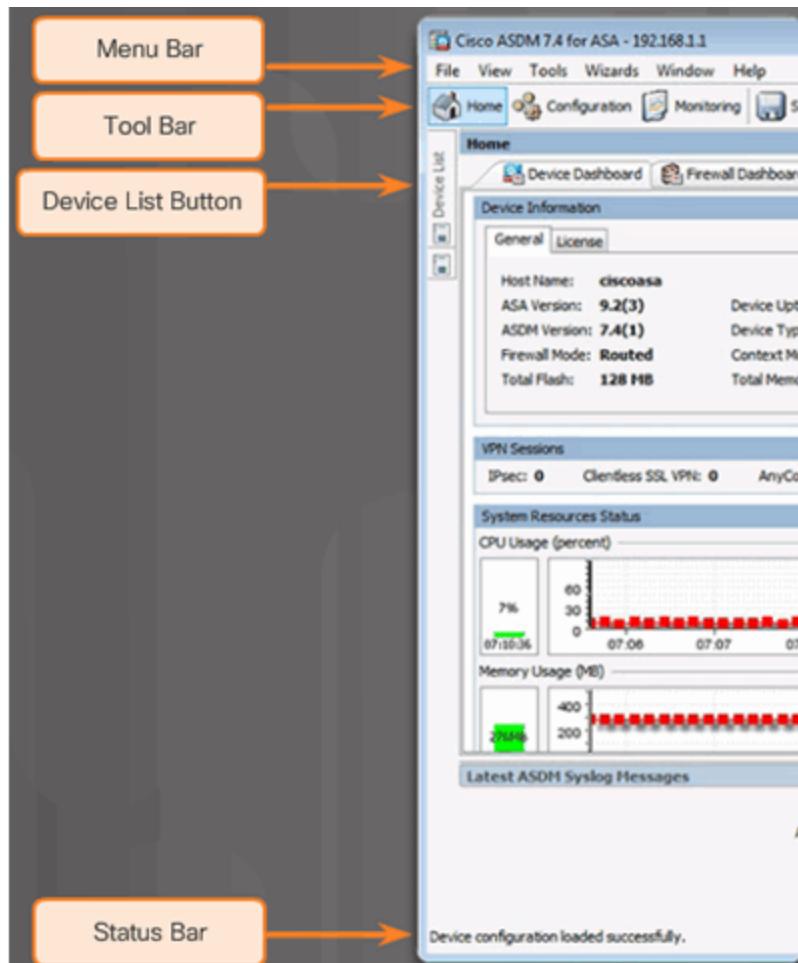
### ASDM Device Dashboard Page

The screenshot shows the Cisco ASDM 7.4 Device Dashboard for ASA 192.168.1.1. The dashboard includes several panels: "Device Information" (Host Name: ciscoasa, ASA Version: 9.2(3), ASDM Version: 7.4(1), Firewall Mode: Routed, Total Flash: 128 MB); "Interface Status" (inside interface IP 192.168.1.1/24, Line and Link up, 4 Kbps); "VPN Sessions" (IPsec: 0, Clientless SSL VPN: 0, AnyConnect Client: 0); "System Resources Status" (CPU Usage: 7%, Memory Usage: 400 MB); "Traffic Status" (Connections Per Second Usage chart showing UDP: 0, TCP: 0, Total: 0 over time); and "Latest ASDM Syslog Messages" (disabled). A message at the bottom says "ASDM logging is disabled. To enable ASDM logging with informational level, click the button below." with an "Enable Logging" button. The status bar at the bottom shows "Device configuration loaded successfully.", "admin> 15", and "4/3/15 7:10:36 AM UTC".

## ASDM Firewall Dashboard Page



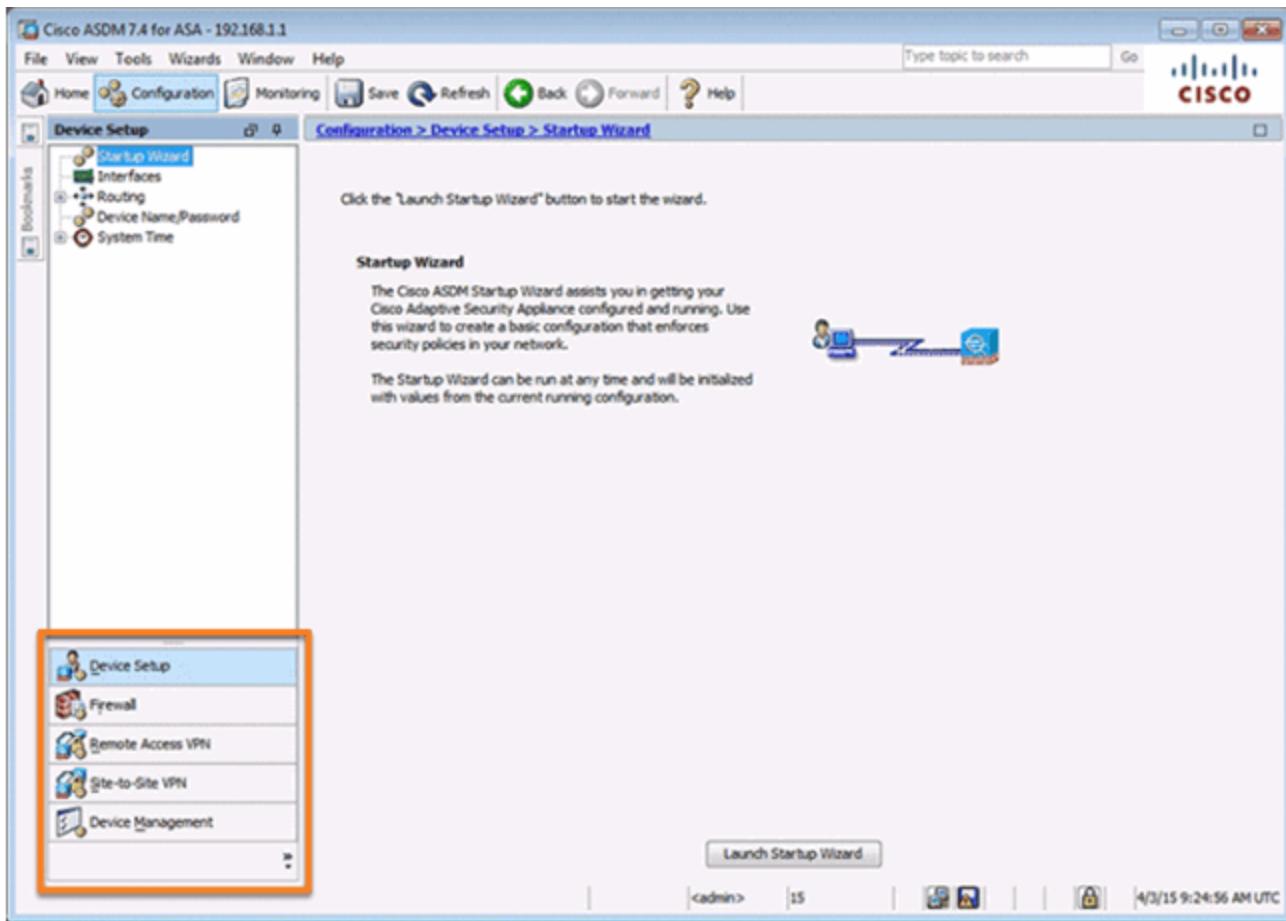
## ASDM Page Elements



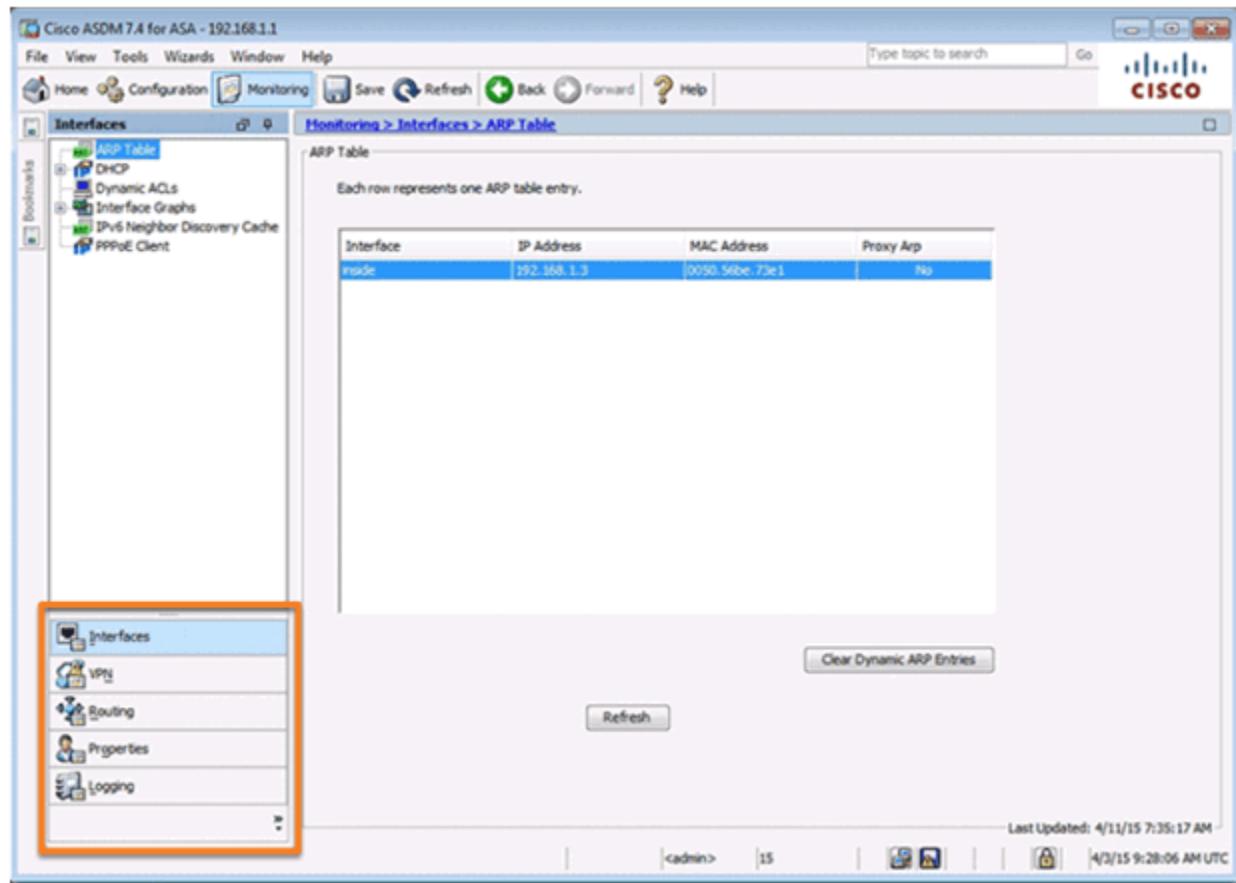
## ASDM Configuration and Monitoring Views

---

### Configuration View



## Monitoring View

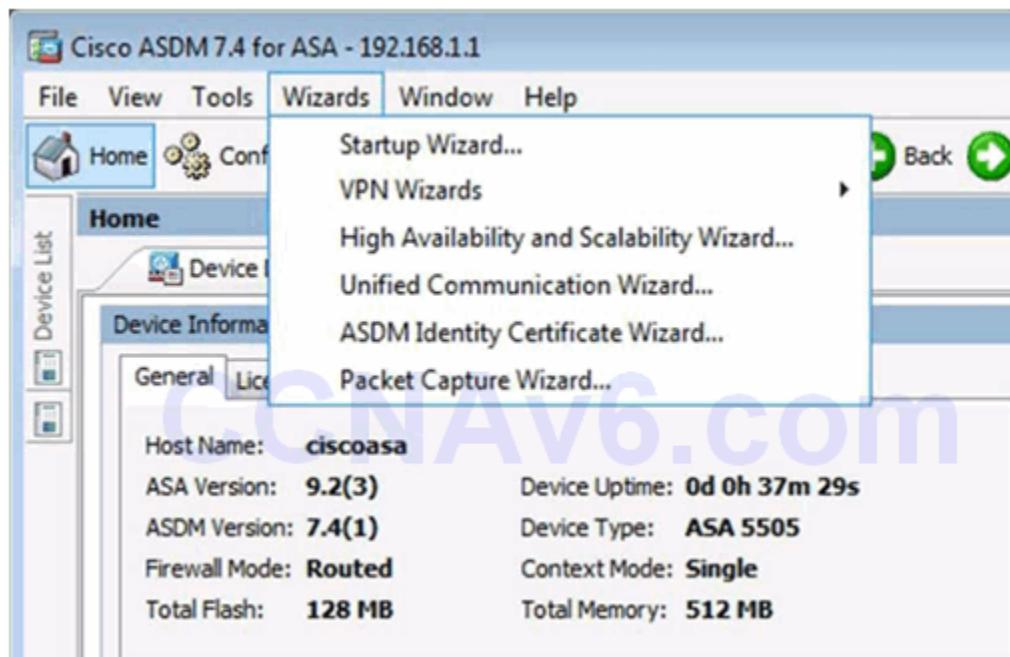


## Configure and Access on an ASA5505



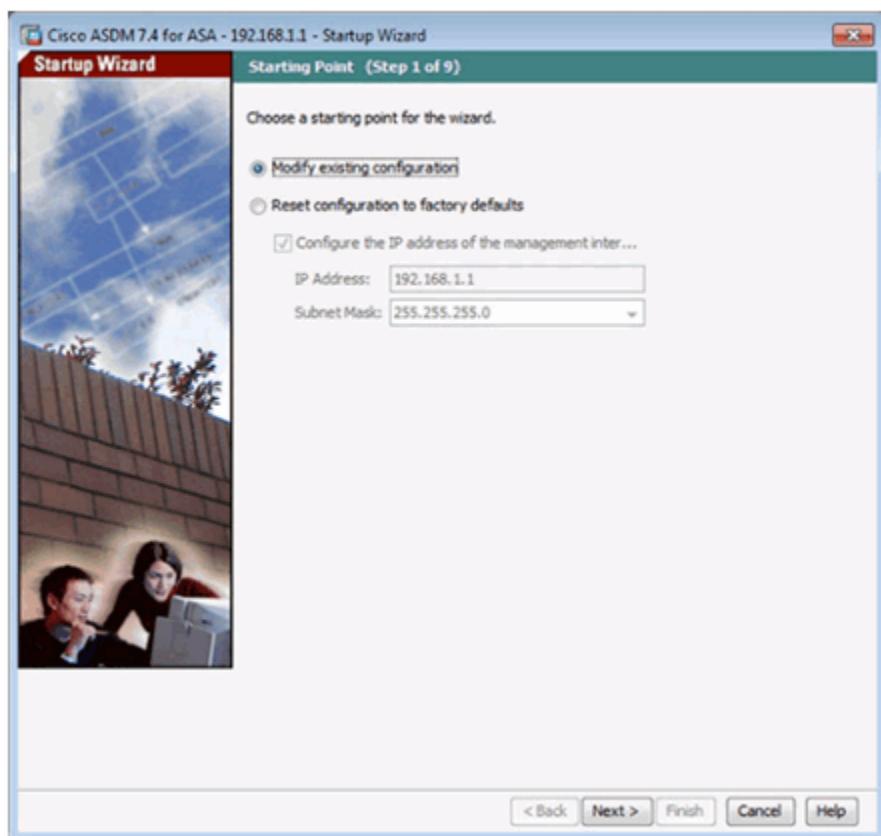
## Topic 10.1.2: ASDM Wizard Menu

### ASDM Wizards

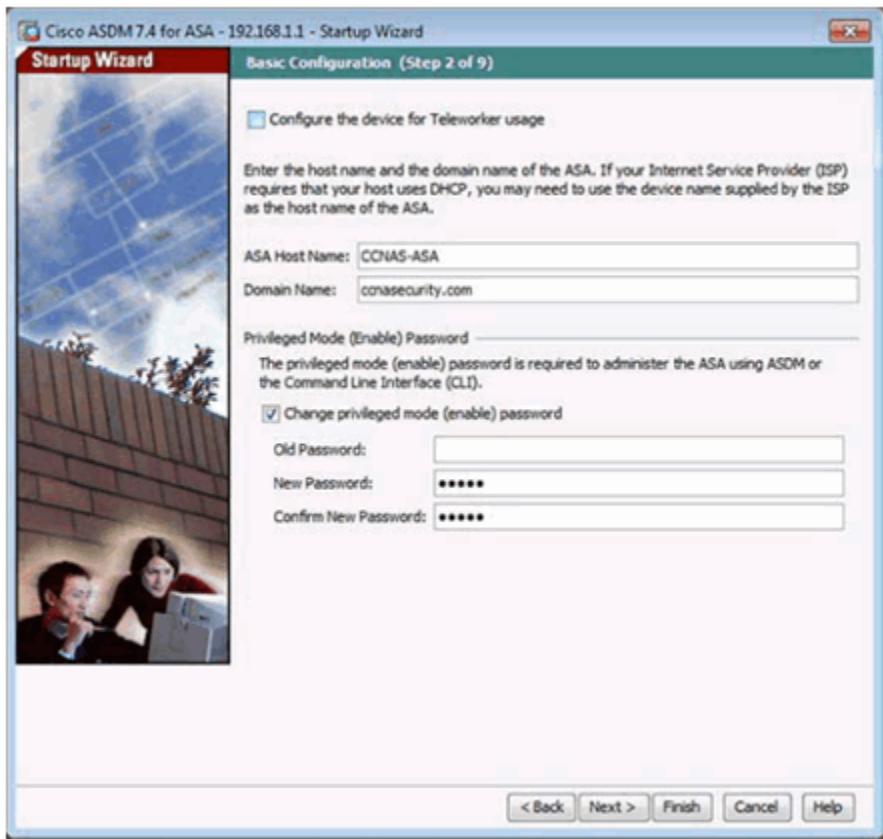


## The Startup Wizard

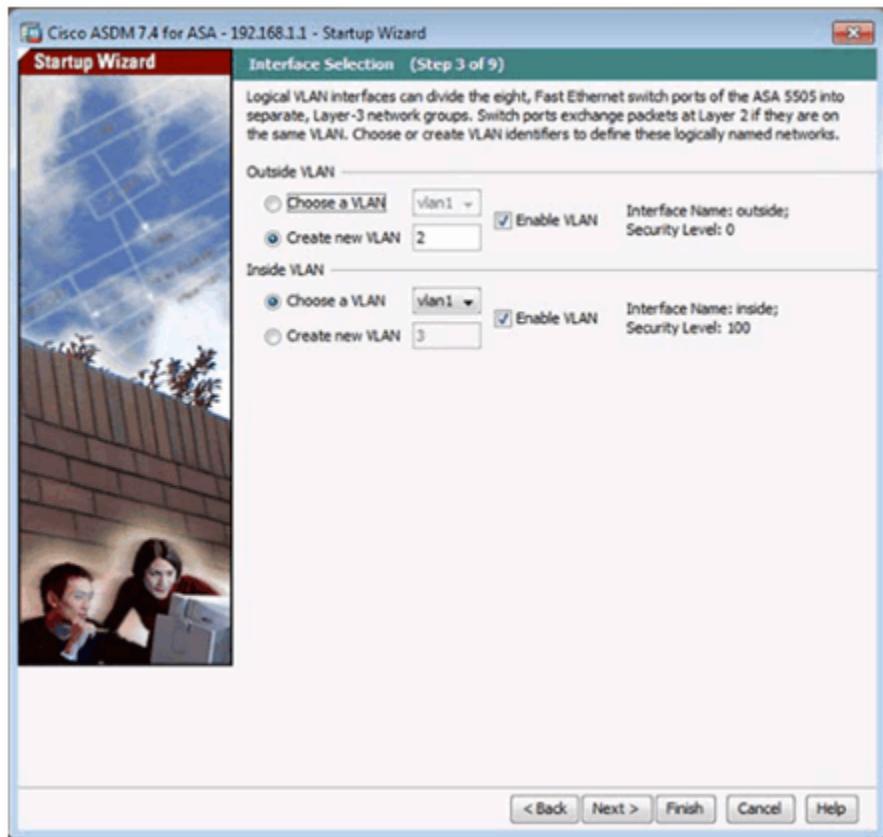
Startup Wizard Starting Point Window



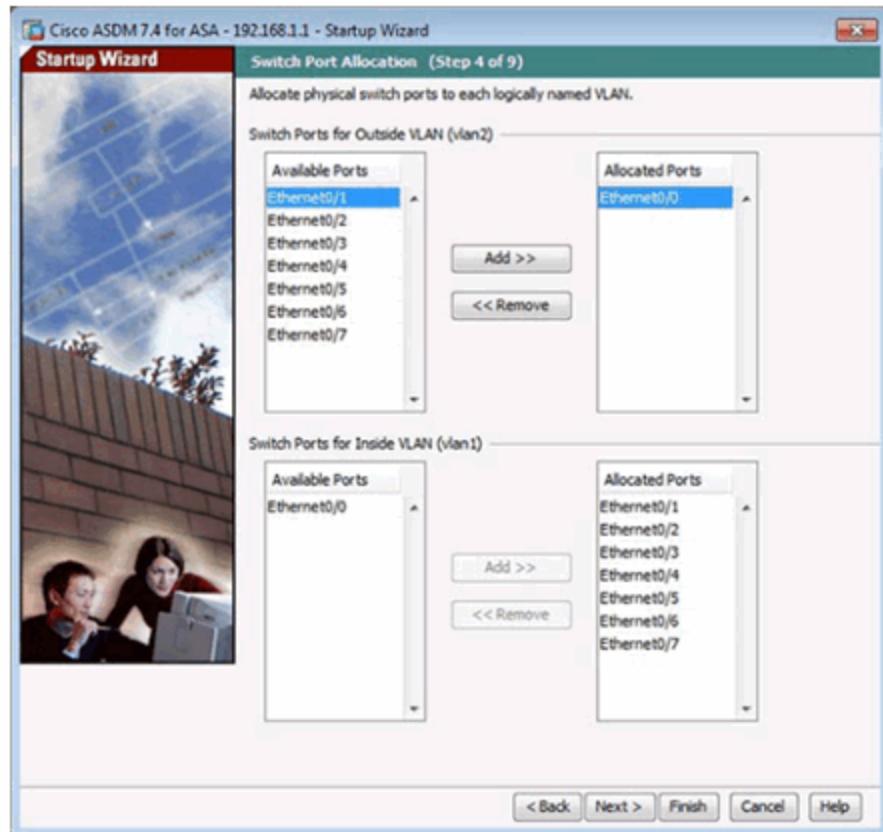
Startup Wizard Basic Configuration Window



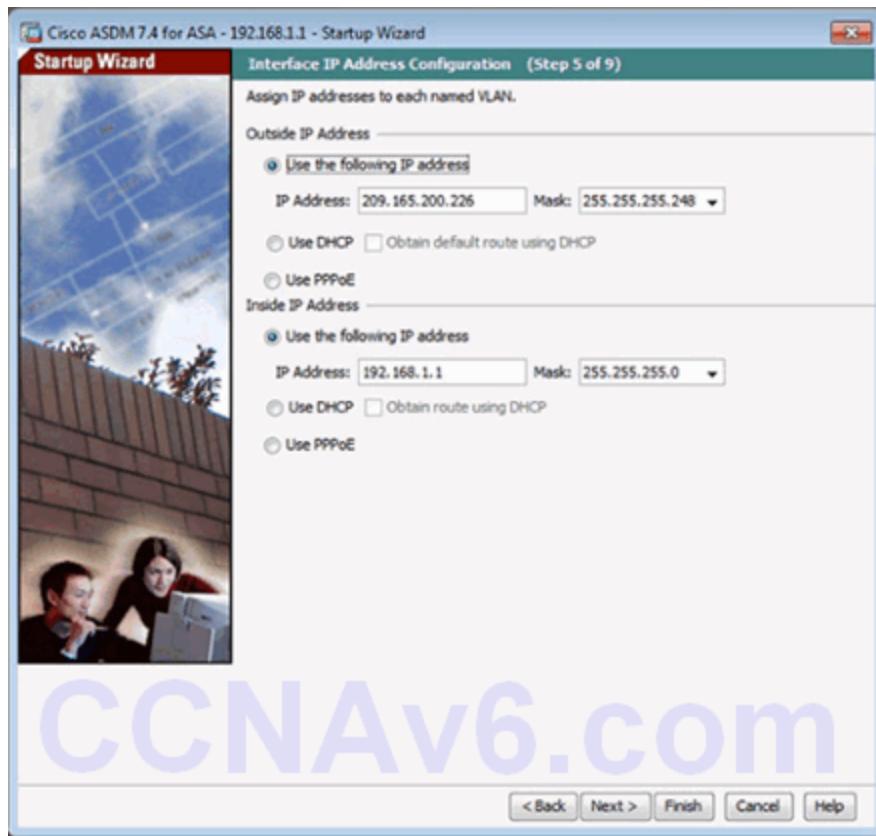
Startup Wizard Interface Selection Window



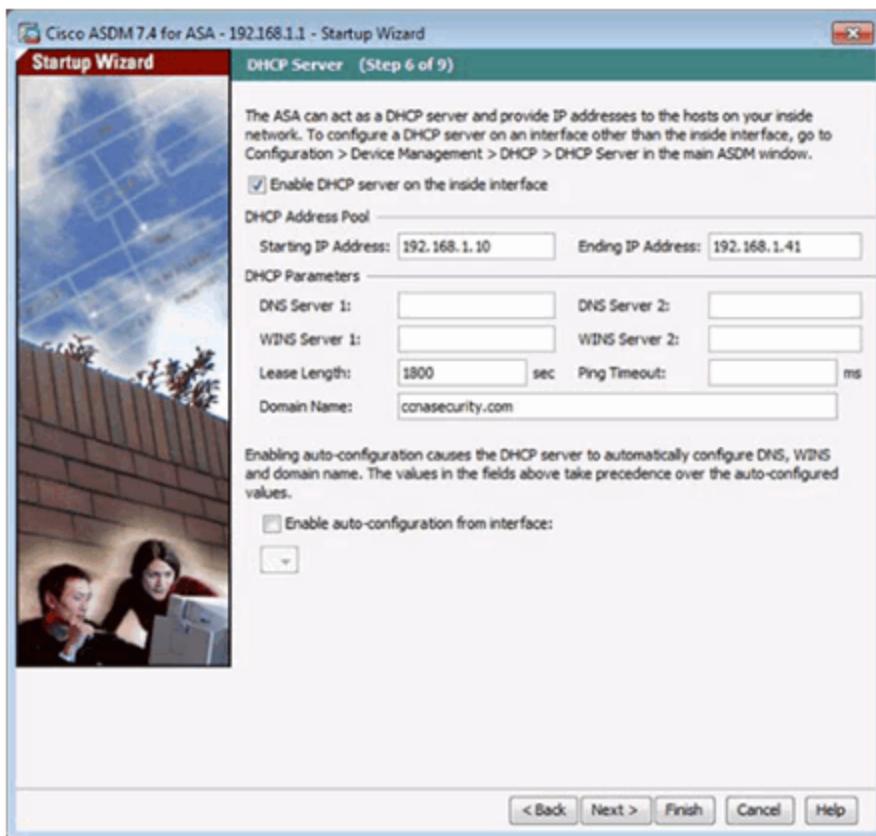
## Startup Wizard Switch Port Allocation Window



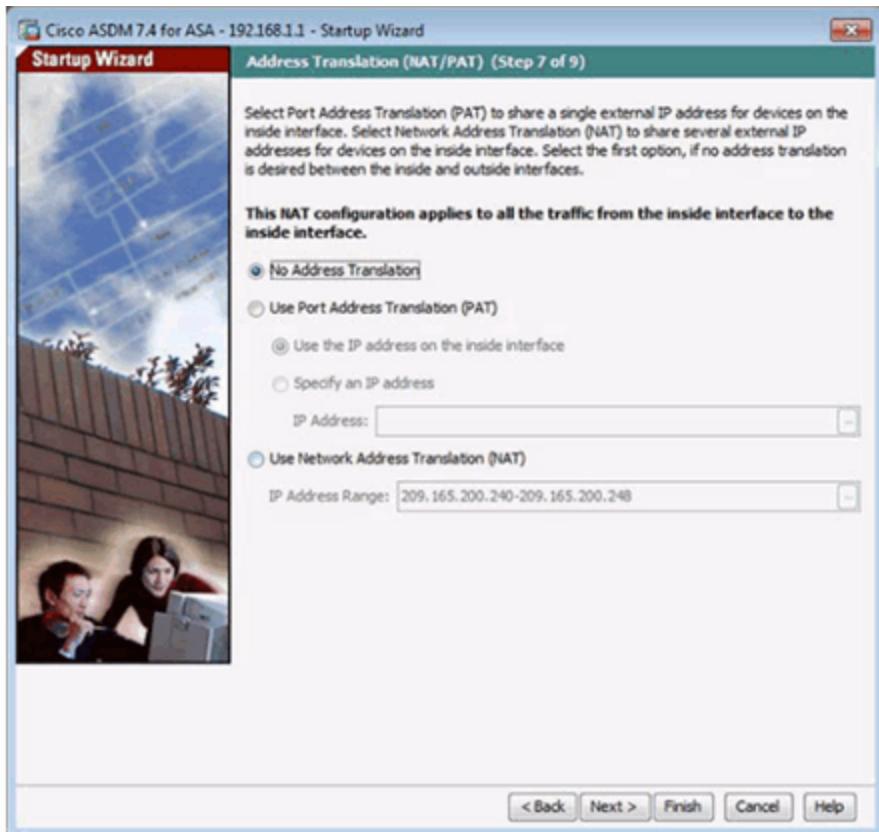
## Startup Wizard Interface IP Address Configuration Window



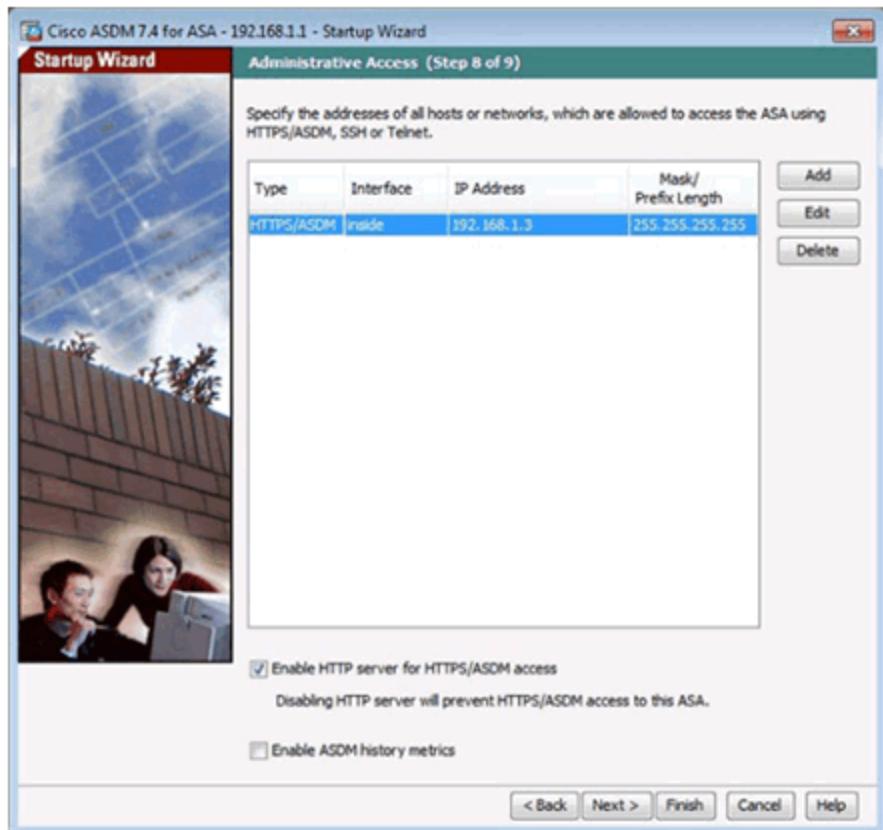
## Startup Wizard DHCP Server Window



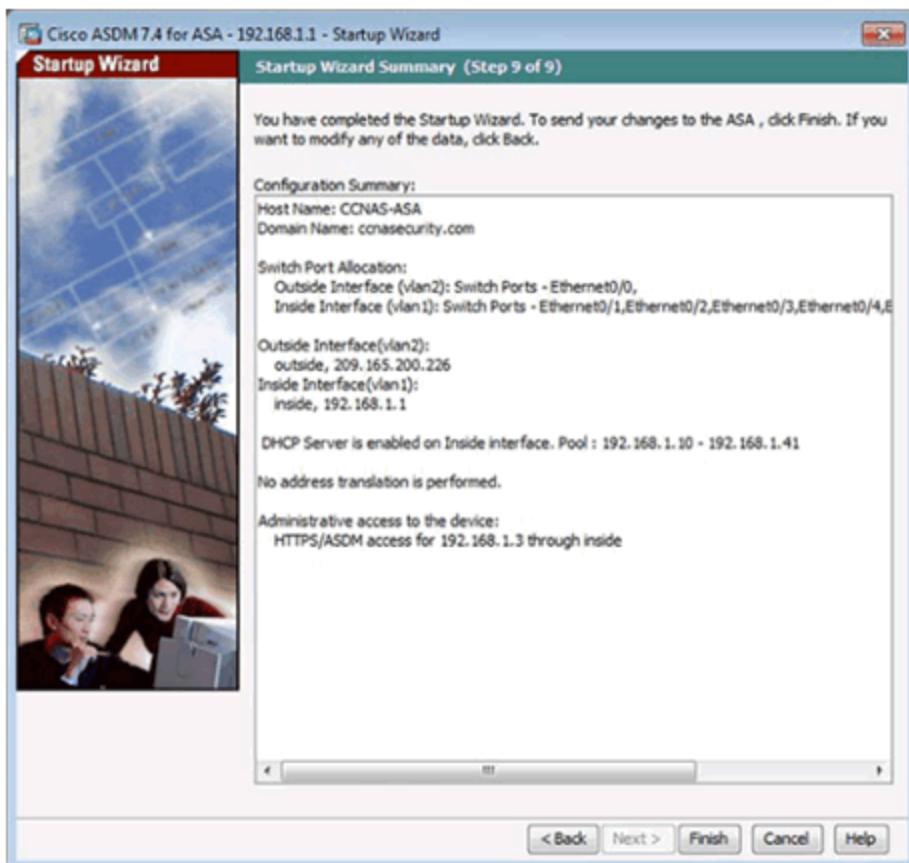
## Startup Wizard Address Translation (NAT/PAT) Window



## Startup Wizard Administrative Access Window

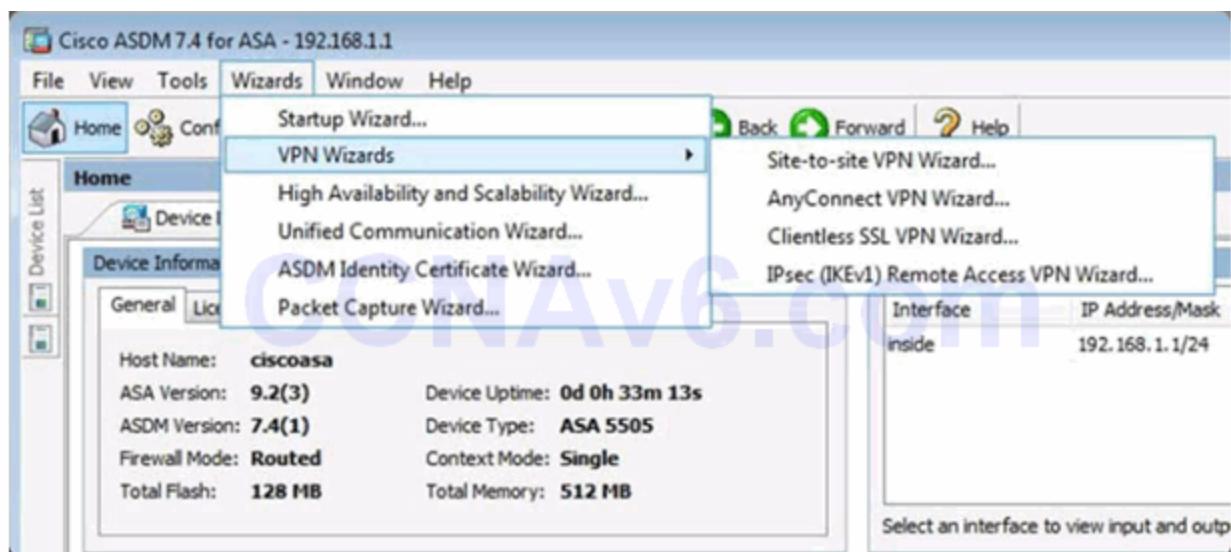


Startup Wizard Summary Window

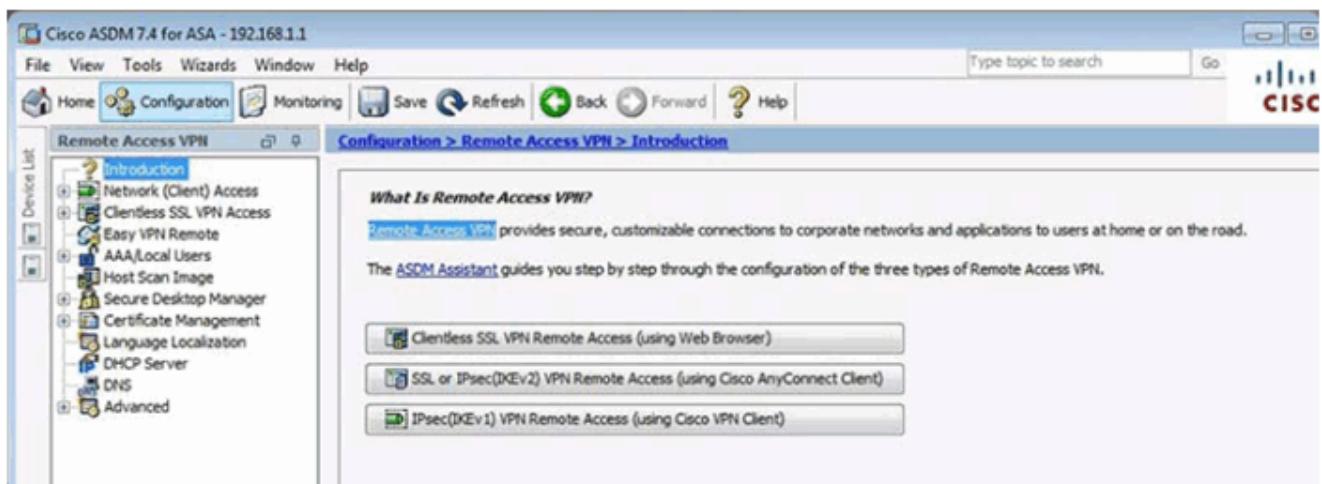


## Different Types of VPN Wizards

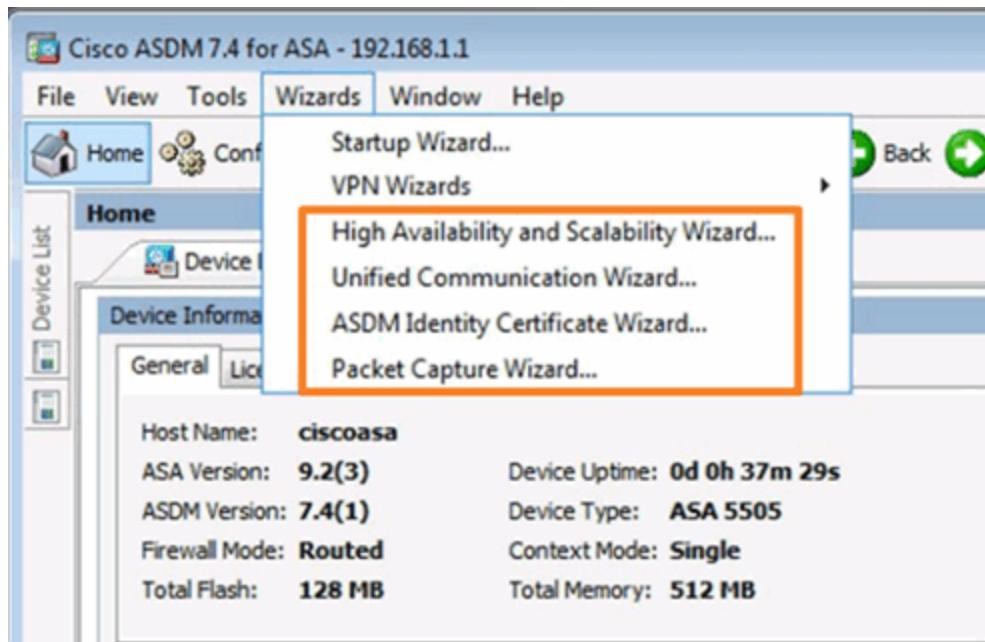
### ASDM VPN Wizards



### ASDM Remote Access VPN Assistant



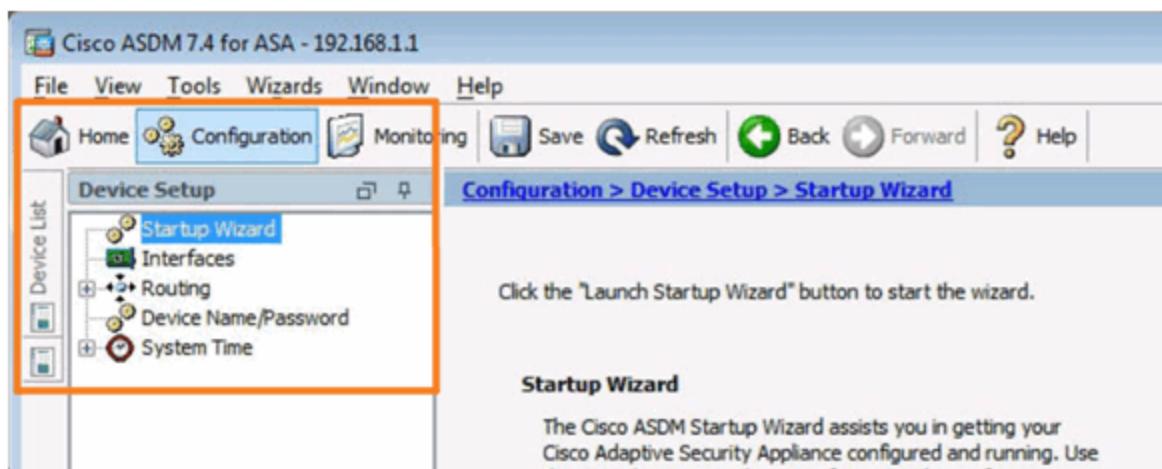
### Other Wizards



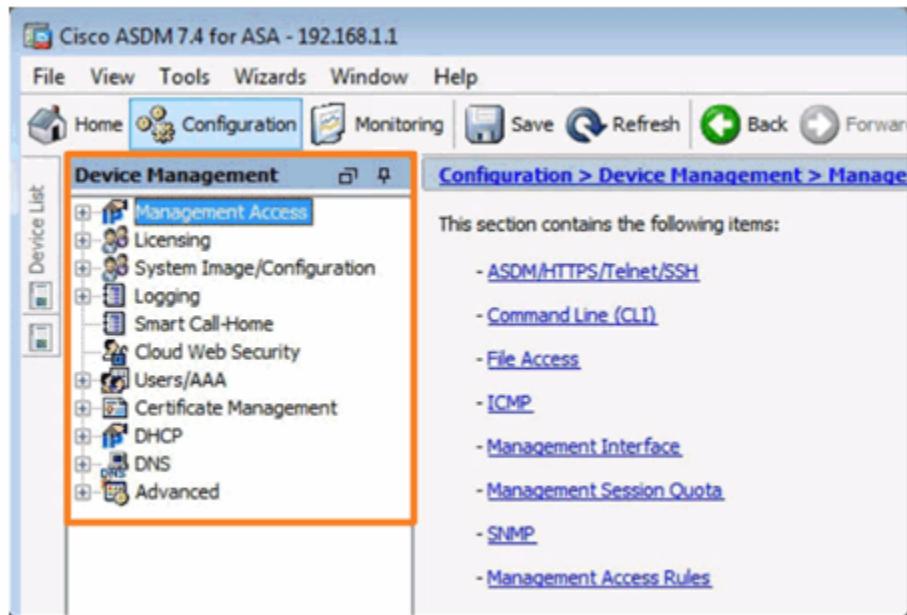
## Topic 10.1.3: Configuring Management Settings and Services

### Configuring Settings in ASDM

Configuration Device Setup Tab

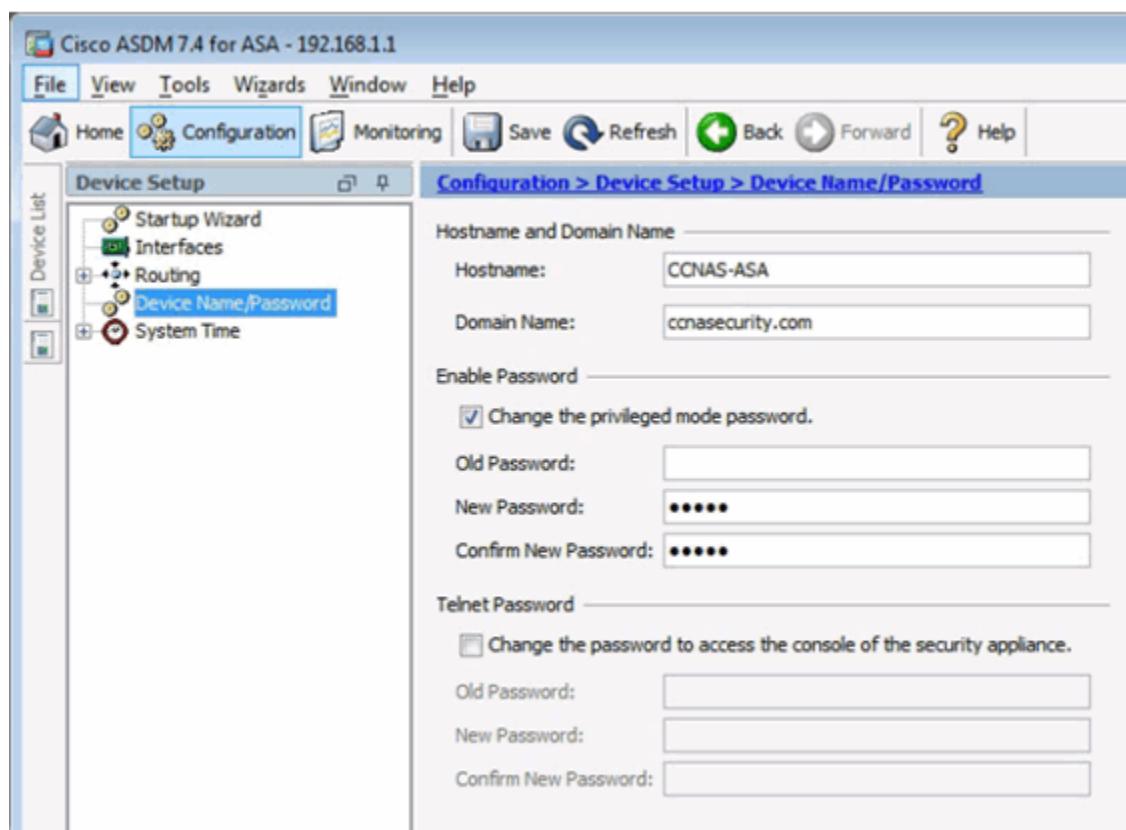


Configuration Device Management Tab



## Configuring Basic Settings in ASDM

Configuring Hostname, Domain Name, and Enable Password



Configuring a Master Passphrase

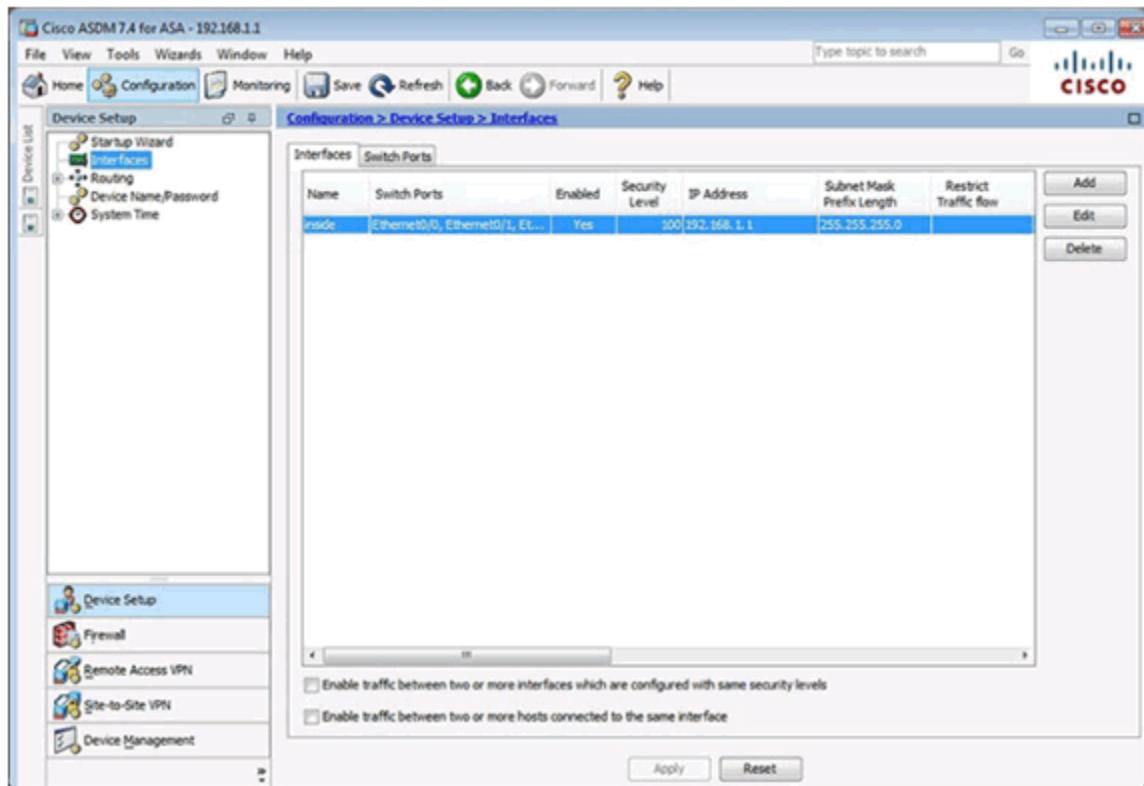
The screenshot shows the Cisco ASDM 7.4 interface for ASA 192.168.1.1. The left sidebar has a tree view under 'Device Management' with nodes like Management Access, Licensing, System Image/Configuration, Logging, Smart Call-Home, Cloud Web Security, Users/AAA, Certificate Management, DHCP, DNS, and Advanced (which is expanded to show ARP, Embedded Event Manager, HTTP Redirect, History Metrics, IPv6 Neighbor Discovery Cache, Master Passphrase, Priority Queue, Rule Engine, SSL Settings, and WCCP). The main pane shows the 'Master Passphrase' configuration page. It includes a note about reversible encryption of supported shared keys and passwords, a checkbox for 'Enable Advanced Encryption Standard (AES) password encryption', and fields for 'Old master passphrase', 'New master passphrase', and 'Confirm master passphrase'.

## Configuring Legal Notification

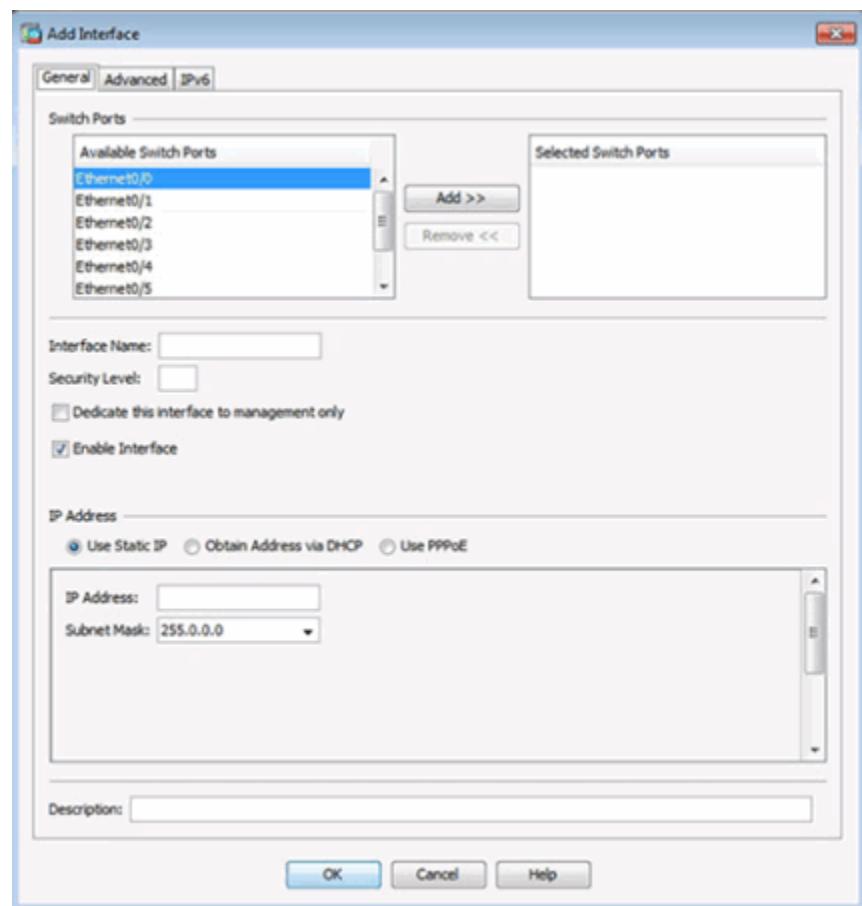
The screenshot shows the 'Banner' configuration page under 'Management Access' in the 'Command Line (CLI)' section. The left sidebar is identical to the previous screenshot. The main pane allows configuring four types of banners: 'Session (exec) Banner', 'Login Banner', 'Message-of-The-Day (motd) Banner', and 'ASDM Banner'. Each banner is represented by a large text input field.

## Configuring Interfaces in ASDM

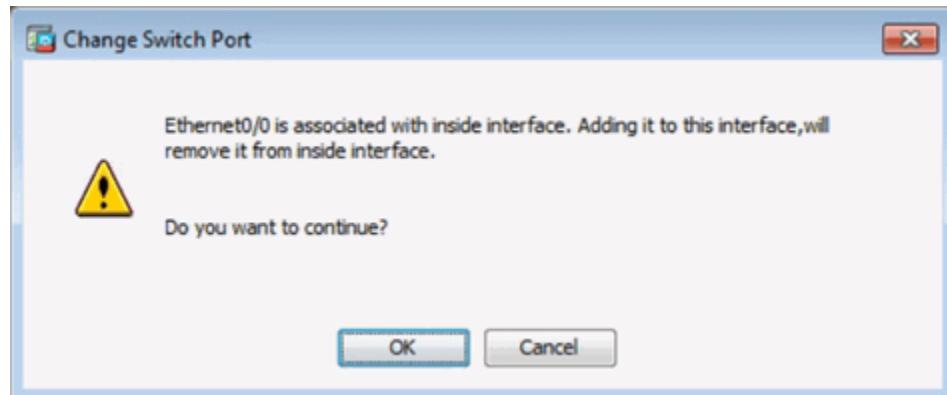
### Configuring Interfaces



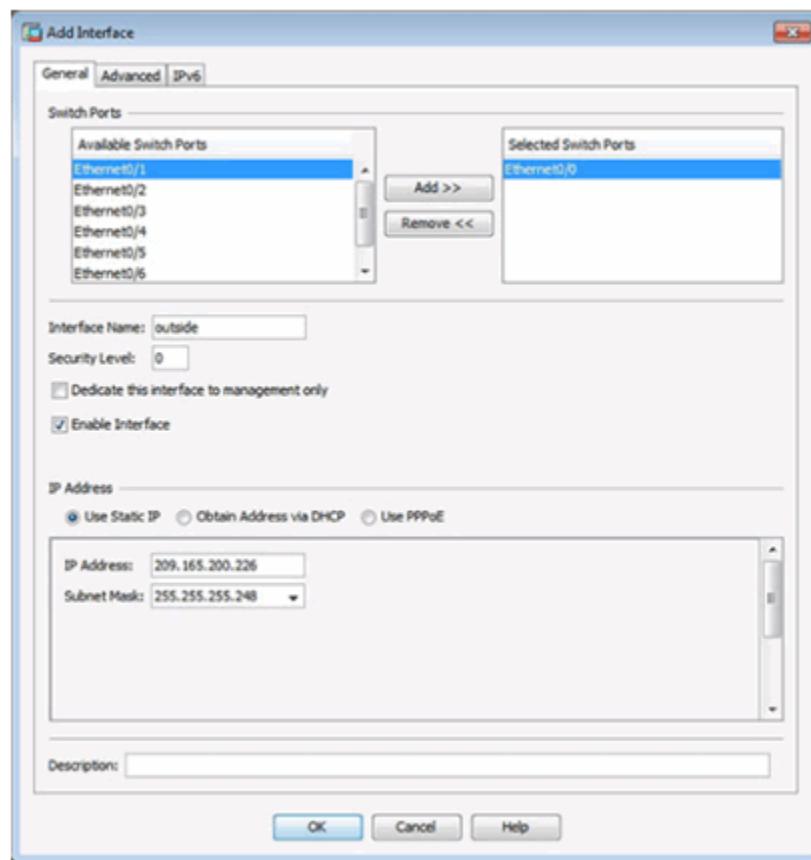
## Adding an Outside Interface



## Change Switch Port Window



## Adding an Outside Interface



## Advanced Outside Interface Settings

**Add Interface**

General Advanced IPv6

MTU: 1500 VLAN ID: 2

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			

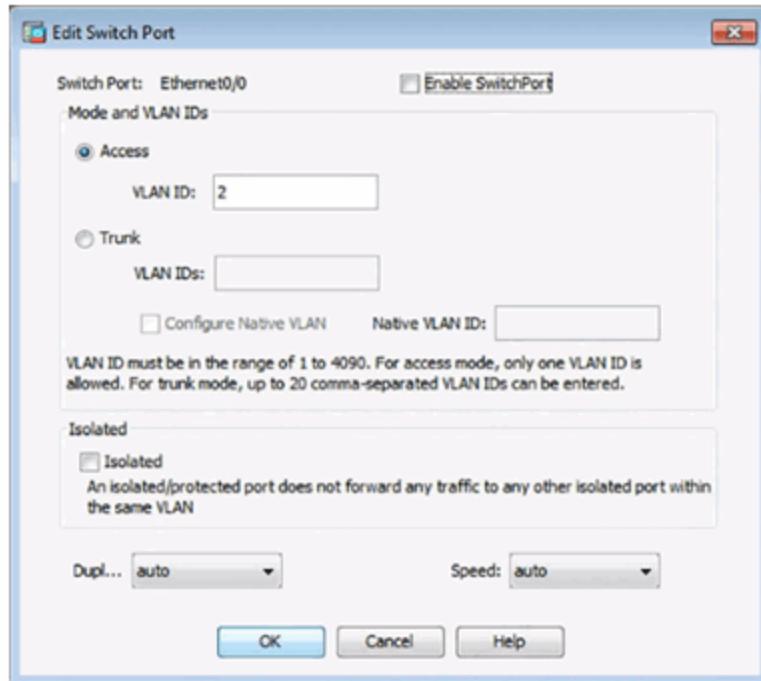
Add Edit Delete

## Verifying Interfaces

**Configuration > Device Setup > Interfaces**

Interfaces		Switch Ports							
Switch Port	Enabled	Associated VLANs	Associated Interface Names	Mode	Protected	Duplex	Speed		
Ethernet0/0	No	2	outside	Access	No	auto	auto	Edit	
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		

## Enable Switch Ports



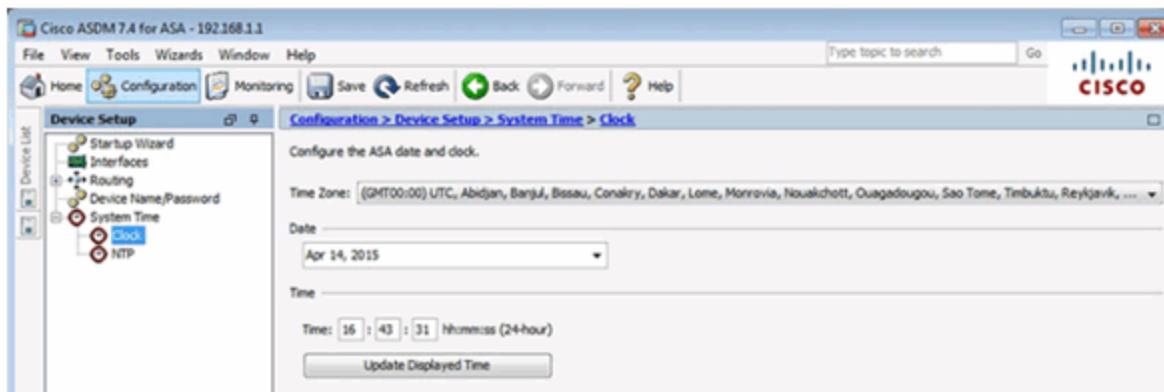
## Apply Configuration

Configuration > Device Setup > Interfaces						
Interfaces		Switch Ports				
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	

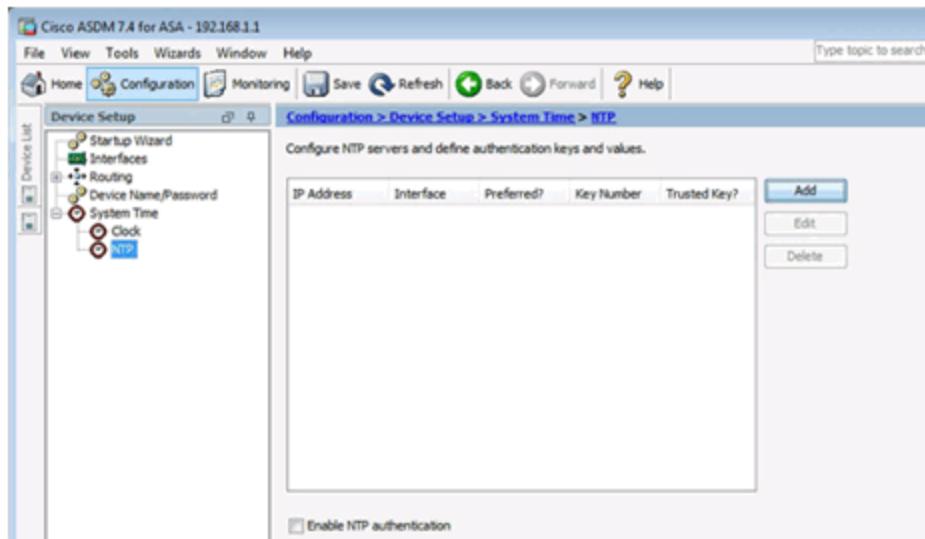
Add  
Edit  
Delete

## Configuring the System Time in ASDM

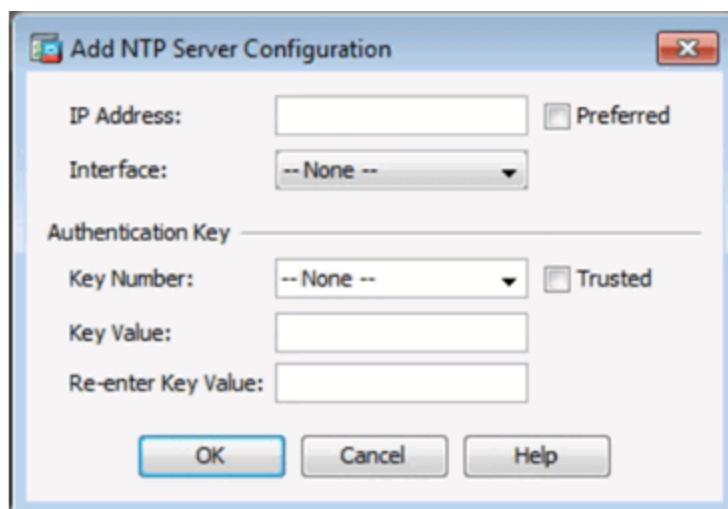
### Manually Change the System Time



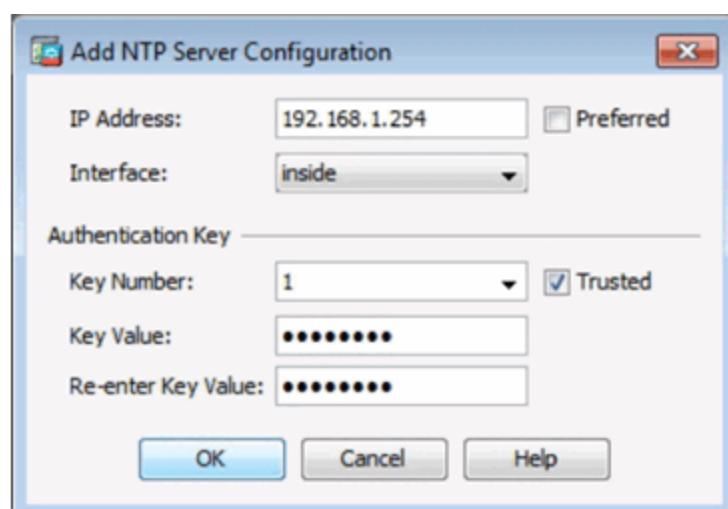
### Use NTP to Change the System Time



## Add an NTP Server



## Configure an NTP Server



## 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

Add Edit Delete

Enable NTP authentication

## Configuring Routing in ASDM

### Configuring Routing

Cisco ASDM 7.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward

Device Setup

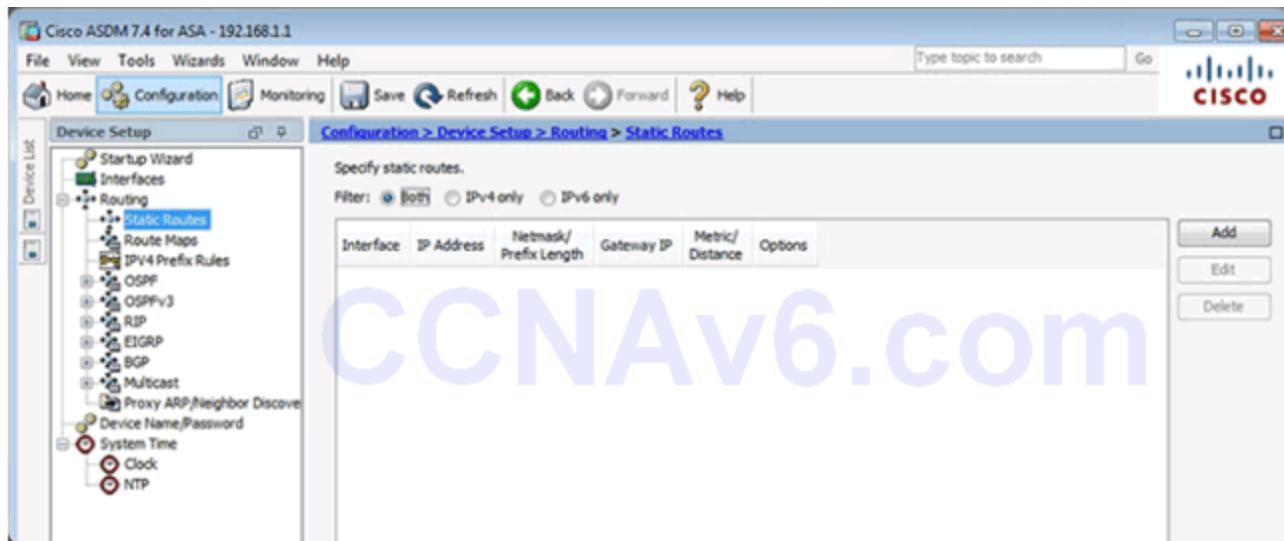
- Startup Wizard
- Interfaces
- Routing
  - Static Routes
  - Route Maps
  - IPv4 Prefix Rules
- OSPF
- OSPFv3
- RIP
- EIGRP
- BGP
- Multicast
- Proxy ARP/Neighbor Discover
- Device Name/Password
- System Time
  - Clock
  - NTP

Configuration > Device Setup > Routing

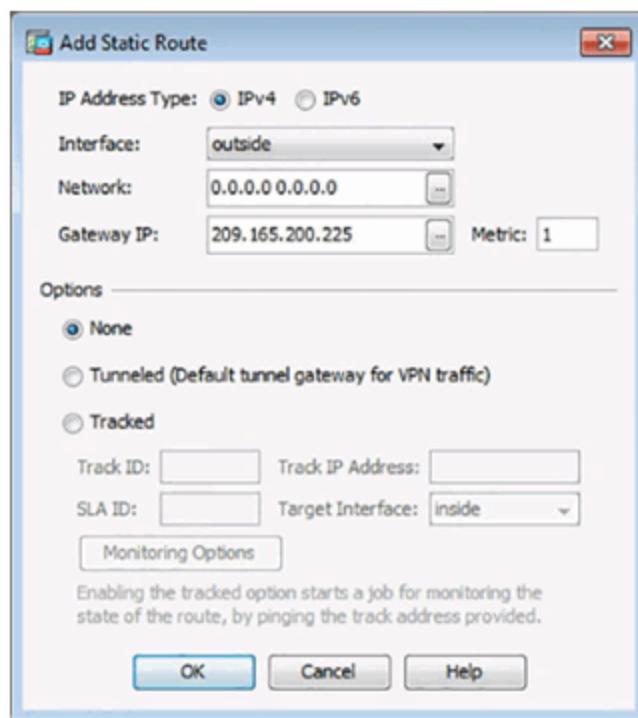
This section contains the following items:

- [Static Routes](#)
- [Route Maps](#)
- [IPv4 Prefix Rules](#)
- [OSPF](#)
- [OSPFv3](#)
- [RIP](#)
- [EIGRP](#)
- [BGP](#)
- [Multicast](#)
- [Proxy ARP/Neighbor Discovery](#)

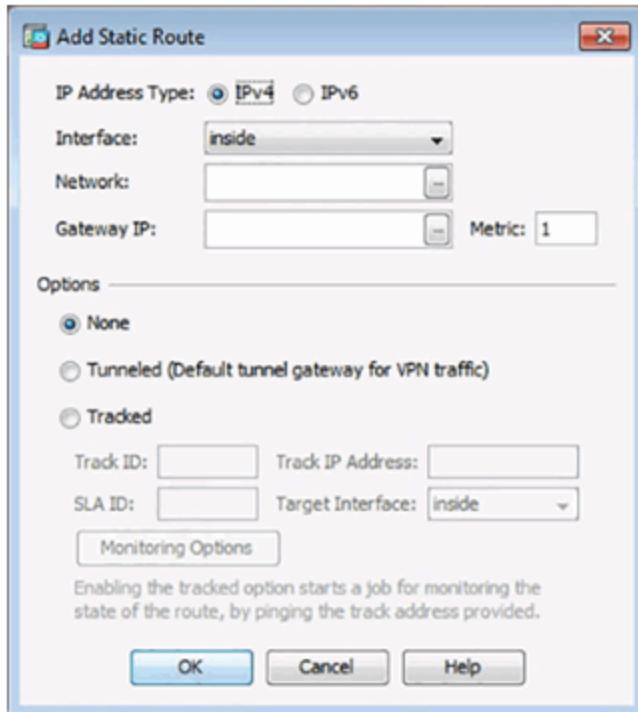
### Configuring a Default Static Route



## Add or Edit Route Window



## Add Static Route Details



## Apply the Configuration

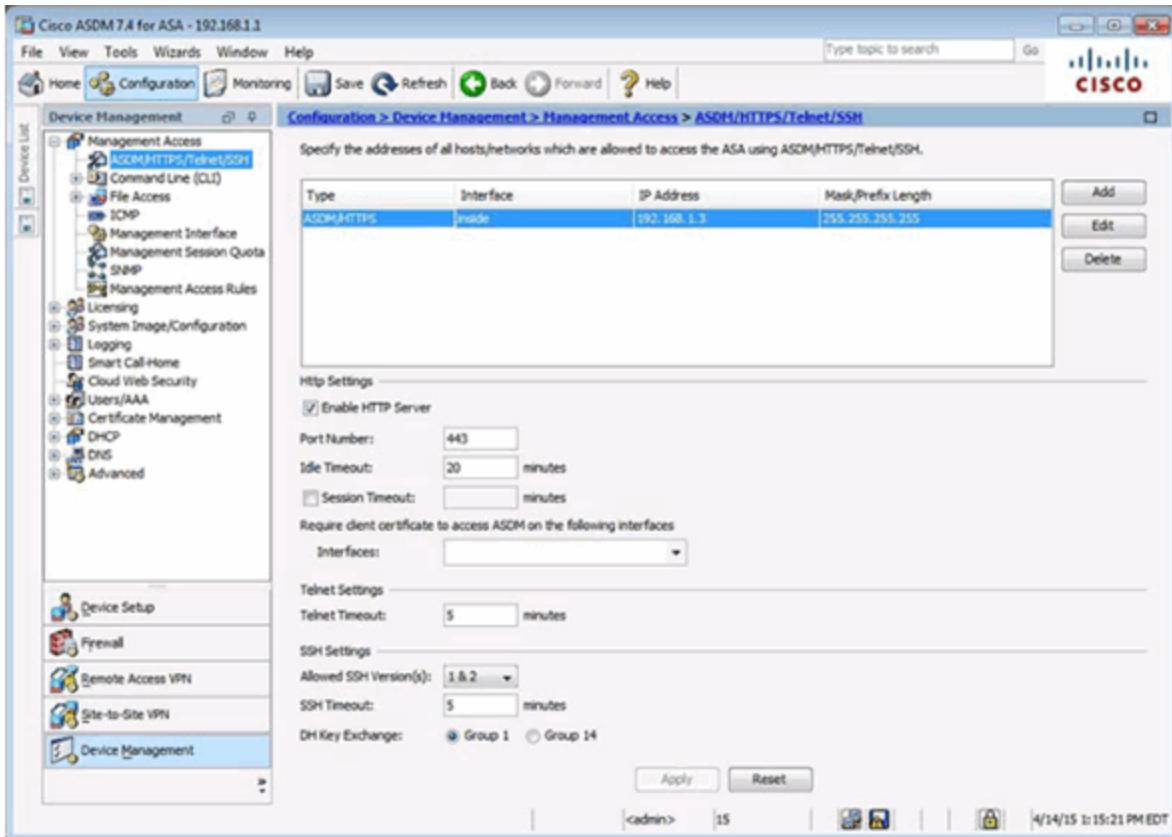
The screenshot shows the 'Static Routes' configuration page in ASDM. The title bar says 'Configuration > Device Setup > Routing > Static Routes'. It says 'Specify static routes.' and has a 'Filter' dropdown set to 'Both'. A table lists one static route:

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

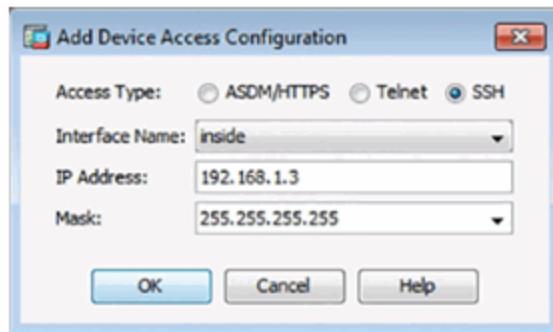
On the right, there are 'Add', 'Edit', and 'Delete' buttons.

## Configuring Device Management Access in ASDM

Configure ASDM/HTTPS/Telnet/SSH Access



Add Device Access Configuration Window



Configure SSH Settings

**Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**

Specify the addresses of all hosts/networks which are allowed to access the ASA using ASDM/HTTPS/Telnet/SSH.

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

**Add** **Edit** **Delete**

**Http Settings**

Enable HTTP Server

Port Number:

Idle Timeout:  minutes

Session Timeout:  minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

**Telnet Settings**

Telnet Timeout:  minutes

**SSH Settings**

Allowed SSH Version(s):

SSH Timeout:  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** **Type topic to search Go**

**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
inside	No	-	-	-	-	-
outside	No	-	-	-	-	-

**Edit**

**Global DHCP Options**

Enable auto-configuration from interface:   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

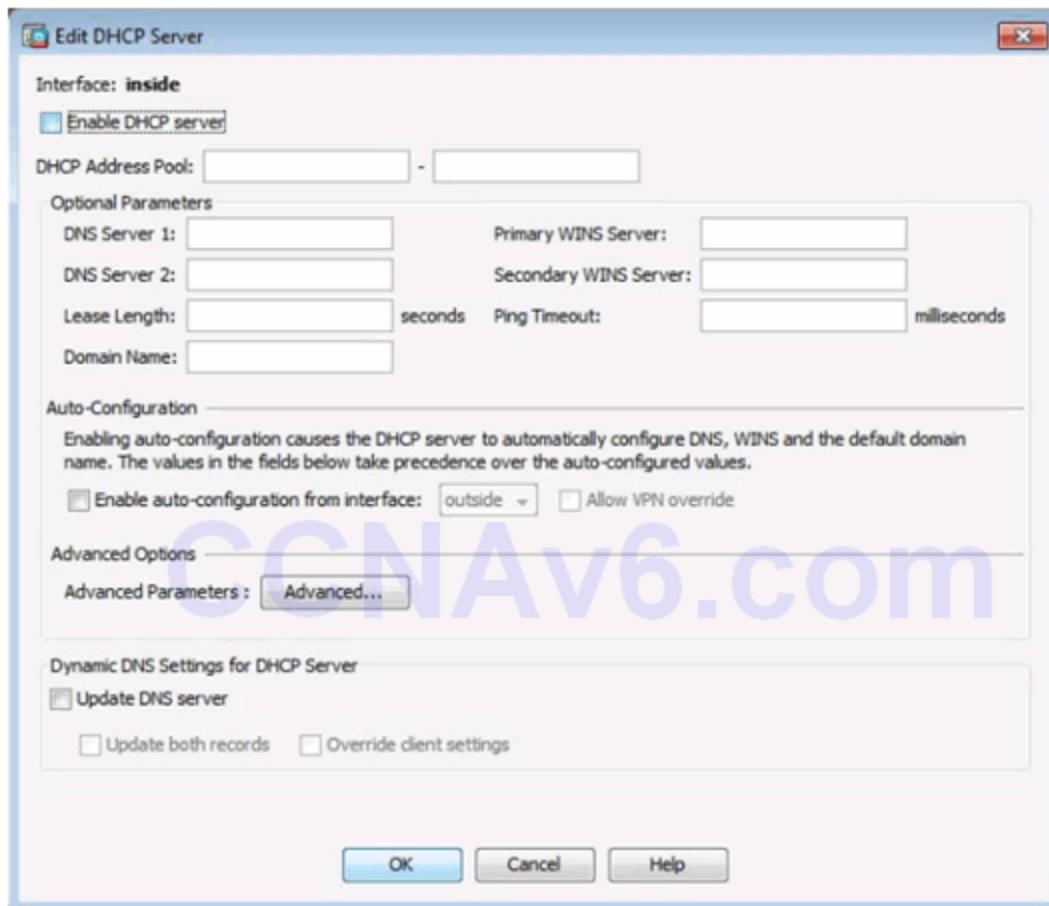
**Advanced...**

**Dynamic DNS Settings for DHCP Server**

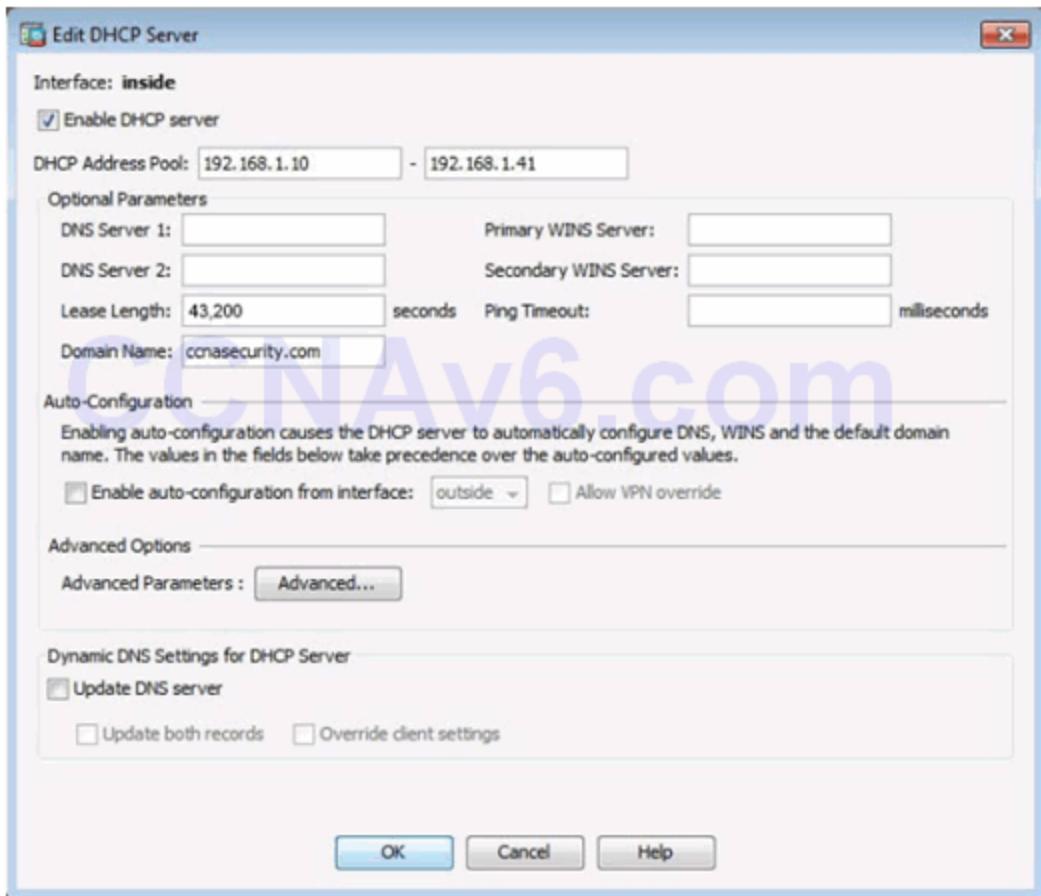
Update DNS Server  
 Update Both Records  Override Client Settings

**Apply** **Reset**

## Edit DHCP Server Window



## Configuring DHCP Server Services



## Verifying DHCP Server Services

[Configuration > Device Management > DHCP > DHCP Server](#)

Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout	Edit
inside	Yes	192.168.1.10 - 192.168.1.41			ccnasecurity....		
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

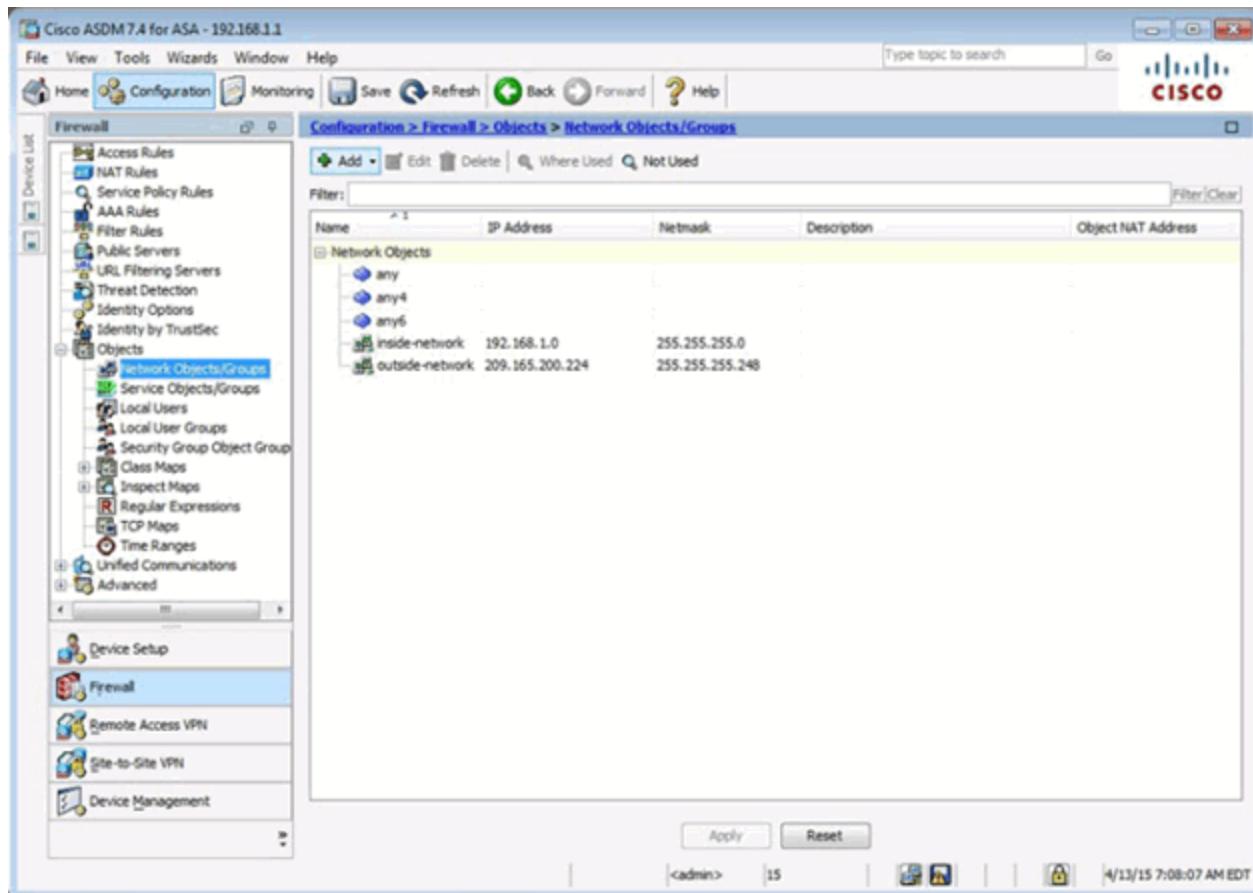
## Topic 10.1.4: Configuring Advanced ASDM Features

---

### Objects in ASDM

---

Network Objects/Groups Page



## Adding a Network Object/Group

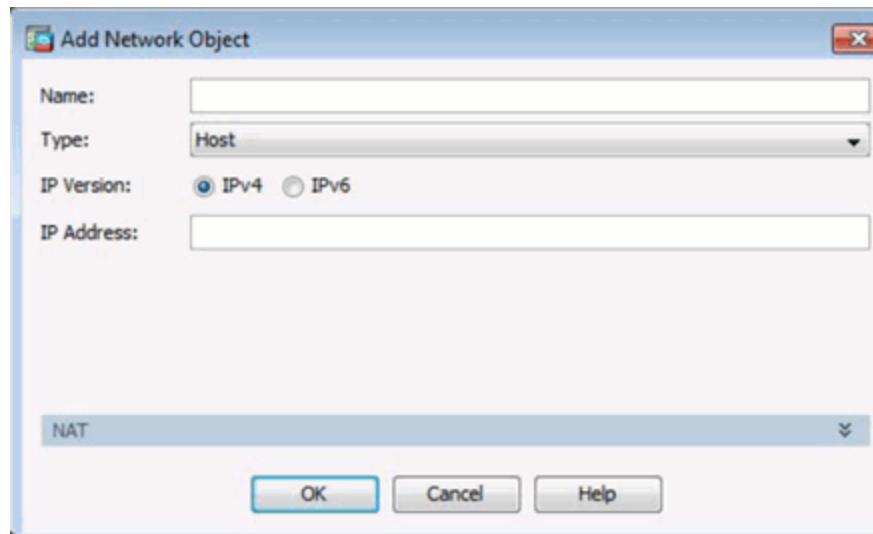
This is a screenshot of the 'Add Network Object' dialog box. At the top are buttons for 'Add', 'Edit', 'Delete', 'Where Used', and 'Not Used'. Below is a list of options:

- Network Object...
- Network Object Group...

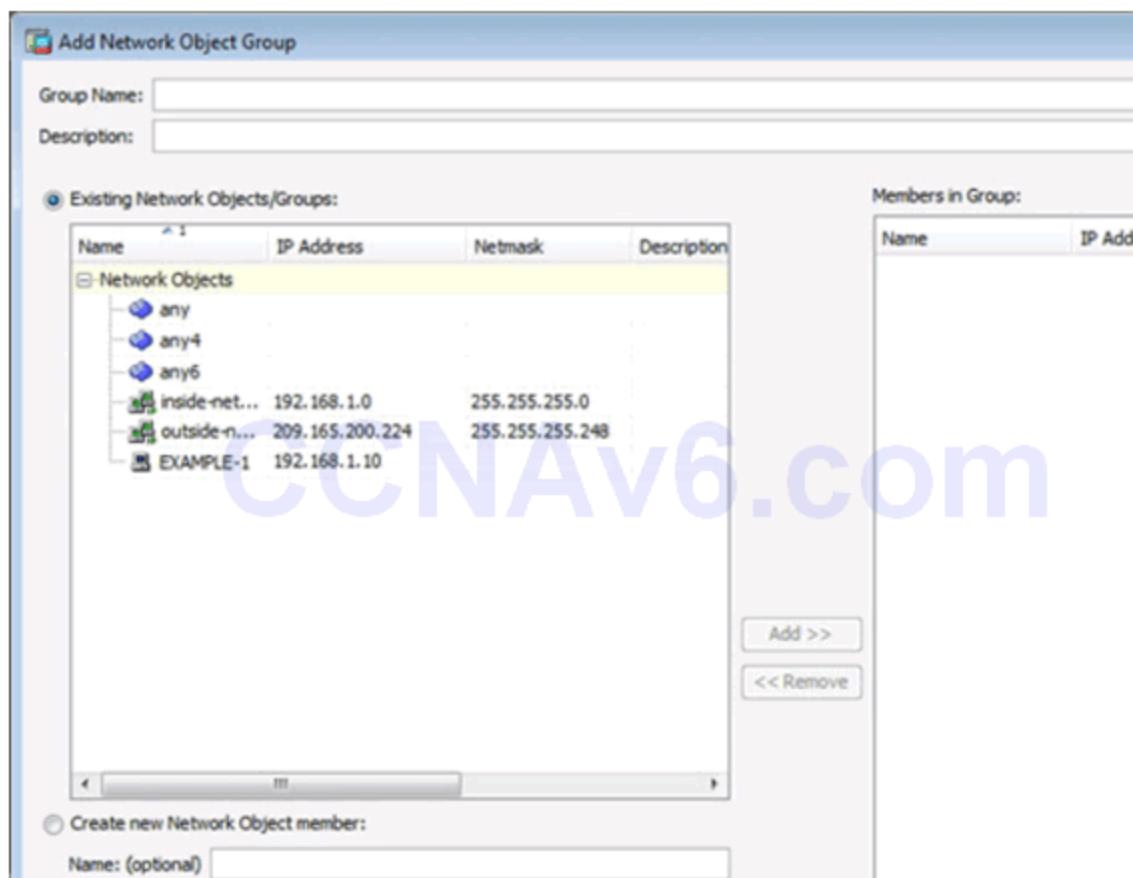
The 'Network Objects' section shows the same list as the main configuration screen:

- any
- any4
- any6
- inside-network 192.168.1.0 255.255.255.0
- outside-network 209.165.200.224 255.255.255.248

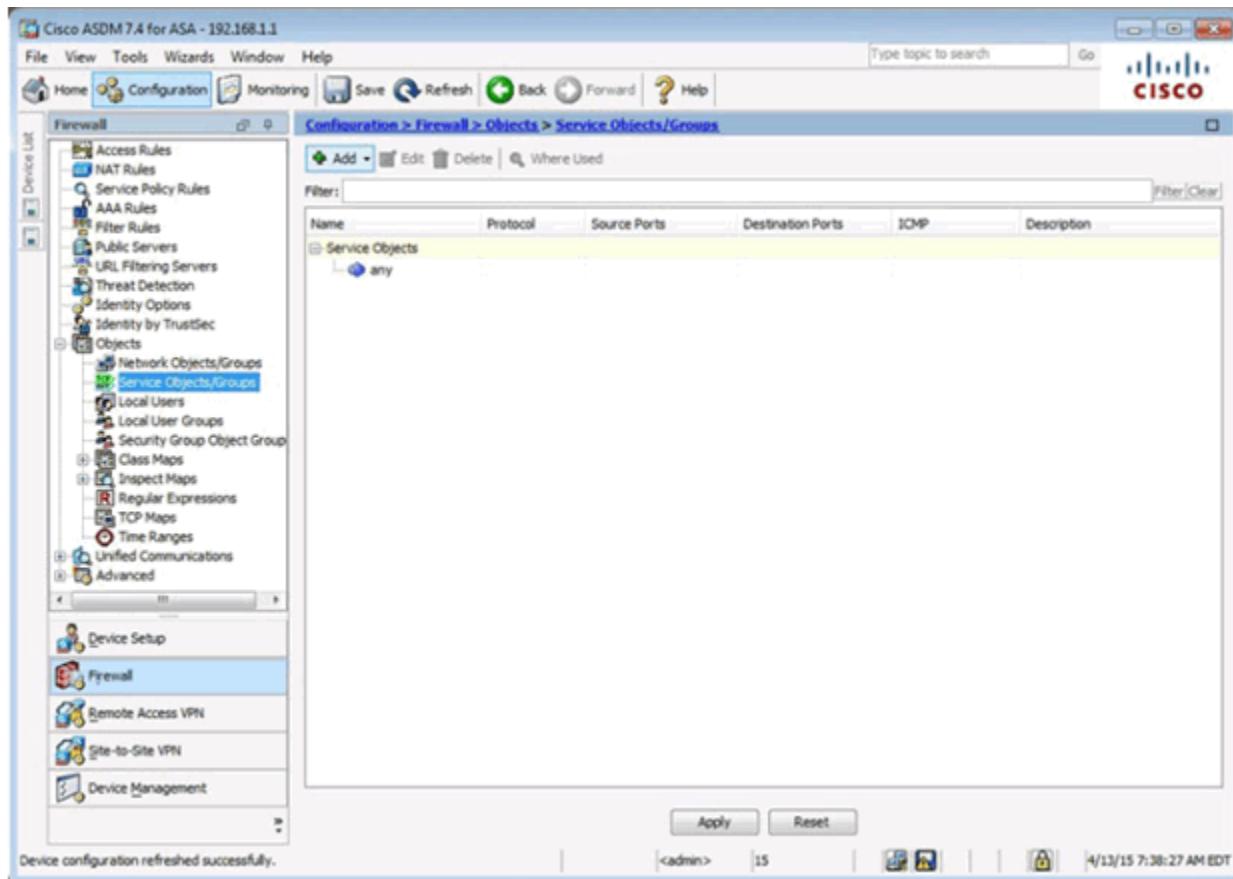
## Add Network Object Window



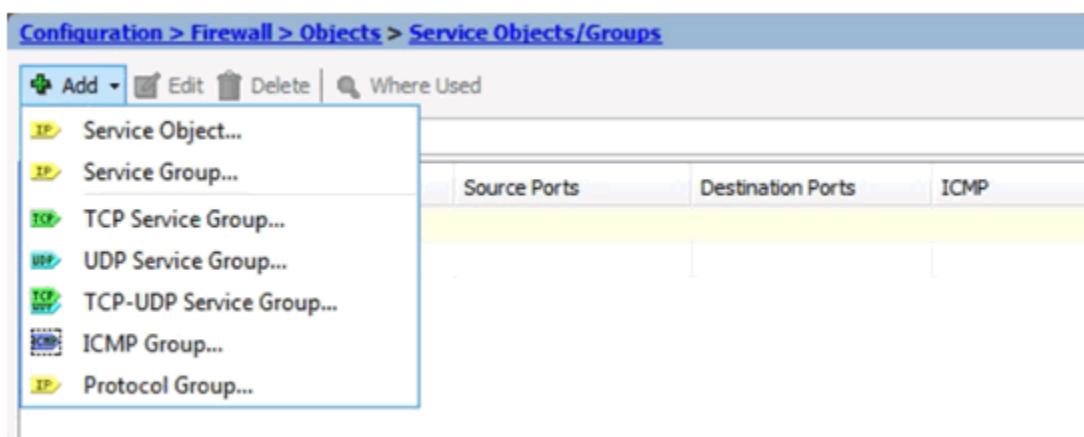
Add Network Object Group Window



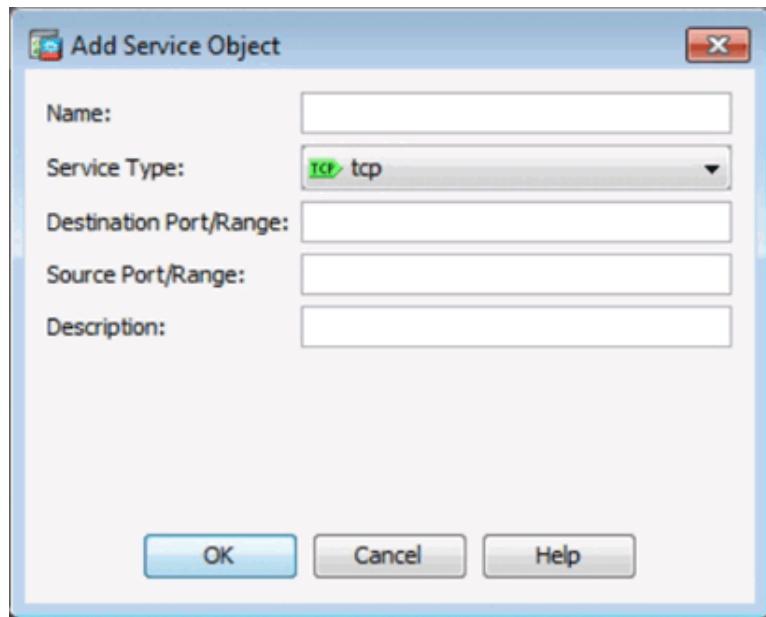
Service Objects/Group Page



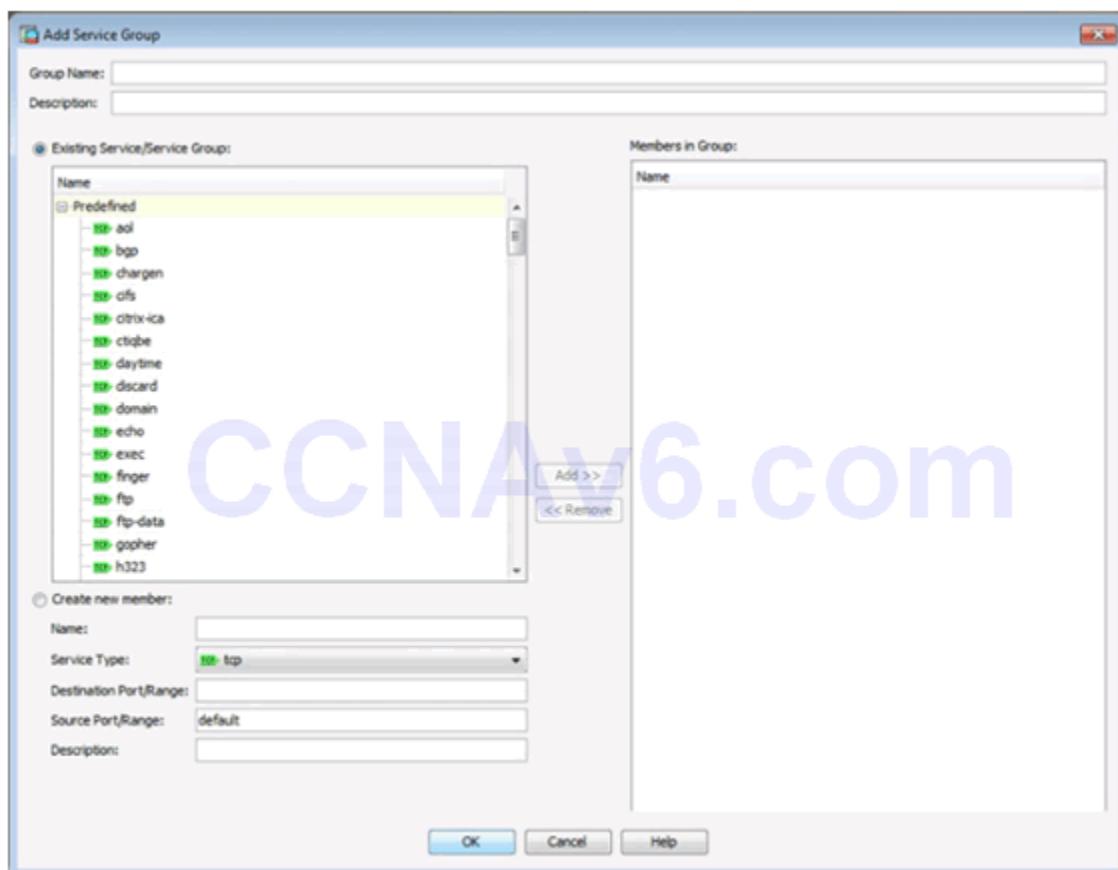
## Adding a Service Object/Group



## Add Service Object Window

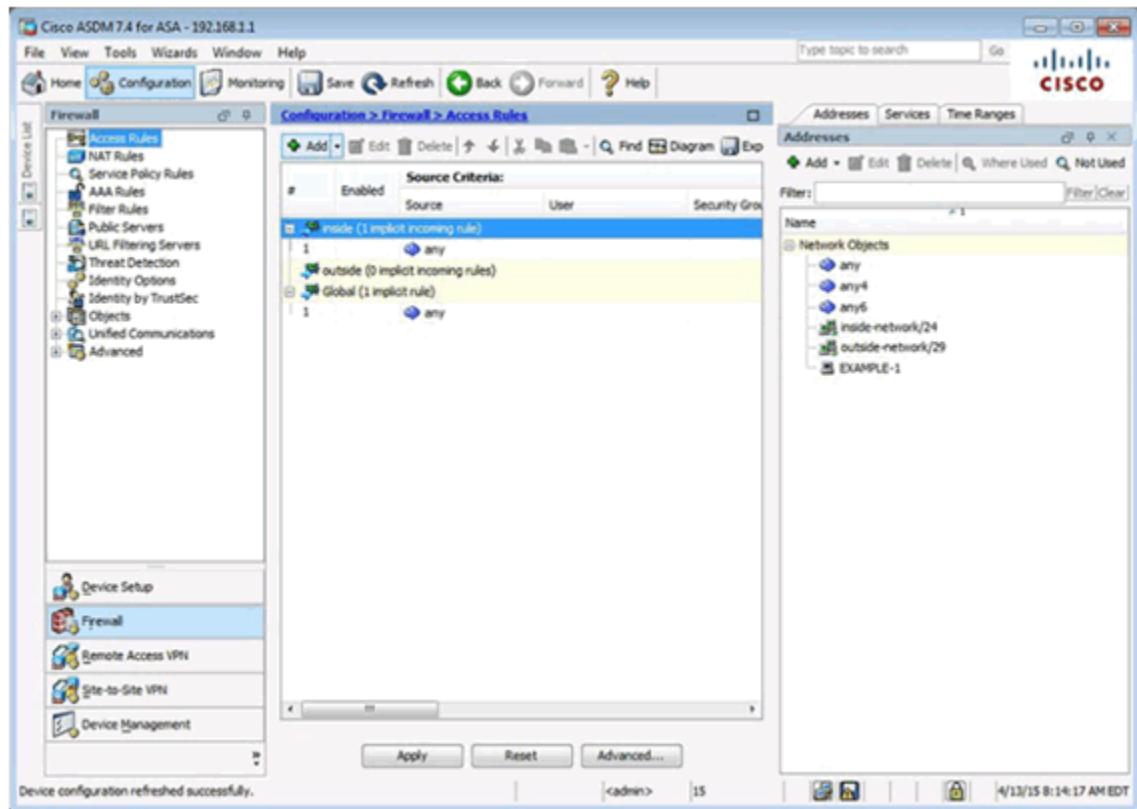


Add Service Object Group Window

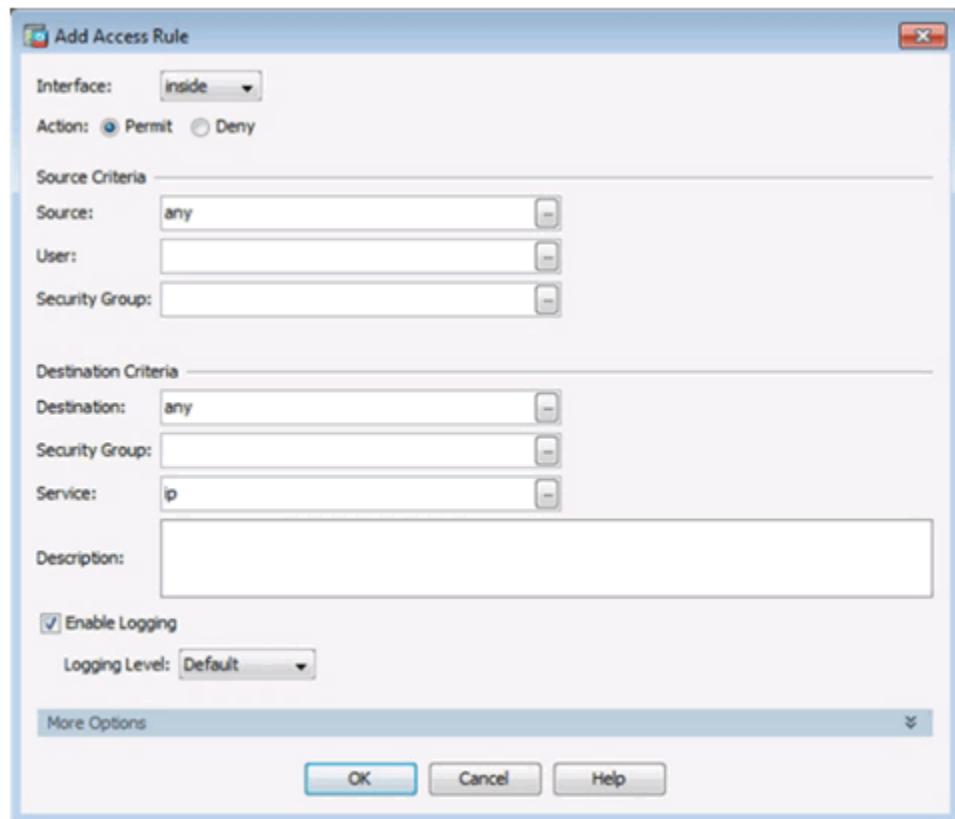


## Configuring ACLs Using ASDM

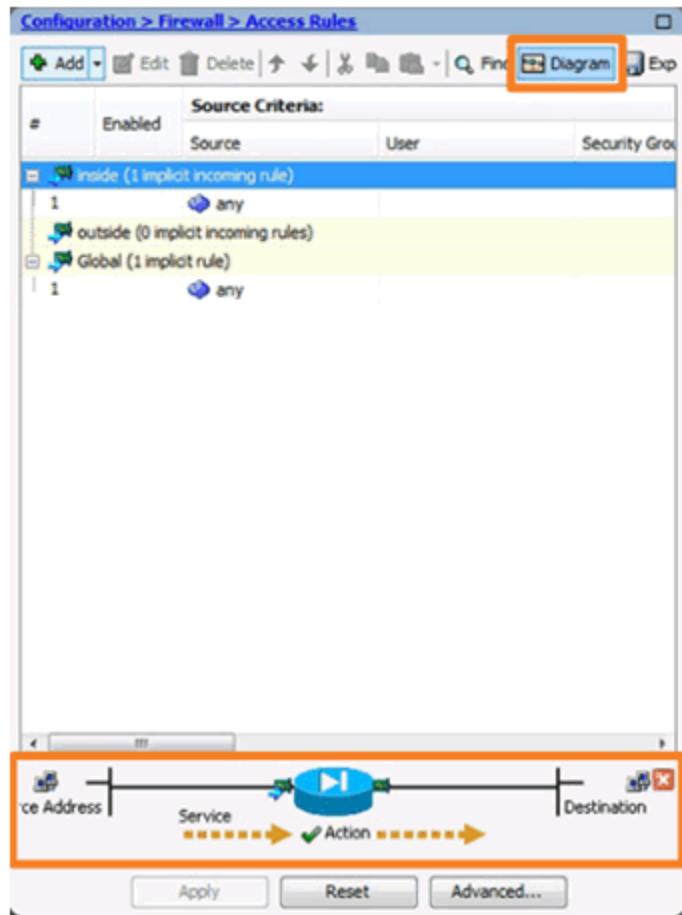
ACLs in ASDM



Add Access Rule Window

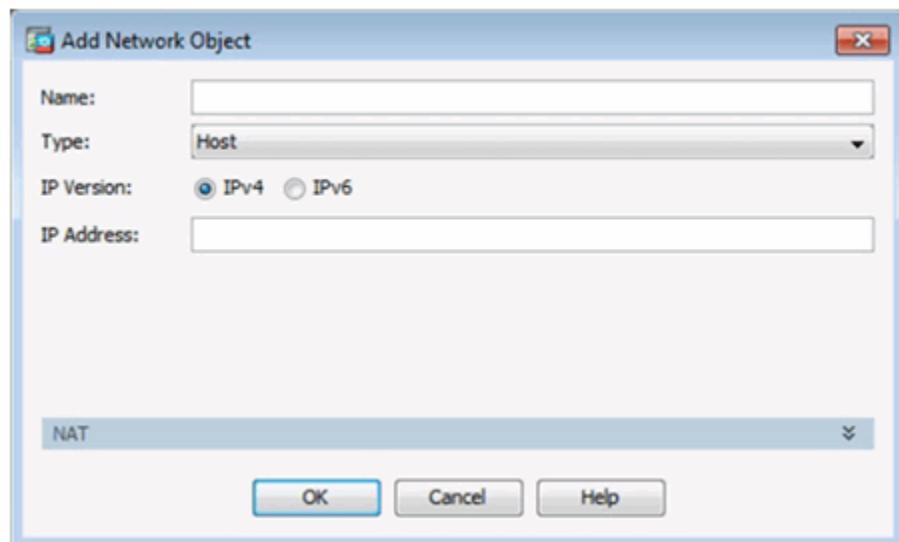


Diagramming Access Rules

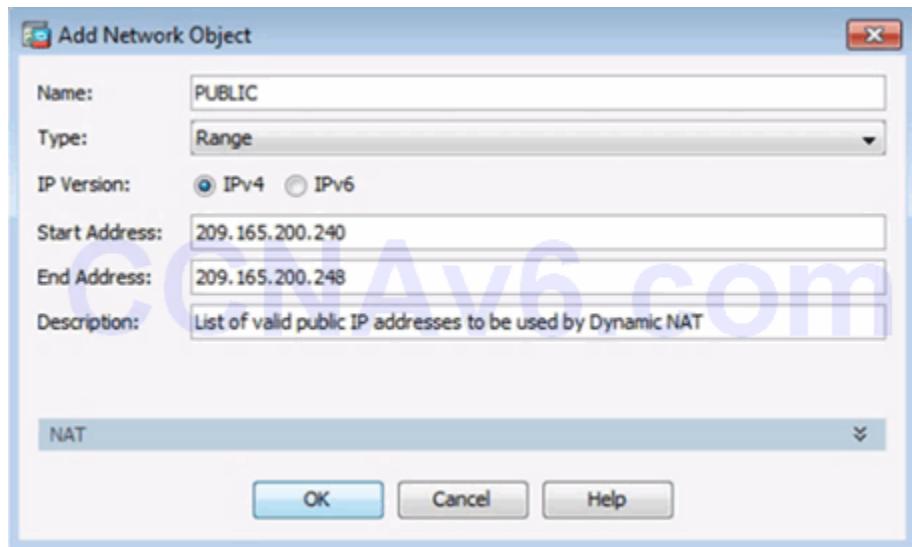


## Configuring Dynamic NAT in ASDM

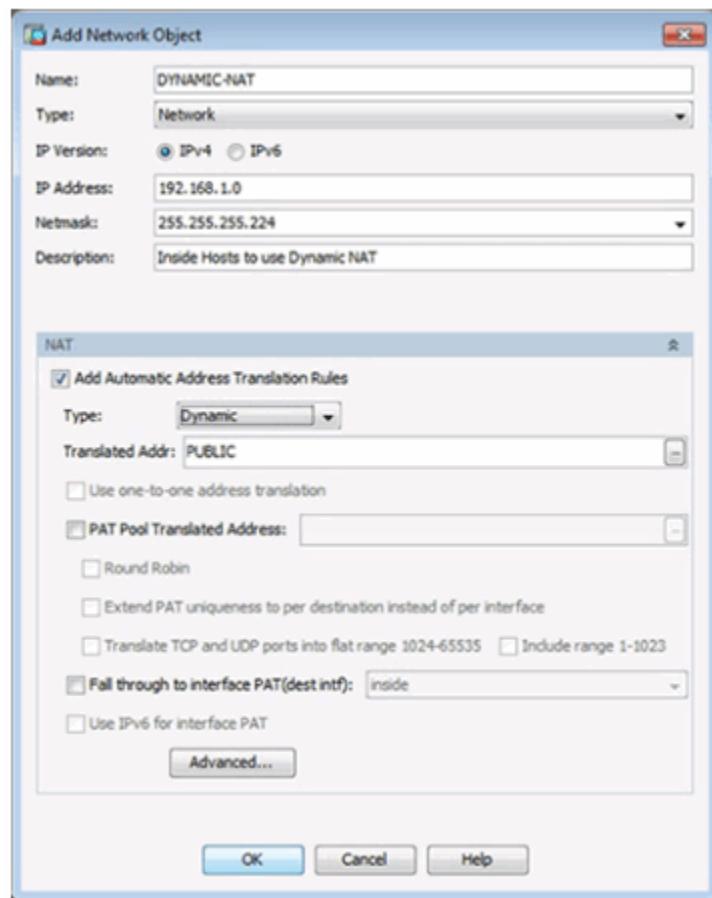
Add Network Object Window



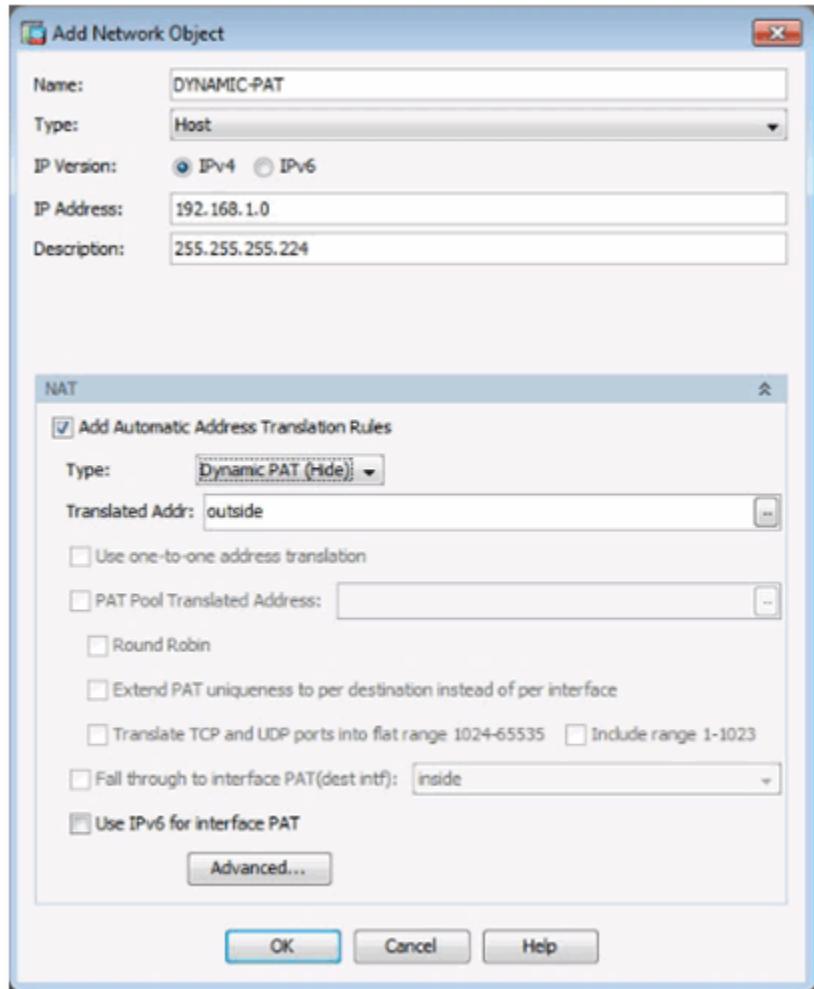
Creating a Network Object for Public Addresses



## Creating a Network Object for Dynamic NAT



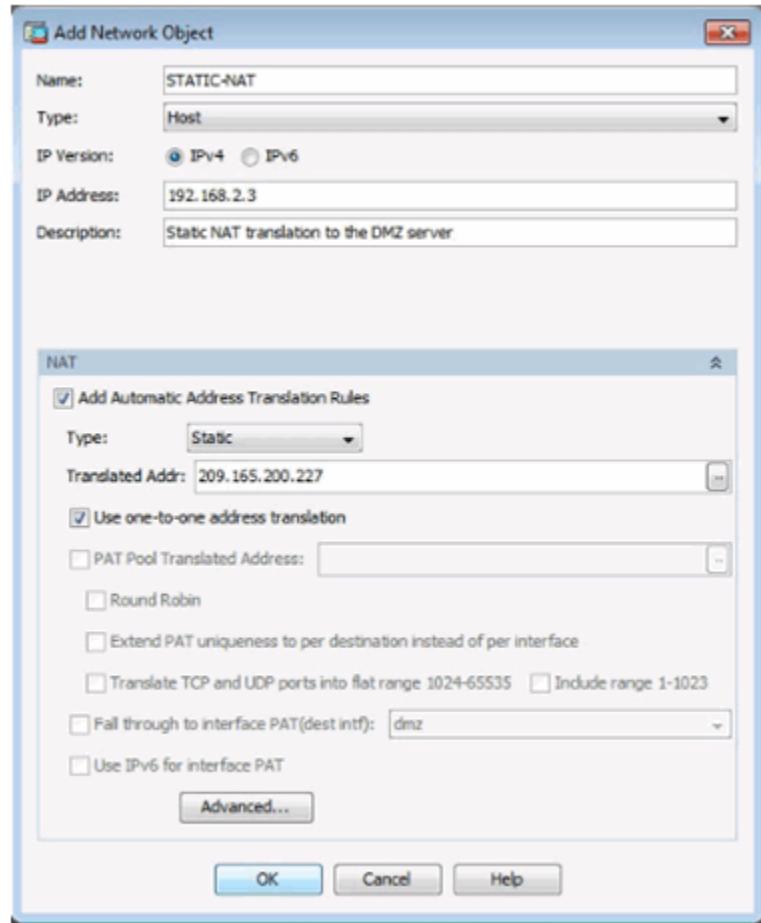
## Configuring Dynamic PAT in ASDM



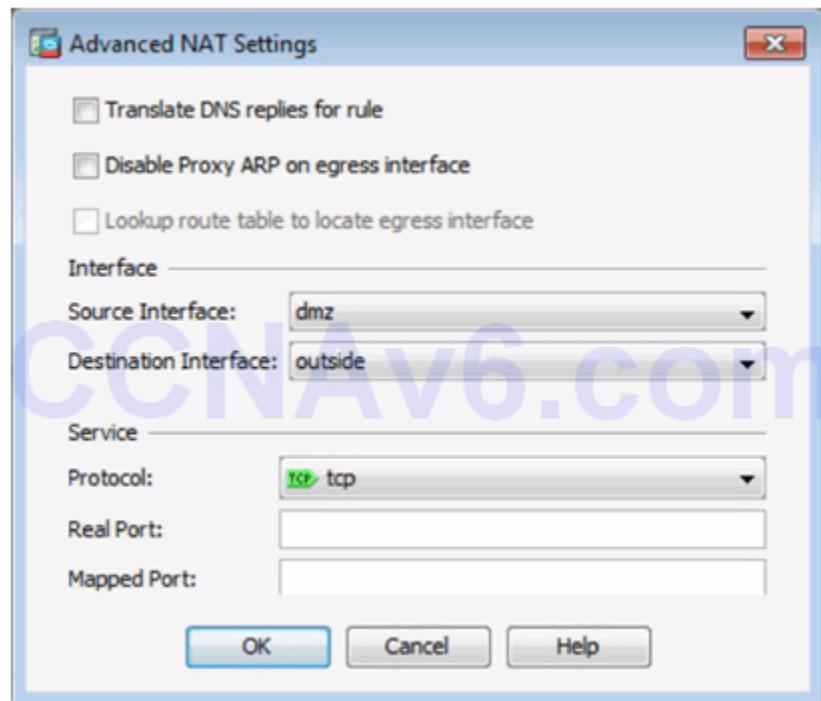
## Configuring Static NAT in ASDM

---

Static NAT in ASDM



## Advanced Static NAT Settings in ASDM



## Configuring AAA Authentication

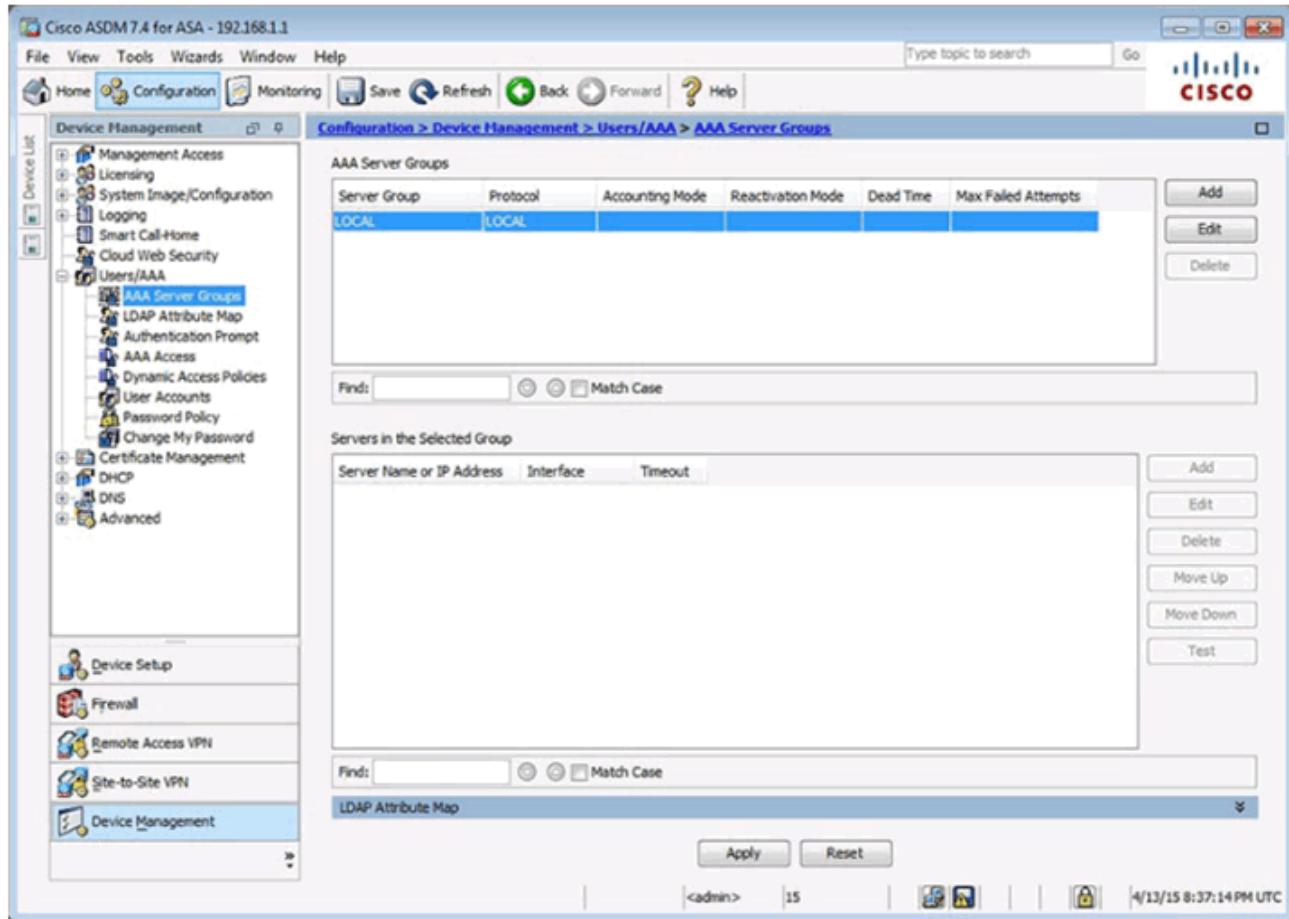
## User Accounts Page

The screenshot shows the Cisco ASDM 7.4 interface for ASA 192.168.1.1. The left sidebar has a tree view under 'Device Management' with nodes like Management Access, Licensing, System Image/Configuration, Logging, Smart Call-Home, Cloud Web Security, Users/AAA, AAA Server Groups, LDAP Attribute Map, Authentication Prompt, AAA Access, Dynamic Access Policies, User Accounts (which is selected), Password Policy, Change My Password, Certificate Management, DHCP, DNS, and Advanced. The main pane title is 'Configuration > Device Management > Users/AAA > User Accounts'. It contains instructions about creating entries in the ASA local user database, enabling command authorization, and AAA authentication console commands. A table lists a single user account: 'enable\_15' with privilege level 15, access restrictions set to 'Full', and both VPN Group Policy and VPN Group Lock set to 'N/A'. There are 'Add', 'Edit', and 'Delete' buttons on the right.

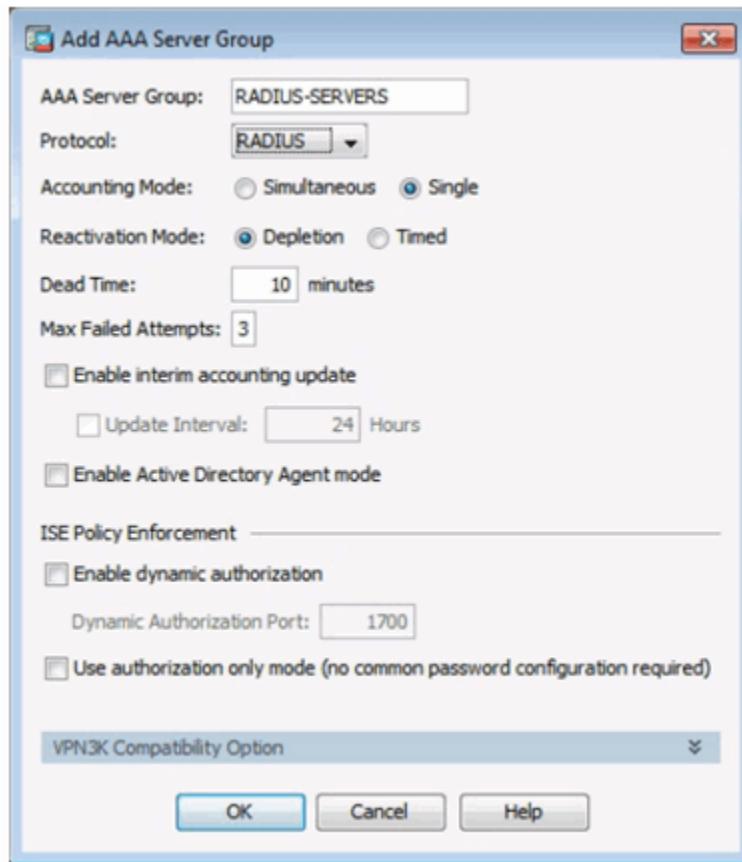
## Add User Account Window

The screenshot shows the 'Add User Account' dialog box. On the left, there's a sidebar with 'Identity' selected, showing options for Public Key Authentication, Public Key Using PKF, and VPN Policy. The main area has fields for 'Username' (ADMIN), 'Password', and 'Confirm Password', all containing asterisks. There's a checkbox for 'User authenticated using MSCHAP'. Below it, 'Access Restriction' is set to 'Full access(ASDM, SSH, Telnet and Console)' with a privilege level of 15. There are also options for 'CLI login prompt for SSH, Telnet and console (no ASDM access)' and 'No ASDM, SSH, Telnet or Console access'. At the bottom, there are 'Find', 'Next', 'Previous', 'OK', 'Cancel', and 'Help' buttons.

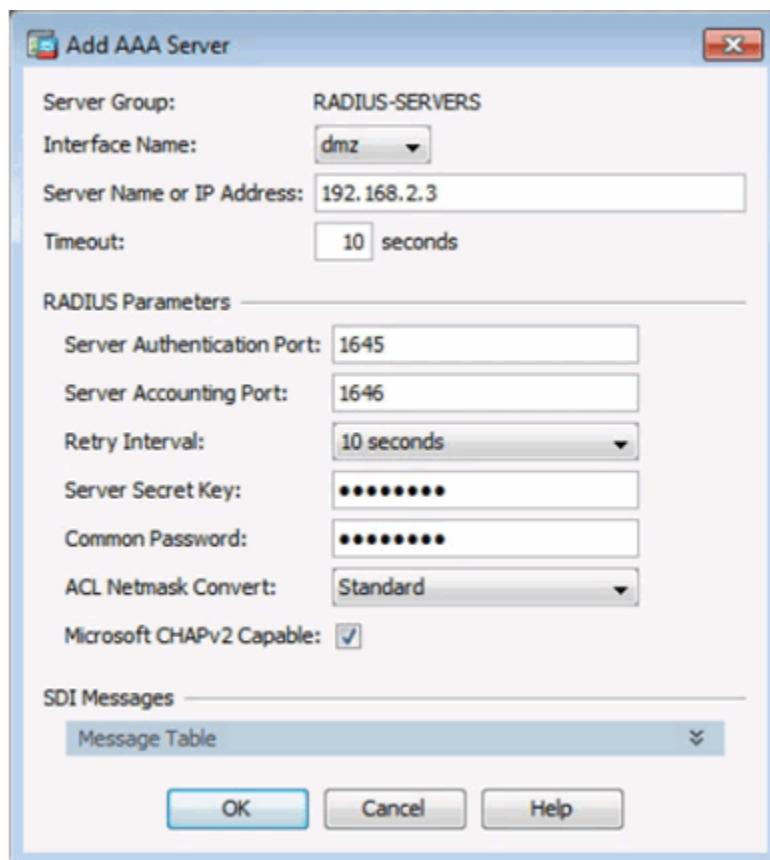
## AAA Server Groups Page



Add AAA Server Group Window



Add AAA Server Window



## Completed AAA Server Groups Window

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

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

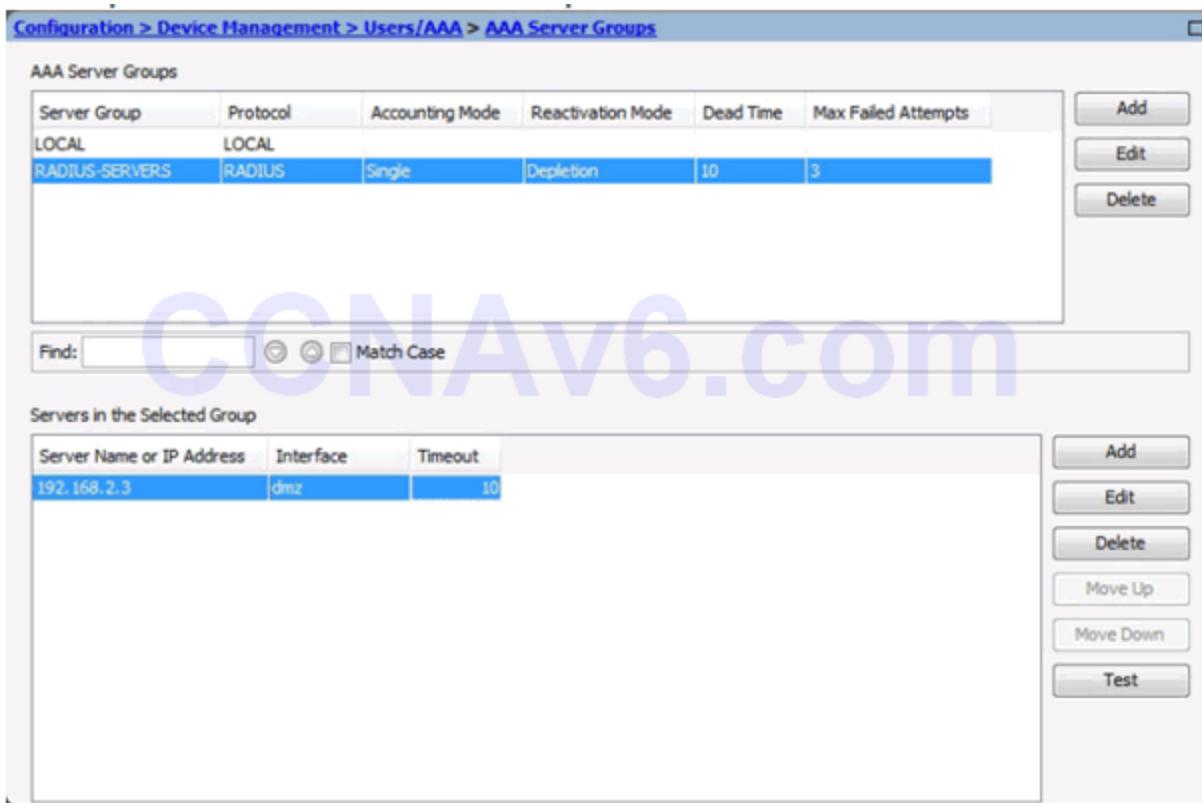
Add Edit Delete

Find:     Match Case

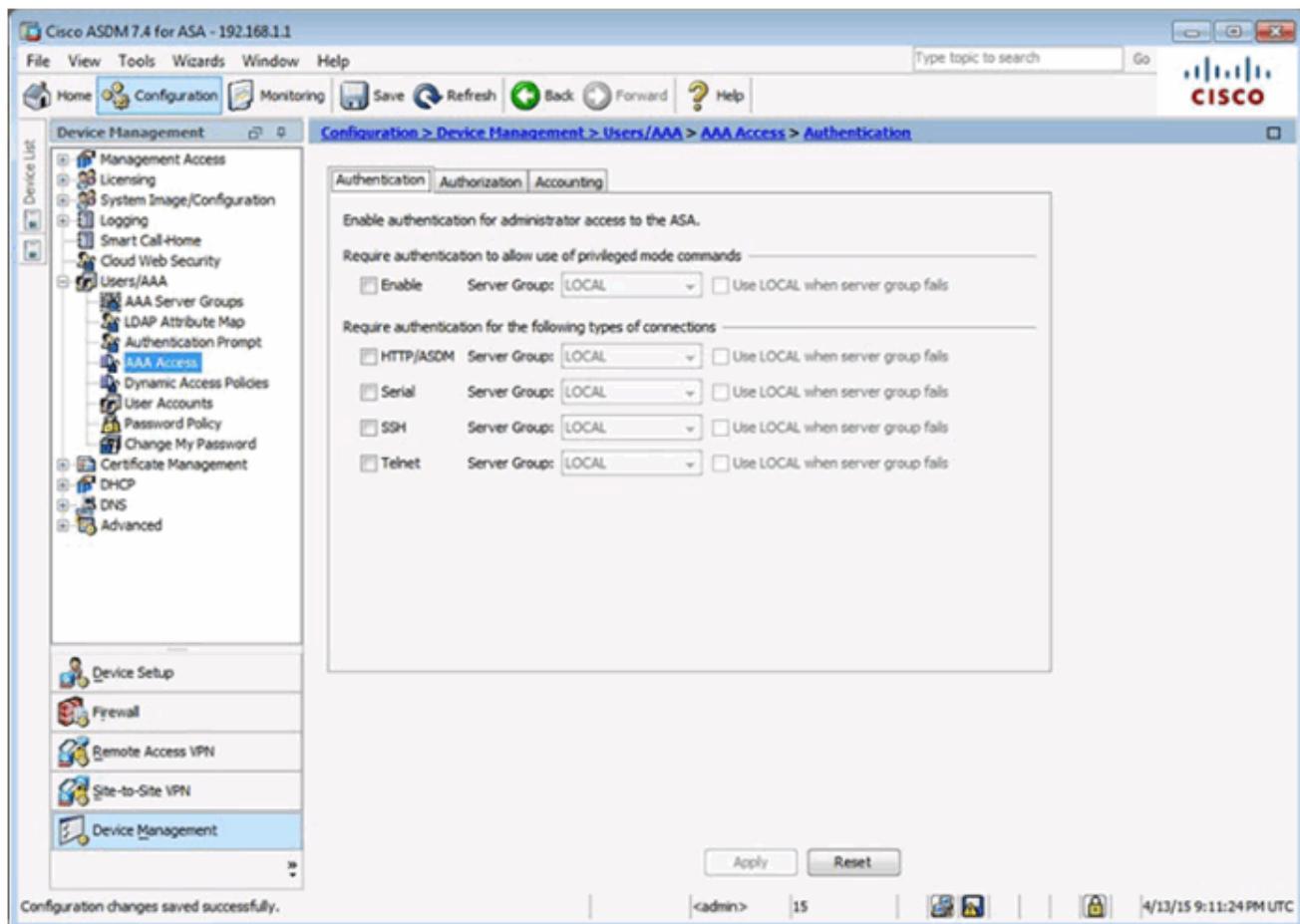
Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.2.3	dmz	10

Add Edit Delete Move Up Move Down Test



## AAA Access Page



## 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

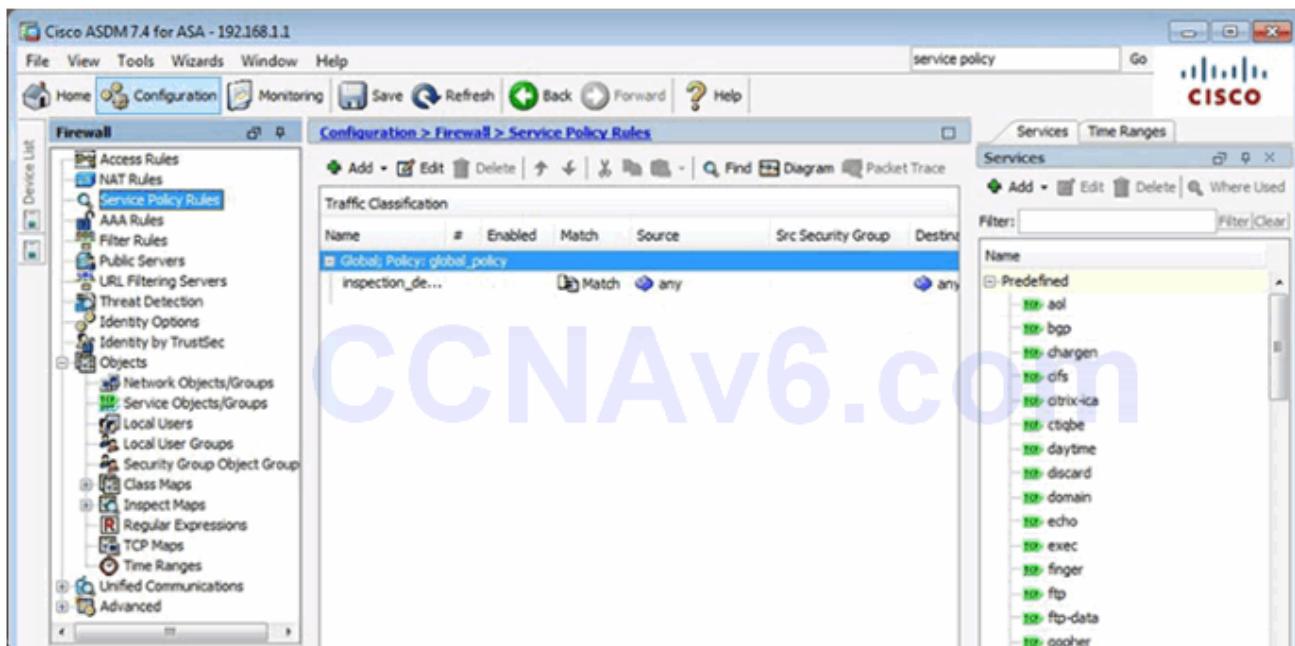
Enable   Server Group: RADIUS-SERVERS    Use LOCAL when server group fails

Require authentication for the following types of connections

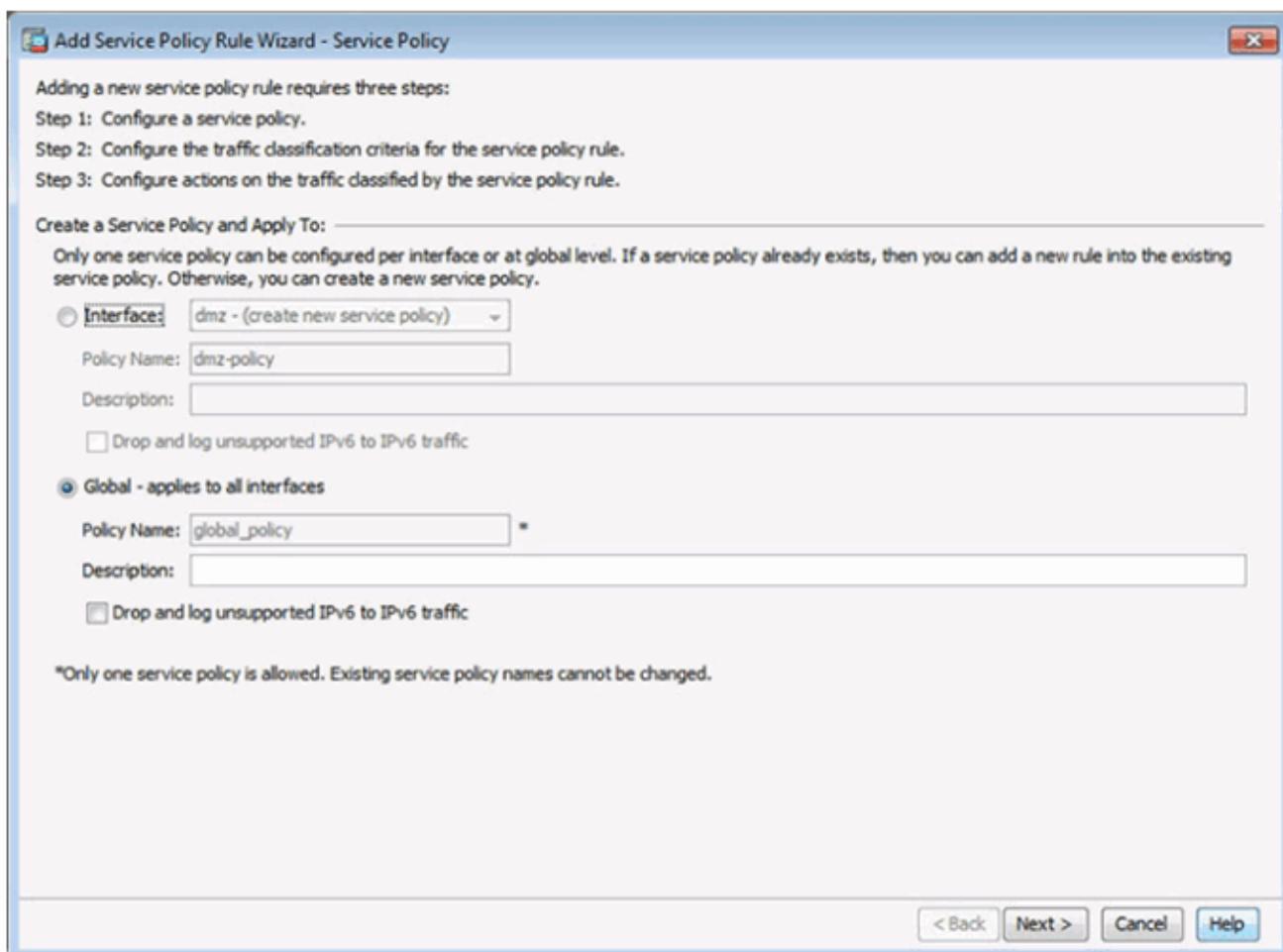
<input checked="" type="checkbox"/> HTTP/ASDM	Server Group: RADIUS-SERVERS	<input checked="" type="checkbox"/> Use LOCAL when server group fails
<input type="checkbox"/> Serial	Server Group: LOCAL	<input type="checkbox"/> Use LOCAL when server group fails
<input checked="" type="checkbox"/> SSH	Server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

## Configuring a Service Policy Using ASDM

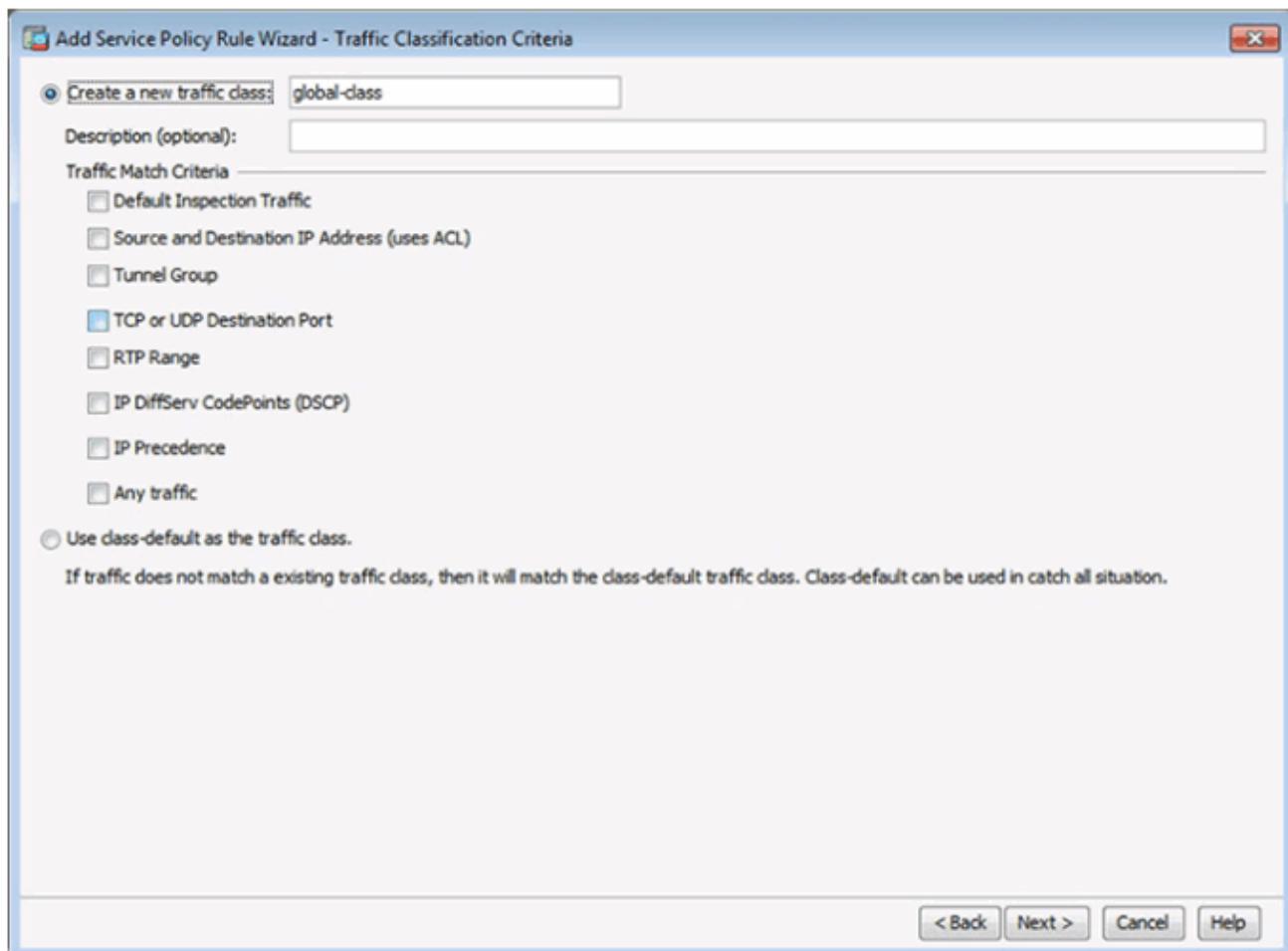
### Service Policy in ASDM



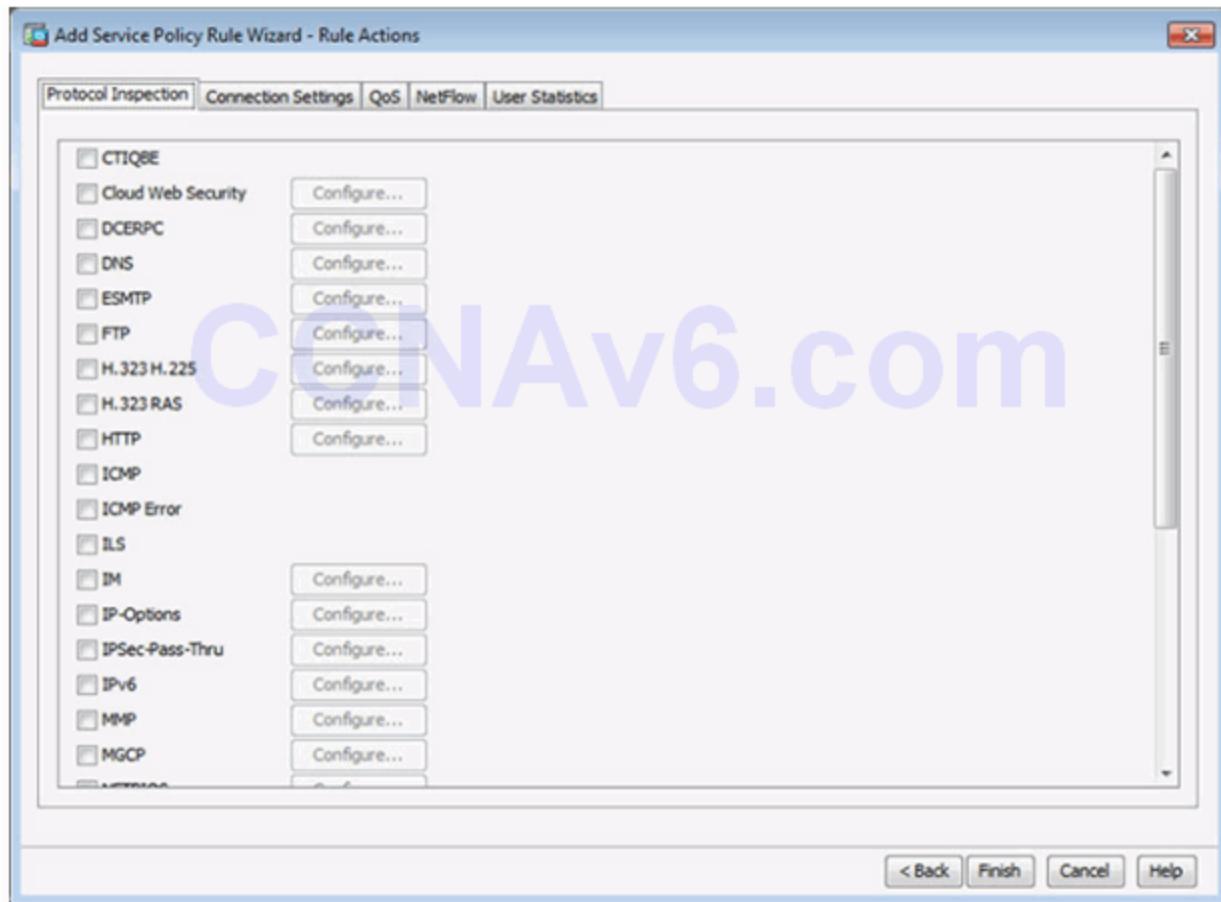
## Configure a Service Policy



## Configure Traffic Classification Criteria



## Configure Actions



## Section 10.2: ASA VPN Configuration

---

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

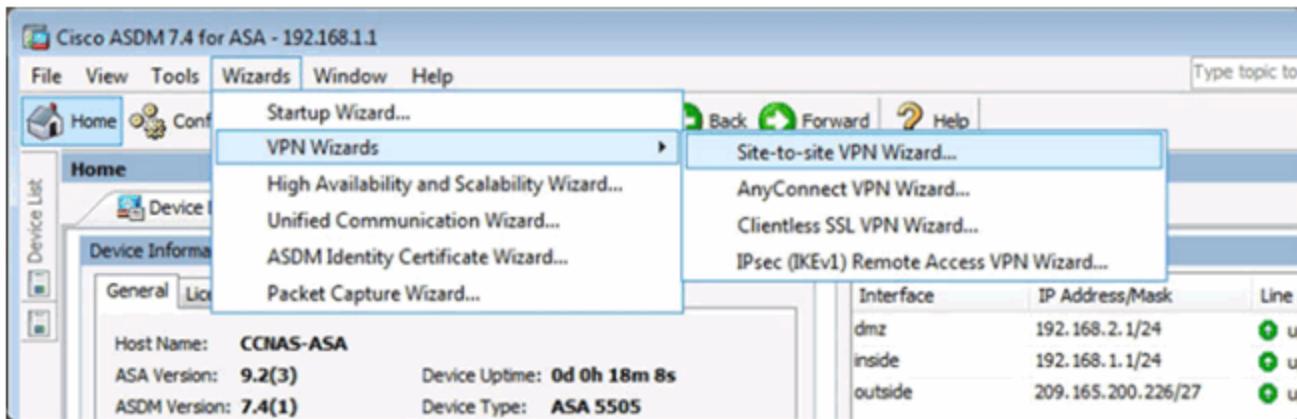
- Explain how the ASA supports site-to-site VPNs.
- Configure remote-access VPNs on an ASA.
- Configure remote-access VPN support using a clientless SSL VPN.
- Configure remote-access VPN support using Cisco AnyConnect.

### Topic 10.2.1: Site-to-Site VPNs

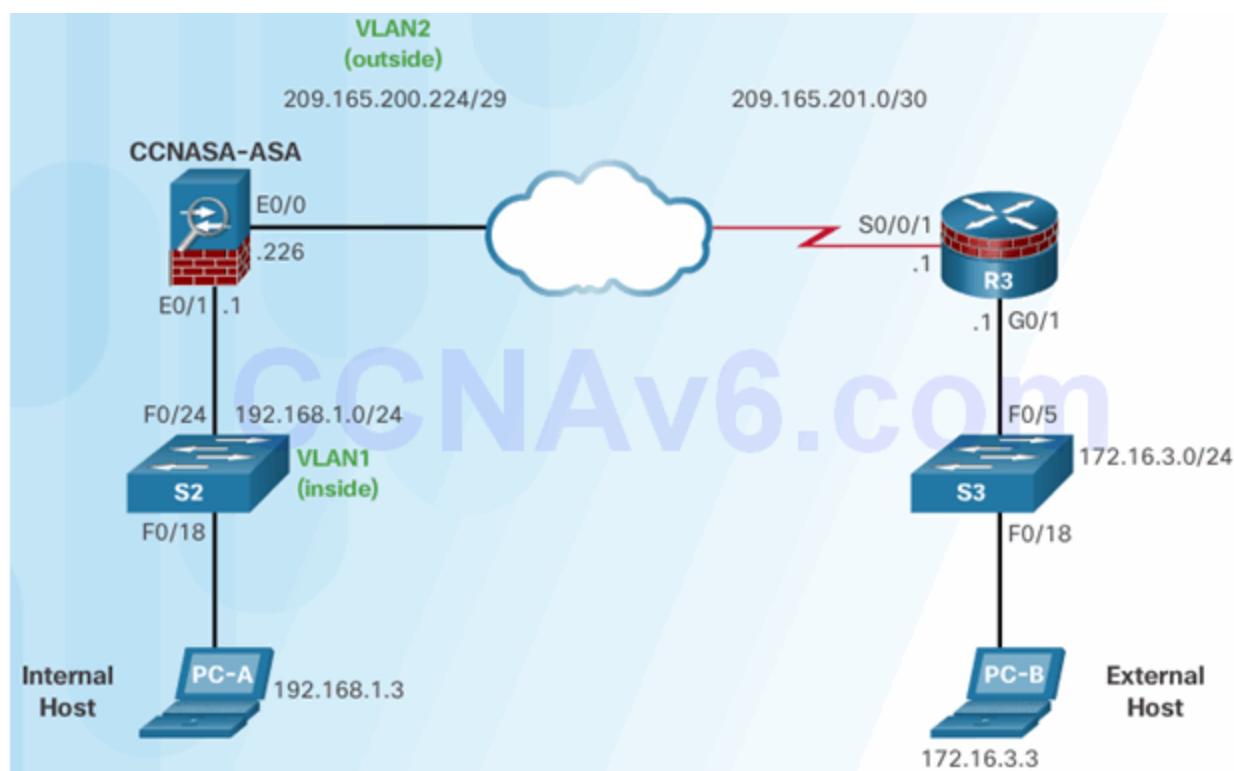
---

#### 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)#

```

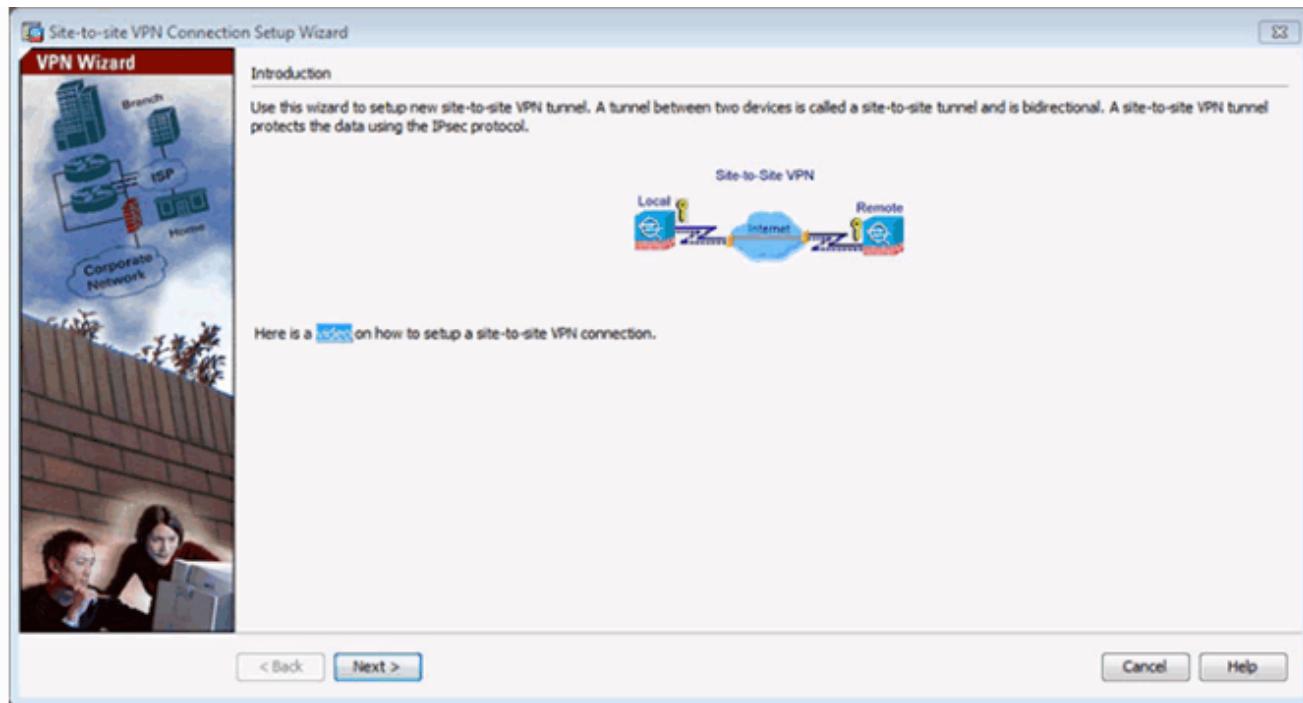
## Configuring the ASA Site-to-Site VPNs Using ASDM

### Basic ISR Configuration

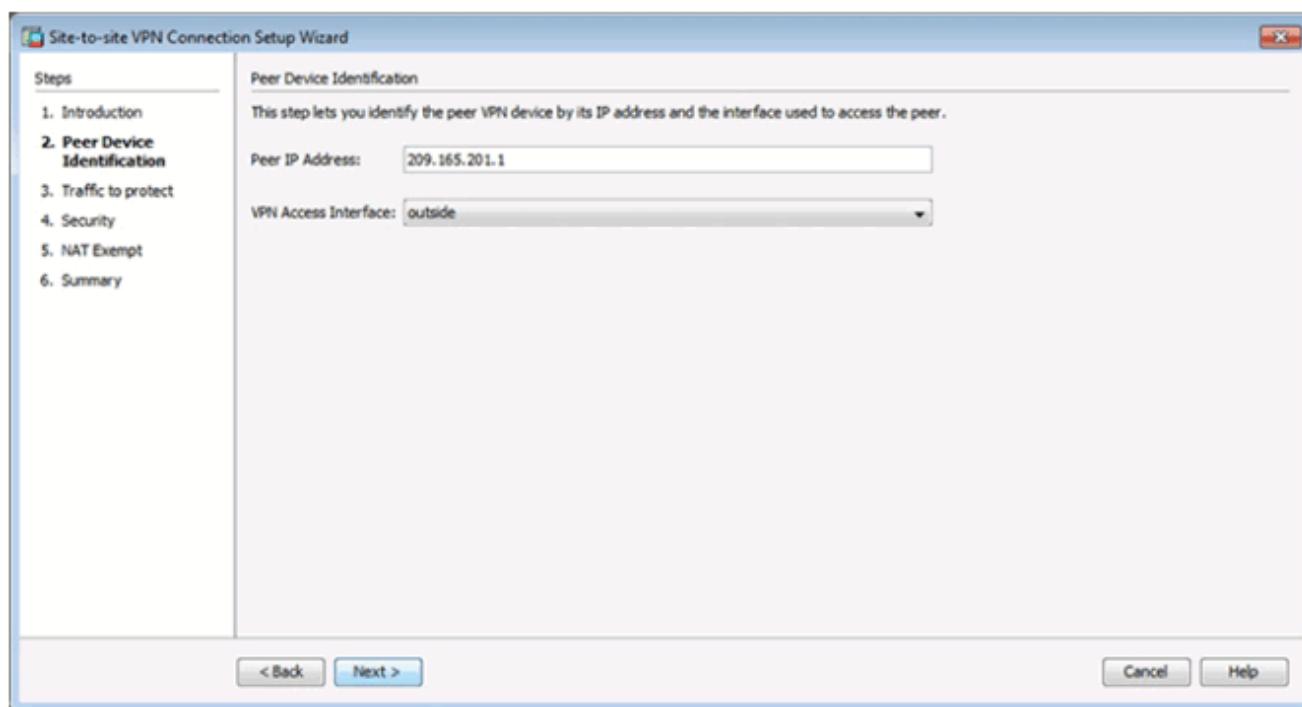
```
CNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface 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)#

```

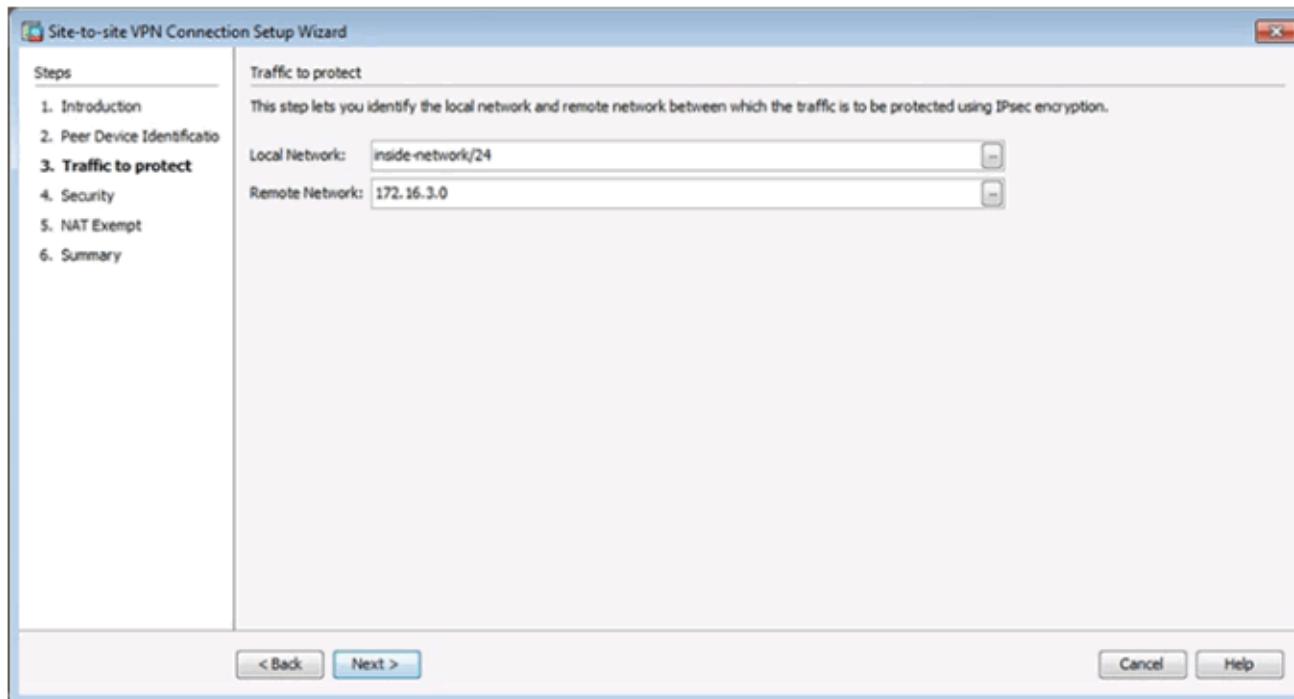
## Introduction Window



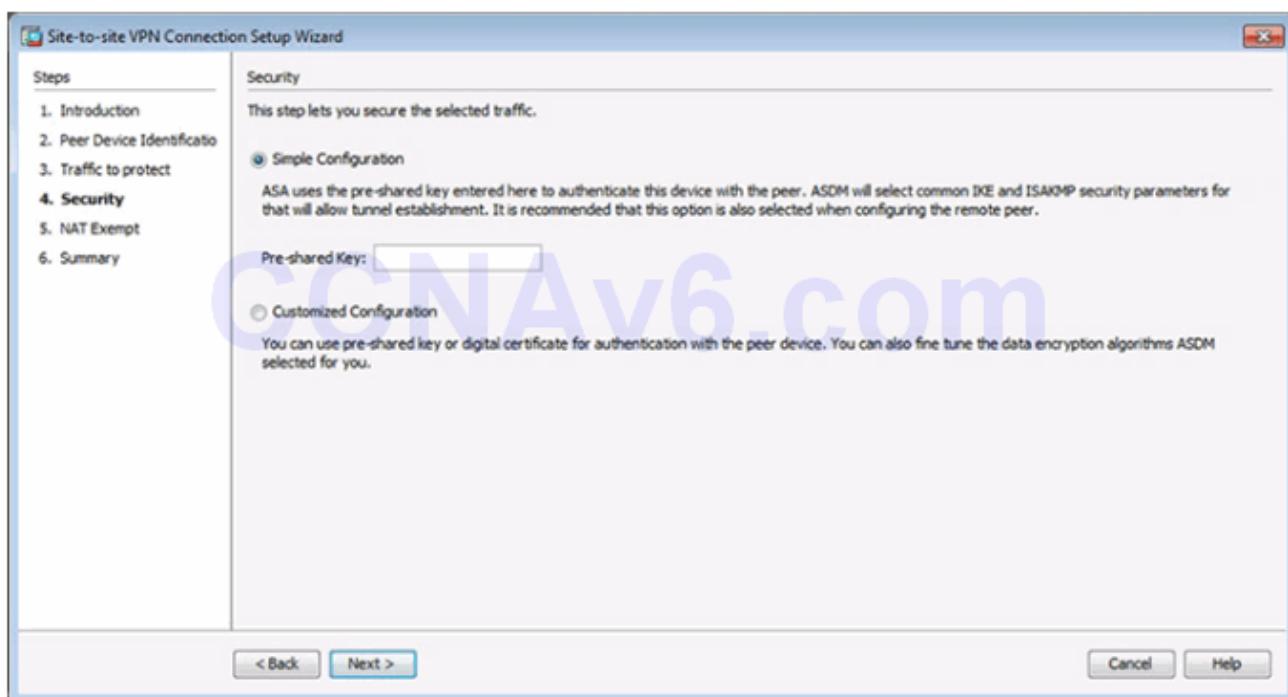
## Peer Device Identification Window



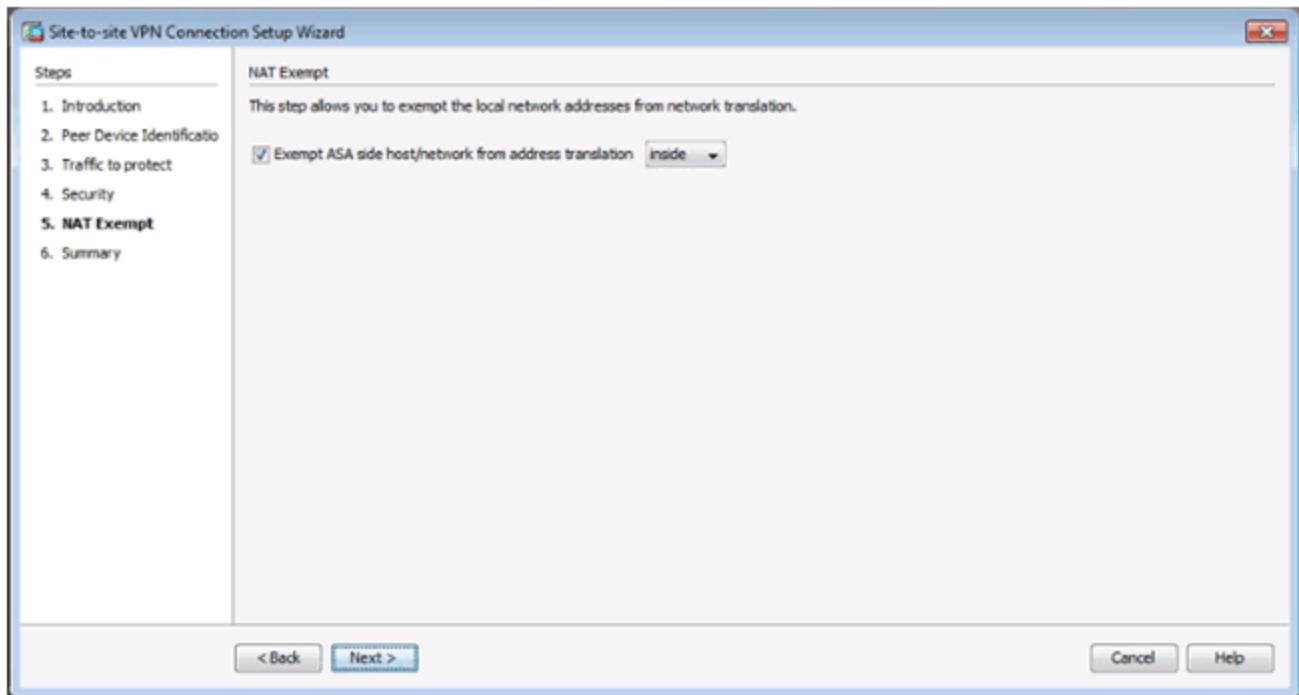
## Traffic to Protect Window



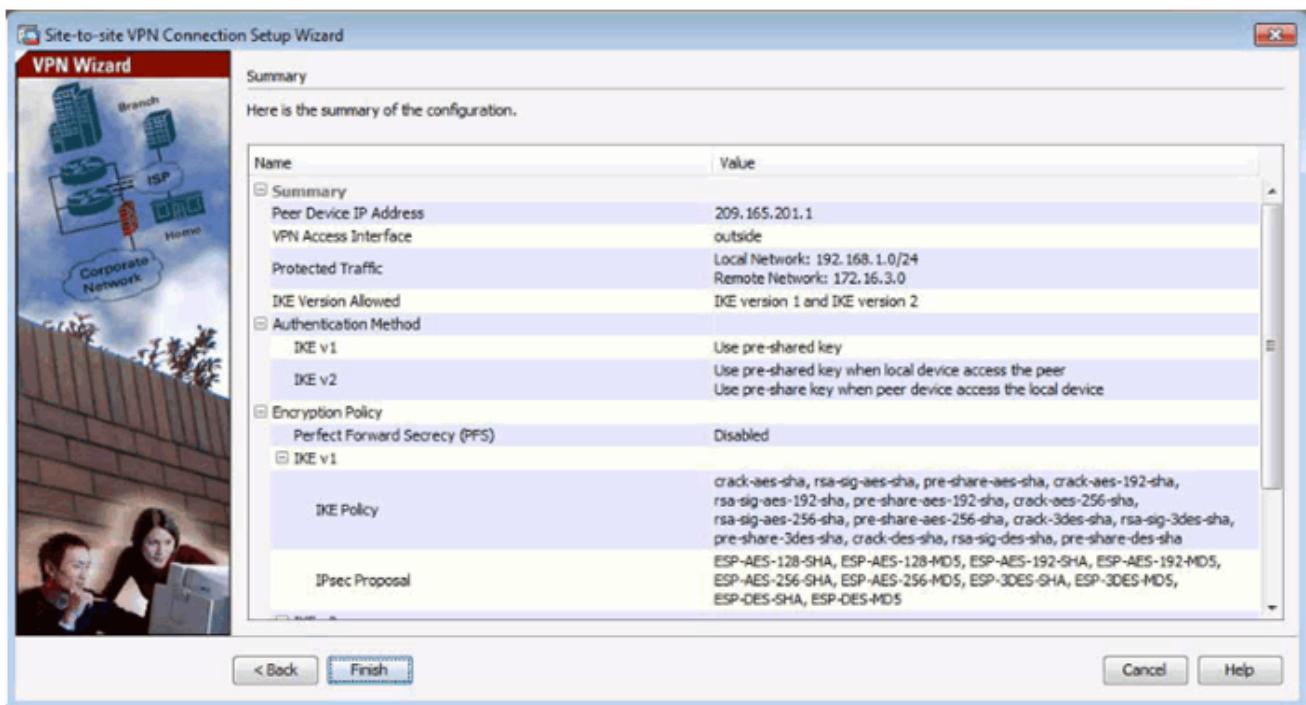
## Security Window



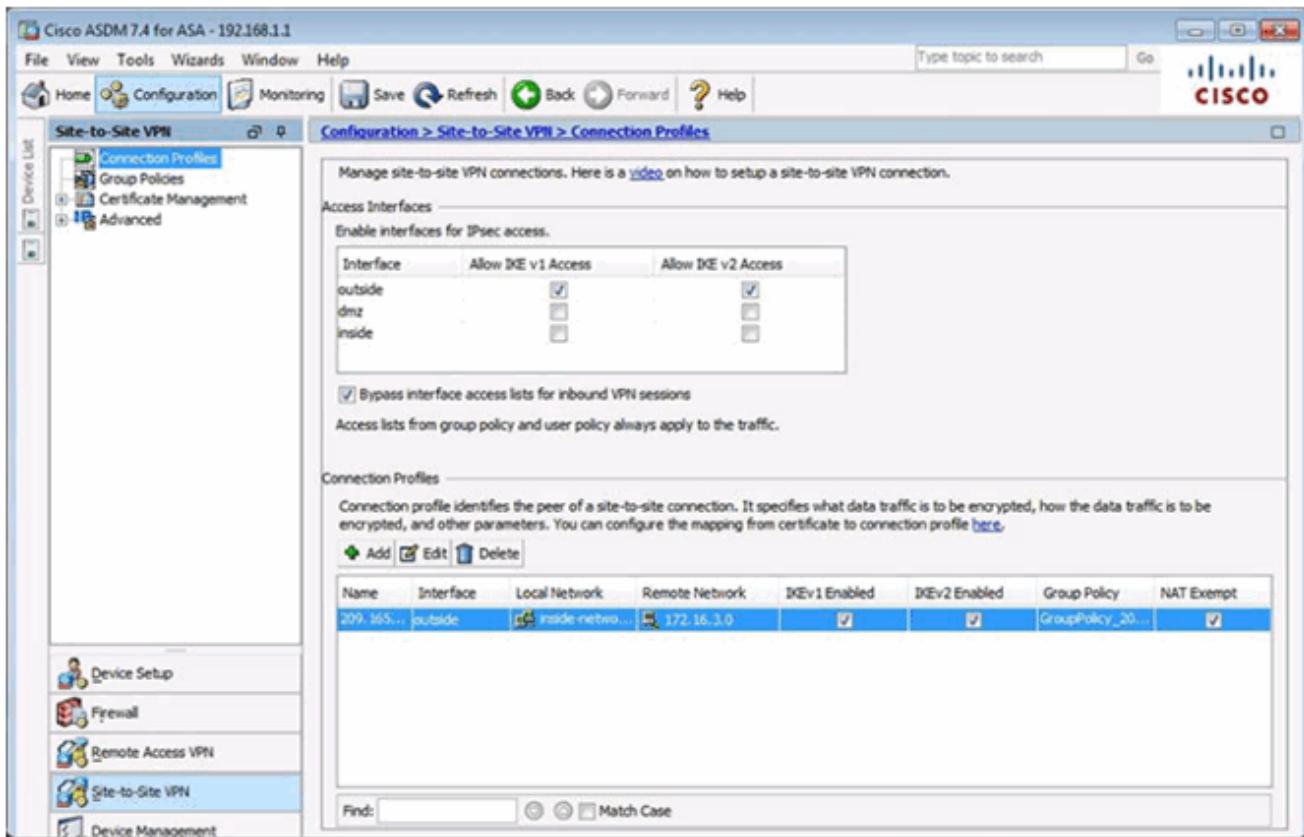
## NAT Exempt Window



## 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

```
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>
```

## Monitoring the VPN Tunnel

The screenshot shows the Cisco ASDM 7.4 for ASA interface. The left sidebar has a tree view with 'VPN Statistics' selected under 'VPN'. The main pane title is 'Monitoring > VPN > VPN Statistics > Sessions'. It lists two sessions:

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	1	1	1
IKEv1 IPsec	1	1	1	1

Below the table, there's a 'Filter By' dropdown set to 'IPsec Site-to-Site' and a 'Logout' button. A note says 'To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.' At the bottom, it says 'Data Refreshed Successfully.', 'Last Updated: 4/21/15 3:24:15 PM', and '4/21/15 10:23:17 PM UTC'.

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

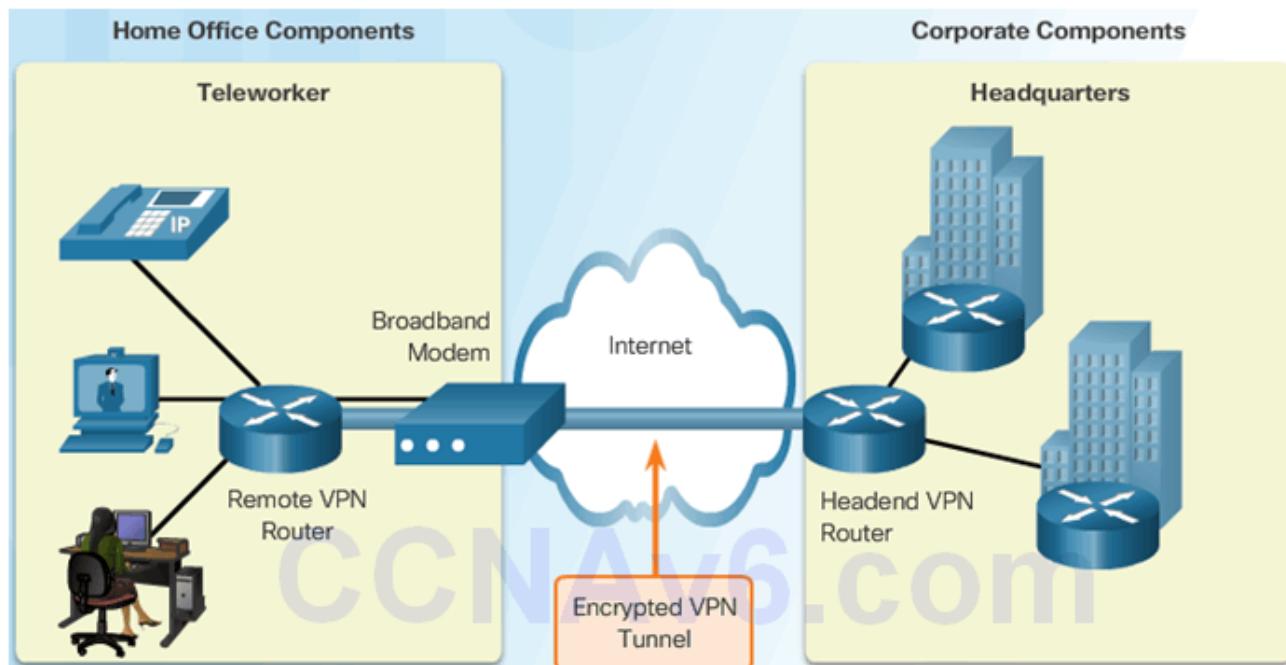
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=64ms TTL=127
Reply from 192.168.1.3: bytes=32 time=65ms TTL=127
Reply from 192.168.1.3: bytes=32 time=67ms TTL=127
Reply from 192.168.1.3: bytes=32 time=69ms TTL=127

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

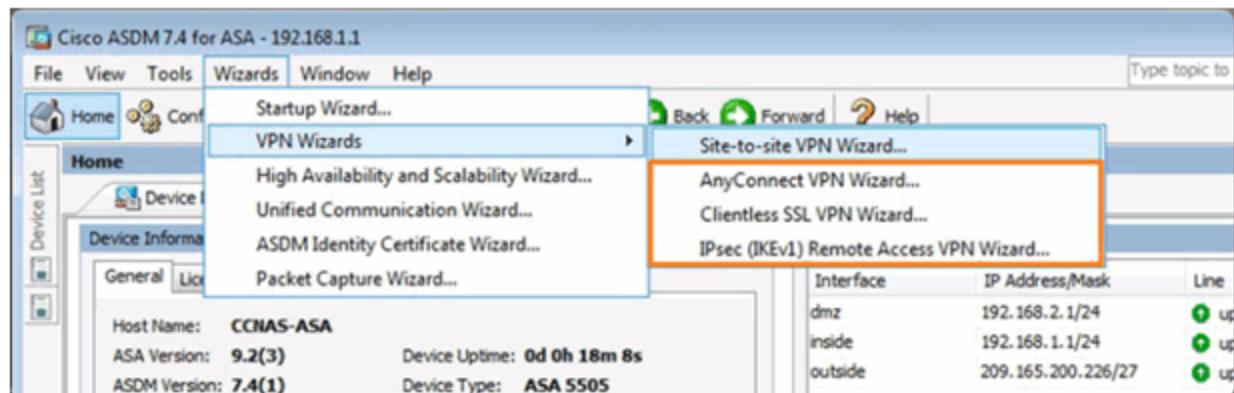
SSL

## Comparing IPsec and SSL

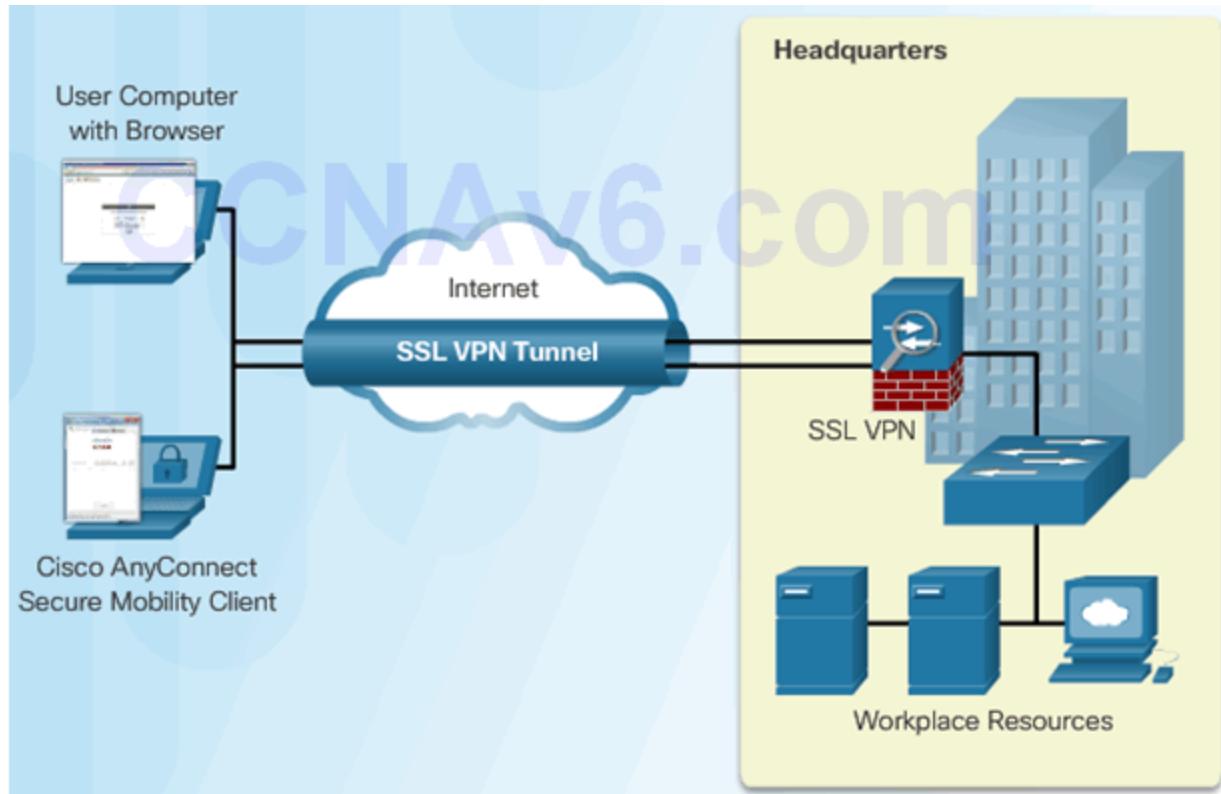
	IPSec	SSL
Applications supported	<b>Extensive</b> - all IP-based applications are supported.	<b>Limited</b> - only web-based applications and file sharing are supported.
Authentication strength	<b>Strong</b> - using two-way authentication with shared keys or digital certificates.	<b>Moderate</b> - using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

## ASA SSL VPNs

### Remote Access VPN Wizards

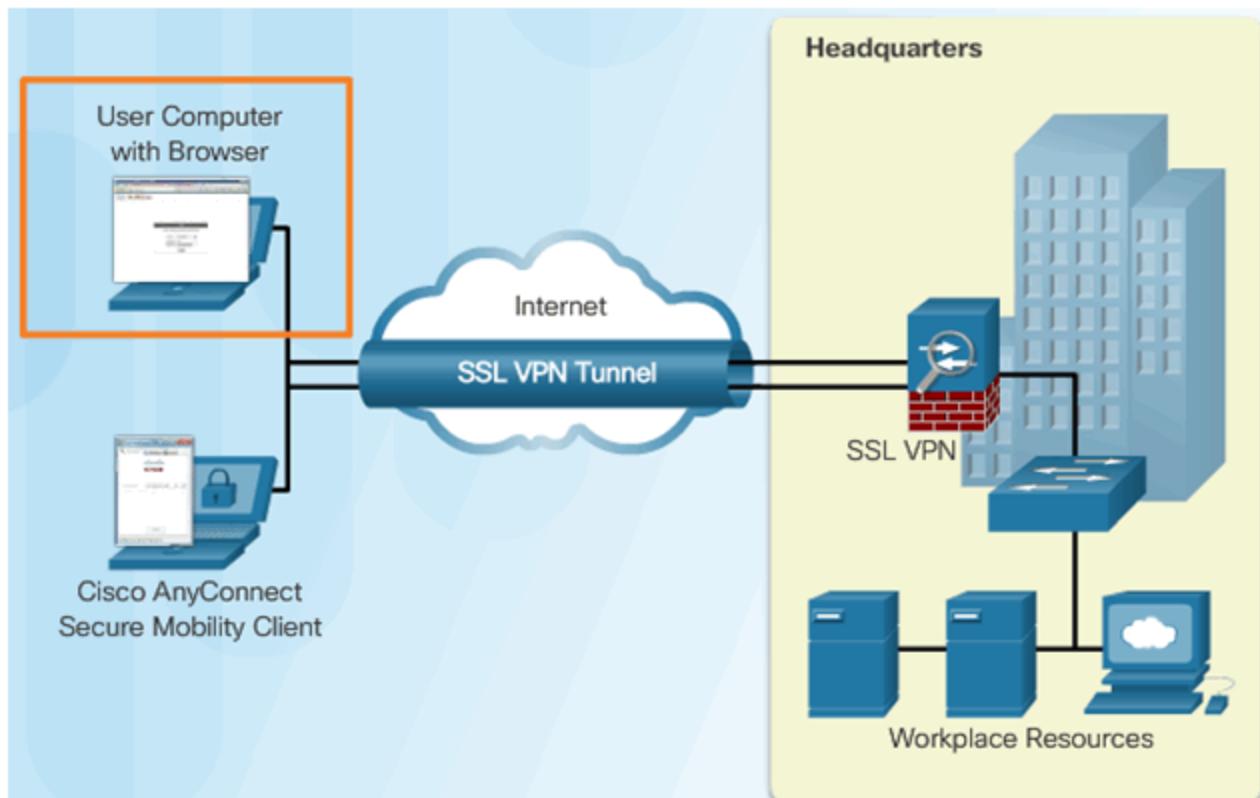


### Cisco ASA SSL Remote Access VPN Solutions

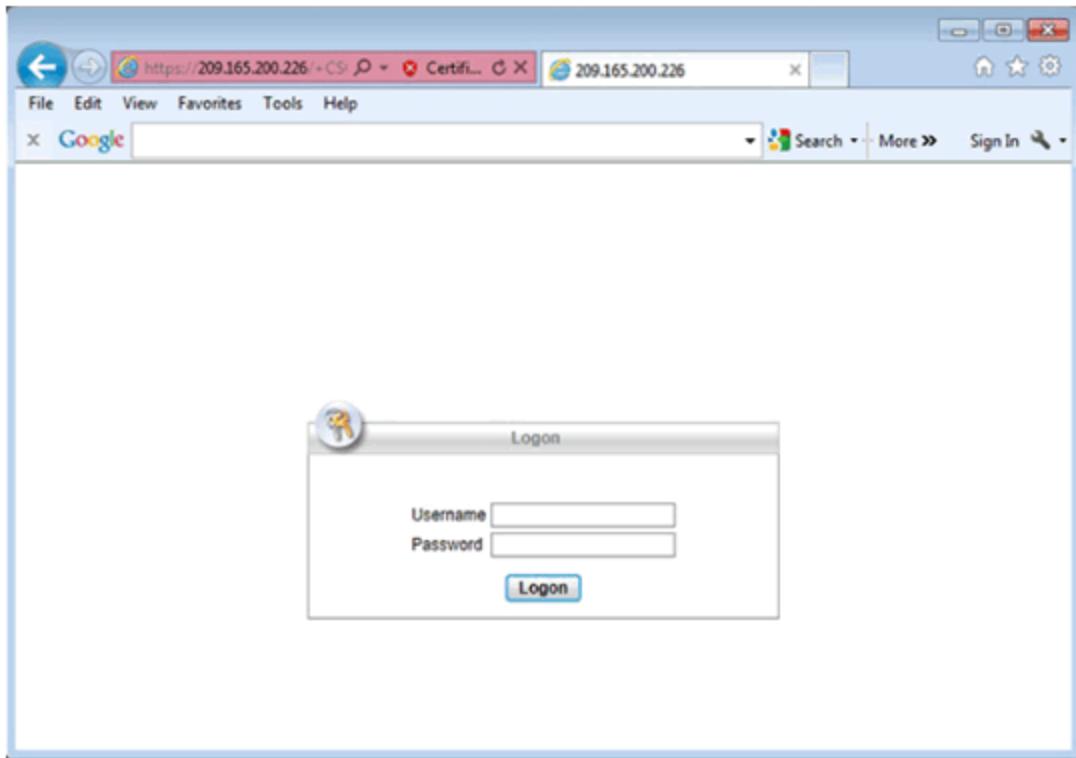


## Clientless SSL VPN Solution

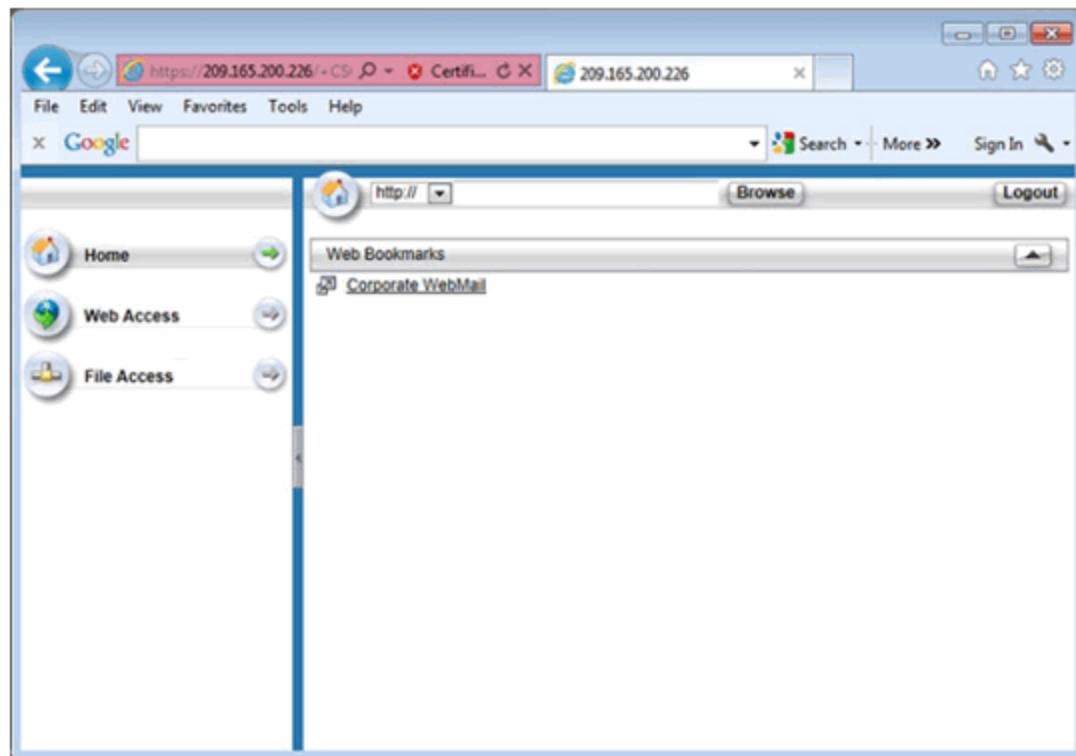
Cisco ASA Clientless SSL VPN Deployment



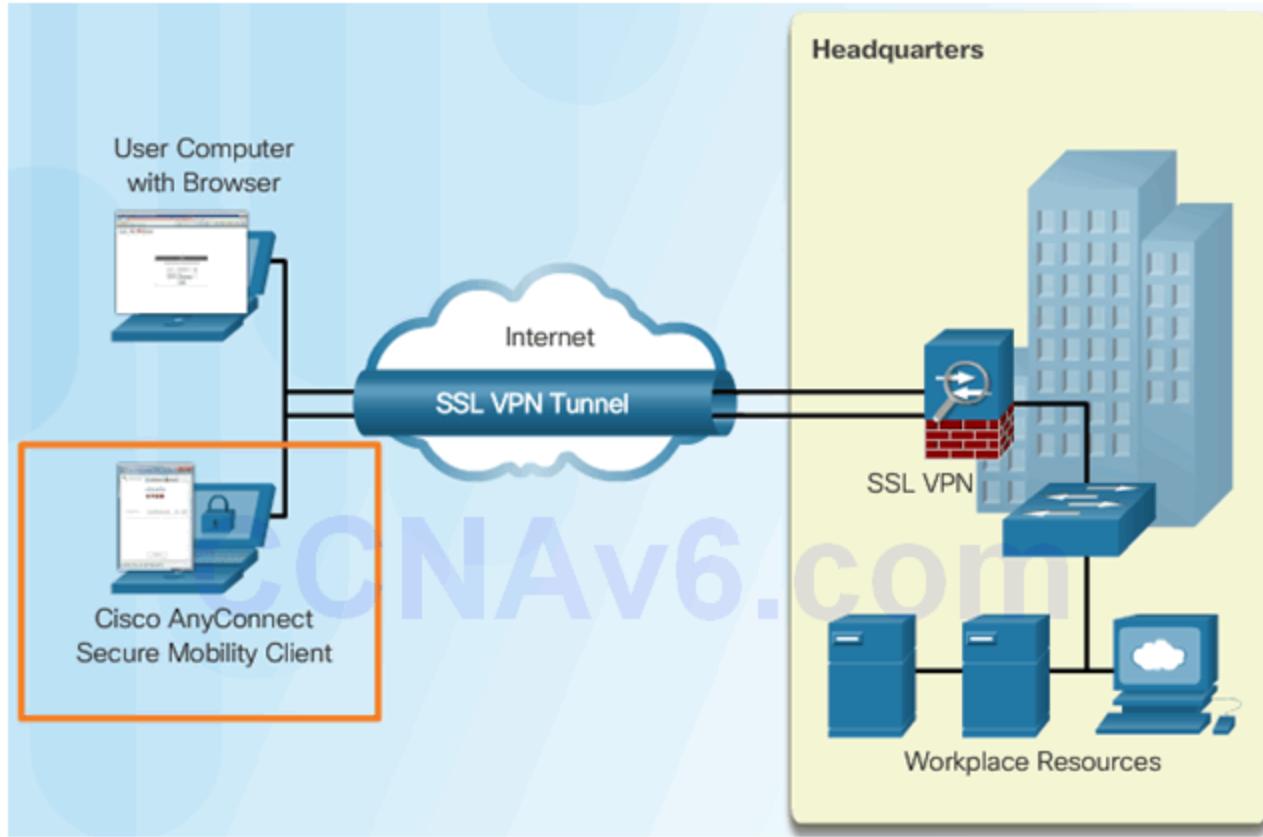
## Clientless Login Web page



## Web Portal Home Page

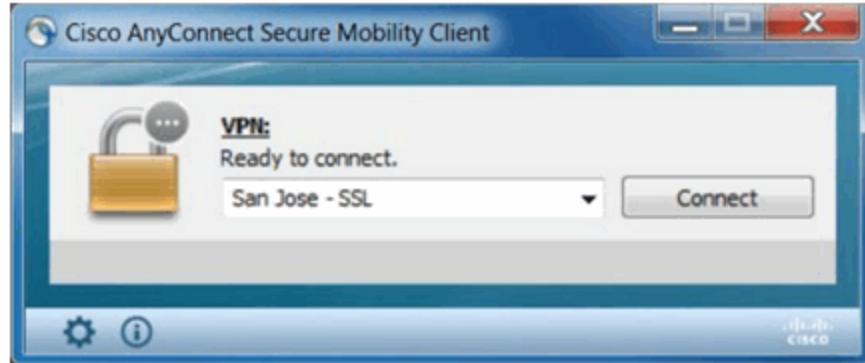


## Client-Based SSL VPN Solution

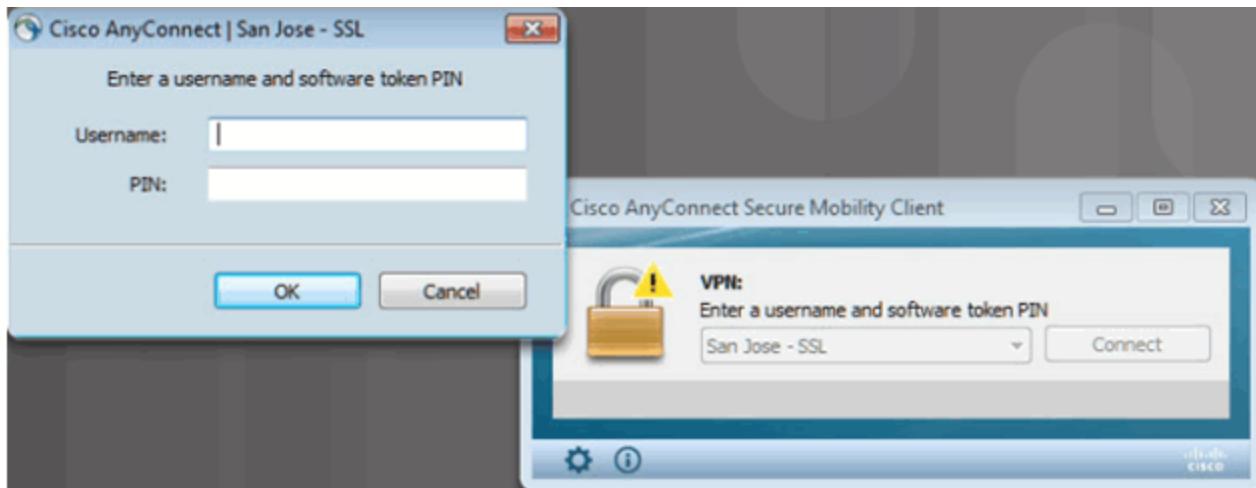


## Cisco AnyConnect Secure Mobility Client

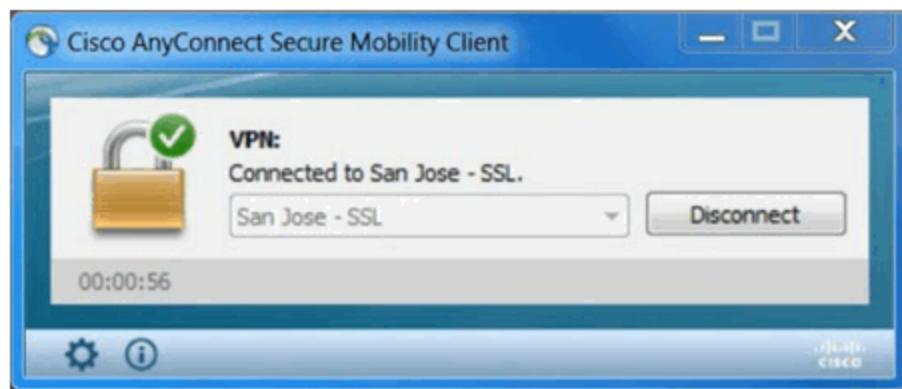
AnyConnect Connection Window



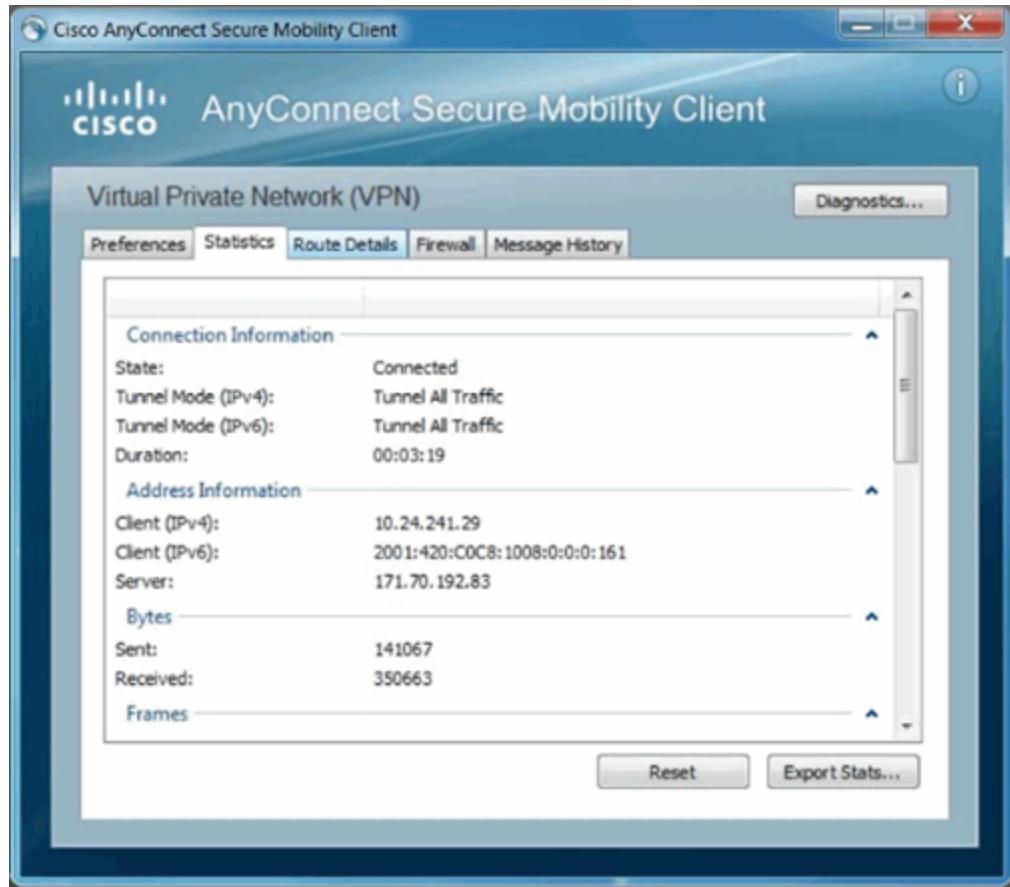
AnyConnect Authenticate Window



AnyConnect Authenticated Window



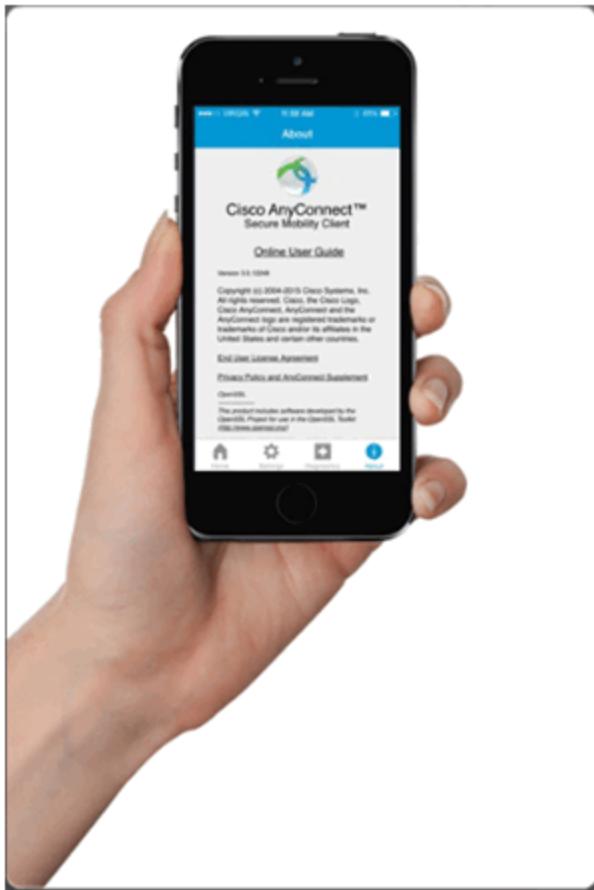
AnyConnect Statistics Window



## AnyConnect for Mobile Devices

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

- iOS
- Android
- BlackBerry
- Windows Mobile



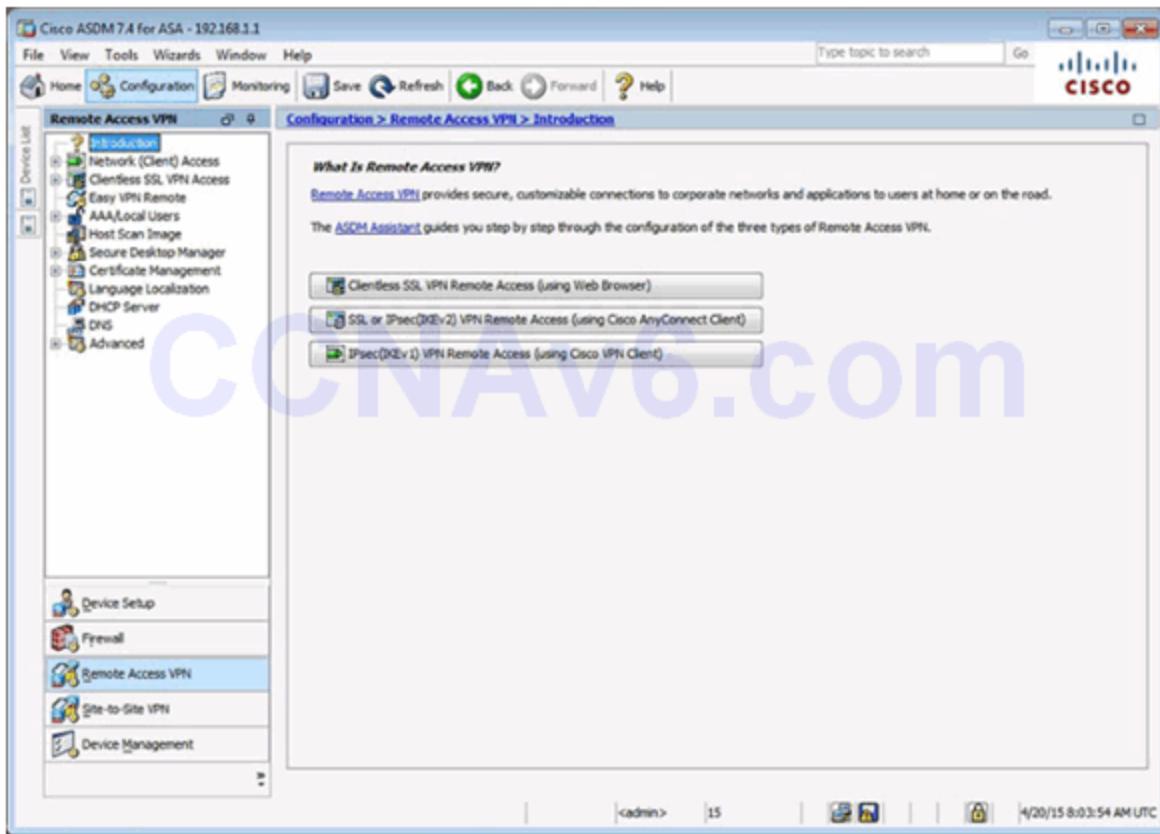
## Topic 10.2.3: Configuring Clientless SSL VPN

---

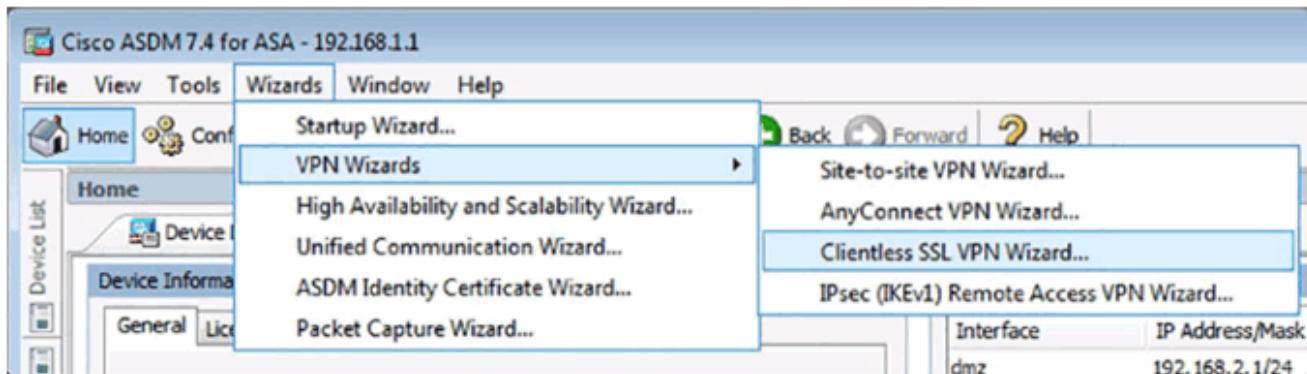
### Configuring Clientless SSL VPN on an ASA

---

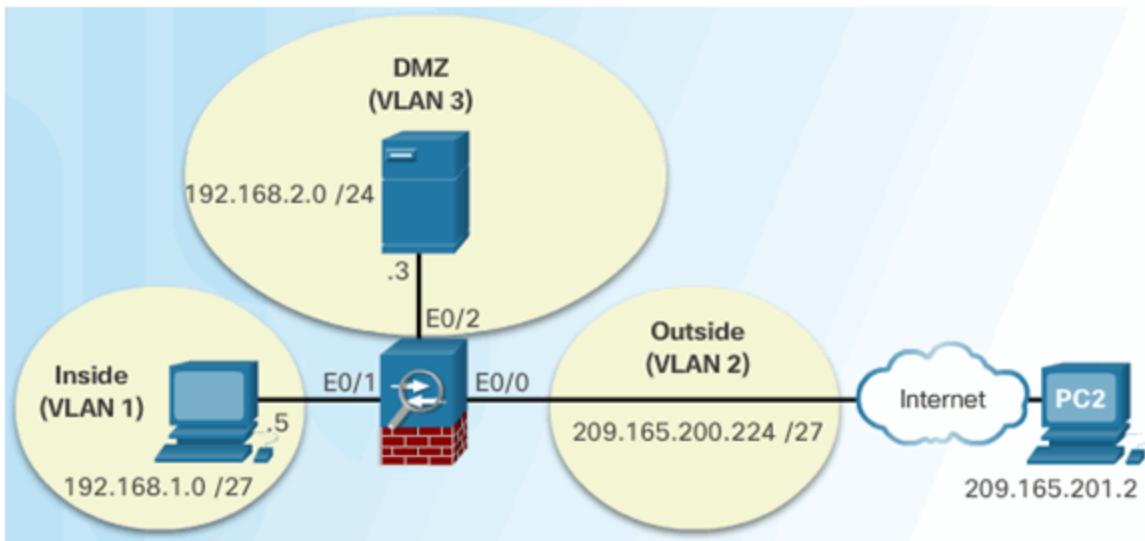
ASDM Assistant



## Clientless VPN Wizard

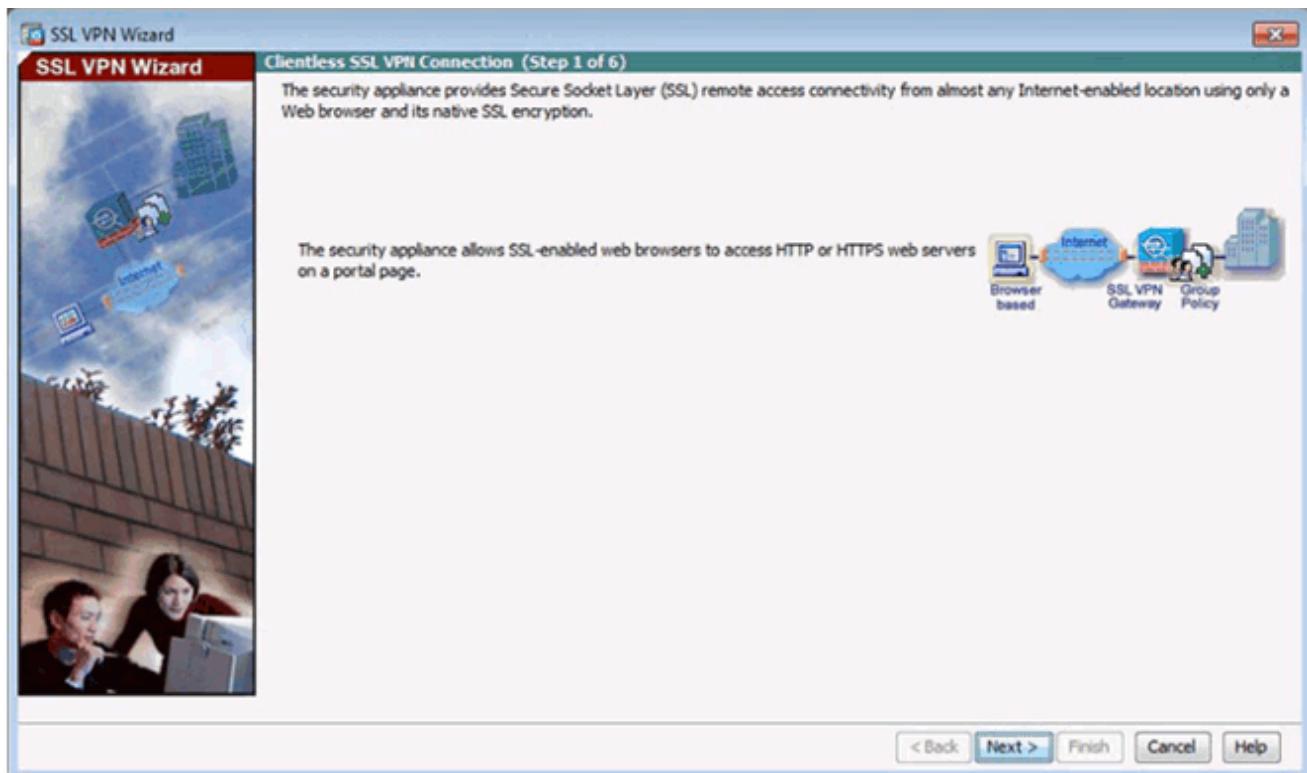


## Sample Clientless VPN Topology

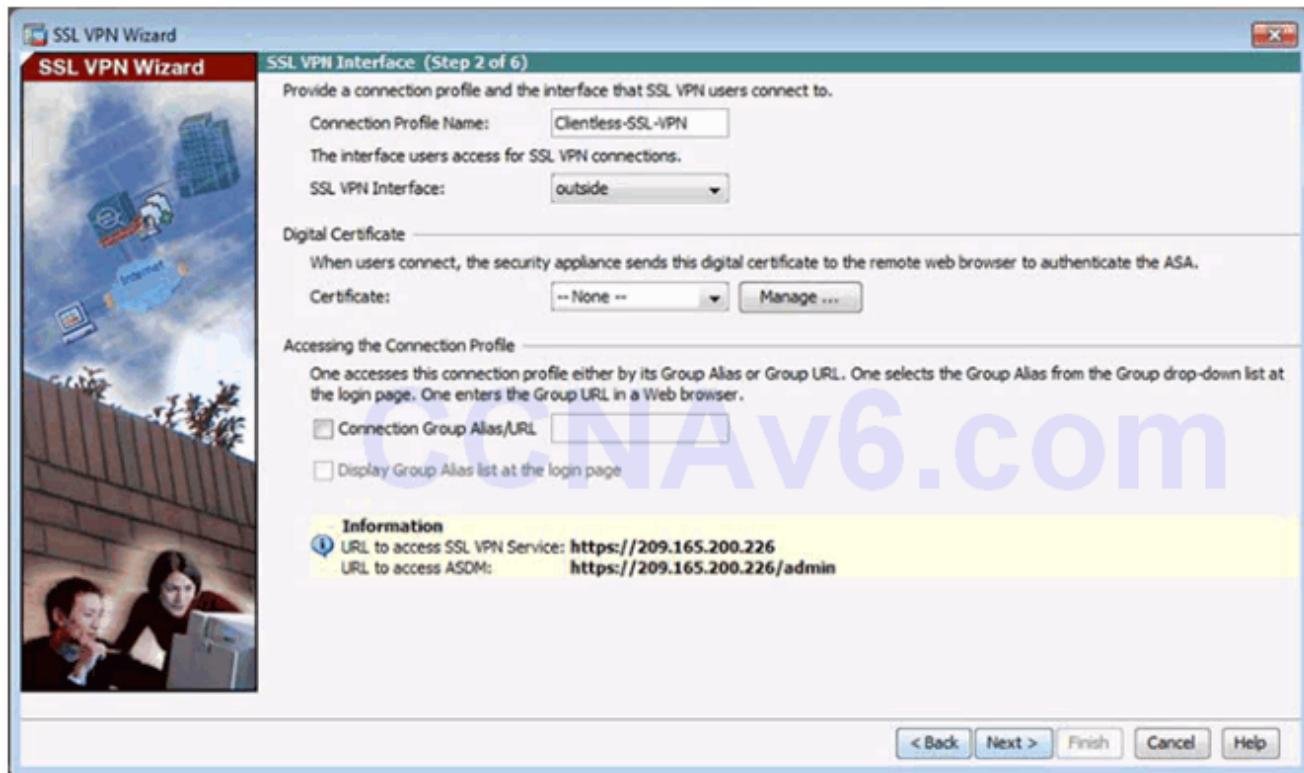


## Clientless SSL VPN

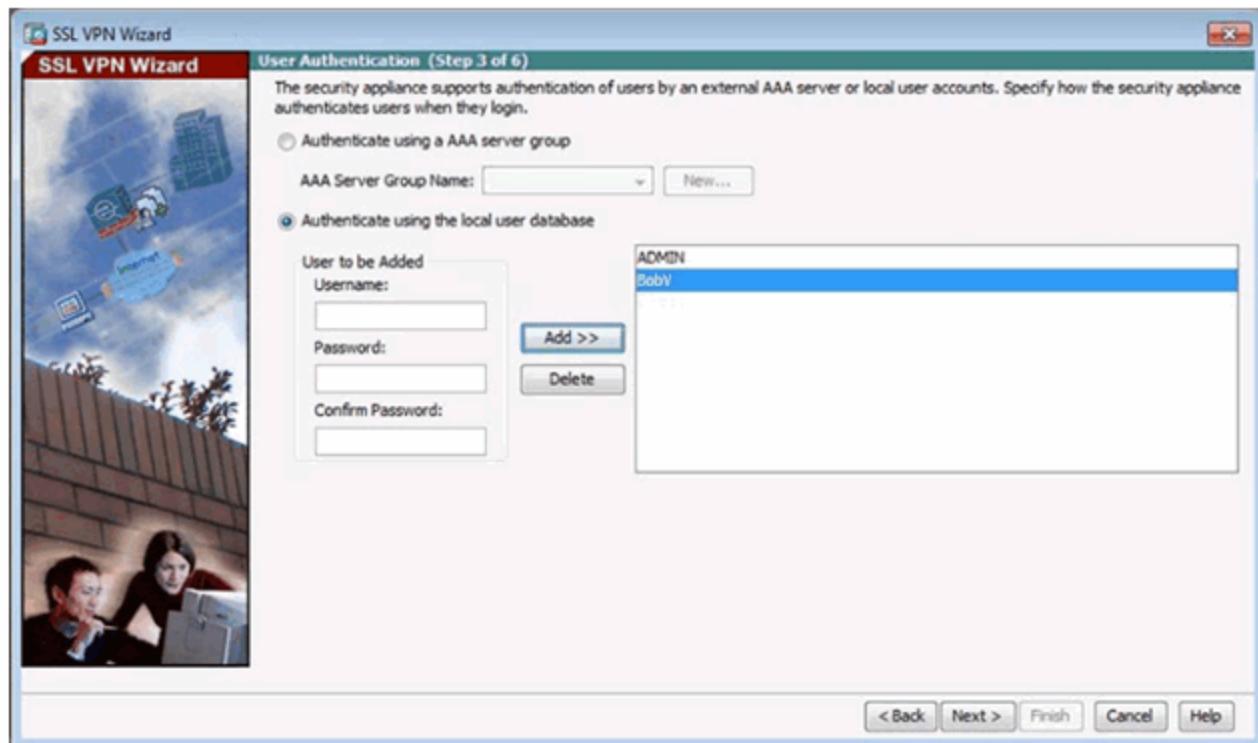
### Clientless SSL VPN Introduction Window



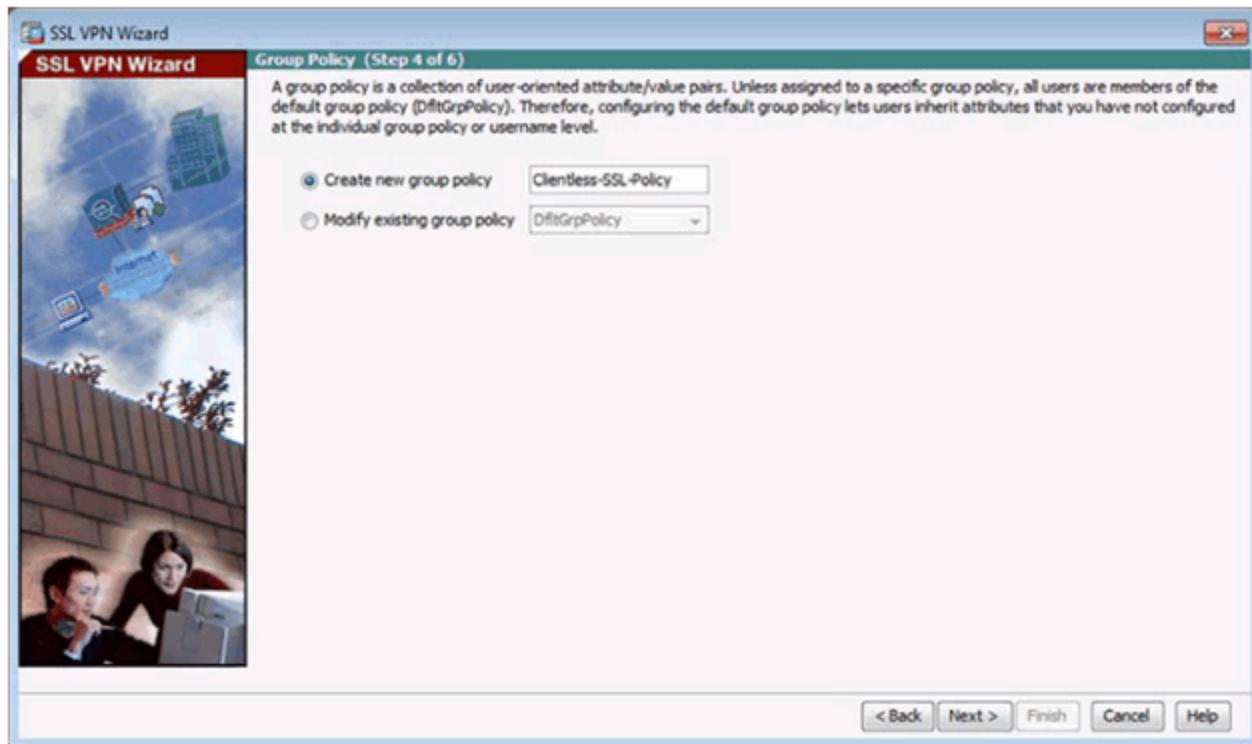
### SSL VPN Interface Window



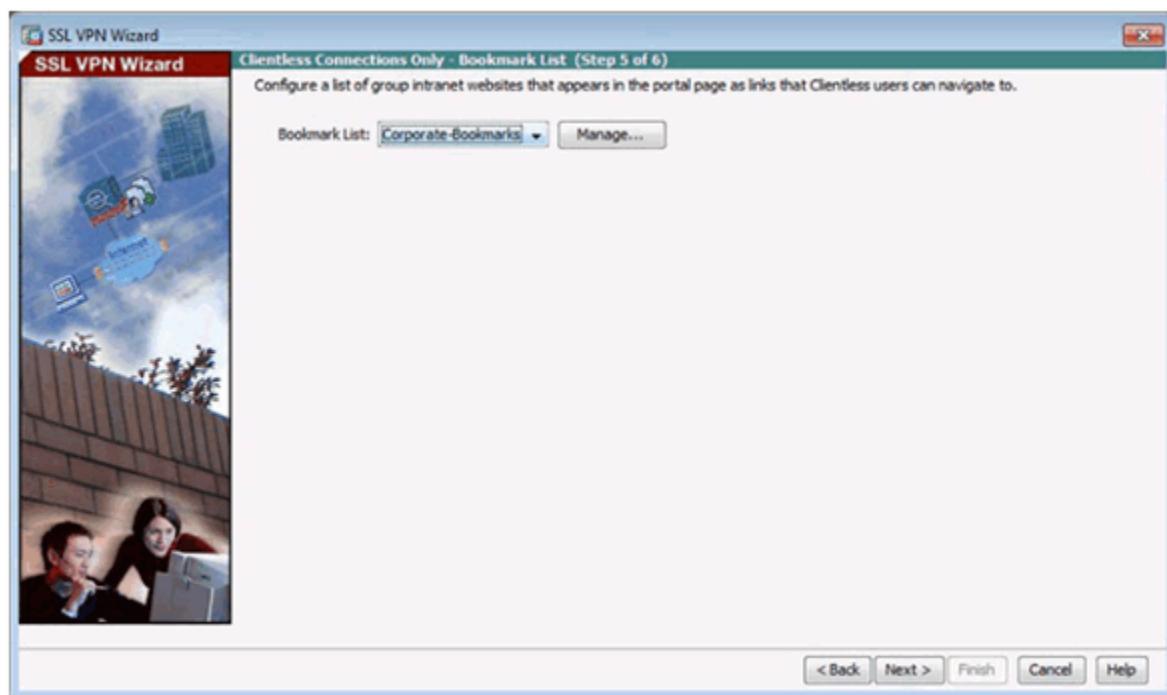
User Authentication Window



Group Policy Window



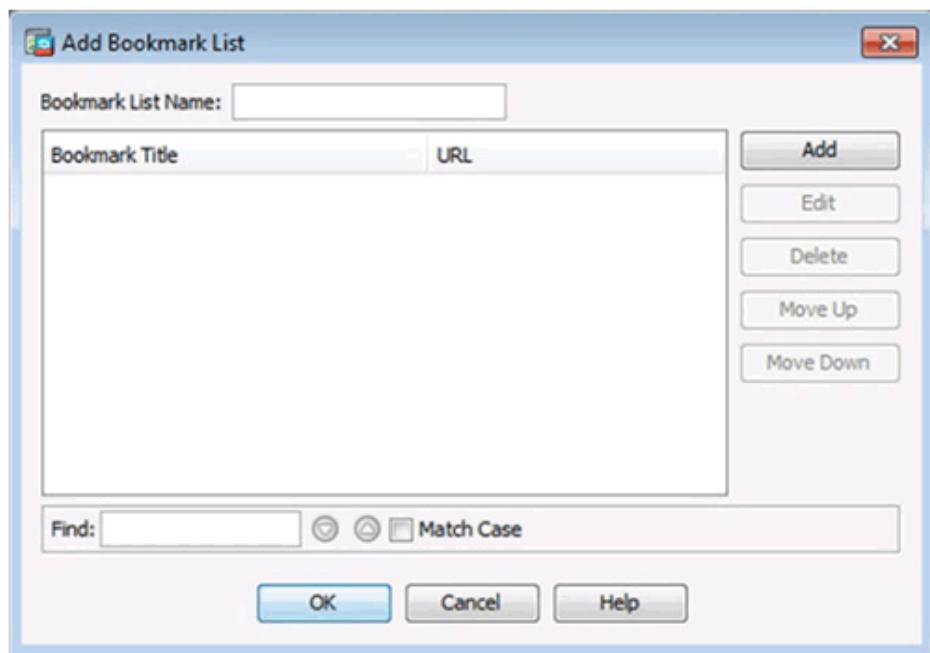
Bookmark List Window



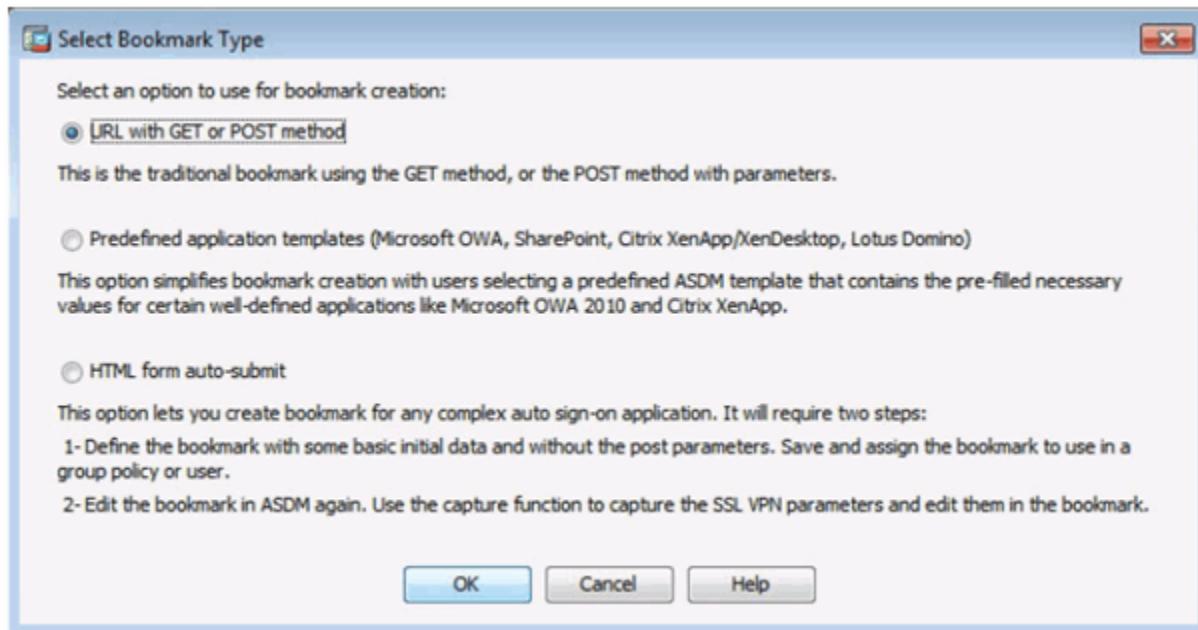
Configure GUI Customization Objects Window



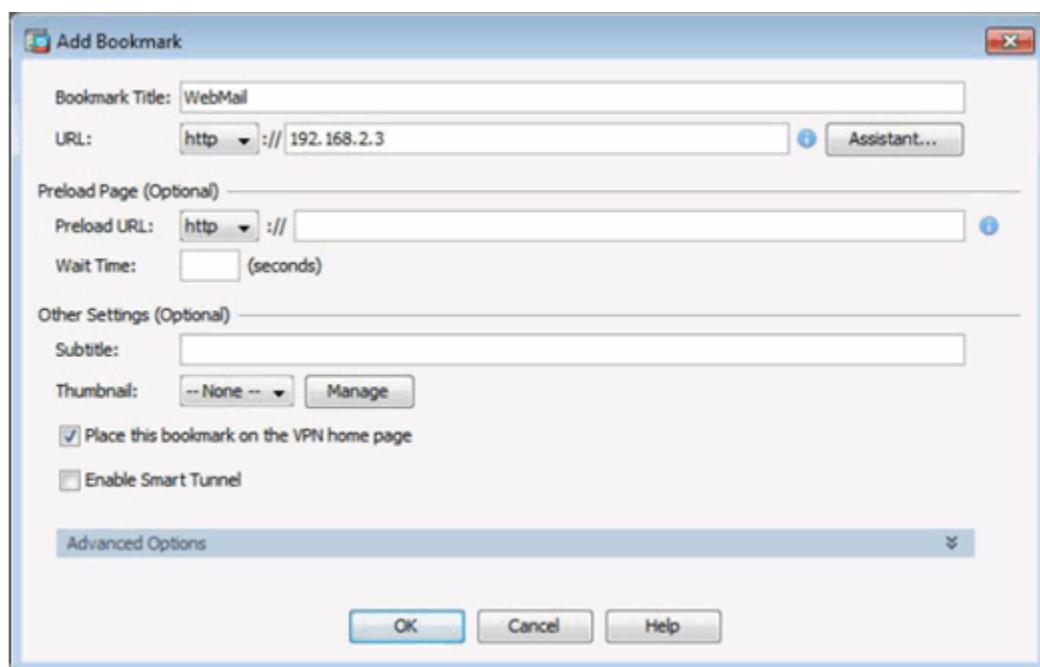
Add Bookmark List Window



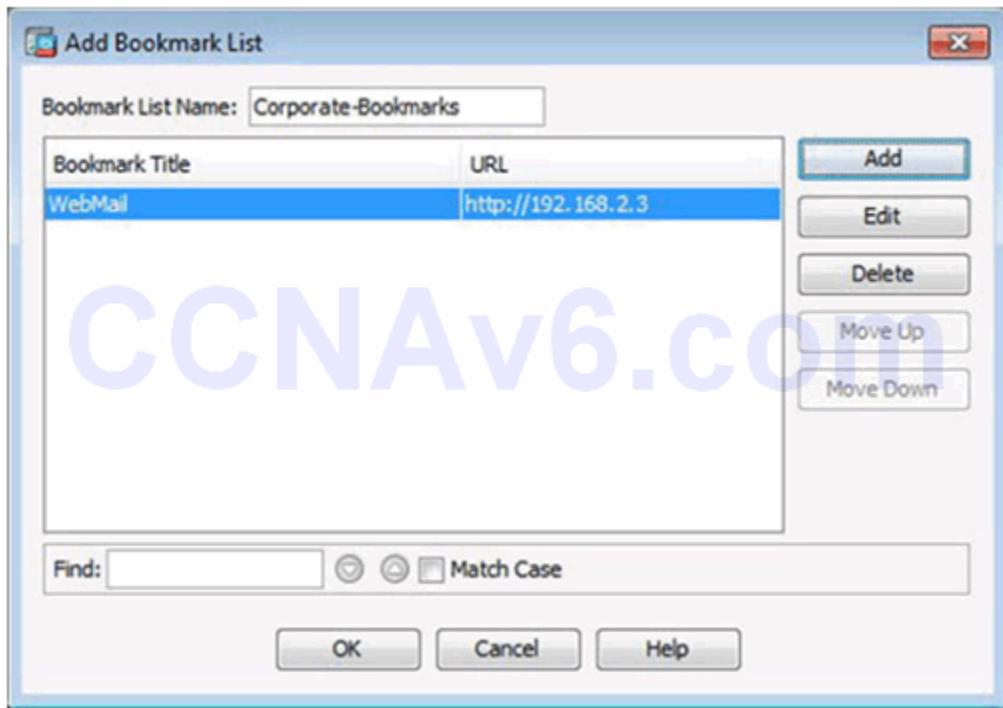
Select Bookmark Type Window



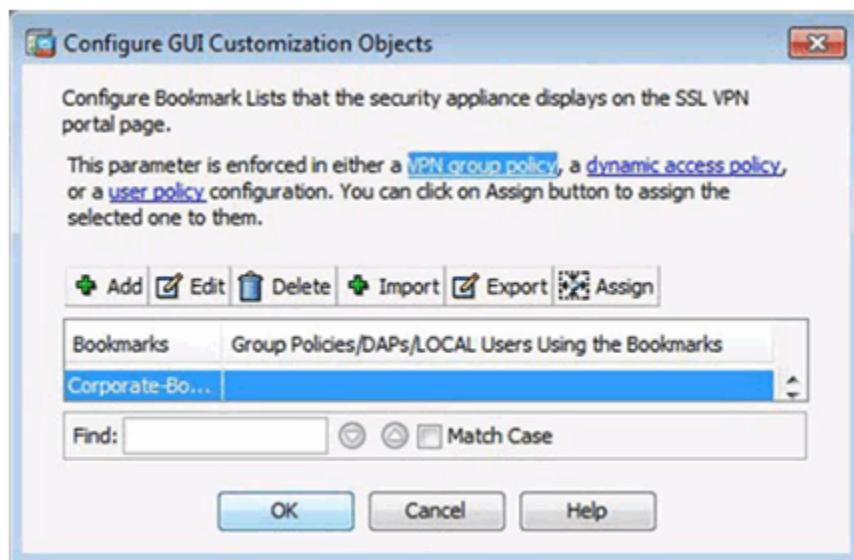
## Add Bookmark Window



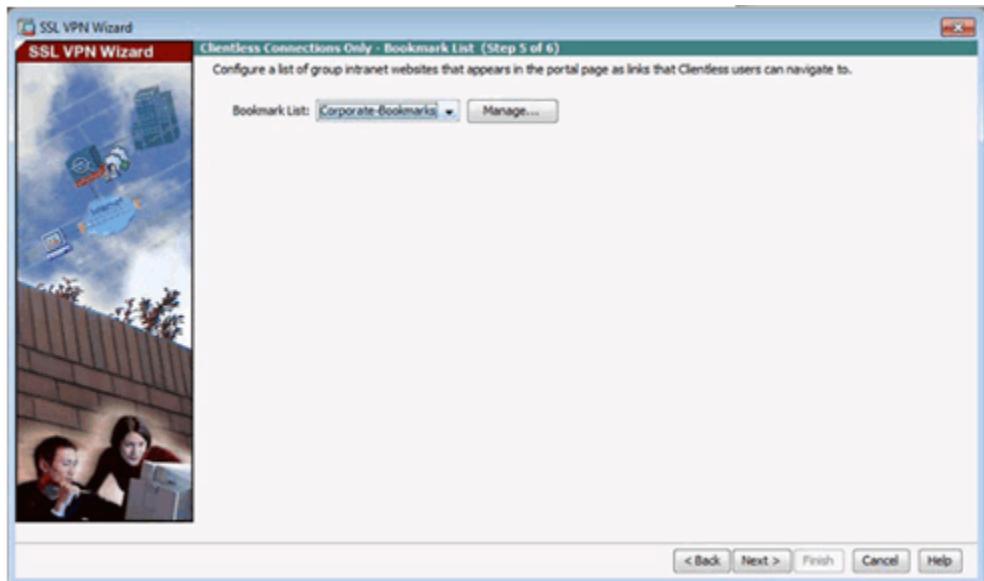
## Revised Add Bookmark List Window



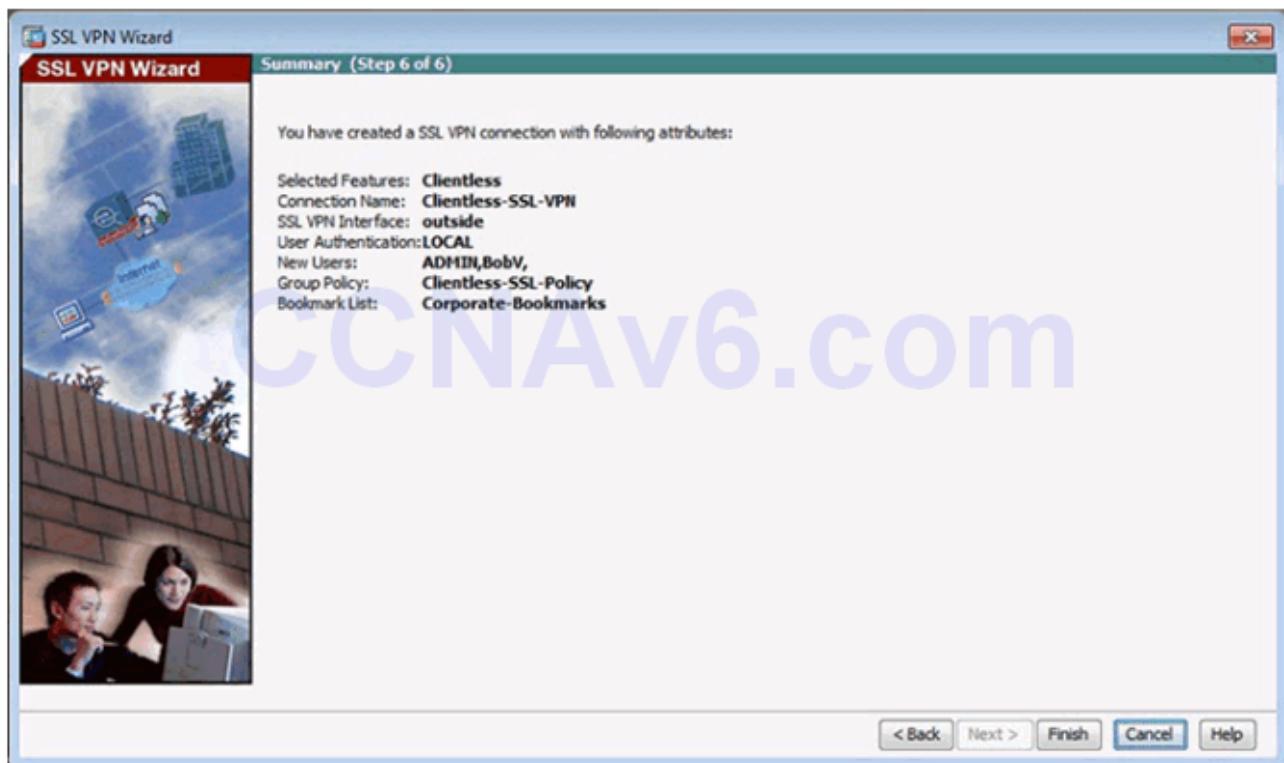
Revised Configure GUI Customization Objects Window



Revised Bookmark List Window



Summary Window



## Verifying Clientless SSL VPN

**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**

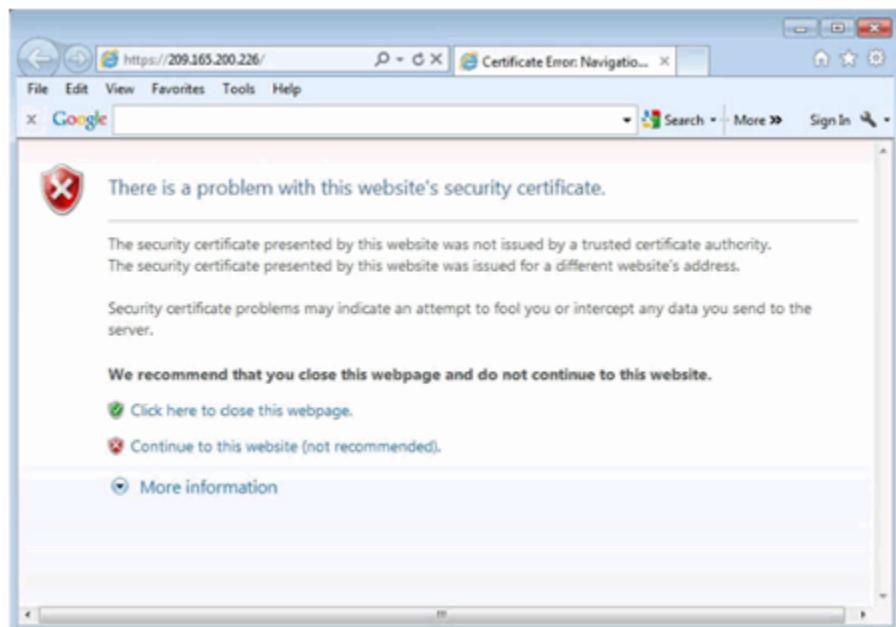
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<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

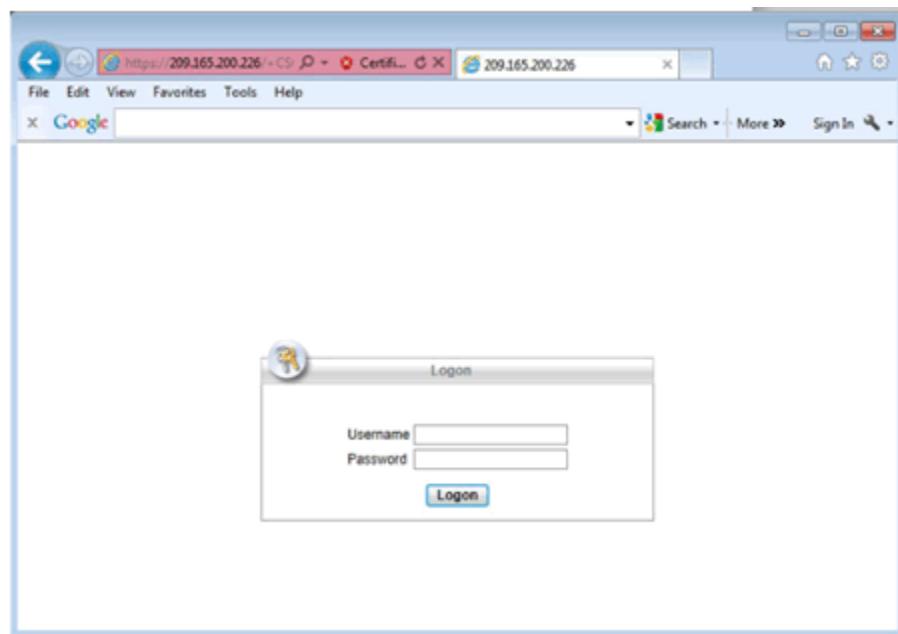
**Buttons:** Add, Edit, Delete, Find, Match Case, Apply, Reset

## Testing the Clientless SSL VPN Connection

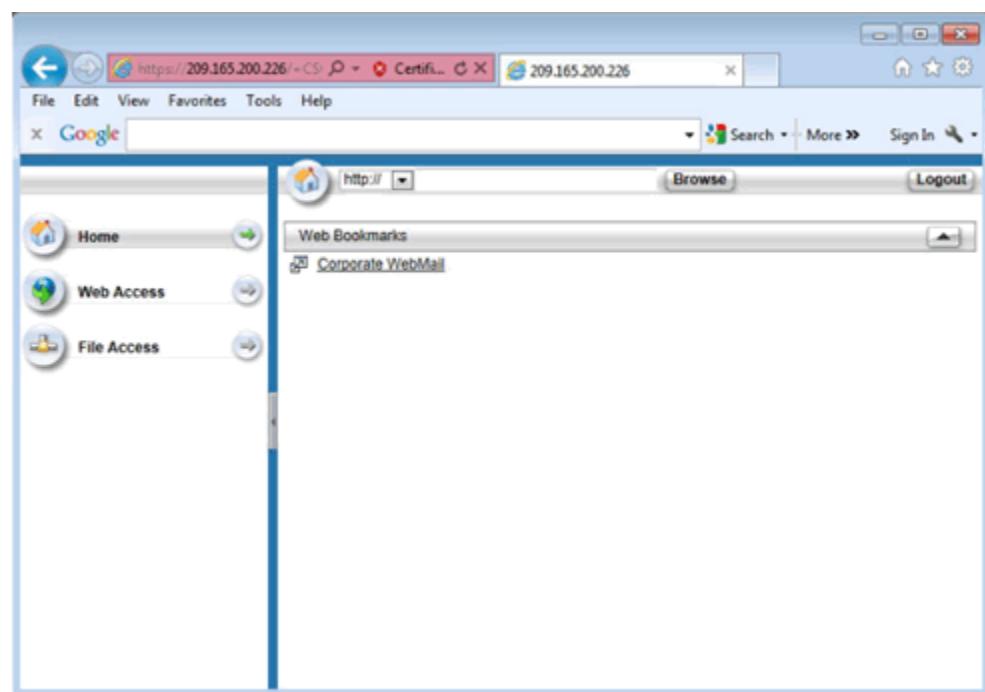
### Security Certificate Window



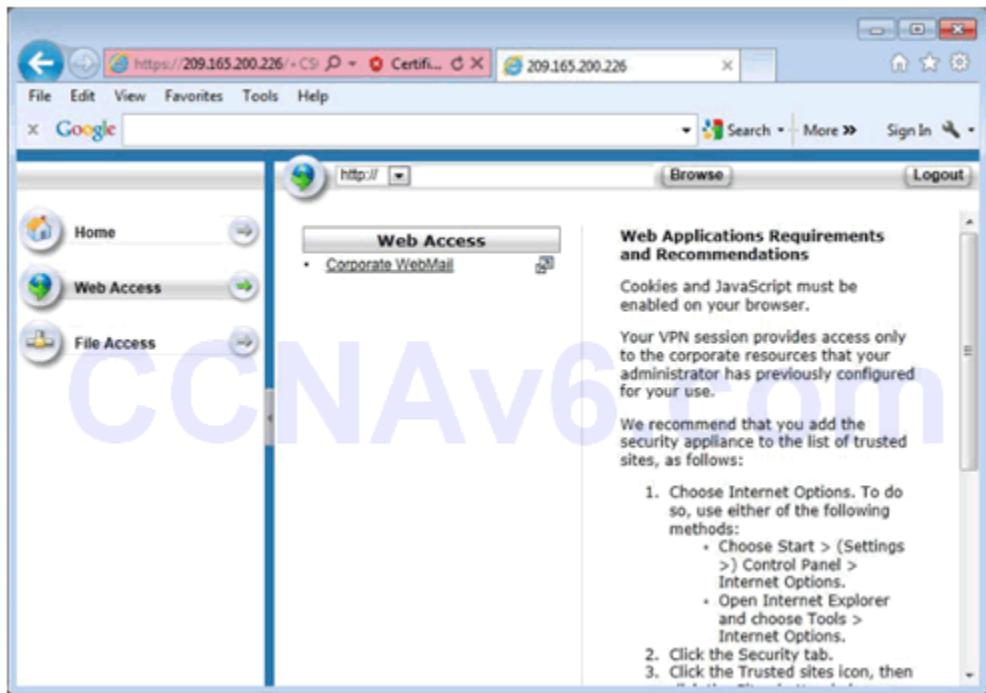
### Logon Window



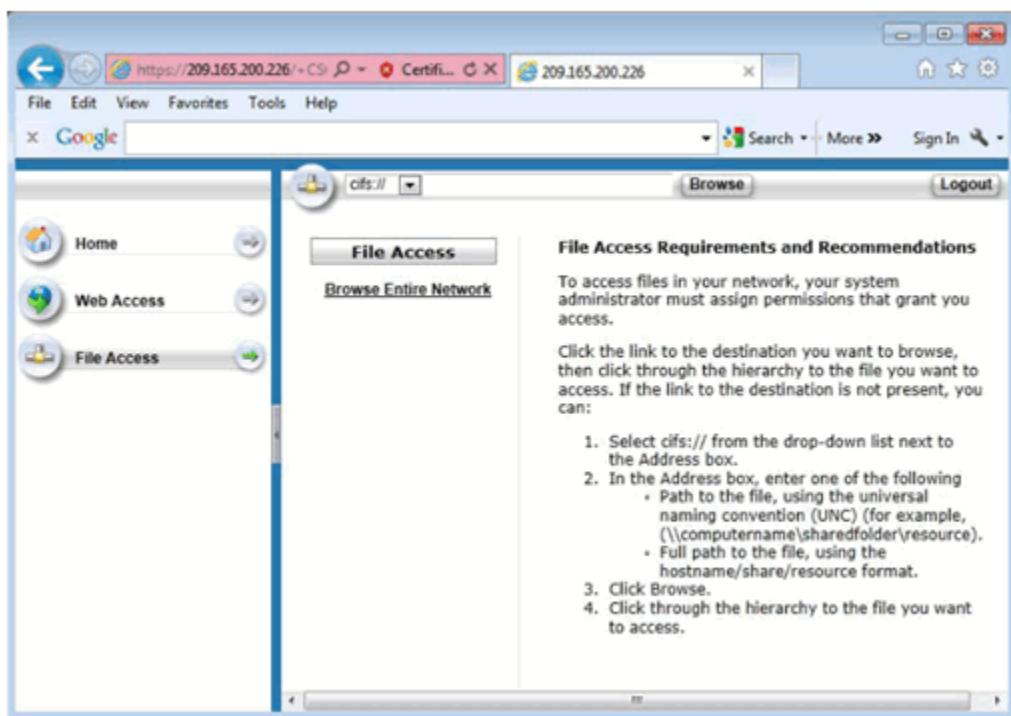
Web Portal Home Page



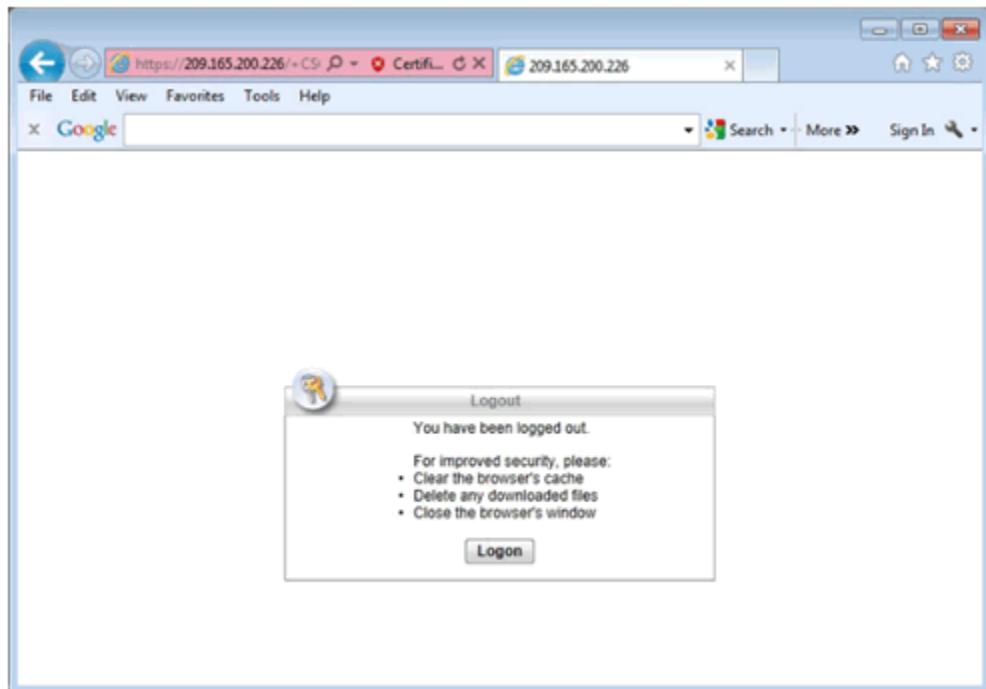
Web Portal Web Access Page



## 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

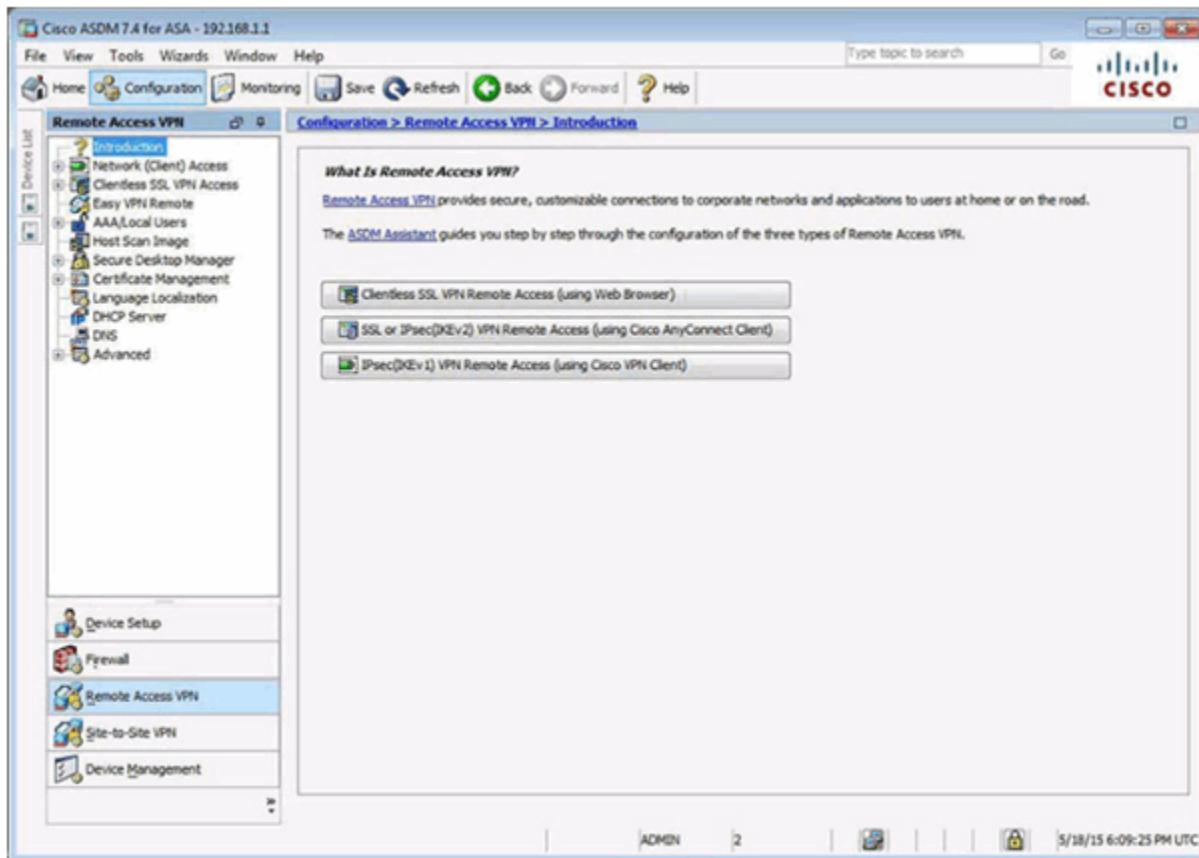
  username ADMIN password 3MBOT/Mpbpc4KbOv encrypted privilege 0
  username ADMIN attributes
  vpn-group-policy Clientless-SSL-Policy
  username BobV password AOvleG/KWkzEwhtN encrypted privilege 0
  username BobV attributes
  vpn-group-policy Clientless-SSL-Policy

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

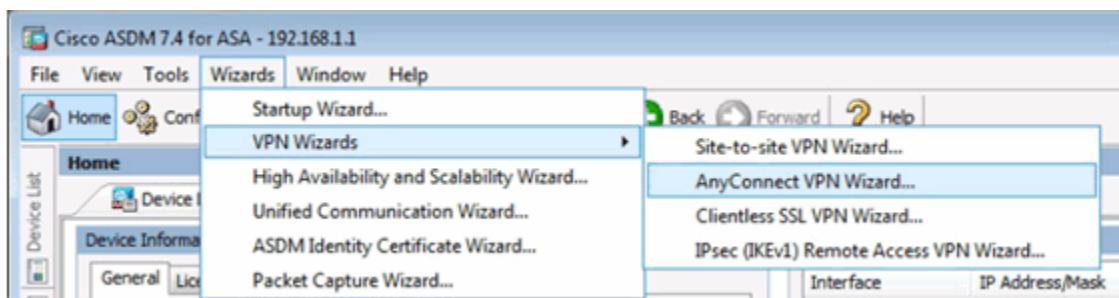
## Topic 10.2.4: Configuring AnyConnect SSL VPN

### Configuring SSL VPN AnyConnect

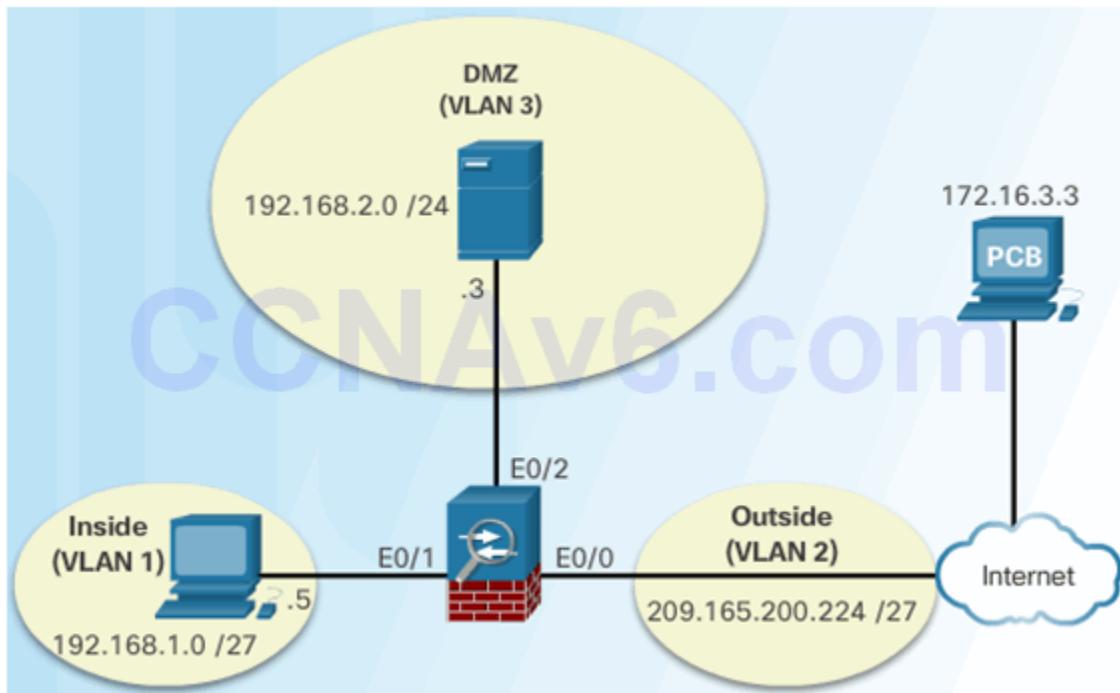
ASDM Assistant



## Client-Based VPN Wizard



## Sample SSL VPN Topology

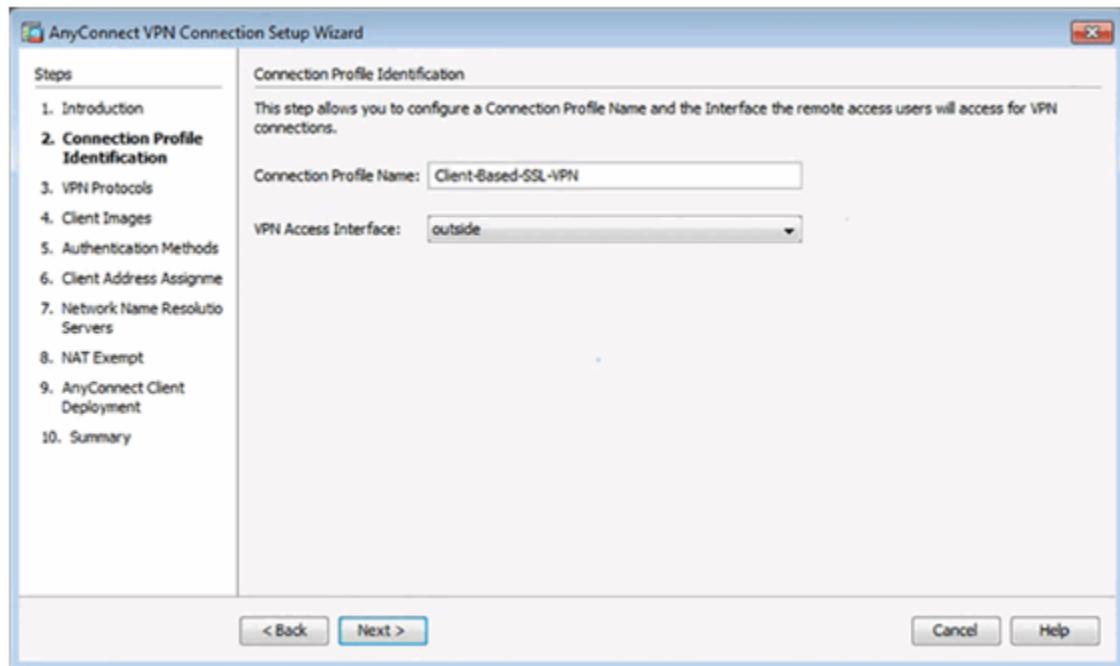


## AnyConnect SSL VPN

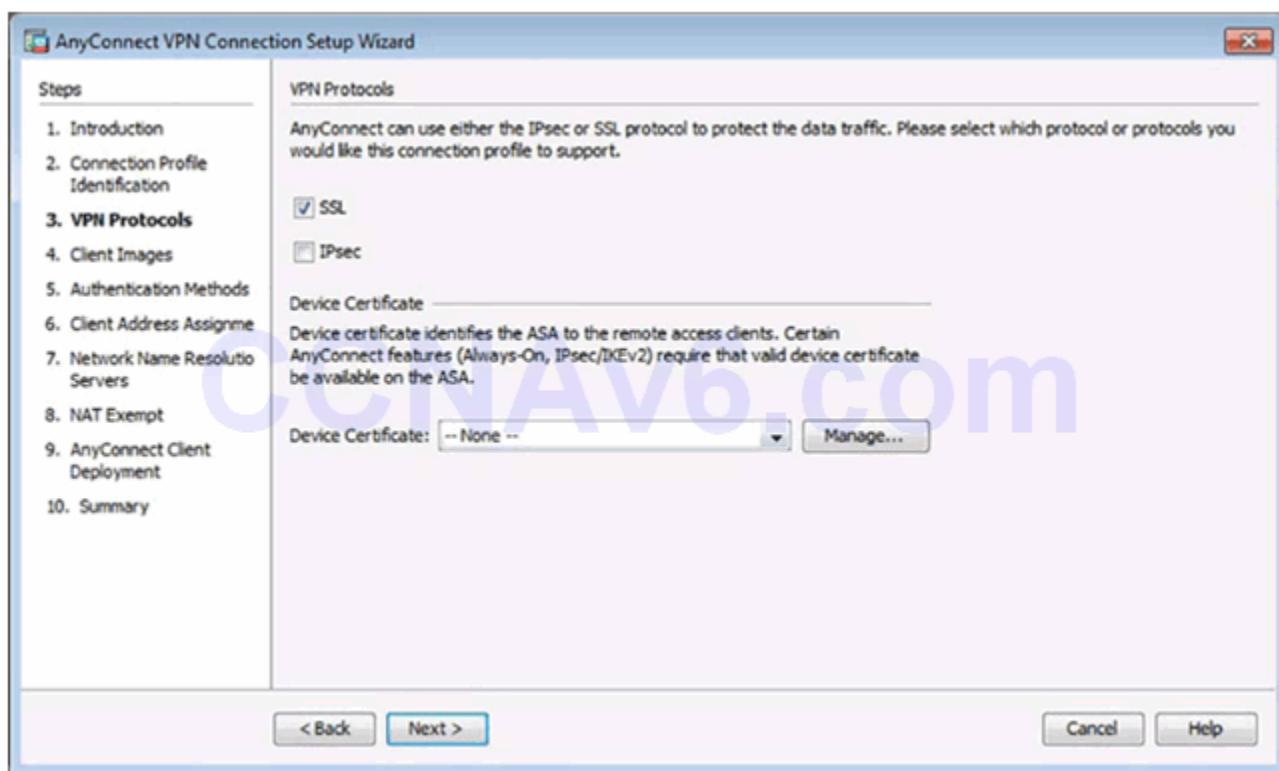
AnyConnect VPN Wizard Introduction Window



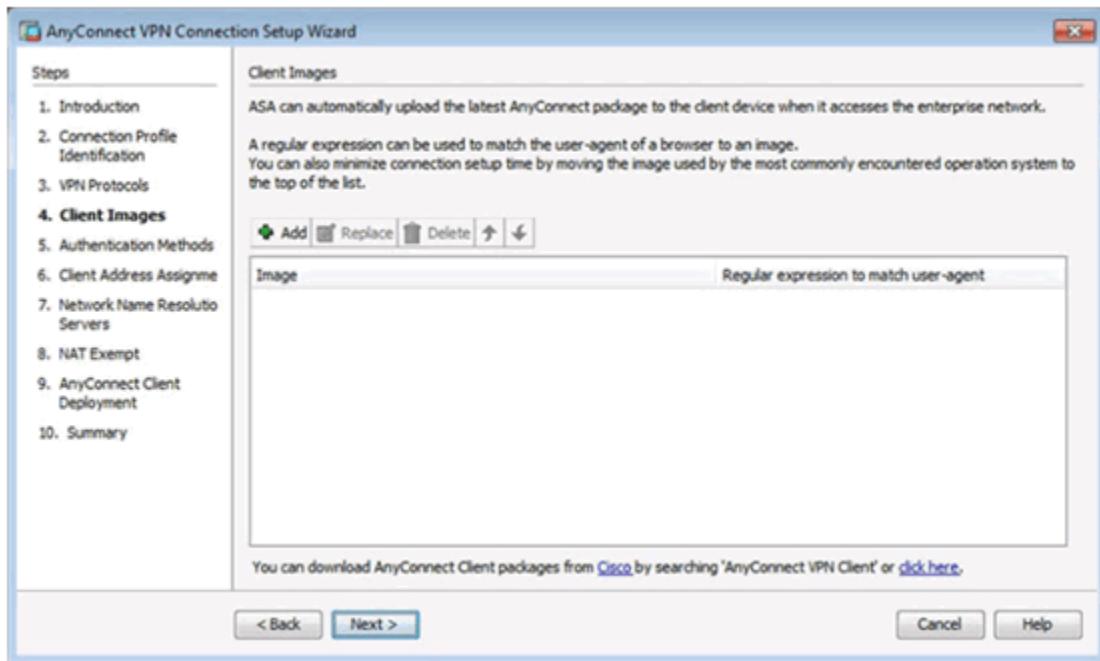
Connection Profile Identification Window



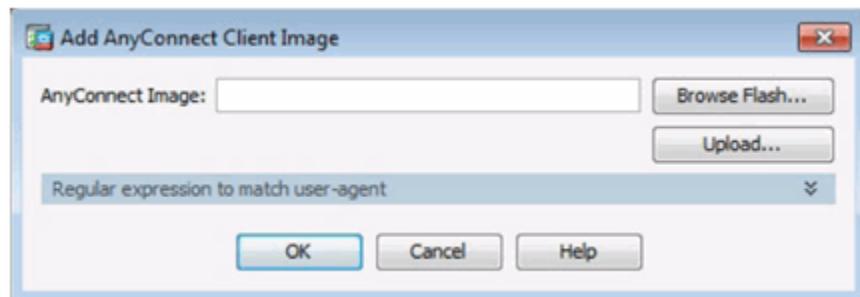
VPN Protocols Window



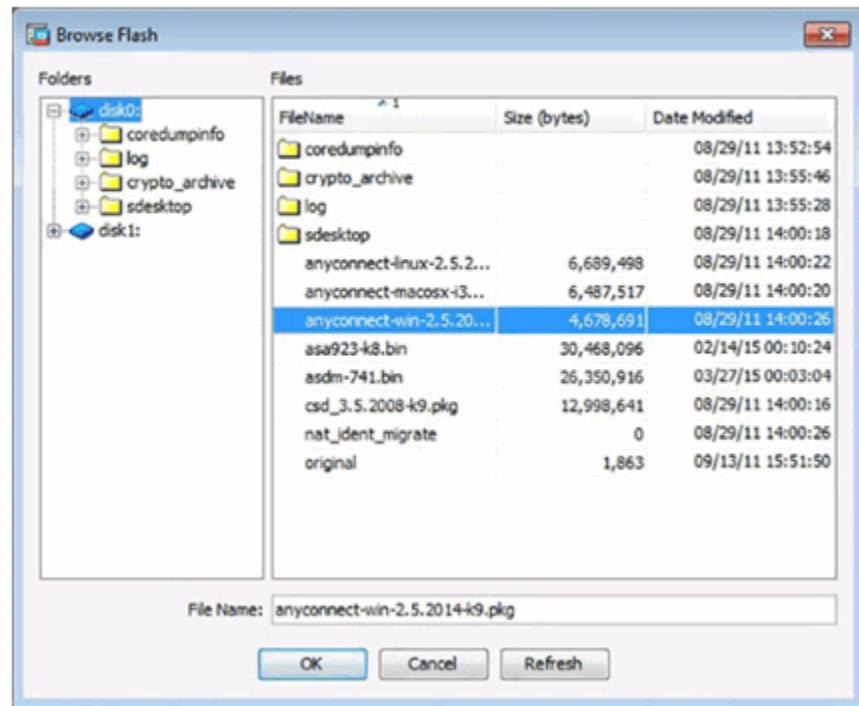
Client Images Window



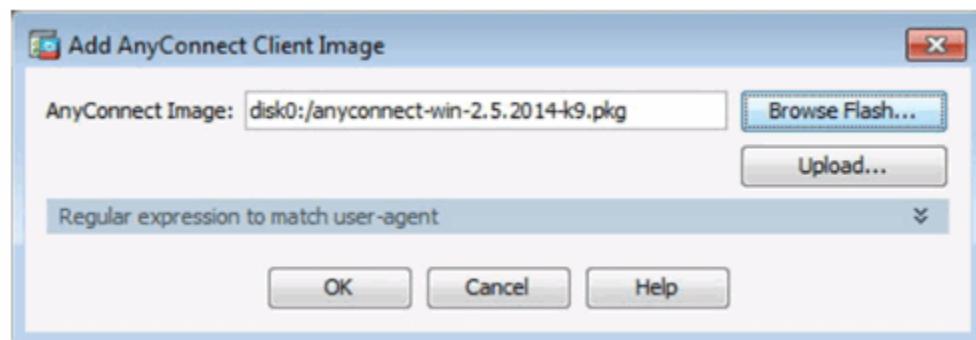
Add AnyConnect Client Image Window



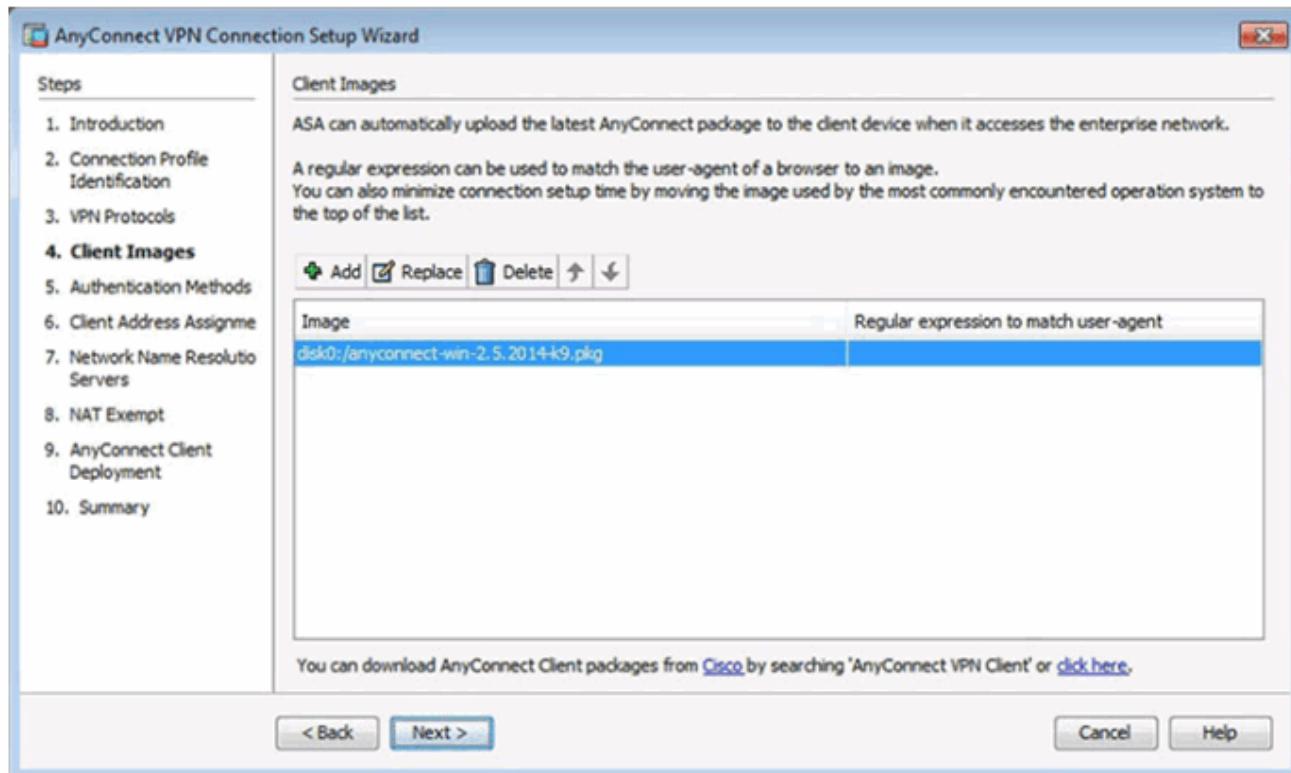
Browse Flash Window



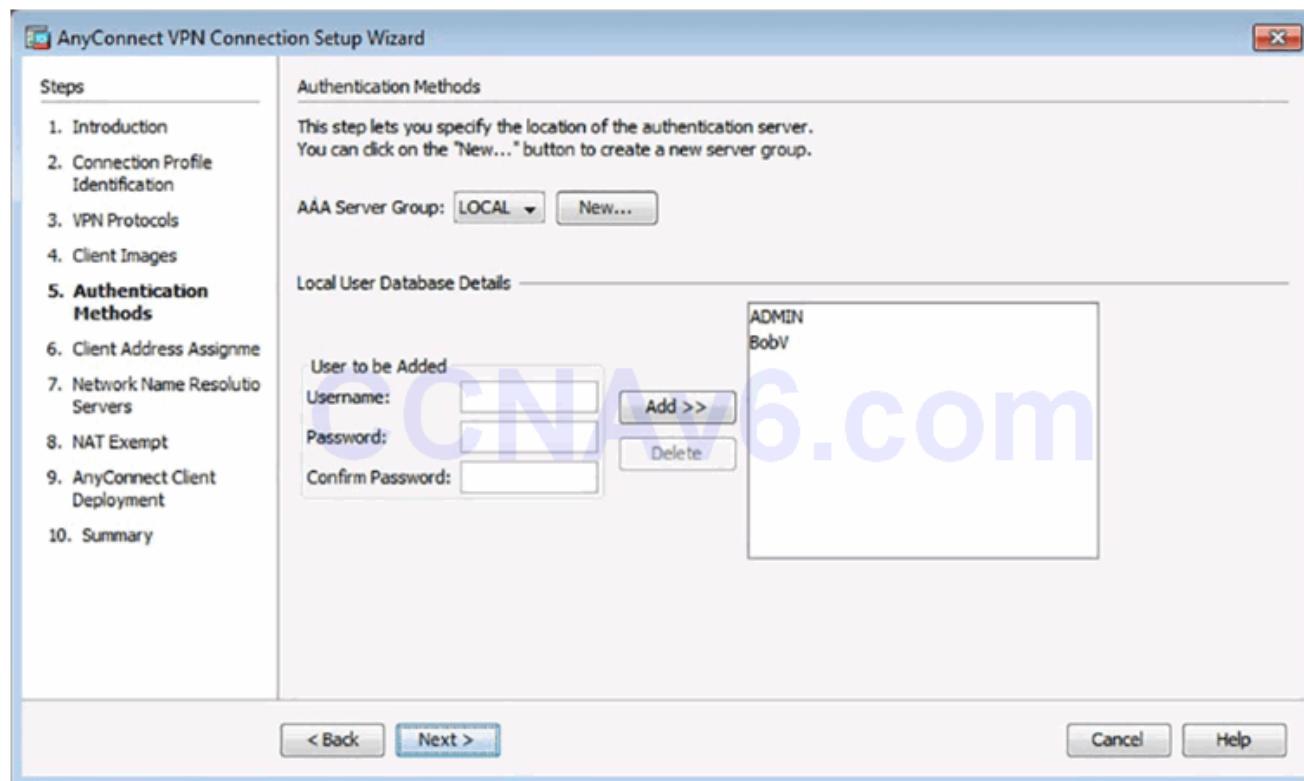
Add AnyConnect Client Image Window



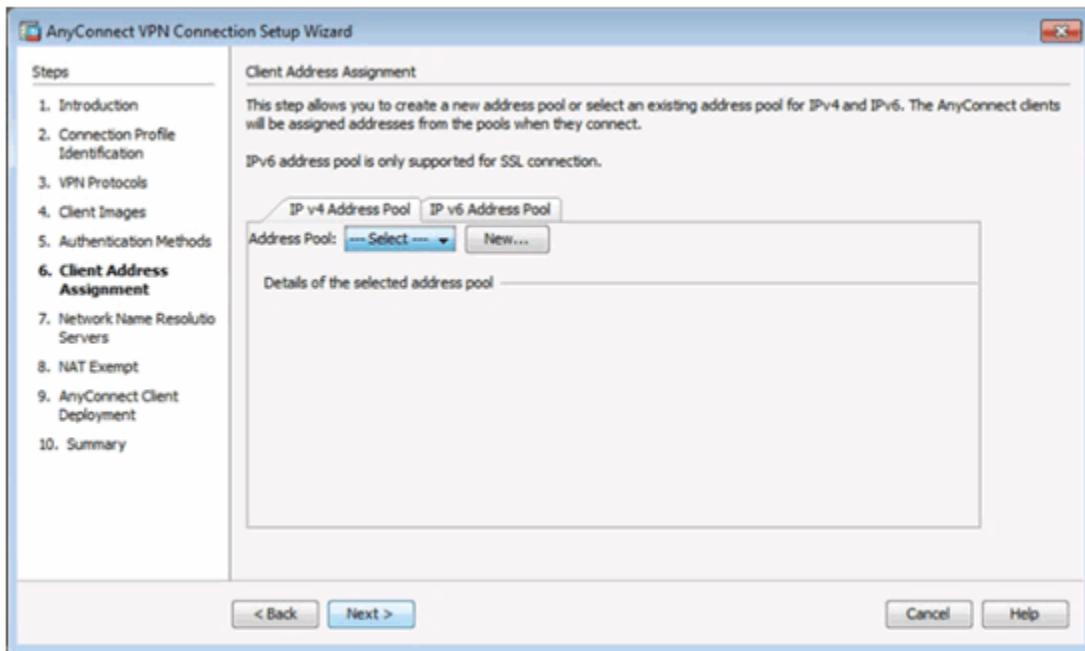
Completed Client Images Window



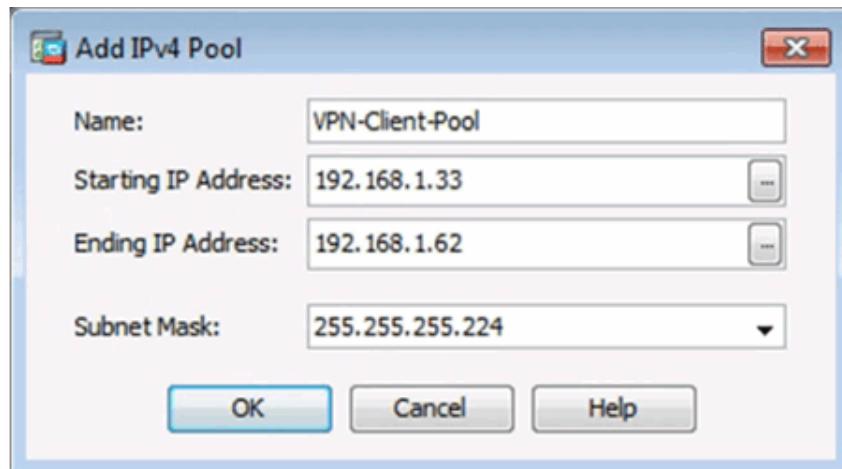
Authentication Methods Window



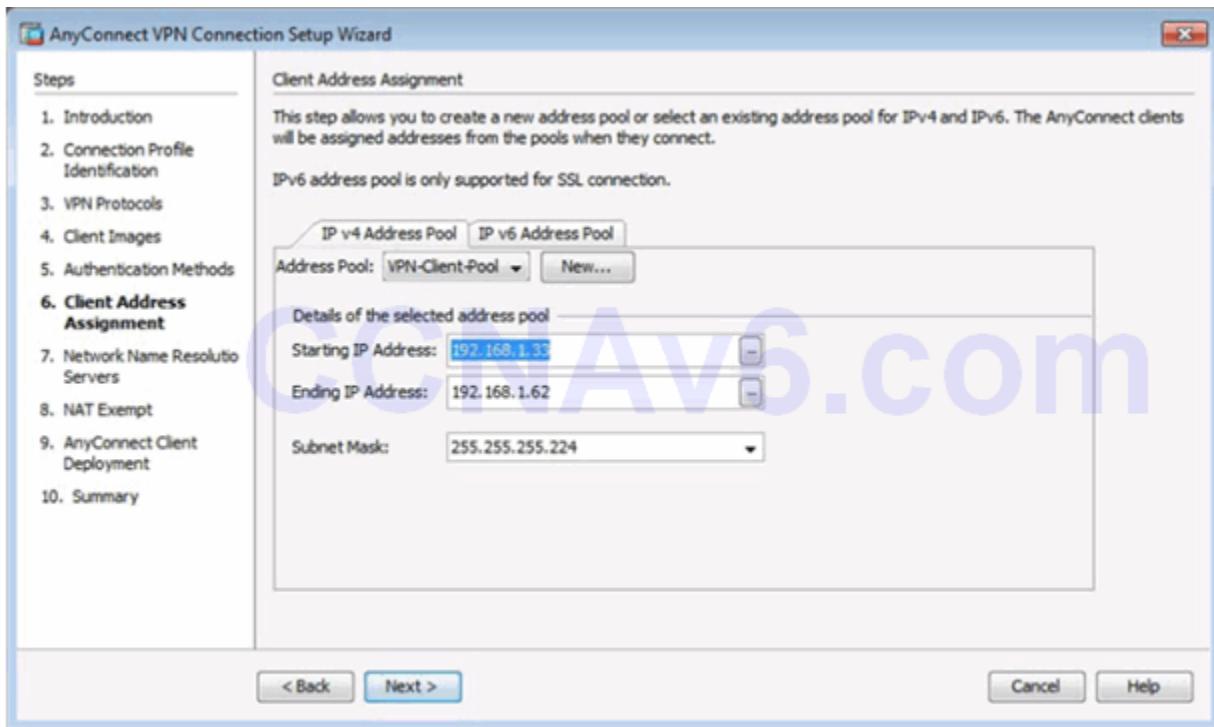
Client Address Management Window



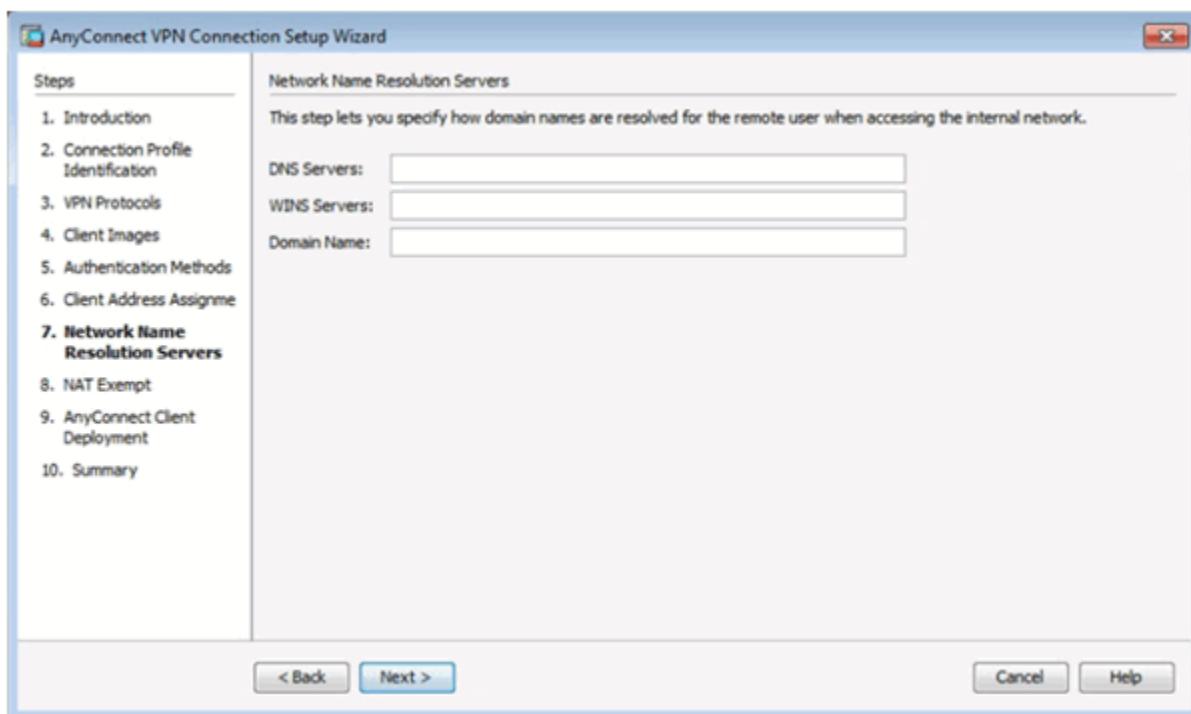
Add IPv4 Window



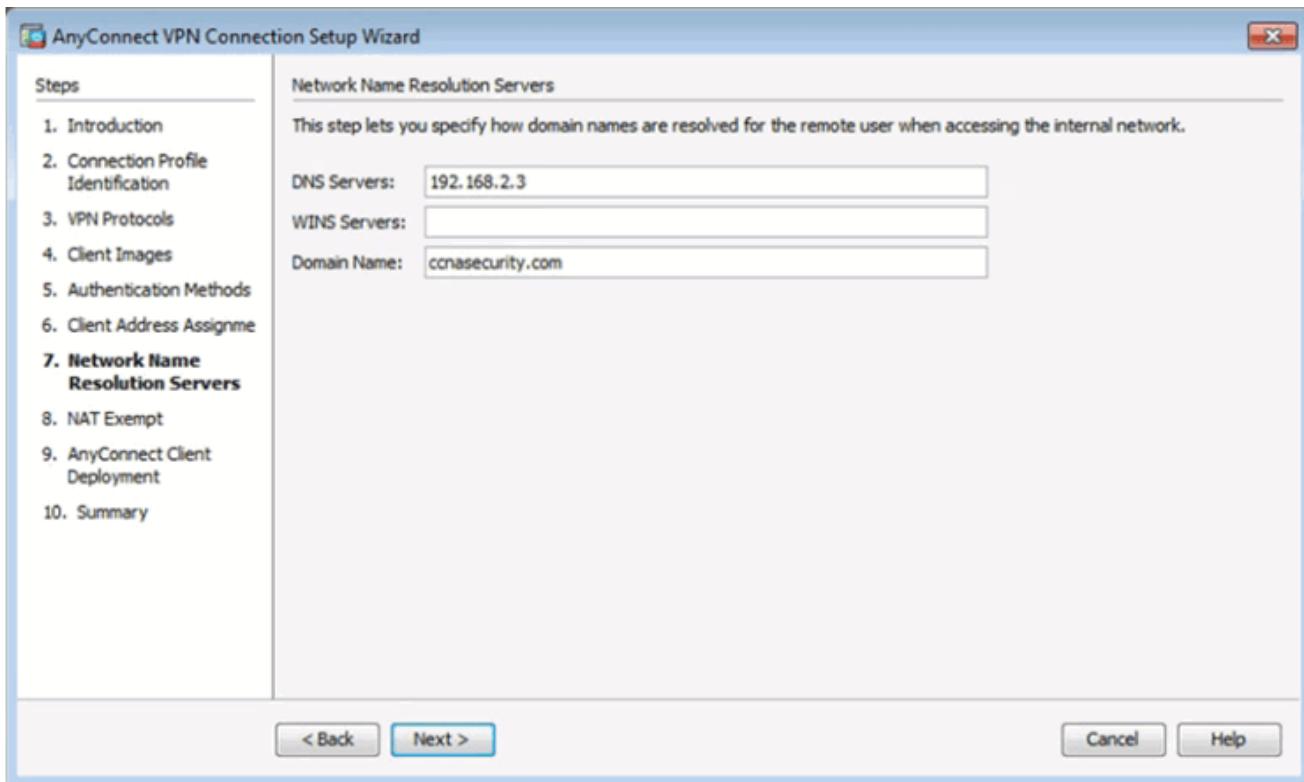
Completed Client Address Management Window



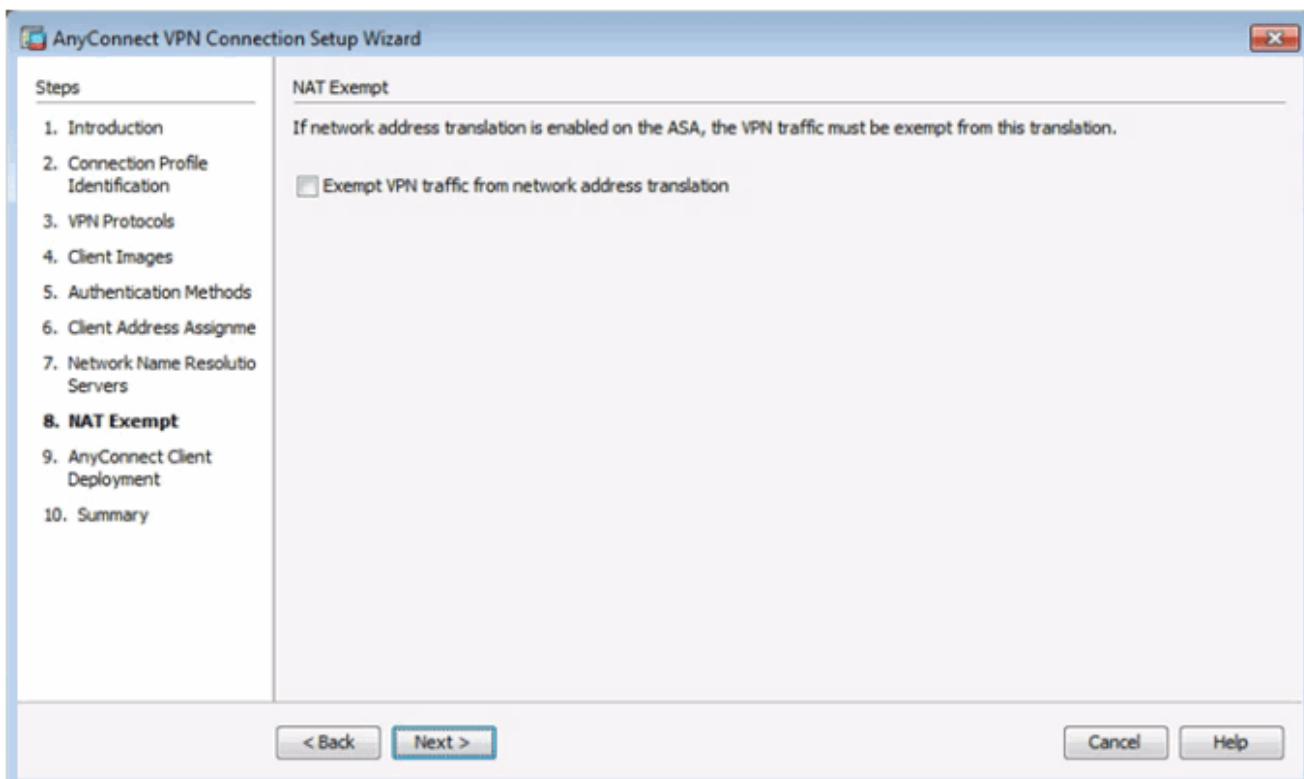
Network Name Resolution Servers Window



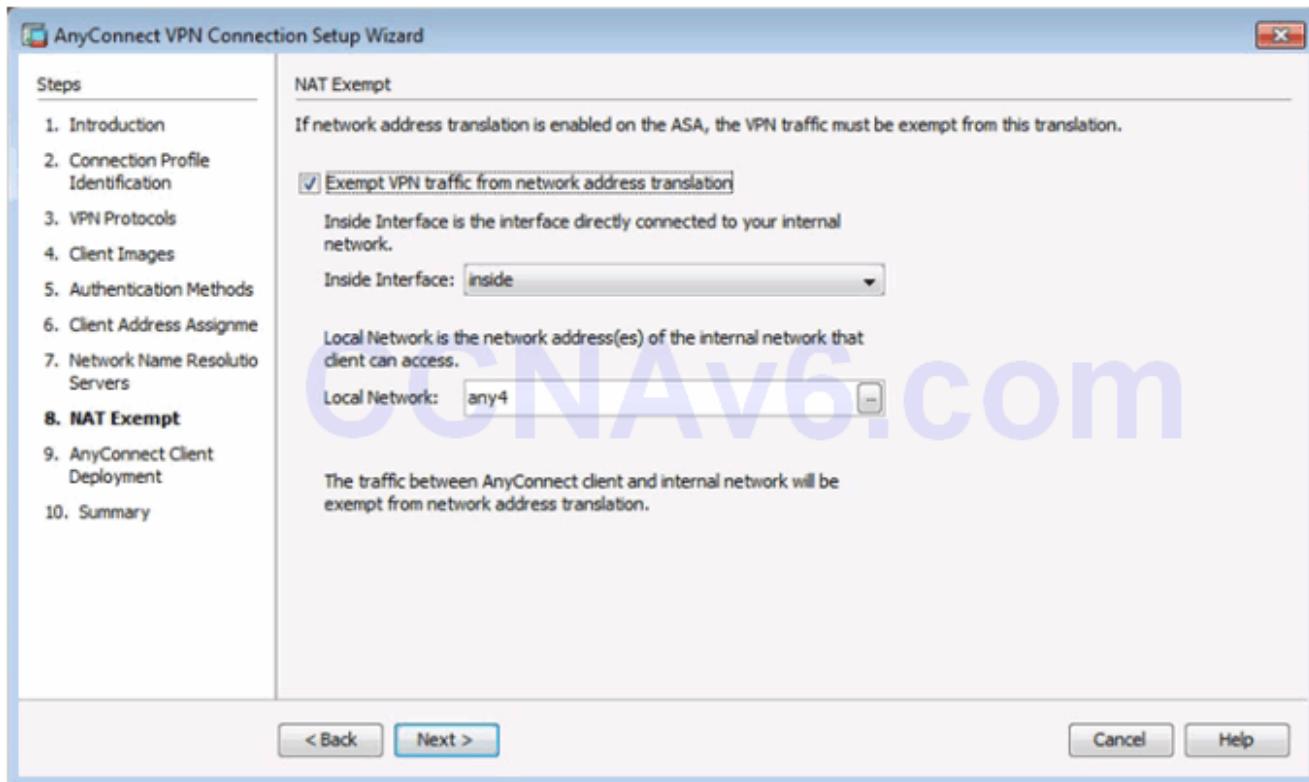
Completed Network Name Resolution Servers Window



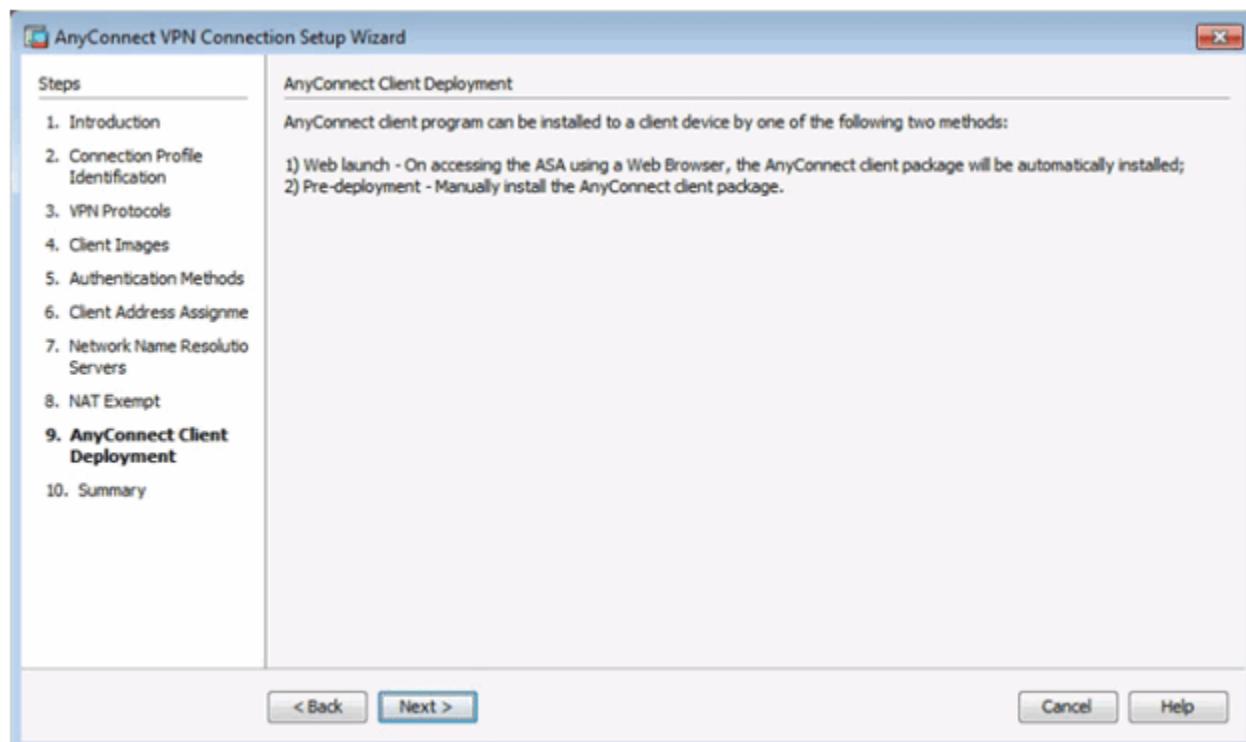
## NAT Exempt Window



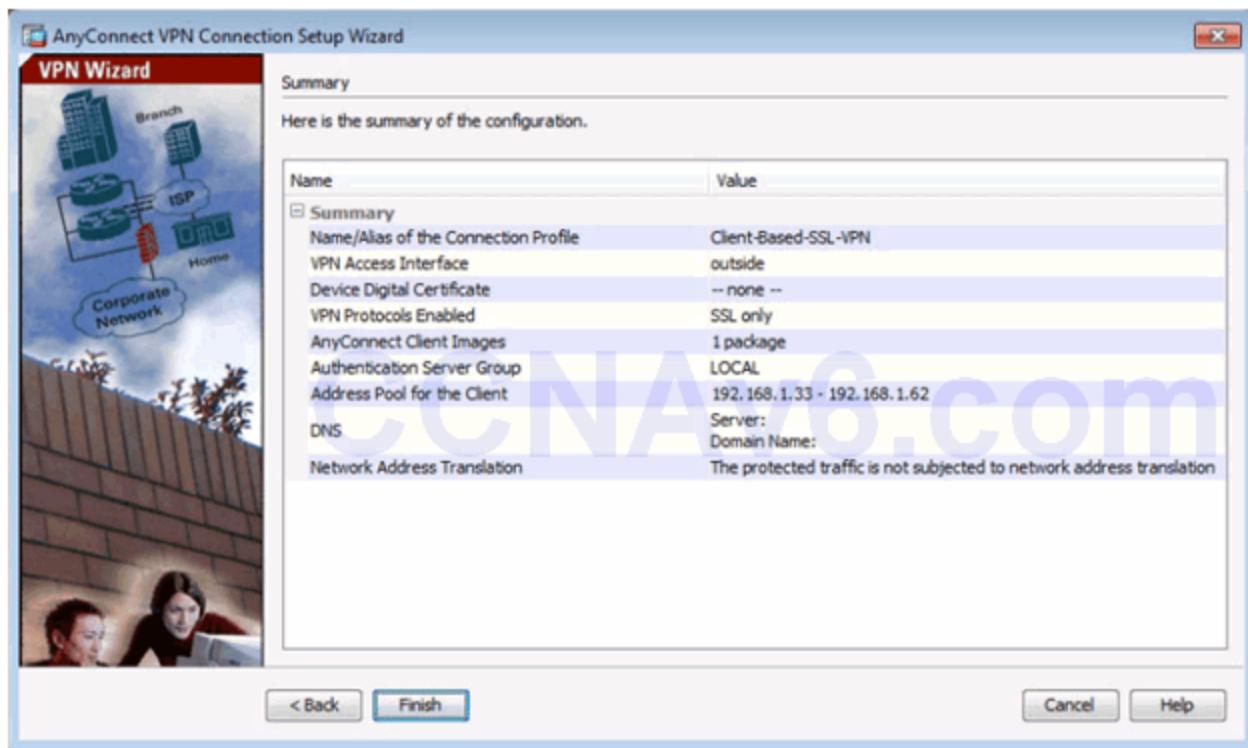
## Completed NAT Exempt Window



## AnyConnect Client Deployment



## Summary Window



## Verifying AnyConnect Connection

### AnyConnect Connection Profiles Page

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.

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).

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.

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](#).

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

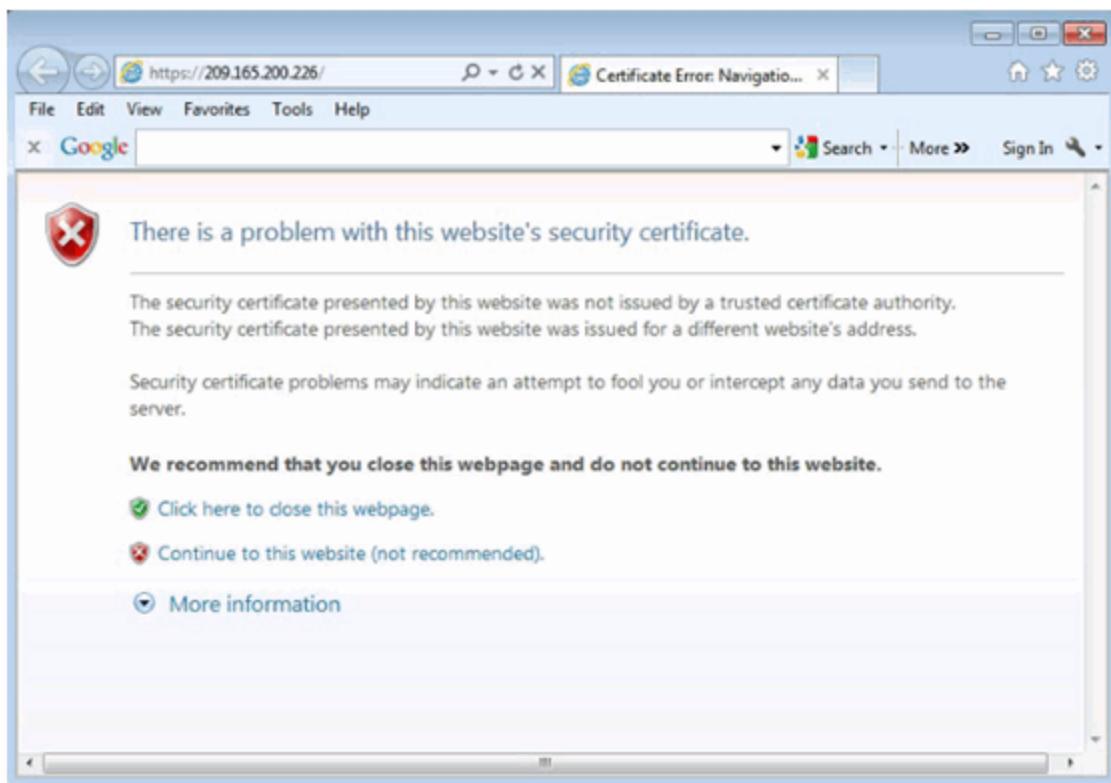
### Verifying the Client-Based Configuration

Connection Profiles					
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
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...

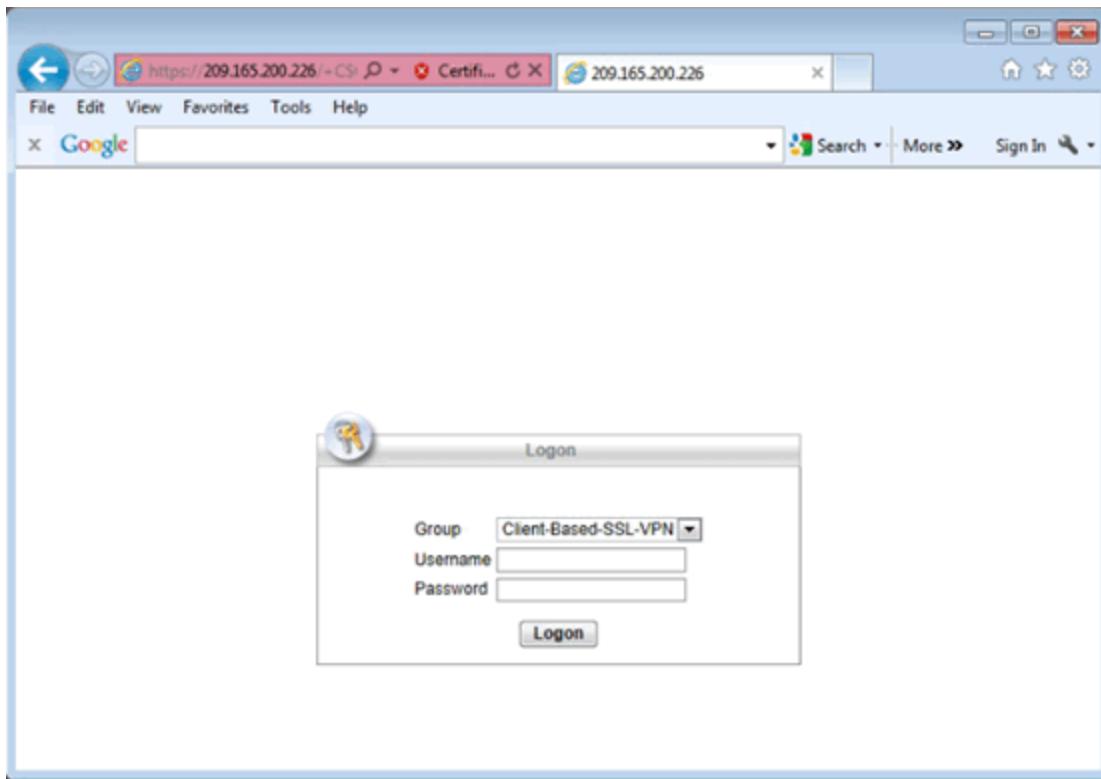
Let group URL take precedence if group URL and certificate map match different connection profiles. Otherwise, the connection profile that matches the certificate map will be used.

## Install the AnyConnect Client

### Security Certificate Window



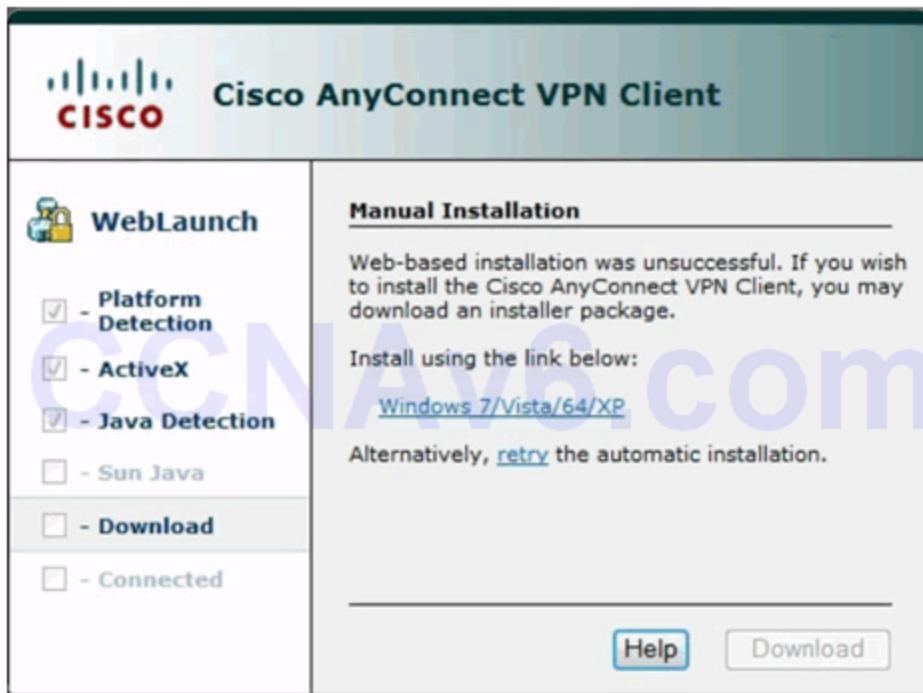
### Logon Window



Cisco AnyConnect VPN Client Window



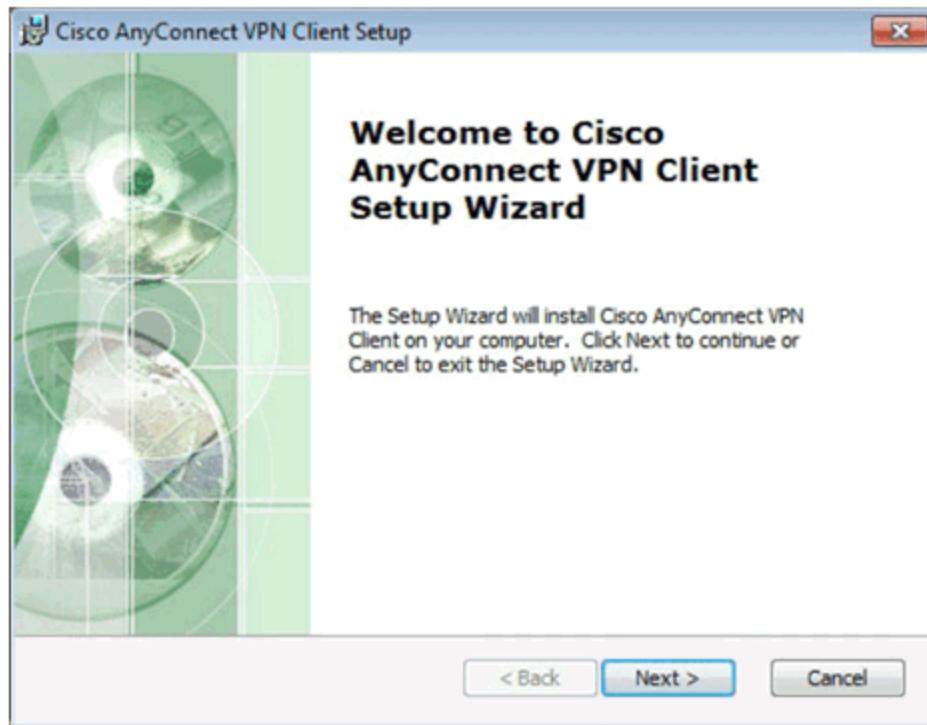
Manual Installation Window



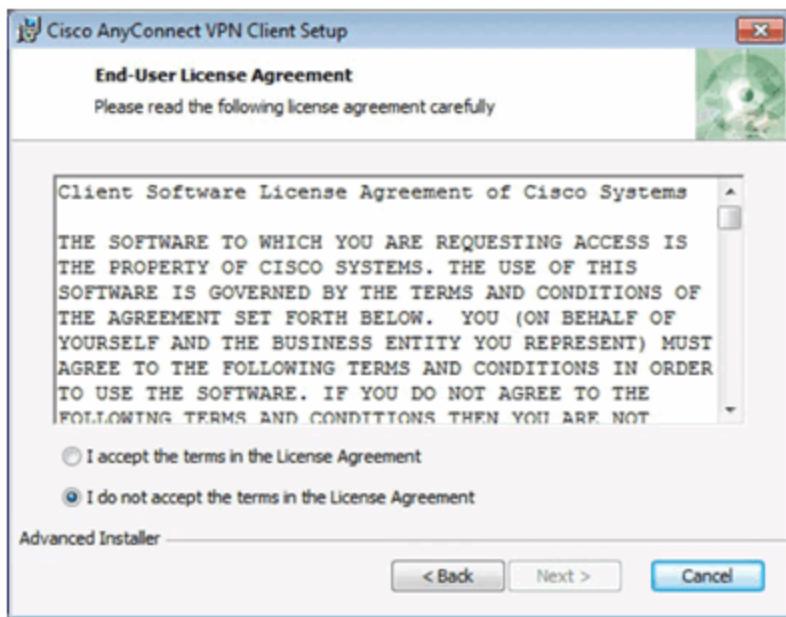
## Run Installer Window



## Cisco AnyConnect VPN Client Setup Window



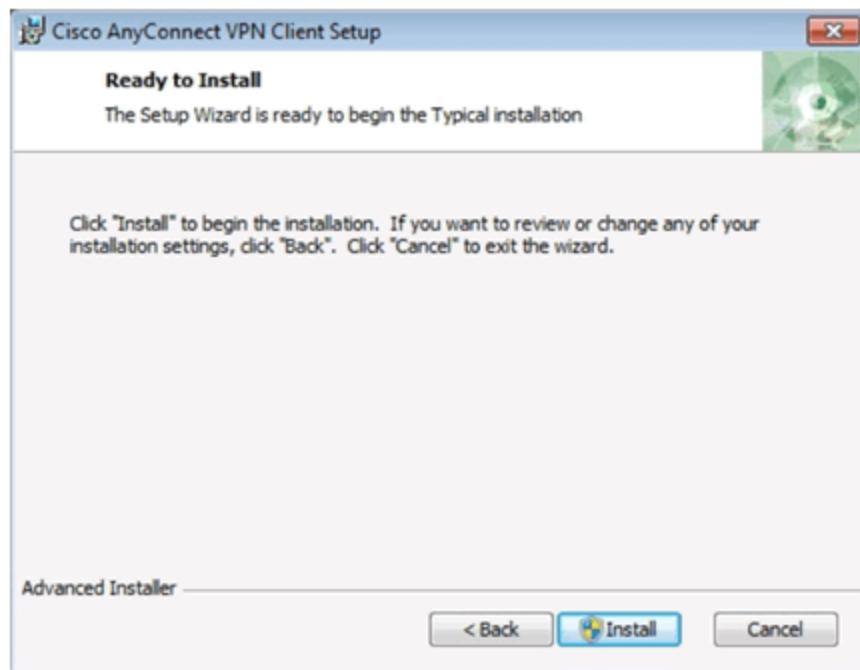
End-User Agreement Window



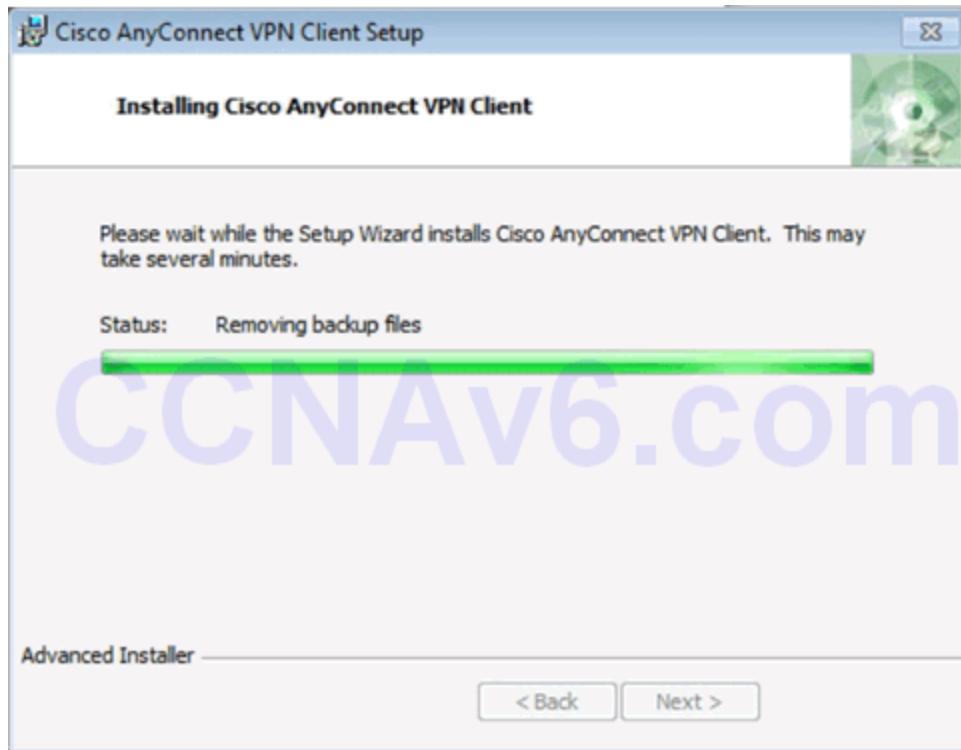
User Account Control Security Window



Ready to Install AnyConnect Client



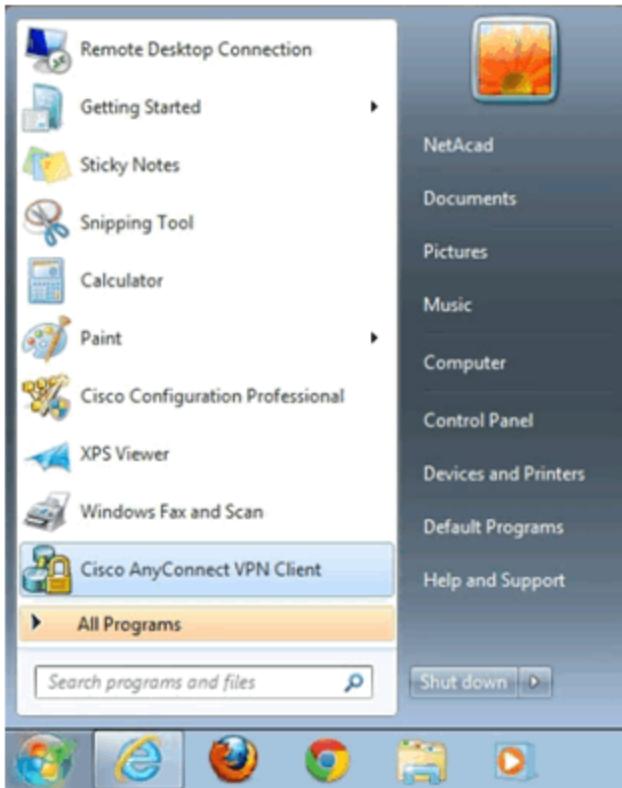
Installing the AnyConnect Client



Complete Cisco AnyConnect VPN Installation



Start the Cisco AnyConnect VPN Cisco



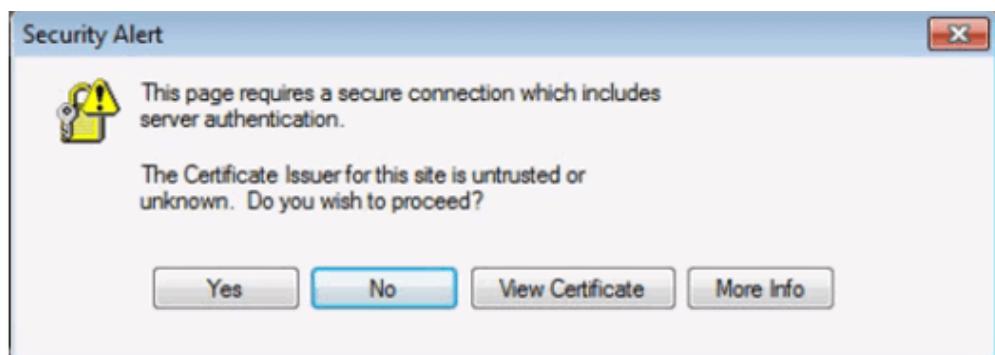
Cisco AnyConnect VPN Client Window



Cisco AnyConnect VPN Connect Window



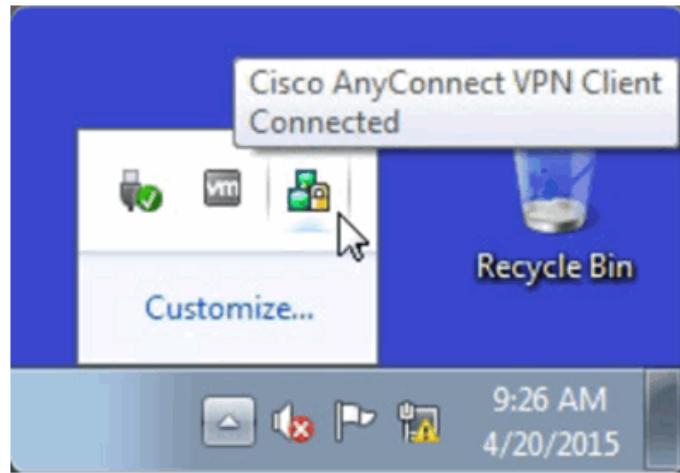
Certificate Security Warning Window



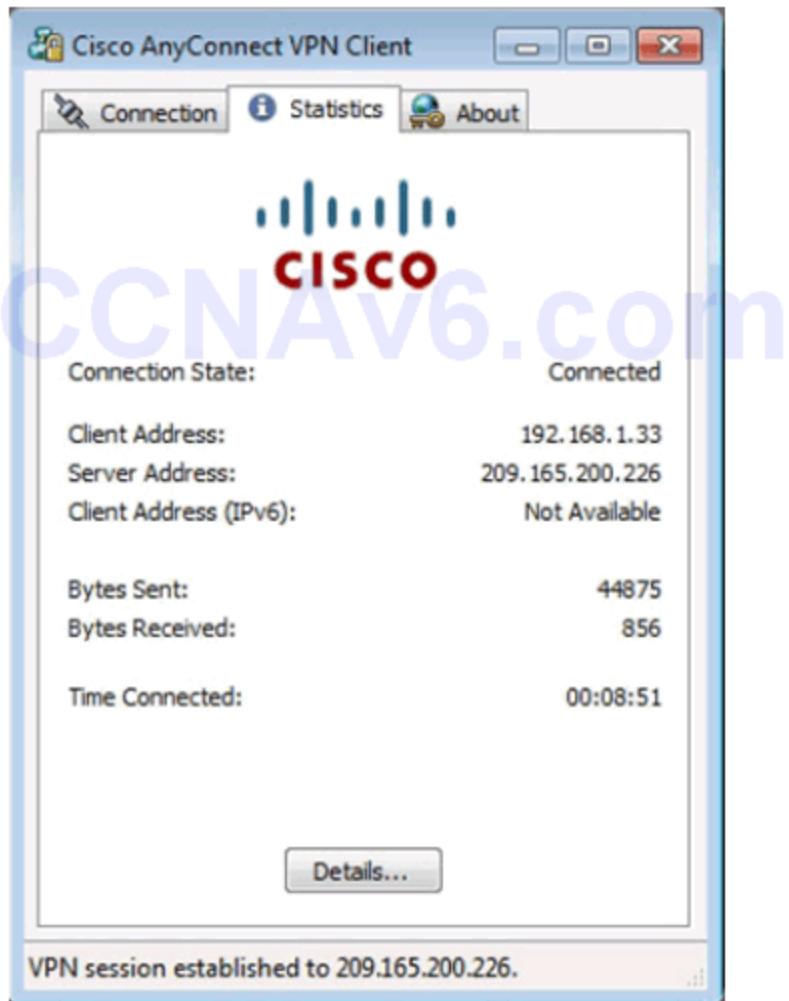
Cisco AnyConnect VPN Authentication Window



Cisco AnyConnect VPN Icon in System Tray



Cisco AnyConnect VPN Client Status



Verifying Connectivity to Internal Network

```
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 3:

Connection-specific DNS Suffix . : ccnasecurity.com
IPv4 Address . . . . . : 192.168.1.33
Subnet Mask . . . . . : 255.255.255.224
Default Gateway . . . . . : 192.168.1.34

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=85ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128
Reply from 192.168.1.3: bytes=32 time=84ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 85ms, Average = 84ms

C:\Users\NetAcad>
```

## 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.

## **Download Slide PowerPoint (pptx):**

[sociallocker id="54558"][Click here](#)[/sociallocker]