# Cisco ASA Firewall

CCS Module 4

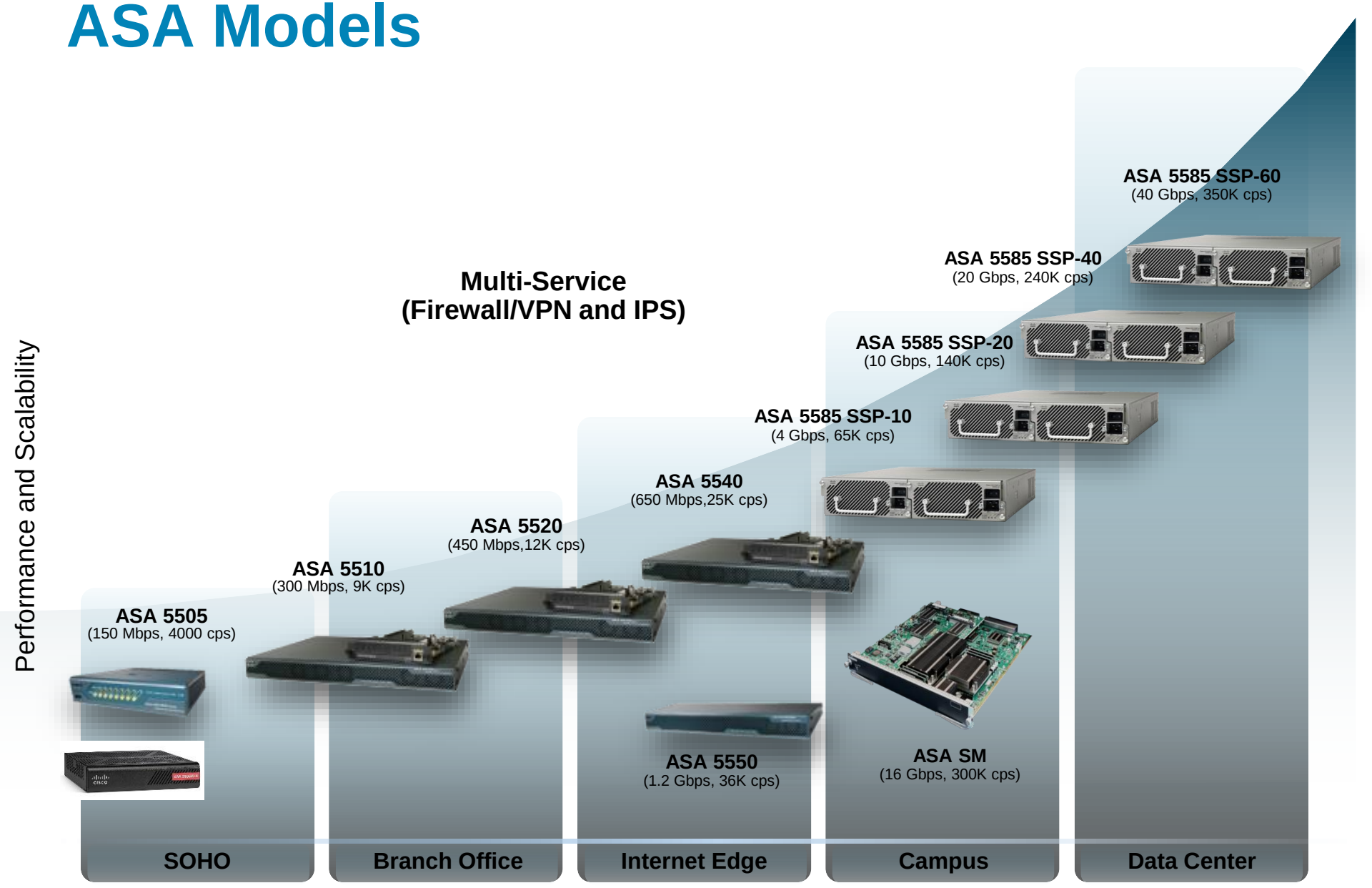
# Agenda

- **Concepts**
- **Basic Setup**
- **Objects**
- **ACL**
- **NAT**
- **AAA**
- **MPF**
- **VPNs**
  - Site-to-Site
  - Clientless
  - AnyConnect

# ASA 5500 Firewall Solution

- The ASA 5500 firewall appliance is a multi-service standalone appliance that is a primary component of the Cisco SecureX architecture
- There are six ASA models, ranging from the basic 5505 branch office model to the 5585 data center version
- The choice of ASA model will depend on an organization's requirements, such as:
  - Maximum throughput
  - Maximum connections per second
  - Available budget
- The biggest difference between models is the:
  - Maximum traffic throughput handled by the device
  - The types and the number of interfaces on the device

# ASA Models



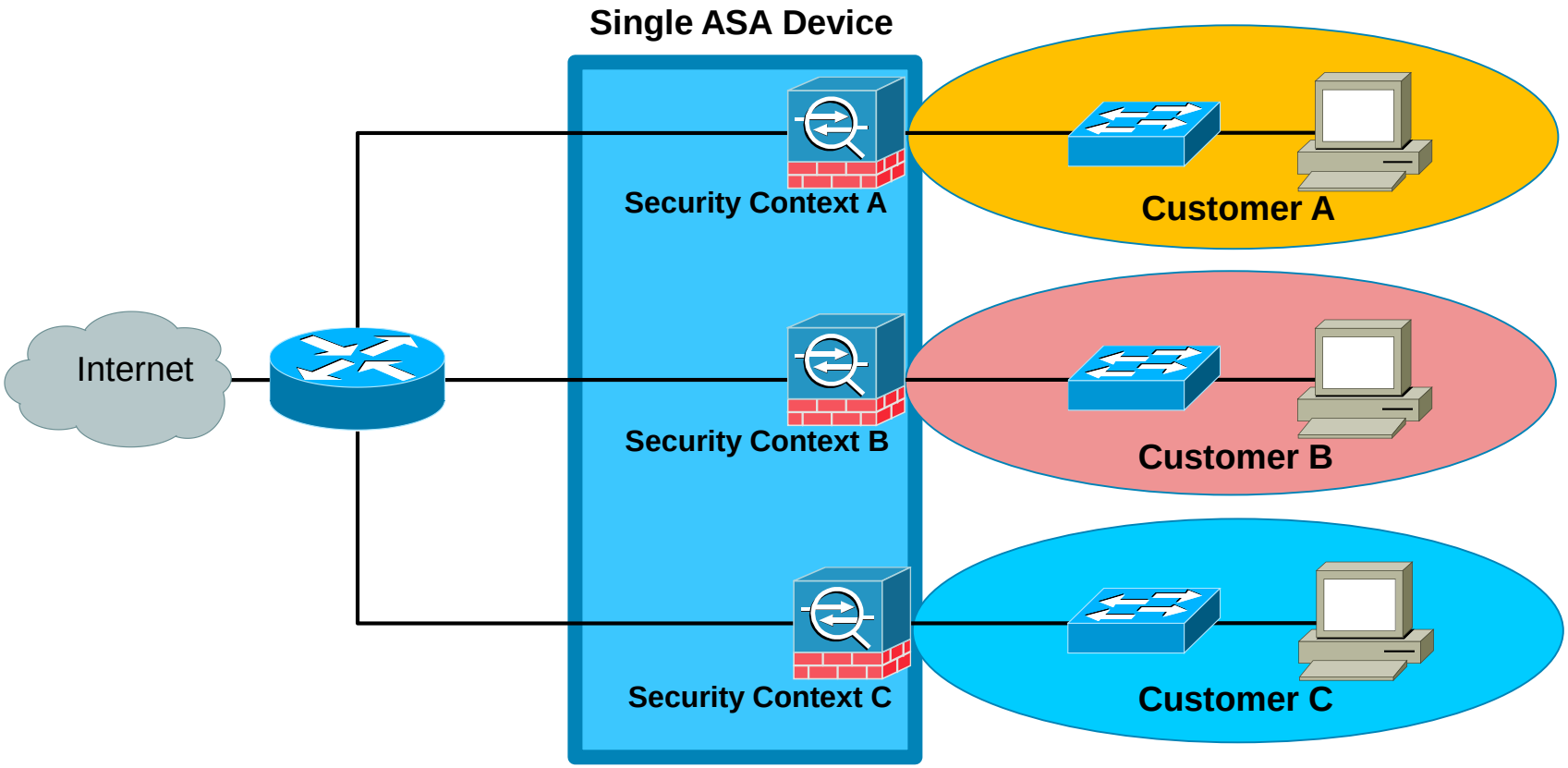

* Mbps and Gbps = maximum throughput * cps = maximum connection per second

# ASA Features

- **Stateful firewall**
  - Only packets matching a known active connection will be allowed by the firewall; others will be rejected
- **VPN Concentrator**
  - The ASA supports IPsec and SSL remote access and IPsec site-to-site VPN features
- **Intrusion Prevention**
  - Advanced threat control is provided by adding the Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) and Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC)
- **Threat Control**
  - Additional anti-malware threat control capabilities are provided by adding the Content Security and Control (CSC) module
- **Virtualization**
  - A single ASA can be partitioned into multiple virtual devices called security contexts
  - Each context is an independent device, with its own security policy, interfaces, and administrators
- **High-Availability**
  - Two ASAs can be paired into an active / standby failover configuration to provide device redundancy.
  - One ASA is the primary (active) device while the other is the secondary (standby) device.
  - Both ASAs must have identical software, licensing, memory, and interfaces
- **Identity Firewall**
  - The ASA can provide access control using Windows Active Directory login information.
  - Identity-based firewall services allow users or groups to be specified instead of being restricted by traditional IP address-based rules.

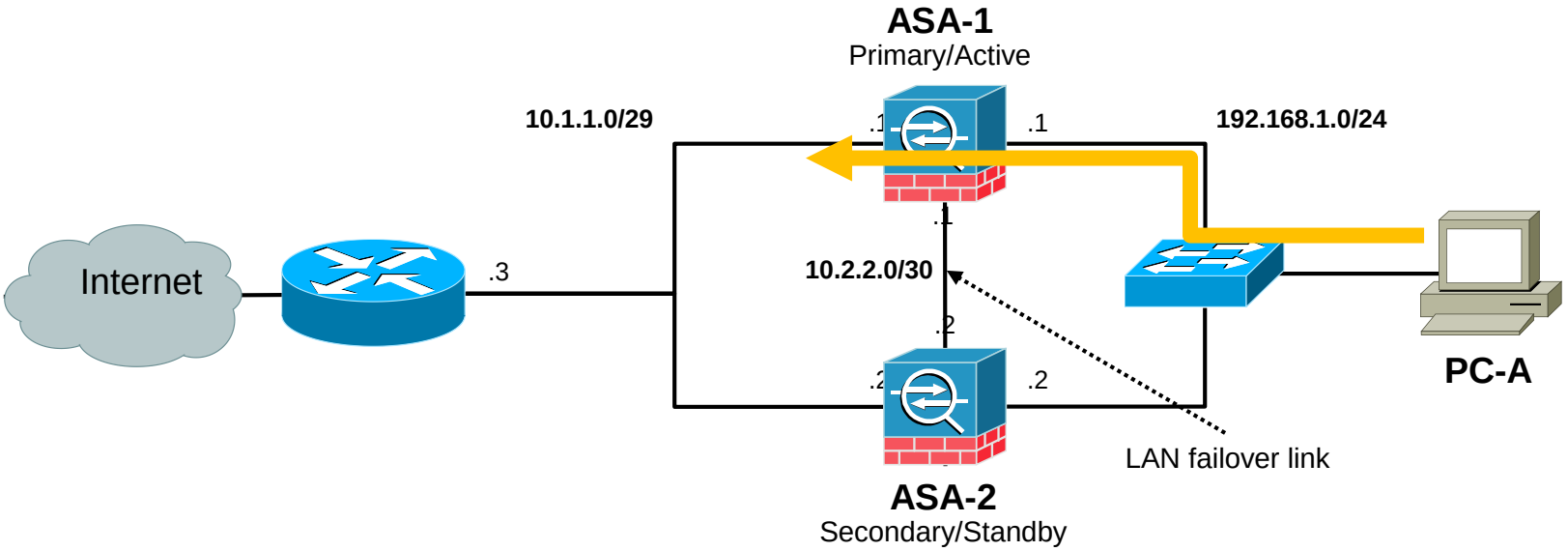
# Advanced ASA Feature: Virtualization

- One single ASA device is divided into three virtual ASA devices (security context) serving the needs of three separate customers.



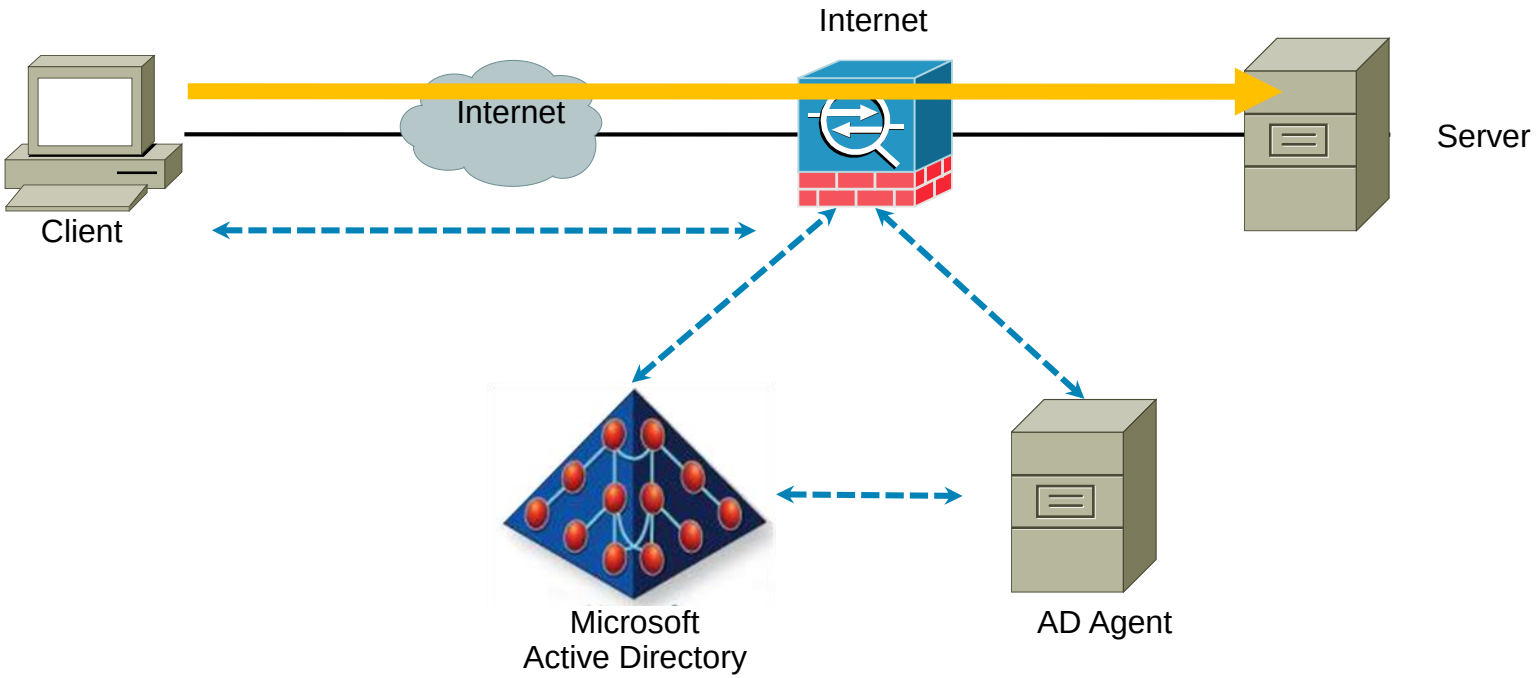
# Advanced ASA Feature: High Availability

- ASA-1 and ASA-2 are identical ASA devices configured for failover and each device monitors the other device over the LAN failover link
- If ASA-2 detects that ASA-1 has failed, then ASA-2 would become the Primary/Active firewall gateway and traffic from PC-A would take the preferred path using ASA-2



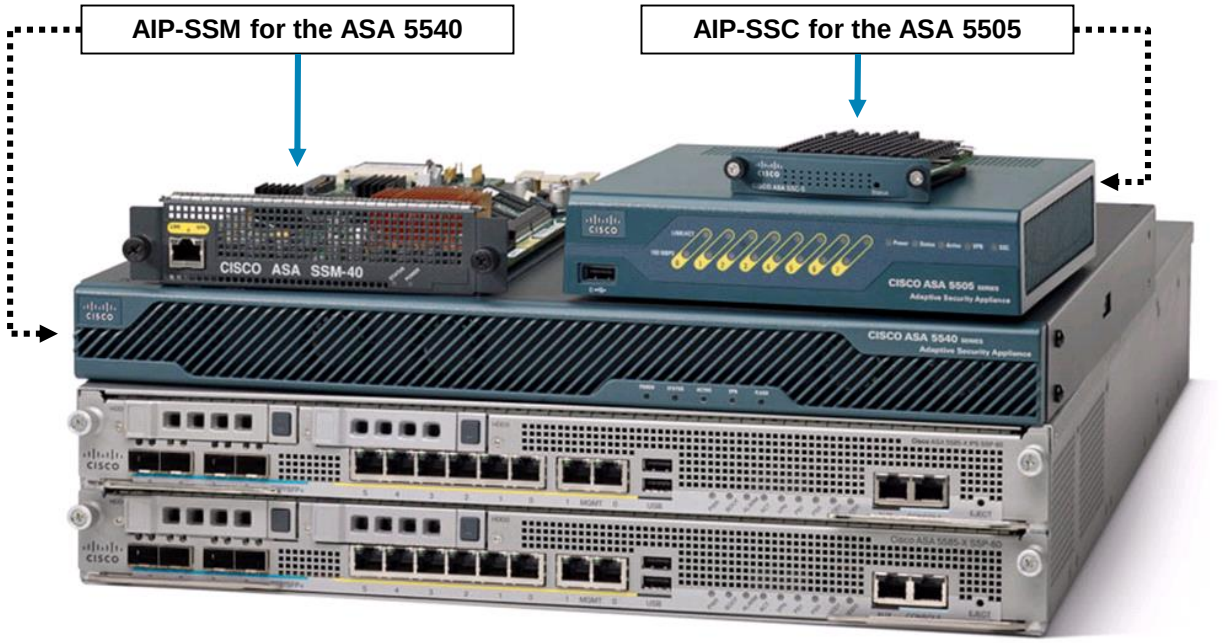
# Advanced ASA Feature: Identity Firewall

- A Client attempting to access Server resources must first be authenticated using the Microsoft Active Directory



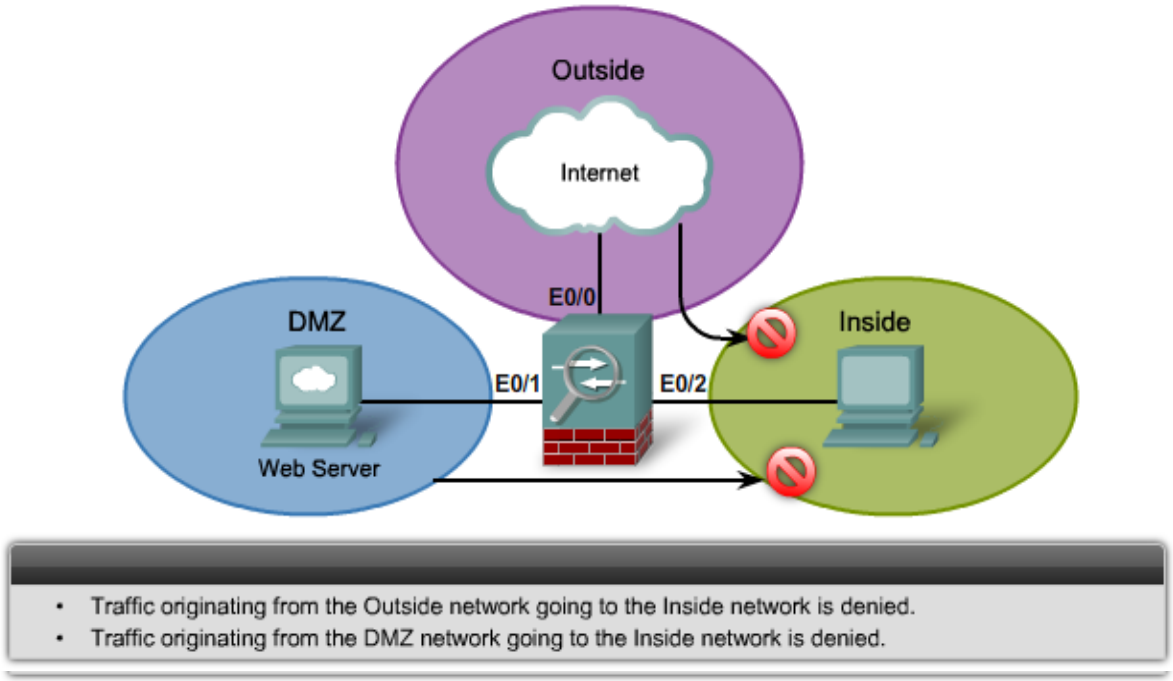
# Advanced ASA Feature: Identity Firewall

- Full IPS features are provided by integrating special hardware modules with the ASA architecture.
  - The Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) is for the ASA 5540 device.
  - The Cisco Advanced Inspection and Prevention Security Services Card (AIP-SSC) is for the ASA 5505 device.

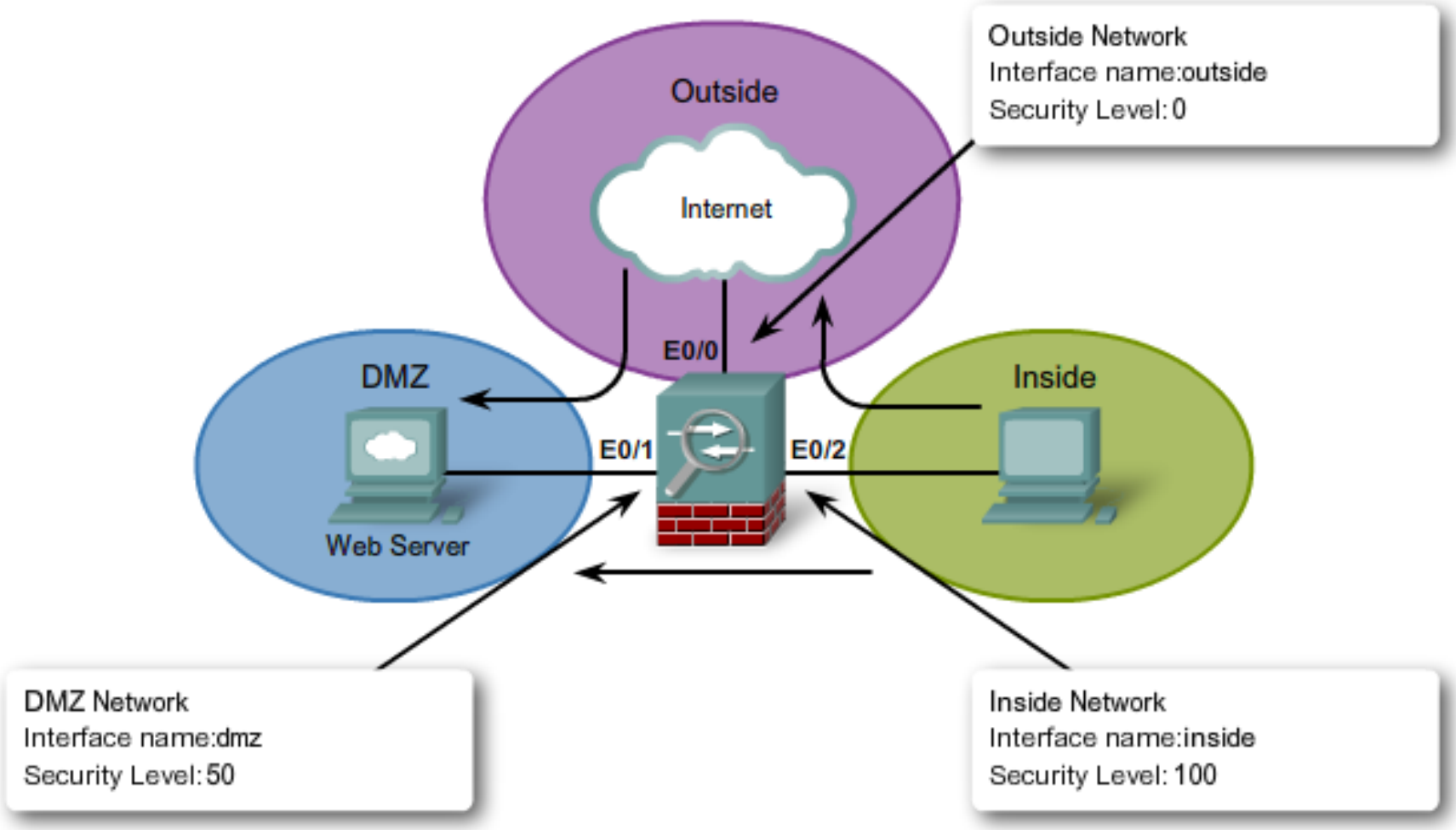


# Networks on a Firewall

- **Inside network**
  - Network that is protected and behind the firewall.
- **DMZ**
  - Demilitarized zone, while protected by the firewall, limited access is allowed to outside users.
- **Outside network**
  - Network that is outside the protection of the firewall.



# Security Levels

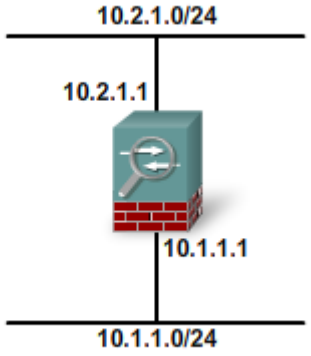


# Routed vs. Transparent Mode

- An ASA device can operate in one of two modes:

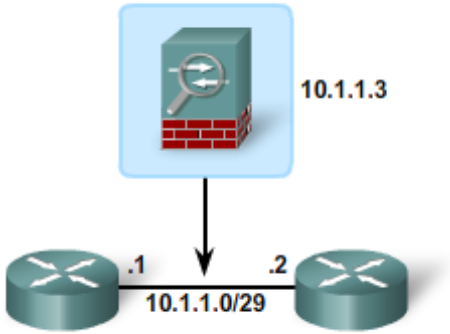
**Routed Mode**

- Is the traditional firewall deployment mode.
- Separates two Layer 3 domains.
- Provides a NAT boundary.
- Applies policy to flows as they transit the firewall.




**Transparent Mode**

- Operates at Layer 2.
- Integrates with existing networks without the need for re-addressing.
- Simplifies internal firewalling and network segmentation.



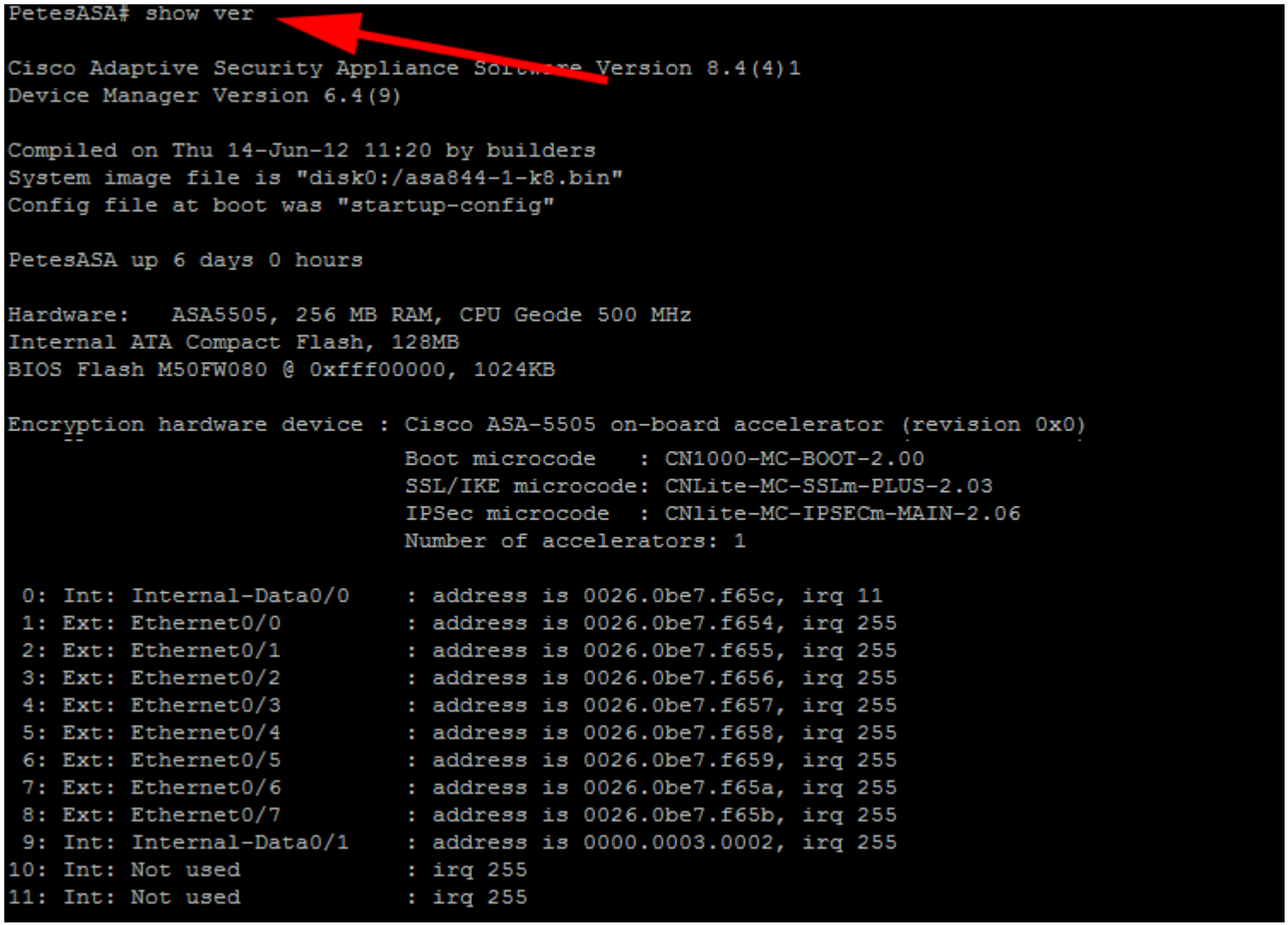
# ASA Licenses

- ASA appliances come pre-installed with either a:
  - Base license
  - Security Plus license
- To verify the license information on an ASA device, use the commands:

```
show version
show activation-key
```

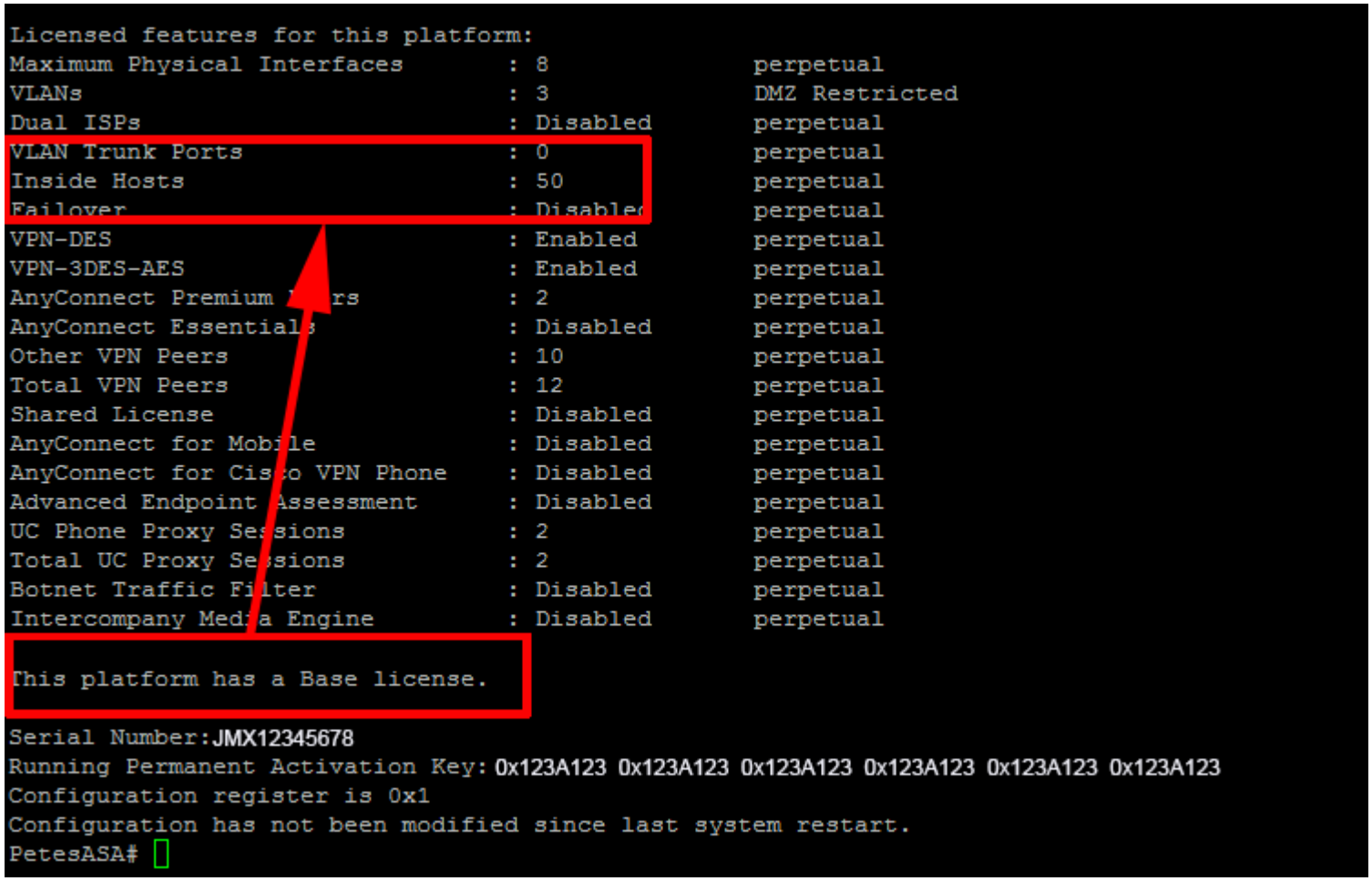
- Combining additional licenses to the pre-installed licenses creates a permanent license
  - The permanent license is activated by installing a permanent activation key using the **`activation-key`** command
  - Only one permanent license key can be installed and once it is installed, it is referred to as the running license

# Applying Key ①




http://www.petenetlive.com/KB/Media/0000701/00004.png

# Applying Key ②




http://www.petenetlive.com/KB/Media/0000701/00004.png

# ASA 5505 Base License

AEOS Approaching End Of Sale

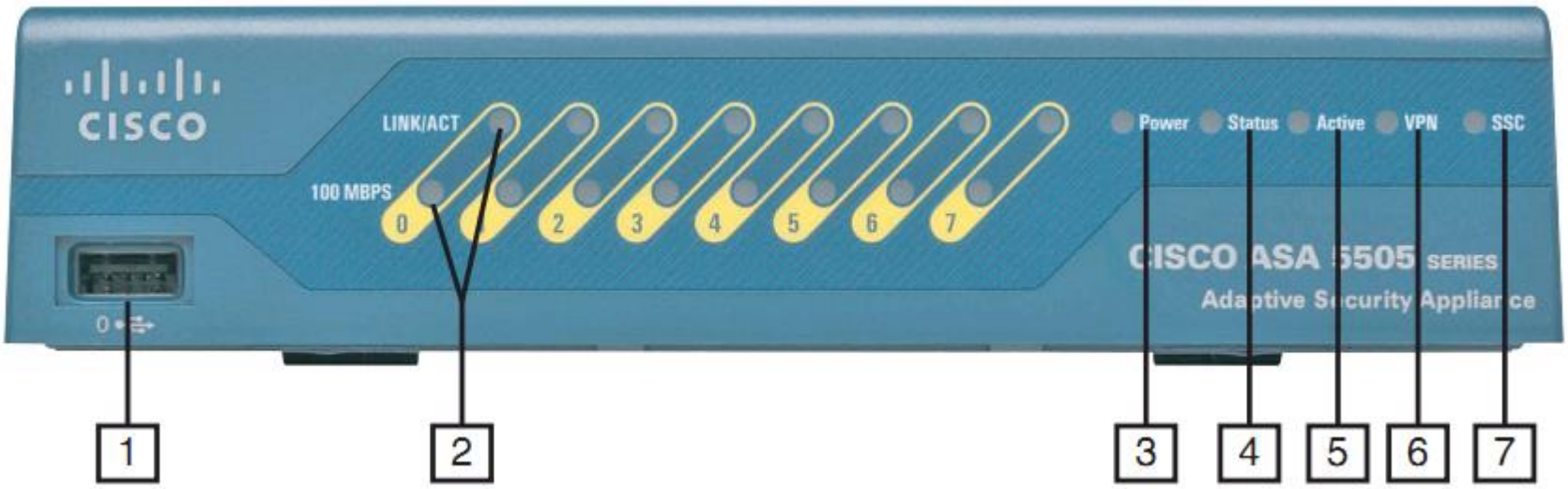
| | 5505 | | 5510 | | 5512-X | | 5585-X SSP-10 | | 5585-X SSP-20 | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Feature** | **Base** | **Sec Plus** | **Base** | **Sec Plus** | **Base** | **Sec Plus** | **Base** | **Sec Plus** | **Base** | **Sec Plus** |
| IPSec Peers | 10 | 25 | 250 | 250 | 250 | 250 | 5K | 5K | 10K | 10K |
| Concurrent Connections | 10K | 25K | 50K | 130K | 100K | 250K | 1M | 1M | 2M | 2M |
| VLANs | 3 Routed* 2 xparent* | 20 Routed* 3 xparent* | 50 | 100 | 50 | 100 | 1024 | 1024 | 1024 | 1024 |
| Trunking | No | Yes (8) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Contexts | No | No | No | 2 | No | 2 | 100 | 100 | 250 | 250 |
| Failover | No | Yes, Active/Stdby not stateful | No | Yes AS/AA | No | Yes AS/AA | Yes AS/AA | Yes AS/AA | Yes AS/AA | Yes AS/AA |
| Interface Speeds | 8 FE | 8 FE | 5 FE | 3 FE, 2 GE | 6 GE | 6 GE | 10GE Disabled | 10GE Enabled | 10GE Disabled | 10GE Enabled |
| Interfaces of all Types, Max | 52 | 120 | 240 | 440 | 328 | 528 | 4176 | 4176 | 4176 | 4176 |
| VPN Load Balancing | No | No | No | Yes | No | Yes | Yes | Yes | Yes | Yes |
| Required Version | | 7.2.(2)+ | | 7.2.(3)+ | | 8.6(1)+ | | 8.2(4) | | 8.2(3) |

http://www.tunnelsup.com/images/asasecplus.png

# ASA 5505 Base License

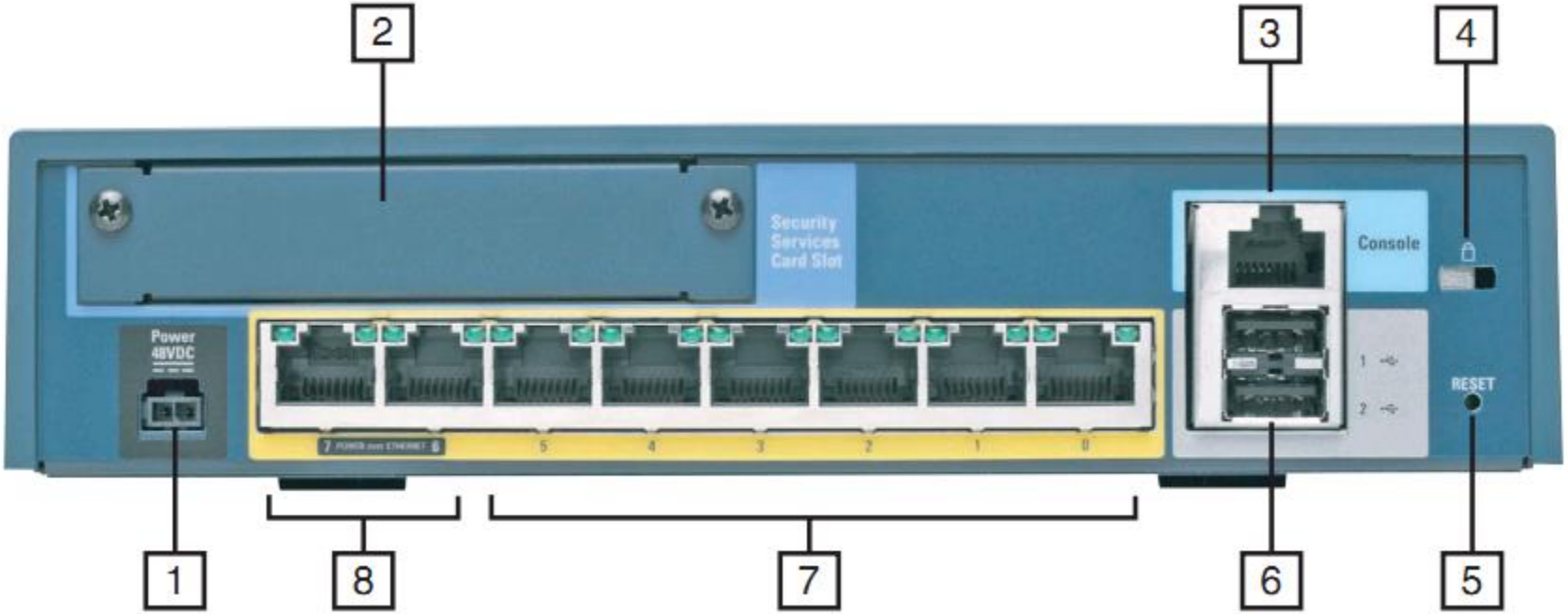
```
ciscoasa# show version

<Output omitted>

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 10             perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

Serial Number: JMX15364077
Running Permanent Activation Key: 0x970bc671 0x305fc569 0x70d21158 0xb6ec2ca8 0x8a003fb9
Configuration register is 0x41 (will be 0x1 at next reload)
Configuration last modified by enable_15 at 10:03:12.749 UTC Fri Sep 23 2011
ciscoasa#
```

# ASA 5505 Front Panel



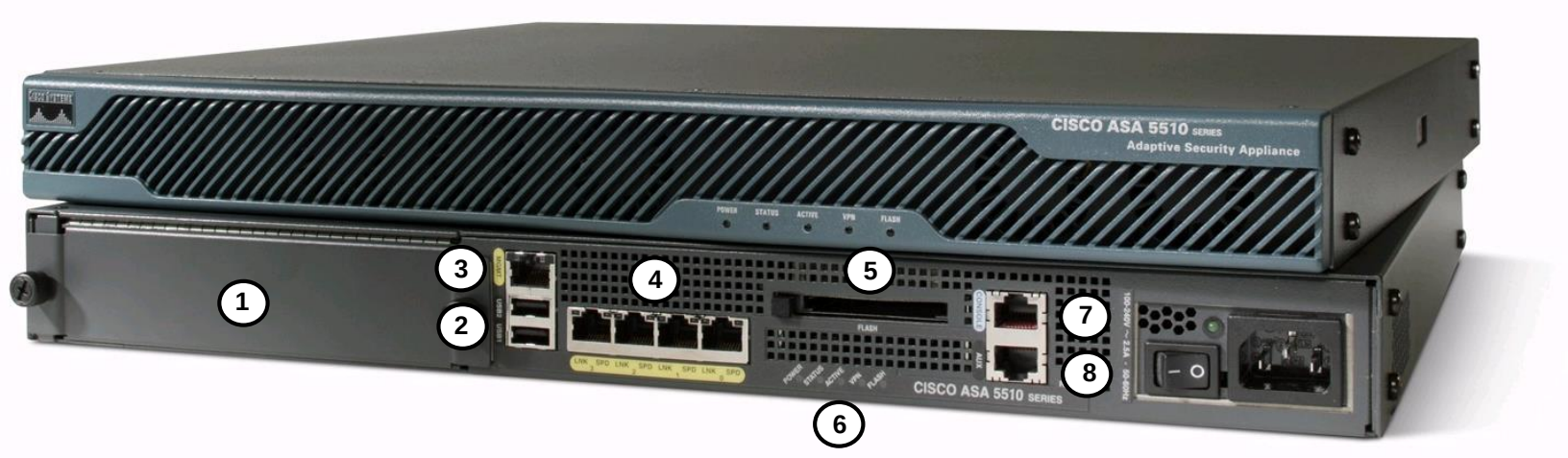

| | | | |
|---|---|---|---|
| 1 | USB 2.0 interface | 5 | Active LED |
| 2 | Speed and Link Activity LEDs | 6 | VPN LED |
| 3 | Power LED | 7 | Security Service Card (SSC) LED |
| 4 | Status LED | | |

# ASA 5505 Back Panel




| | | | |
|---|---|---|---|
| 1 | Power connector (48 VDC) | 5 | Reset button |
| 2 | SSC slot | 6 | Two USB 2.0 ports |
| 3 | Serial console port | 7 | 10/100 Ethernet switch (ports 0 – 5) |
| 4 | Lock slot | 8 | 10/100 Power over Ethernet (PoE) switch ports (ports 6 and 7) |

# ASA 5510 Back Panel




| | | | |
|---|---|---|---|
| 1 | Security Services Module (SSM) slot | 5 | Flash card slot |
| 2 | Two USB 2.0 ports | 6 | Power, status, active, VPN, and flash LED indicators |
| 3 | Out of band (OOB) management interface | 7 | Serial console port |
| 4 | 4 Fast Ethernet interfaces | | Auxiliary port |

# Configure Basic Settings

# ASA Command Line Interface (CLI)

- The ASA CLI is a proprietary OS which has a similar look and feel to the router IOS
- Like a Cisco IOS router, the ASA recognizes the following:
  - Abbreviation of commands and keywords
  - Using the Tab key to complete a partial command
  - Using the help key (**?**) after a command to view additional syntax
- Unlike an ISR, the ASA:
  - Can execute any ASA CLI command regardless of the current configuration mode prompt and does not require or recognize the **do** IOS CLI command
  - Can provide additional help listing a brief command description and syntax by using the EXEC command **help** followed by the CLI command (e.g., **help reload**)
  - Interrupts **show** command output by simply using the letter **Q**
    - Unlike the **Ctrl+C** (**^C**) IOS CLI key sequence

# Common IOS and Equivalent Commands

| IOS Router Command | Equivalent ASA Command |
|---|---|
| **enable secret** *password* | **enable password** *password* |
| **line con 0**<br>**password** *password*<br>**login** | **passwd** *password* |
| **ip route** | **route outside** |
| **show ip interfaces brief** | **show interface ip brief** |
| **show ip route** | **show route** |
| **show vlan** | **show switch vlan** |
| **show ip nat translations** | **show xlate** |
| **copy running-config startup-config** | **write** [**memory**] |
| **erase startup-config** | **write erase** |

# ASA Factory Default Configurations

```
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
```

→ Default management settings.

```
interface Ethernet0/0
 switchport access vlan 2
 no shut
!
```

→ The outside interface is configured.

```
interface Ethernet0/1
 no shut
```

→ E0/1 is configured as the outside interface. E0/2 – E0/7 are not configured and are all shutdown.

**<Output omitted>**

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
```

→ Inside network VLAN (VLAN 1) is configured with name (inside), security level (100) and internal IP address.

```
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
```

→ Outside network VLAN (VLAN 2) is configured with name (outside), security level (0) and to acquire its IP address and default route from the upstream device.

**<Output Omitted>**

```
object network obj_any
 nat (inside,outside) dynamic interface
```

→ PAT is configured so that inside addresses are translated using the outside interface IP address.

**<Output Omitted>**

```
http server enable
http 192.168.1.0 255.255.255.0 inside
```

→ HTTP access for ASDM is configured.

**<Output Omitted>**

```
dhcpd auto_config outside
!
```

→ The outside is to discover its WINS, DNS, and domain information from the upstream devices.

```
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
```

→ DHCP Server settings for inside hosts.

**<Output Omitted>**

# CLI Setup Initialization Wizard

- If the default configuration is not required, erase and reload the ASA using the **`write erase`** and **`reload`** commands
  - Note that the ASA does not recognize the **`erase startup-config`** command
- Once rebooted, the CLI Setup Initialization wizard prompts to pre-configure the firewall appliance using interactive prompts
  - Entering “no” cancels the wizard and the ASA will display its default prompt
- The Setup Initialization wizard is an optional method for initially configuring an ASA
  - It also provides most of the settings needed to access the ASA using ASDM

# CLI Setup Initialization Wizard

- The CLI Setup Initialization wizard configures the following:
  - Firewall mode
  - Enable password
  - Enable password recovery
  - Time and date settings
  - Inside IP address and mask
  - ASA device host name
  - Domain name

# CLI Setup Initialization Wizard

```
<Bootup output omitted>

Pre-configure Firewall now through interactive prompts [yes]?
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2012]:
  Month [Oct]:
  Day [3]:
  Time [03:44:47]: 6:49:00
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 6:49:00 Oct 3 2011
Firewall Mode: Routed
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: CCNAS-ASA
Domain name: ccnasecurity.com
IP address of host running Device Manager: 192.168.1.2

Use this configuration and write to flash? yes
INFO: Security level for "management" set to 0 by default.
WARNING: http server is not yet enabled to allow ASDM access.
Cryptochecksum: ba17fd17 c28f2342 f92f2975 1e1e5112

2070 bytes copied in 0.910 secs

Type help or '?' for a list of available commands.
CCNAS-ASA>
```

Default values are displayed in brackets [ ].
To accept the default input, press Enter.

# Configure Basic Settings

- Basic management settings are configured in global configuration mode

- The first time global configuration mode is accessed, a message prompting you to enable the Smart Call Home feature appears
  - This feature offers proactive diagnostics and real-time alerts on select Cisco devices, which provides higher network availability and increased operational efficiency
  - To participate, a CCO ID is required and the ASA device must be registered under a Cisco SMARTnet Service contract

# Steps to Configure Basic Settings

1) Configure basic management settings
   - (i.e., hostname, domain name, and enable password.)
2) Enable the master passphrase
3) Configure the Inside and Outside SVIs (on an ASA 5505)
4) Assign Layer 2 ports to VLANs (on an ASA 5505)
5) Enable Telnet, SSH, and HTTPS access
6) Configure time services
7) Configure a default route

# 1 - Configure Basic Management Settings

- In global configuration mode, configure the ASA host name, domain name, and privileged EXEC mode password using the following commands:
  - **hostname** *name* - Changes the name of the ASA
  - **domain-name** *name* - Changes the domain name
  - **enable password** *password* - Configures the privileged EXEC mode password
    - Note that there is no secret option
  - **passwd** *password* - Configures the Telnet / SSH password

```
ciscoasa# conf t
ciscoasa(config)# hostname CCNAS-ASA
CCNAS-ASA(config)# domain-name ccnasecurity.com
CCNAS-ASA(config)# enable password class
CCNAS-ASA(config)# passwd cisco
```

# 2 - Enable the Master Passphrase

- A master passphrase securely stores plaintext passwords in encrypted format
  - Similar to the IOS **`service password-encryption`** command
- To configure a master passphrase, use the following commands:
  - **`key config-key password-encryption`** [*new-passphrase* [*old-passphrase*]]
    - Creates or changes an existing master passphrase (8 to 128 characters in length)
  - **`password encryption aes`**
    - Enables password encryption

```
CCNAS-ASA(config)# key config-key password-encryption cisco123
CCNAS-ASA(config)# password encryption aes
```

# 3 - Configure Inside and Outside SVIs

- On ASA 5510 and higher, routed interfaces are configured with IP configurations.
- However, the ASA 5505 has an integrated 8 port Layer 2 switch and therefore IP configurations are accomplished by:
  - Configuring the inside and outside switched virtual interfaces (SVIs) by assigning interface names, security level, and IP address.
  - Assigning Layer 2 ports to the inside and outside SVI VLANs.

# 3 - Configure Inside and Outside SVIs

- Use the following commands to configure the inside and outside SVI VLAN interfaces:
  - **interface vlan** *vlan-number* - Creates a switch virtual interface (SVI)
  - **nameif** {**inside** | **outside** | *name*} - Assigns an interface name

```
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)# security-level 100
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# exit
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)# security-level 0
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# exit
```

# 3 - Configure Inside and Outside SVIs

- Optionally, instead of manually configuring an IP address, the interface could also be configured as a:
  - DHCP client using the **`ip address dhcp [setroute]`** command
  - PPPoE client using the **`ip address pppoe [setroute]`** command

# 3 - Configure Inside and Outside SVIs

- An ASA 5505 with the Security Plus License automatically supports the creation of additional VLANs to create other zones such as a DMZ zone.
- However, an ASA 5505 with a Basic License only supports a third “restricted" SVI
  - This SVI is limited from initiating contact to another specified VLAN
- The following command must be configured to support the third restricted VLAN SVI on an ASA 5505 with a Base License:
  - **`no forward interface vlan`** *`vlan-id`*
    - *`vlan-id`* specifies the VLAN to which this interface cannot initiate traffic
  - Configure this command only once the inside and outside VLAN interfaces are configured
- The new SVI must also be named, assigned a security level value, and IP address

# 4 - Assign Layer 2 ports to VLANs

- The Layer 2 ports must be assigned to a VLAN
  - By default, all ports are members of VLAN 1
- Use the following commands to change the VLAN assignment:
  - **`interface`** *`interface number`* – Enter interface configuration mode
  - **`switchport access vlan`** *`vlan-id`* – Change the VLAN assignment

```
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)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shut
CCNAS-ASA(config-if)# exit
```

# Verify SVI and Interface Settings

```
CCNAS-ASA# show switch vlan
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    inside                              up        Et0/1, Et0/2, Et0/3, Et0/4
                                                   Et0/5, Et0/6, Et0/7
2    outside                             up        Et0/0
CCNAS-ASA#
CCNAS-ASA# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  up                    up
Ethernet0/1                unassigned      YES unset  up                    up
Ethernet0/2                unassigned      YES unset  administratively down up
Ethernet0/3                unassigned      YES unset  administratively down up
Ethernet0/4                unassigned      YES unset  administratively down down
Ethernet0/5                unassigned      YES unset  administratively down down
Ethernet0/6                unassigned      YES unset  administratively down down
Ethernet0/7                unassigned      YES unset  administratively down down
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Vlan1                      192.168.1.1     YES manual up                    up
Vlan2                      209.156.200.226 YES manual up                    up
Virtual0                   127.0.0.1       YES unset  up                    up
CCNAS-ASA#
```

# 5 - Enable Telnet, SSH, and HTTPS Access

- Enable Telnet access (if required)
  - Telnet does not work on security-level 0 interface
  - SSH is recommended instead of Telnet
- Although simple authentication is provided using the **passwd** command, securing Telnet access using AAA authentication and the local database is recommended.
- Use the following commands to enable AAA authentication:
  - **username** *name* **password** *password*
  - **aaa authentication** {**telnet** | **ssh**} **console** {**LOCAL** | *TACACS-server* | *RADIUS-server*}
  - **telnet** *host-ip host-mask* **inside**
  - **telnet timeout** *minutes*

```
CCNAS-ASA(config)# username admin password class
CCNAS-ASA(config)# aaa authentication telnet console LOCAL
CCNAS-ASA(config)# telnet 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# telnet timeout 10
```

# 5 - Enable Telnet, SSH, and HTTPS Access

- Similarly configured as Telnet but requires:
  - AAA authentication to be enabled
  - RSA crypto key generated
- To verify the SSH configuration, use the **show ssh** command

```
CCNAS-ASA(config)# username admin password class
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# crypto key generate rsa modulus 2048
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
CCNAS-ASA(config)# ssh 192.168.1.3 255.255.255.255 inside
CCNAS-ASA(config)# ssh timeout 10
CCNAS-ASA(config)# exit
CCNAS-ASA#
CCNAS-ASA# show ssh
Timeout: 10 minutes
Versions allowed: 1 and 2
192.168.1.3 255.255.255.255 inside
```

# 5 - Enable Telnet, SSH, and HTTPS Access

- HTTPS is required for ASDM.
- To remove and disable the ASA HTTP server service, use the **clear configure http** global configuration command.

```
CCNAS-ASA(config)# http server enable
CCNAS-ASA(config)# http 192.168.1.3 255.255.255.255 inside
```

# 6 - Configure Time Services

- Time setting can be set by configuring the local system time.
- This is not the recommended method.
- Use an authoritative time source and NTP.

```
CCNAS-ASA# clock set 8:05:00 3 OCT 2011
```

# 6 - Configure NTP Time Services

- Network Time Protocol (NTP) services can be configured using the following commands:
  - **ntp server** *ip-address* - Identifies the NTP server address.
  - **ntp authentication-key** - Configures the authentication key and password.
  - **ntp trusted-key** *value* - Identifies which configured key is to be trusted.
  - **ntp authenticate** - Enables NTP authentication.
- To verify the NTP configuration and status, use the **show ntp status** and **show ntp associations** commands

```
CCNAS-ASA(config)# ntp server 10.10.10.1
CCNAS-ASA(config)# ntp authentication-key 1 md5 cisco123
CCNAS-ASA(config)# ntp trusted-key 1
CCNAS-ASA(config)# ntp authenticate
```

# 7 - Configure a Default Route

- If an ASA an configured as a DHCP or PPPoE client, then it most probably is getting its default route provided by the upstream device.
  - Otherwise, the ASA will require a default static route to be configured.
  - To verify the route entry, use the **`show route`** command.

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    209.165.200.224 255.255.255.248 is directly connected, outside
C    192.168.1.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
CCNAS-ASA(config)#
```

# Verify Basic Settings

```
CCNAS-ASA# show switch vlan
VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------------------------
1    inside                          up        Et0/1, Et0/2, Et0/3, Et0/4
                                               Et0/5, Et0/6, Et0/7
2    outside                         up        Et0/0
CCNAS-ASA#
CCNAS-ASA# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES unset  up                    up
Ethernet0/1                unassigned      YES unset  up                    up
Ethernet0/2                unassigned      YES unset  administratively down up
Ethernet0/3                unassigned      YES unset  administratively down up
Ethernet0/4                unassigned      YES unset  administratively down down
Ethernet0/5                unassigned      YES unset  administratively down down
Ethernet0/6                unassigned      YES unset  administratively down down
Ethernet0/7                unassigned      YES unset  administratively down down
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Vlan1                      192.168.1.1     YES manual up                    up
Vlan2                      209.156.200.226 YES manual up                    up
Virtual0                   127.0.0.1       YES unset  up                    up
CCNAS-ASA#
```

# DHCP Server Services

- To enable an ASA as a DHCP server and provide DHCP services to inside hosts, configure the following:
  - **dhcpd enable inside** - Enables the DHCP server service (daemon) on the inside interface of the ASA.
  - **dhcpd address** *[start-of-pool]-[end-of-pool]* **inside**
    - Defines the pool of IP addresses and assigns the pool to inside users.
    - Notice that the start and end of pools are separated by a hyphen.
  - The ASA 5505 Base license is a 10-user license and therefore the maximum number of DHCP clients supported is 32

```
CCNAS-ASA# conf t
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as:
192.168.1.10-192.168.1.41
CCNAS-ASA(config)# dhcpd address 192.168.1.10-192.168.1.41 inside
CCNAS-ASA(config)# dhcpd enable inside
CCNAS-ASA(config)# dhcpd auto_config outside
```

# Verify DHCP Server Services

```
CCNAS-ASA# show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

CCNAS-ASA# show dhcpd state
Context  Configured as DHCP Server
Interface inside, Configured for DHCP SERVER
Interface outside, Configured for DHCP CLIENT
CCNAS-ASA# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools         1
Automatic bindings    0
Expired bindings      0
Malformed messages    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          0
DHCPREQUEST           0
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             0
DHCPACK               0
DHCPNAK               0
```

# Introducing ASDM

# Cisco ASDM

- Cisco ASA Security Device Manager (ASDM) is a Java-based GUI tool that facilitates the setup, configuration, monitoring, and troubleshooting of Cisco ASAs
- ASDM is now preloaded in flash memory on any ASA running versions 7.0 and later
- ASDM can be:
  - Run as a Java Web Start application that is dynamically downloaded from the ASA flash allowing an administrator to configure and monitor that ASA device.
  - Downloaded from flash and installed locally on a host as an application allowing an administrator to manage multiple ASA devices.

# Starting ASDM

1) Verify connectivity to the ASA
2) Open a browser and establish a HTTPS connecting to the ASA
3) Choose to:
   - Install ASDM Launcher and Run ASDM
   - Run ASDM
   - Run the Startup wizard
4) Authenticate to ASDM

# Starting ASDM

- Verify connectivity to the ASA
  - You must be initiating the connecting from the identified trusted host in the HTTP basic settings

```
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)#
```

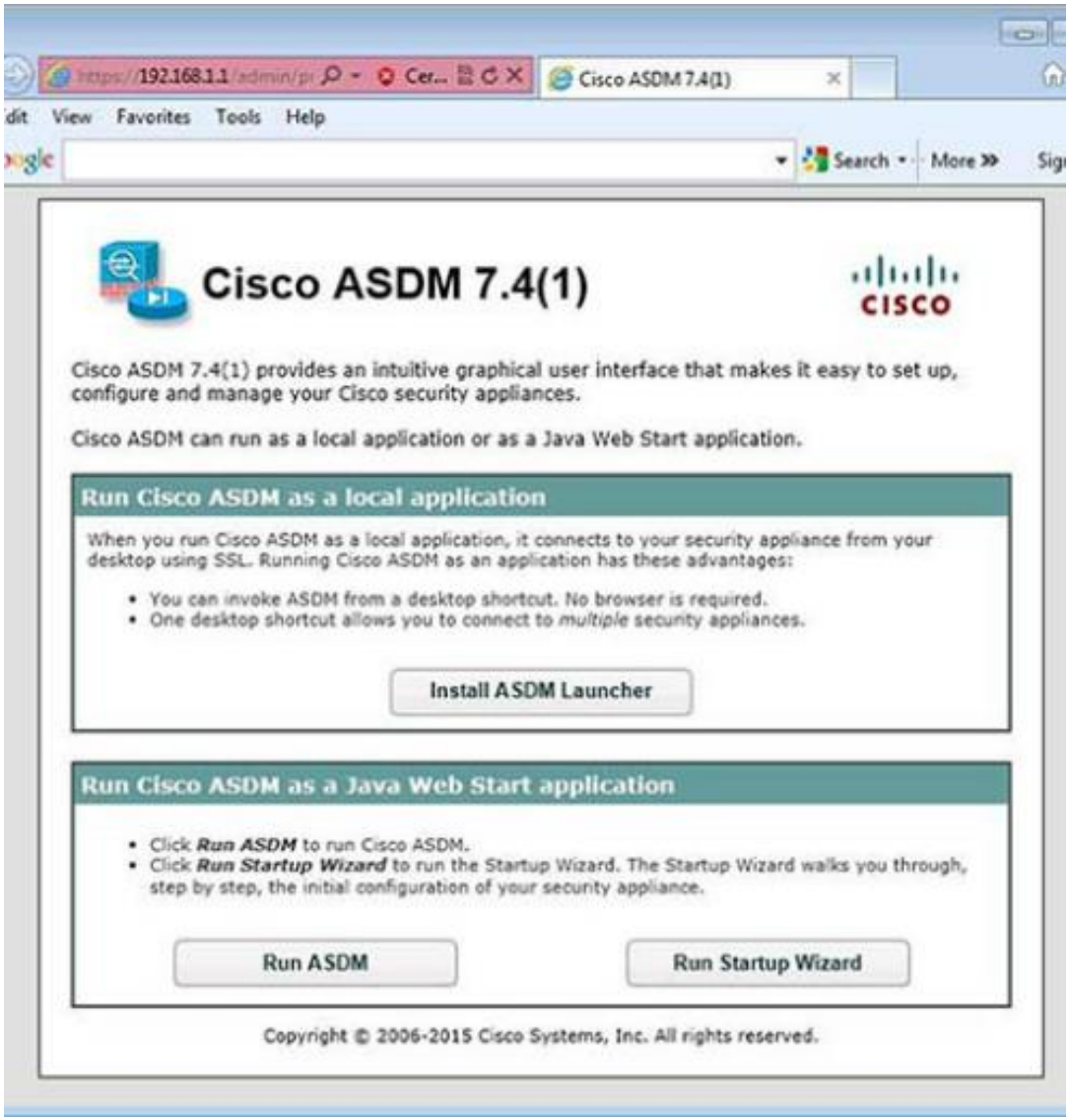
```
ersion 5.1.2600]
 Microsoft Corp.

gs\Netlab>ipconfig

n

 Area Connection:

ific DNS Suffix  . :
  . . . . . . . . . . . : 192.168.1.3
  . . . . . . . . . . . : 255.255.255.0
  . . . . . . . . . . . : 192.168.1.1

gs\Netlab>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms 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 = 6ms, Average = 1ms

C:\Documents and Settings\Netlab>_
```

# Starting ASDM

- Open a browser and establish an SSL connection
  - Click **Yes** to continue and open the ASDM Launch window

# Starting ASDM

- **Install ASDM Launcher and Run ASDM:**
  - Install ASDM locally on the host.
  - The advantage is that ASDM can be used to manage several ASA devices.
- **Run ASDM:**
  - Run ASDM as a Java Web start application.
  - The advantage is that ASDM is not locally installed.
  - An Internet browser is required.
- **Run Startup Wizard:**
  - This choice is similar to the Setup Initialization wizard and provides step-by-step windows to help initially configure the ASA.



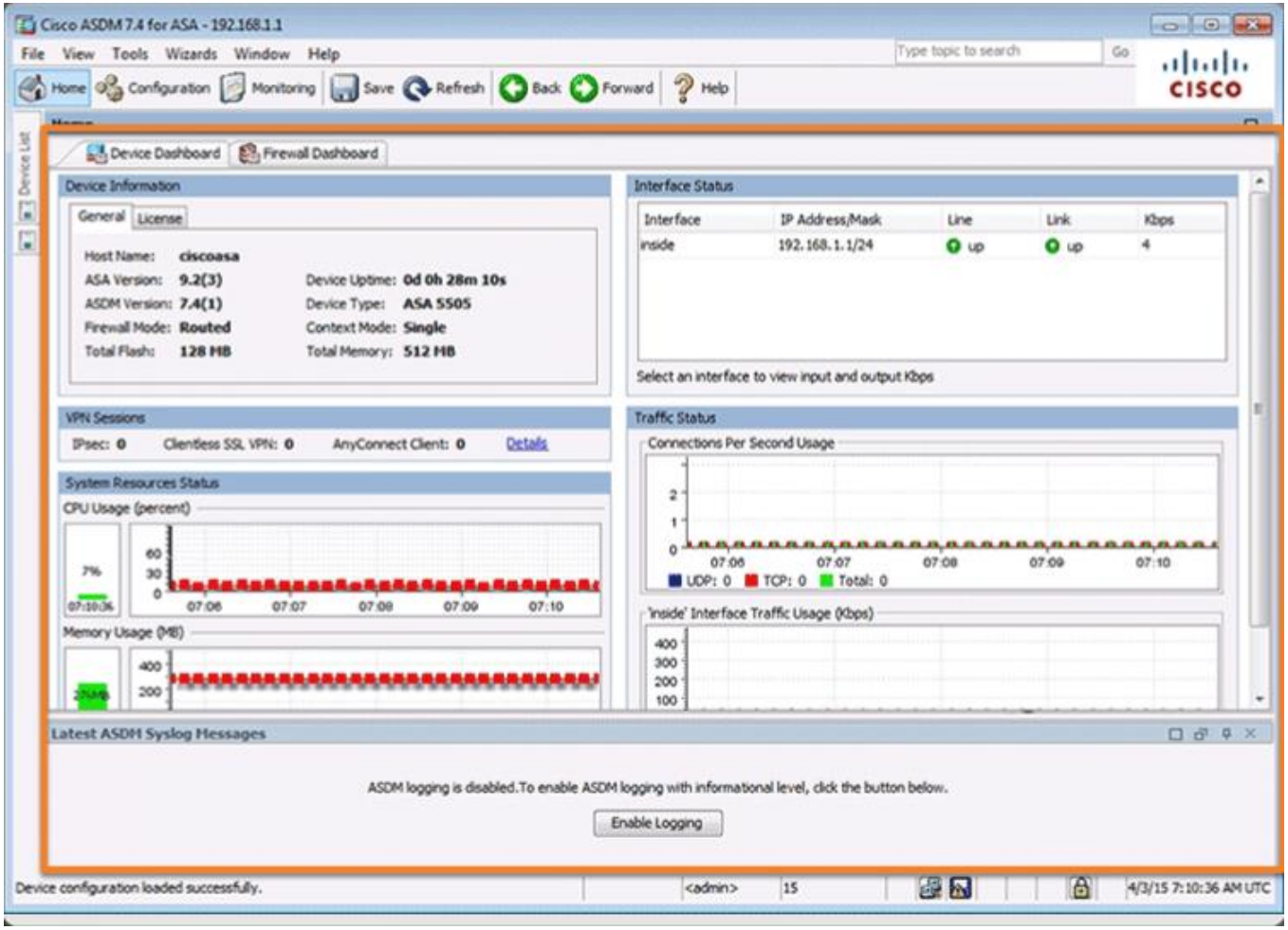
# Starting ASDM

- After choosing **Run ASDM**, authenticate with the ASA.
  - When authentication is successful, the ASDM Home page will be displayed.



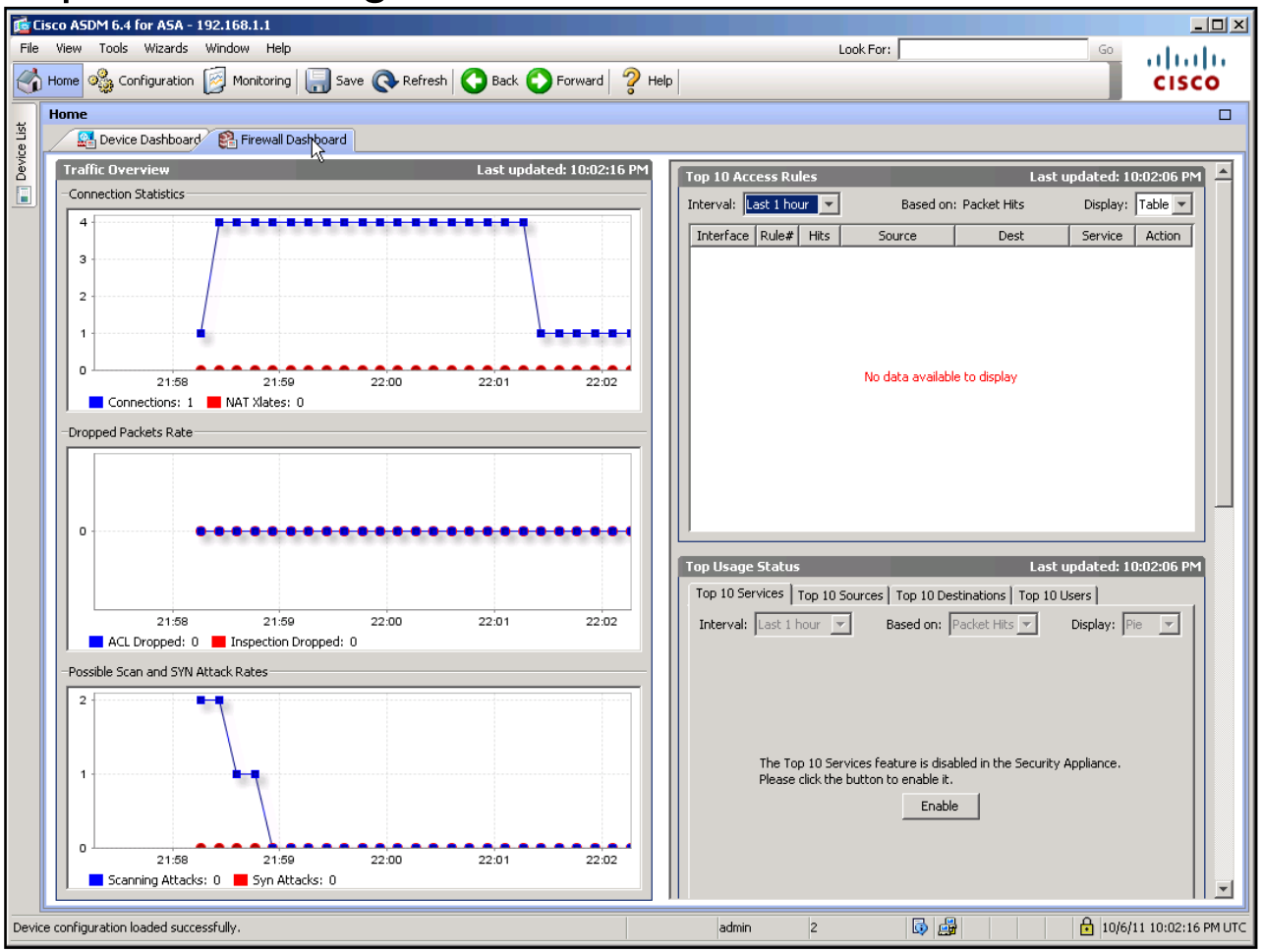
# ASDM Device Dashboard

- The Cisco ASDM Home page displays provides a quick view of the operational status of ASA that is updated every 10 seconds

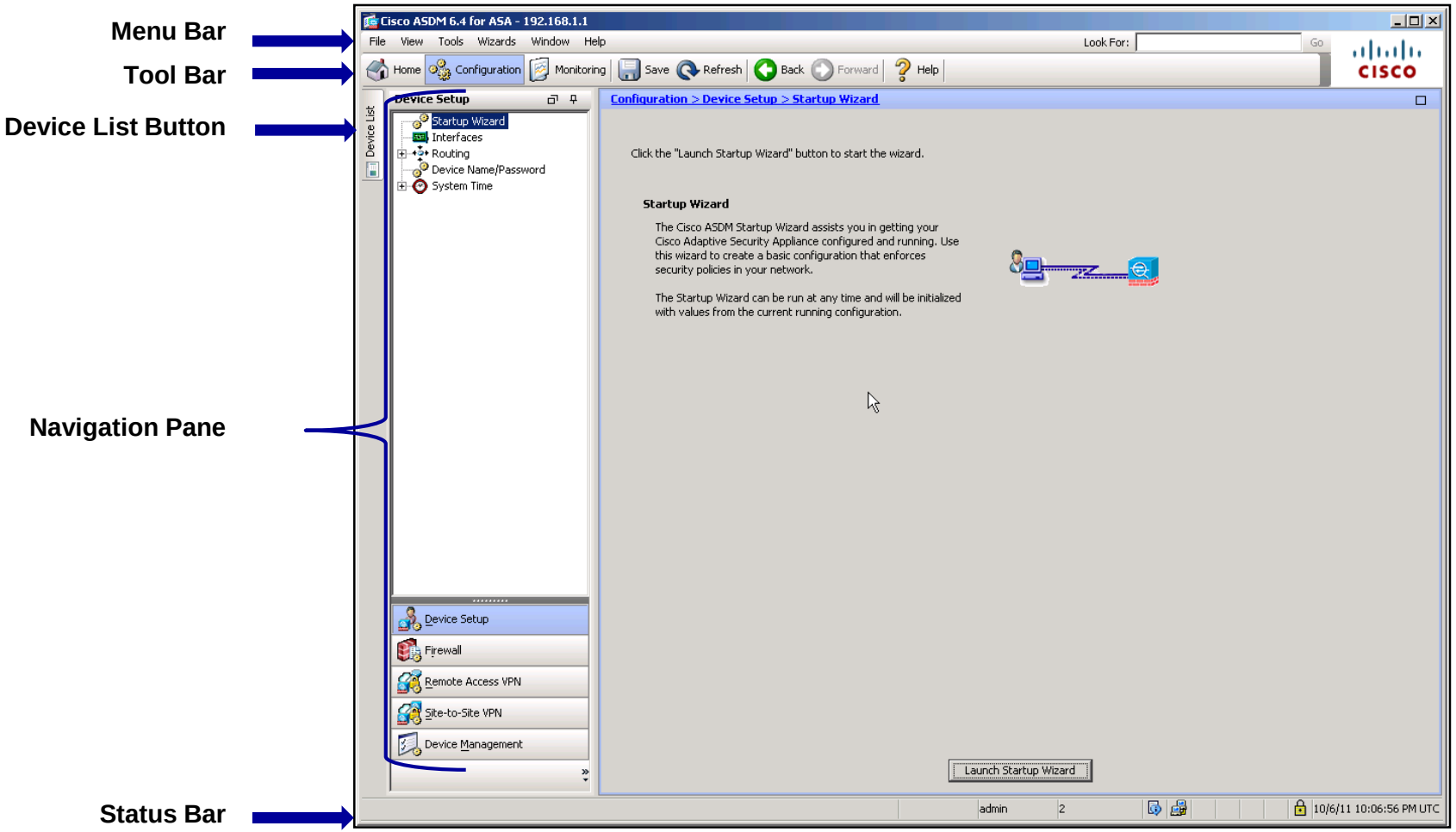


# ASDM Firewall Dashboard

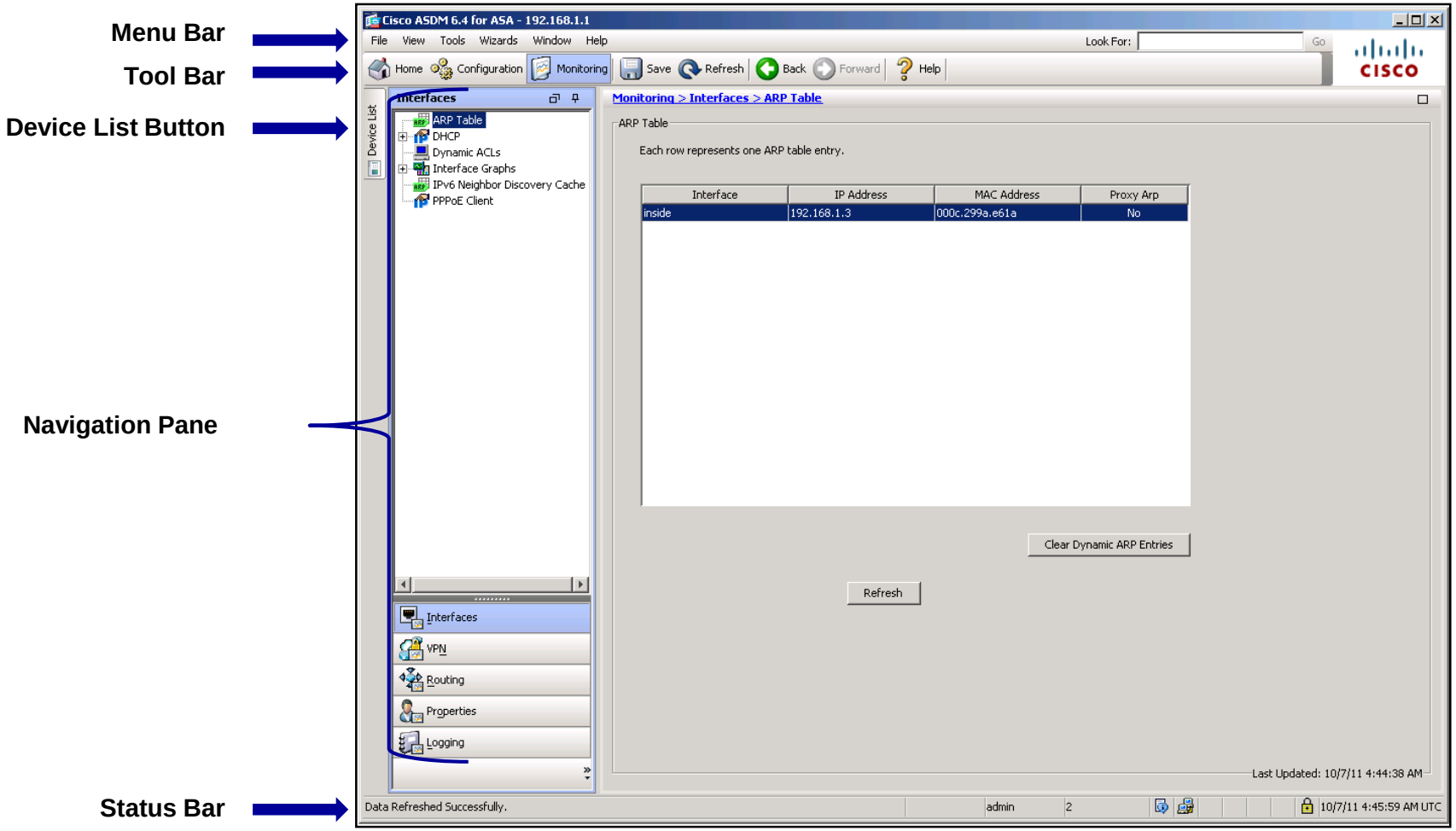
- The Firewall Dashboard provides security related information about traffic that passes through the ASA



# ASDM Configuration View

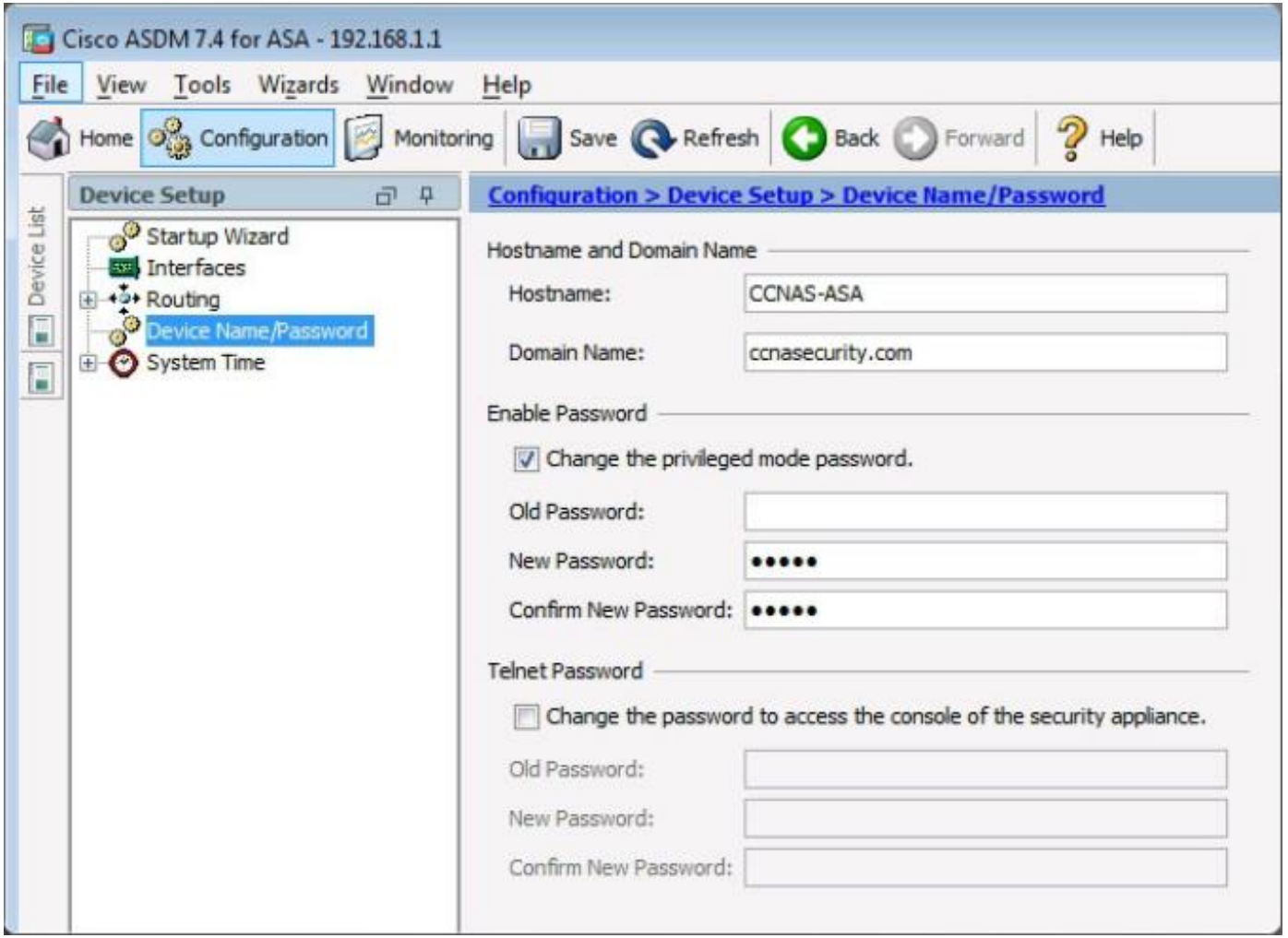


# ASDM Monitoring View



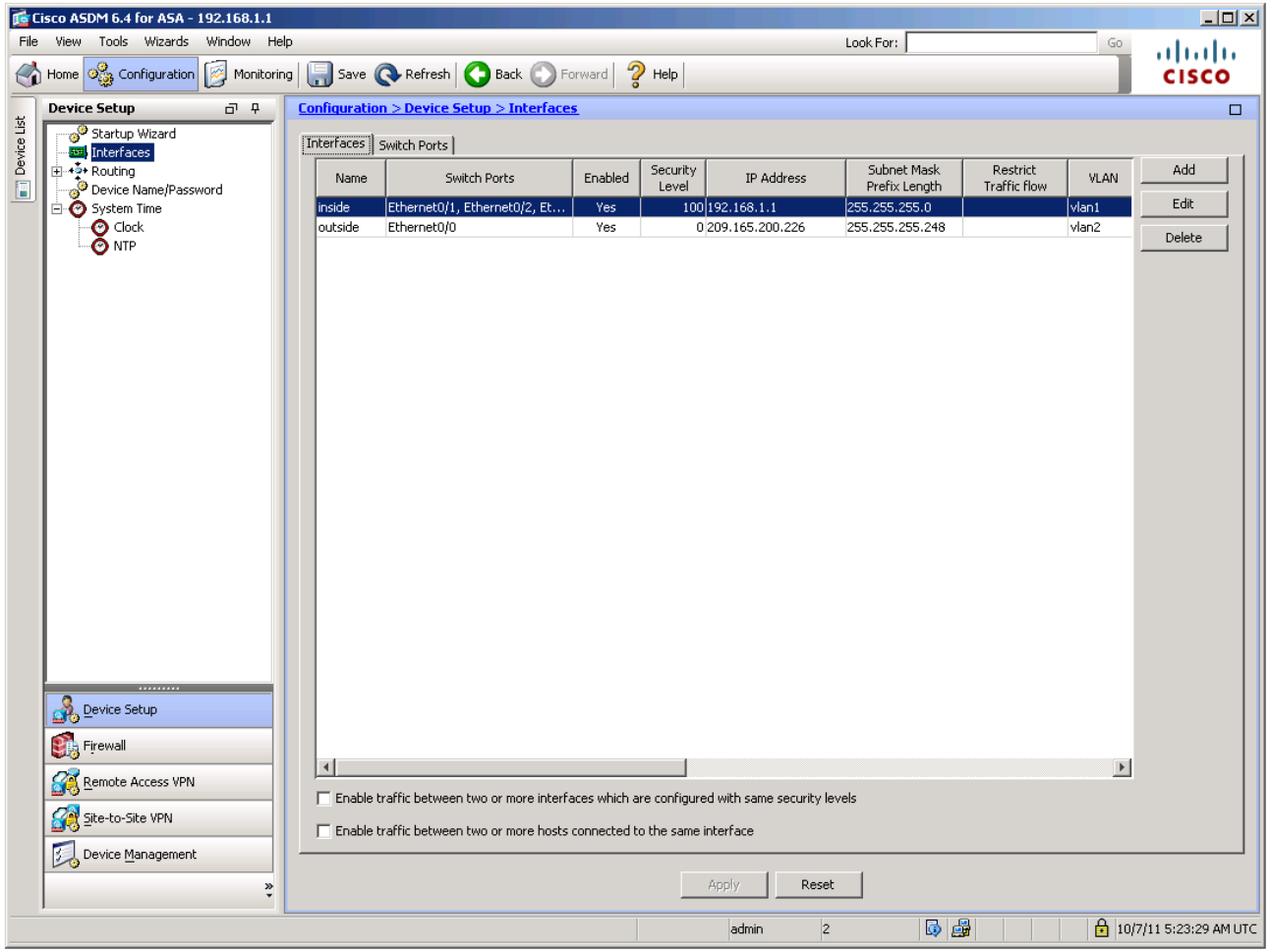
# Configure Hostname and Passwords

- **Configuration > Device Setup > Device Name/Password**



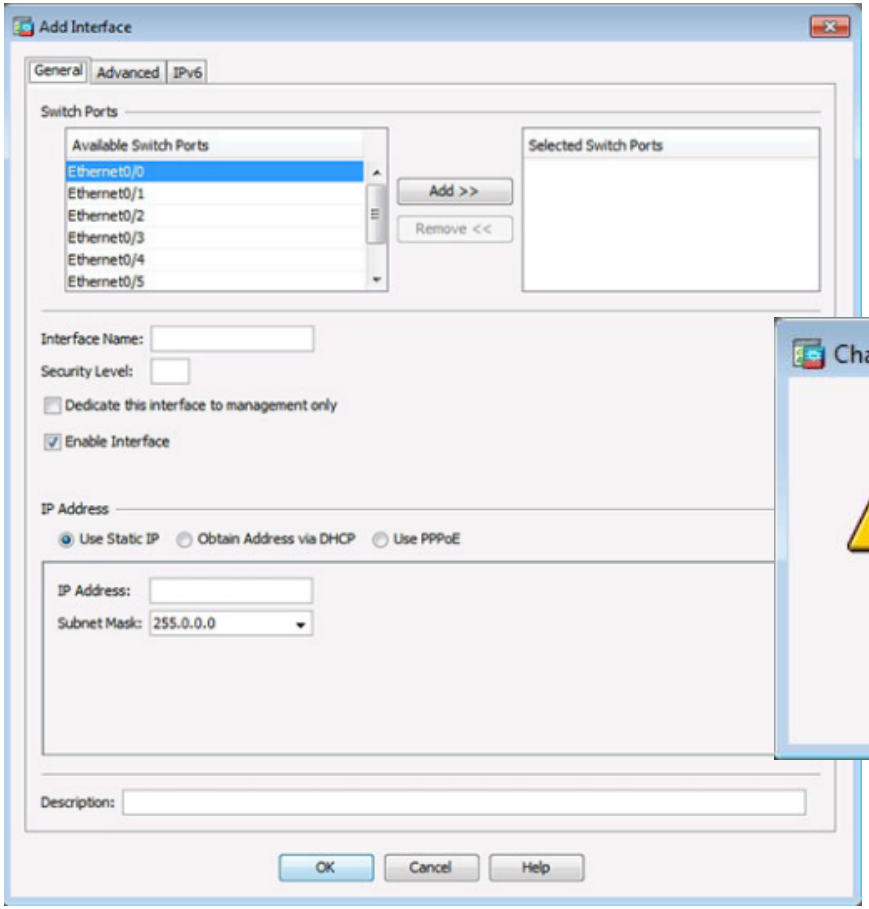
# Interfaces

- **Configuration > Device Setup > Interfaces > Interfaces**

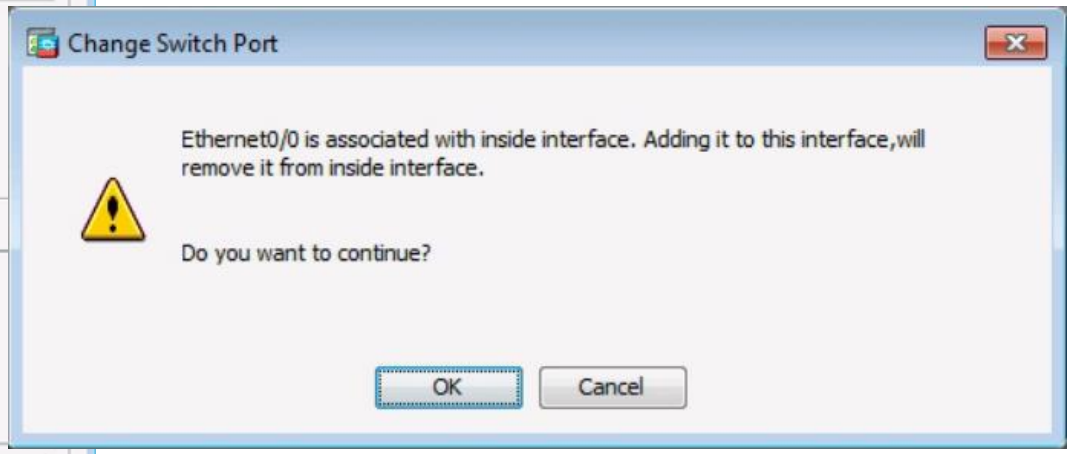


# Configuring Interfaces (Cont.)

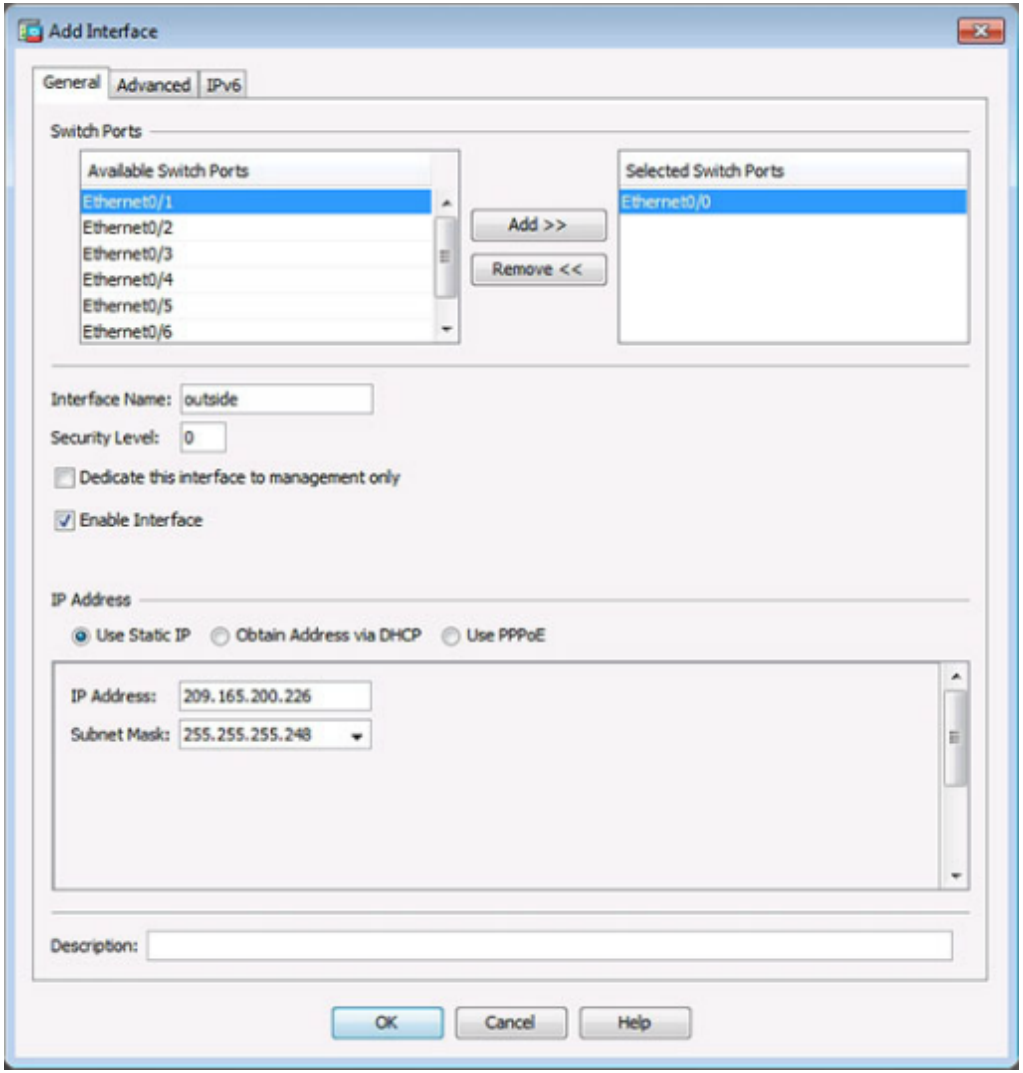
## Adding an Outside Interface




## Change Switch Port Window



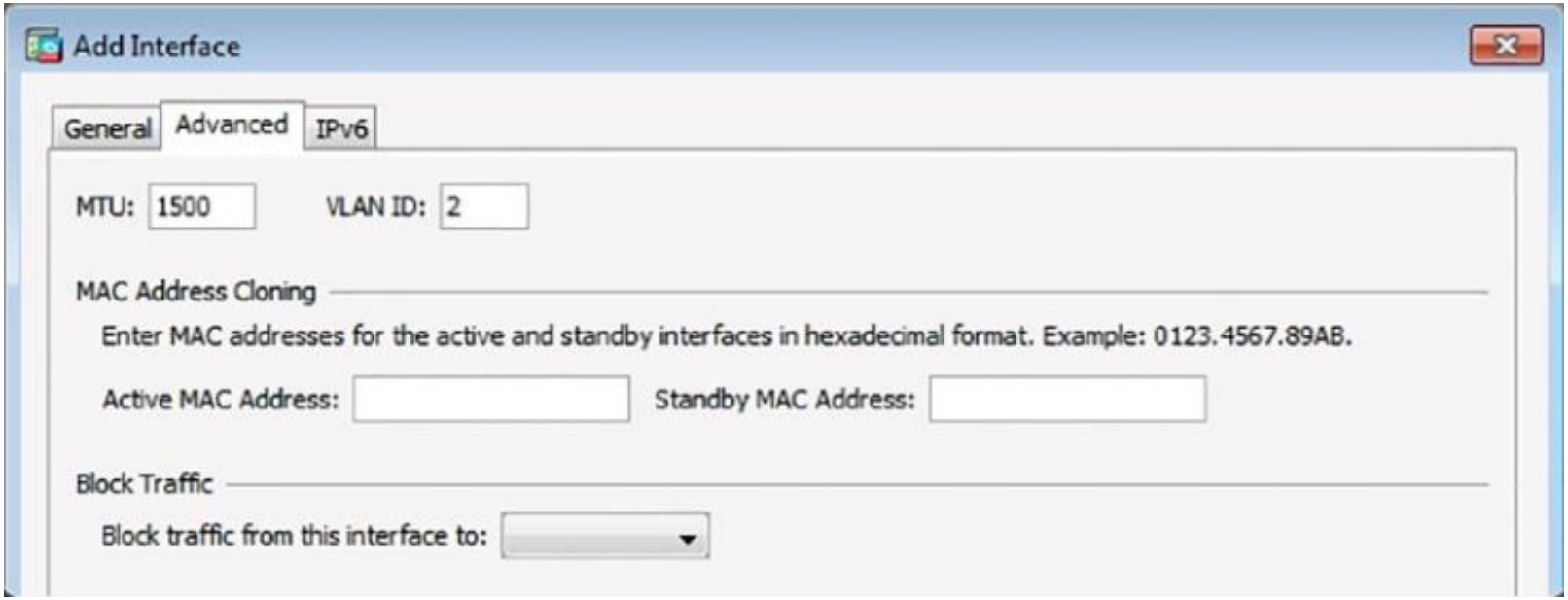
# Configuring Interfaces (Cont.)




Adding an Outside Interface

# Configuring Interfaces (Cont.)

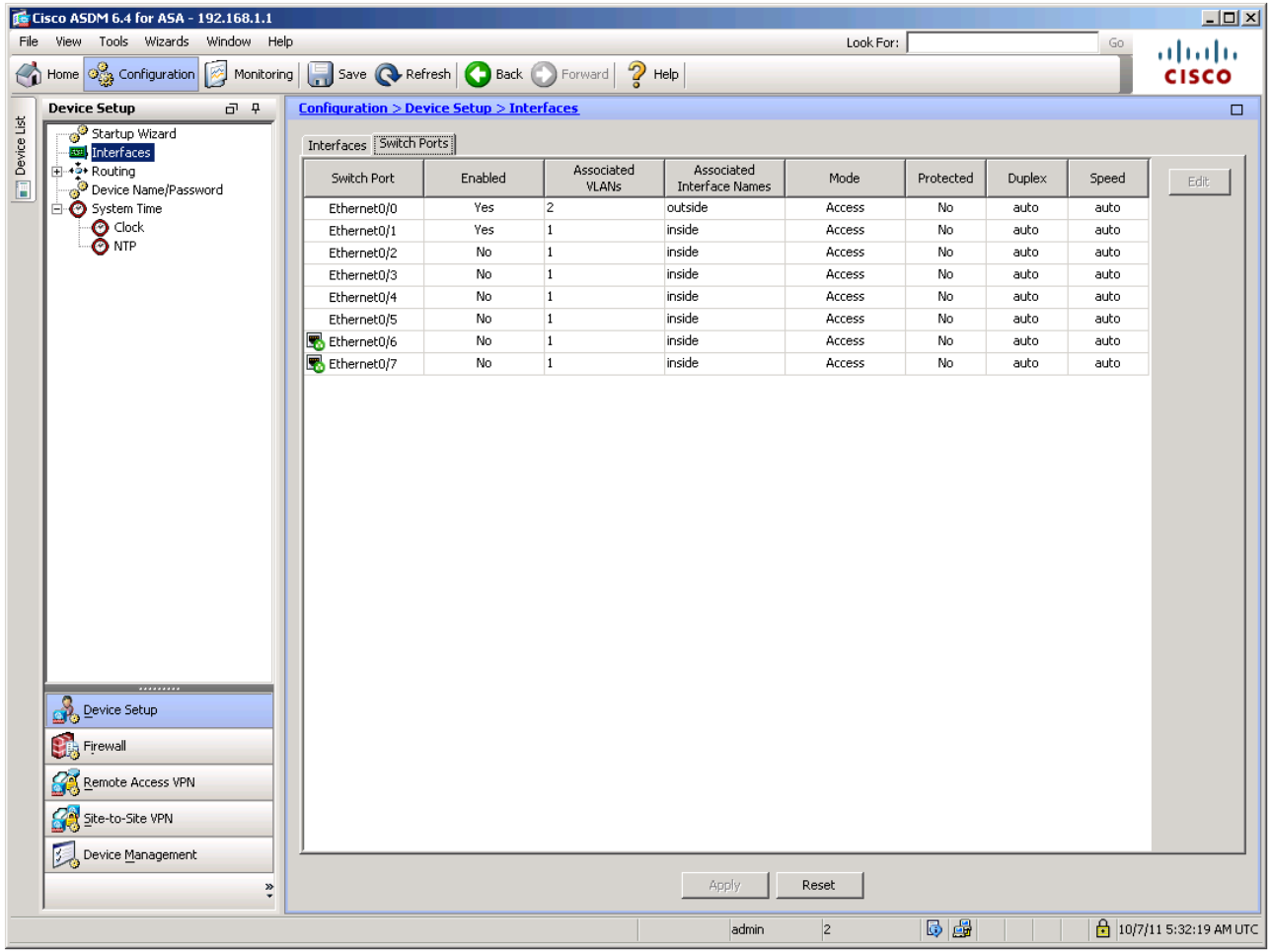
Advanced Outside Interface Settings



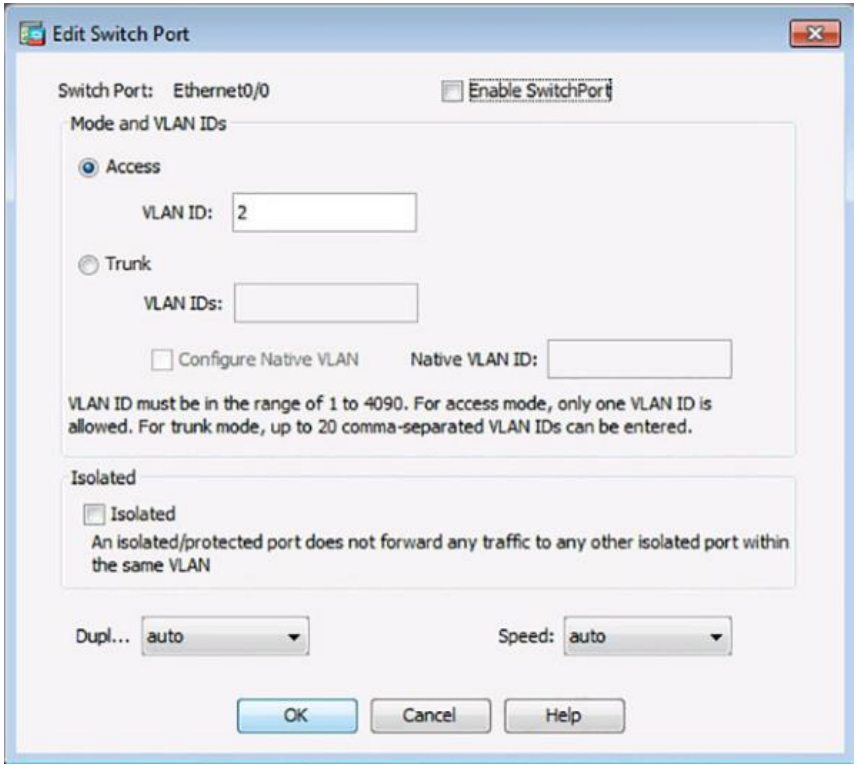

Updated Interface Page

# Layer 2 Switch Ports

- **Configuration > Device Setup > Interfaces > Switch Ports**



# Configuring Interfaces

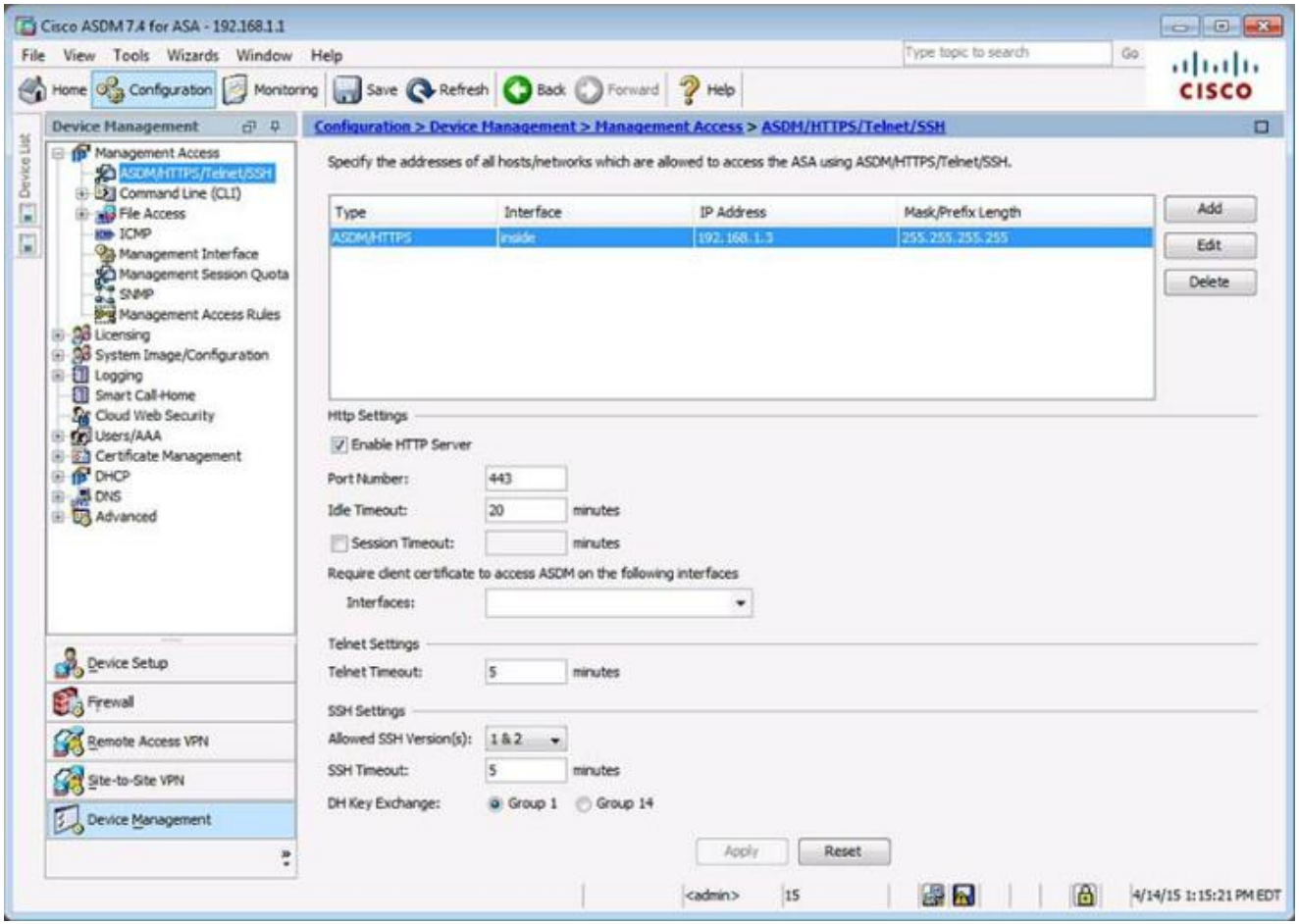



Enable Switch Ports

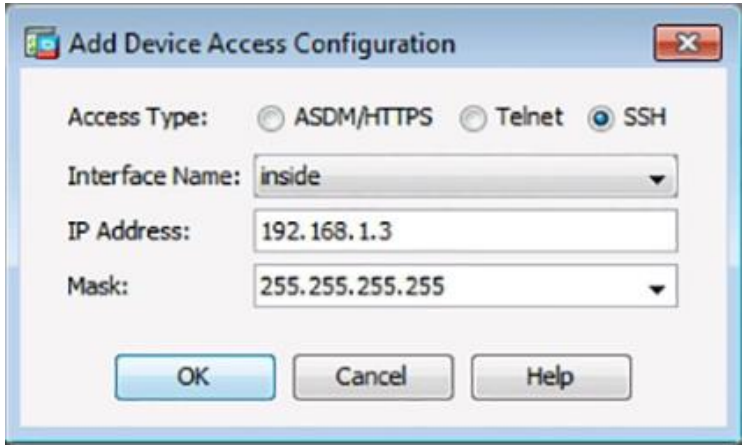
Apply Configuration

# Configuring Device Management Access

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

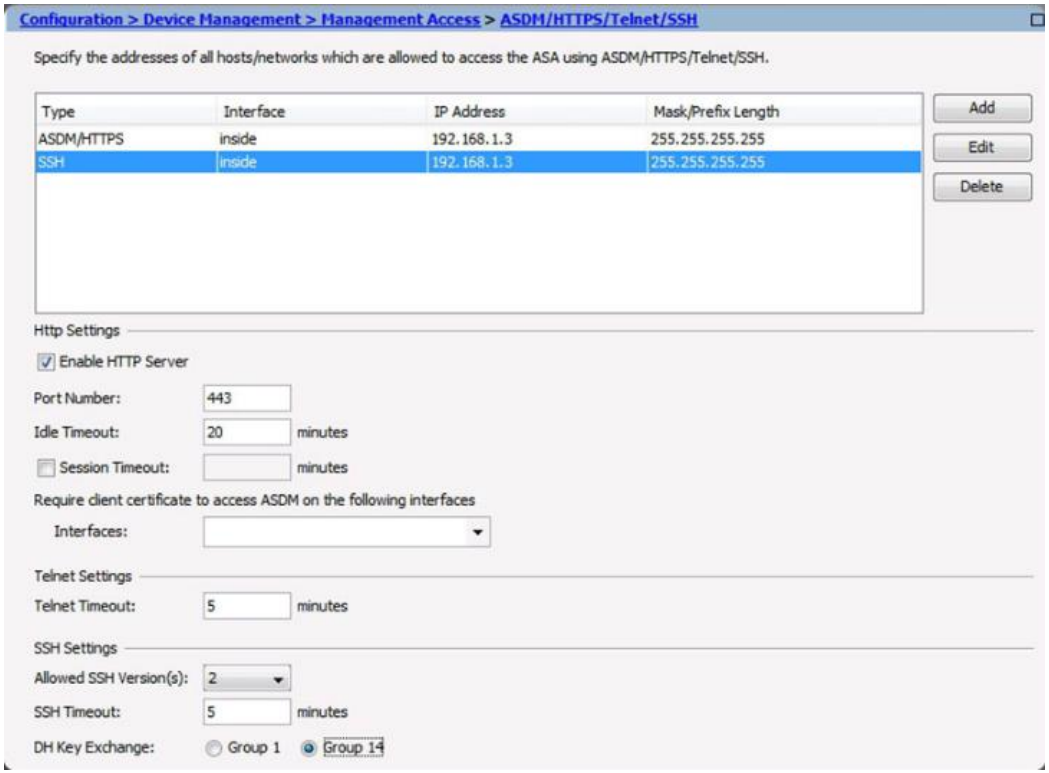


# Configuring Device Management Access

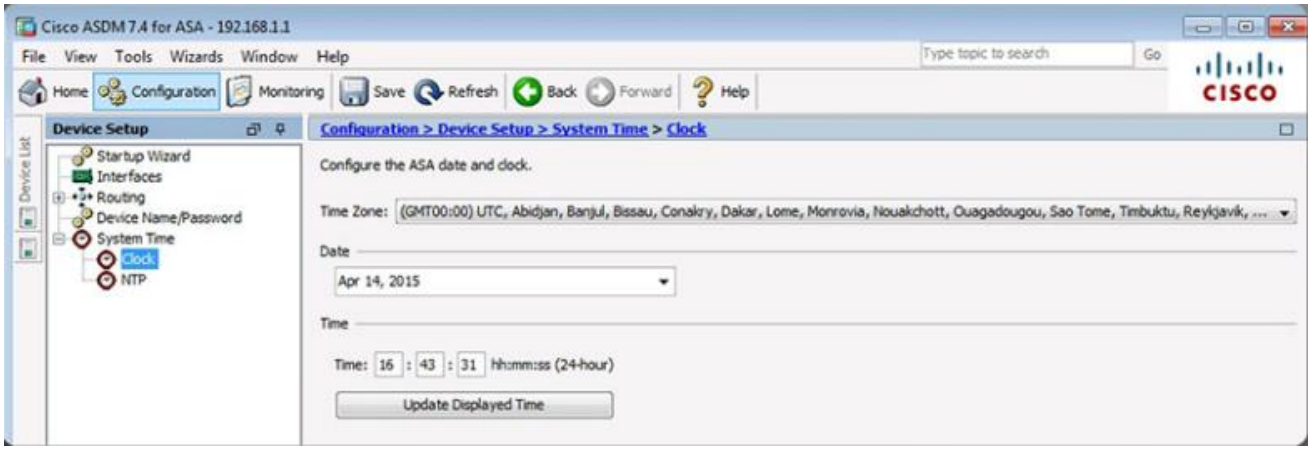



Add Device Access Configuration Window

Configure SSH Settings

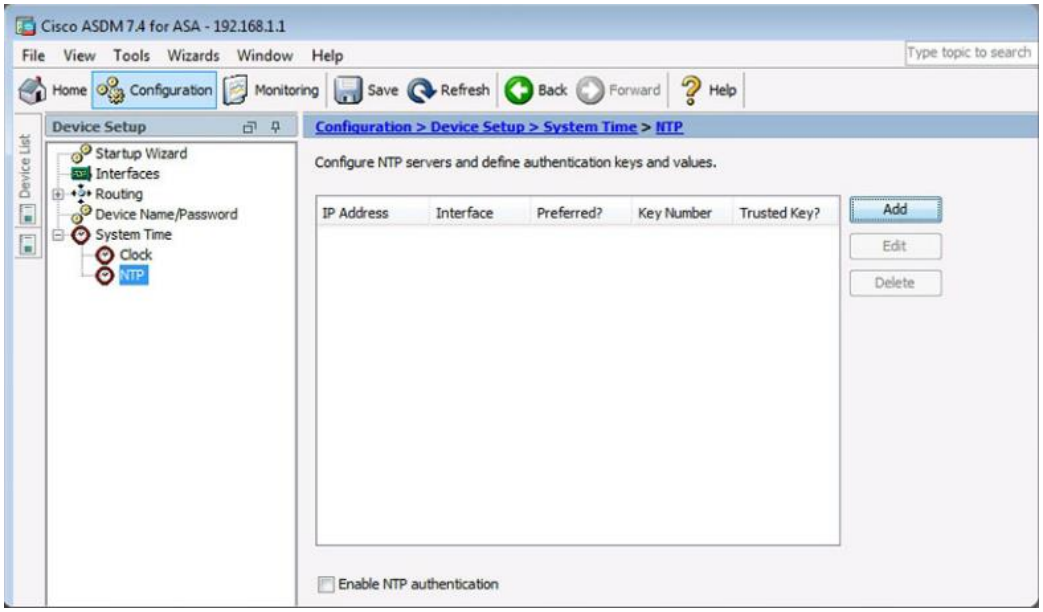


# Configuring the System Time

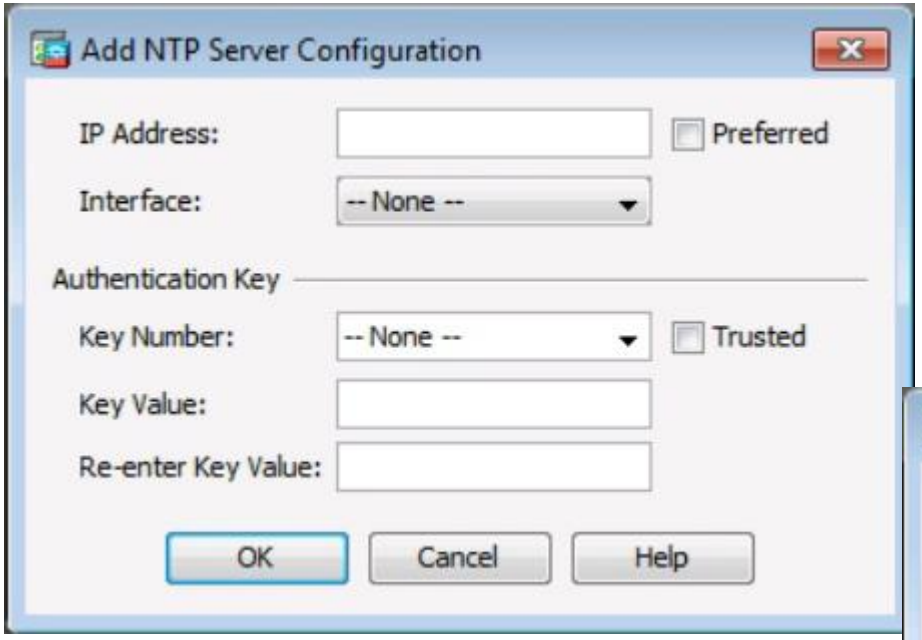



Manually Change the System Time

Use NTP to Change the System Time

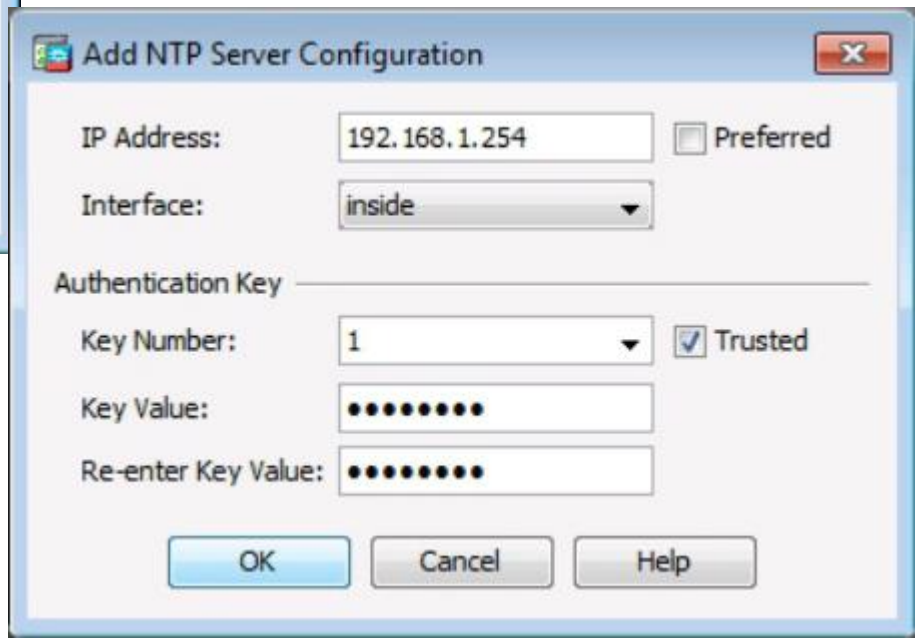


# Configuring the System Time



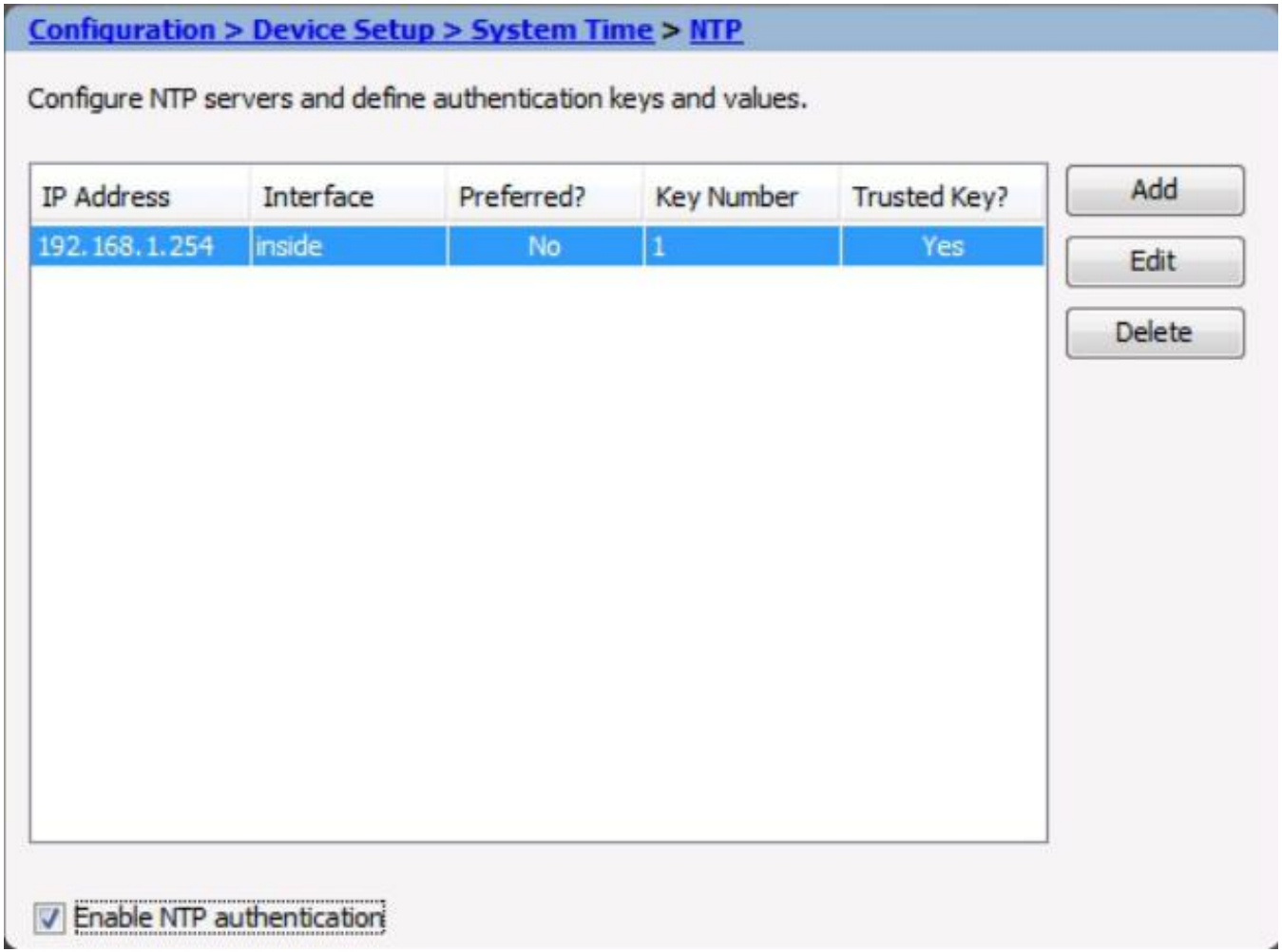

Configure an NTP Server

Add an NTP Server

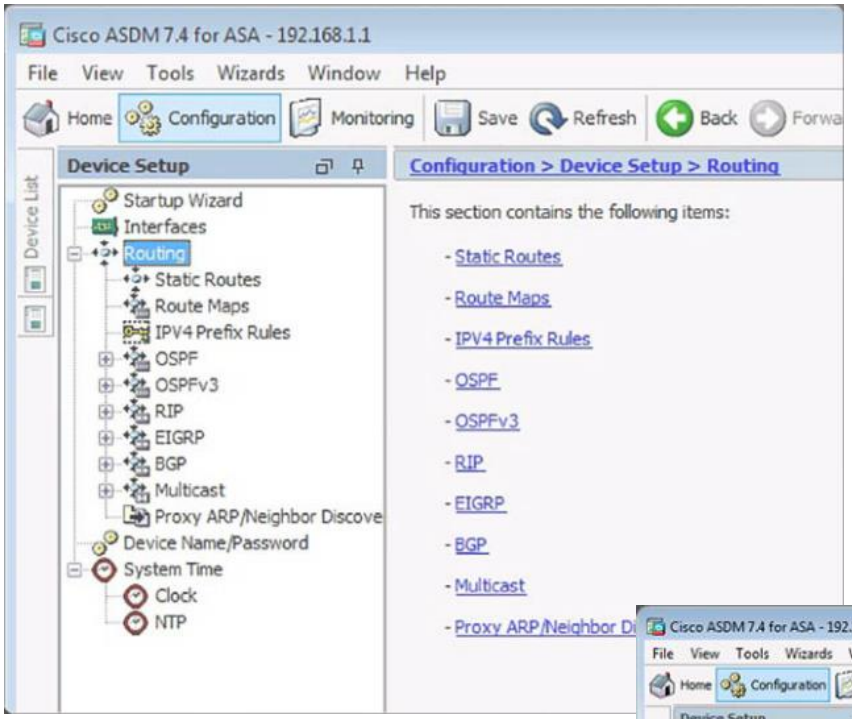


# Configuring the System Time

Apply the Configuration

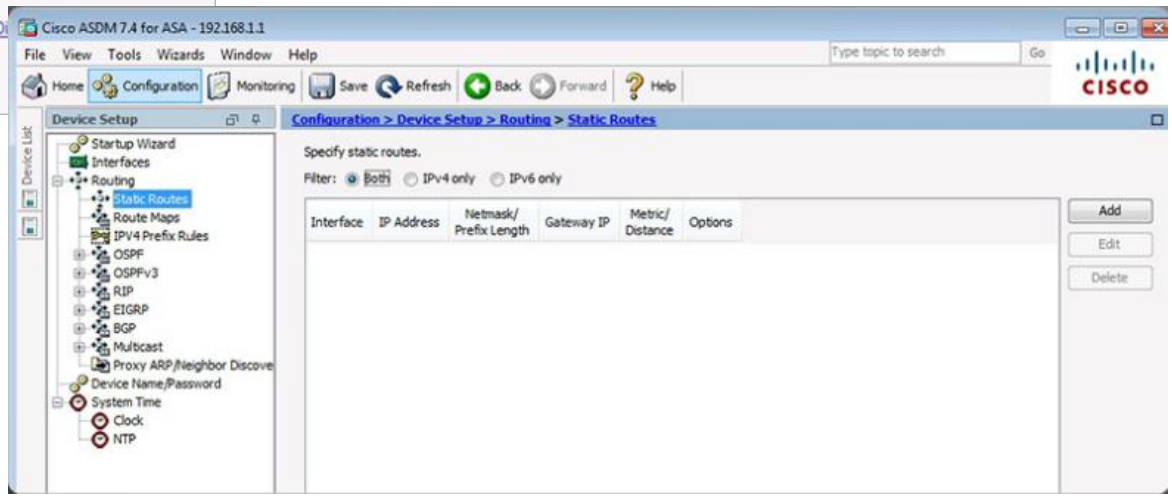


# Configuring Routing




- **Configuration > Device Setup > Routing > Static Routes**

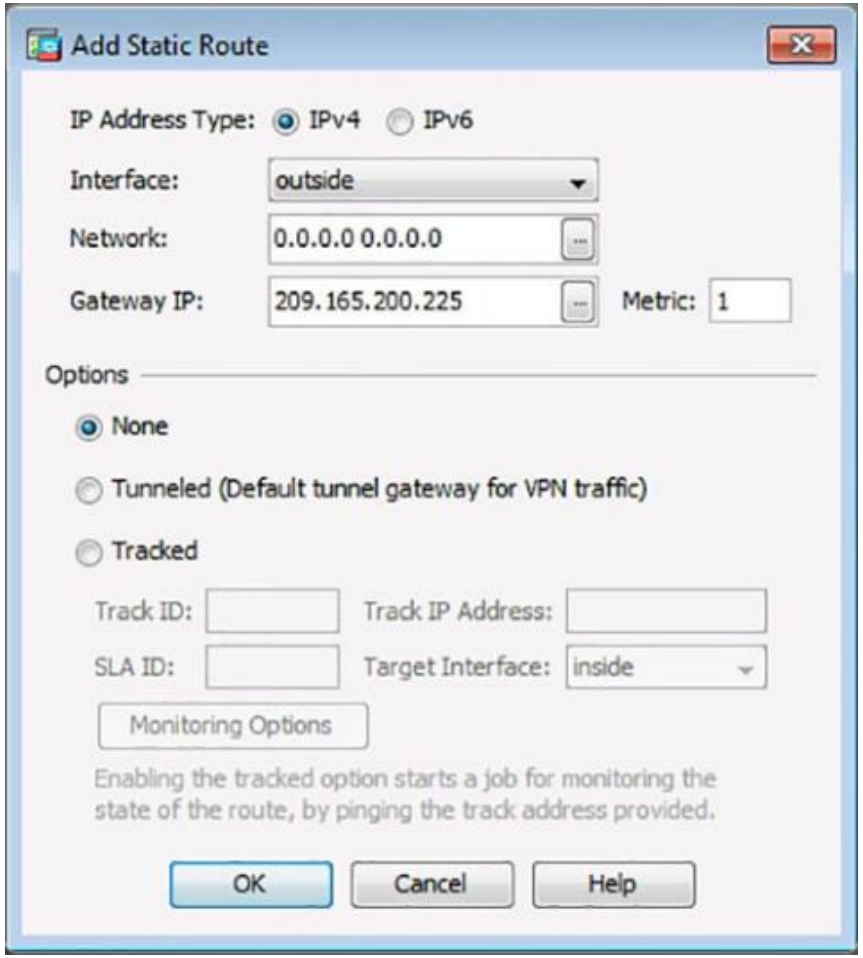
Configuring Routing



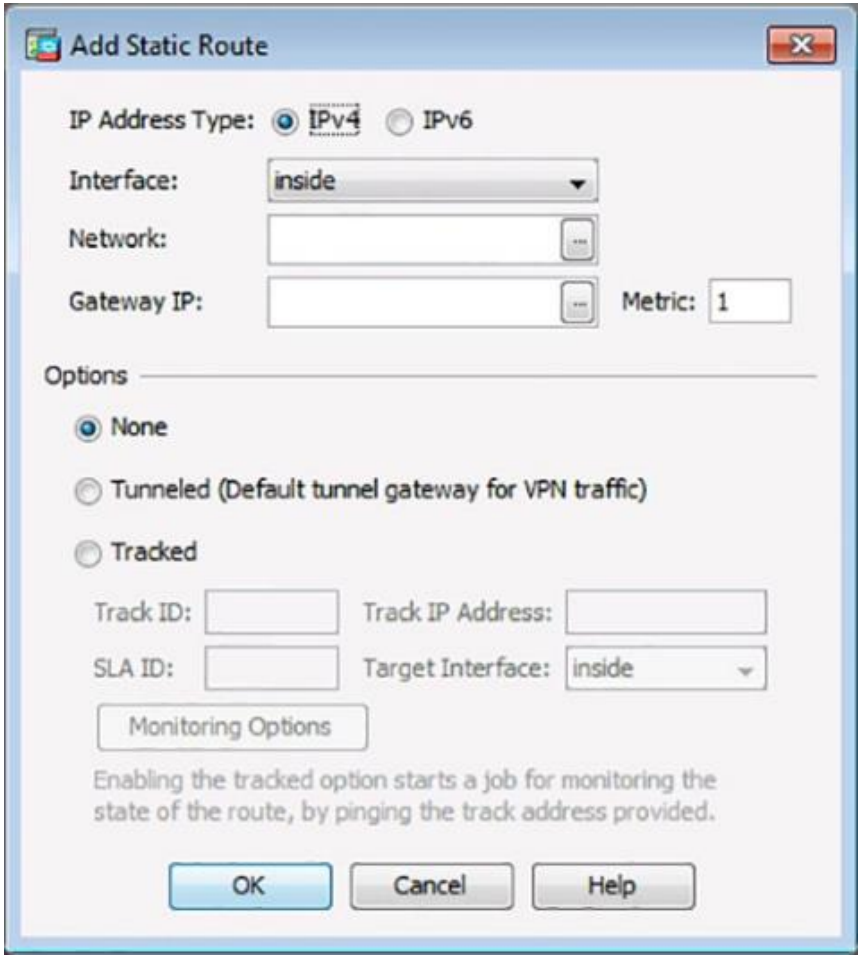

Configuring a Default Static Route

# Configuring Routing

## Add or Edit Route Window

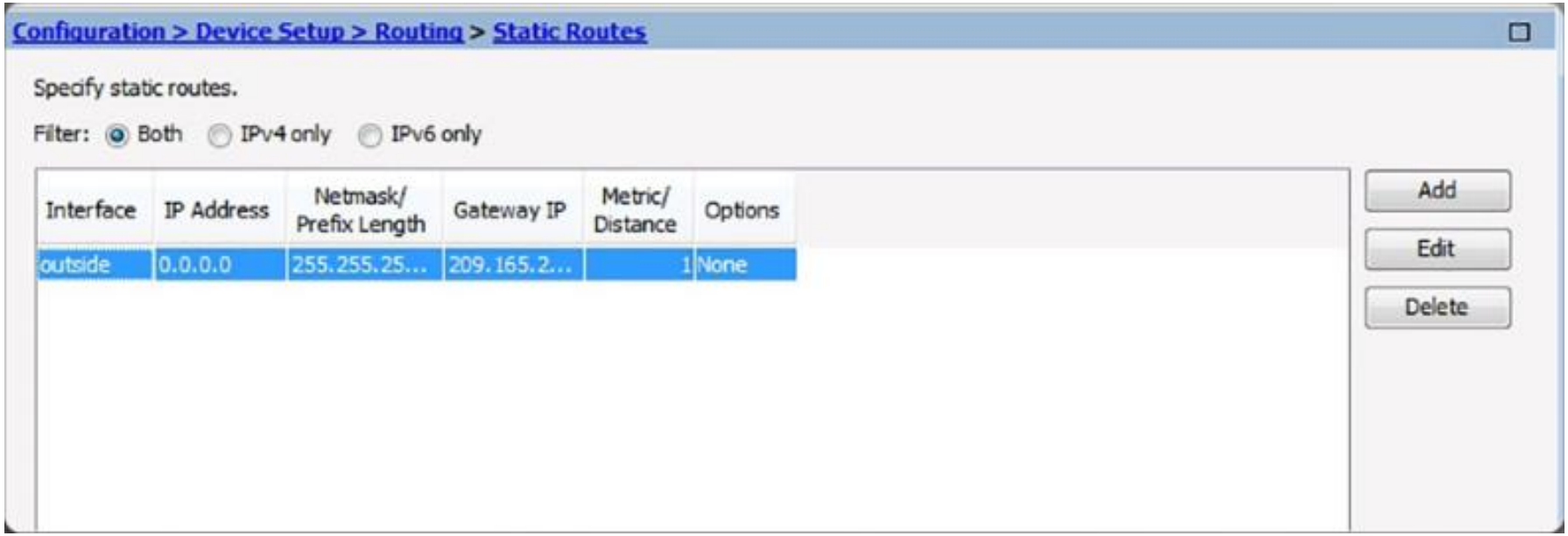



## Add Static Route Details



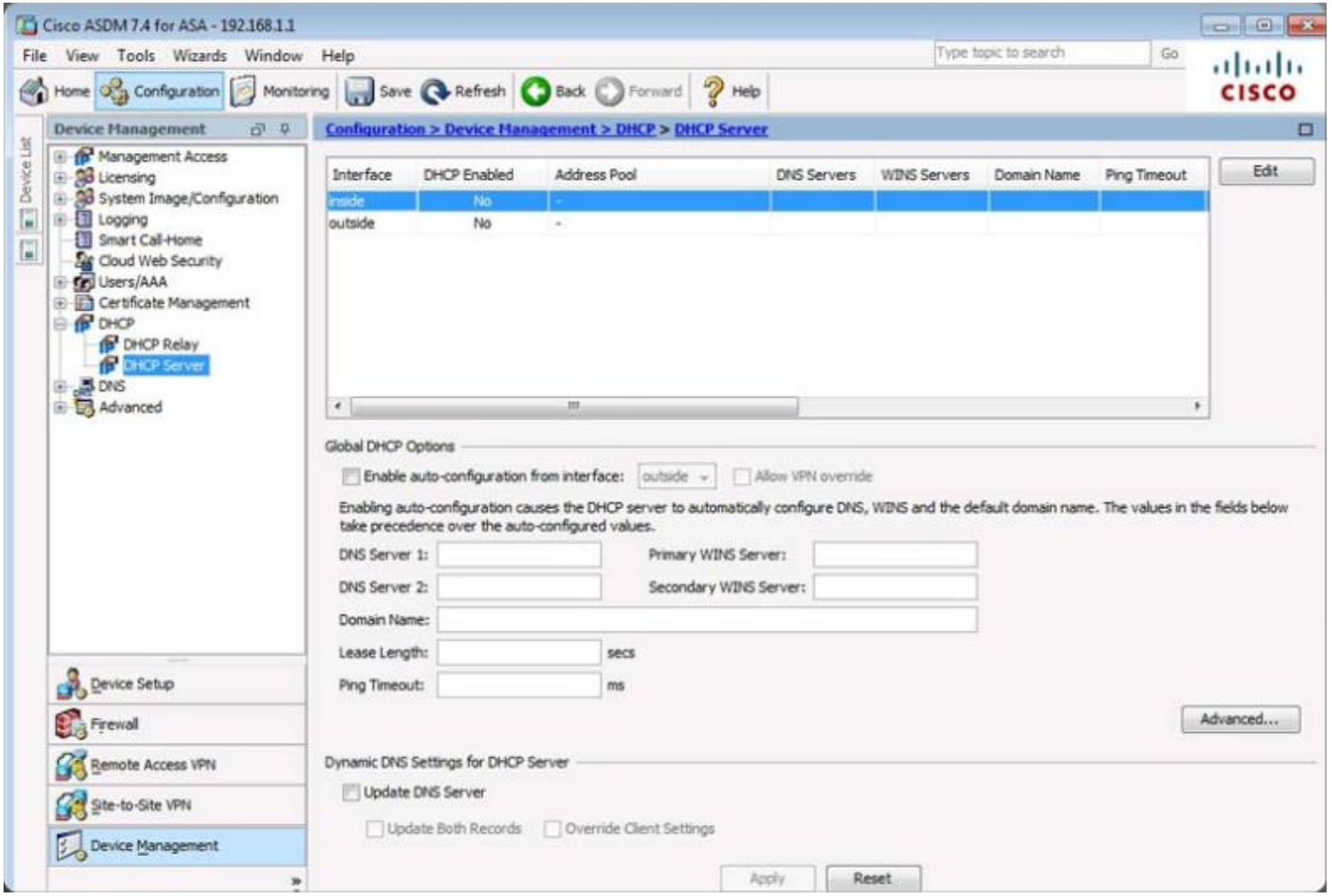
# Configuring Routing

Apply the Configuration



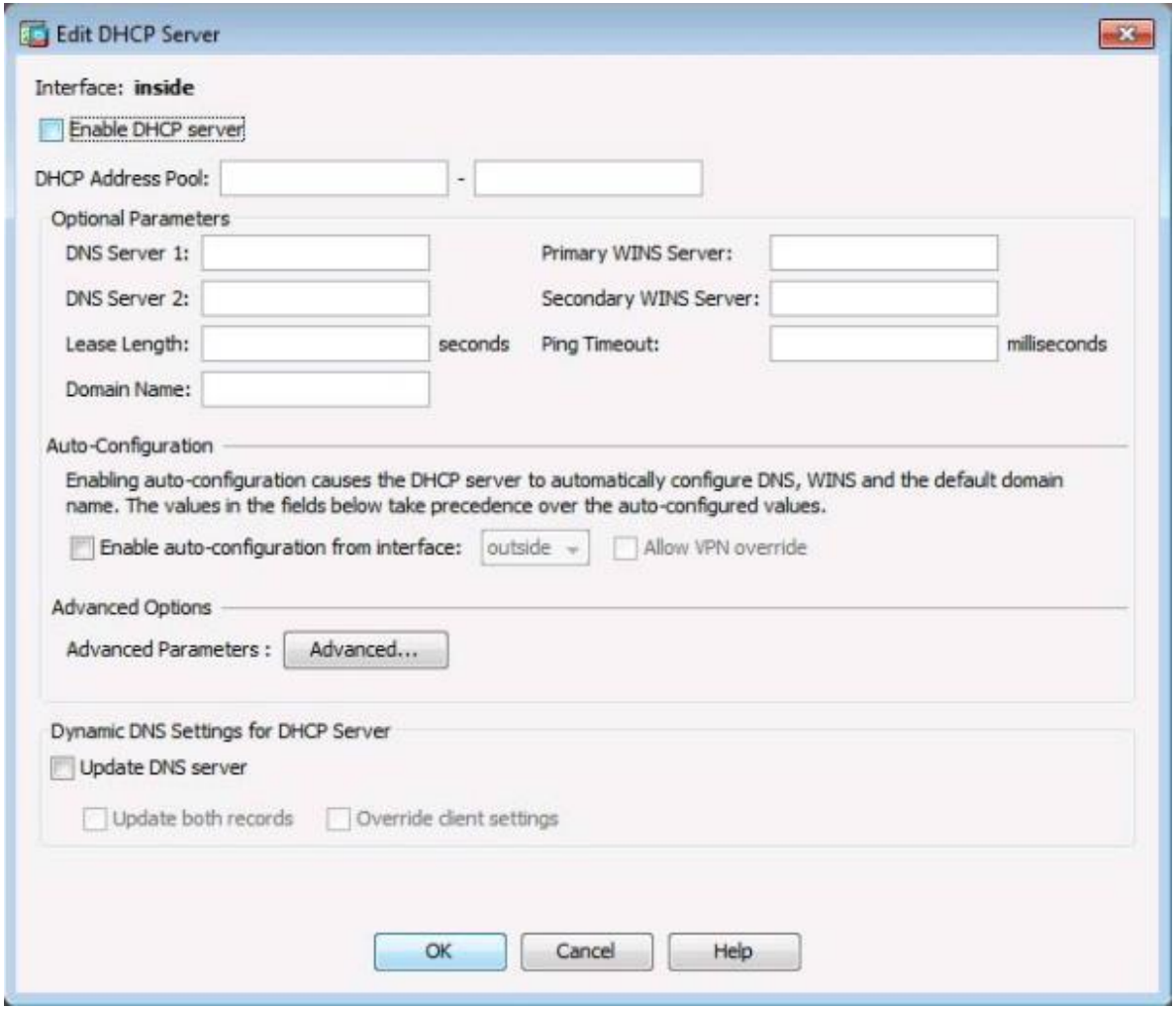
# Configuring DHCP Services

## DHCP Server Page



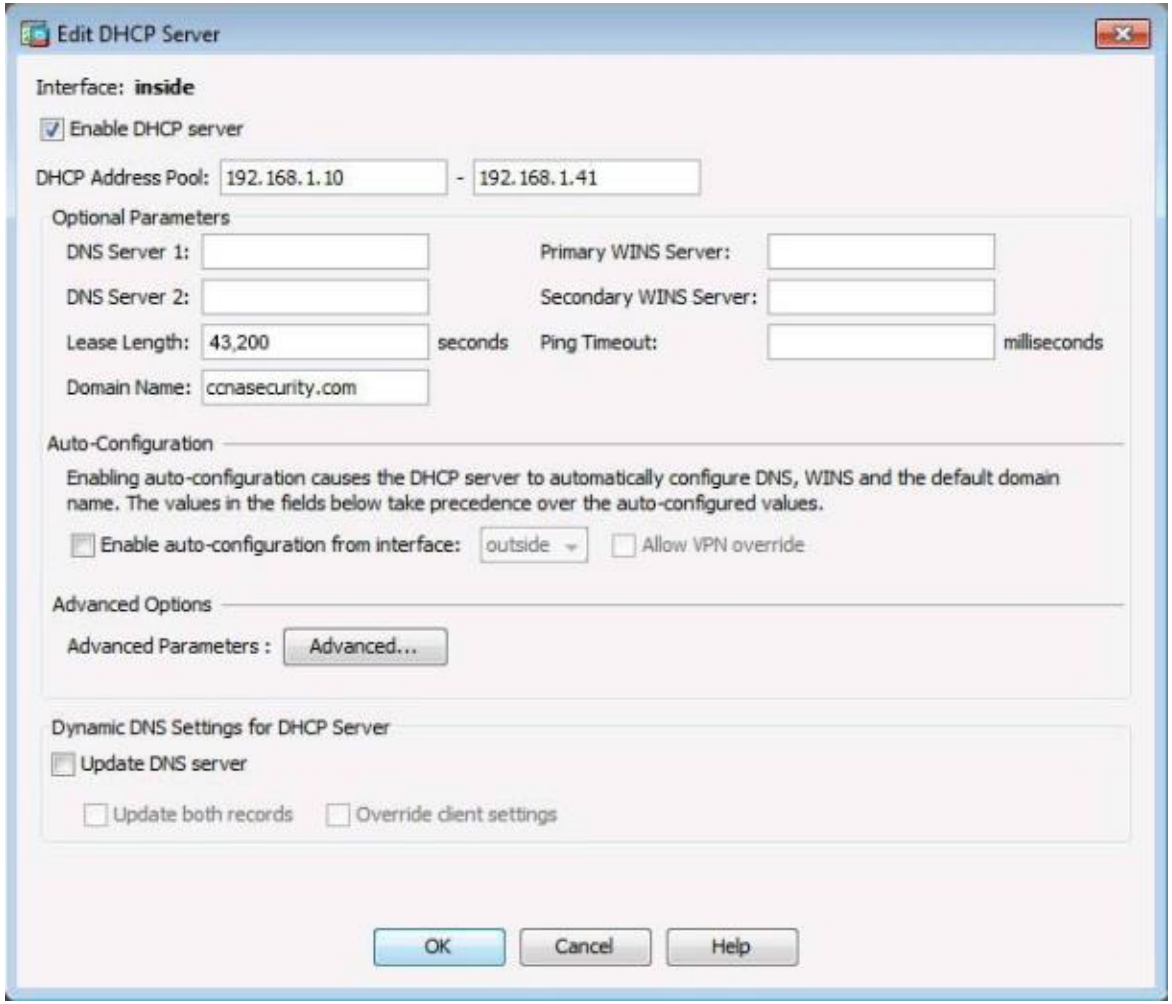
# Configuring DHCP Services

## Edit DHCP Server Window



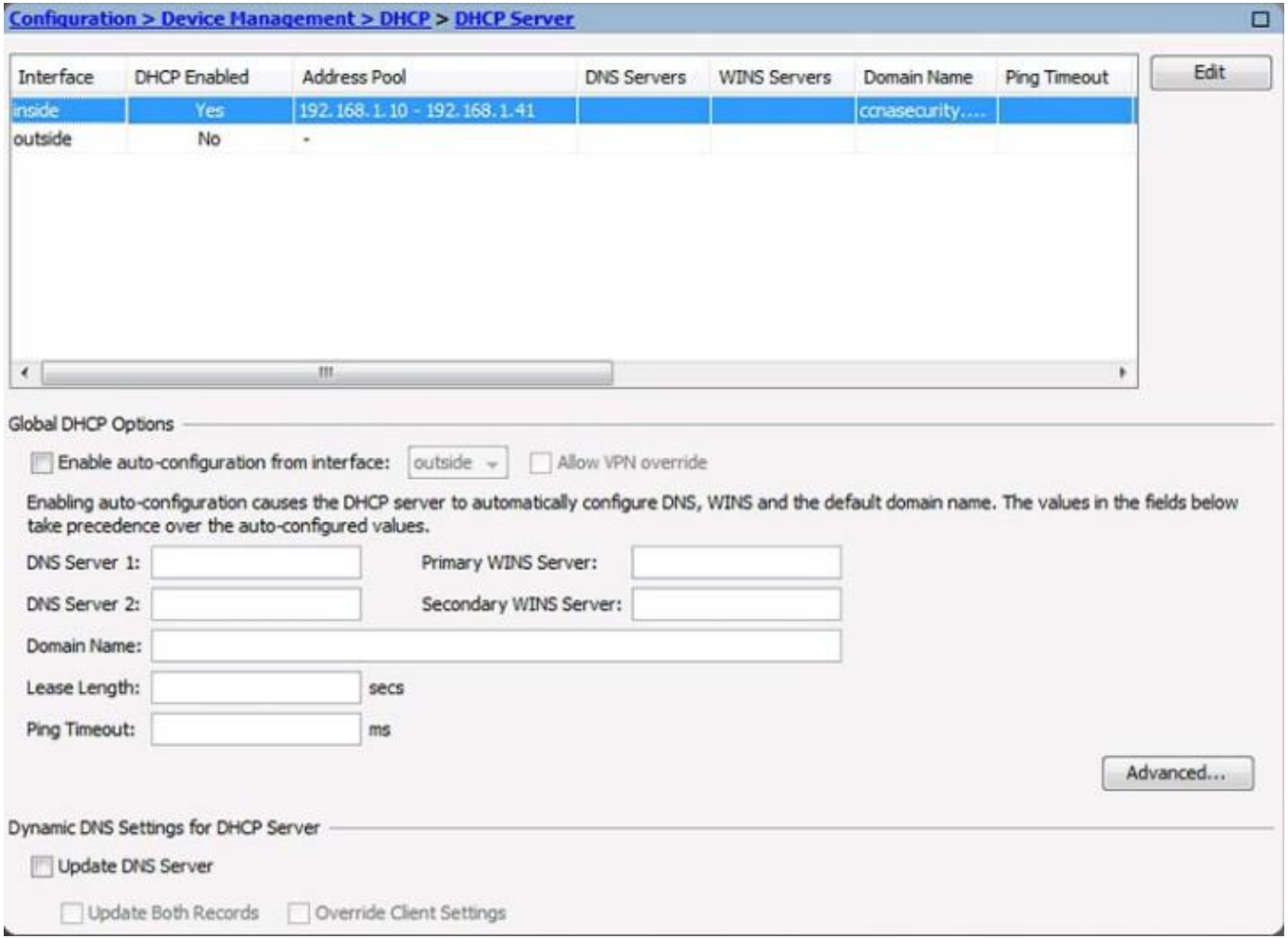
# Configuring DHCP Services

## Configuring DHCP Server Services



# Configuring DHCP Services

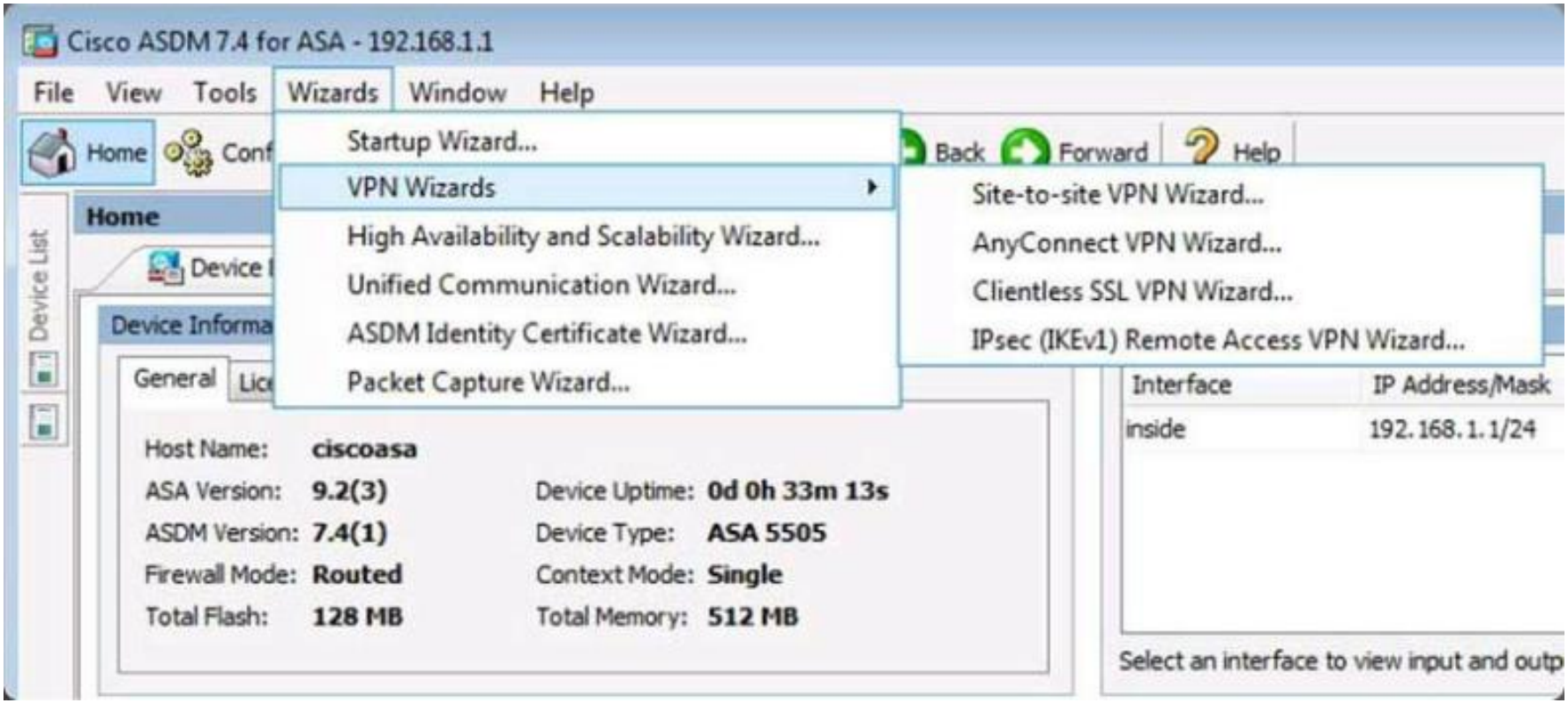
## Verifying DHCP Server Services



# ASDM Startup Wizard

# ASDM Wizards

- ASDM has 6 wizards to choose from:

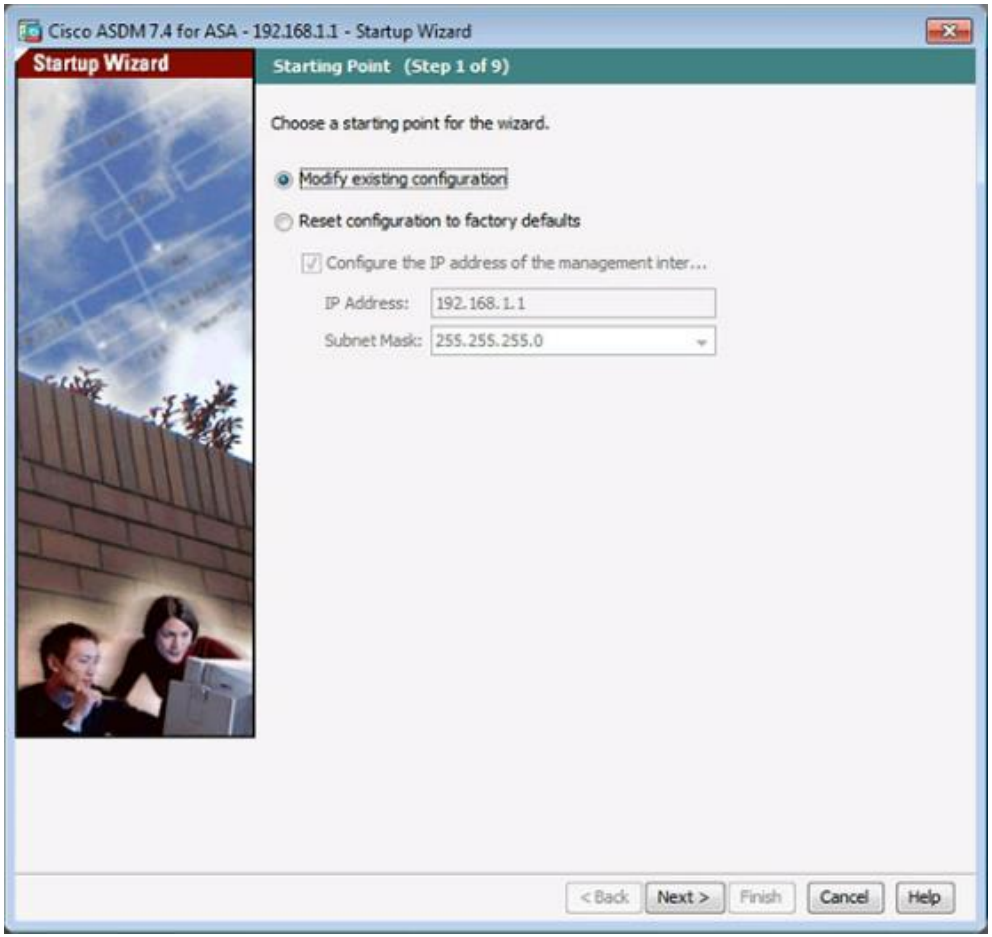


# ASDM Startup Wizard

- The Startup wizard is similar to the interactive Setup Initialization wizard and can be accessed:
  - When launching ASDM from a browser, choose **Run Startup Wizard**.
  - From the Tool bar, choose **Configuration** > **Device Setup** > **Startup Wizard**.
  - From the Menu bar, choose **Wizards** > **Startup Wizard**.

# Startup Wizard - Step 1 of 9

- After the Startup wizard has been launched, the Starting Point window (also referred to as the Welcome window) is displayed.
- It provides a choice to:
  - **Modify existing configuration**
  - **Reset configuration to factory defaults**
- Select an option and click **Next** to continue.

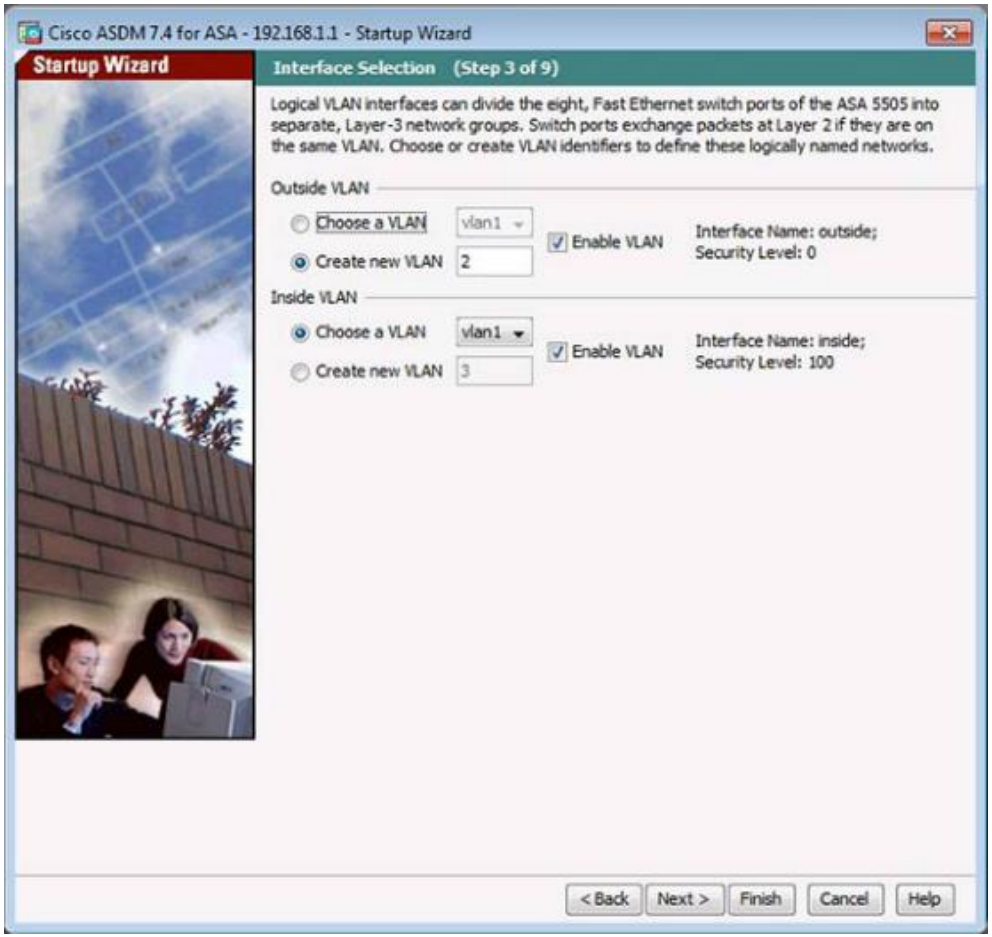


# Startup Wizard - Step 2 of 9

- Complete the basic ASA management configuration consisting of:
  - A host name
  - Domain name
  - Privileged EXEC password
- Optionally, this step also allows the administrator to deploy the ASA for a remote worker.
- Complete the options and click **Next** to continue.

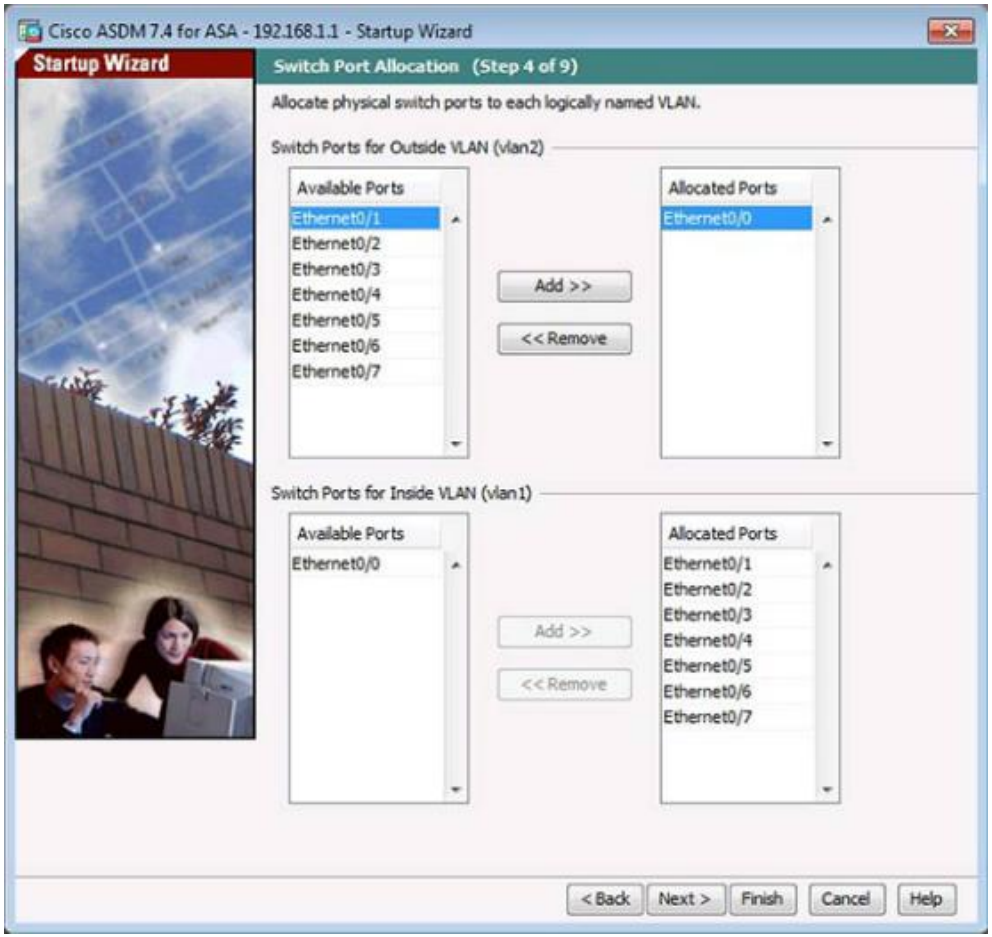
# Startup Wizard - Step 3 of 9

- Create the VLAN switch interfaces.
- This step is specific to the ASA 5505 model.
- Complete the options and click **Next** to continue.



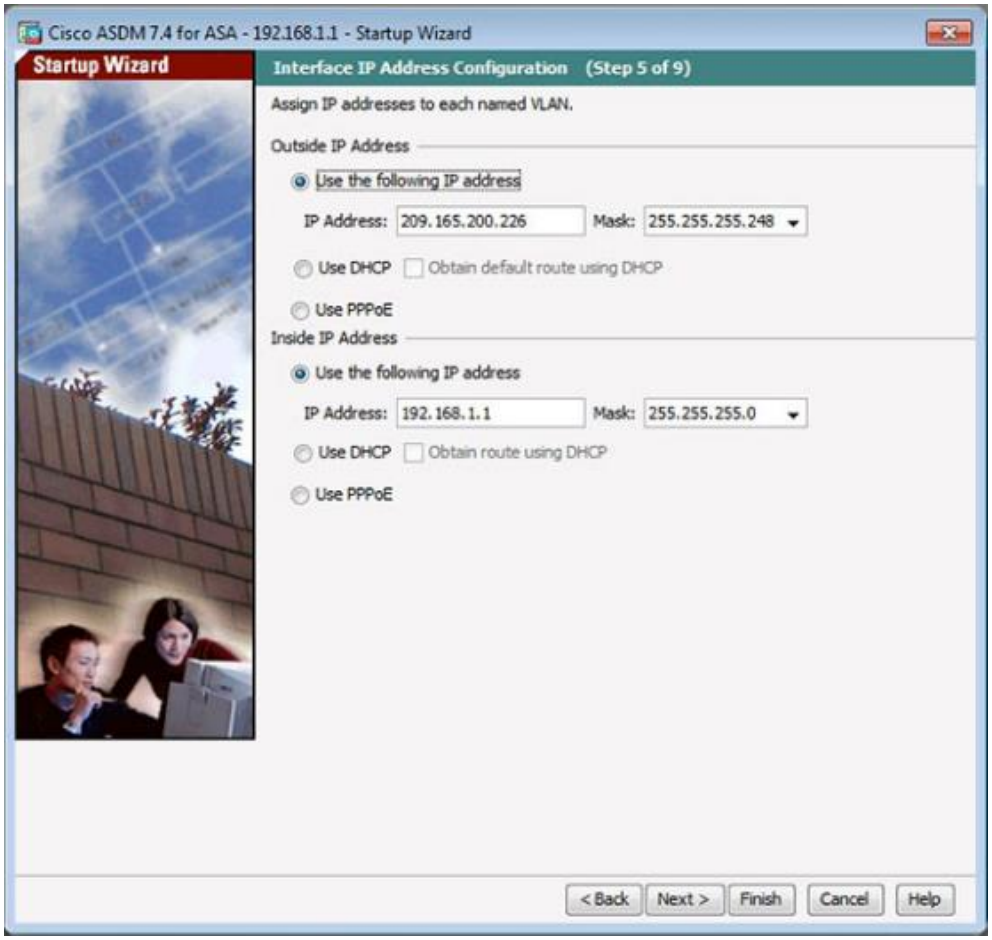
# Startup Wizard - Step 4 of 9

- Map the physical Layer 2 switch ports to the logically named VLANs in the previous step.
- By default, all switch ports are assigned to VLAN 1 (Inside).
- Click **Next** to continue.



# Startup Wizard - Step 5 of 9

- Identify the inside and outside IP addresses for the defined VLANs.
- Note that these addresses could also be created using DHCP or PPPoE.
- Complete the options and click **Next** to continue.

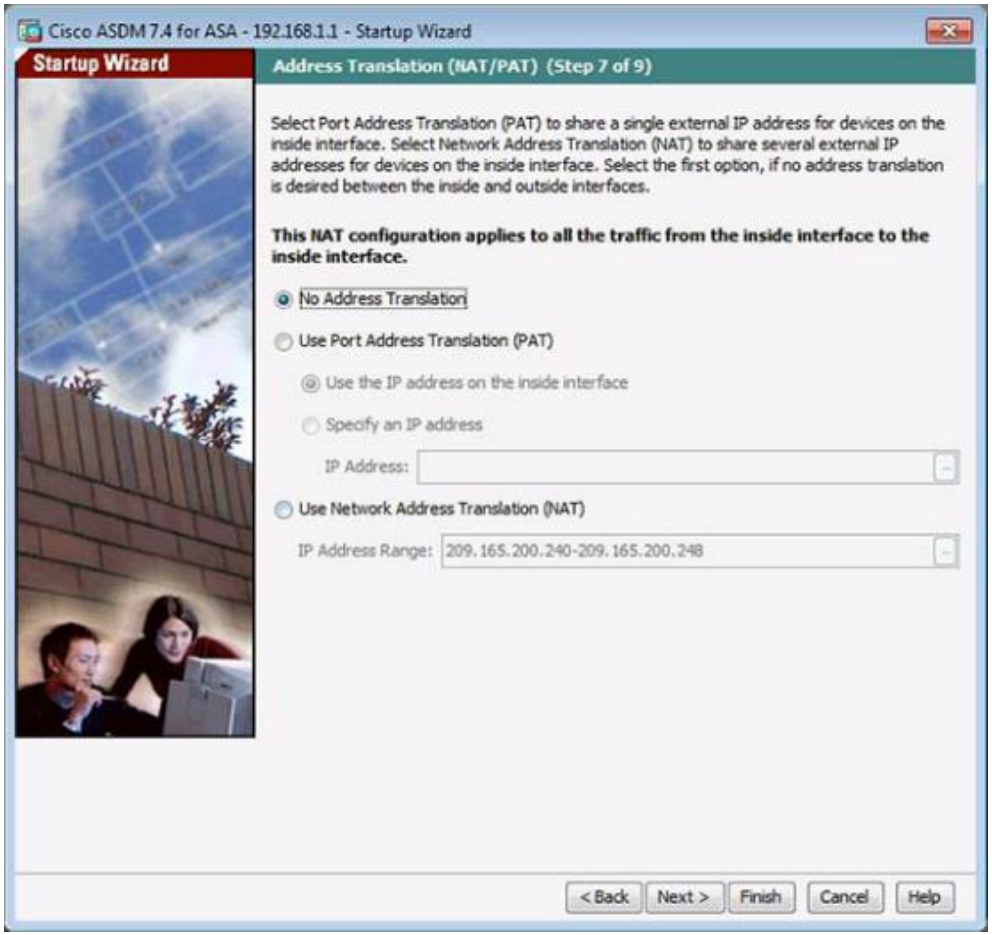


# Startup Wizard - Step 6 of 9

- Enable the DHCP service for inside hosts.
- All DHCP related options are defined in this window.
- Complete the options and click **Next** to continue.

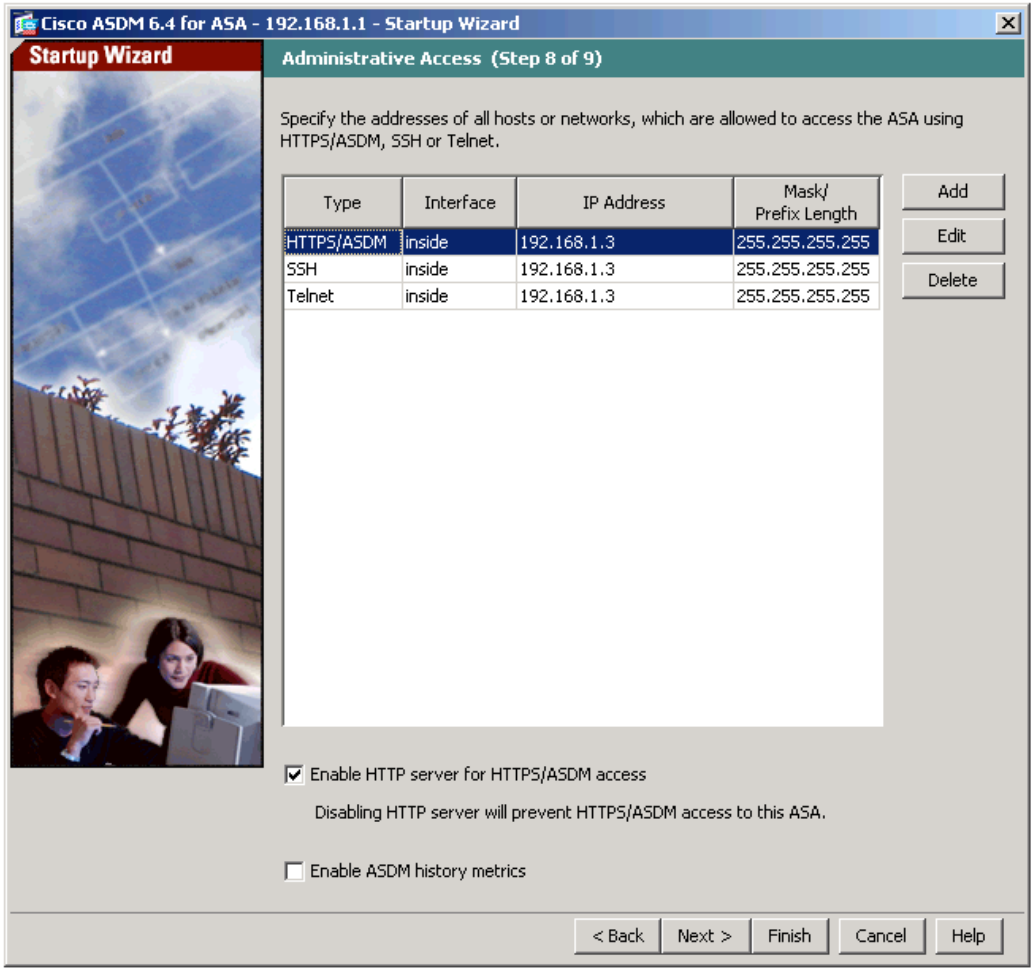
# Startup Wizard - Step 7 of 9

- Enable PAT or NAT.
- Complete the options and click **Next** to continue.



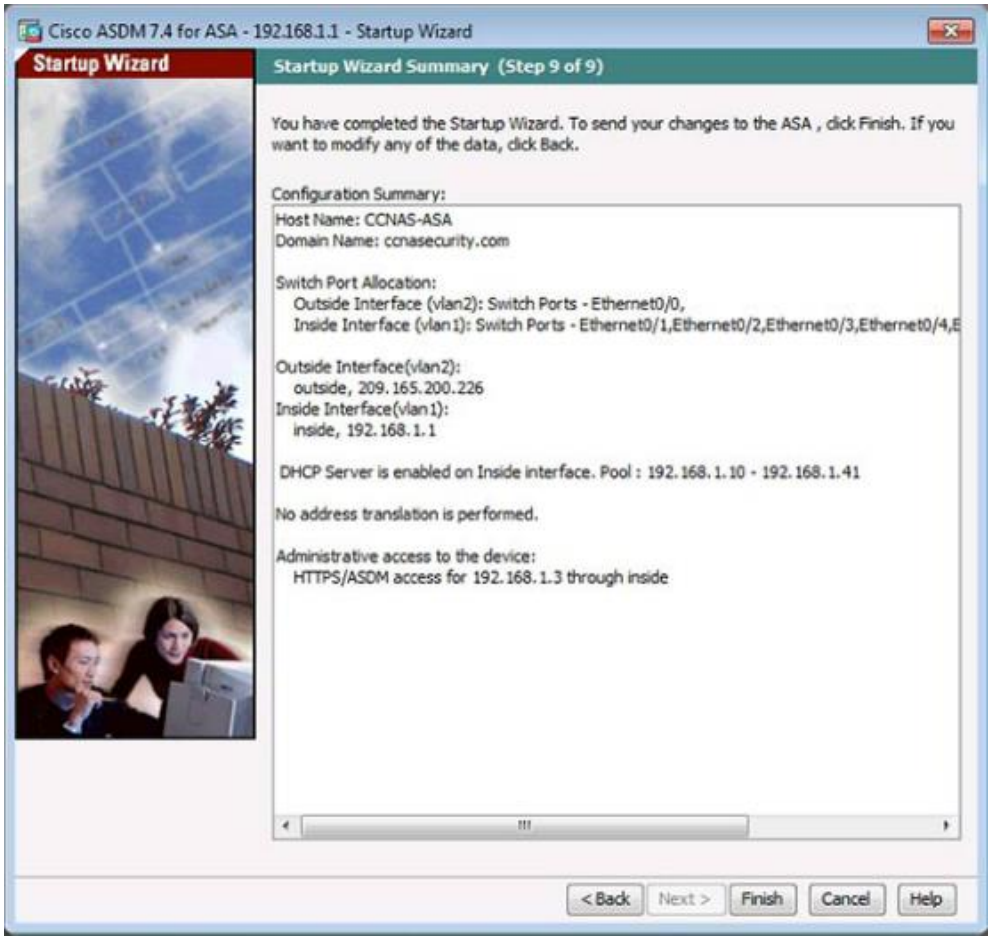
# Startup Wizard - Step 8 of 9

- Specify which host or hosts are allowed to access the ASA using either HTTPS/ASDM, SSH, or Telnet.
- Complete the options and click **Next** to continue.



# Startup Wizard - Step 9 of 9

- Review the proposed configuration.
- Changes can be made by clicking the **Back** button or saved by clicking the **Finish** button.

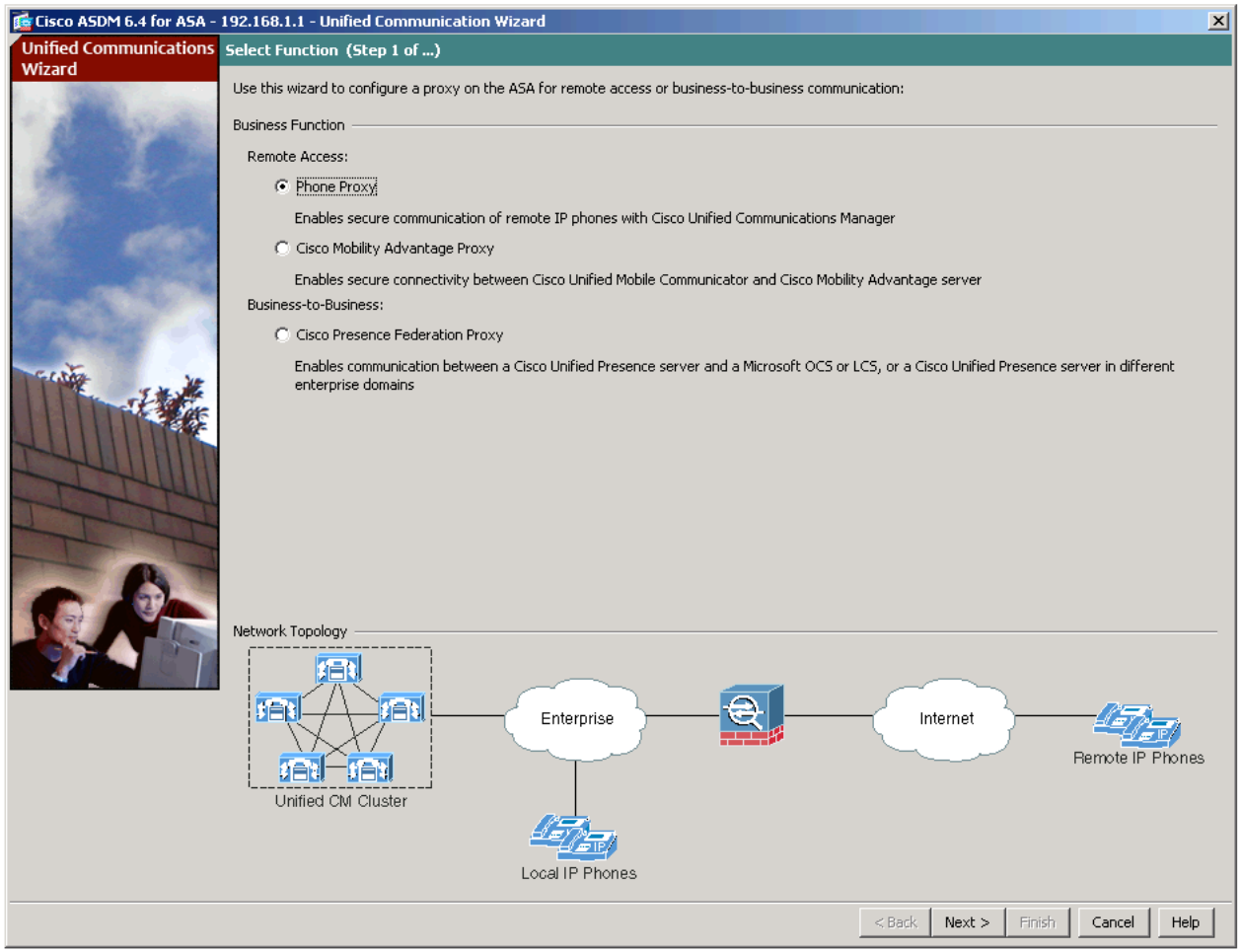


# ASDM VPN Wizards

- Wizard to configure site-to-site and remote-access VPNs

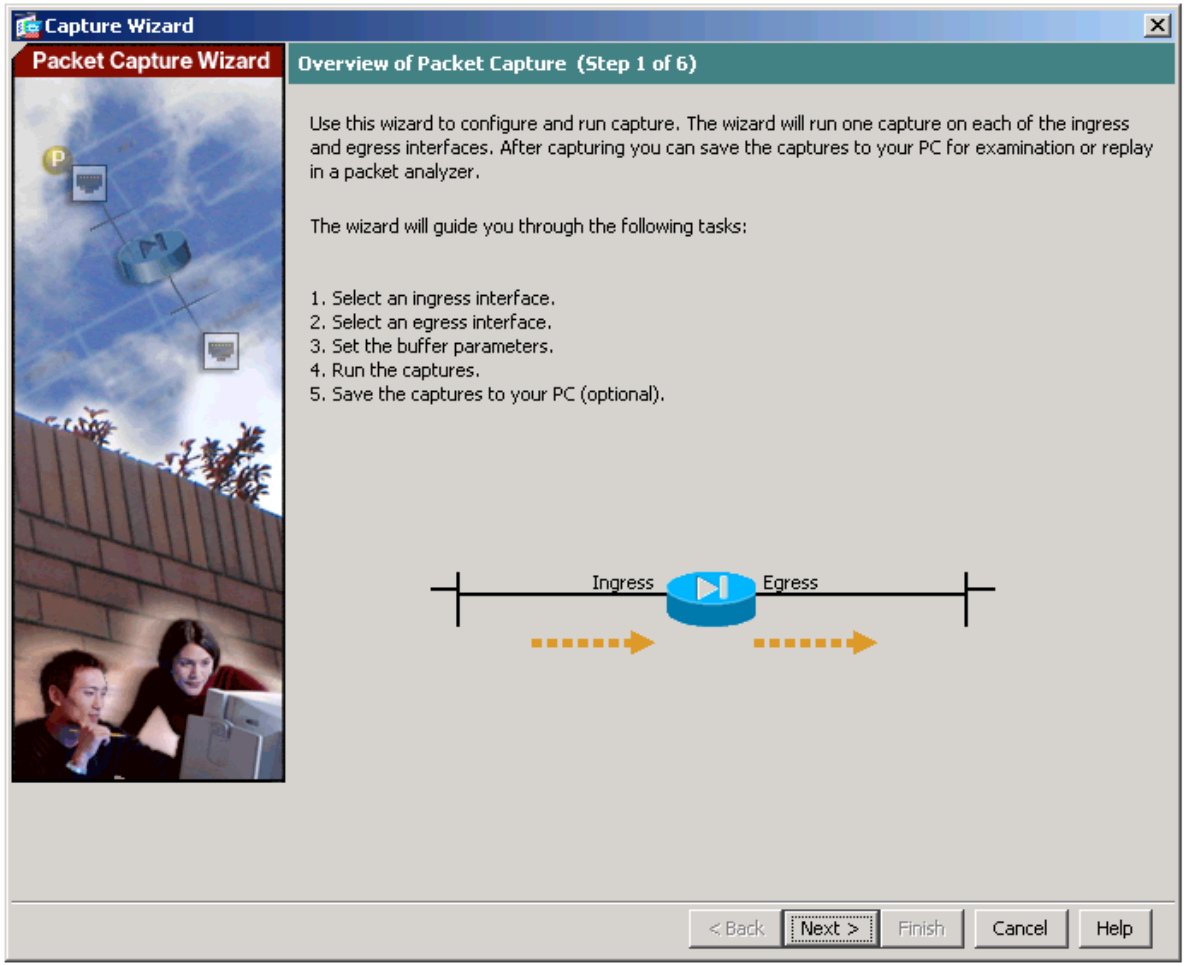
# ASDM Unified Communication Wizard

- Configure the ASA to support the Cisco Unified Communications Proxy feature



# ASDM Packet Capture Wizard

- Use the wizard for troubleshooting and testing purposes.



# Objects and Object Groups

# Objects and Object Groups

- An object can be defined with a particular IP address and netmask pair or a protocol (and, optionally, a port) and it can be re-used in several configurations.
- The advantage is that when an object is modified, the change is automatically applied to all rules that use the specified object.
  - Therefore, objects make it easy to maintain configurations.
- Objects can be used in NAT, access lists, and object groups.

# Objects

- The ASA supports two types of objects
- **Network object:**
  - Contains a single IP address/mask pair
  - Can be defined by host, subnet, or range of addresses
- **Service object:**
  - Contains a protocol and optional source and/or destination port

- A network object is required to configure NAT

```
CCNAS-ASA(config)# object ?

configure mode commands/options:
  network  Specifies a host, subnet or range IP addresses
  service  Specifies a protocol/port
CCNAS-ASA(config)#
```

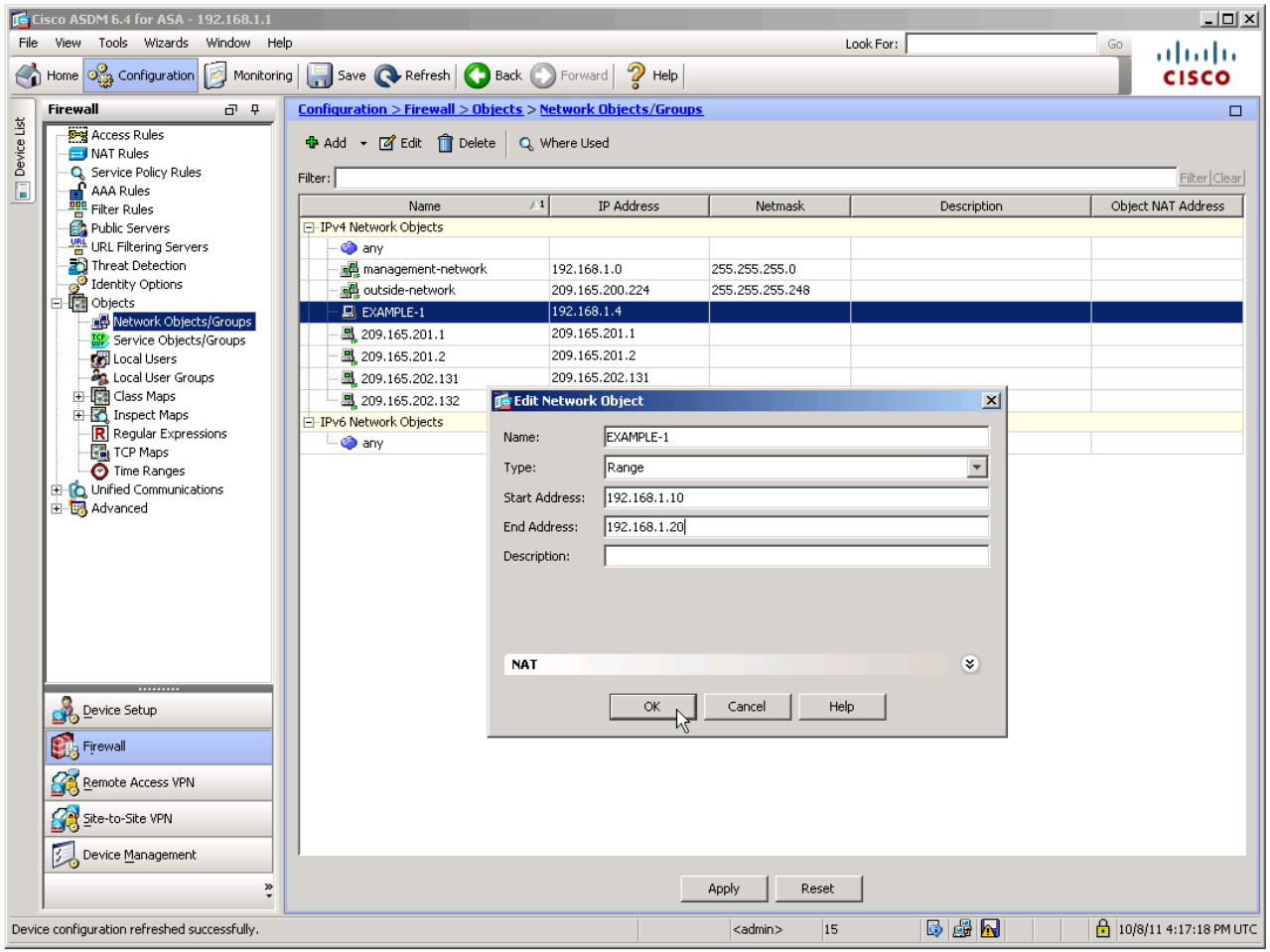
# Configuring a Network Object

- To create a network object, use the **object network** *object-name* global configuration command
  - The prompt will change to the network object configuration mode
- A network object can contain only one IP address and mask pair
  - Entering a second IP address/mask pair will replace the existing configuration
- To erase all network objects, use the **clear config object network** command
  - Note that this command clears all network objects

```
CCNAS-ASA(config)# object network EXAMPLE-1
CCNAS-ASA(config-network-object)# host 192.168.1.4
CCNAS-ASA(config-network-object)# range 192.168.1.10 192.168.1.20
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object network EXAMPLE-1
 range 192.168.1.10 192.168.1.20
CCNAS-ASA(config)#
```

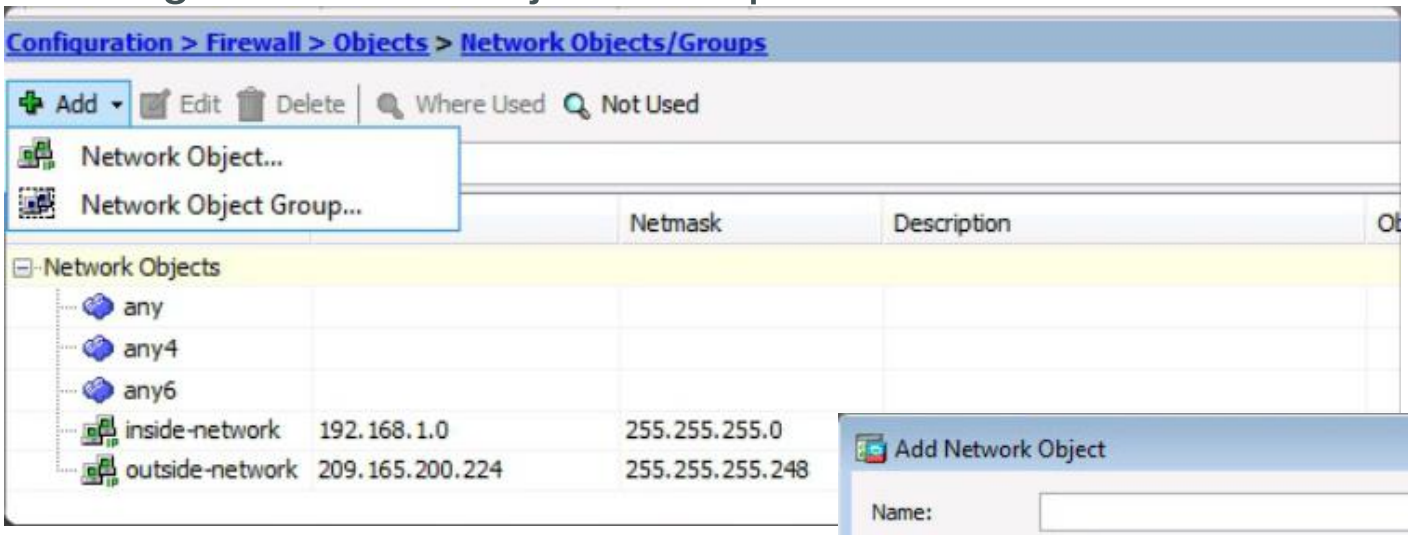
# Configuring a Network Object using ASDM

- **Configurations > Firewall > Objects > Network Objects/Groups**

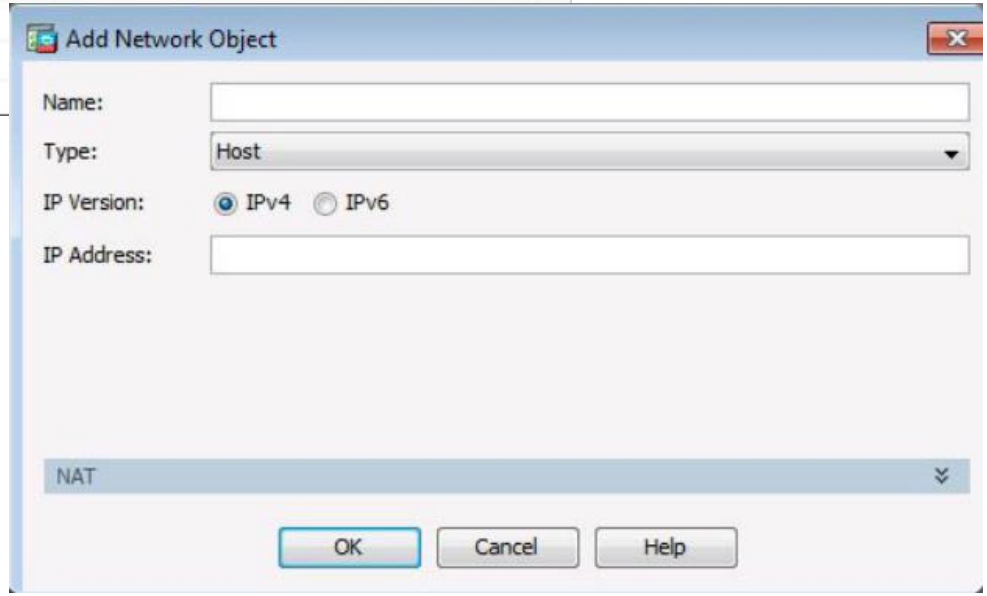


# Objects in ASDM (Cont.)

Adding a Network Object/Group




Add Network Object Window



# Configuring a Service Object

- To create a network object, use the **`object service`** *`object-name`* global configuration command.
  - The prompt will change to the network object configuration mode.
- A service object name can only be associated with one protocol and port (or ports).
  - If an existing service object is configured with a different protocol and port (or ports), the new configuration replaces the existing protocol and port (or ports) with the new ones.

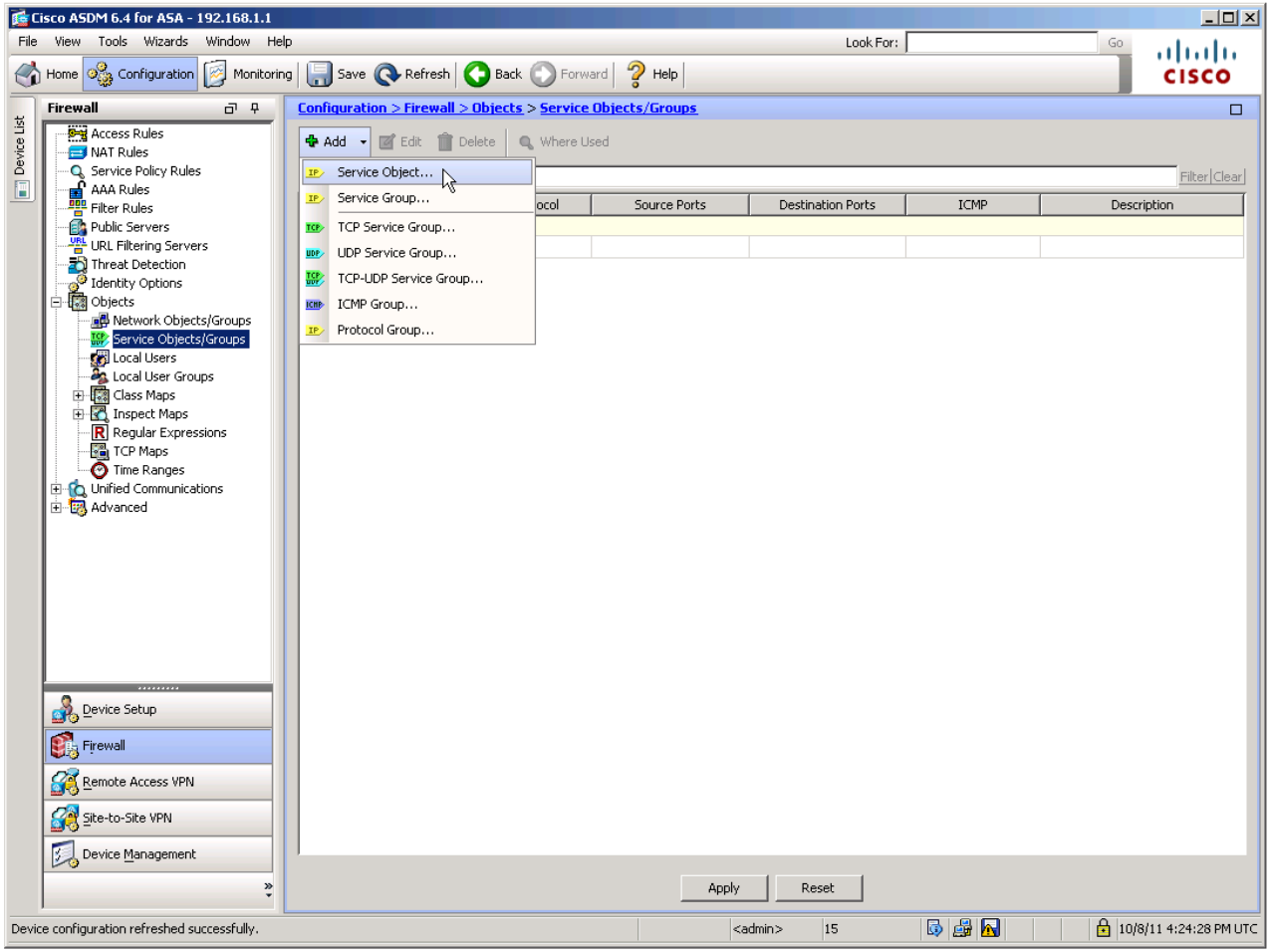
```
CCNAS-ASA(config)# object service SERV-1
CCNAS-ASA(config-service-object)# service tcp destination eq ftp
CCNAS-ASA(config-service-object)# service tcp destination eq www
CCNAS-ASA(config-service-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object
object service SERV-1
 service tcp destination eq www
CCNAS-ASA(config)#
```

# Service Objects

- There are five service options:
  - **service** *protocol* [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies an IP protocol name or number.
  - **service tcp** [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies that the service object is for the TCP protocol.
  - **service udp** [**source** [*operator port*]] [**destination** [*operator port*]]
    - Specifies that the service object is for the UDP protocol.
  - **service icmp** *icmp-type*
    - Specifies that the service object is for the ICMP protocol.
  - **service icmp6** *icmp6-type*
    - Specifies that the service object is for the ICMPv6 protocol.

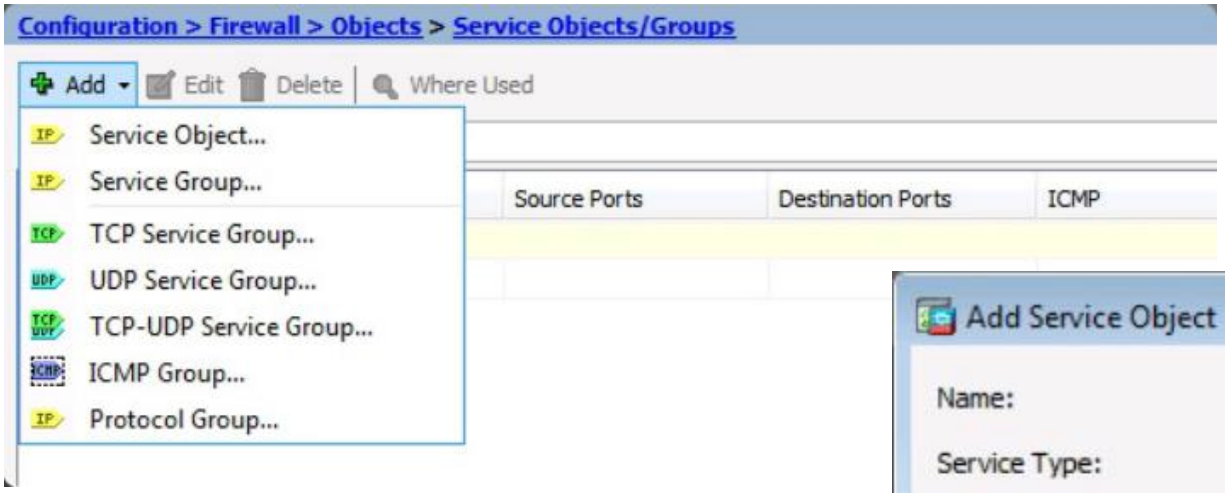
# Configuring a Service Object using ASDM

- Configurations > Firewall > Objects > Service Objects/Groups

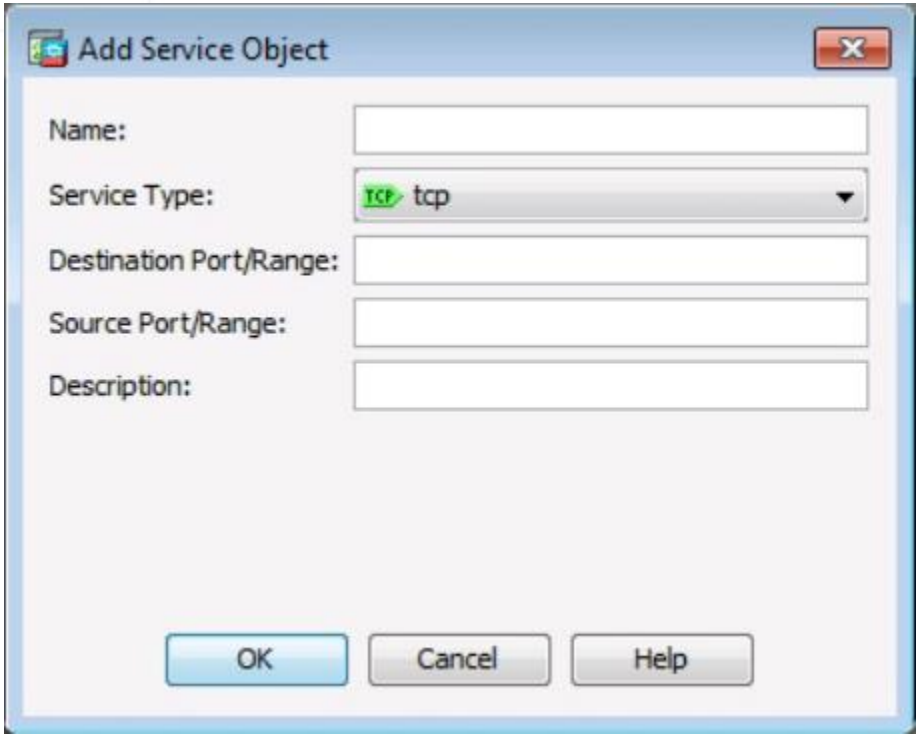


# Objects in ASDM (Cont.)

Adding a Service Object/Group




Add Service Object Window



# Object Groups

- Object groups are used to group objects
  - Objects can be attached or detached from multiple object groups
- Objects can be attached or detached from one or more object groups when needed, ensuring that the objects are not duplicated but can be re-used wherever needed
- You can create network, protocol, and ICMP-type objects groups created using the **`object-group {network | protocol | icmp-type}`** *`group-name`* command
- You can also create service objects groups by using **`object-group service`** *`group-name`* **`[tcp | udp | tcp-udp]`**

# Object Groups

| Object-Group | Description |
|---|---|
| **Network** | • Specifies a list of IP host, subnet, or network addresses. |
| **Protocol** | • Combines IP protocols (such as TCP, UDP, and ICMP) into one object.<br>• For example, to add both TCP and UDP services of DNS, create an object group and add TCP and UDP protocols into that group. |
| **ICMP** | • The ICMP protocol uses unique types to send control messages (RFC 792).<br>• The ICMP-type object group can group the necessary types for security needs. |
| **Service** | • Used to group TCP, UDP, or TCP and UDP ports into an object.<br>• It can contain a mix of TCP services, UDP services, ICMP-type services, and any protocol such as ESP, GRE, and TCP. |

```
CCNAS-ASA(config)# object-group ?

configure mode commands/options:
  icmp-type  Specifies a group of ICMP types, such as echo
  network    Specifies a group of host or subnet IP addresses
  protocol   Specifies a group of protocols, such as TCP, etc
  service    Specifies a group of TCP/UDP ports/services
  user       Specifies single user, local or import user group
CCNAS-ASA(config)# object-group
```

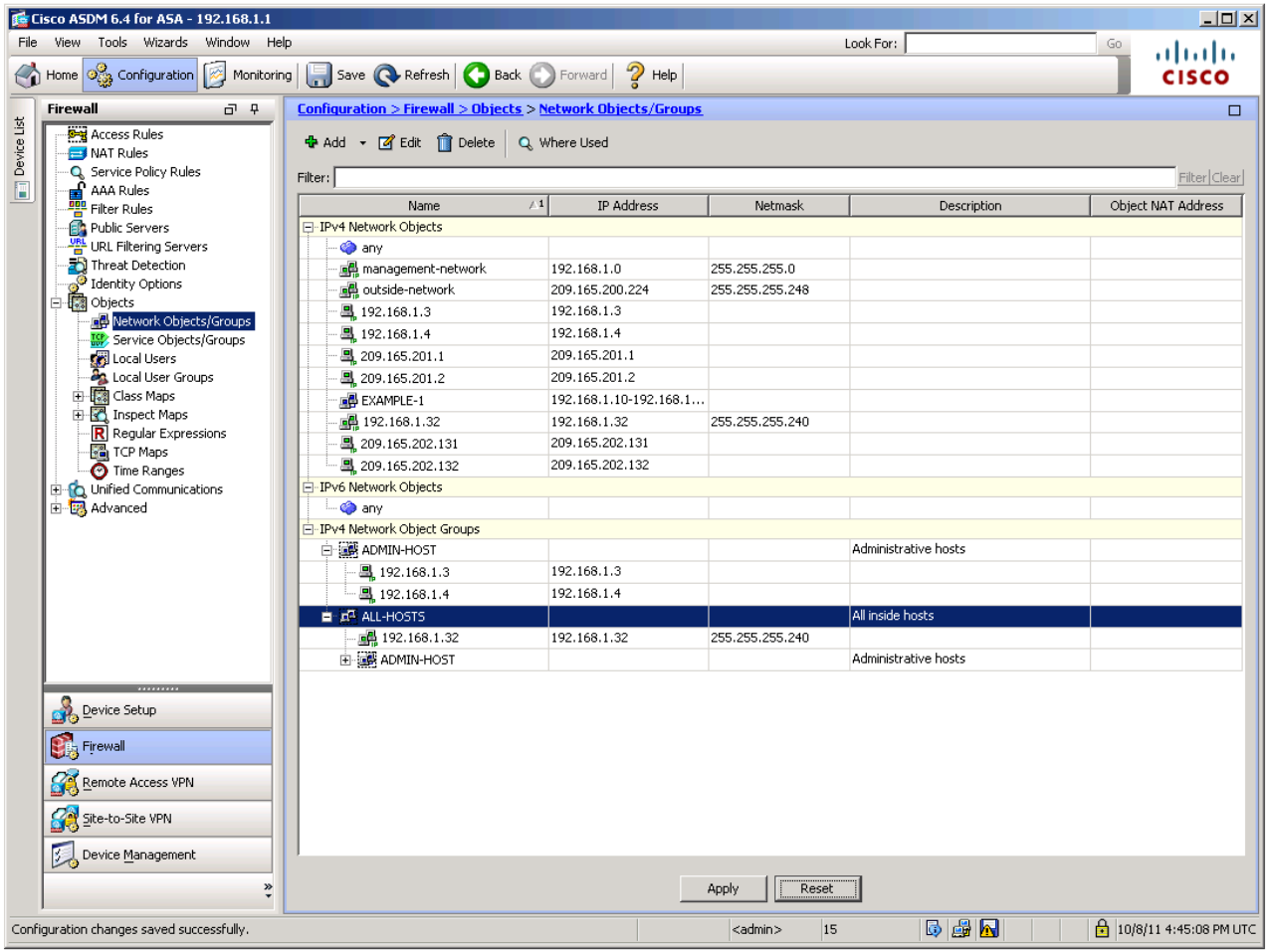
# Network Object Group

- To configure a network object group, use the **object-group network** *grp-name* global configuration command.
- Add network objects to the network group using the commands:
  - **network-object**
  - **group-object**

```
CCNAS-ASA(config)# object-group network ADMIN-HOST
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.3
CCNAS-ASA(config-network-object-group)# network-object host 192.168.1.4
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)# object-group network ALL-HOSTS
CCNAS-ASA(config-network-object-group)# network-object 192.168.1.32 255.255.255.240
CCNAS-ASA(config-network-object-group)# group-object ADMIN-HOST
CCNAS-ASA(config-network-object-group)# exit
CCNAS-ASA(config)# show run object-group
object-group network ADMIN-HOST
 description Administrative host IP addresses
 network-object host 192.168.1.3
 network-object host 192.168.1.4
object-group network ALL-HOSTS
 network-object 192.168.1.32 255.255.255.240
 group-object ADMIN-HOST
CCNAS-ASA(config)#
```

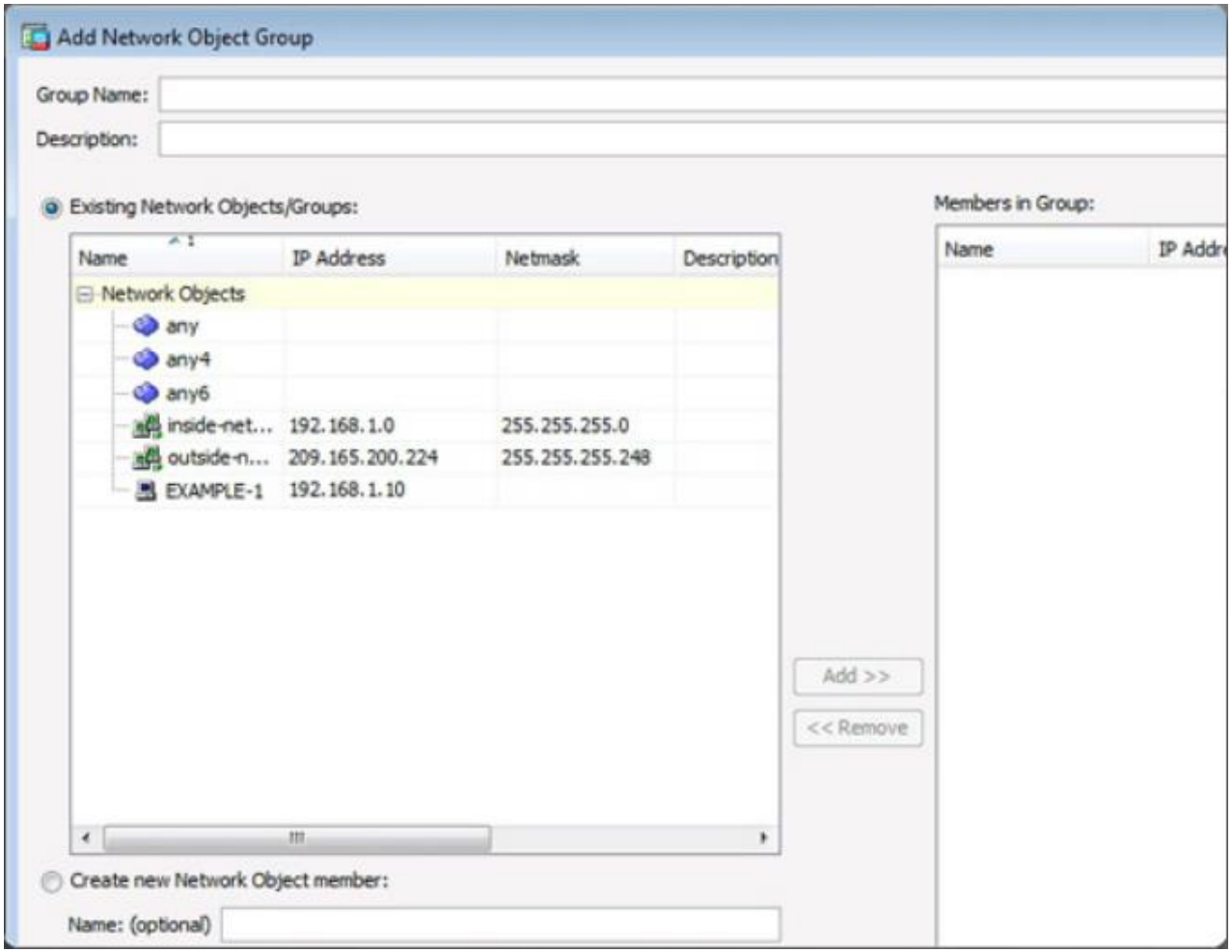
# Network Object Group using ASDM

- **Configuration > Firewall > Objects > Network Objects/Groups**



# Objects in ASDM (Cont.)

Add Network Object Group Window



# Protocol Object Group

- To configure a protocol object group, use the **object-group protocol** *grp-name* global configuration command.
- Add network objects to the protocol group using the commands:
  - **protocol-object**
  - **group-object**

```
CCNAS-ASA(config)# object-group protocol PROTO-1
CCNAS-ASA(config-protocol-object-group)# protocol-object udp
CCNAS-ASA(config-protocol-object-group)# protocol-object ipsec
CCNAS-ASA(config-protocol-object-group)# exit
CCNAS-ASA(config)# object-group protocol PROTO-2
CCNAS-ASA(config-protocol-object-group)# protocol-object tcp
CCNAS-ASA(config-protocol-object-group)# group-object PROTO-1
CCNAS-ASA(config-protocol-object-group)# exit
CCNAS-ASA(config)# show running-config object-group protocol
object-group protocol PROTO-1
 protocol-object udp
 protocol-object esp
object-group protocol PROTO-2
 protocol-object tcp
 group-object PROTO-1
CCNAS-ASA(config)#
```

# ICMP Object Group

- To configure an ICMP object group, use the **object-group icmp-type** *grp-name* global configuration command.
- Add ICMP objects to the protocol group using the commands:
  - **icmp-object**
  - **group-object**

```
CCNAS-ASA(config)# object-group icmp-type ICMP-ALLOWED
CCNAS-ASA(config-icmp-object-group)# icmp-object echo
CCNAS-ASA(config-icmp-object-group)# icmp-object time-exceeded
CCNAS-ASA(config-icmp-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config object-group id ICMP-ALLOWED
object-group icmp-type ICMP-ALLOWED
 icmp-object echo
 icmp-object time-exceeded
CCNAS-ASA(config)#
```

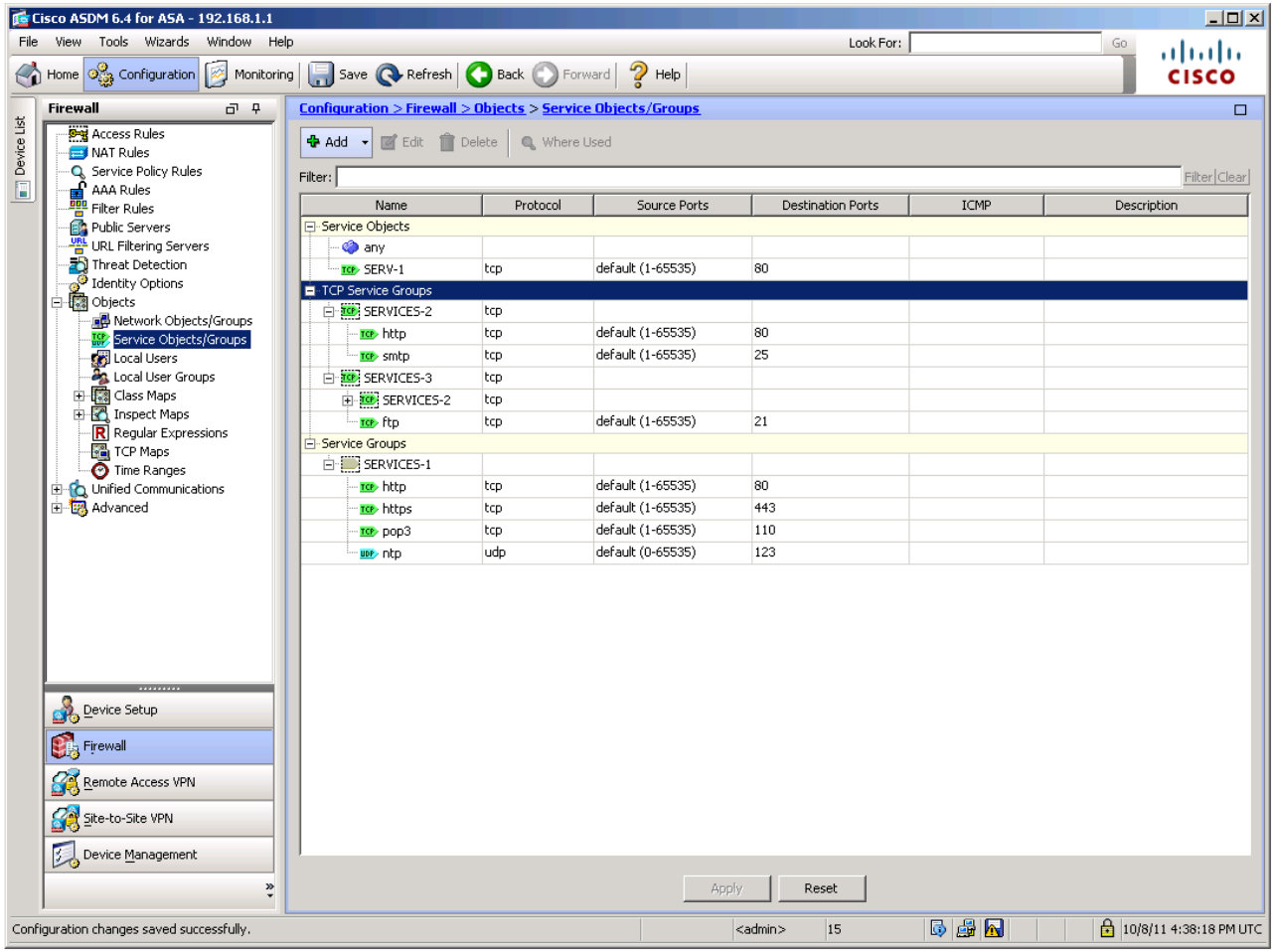
# Service Object Group

- To configure a service object group, use the **object-group service** *grp-name* global configuration command.
- Add service objects to the protocol group using the commands:
  - **service-object**
  - **group-object**

```
CCNAS-ASA(config)# object-group service SERVICES-1
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq www
CCNAS-ASA(config-service-object-group)# service-object tcp destination eq https
CCNAS-ASA(config-service-object-group)# service-object udp destination eq ntp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-2 tcp
CCNAS-ASA(config-service-object-group)# port-object eq pop3
CCNAS-ASA(config-service-object-group)# port-object eq smtp
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service SERVICES-3 tcp
CCNAS-ASA(config-service-object-group)# group-object SERVICES-2
CCNAS-ASA(config-service-object-group)# port-object eq ftp
CCNAS-ASA(config-service-object-group)# port-object range 2000 2005
CCNAS-ASA(config-service-object-group)# exit
CCNAS-ASA(config)#
```

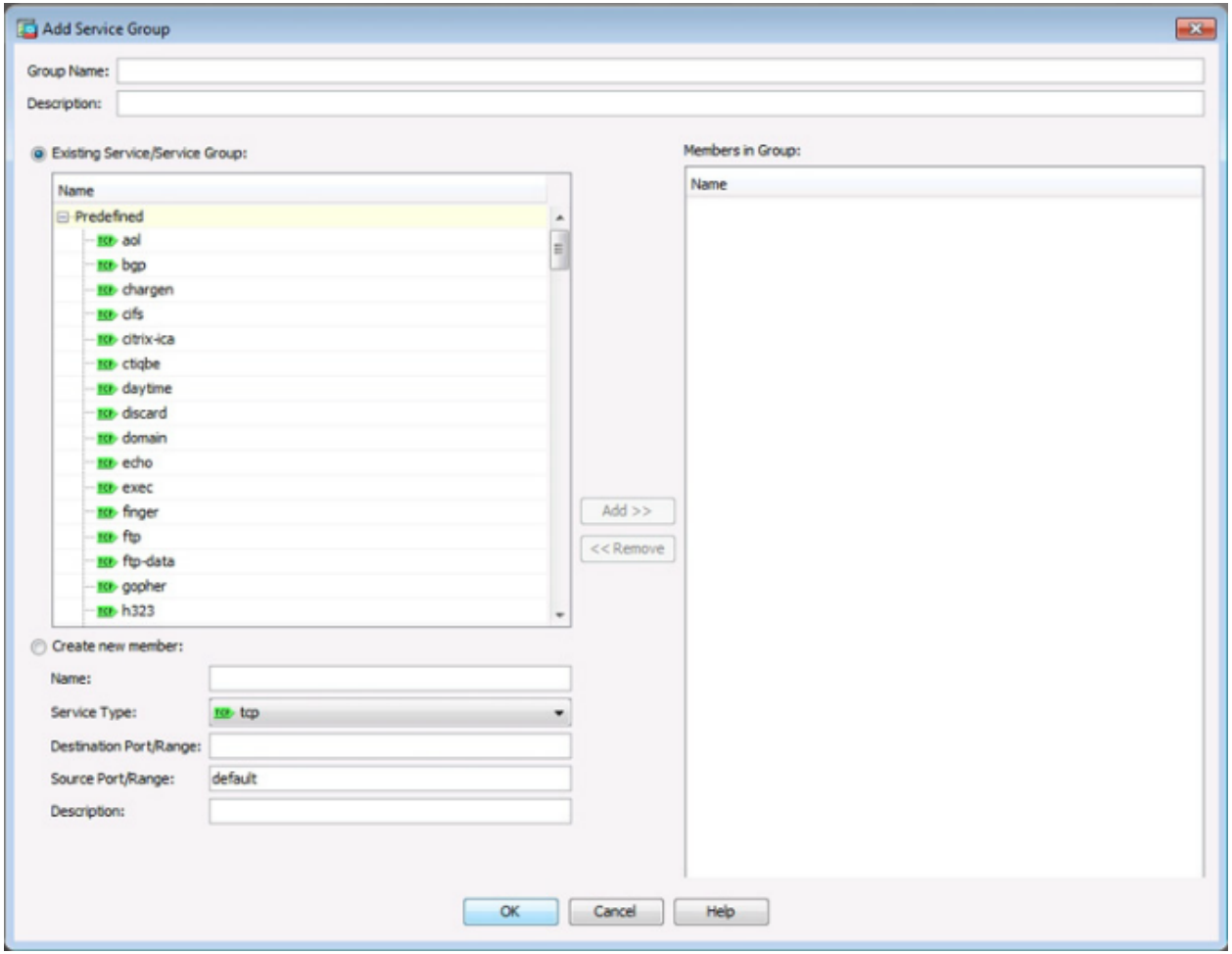
# Services Object Group

- **Configuration > Firewall > Objects > Service Objects/Groups**



# Objects in ASDM (Cont.)

Add Service Object Group Window



# Access Lists

# Similarities Between ASA and IOS ACLs

- Both ACLs are made up of one or more access control entries (ACEs)
- Both ACLs are processed sequentially from top down
- Both follow the 1st ACE match will cause the ACL to be exited
- Both have the implicit deny all at the bottom
- Both support remarks added per ACE or ACL
- Both follow the one access list per interface, per protocol, per direction rule
- Both ACLs can be enabled/disabled based on time ranges

# Differences Between ASA and IOS ACLs

- The ASA ACL uses a network mask (e.g., 255.255.255.0)
  - The IOS ACL uses the wildcard mask (e.g., 0.0.0.255)
- ACLs are always named instead of numbered
  - ASA ACLs can be numbered but unlike IOS ACL the numbers have no significance other than naming the ACL
- By default, security levels apply access control without an ACL configured

# ACL Function

- ACLs on a security appliance can be used:
  - Through-traffic packet filtering:
    - Traffic is passing through the appliance from one interface to another interface
    - The configuration requires an ACL to be defined and then applied to an interface
  - To-the-box-traffic packet filtering:
    - Also known as a management access rule, traffic (e.g., Telnet, SSH, SNMP) is destined for the appliance
    - Introduced to filter traffic destined to the control plane of the ASA
    - It is completed in one step but requires an additional set of rules to implement access control

# Five Types of ASA ACL Types

- The ASA supports five types of ACLs

| ACL Type | Description |
|---|---|
| **Extended** | • Most popular type of ASA ACL.<br>• Filters on source/destination port and protocol. |
| **Standard** | • Used for routing protocols, not firewall rules.<br>• Cannot be applied to interfaces to control traffic. |
| **IPv6** | • Used to support IPv6 addressing. |
| **Webtype** | • Used for clientless SSL VPN. |
| **Ethertype** | • Specifies network layer protocol.<br>• Only used with transparent mode. |

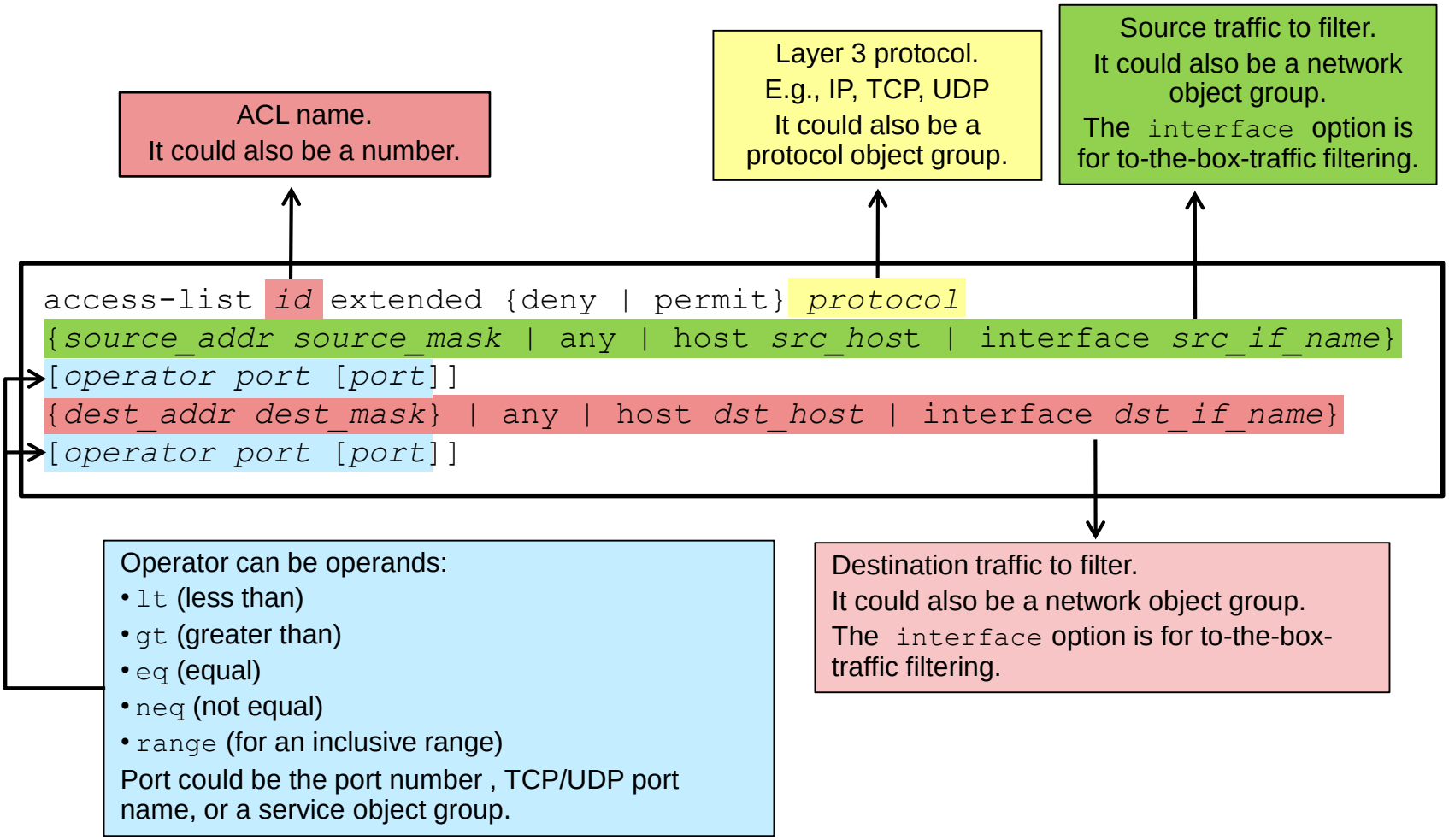
# ACL Applications

| ACL Use | ACL Type | Description |
|---|---|---|
| Provide through-traffic network access | Extended | • By default, the ASA does not allow lower security traffic to a higher security interface unless it is explicitly permitted. |
| Identify traffic for AAA rules | Extended | • Used in AAA access lists to identify traffic. |
| Identify addresses for NAT | Extended | • Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses. |
| Establish VPN access | Extended | • Used in VPN commands. |
| Identify traffic Modular Policy Framework (MPF) | Extended | • Used to identify traffic in a class map, which is used for features that support MPF. |
| Identify OSPF route redistribution | Standard | • Standard access lists include only the destination address.<br>• Used to control the redistribution of OSPF routes. |
| Control network access for IPV6 networks | IPv6 | • Used for control traffic in IPv6 networks. |

# Extended ACL Command Syntax

```
CCNAS-ASA(config)# help access-list

USAGE:


Extended access list:
          Use this to configure policy for IP traffic through the firewall

[no] access-list <id> [line <line_num>] [extended] {deny | permit}
                     {<protocol> | object-group {<service_obj_grp_id> |
                     <protocol_obj_grp_id>} | object <service_object_name>}
                     [user-group [<domain_nickname>\\]<user_group_name> |
                      user [<domain_nickname>\]<user_name> |
                      object-group-user < object_group_user_name>]
                     {host <sip> | <sip> <smask> | interface <ifc> | any |
                     object-group <network_obj_grp_id> |
                     object <network_obj_name>}
                     [<operator> <port> [<port>] |
                     object-group <service_obj_grp_id>]
                     {host <dip> | <dip> <dmask> | interface <ifc> | any |
                     object-group <network_obj_grp_id> |
                     object <network_obj_name>}
                     [<operator> <port> [<port>] |
                     object-group <service_obj_grp_id>]
                     [log [disable] | [<level>] | [default] [interval <secs>]]

<Output omitted>
```

# Condensed ACL



# Access-group Syntax

- To provide through-traffic network access, the ACL must be applied to an interface.
  - **access-group** *acl-id* {**in** | **out**} **interface** *interface-name* [**per-user-override** | **control-plane**]

| Syntax | Description |
|---|---|
| **access-group** | Keyword used to apply an ACL to an interface. |
| *acl-id* | The name of the actual ACL to be applied to an interface. |
| **in** | The ACL will filter inbound packets. |
| **out** | The ACL will filter outbound packets. |
| **interface** | Keyword to specify the interface to which to apply the ACL. |
| *interface_name* | The name of the interface to which to apply an ACL. |
| **per-user-override** | Option that allows downloadable ACLs to override the entries on the interface ACL. |
| **control-plane** | Specifies if the rule is for to-the-box traffic. |

# ACL Examples

| ACL Examples |
| --- |
| |
| |
| |
| |

# Allowing Same Security Level Communication

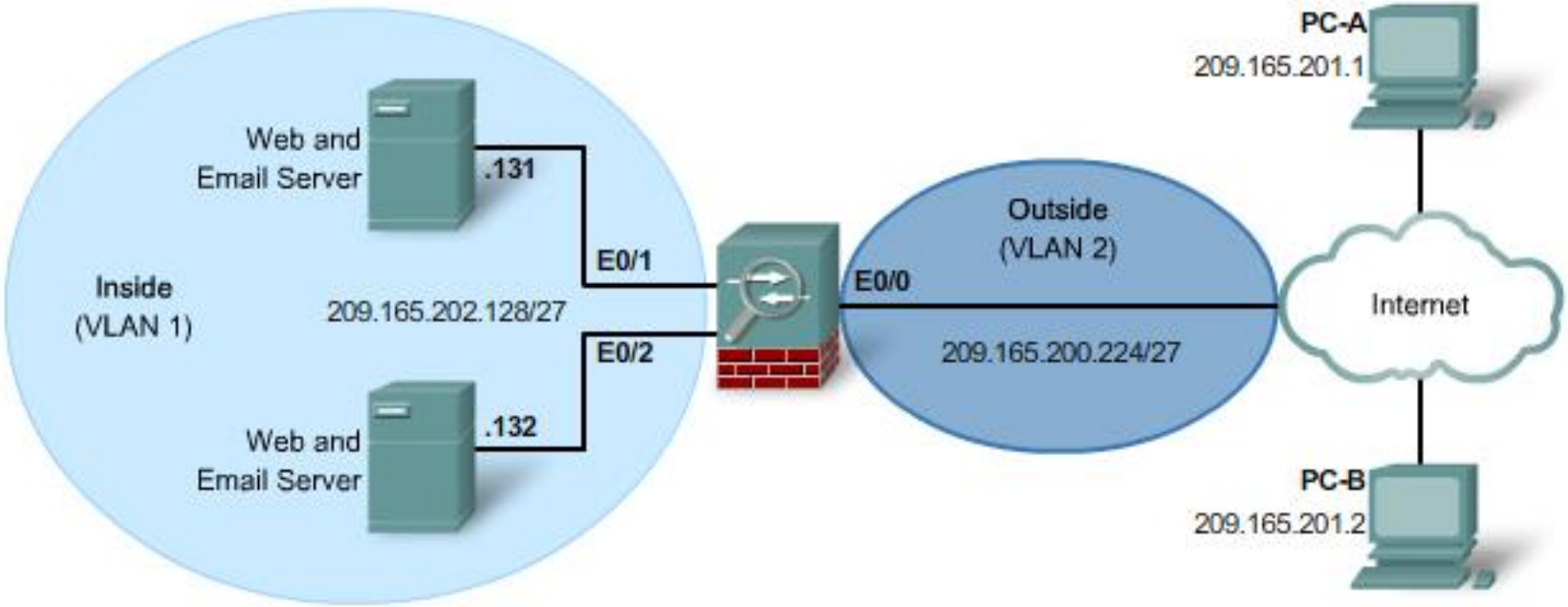
- By default, interfaces on the same security level:
  - Cannot communicate with each other.
  - Packets cannot enter and exit the same interface.
    - Useful for VPN traffic that enters an interface, but is then routed out the same interface.
- Use the **`same-security-traffic permit inter-interface`** enables interfaces on the same security level so that they can communicate with each other.
- Use the **`same-security-traffic permit intra-interface`** command to enable communication between hosts connected to the same interface.

# Verifying ACLs

- To verify the ACL syntax, use the following commands:
  - **`show running-config access-list`**
  - **`show access-list`**

# ACL - Example 1

- PC-A and PC-B are external hosts that require access to the two internal servers.
  - Each server provides Web and email services.



# ACL - Example 1

```
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-A -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-A -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.1 host
                   209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-B -> Server A for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.131 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.131 eq smtp
CCNAS-ASA(config)# access-list ACL-IN remark Permit PC-B -> Server B for HTTP / SMTP
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.132 eq http
CCNAS-ASA(config)# access-list ACL-IN extended permit tcp host 209.165.201.2 host
                   209.165.202.132 eq smtp
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
```

# ACL - Example 1

- Verify the configuration.
- Notice that there are 9 elements (9 ACEs), excluding the remarks, that must be processed by the ASA.

```
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Permit PC-A -> Server A for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq www
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.131 eq smtp
access-list ACL-IN remark Permit PC-A -> Server B for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq www
access-list ACL-IN extended permit tcp host 209.165.201.1 host 209.165.202.132 eq smtp
access-list ACL-IN remark Permit PC-B -> Server A for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq www
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.131 eq smtp
access-list ACL-IN remark Permit PC-B -> Server B for HTTP / SMTP
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq www
access-list ACL-IN extended permit tcp host 209.165.201.2 host 209.165.202.132 eq smtp
access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# show access-list ACL-IN brief
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
CCNAS-ASA(config)#
```

# ACL with Object Groups - Example 2

- This example achieves the same result as Example 1 except it uses object groups to simplify and modularize the configuration
- The following object groups are created:
  - **TCP:** Protocol object group
  - **Internet-Hosts:** Network object group identifying the two external hosts
  - **Internal-Servers:** Network object group identifying the two internal servers
  - **HTTP-SMTP:** Service object group identifying HTTP and SMTP protocols
- These object groups are then specified in one ACL-IN ACE.
- All remaining traffic will be denied and logged

# ACL with OGs - Example 2

- Create Object groups

```
CCNAS-ASA(config)# object-group protocol TCP
CCNAS-ASA(config-protocol)# description OG identifies TCP as the protocol
CCNAS-ASA(config-protocol)# protocol-object tcp
CCNAS-ASA(config-protocol)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network Internet-Hosts
CCNAS-ASA(config-network)# description OG matches PC-A and PC-B
CCNAS-ASA(config-network)# network-object host 209.165.201.1
CCNAS-ASA(config-network)# network-object host 209.165.201.2
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group network Internal-Servers
CCNAS-ASA(config-network)# description OG matches Web and email Servers
CCNAS-ASA(config-network)# network-object host 209.165.202.131
CCNAS-ASA(config-network)# network-object host 209.165.202.132
CCNAS-ASA(config-network)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object-group service HTTP-SMTP tcp
CCNAS-ASA(config-service)# description OG matches SMTP and HTTP/HTTPS traffic
CCNAS-ASA(config-service)# port-object eq smtp
CCNAS-ASA(config-service)# port-object eq www
CCNAS-ASA(config-service)# exit
CCNAS-ASA(config)#
```

# ACL with OGs - Example 2

- Create the ACL and apply it

```
CCNAS-ASA(config)# access-list ACL-IN remark Only permit PC-A / PC-B -> servers
CCNAS-ASA(config)# access-list ACL-IN extended permit object-group TCP
object-group Internet-Hosts object-group Internal-Servers object-group HTTP-SMTP
CCNAS-ASA(config)# access-list ACL-IN extended deny ip any any log
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-group ACL-IN in interface outside
CCNAS-ASA(config)#
CCNAS-ASA(config)# show running-config access-list
access-list ACL-IN remark Only permit PC-A / PC-B -> servers
access-list ACL-IN extended permit object-group TCP object-group Internet-Hosts object-
group Internal-Servers object-group HTTP-SMTP
CCNAS-ASA(config)#
CCNAS-ASA(config)# show access-list ACL-IN brief
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
CCNAS-ASA(config)#
```

# ACL with OGs - Example 2

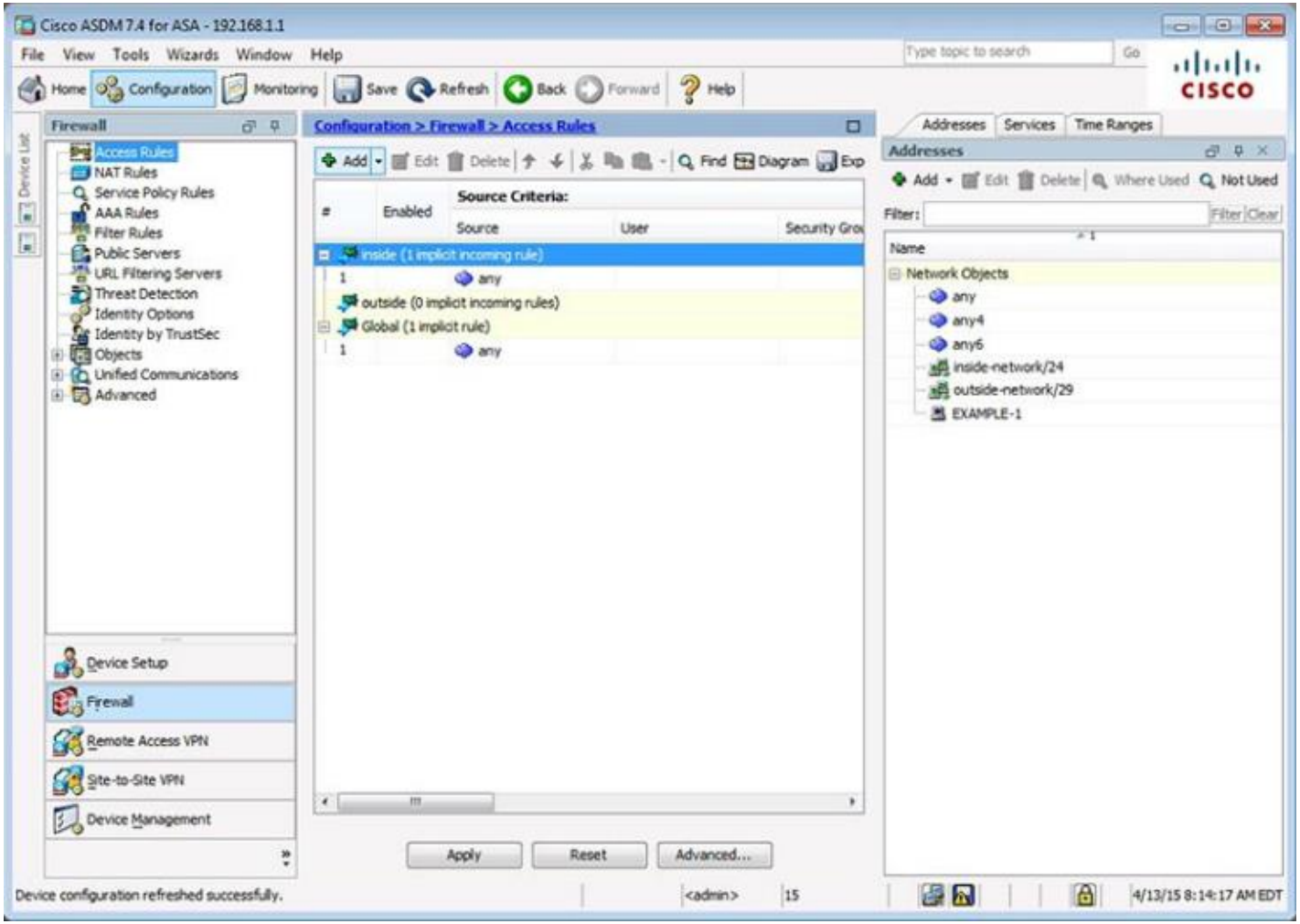
- Display the content of ACL-IN

```
CCNAS-ASA(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list ACL-IN; 9 elements; name hash: 0x44d1c580
access-list ACL-IN line 1 remark Only permit PC-A / PC-B -> servers
access-list ACL-IN line 2 extended permit object-group TCP object-group Internet-Hosts
object-group Internal-Servers object-group HTTP-SMTP 0xbd5ed7a7
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.131 eq
smtp (hitcnt=0) 0x3f0a0233
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.131 eq
www (hitcnt=0) 0xab920b7c
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.132 eq
smtp (hitcnt=0) 0x92b62c8c
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.1 host 209.165.202.132 eq
www (hitcnt=0) 0x52206d23
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.131 eq
smtp (hitcnt=0) 0x68a43a2d
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.131 eq
www (hitcnt=0) 0x46270b1a
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.132 eq
smtp (hitcnt=0) 0x9fe1ca85
  access-list ACL-IN line 3 extended permit tcp host 209.165.201.2 host 209.165.202.132 eq
www (hitcnt=0) 0x598855e6
access-list ACL-IN line 4 extended deny ip any any log informational interval 300
(hitcnt=0) 0x4d6e3bb6
CCNAS-ASA(config)#
```

# Configuring ACLs Using ASDM

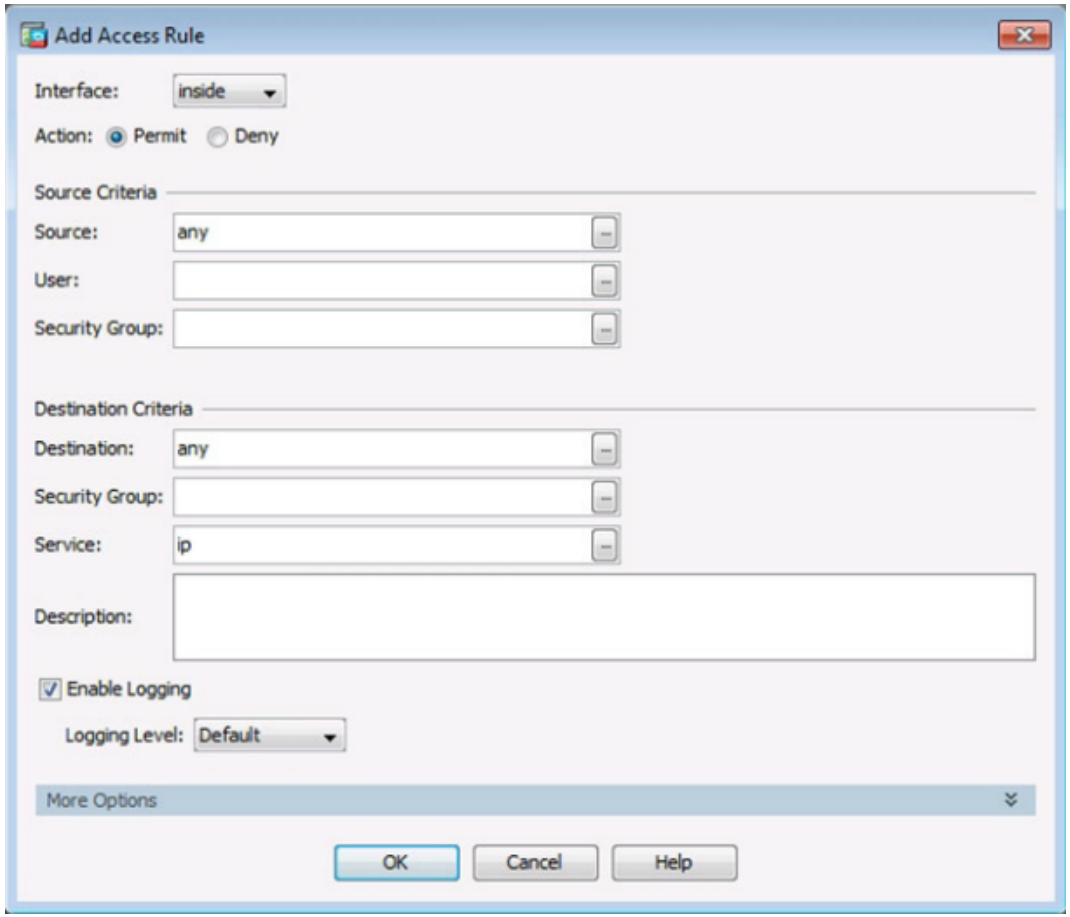
ACLs in ASDM

**Configuration > Firewall > Access Rules**

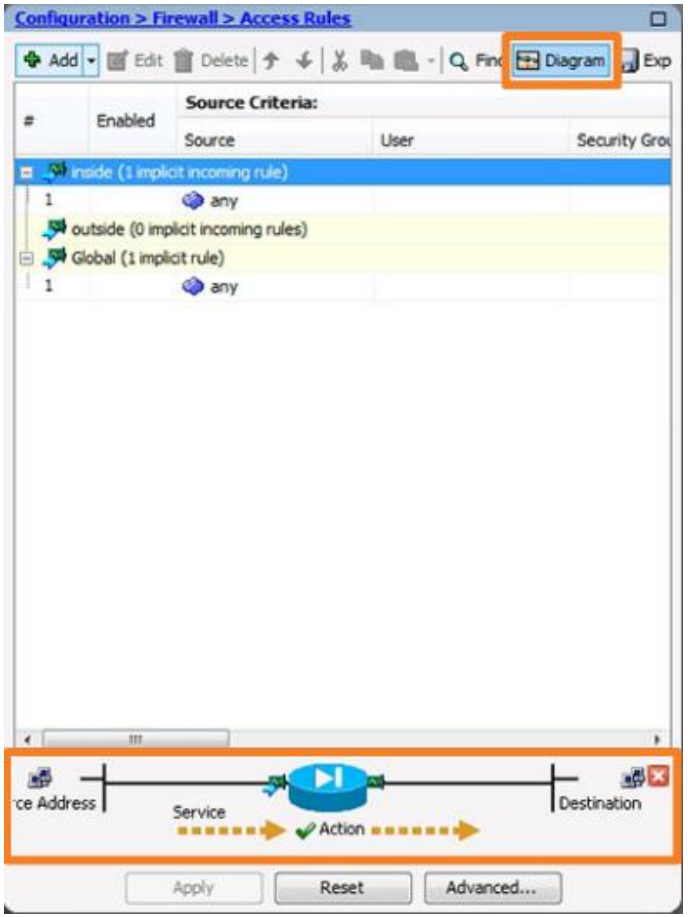


# Configuring ACLs Using ASDM (Cont.)

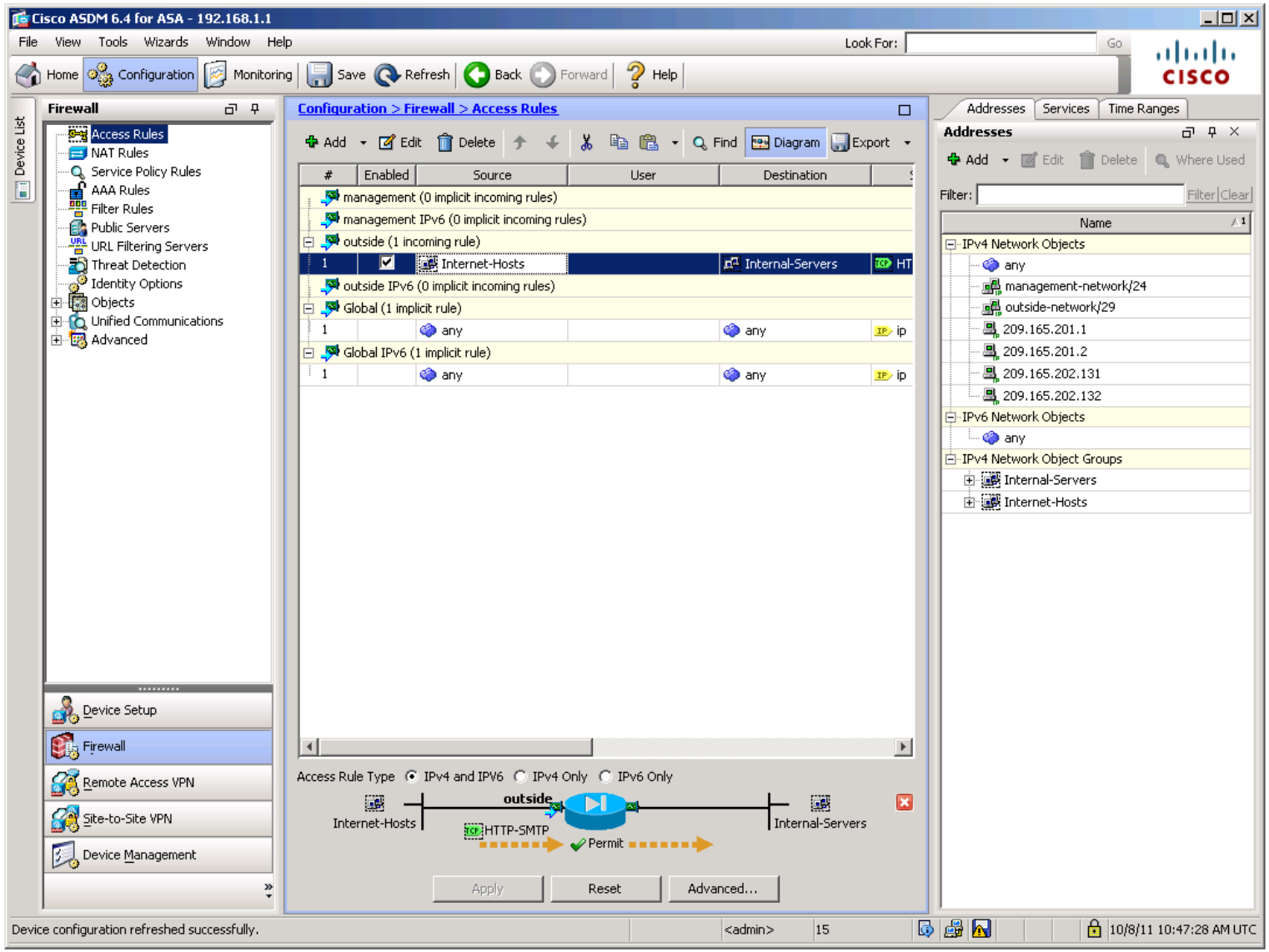
Add Access Rule Window




Diagramming Access Rules



# ACL with Object Group Example

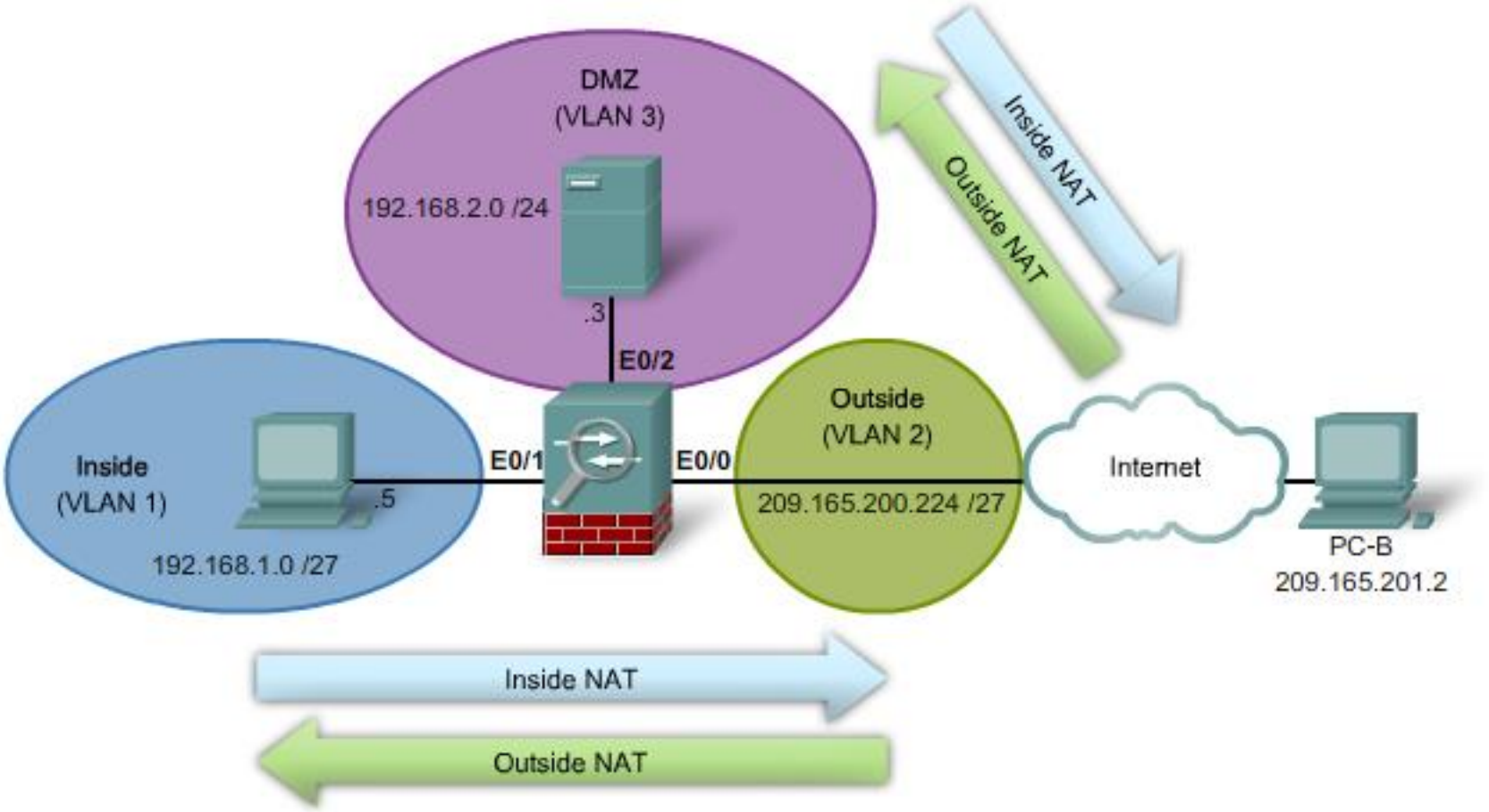


# Network Address Translation

# ASA NAT Services

- Like IOS routers, the ASA supports the following NAT and PAT deployment methods:
- **Inside NAT**
  - Typical NAT deployment method when the ASA translates the internal host address to a global address
  - The ASA restores return traffic the original inside IP address
- **Outside NAT**
  - Deployment method used when traffic from a lower-security interface is destined for a higher-security interface
  - This method may be useful to make a host on the outside appear as one from a known internal IP address
- **Bidirectional NAT**
  - Both inside NAT and outside NAT are used together

# NAT Deployment Methods



# Auto NAT

- Introduced in ASA version 8.3, the Auto NAT feature has simplified the NAT configuration as follows:
  1. Create a network object
  2. Identify host(s) network to be translated
  3. Define the **`nat`** command parameters

**NOTE:**

- Prior to ASA version 8.3, NAT was configured using the **`nat`**, **`global`**, and **`static`** commands
- The **`global`** and **`static`** commands are no longer recognized

# Configuring NAT

- The ASA divides the NAT configuration into two sections:
  - The first section defines the network to be translated using a network object.
  - The second section defines the actual **`nat`** command parameters.
- These appear in two different places in the running-config.

```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
CCNAS-ASA# show running-config nat
!
object network INSIDE-NET
 nat (inside,outside) dynamic interface
CCNAS-ASA#
CCNAS-ASA# show running-config object
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.224
CCNAS-ASA#
```

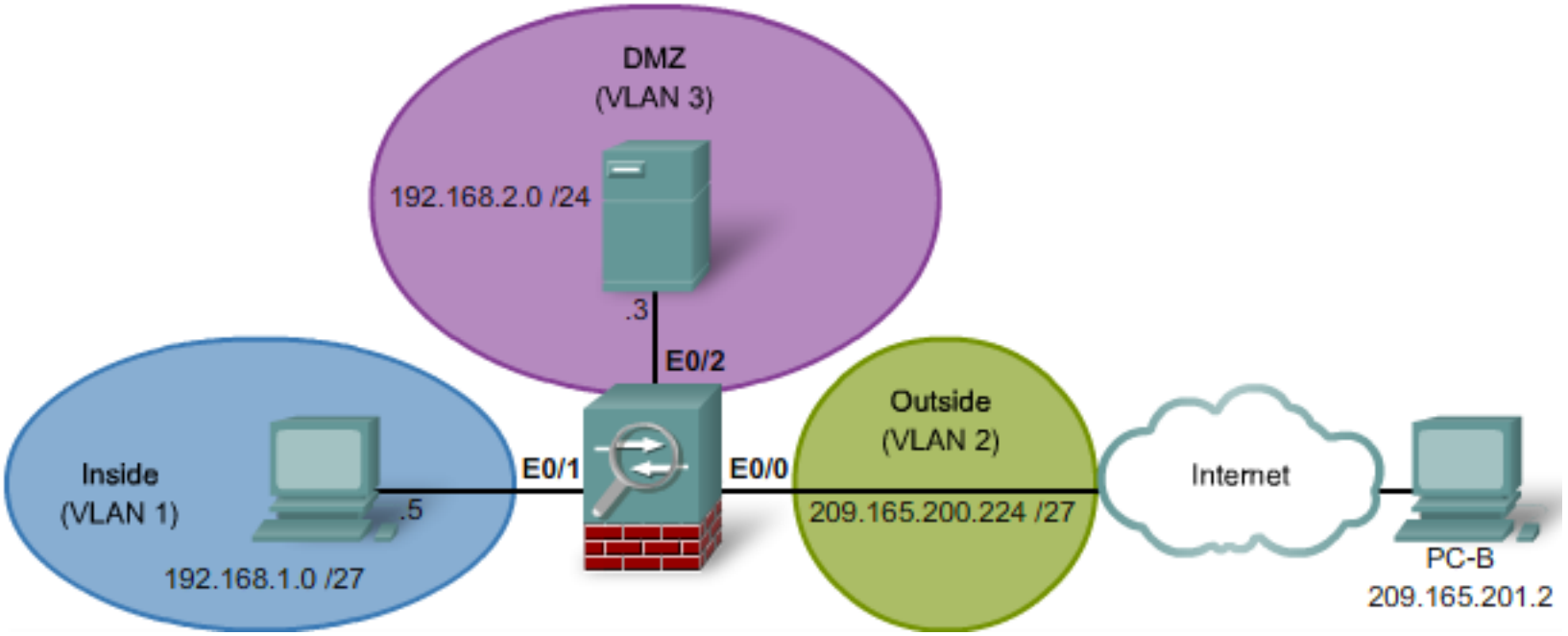
# Types of NAT Configurations

- **Dynamic NAT**
  - Many-to-many translation
  - Typically deployed using inside NAT
- **Dynamic PAT**
  - Many-to-one translation
  - Usually an inside pool of private addresses overloading an outside interface or outside address
  - Typically deployed using inside NAT
- **Static NAT**
  - A one-to-one translation
  - Usually an outside address mapping to an internal server
  - Typically deployed using outside NAT
- **Twice-NAT**
  - ASA version 8.3 NAT feature that identifies both the source and destination address in a single rule (nat command)
  - Used when configuring remote-access IPsec and SSL VPNs

# Configuring Dynamic NAT

- To configure dynamic NAT, two network objects are required
- The first network object identifies the pool of public IP addresses that internal addresses will be translated to
  - **object network** *mapped-obj*
    - Names the network object that identifies the pool of public addresses
  - **range** *ip-addr-1 ip-addr-n*
    - Assigns the public pool IP addresses in a range
- The second network object binds the two objects together
  - **object network** *nat-object-name*
    - Names the NAT object to bind the inside subnet with the public pool network object
  - **subnet** *net-address net-mask*
    - Identifies the inside network subnet to the named object
  - **nat (***real-ifc,mapped-ifc***) dynamic** *mapped-obj*
    - Traffic going from the *real-ifc* and going to the *mapped-ifc* will be dynamically assigned addresses from the public pool of addresses

# Configuring Dynamic NAT Example

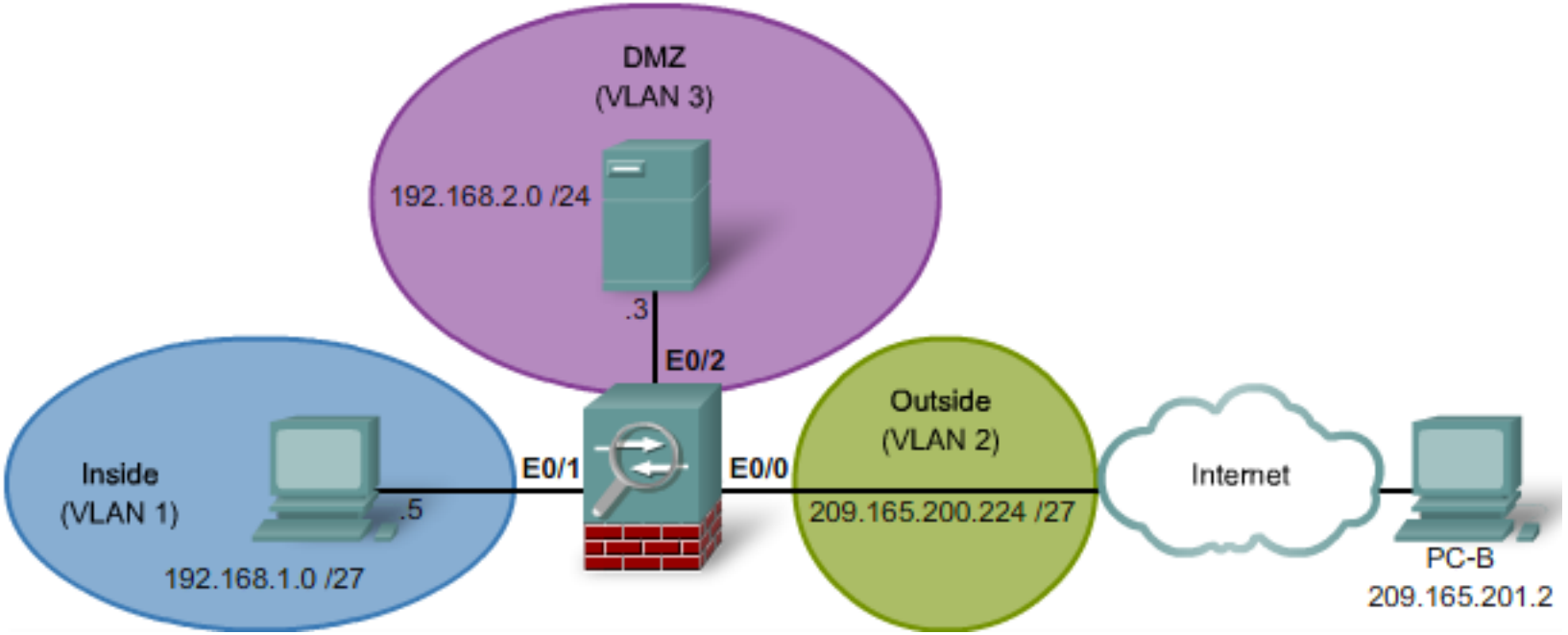



```
CCNAS-ASA(config)# object network PUBLIC-IP
CCNAS-ASA(config-network-object)# range 209.165.200.240 255.255.255.240
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic PUBLIC-IP
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

# Configuring Dynamic PAT

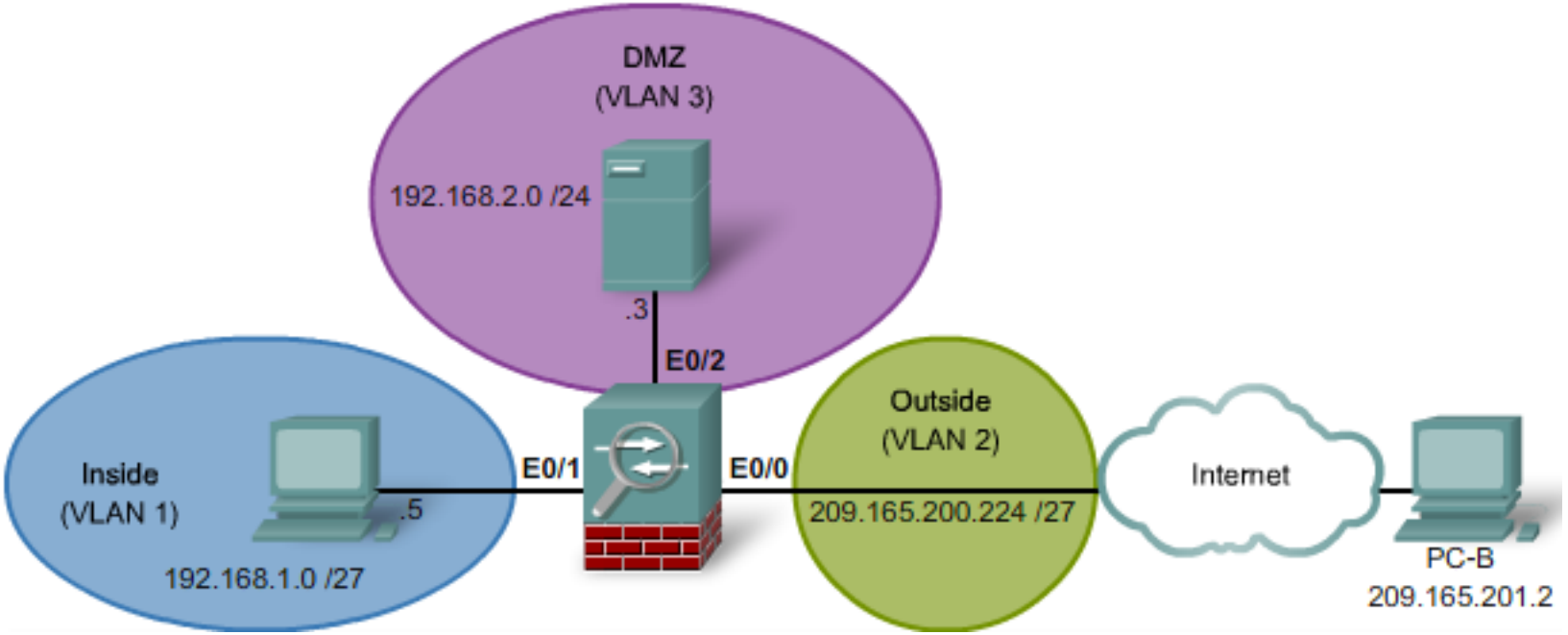
- Dynamic PAT is when the outside interface IP address or another specified IP address is overloaded.
- Only one network object is required to configure dynamic PAT:
  - **object network** *nat-object-name*
    - Names the static NAT object.
  - **subnet** *net-address net-mask*
    - Identifies the inside network subnet as the network object.
  - **nat (***real-ifc,mapped-ifc***) dynamic** [**interface** | *ip-address*]
    - Traffic going from the *real-ifc* interface to the *mapped-ifc* interface will be dynamically the IP address of the outside interface or a specified outside IP address.
    - The parentheses and comma **(,)** are required.

# Configuring Dynamic PAT Example




```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

# Configuring Dynamic PAT Example




```
CCNAS-ASA(config)# object network INSIDE-NET
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.224
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic 209.165.200.229
CCNAS-ASA(config-network-object)# end
CCNAS-ASA#
```

- As an alternative, you can specify an outside IP address.

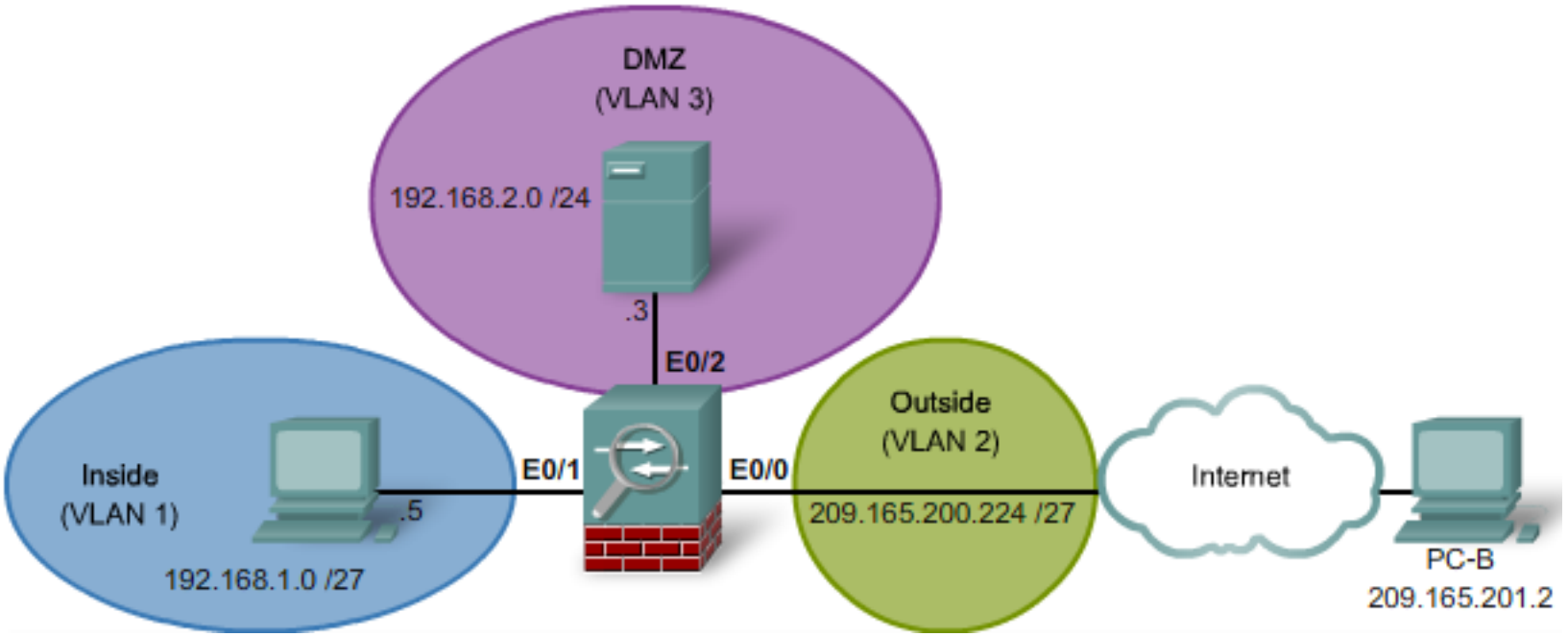
# Configuring Static NAT

- Static NAT maps an inside IP address to an outside address
  - To access Web servers by outside hosts
- To configure static NAT:
  - **`object network`** *`nat-object-name`*
    - Names the static NAT object
  - **`host`** *`ip-addr`*
    - Identifies the inside host IP address
  - **`nat (`***`real-ifc, mapped-ifc`***`) static`** *`mapped-ip-addr`*
    - Statically maps an inside address to an identified outside IP address.
    - The parentheses and comma **`(,)`** are required
    - Note that the **`any`** keyword could be used instead of the interface names to allow the translation of an object between multiple interfaces using one CLI command

**NOTE:**

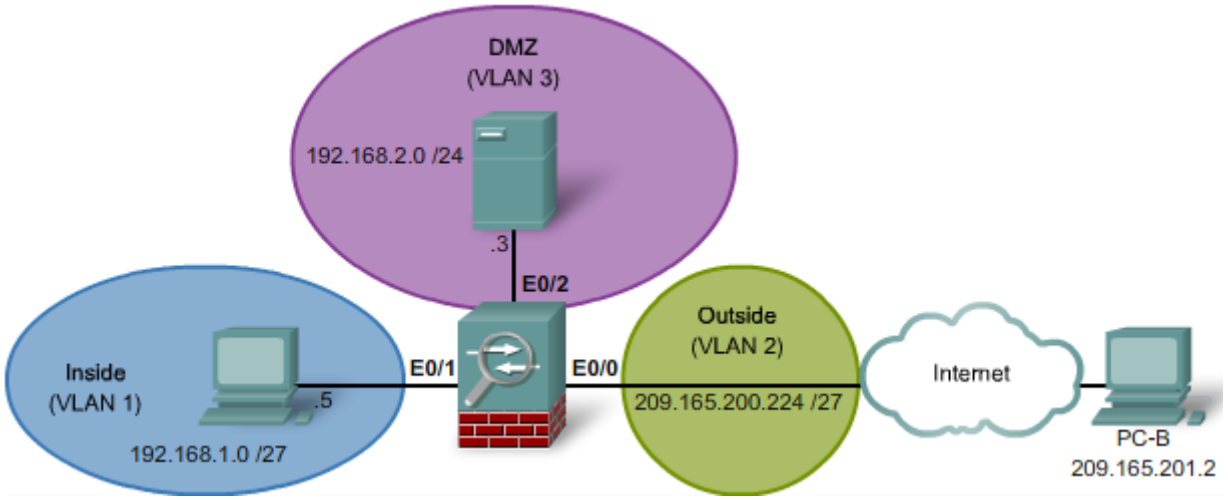
- Static NAT also requires that an ACE be added to the outside interface ACL

# Static NAT Example




```
CCNAS-ASA(config)# object network DMZ-SERVER
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.200.165.227
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
CCNAS-ASA(config)#
```

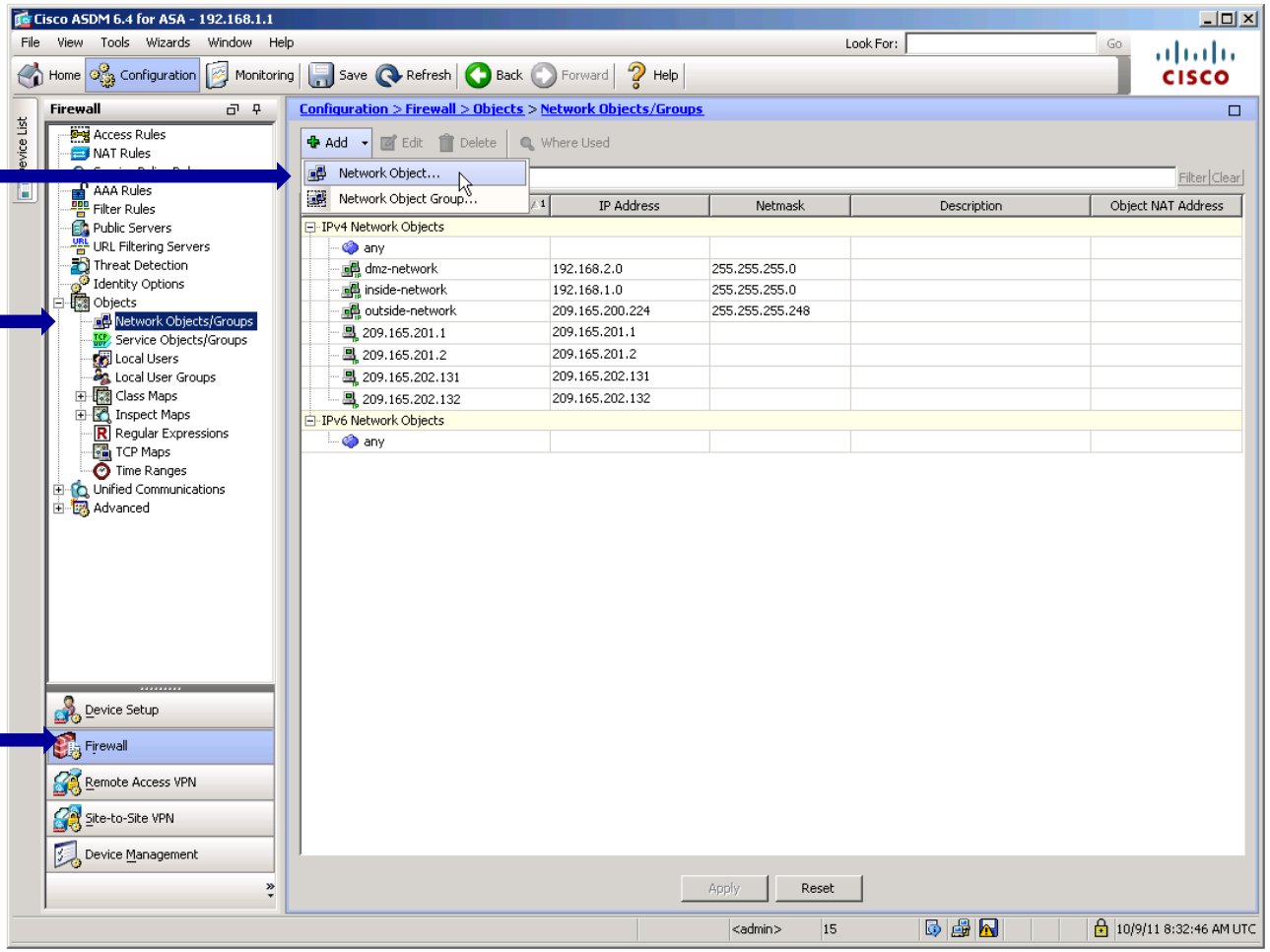
# Verifying Static NAT



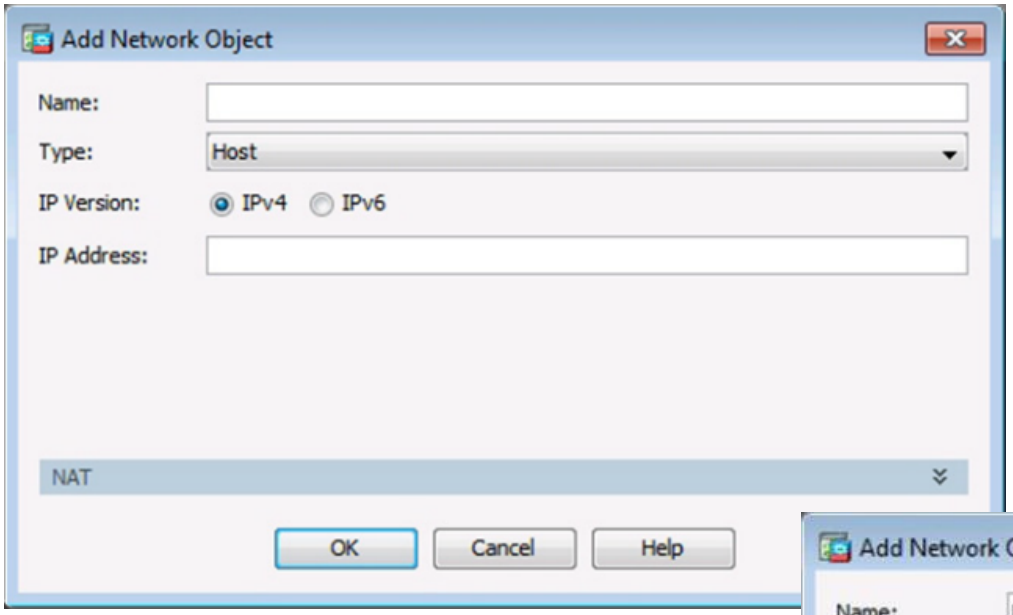

```
CCNAS-ASA# show nat

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ-SERVER 209.165.200.227
    translate_hits = 0, untranslate_hits = 4

2 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 0

CCNAS-ASA# show xlate
1 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from dmz:192.168.2.3 to outside:209.165.200.227 flags s idle 0:22:58 timeout 0:00:00
CCNAS-ASA#
```

# Add Network Object

- **Configuration > Firewall > Objects > Network Objects/Groups**

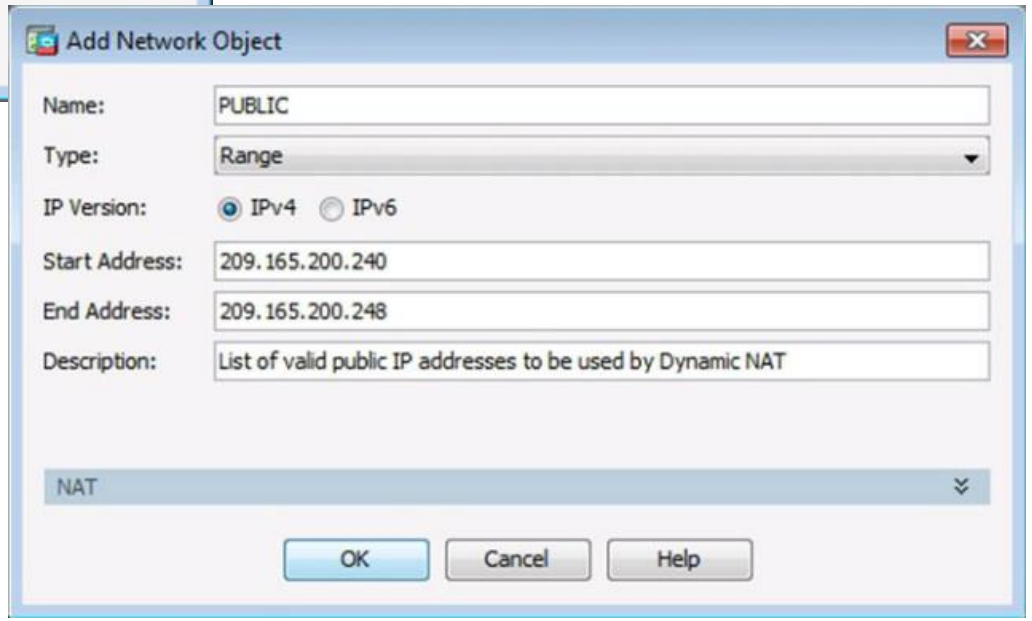


# Configuring Dynamic NAT in ASDM

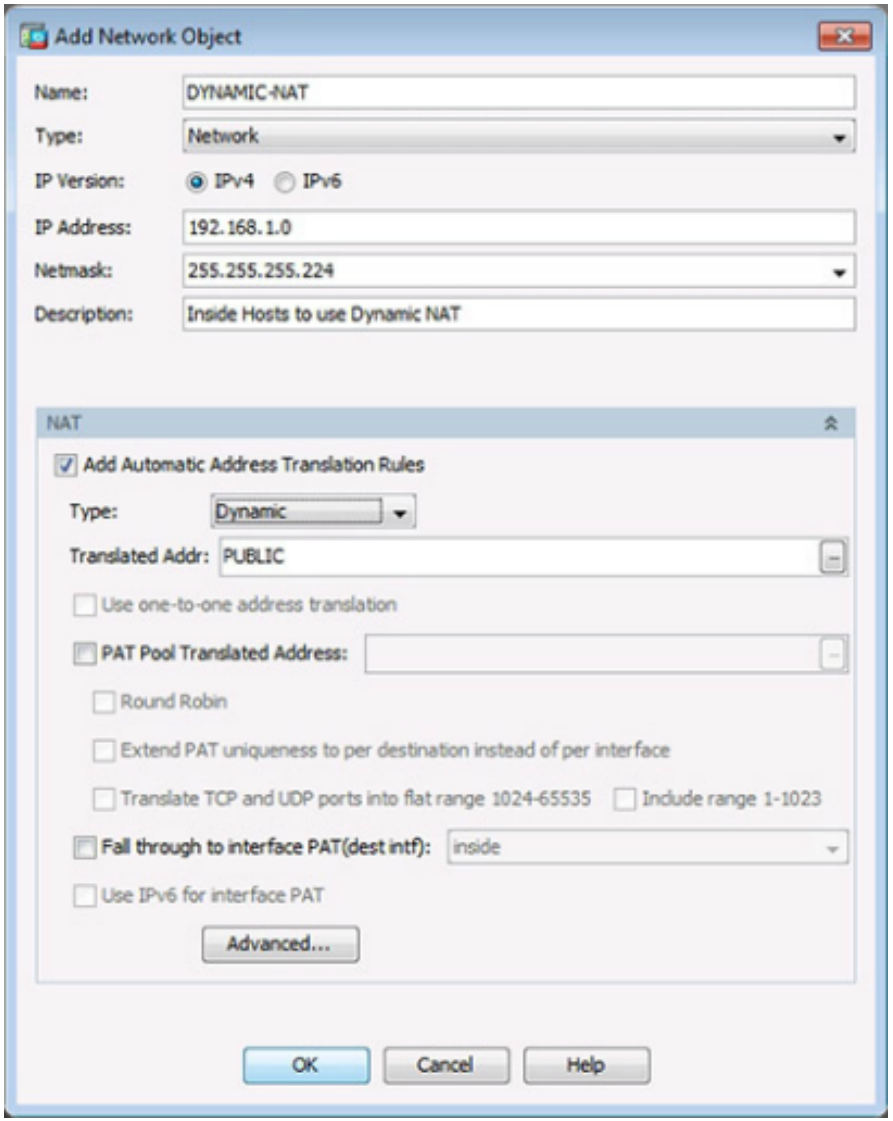



Add Network Object Window

Creating a Network Object for Public Addresses



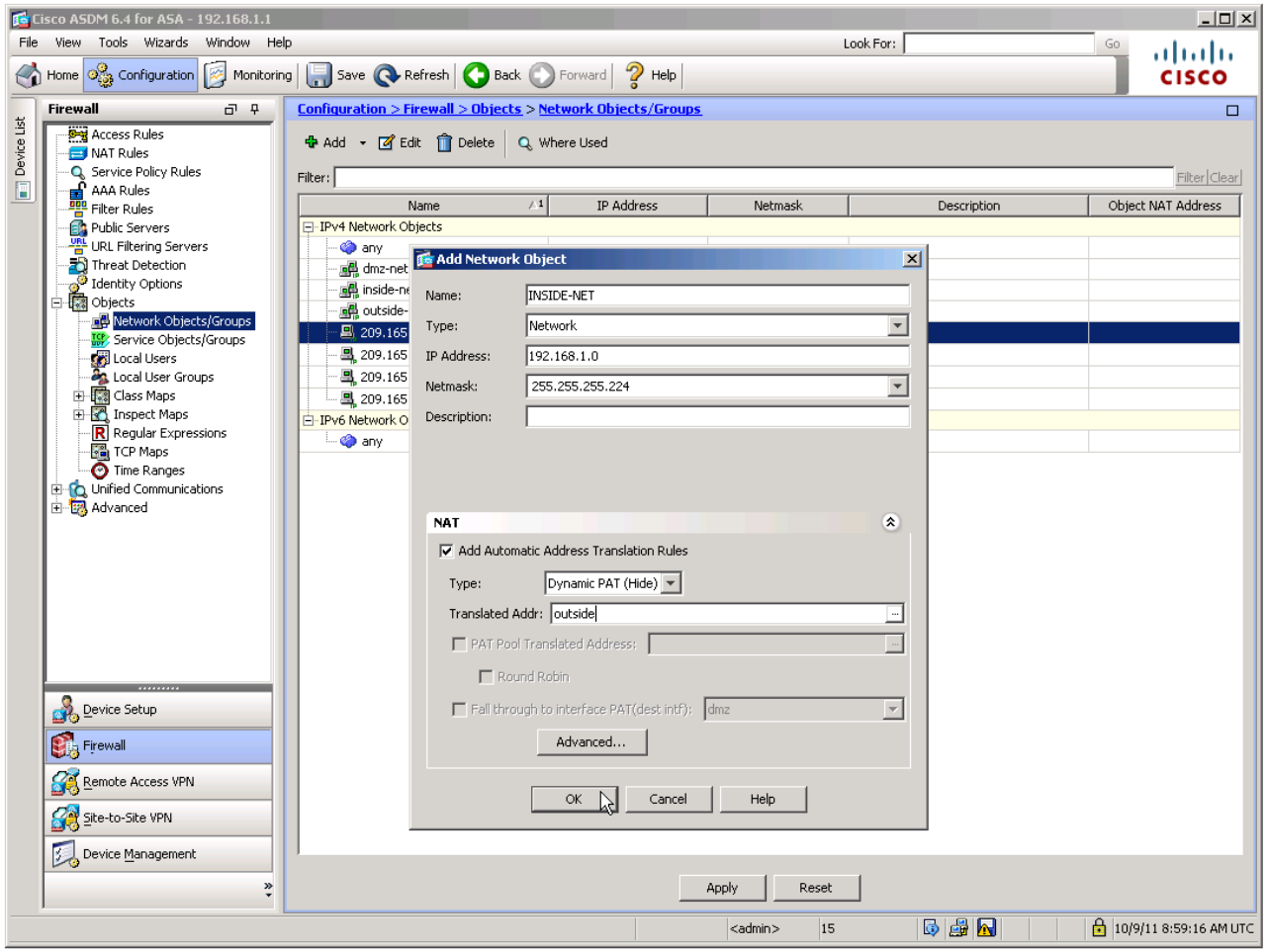
# Configuring Dynamic NAT in ASDM (Cont.)



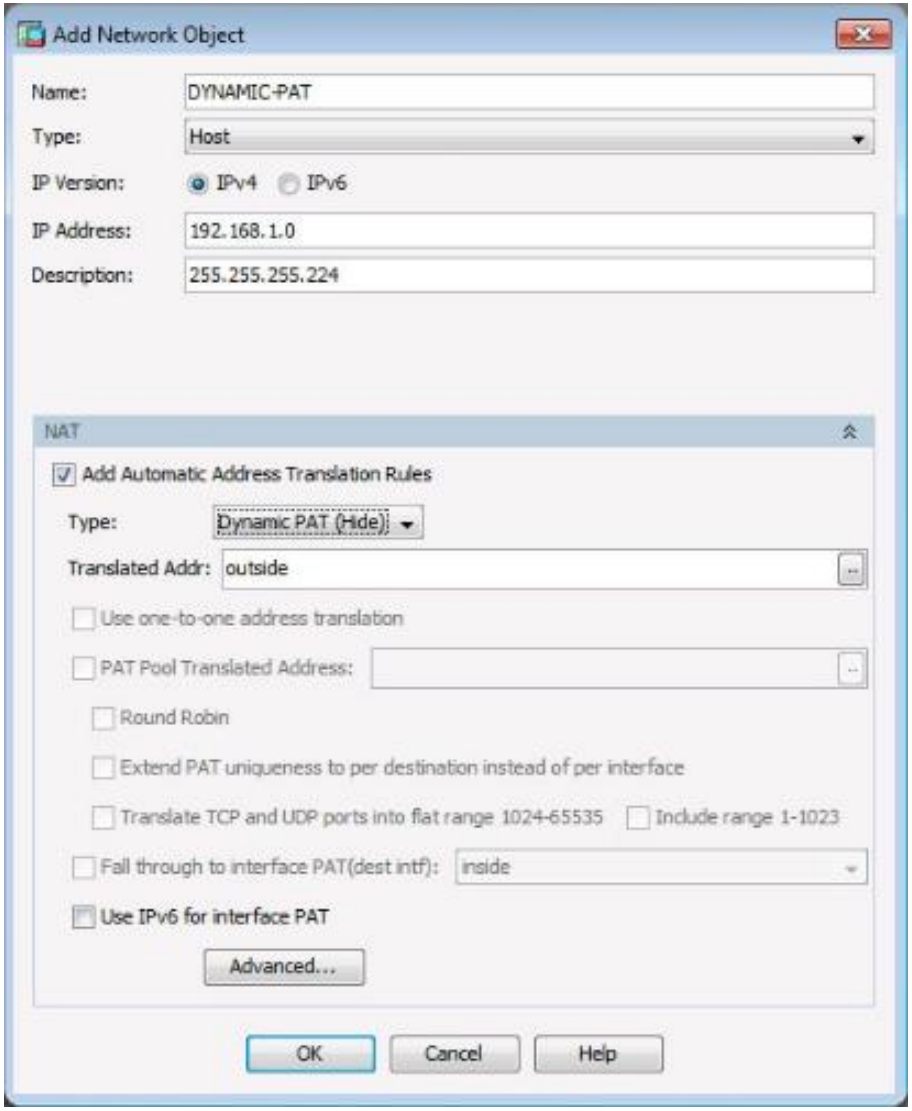

Creating a Network Object for Dynamic NAT

# Dynamic PAT

- **Configuration > Firewall > Objects > Network Objects/Groups**

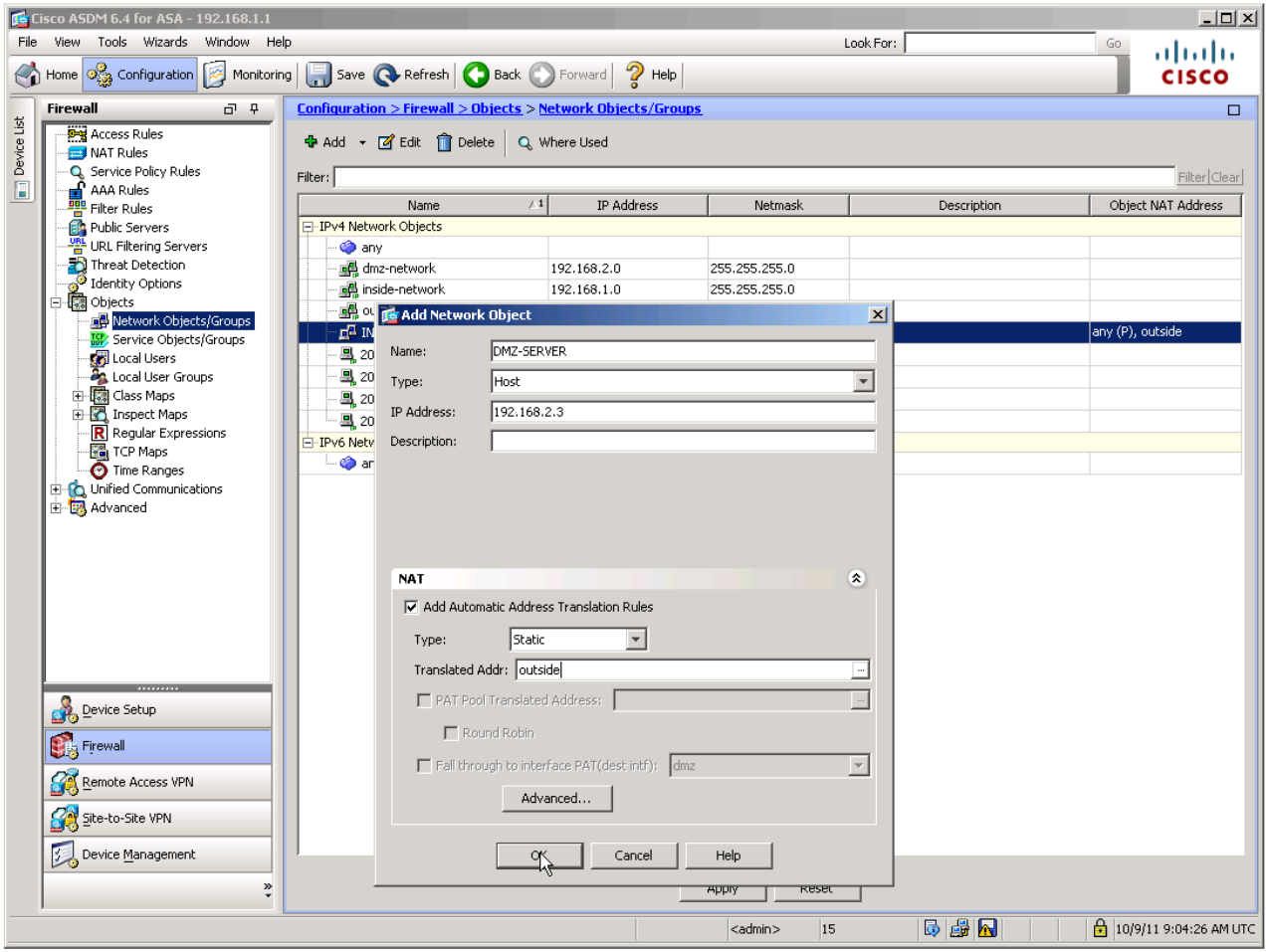


# Configuring Dynamic PAT in ASDM



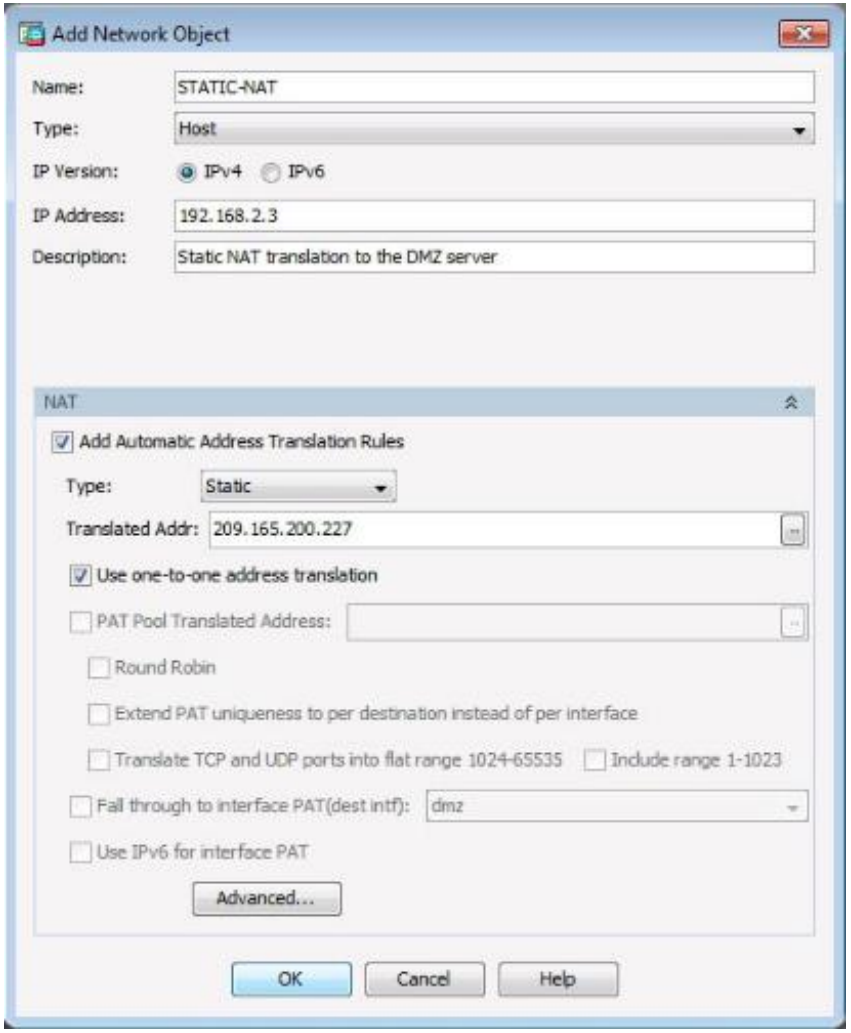
# Static NAT

- **Configuration > Firewall > Objects > Network Objects/Groups**

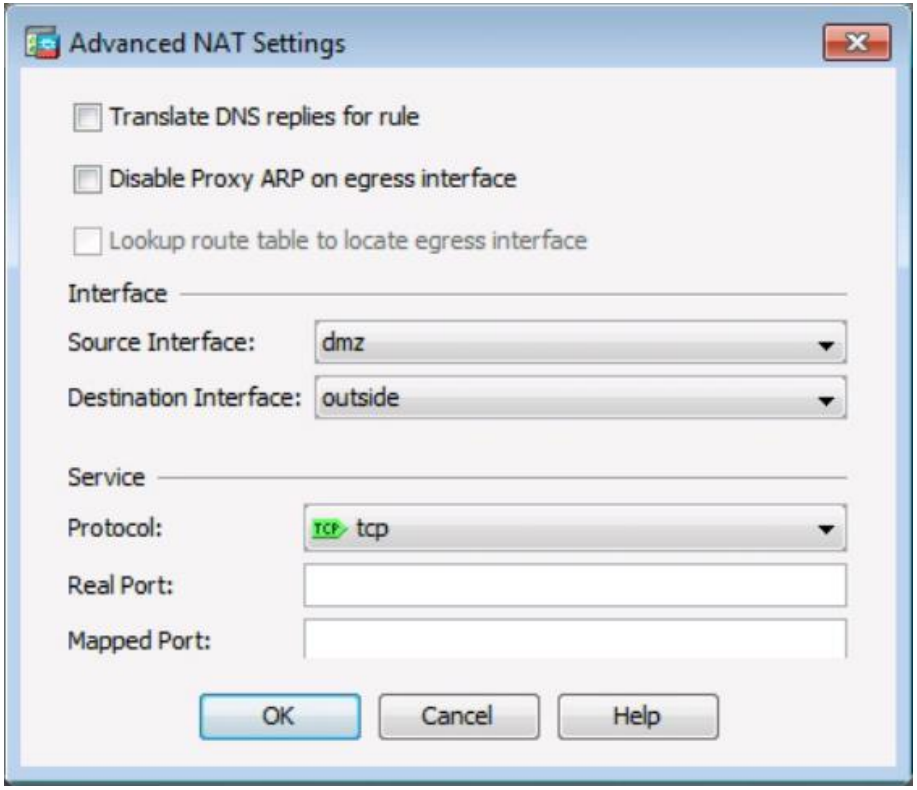


# Configuring Static NAT in ASDM

Static NAT in ASDM

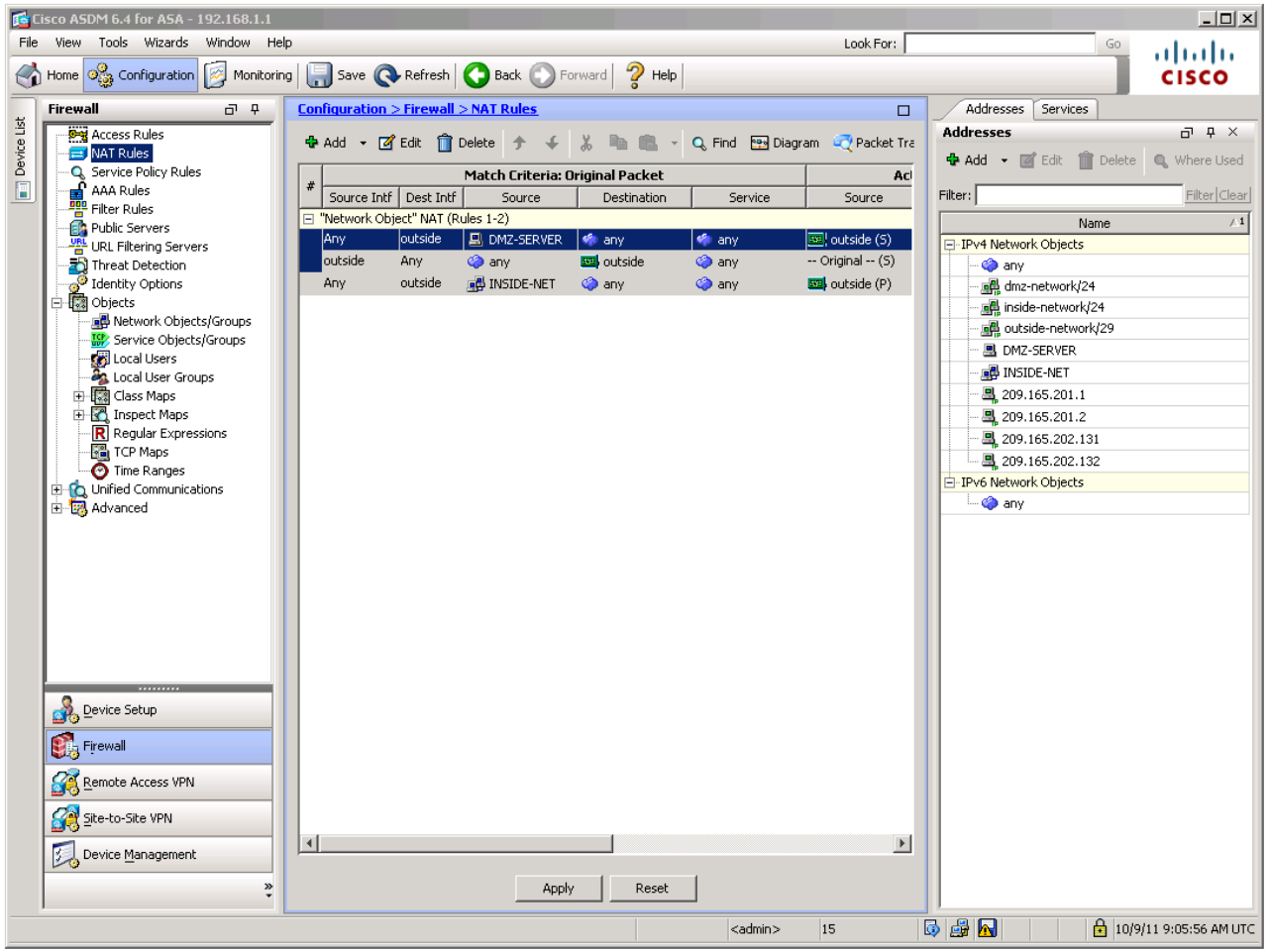



Advanced Static NAT Settings in ASDM



# Verifying NAT

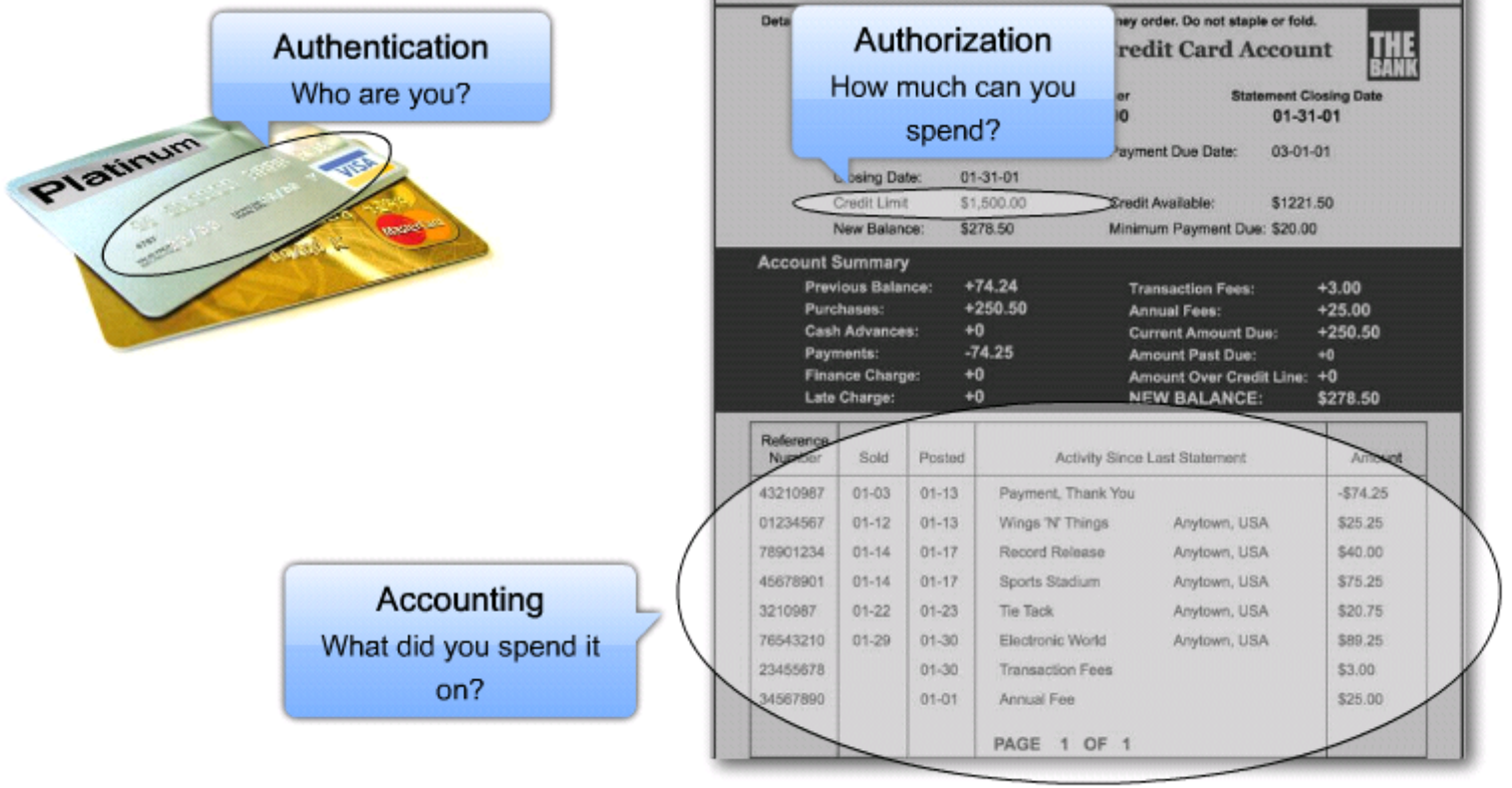
- **Configuration > Firewall > NAT Rules**



# Authentication
# Authorization
# Accounting

# AAA

The AAA Concept is Similar to the Use of a Credit Card



# ASA AAA

- Unlike the ISR, ASA devices do not support local authentication without using AAA
- Cisco ASA can be configured to authenticate using:
  - A local user database
  - An external server for authentication
  - Both

# Local Database AAA Authentication

- Local AAA uses a local database for authentication
  - Users authenticate against the local database entries
  - Local AAA is ideal for small networks that do not need a dedicated server
- Use the **username** *name* **password** *password* [**privilege** *priv-level*] command to create local user accounts
- Use the **aaa authentication** {**enable** | **http** | **ssh** | **telnet**} **console** {*aaa-svr-name* | **LOCAL**} command

```
CCNAS-ASA(config)# username admin password cisco privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication enable console LOCAL
CCNAS-ASA(config)# aaa authentication http console LOCAL
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
CCNAS-ASA(config)# aaa authentication telnet console LOCAL
CCNAS-ASA(config)#
```

# Server-Based AAA Authentication

- Server-based AAA authentication is a far more scalable solution
- Server-based AAA authentication uses an external database server resource leveraging RADIUS or TACACS+ protocols
- To configure a TACACS+ or RADIUS server, use the following commands:
  - **aaa-server** *server-tag* **protocol** *protocol*
    - Creates a TACACS+ or RADIUS AAA server group
  - **aaa-server** *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [**key** *password*]
    - Configures a AAA server as part of a AAA server group. Also configures AAA server parameters that are host-specific
- Configure server based AAA authentication
  - Use the **aaa authentication** {**enable** | **http** | **ssh** | **telnet**} **console** *server-tag* command

# Configuring AAA Authentication

- Configure AAA TACACS+ server and local AAA authentication
  - The local database is used as a backup

```
CCNAS-ASA(config)# username admin password cisco privilege 15
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa-server TACACS-SVR protocol tacacs+
CCNAS-ASA(config-aaa-server-group)# aaa-server TACACS-SVR (dmz) host 192.168.2 cisco123
CCNAS-ASA(config-aaa-server-host)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# show run aaa-server
aaa-server TACACS-SVR protocol tacacs+
aaa-server TACACS-SVR (dmz) host 192.168.2.3
 key *****
CCNAS-ASA(config)#
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication enable console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication http console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication serial console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication ssh console TACACS-SVR LOCAL
CCNAS-ASA(config)# aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)#
CCNAS-ASA(config)#
```

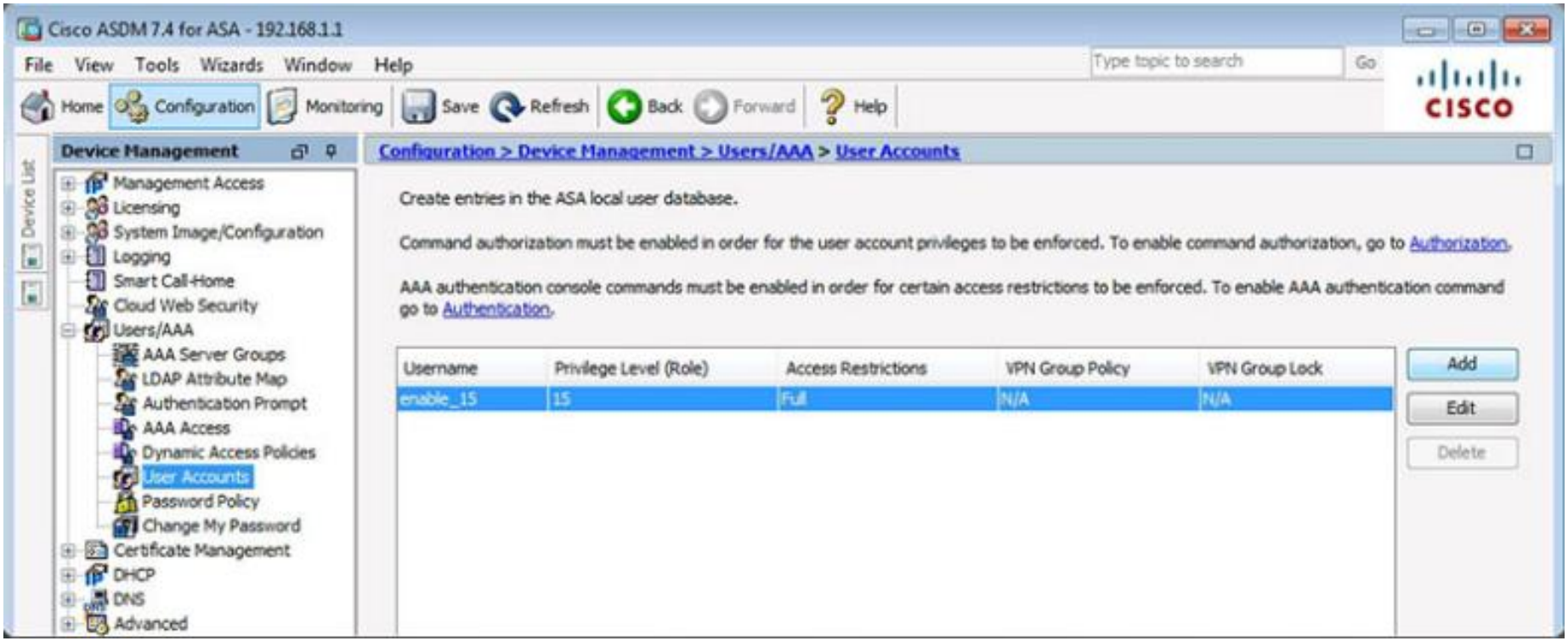
# Verify the AAA Configuration

- Log out and log back in.
- Use the:
  - **show running-conf username** command to view all user accounts.
  - **show running-conf aaa** command to view the AAA configuration.
- Use the **clear config aaa** command to erase AAA.

```
CCNAS-ASA(config)# show run aaa
aaa authentication enable console TACACS-SVR LOCAL
aaa authentication http console TACACS-SVR LOCAL
aaa authentication serial console TACACS-SVR LOCAL
aaa authentication ssh console TACACS-SVR LOCAL
aaa authentication telnet console TACACS-SVR LOCAL
CCNAS-ASA(config)# exit
CCNAS-ASA# disable
CCNAS-ASA> exit

Logoff

Username: admin
Password: *****
Type help or '?' for a list of available commands.
CCNAS-ASA>
```

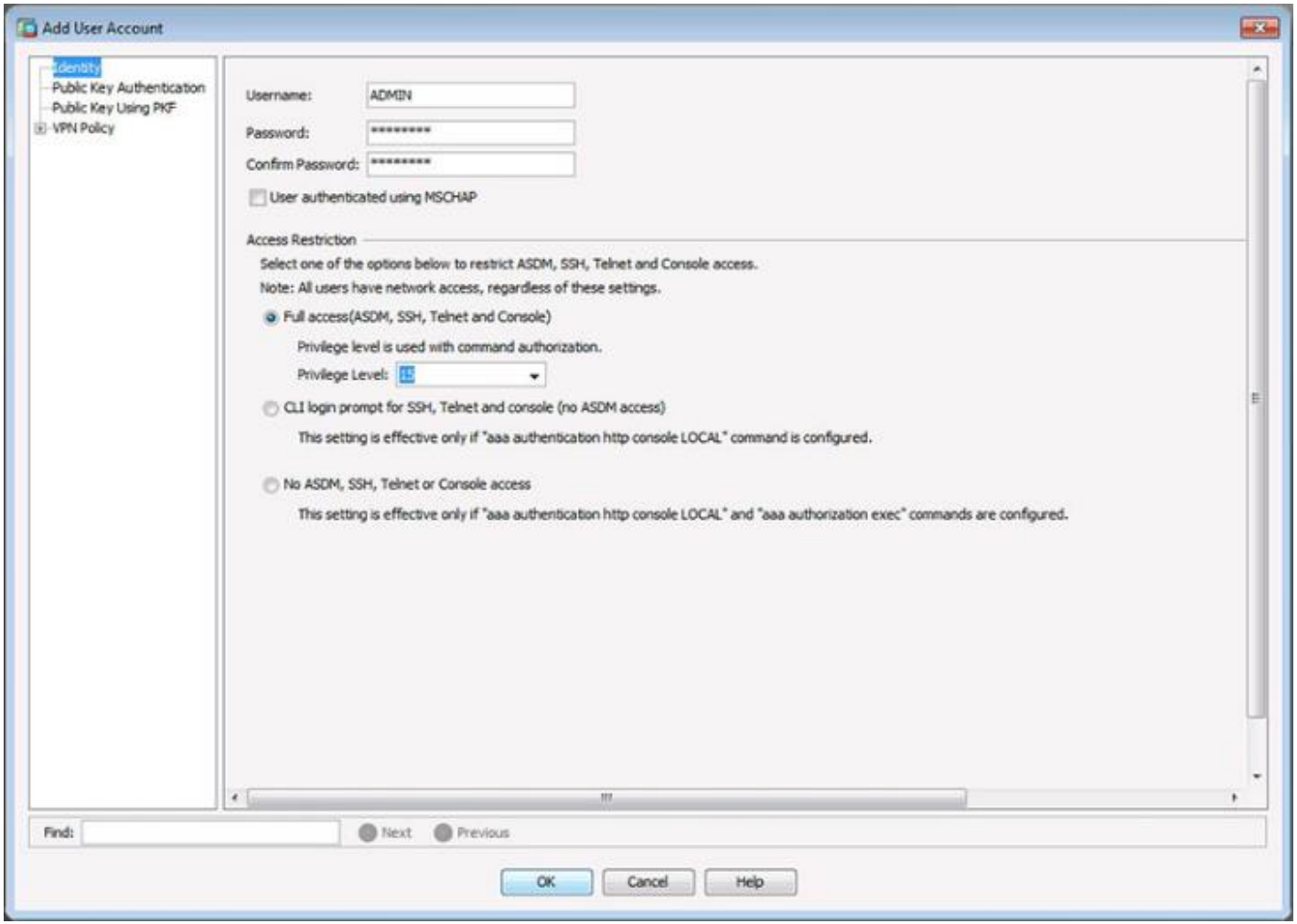
# Add Local Database Entries

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



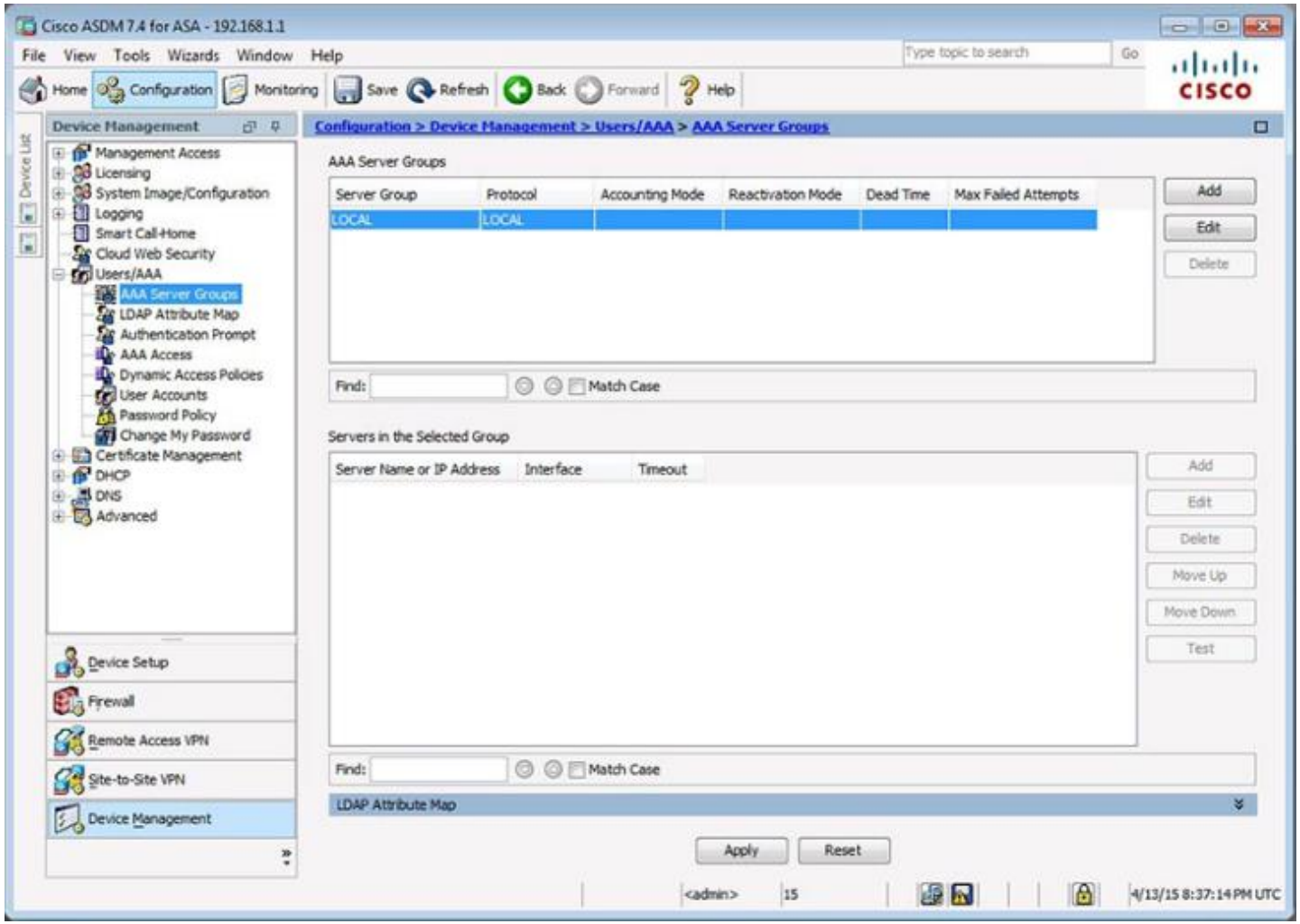
# Add a User

- Click on **Add** and enter the user detail.



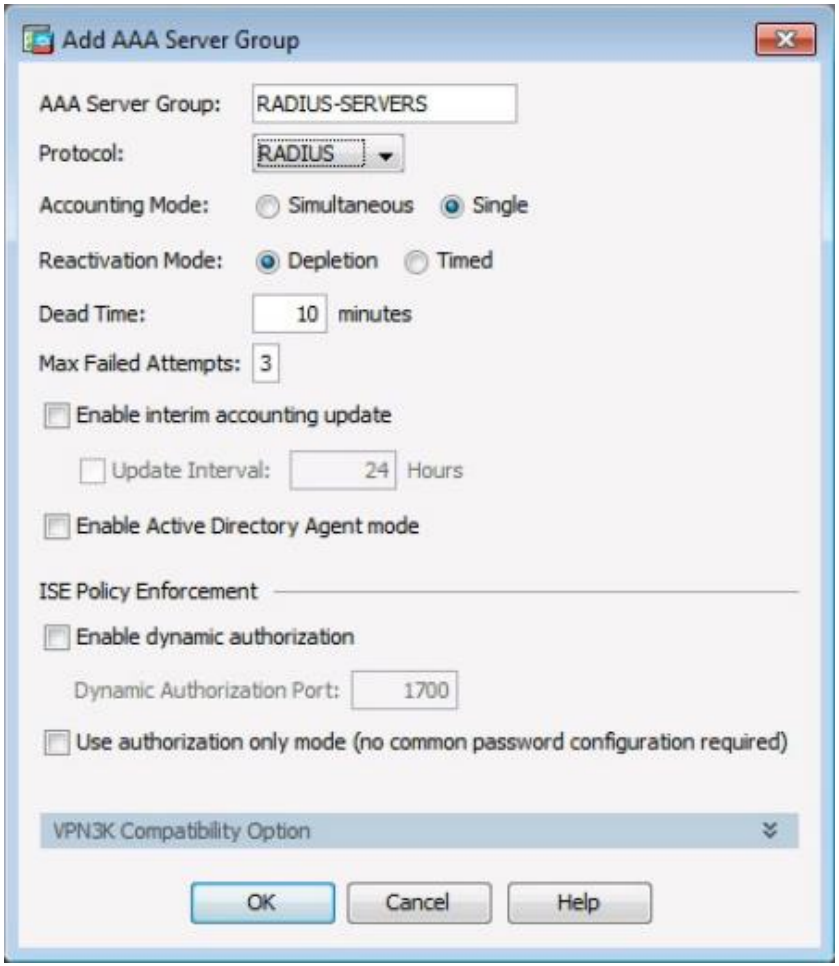
# Configuring AAA Authentication (Cont.)

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

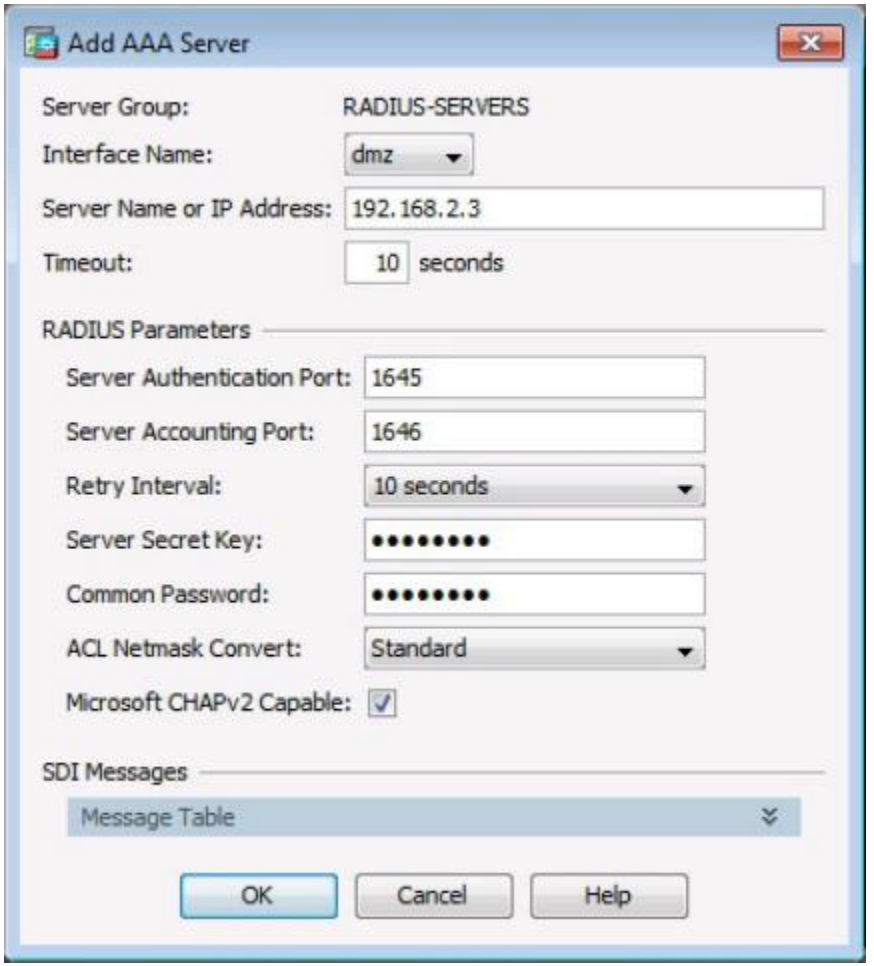


# Configuring AAA Authentication (Cont.)

Add AAA Server Group Window

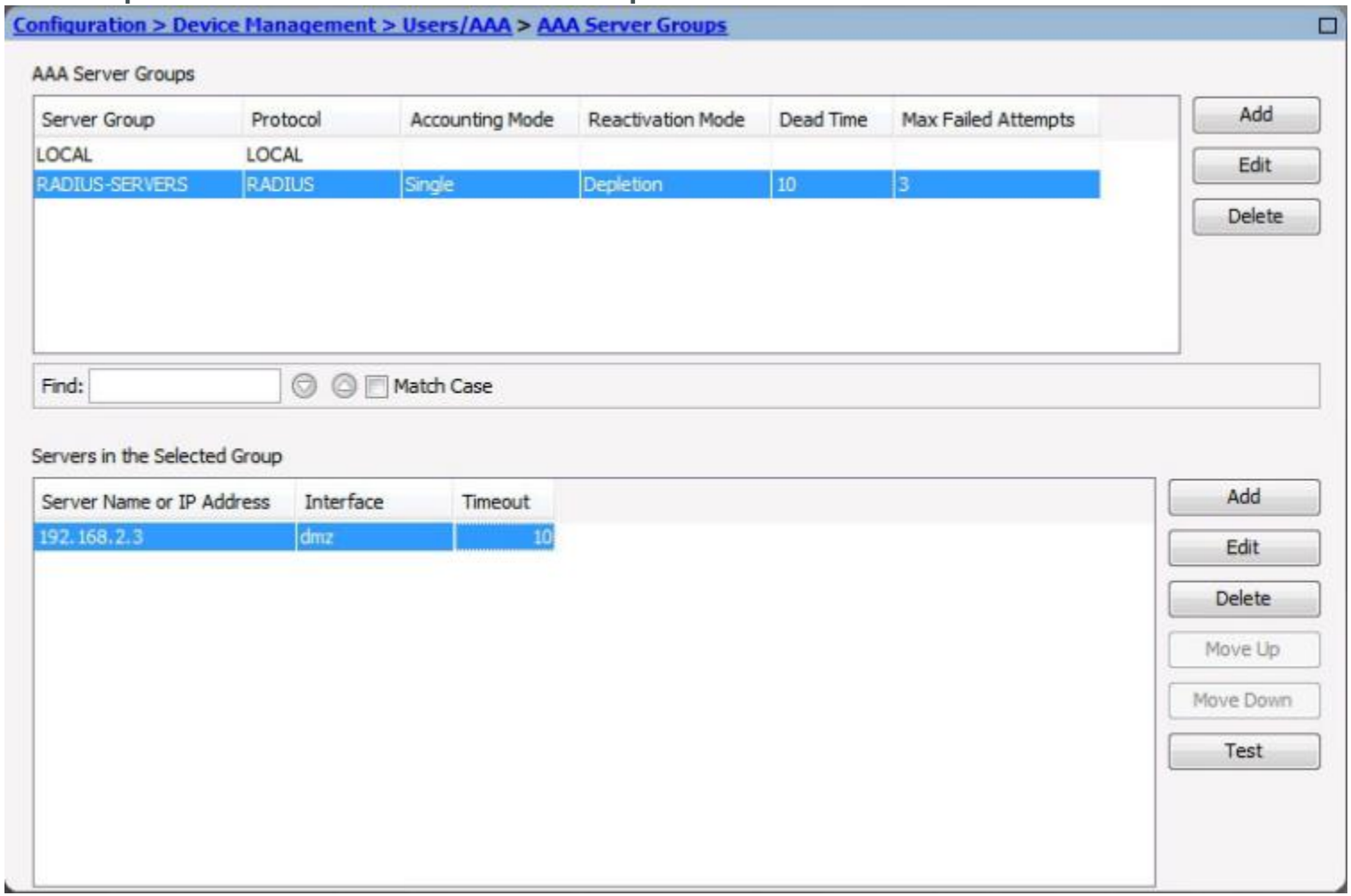



Add AAA Server Window



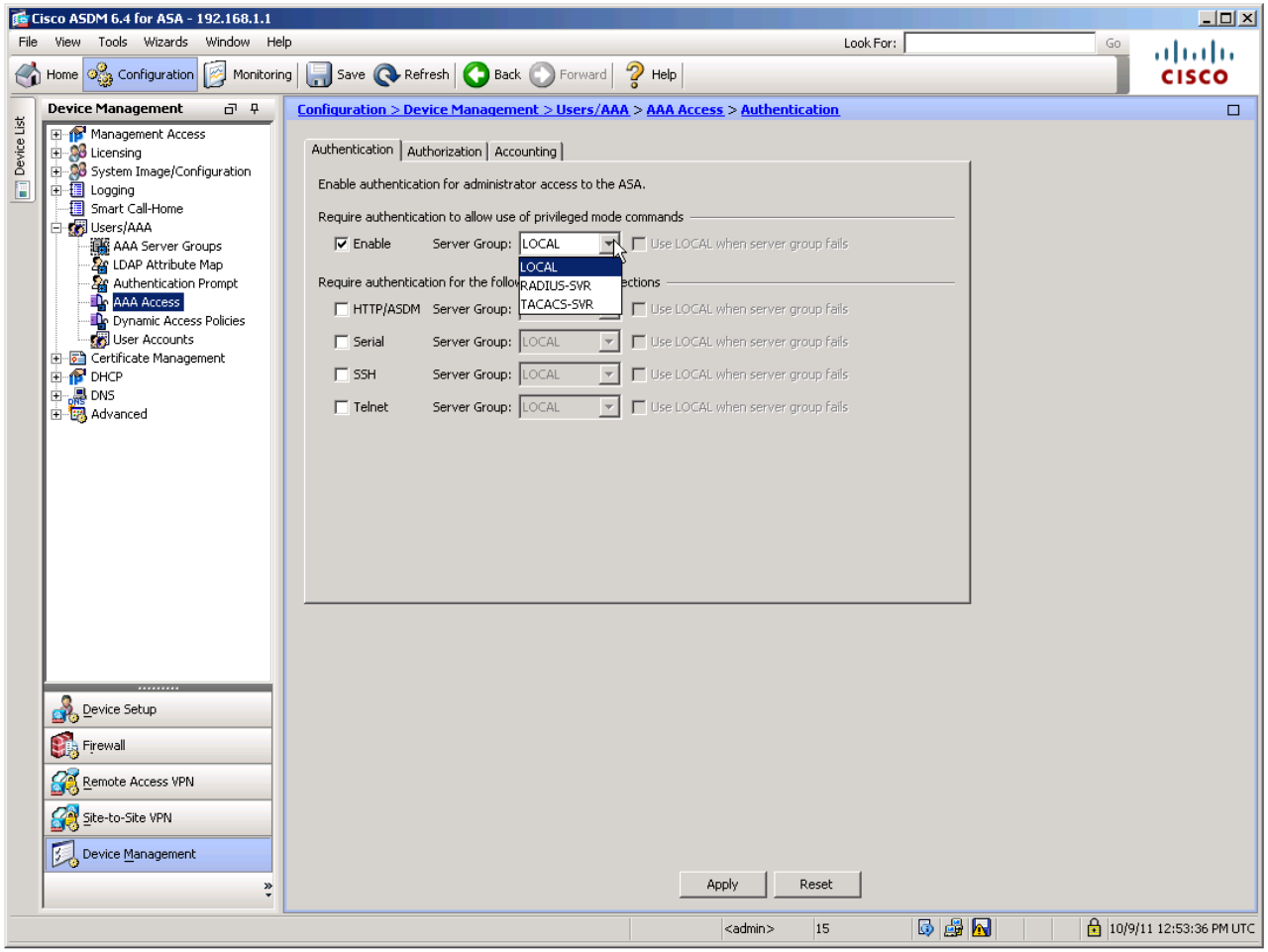
# Configuring AAA Authentication (Cont.)

Completed AAA Server Groups Window



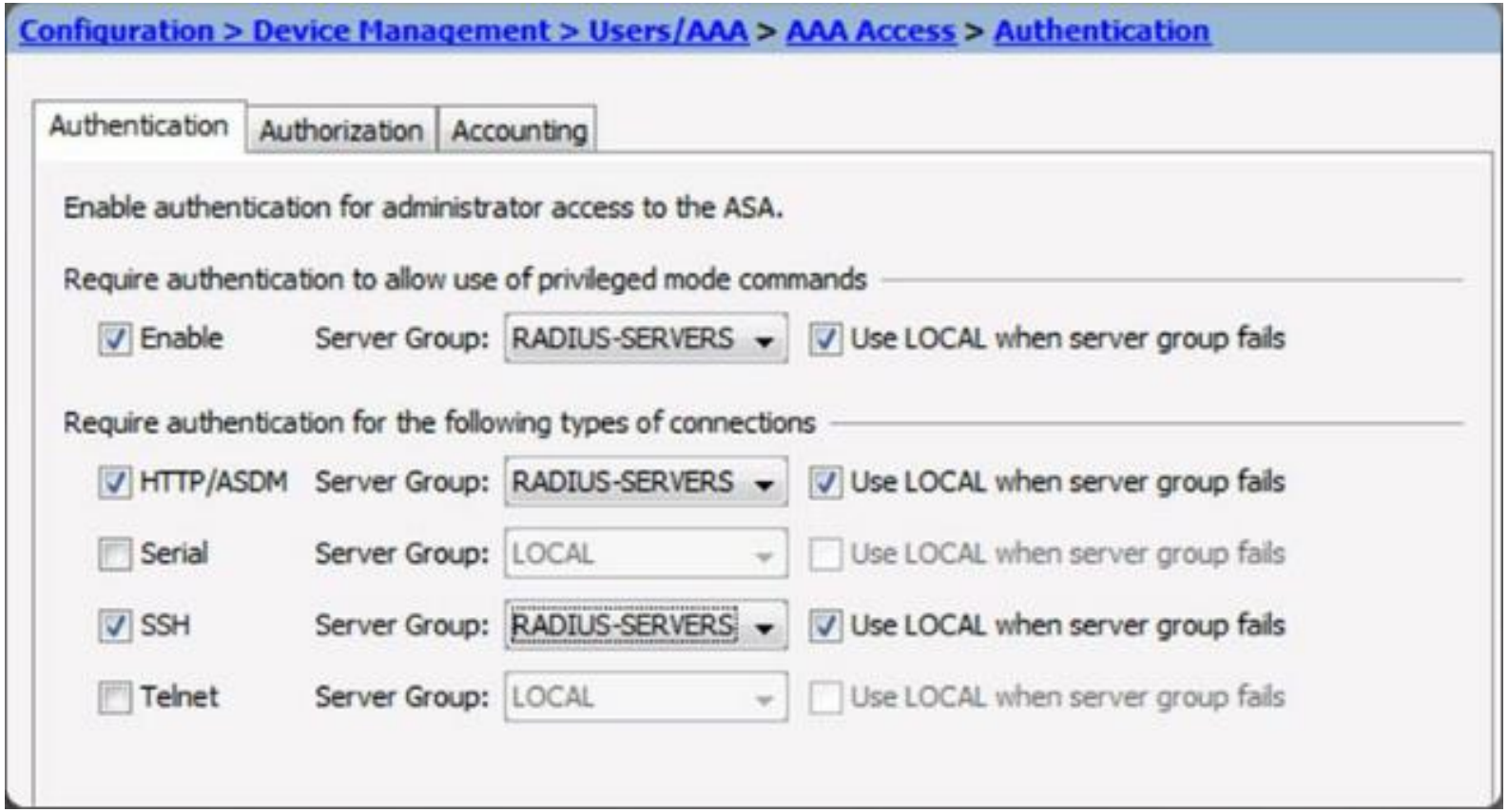
# Enable AAA Authentication

- **Configuration > Firewall > Users/AAA > AAA Access > Authentication**



# Configuring AAA Authentication (Cont.)

AAA Access > Authentication Window



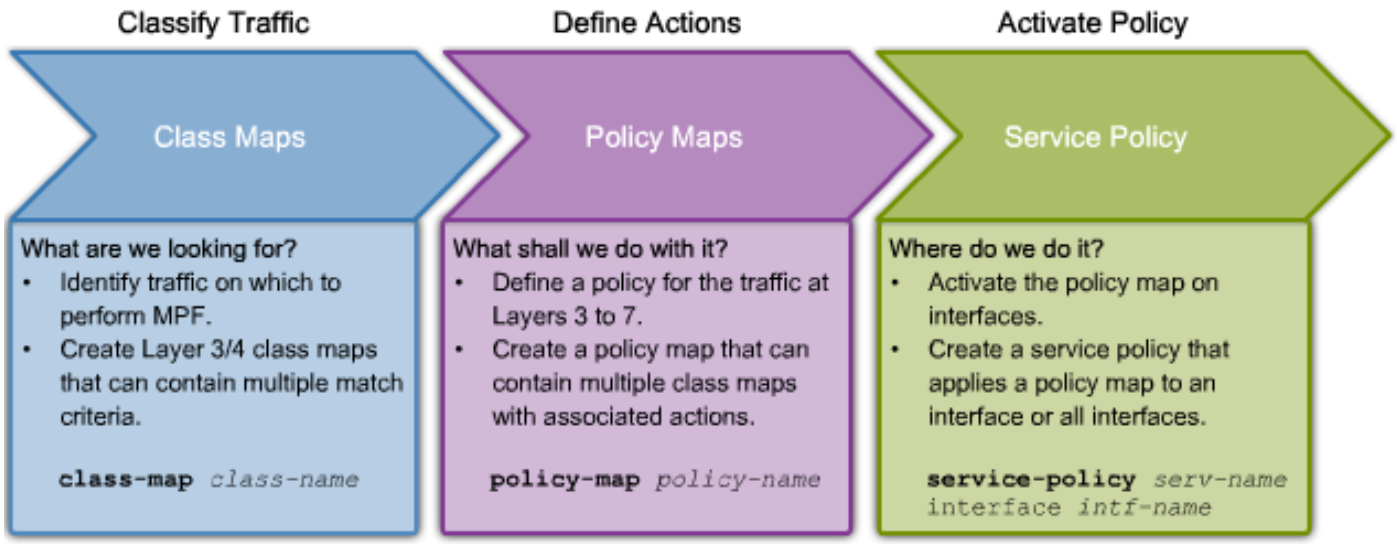
# Modular Policy Framework (MPF)

# Modular Policy Framework (MPF)

- MPF defines a set of rules for applying firewall features, such as traffic inspection and QoS, to the traffic that traverses the ASA
  - It allows granular classification of traffic flows, to apply different advanced policies to different flows.
- Cisco MPF uses these three configuration objects to define modular, object-oriented, hierarchical policies:

# Modular Policy Framework (MPF)

- **Class maps:**
  - Define match criterion by using the **`class-map`** global configuration command
- **Policy maps:**
  - Associate actions to the class map match criteria by using the **`policy-map`** global configuration command
- **Service policies:**
  - Enable the policy by attaching it to an interface, or globally to all interfaces using the **`service-policy`** interface configuration command



# Four Steps to Configure MPF on an ASA

1) Configure extended ACLs to identify specific granular traffic. This step may be optional
2) Configure the class map to identify traffic
3) Configure a policy map to apply actions to those class maps
4) Configure a service policy to attach the policy map to an interface or apply it globally

```
CCNAS-ASA(config)# access-list TFTP-TRAFFIC permit udp any any eq 69
CCNAS-ASA(config)#
CCNAS-ASA(config)# class-map CLASS-TFTP
CCNAS-ASA(config-cmap)# match access-list TFTP-TRAFFIC
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# policy-map POLICY-TFTP
CCNAS-ASA(config-pmap)# class CLASS-TFTP
CCNAS-ASA(config-pmap-c)# inspect tftp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config-pmap)# exit
CCNAS-ASA(config)#
CCNAS-ASA(config)# service-policy POLICY-TFTP global
CCNAS-ASA(config)#
```

# Class Maps

- Class maps are configured to identify Layer 3/4 traffic.
- To create a class map and enter class-map configuration mode, use the **`class-map`** *`class-map-name`* global configuration command.
  - The names "**`class-default`**" and any name that begins with "**`_internal`**" or "**`_default`**" are reserved
  - The class map name must be unique and can be up to 40 characters in length
  - The name should also be descriptive
  - For management traffic destined to the ASA configure the **`class-map type management`** *`class-map-name`* command.

# Class Map Configuration Mode

- In class-map configuration mode, define the traffic to include in the class by matching one of the following characteristics
  - **`description`** - Add description text
  - **`match any`** - Class map matches all traffic
  - **`match access-list`** *`access-list-name`* - Class map matches traffic specified by an extended access list
- To display information about the class map configuration, use the **`show running-config class-map`** command

# Policy Map

Policy maps are used to bind class maps with actions in 3 steps:

1) Use the **`policy-map`** *`policy-map-name`* global command
   - The policy map name must be unique and up to 40 characters in length
2) From policy-map configuration mode (config-pmap), configure:
   - **`description`** - Add description text
   - **`class`** *`class-map-name`*
     - Identify a specific class map on which to perform actions
     - Enter sub-configuration mode
3) Assign actions for the class including:
   - **`set connection`** - sets connection values
   - **`inspect`** - provides protocol inspection servers
   - **`police`** - sets rate limits for traffic in this class

# Verify Policy Map

- To display information about the policy map configuration, use the **`show running-config policy-map`** command.
- To remove all policy maps, use the **`clear configure policy-map`** command in global configuration mode.

# Service Policy

- To activate a policy map globally on all interfaces or on a targeted interface, use the **`service-policy`** global configuration command.
- Use the command to enable a set of policies on an interface.
- The command syntax is as follows:
  - **`service-policy`** *`policy-map-name`* [**`global`** | **`interface`** *`intf`*]

# Verify Service Policy

- To display information about the service policy configuration, use the **`show service-policy`** or the **`show running-config service-policy`** command.
- To remove all service policies, use the **`clear configure service-policy`** command in global configuration mode. The **`clear service-policy`** command clears the service policy statistics.

# Default Class Map Policy

- MPF provides three default settings:
  - Default class map
  - Default policy map
  - Default service policy
- The class map configuration also includes a default Layer 3/4 class map that the ASA uses in the default global policy called **`inspection_default`** and matches the default inspection traffic.
  - **`class-map inspection_default`**
  - **`match default-inspection-traffic`**

# Default Policy Map Policy

- The configuration includes a default Layer 3/4 policy map that the ASA uses in the default global policy.
- It is called `global_policy` and performs inspection on the default inspection traffic.
- There can only be one global policy.
  - Therefore, to alter the global policy, either edit it or replace it.

# ASA Default Policy

- The ASA default configuration includes a global service policy that matches all default application inspection traffic
  - Otherwise, the service policy can be applied to an interface or globally
  - Interface service policies take precedence over the global service policy for a given feature
- To alter the global policy, an administrator needs to either edit the default policy, or disable the default policy and apply a new policy

# Default ASA MPF Policy

```
<Output omitted>

class-map inspection_default
 match default-inspection-traffic

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

service-policy global_policy global

<Output omitted>
```

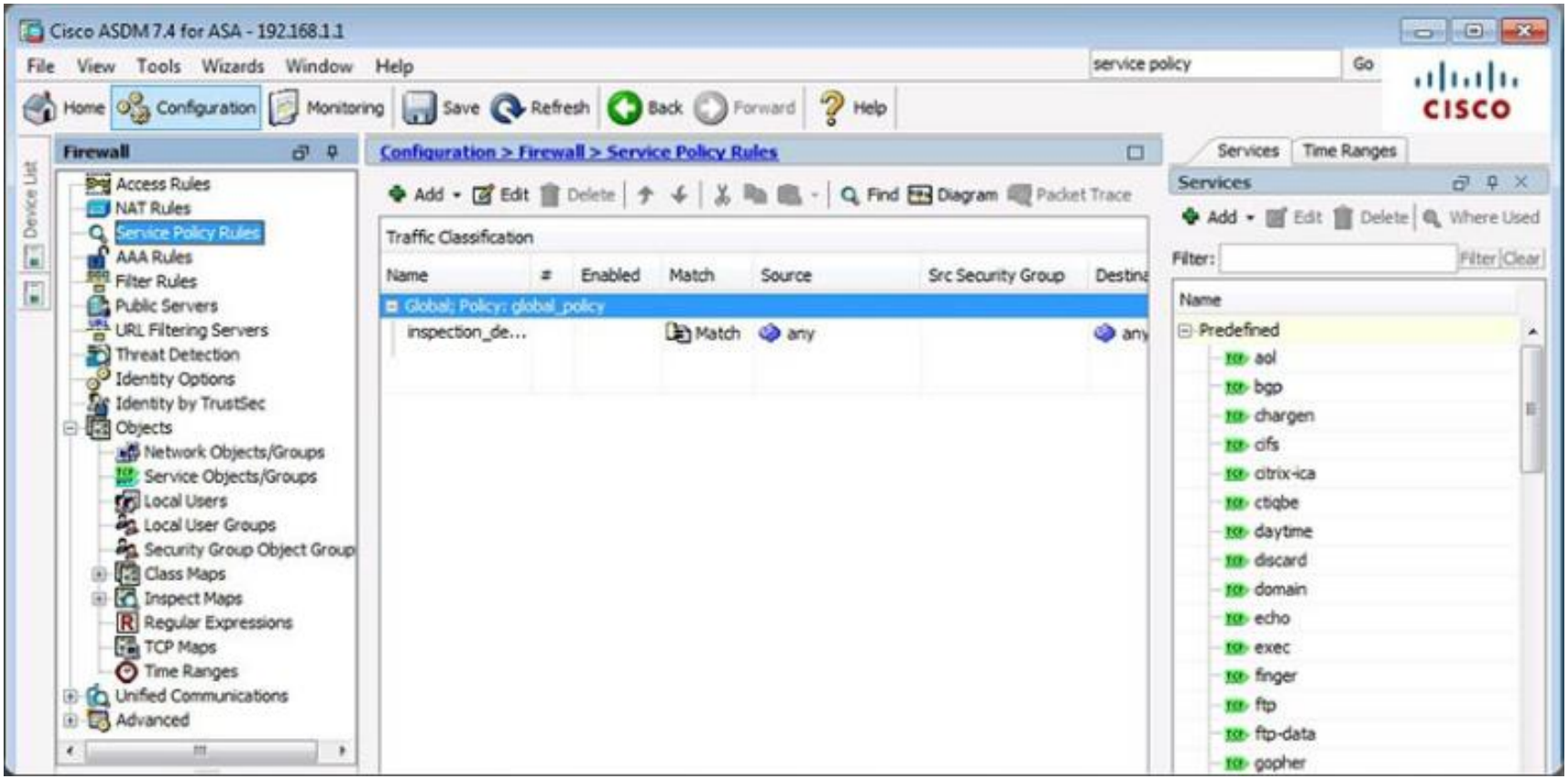
Class map statement matches the keyword "default-inspection-traffic."

Policy map associates actions to the traffic identified in the class map.

Service policy applies a policy map to an interface or as in this case, globally to all interfaces that do not have a specific policy.

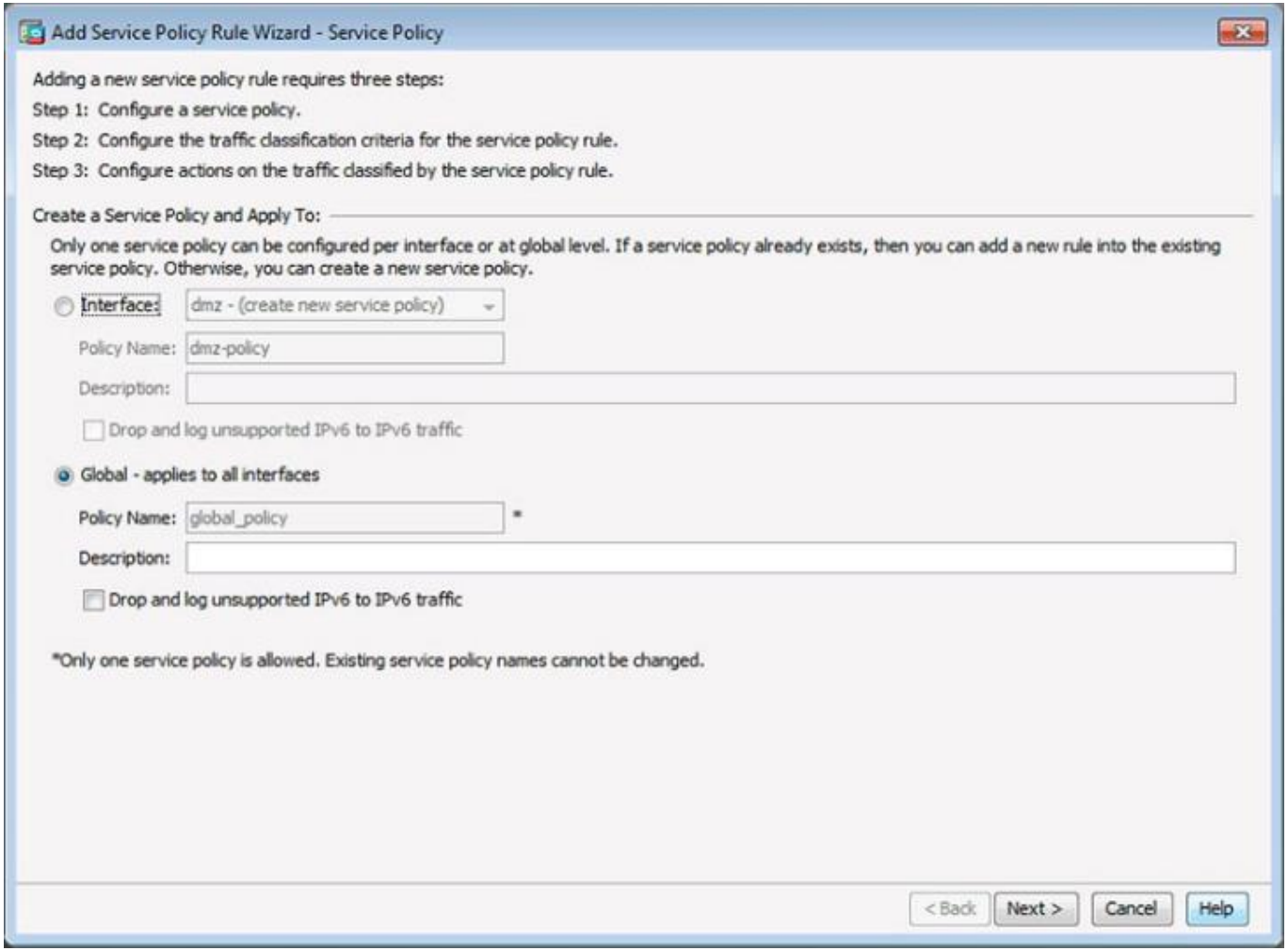
# Configuring a Service Policy

Service Policy in ASDM



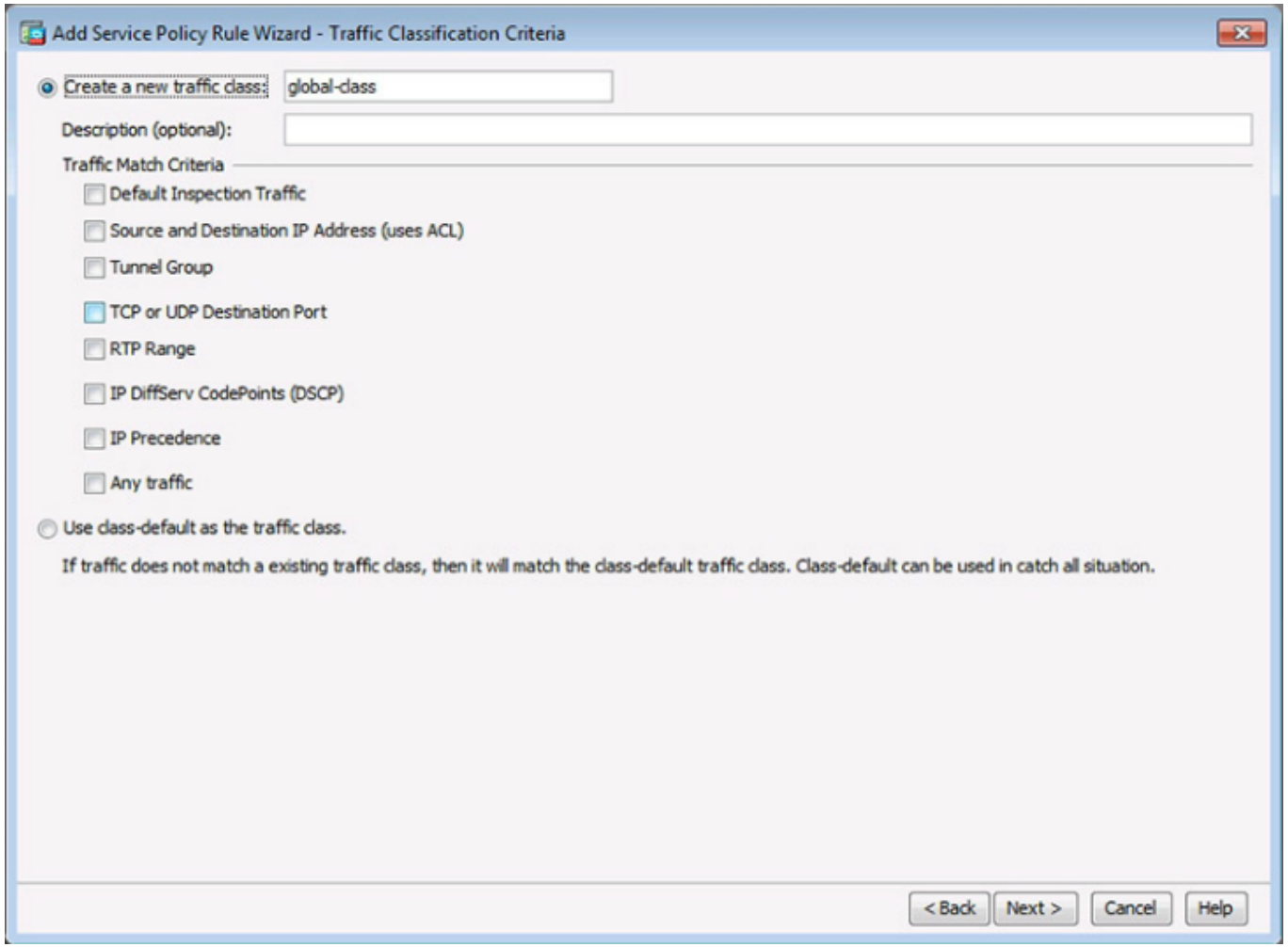
# Configuring a Service Policy

## Configure a Service Policy



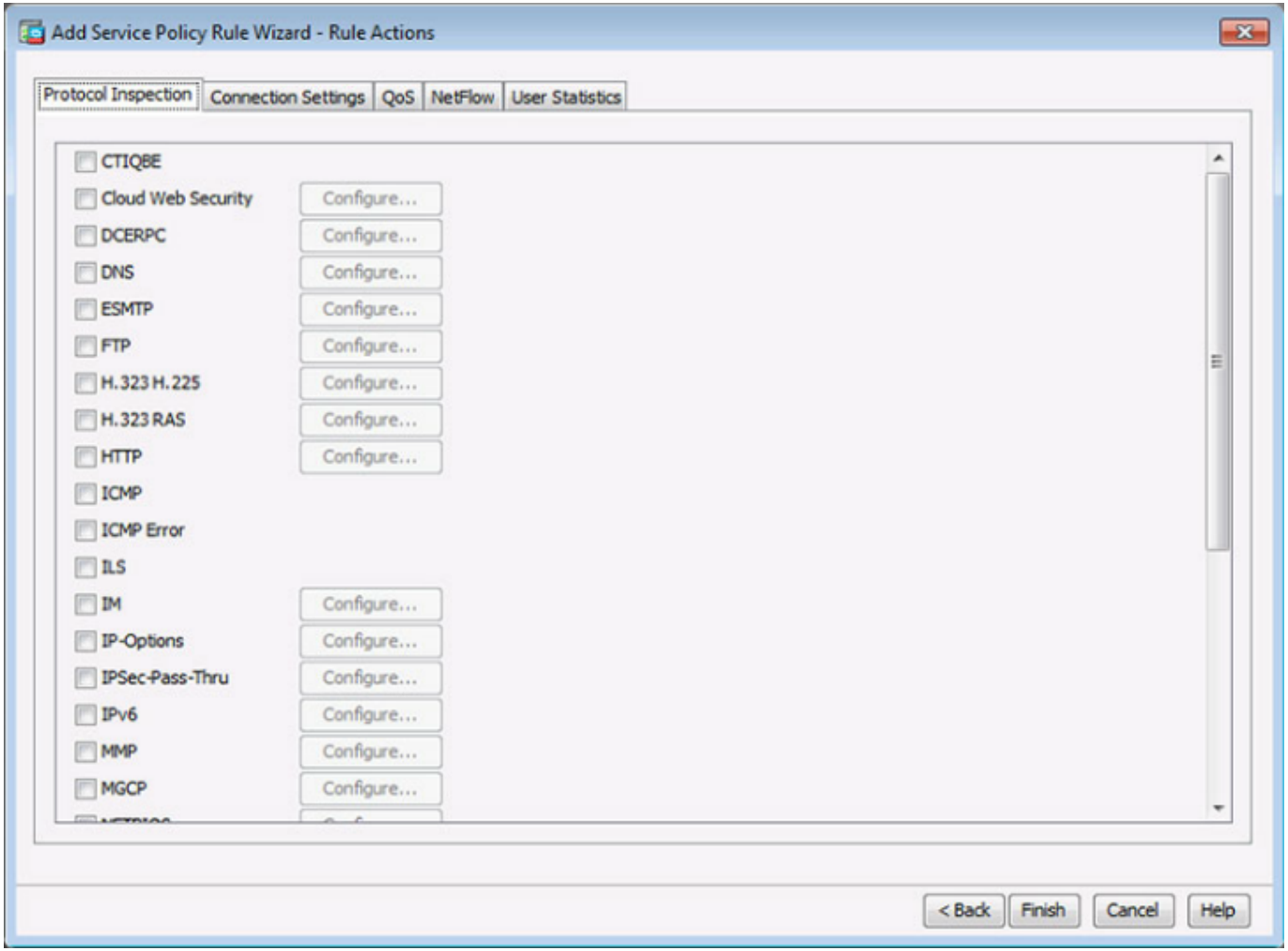
# Configuring a Service Policy

## Configure Traffic Classification Criteria



# Configuring a Service Policy

Configure Actions



# ASA VPN Features

# Remote Access VPNs

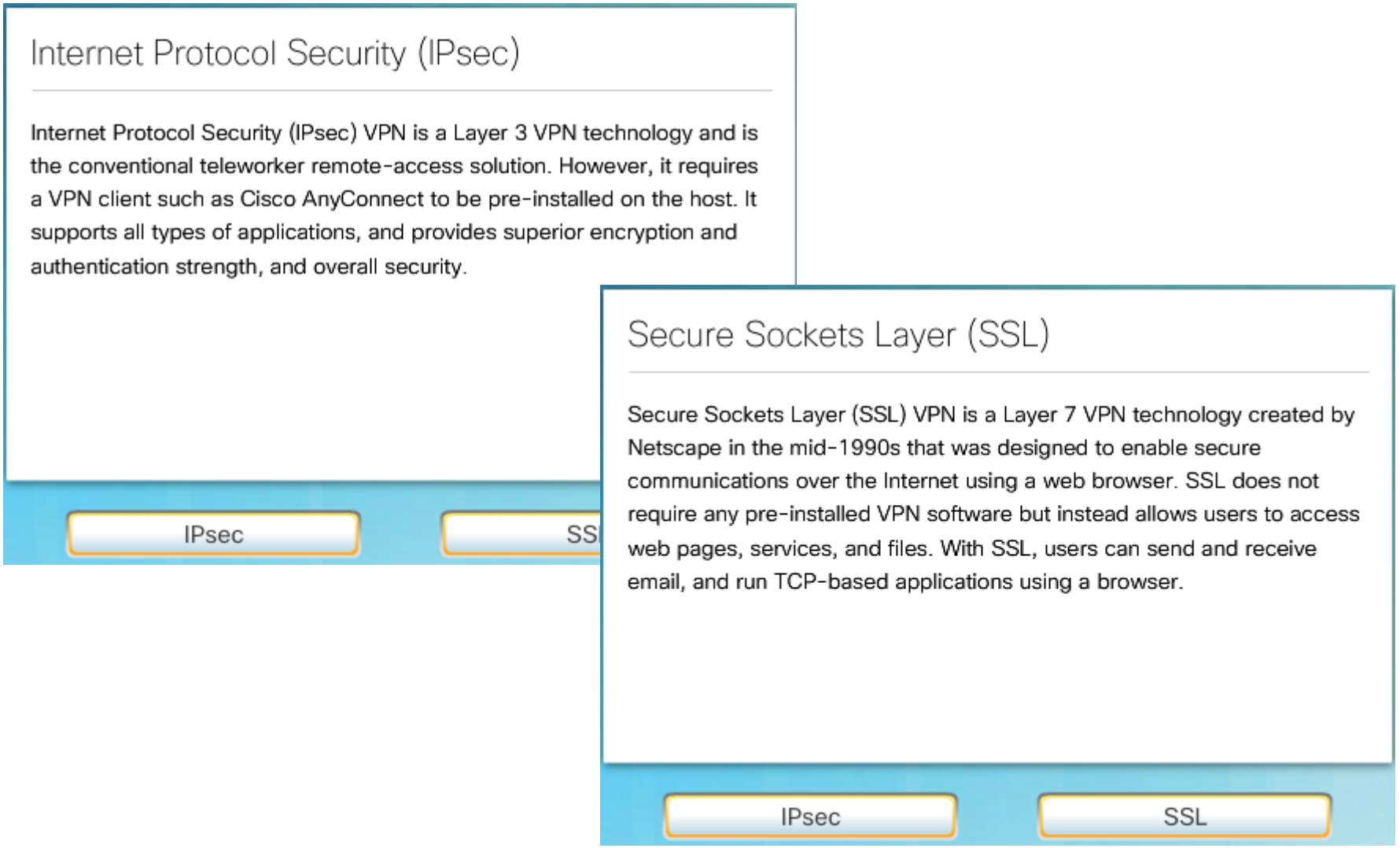
- Enterprise users are requesting support for their mobile devices including smart phones, tablets, notebooks, and a broader range of laptop manufacturers and operating systems.
- This shift has created a challenge for IT security.
- The solution is the use of SSL VPNs to secure access for all users, regardless of the endpoint from which they establish a connection.



# IOS VPN versus ASA VPN

- Both Cisco ISR and ASA provide IPsec and SSL VPN capabilities.
  - ISRs are capable of supporting as many as 200 concurrent users.
  - ASA can support from 10 to 10,000 sessions per device.
- For this reason, the ASA is usually the choice when supporting a large remote networking deployment.

# IPsec Versus SSL

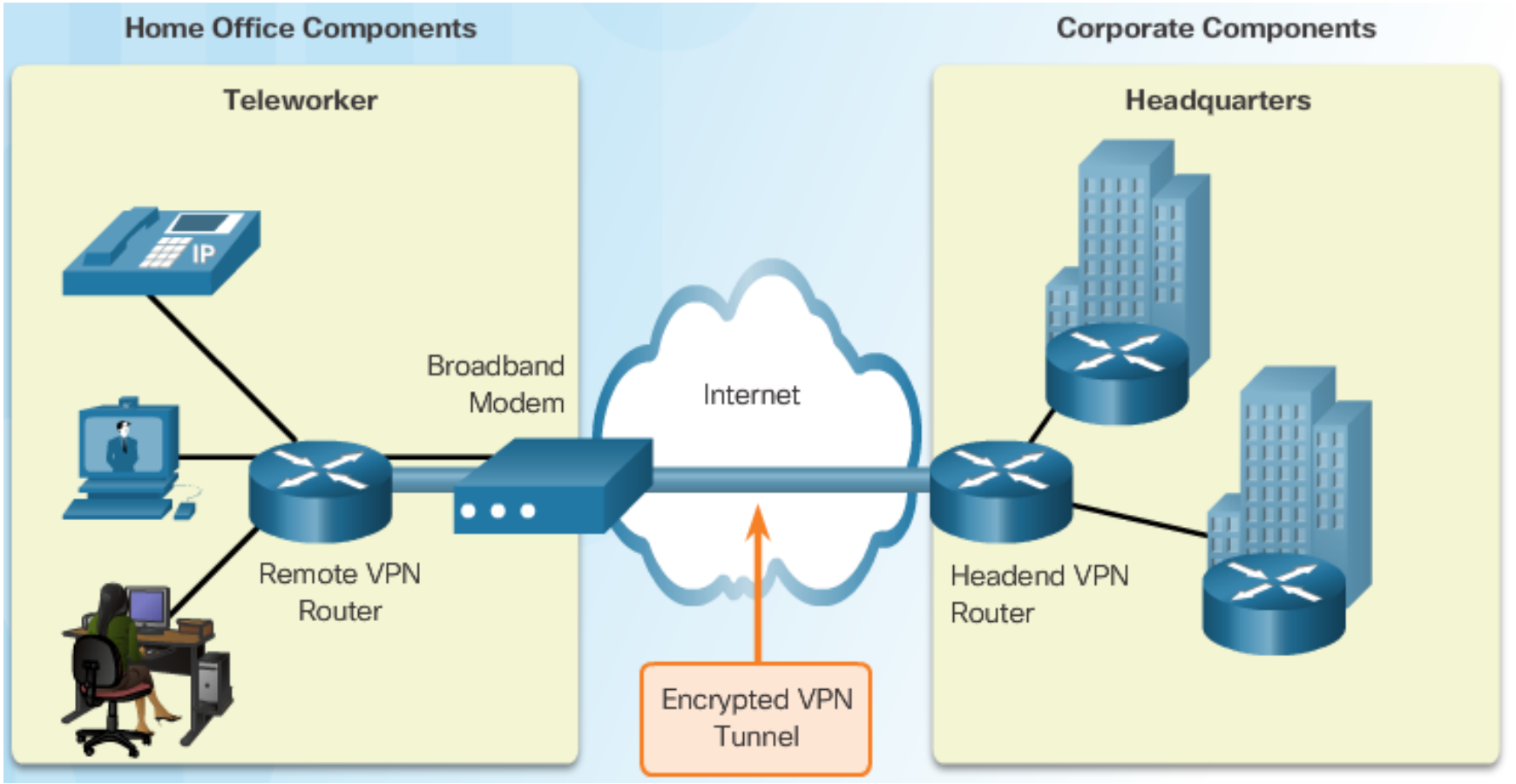


# IPsec Versus SSL (Cont.)

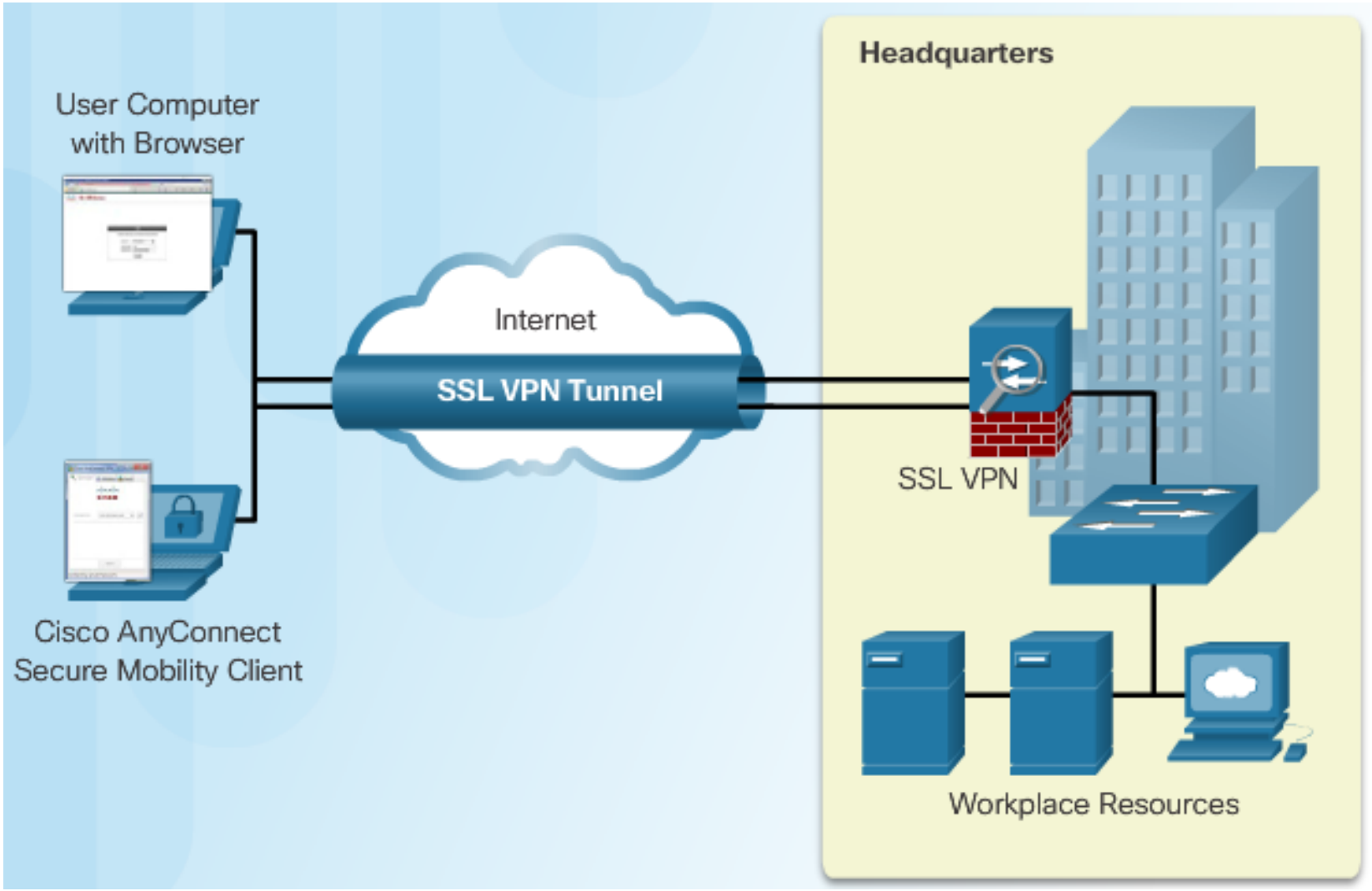
Comparing IPsec and SSL

| | 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. |

# IPSec VPNs

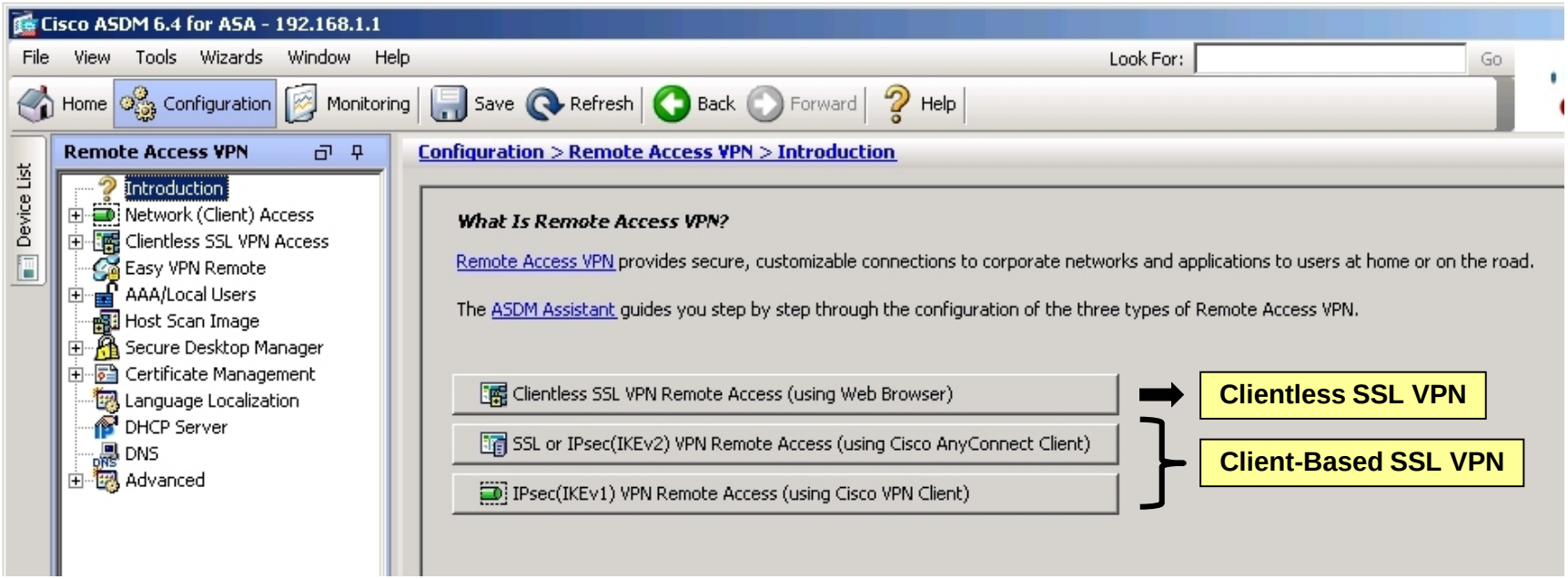

Home Office Components
Corporate Components
Teleworker
Headquarters
IP
Broadband
Modem
Internet
Remote VPN
Router
Headend VPN
Router
Encrypted VPN
Tunnel

# SSL VPNs


Headquarters
User Computer with Browser
Internet
SSL VPN Tunnel
SSL VPN
Cisco AnyConnect Secure Mobility Client
Workplace Resources

# ASA Remote Access VPN Support

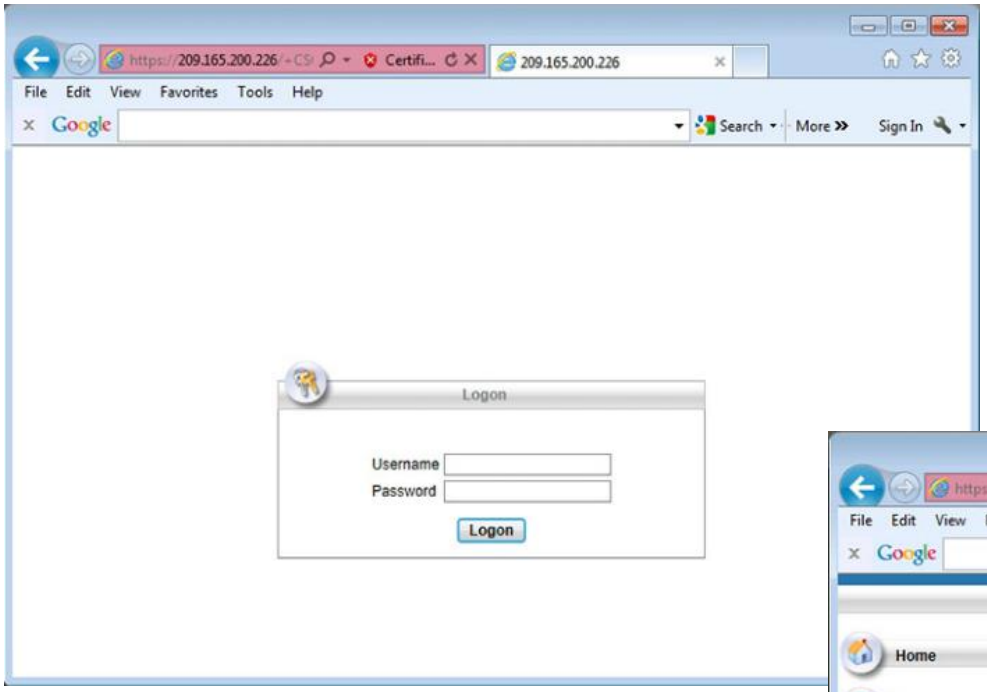
- The ASA supports three types of remote-access VPNs:
  - Clientless SSL VPN Remote Access (using a web browser)
  - SSL or IPsec (IKEv2) VPN Remote Access (using Cisco AnyConnect client)



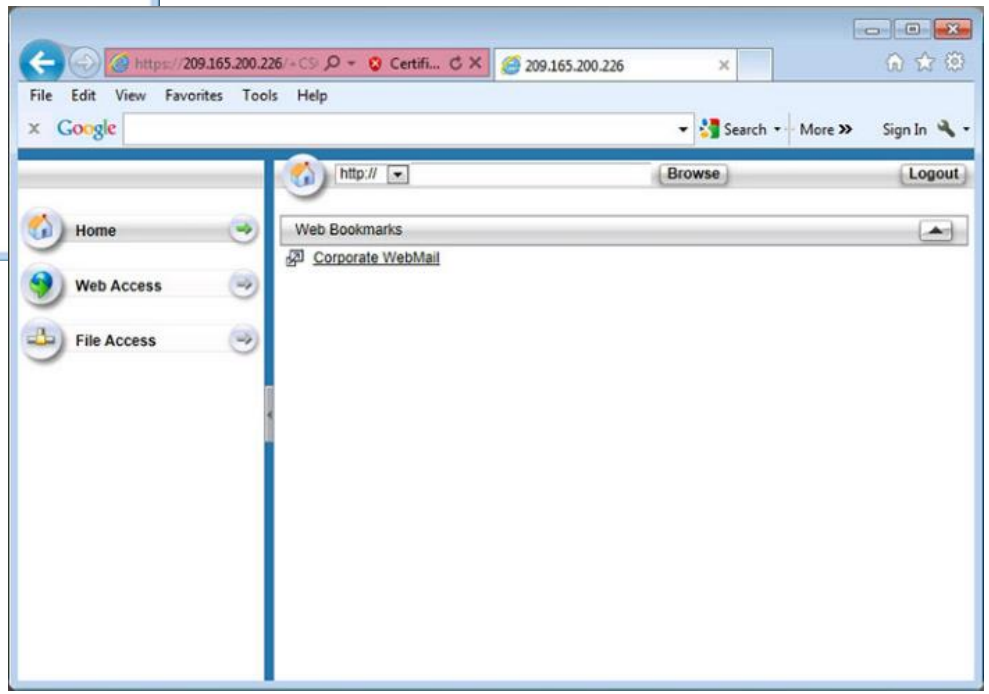
# Clientless versus Client-Based SSL VPN

- **Clientless SSL VPN:**
  - Browser-based VPN that lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser.
  - After authentication, users access a portal page and can access specific, supported internal resources.
- **Client-Based SSL VPN:**
  - Provides full tunnel SSL VPN connection but requires a VPN client application to be installed on the remote host.
  - Requires a client, such as the Cisco AnyConnect VPN client to be installed on the host.
- The AnyConnect client can be manually pre-installed on the host, or downloaded on-demand to a host via a browser.

# Clientless SSL VPN Solution (Cont.)




Clientless Login Web page

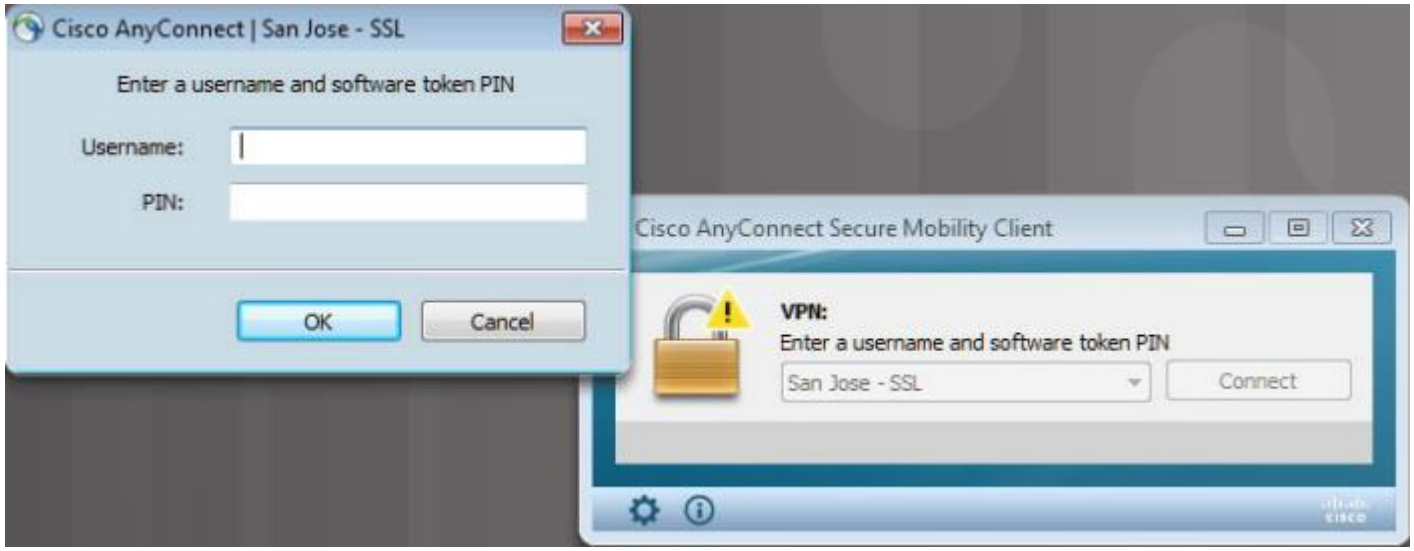



Web Portal Home Page

# Cisco AnyConnect Secure Mobility Client

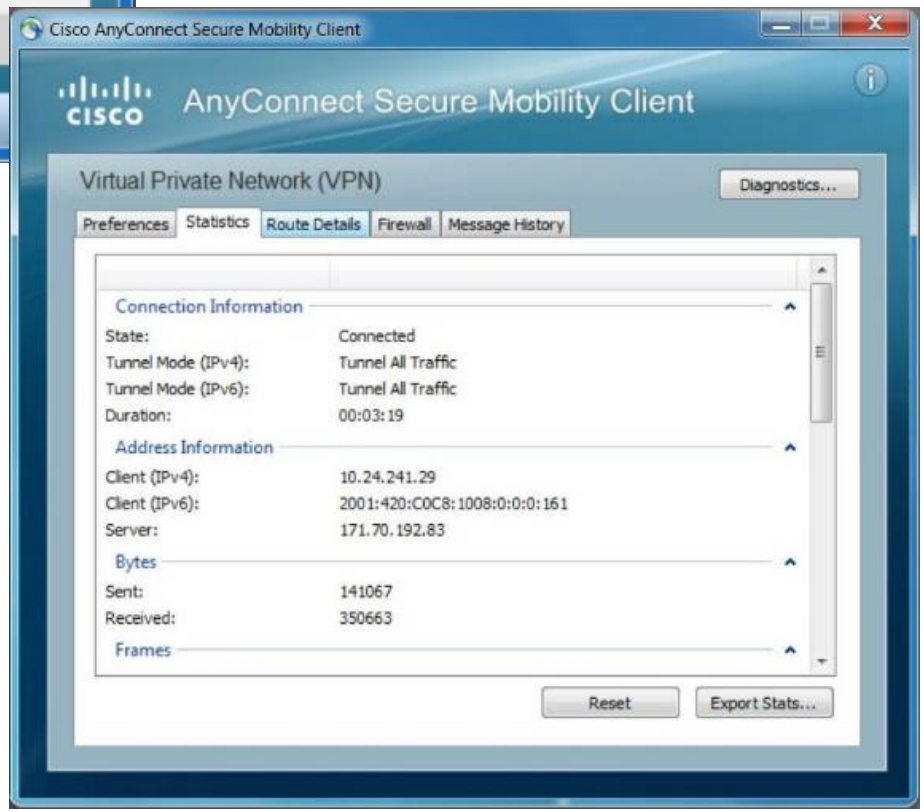

AnyConnect Connection Window

AnyConnect Authenticate Window



# Cisco AnyConnect Secure Mobility Client (Cont.)

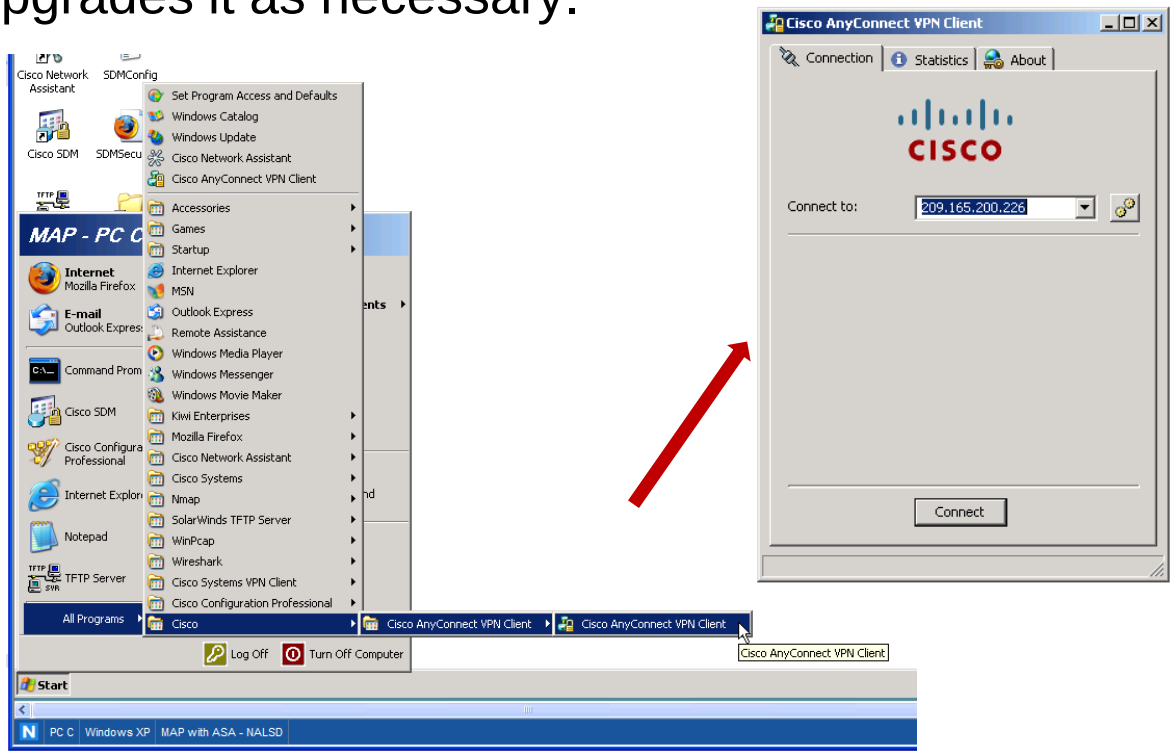

AnyConnect
Authenticated Window




AnyConnect Statistics
Window

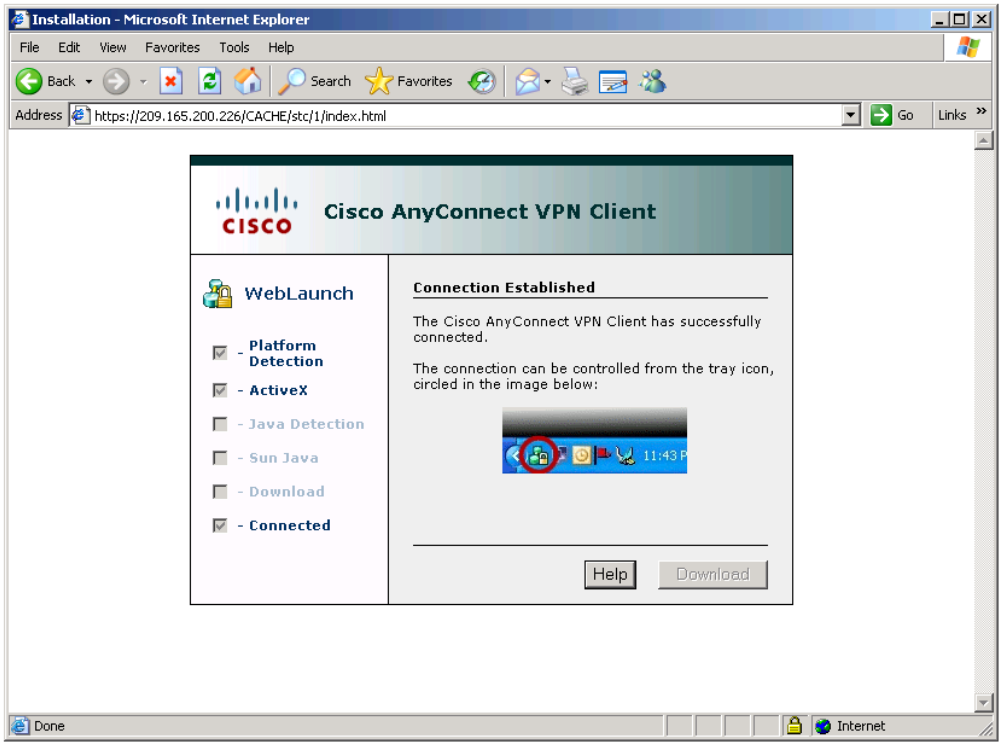
# AnyConnect Previously Installed

- When the AnyConnect client is pre-installed on the host, the VPN connection can be initiated by starting the application.
  - Once the user authenticates, the ASA examines the revision of the client and upgrades it as necessary.



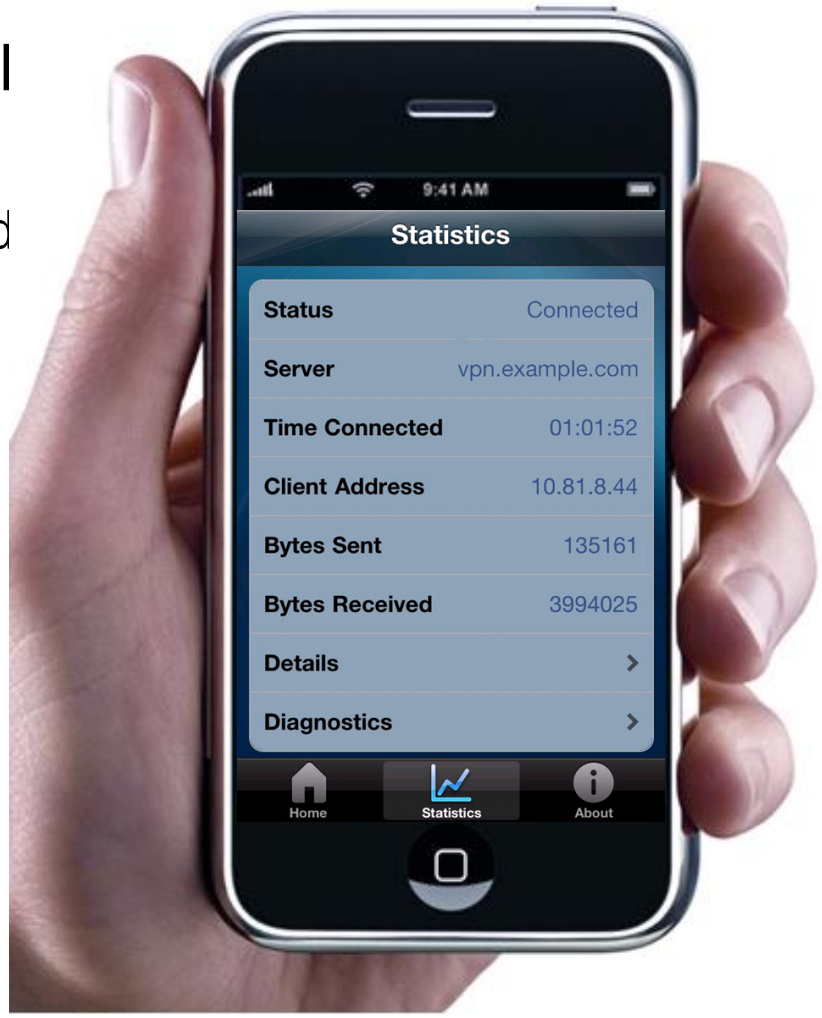
# AnyConnect Downloaded and Installed

- Remote users can connect and authenticate to the ASA and then uploads the AnyConnect client to the host.
  - Windows, Mac OS, and Linux.
  - The AnyConnect client then installs and configures itself and finally establishes an SSL VPN connection.



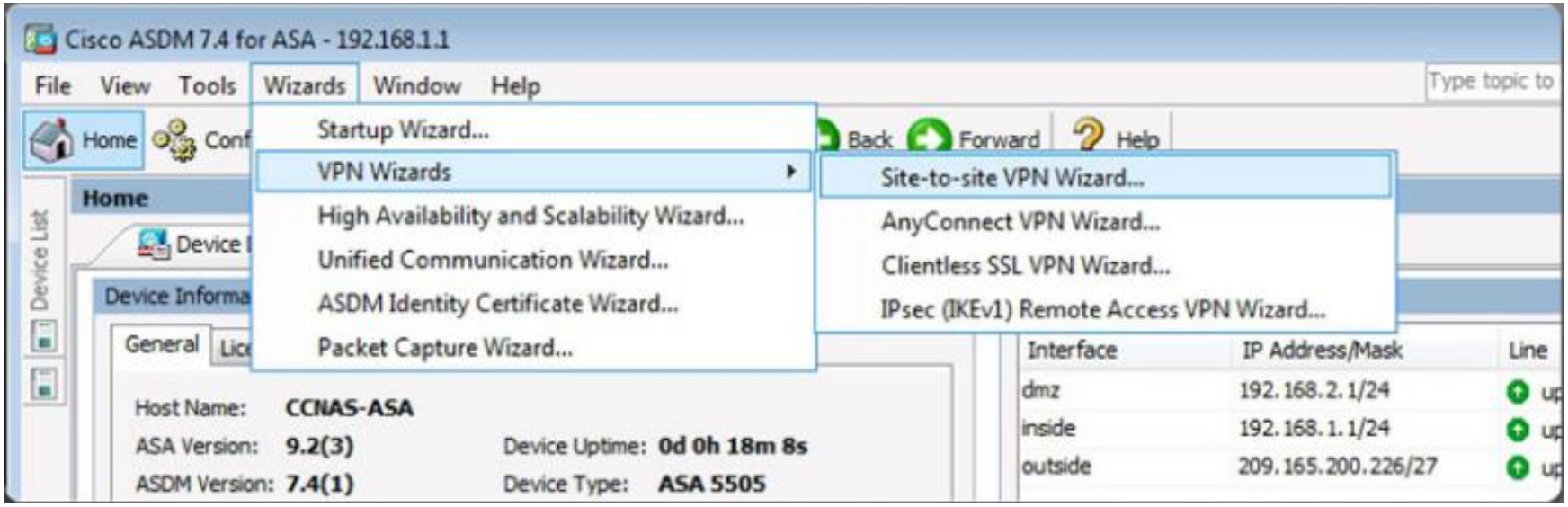
# Consumerization

- To support IT consumerization, tl client is available for free for:
  - iOS devices (iPhone, iPad, and iPod
  - Android OS (select models)
  - BlackBerry
  - Windows Mobile 6.1
  - HP webOS
  - Nokia Symbian

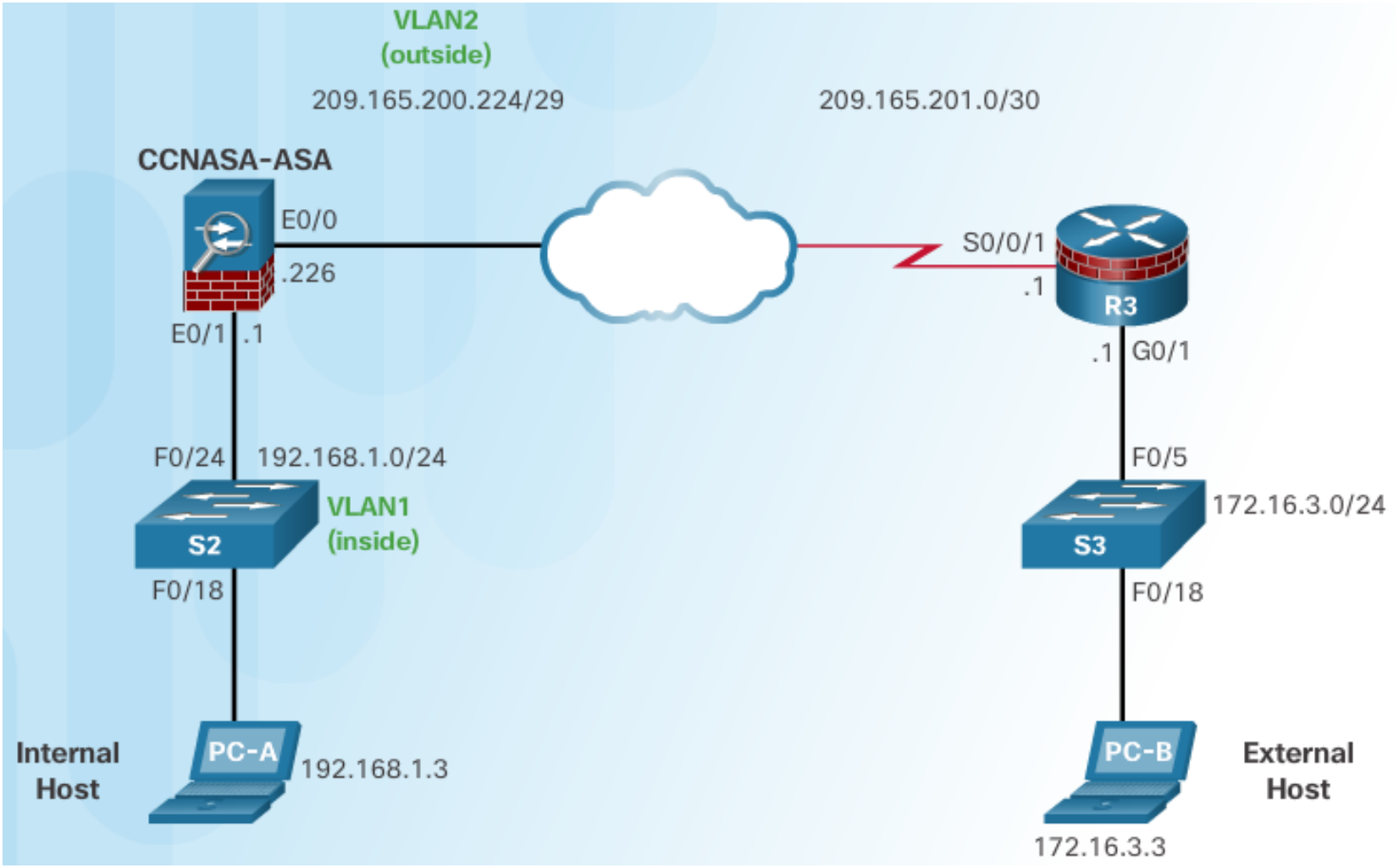


# Site-to-Site VPN Wizard

# 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

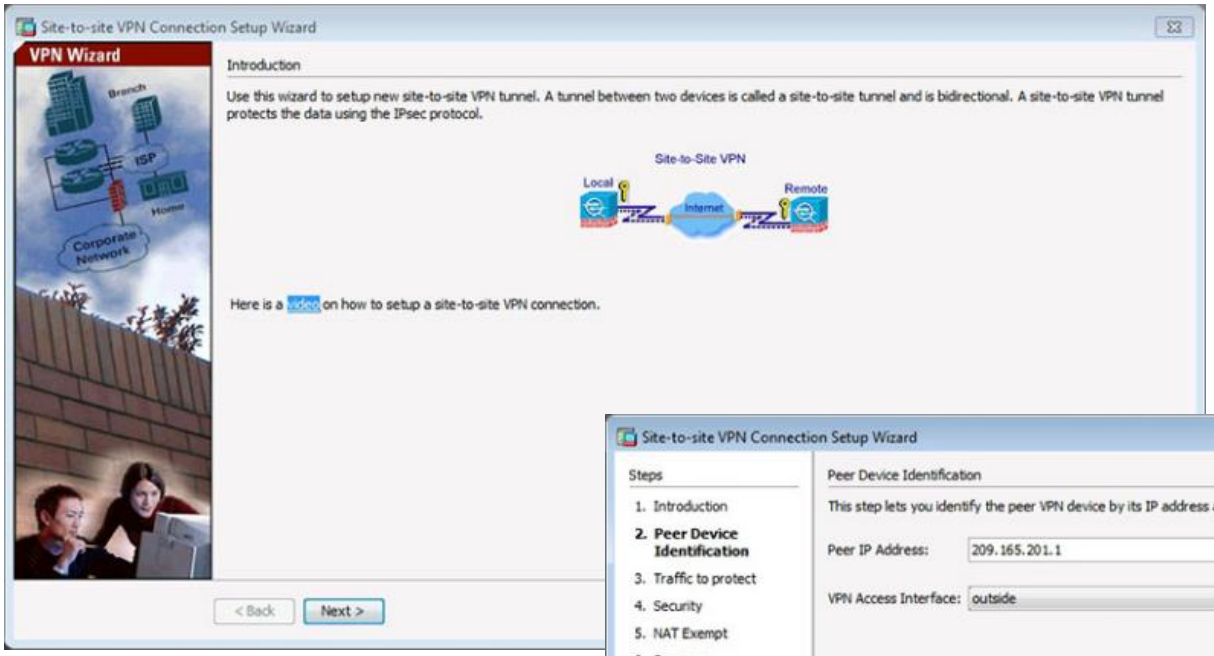
```
R3(config)# crypto map S2S-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)# set peer 209.165.200.226
R3(config-crypto-map)# set transform-set ESP-TUNNEL
R3(config-crypto-map)# match address VPN-ACL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

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

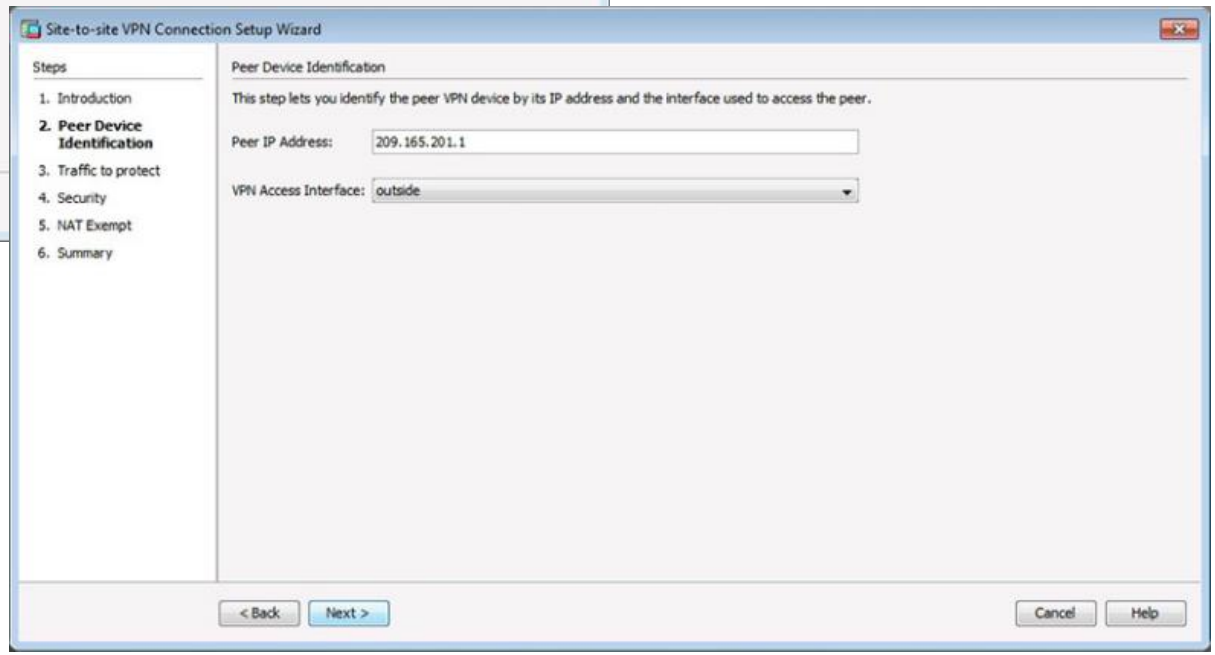
```
CNAS-ASA(config)# enable password class
CCNAS-ASA(config)#
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#
CCNAS-ASA(config-if)# interface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

Basic ISR Configuration

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

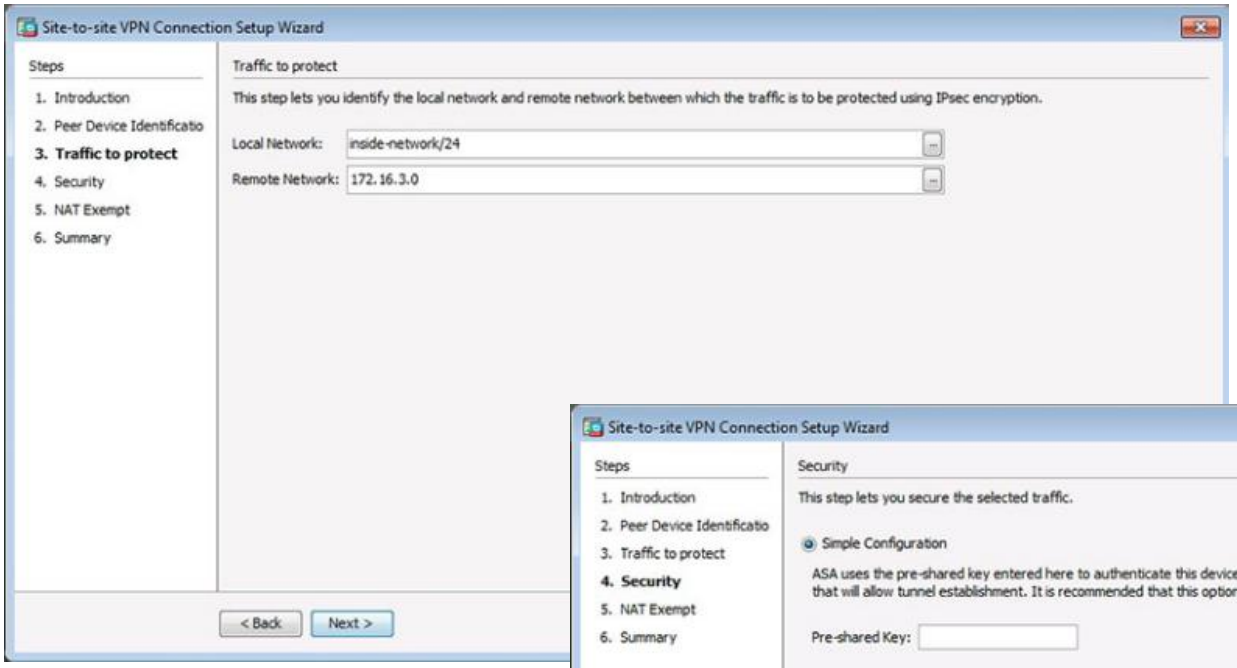



Introduction Window

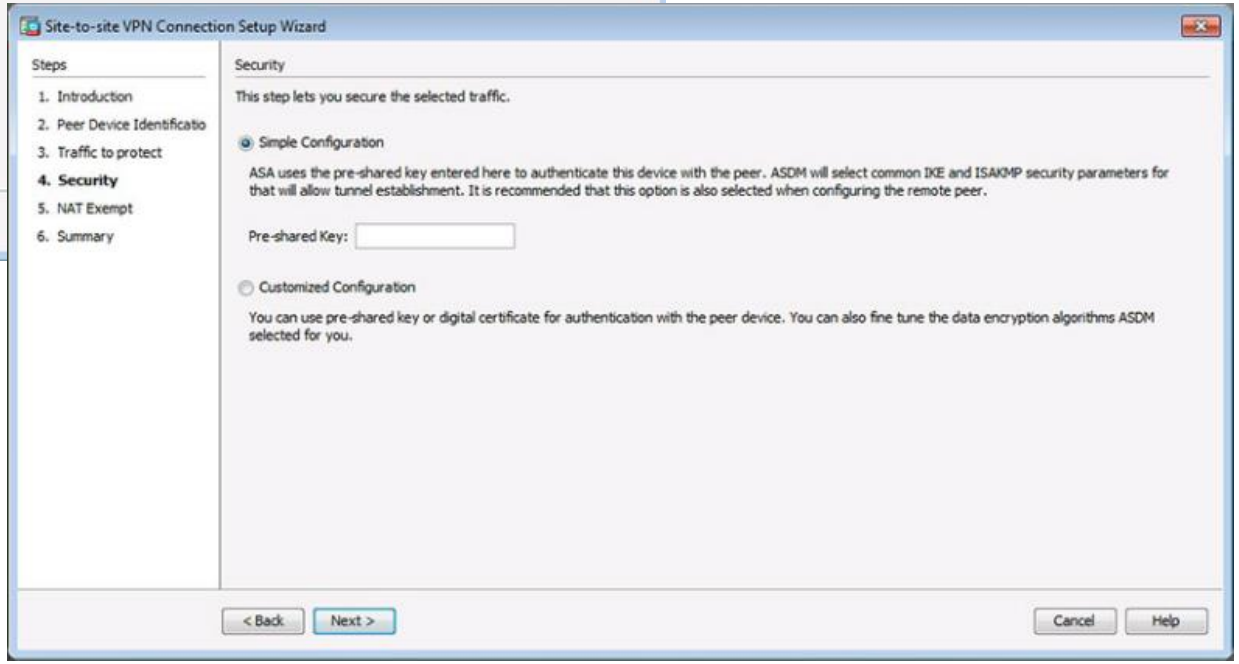



Peer Device Identification Window

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

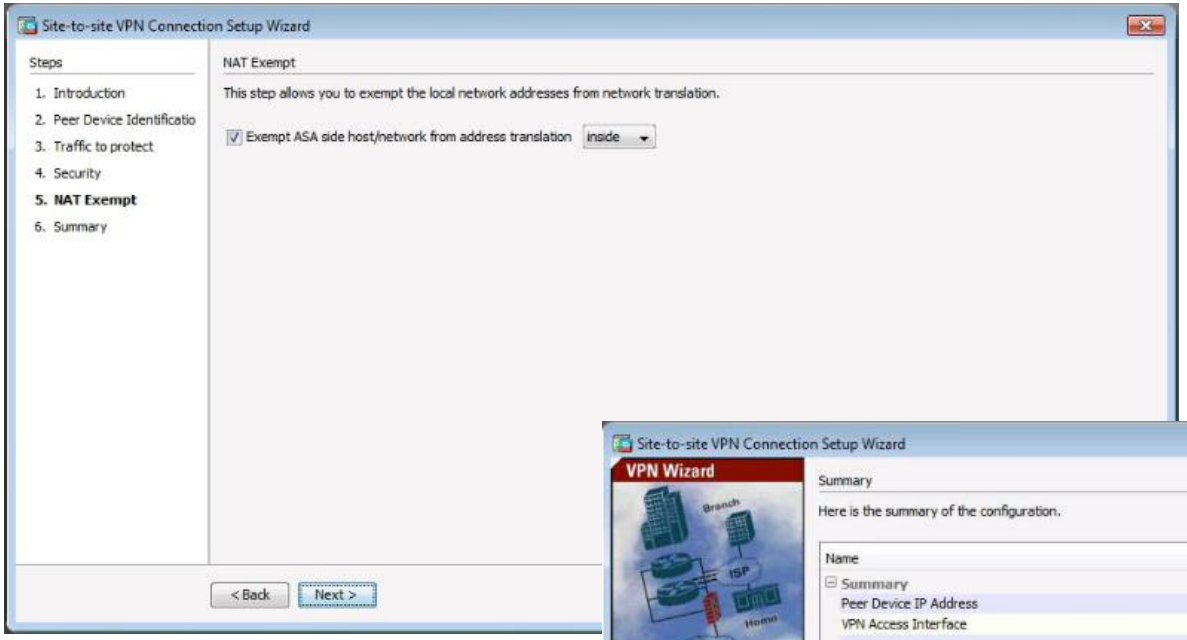



Traffic to Protect Window

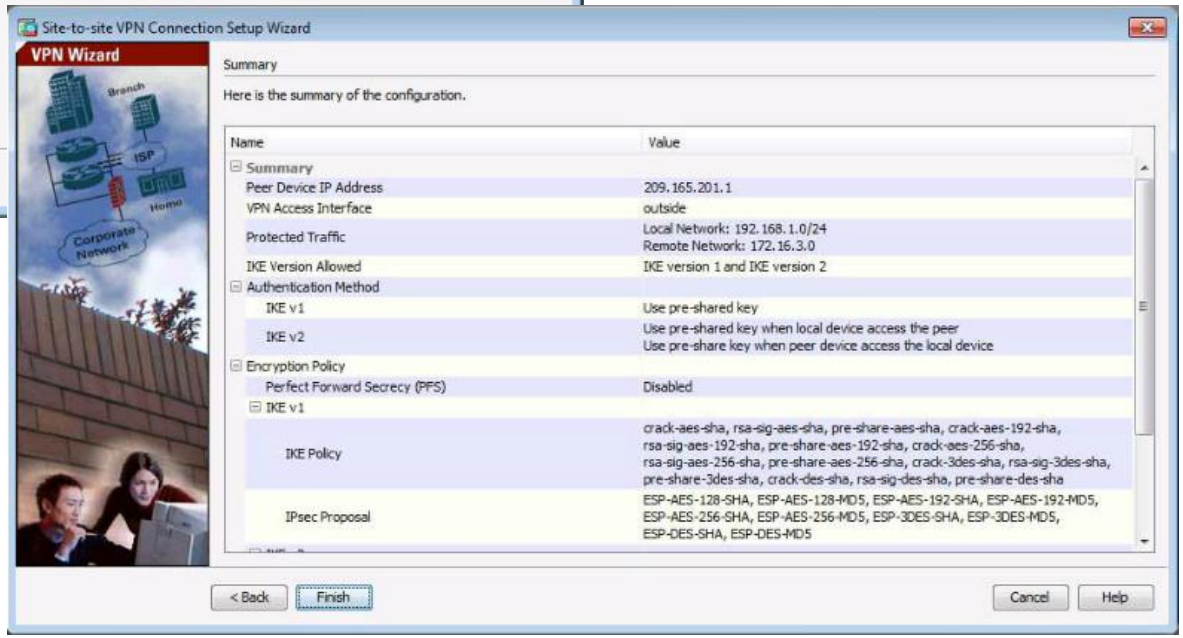



Security Window

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

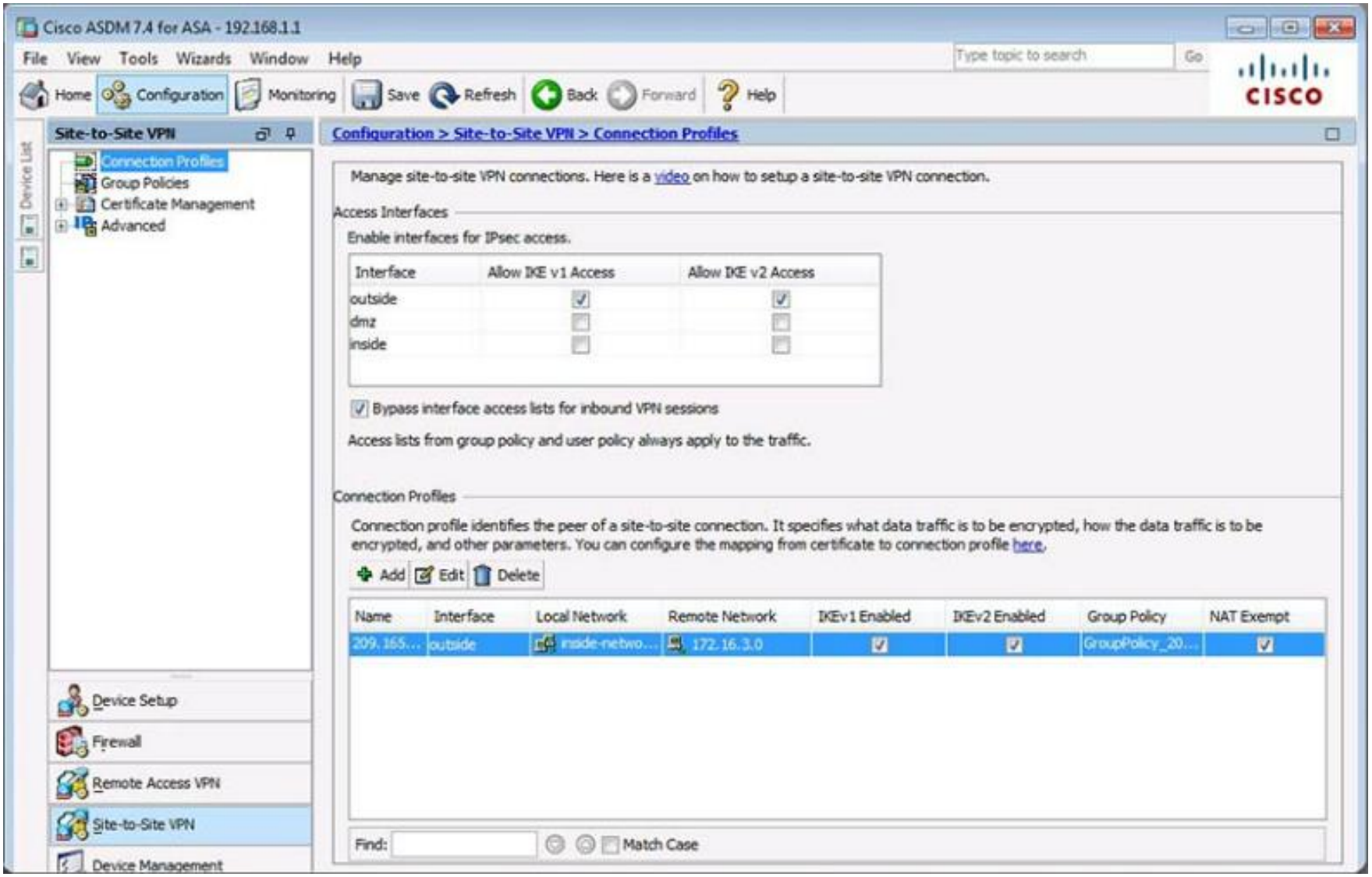



NAT Exempt Window



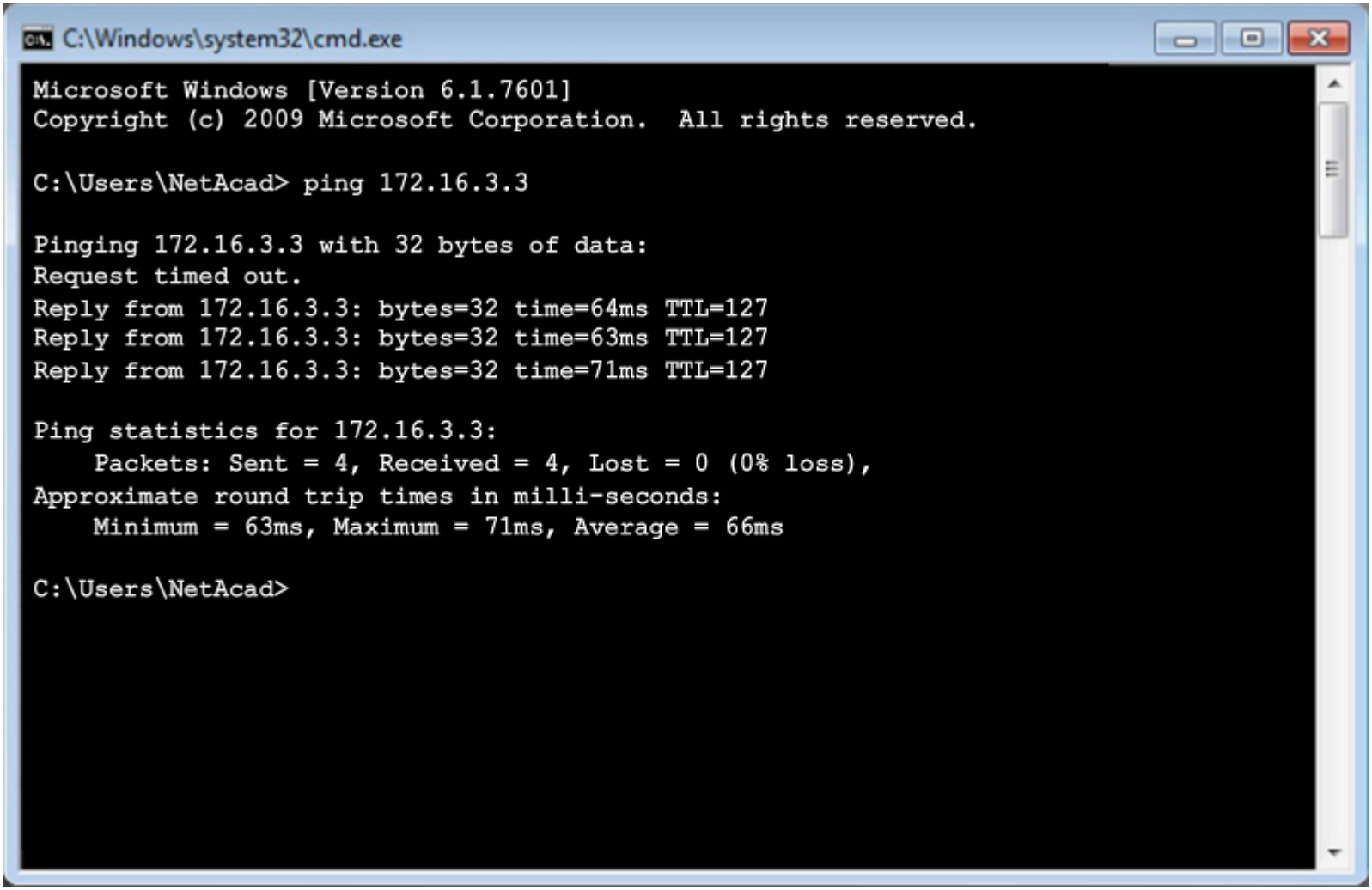

Summary Window

# Verifying Site-to-Site VPNs Using ASDM



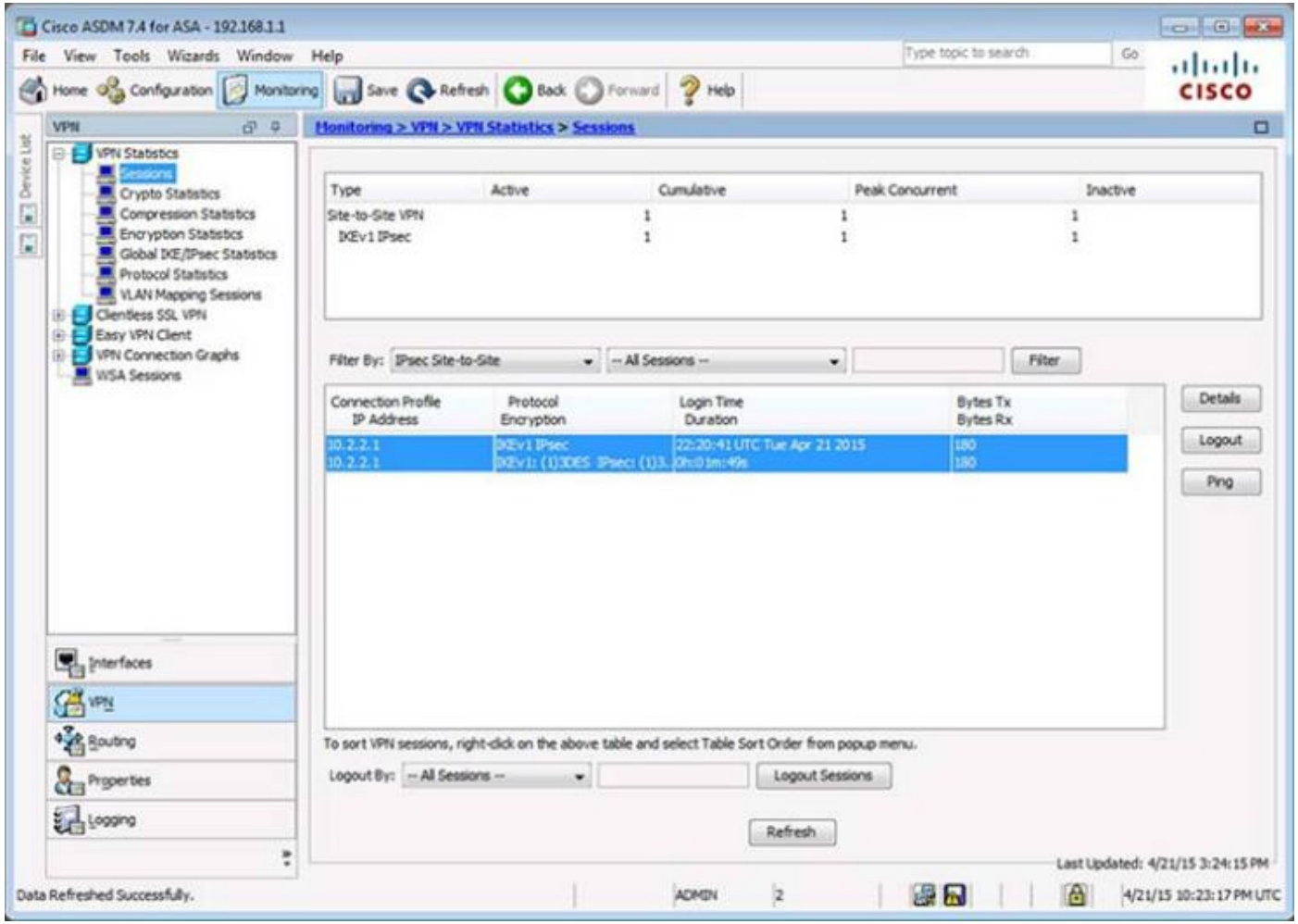
# Test the Site-to-Site VPNs Using ASDM

Establish the VPN Tunnel Connection to the Remote Network



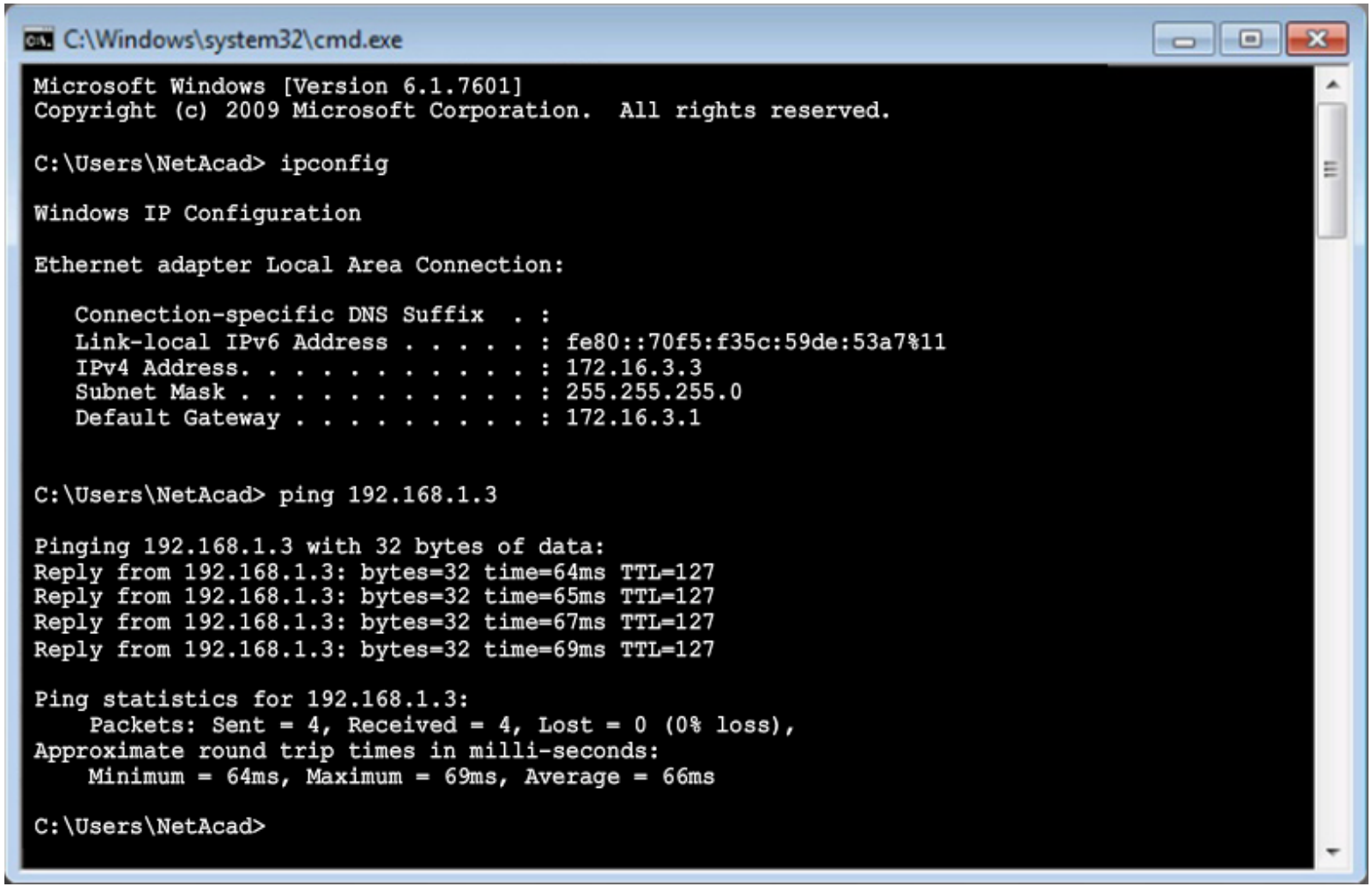
# Test the Site-to-Site VPNs Using ASDM (Cont.)

Monitoring the VPN Tunnel



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

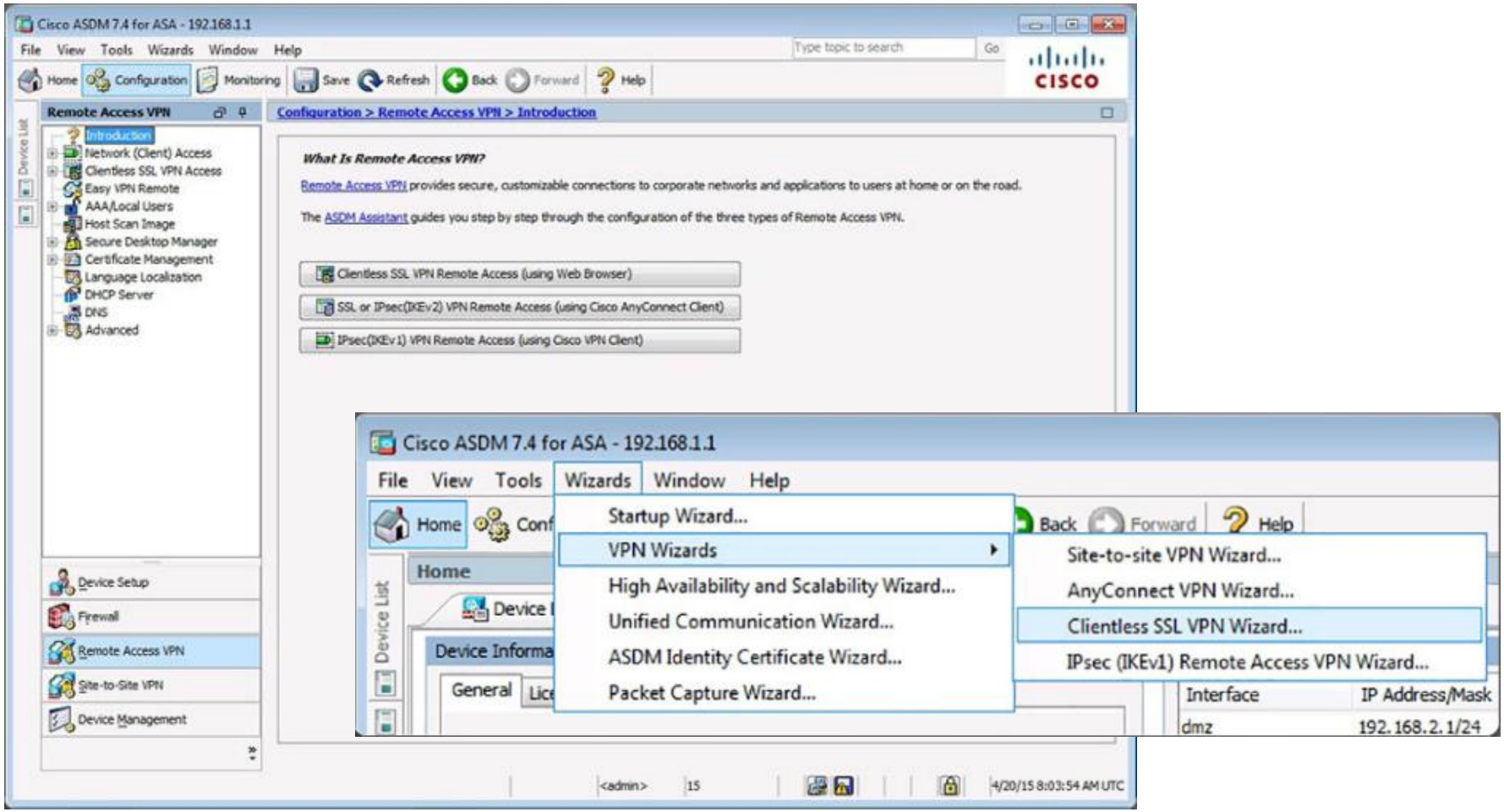
Verify VPN Tunnel Connectivity from the External Host



# Clientless VPN Wizard

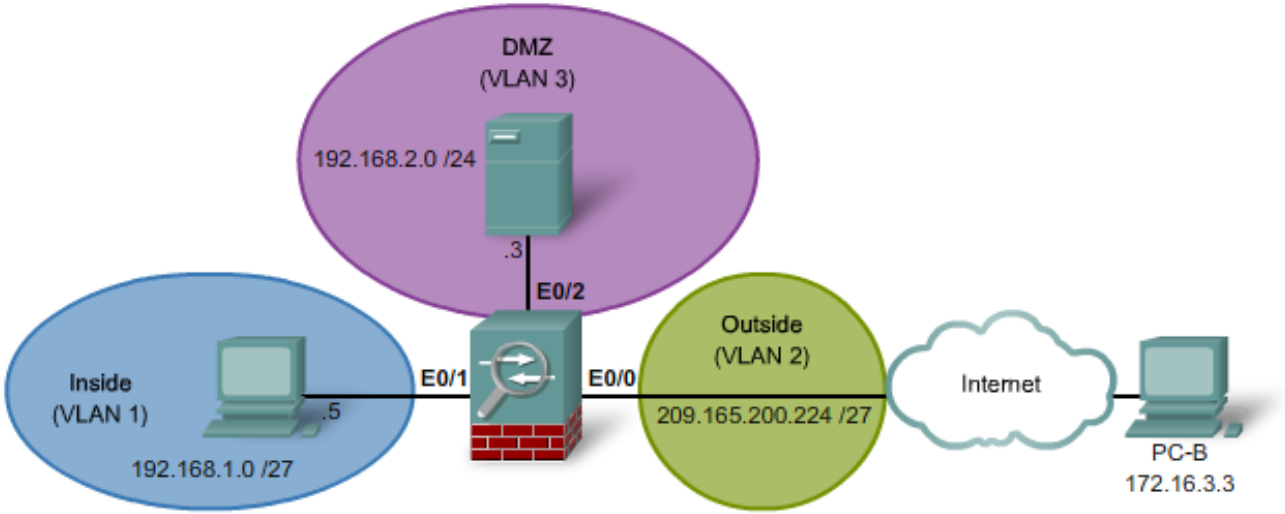
# ASDM Assistant

- Clientless SSL VPN can be configured using the ASDM Assistant or **Wizards** > **VPN Wizards** > **Clientless SSL VPN Wizard**.



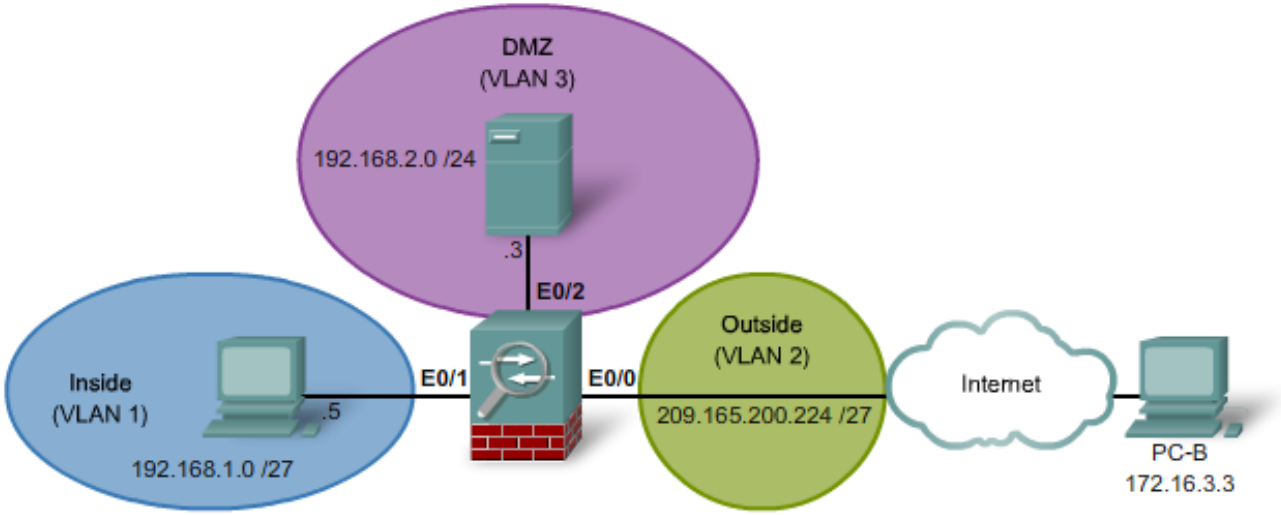
# Clientless SSL VPN Wizard Example

- The topology in this example is as follows:
  - An inside network with security level 100
  - A DMZ with security level 50
  - An outside network with a security level of 0
- Access to the DMZ server is already provided using static NAT.

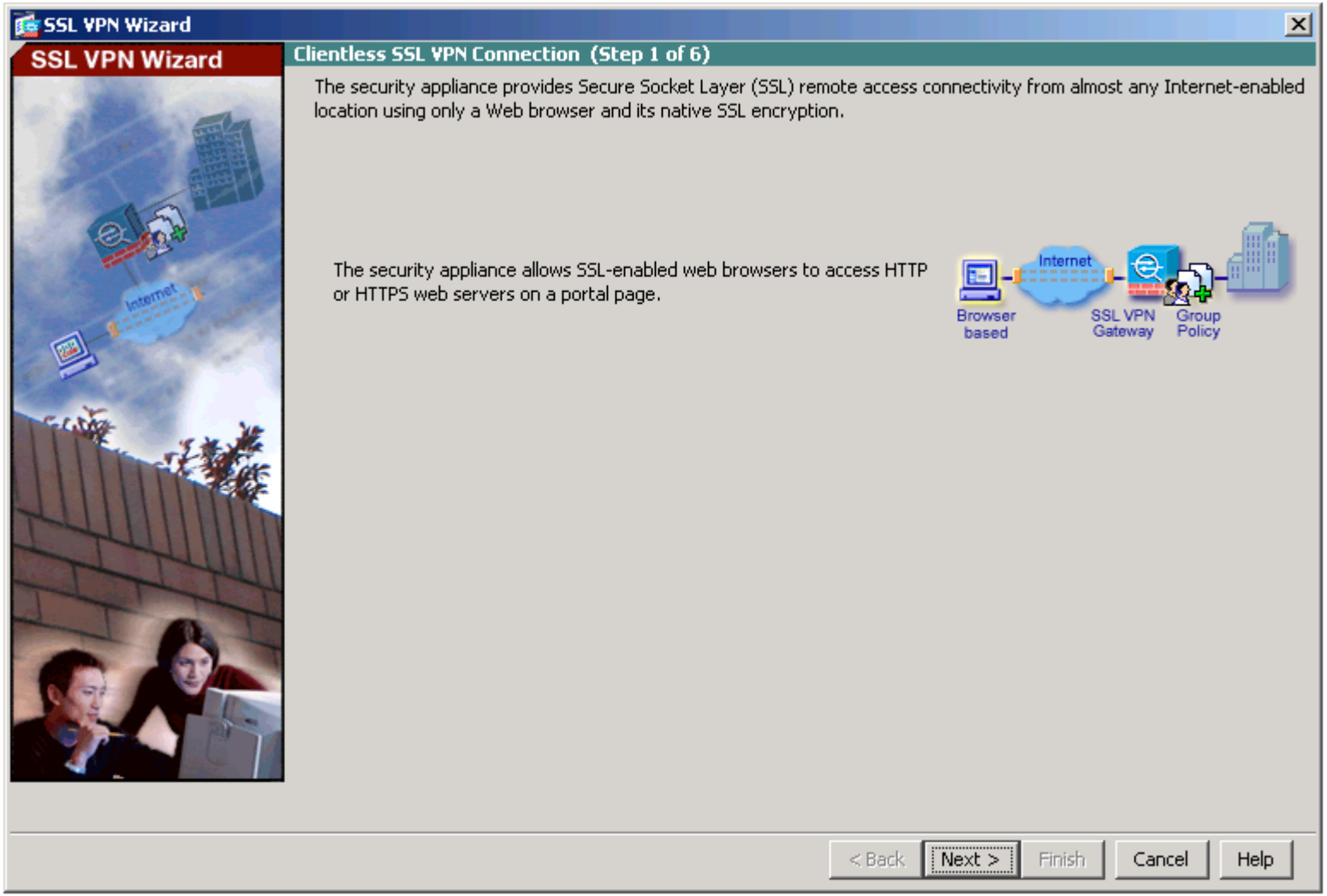


# Clientless SSL VPN Wizard Example

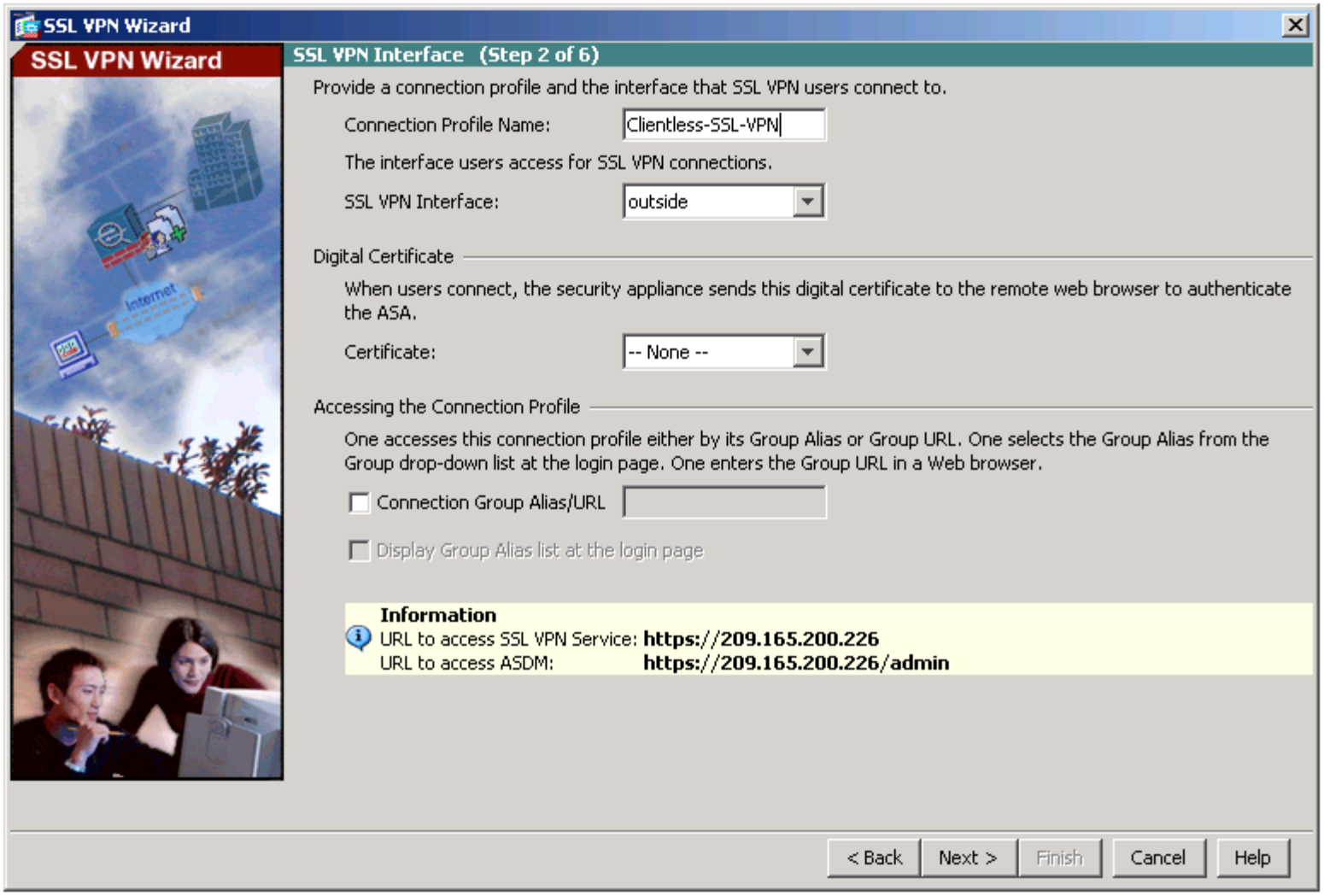
- Assume the outside host requires access to specific applications which do not need a full tunnel SSL VPN.
- For this reason, the remote host will use a secure web browser connection to access select corporate resources.



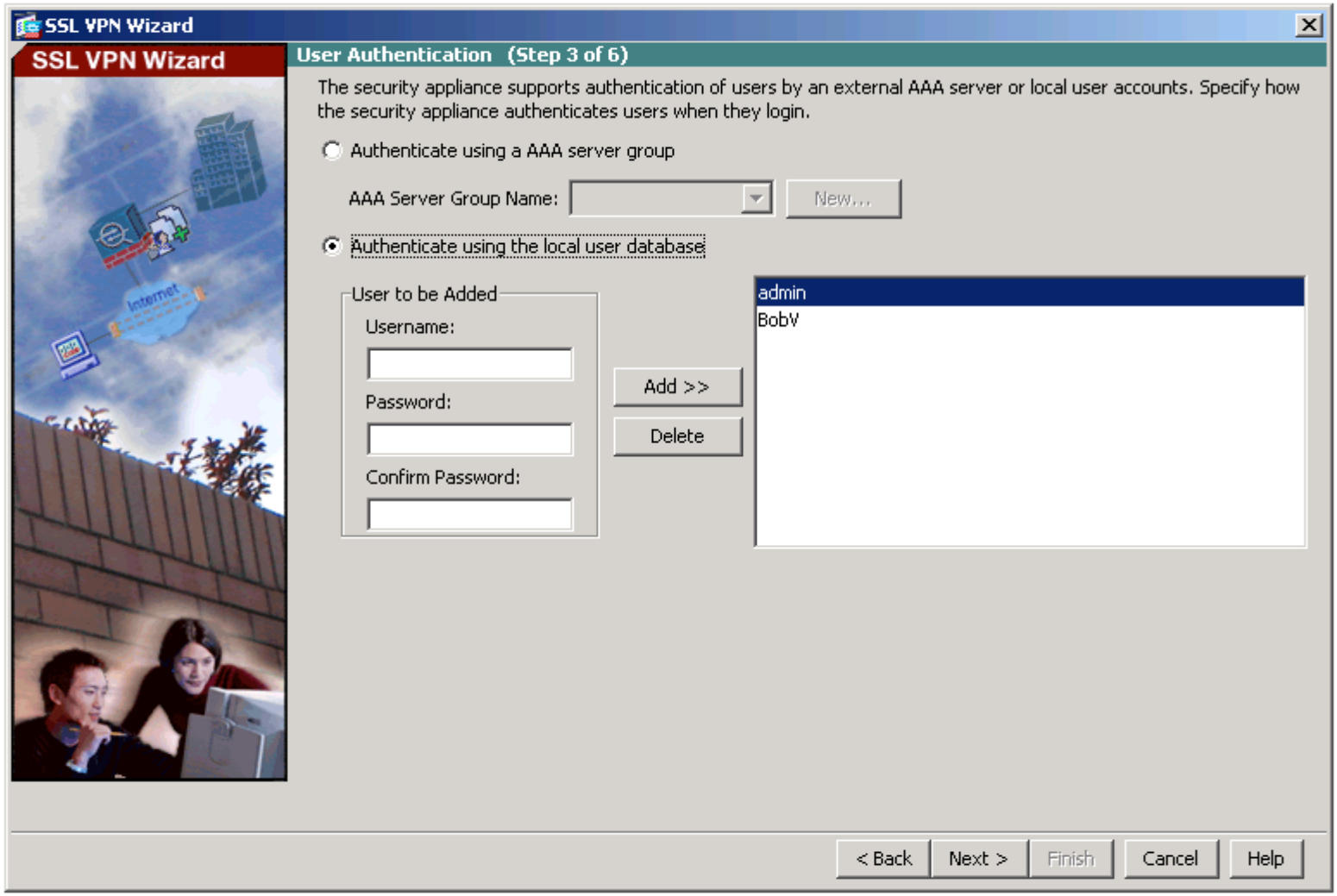
# 1 - SSL VPN Welcome Window



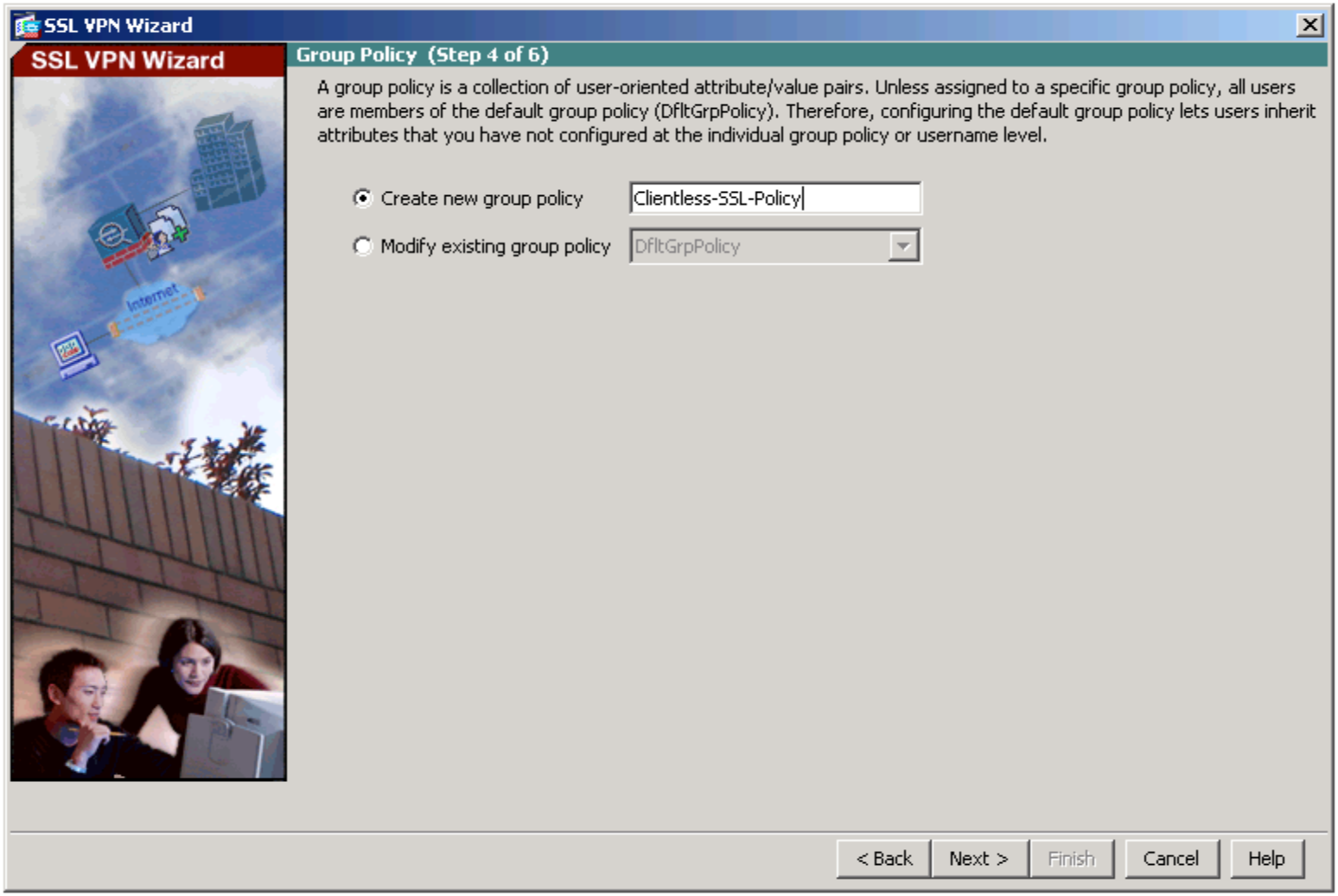
# 2 - SSL VPN Interface



# 3 - User Authentication

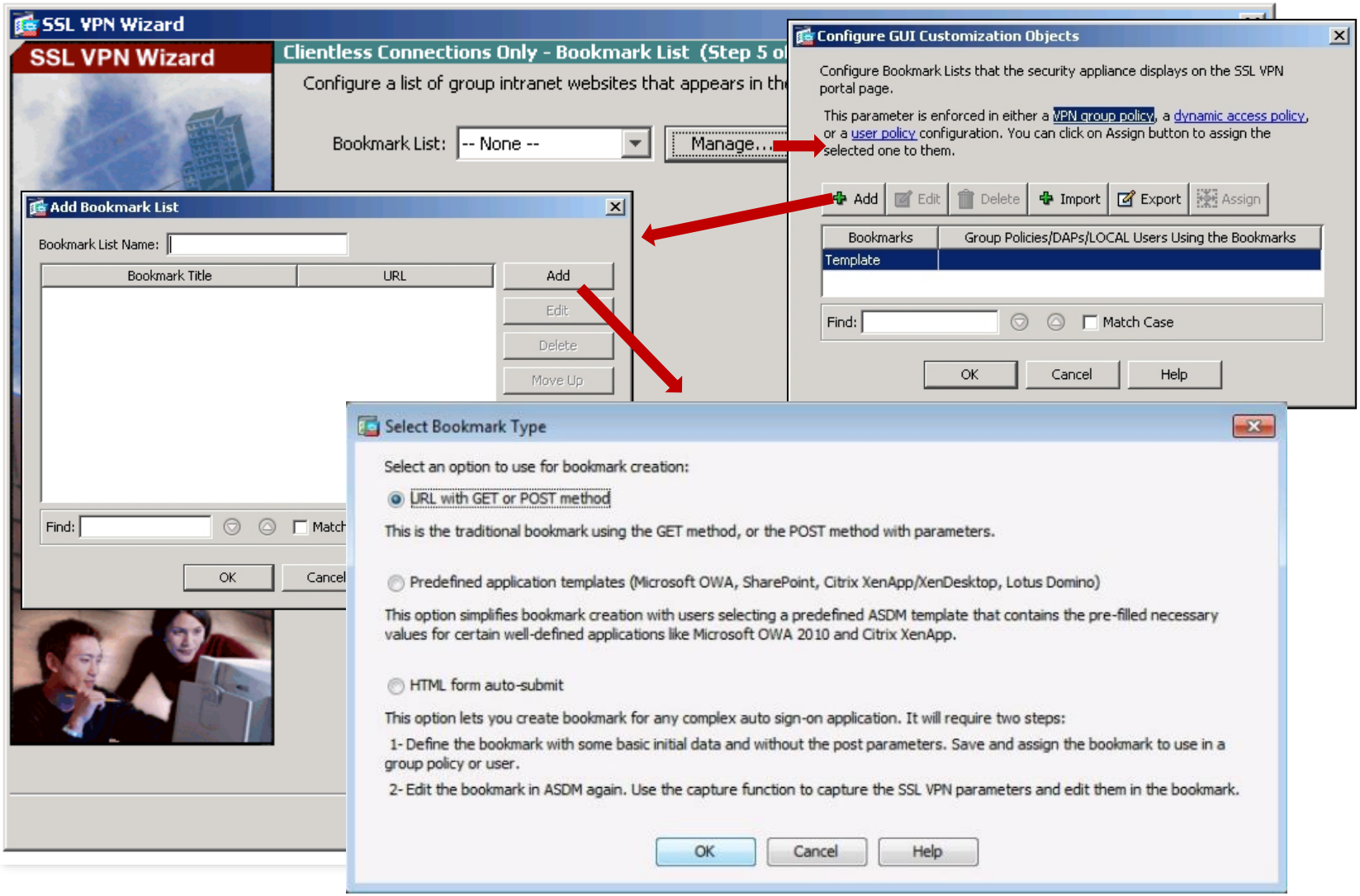


# 4 - Group Policy

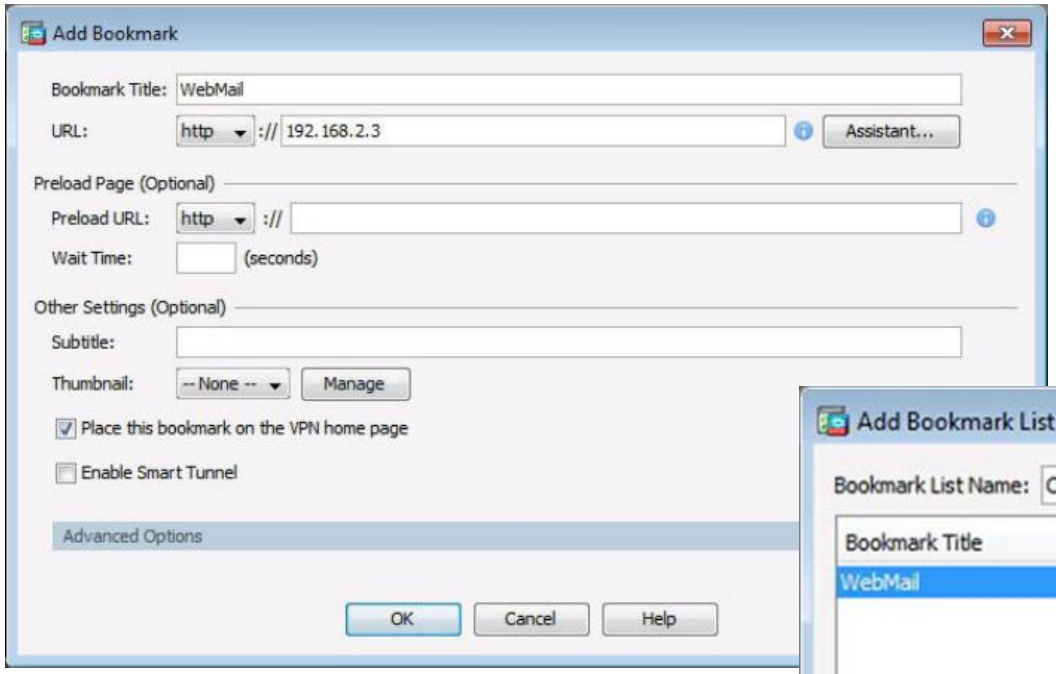


# 5 - Bookmark Lists

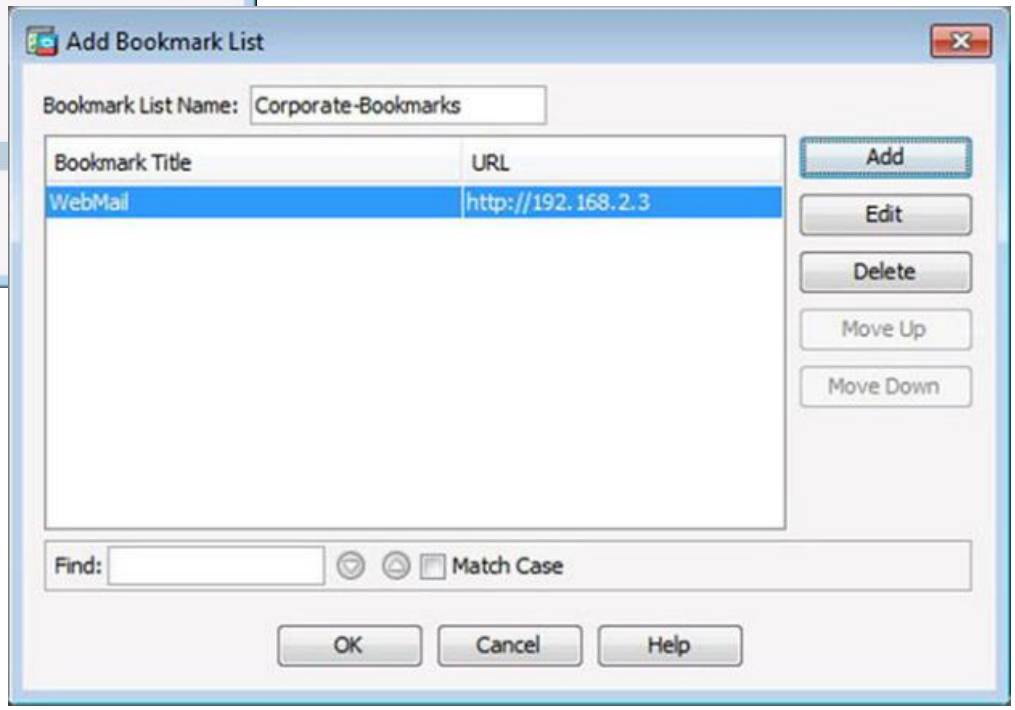
A bookmark list is a set of URLs that is configured to be used in the clientless SSL VPN web portal.



# 5 - Bookmark Lists

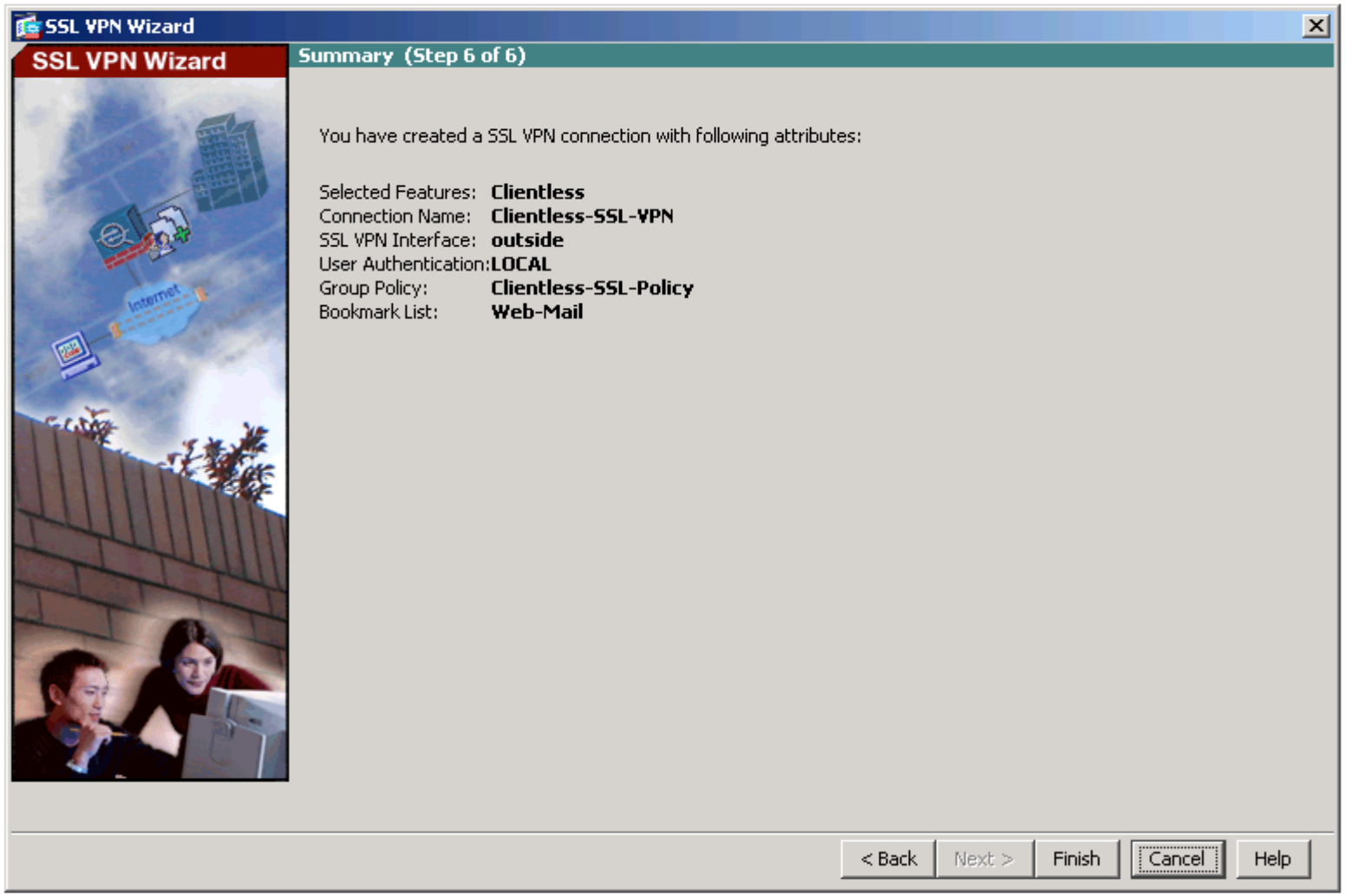



Add Bookmark Window



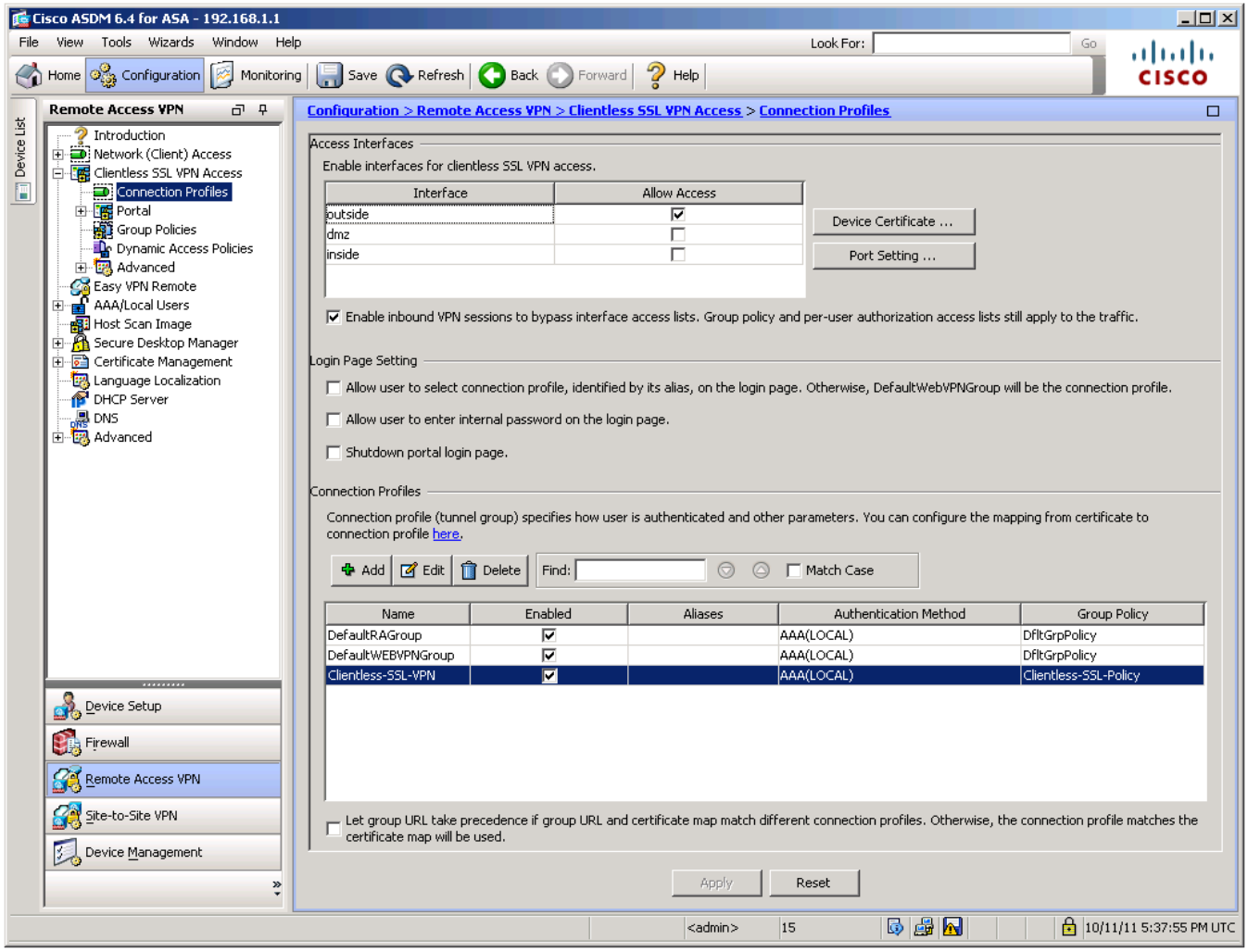

Revised Add Bookmark List Window

# 6 - Summary


SSL VPN Wizard
SSL VPN Wizard
Summary (Step 6 of 6)
You have created a SSL VPN connection with following attributes:
Selected Features: Clientless
Connection Name: Clientless-SSL-VPN
SSL VPN Interface: outside
User Authentication: LOCAL
Group Policy: Clientless-SSL-Policy
Bookmark List: Web-Mail
Internet
< Back
Next >
Finish
Cancel
Help

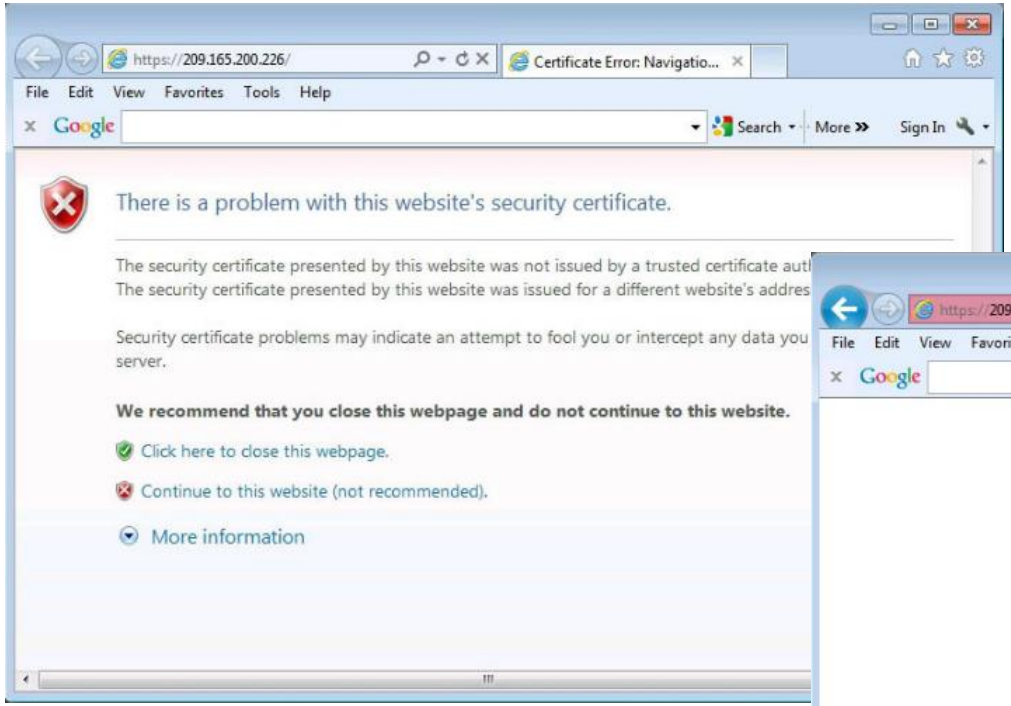
# Verifying Clientless SSL VPN

- **Configurations > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**

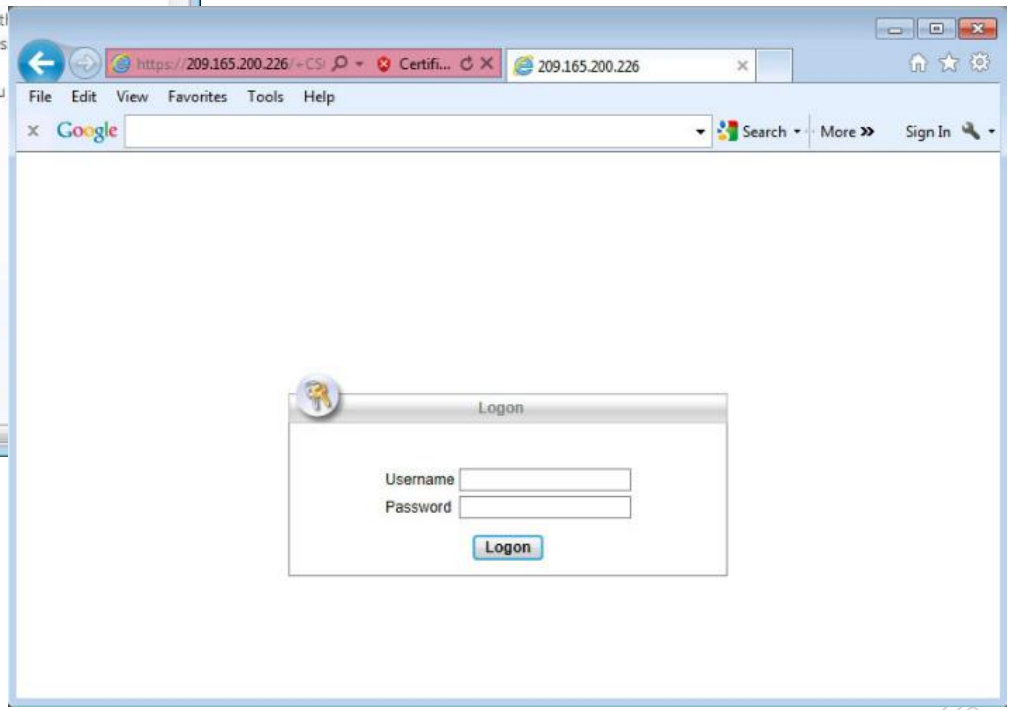


# Login From the Remote Host

- From a web browser, enter the public address of the ASA device
  - Be sure to use secure HTTP (HTTPS)

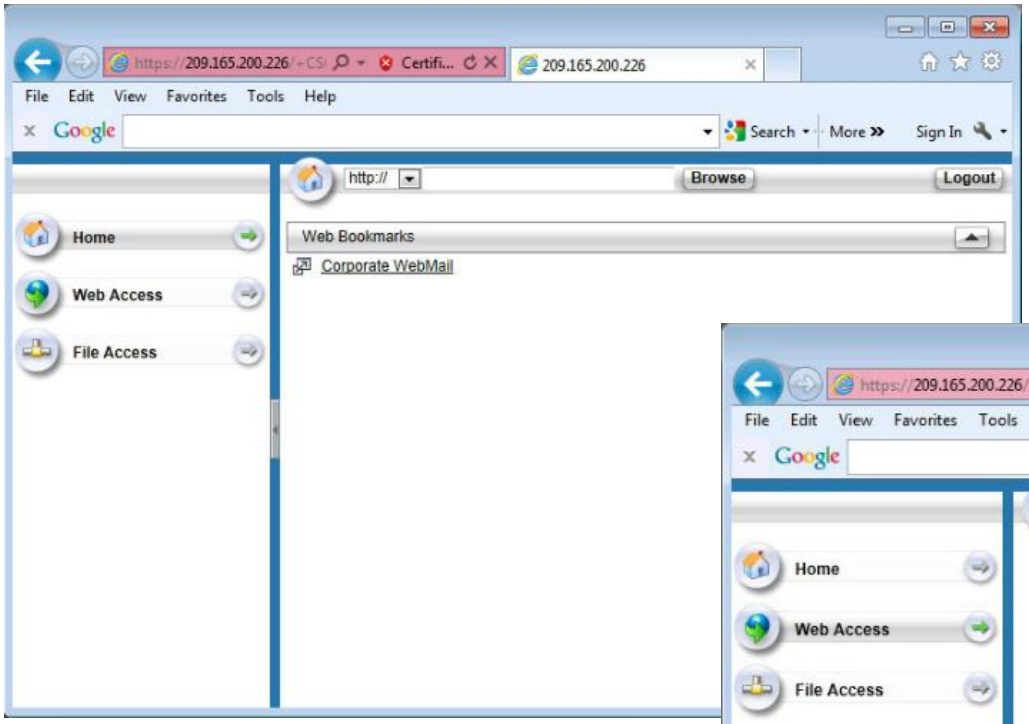



Security Certificate Window

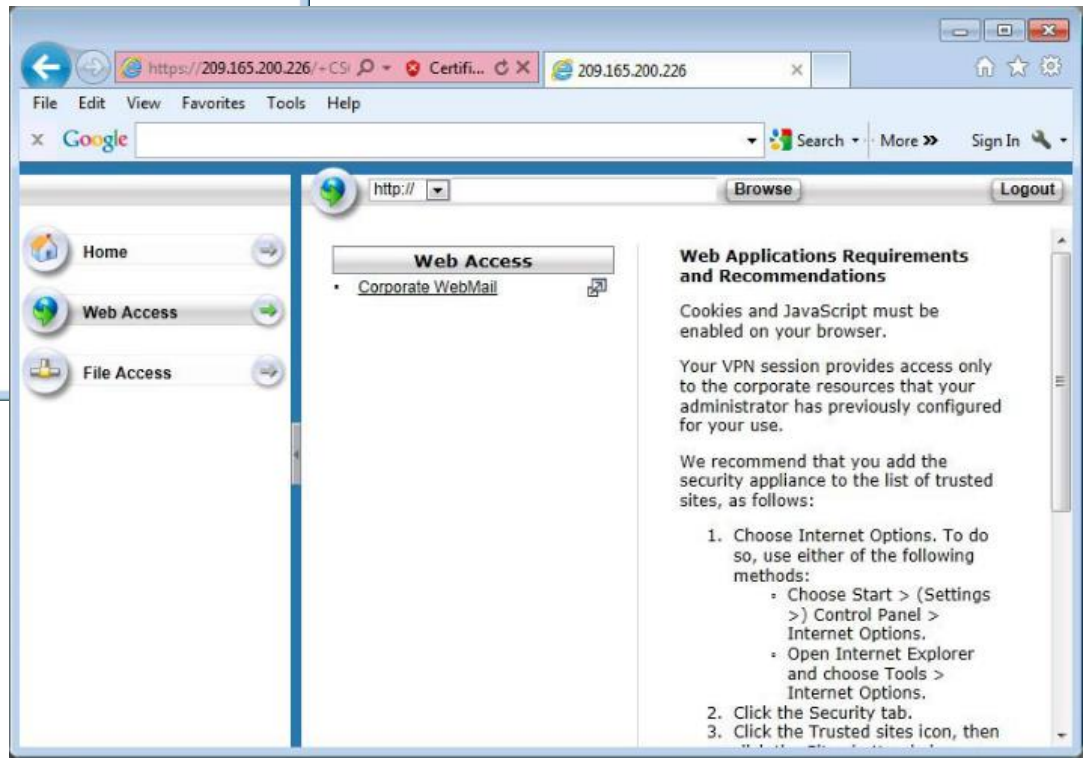



Logon Window

# Testing the Clientless SSL VPN Connection (Cont.)

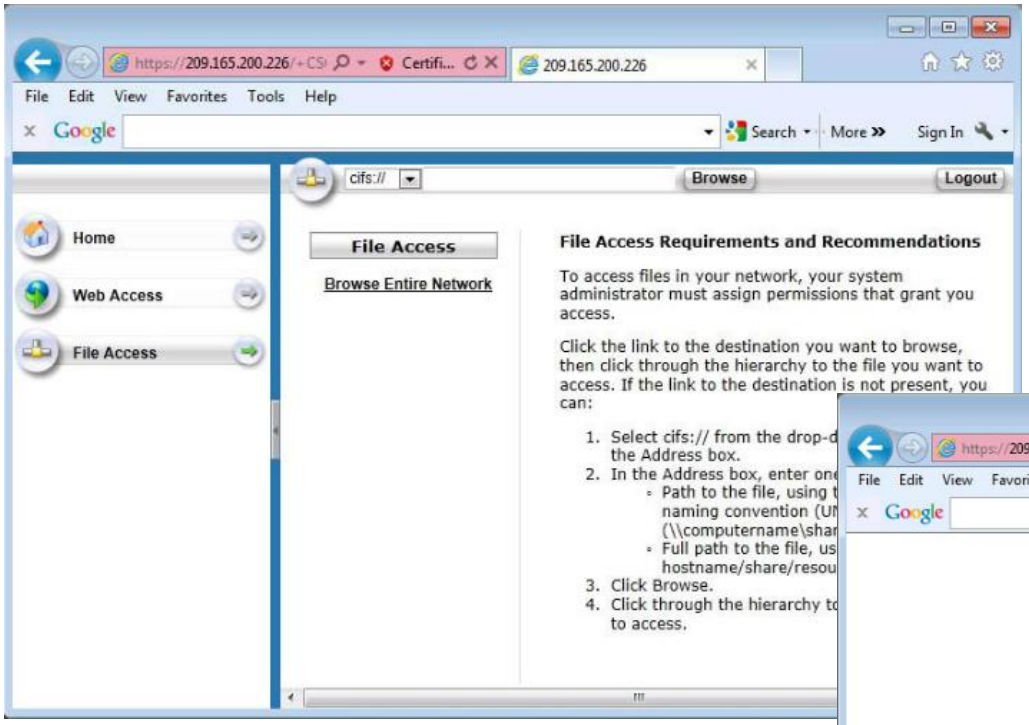



Web Portal Home Page

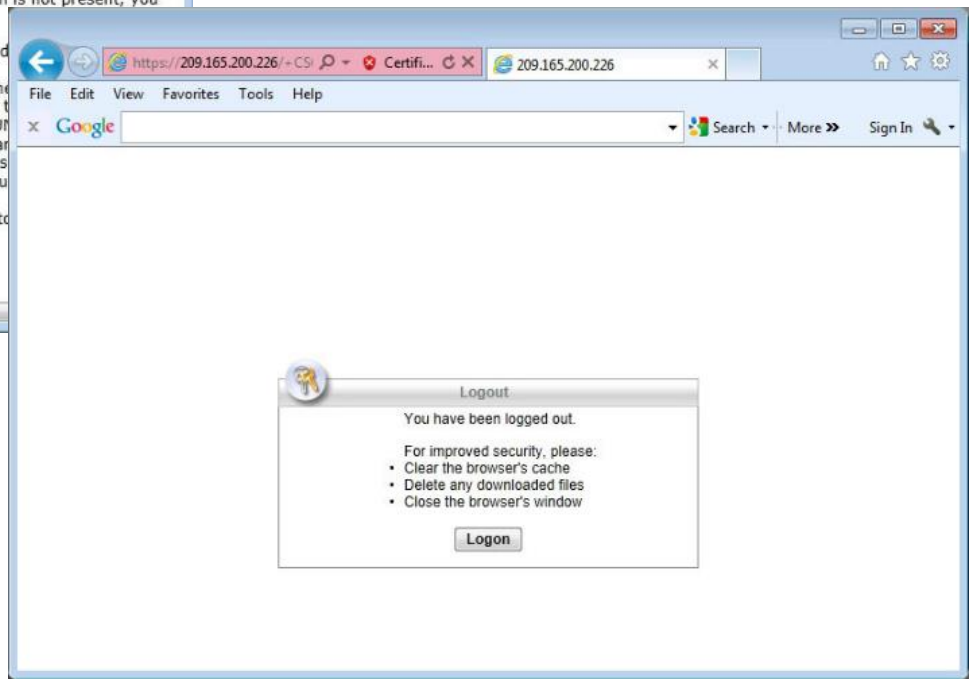



Web Portal Web Access Page

# Testing the Clientless SSL VPN Connection (Cont.)



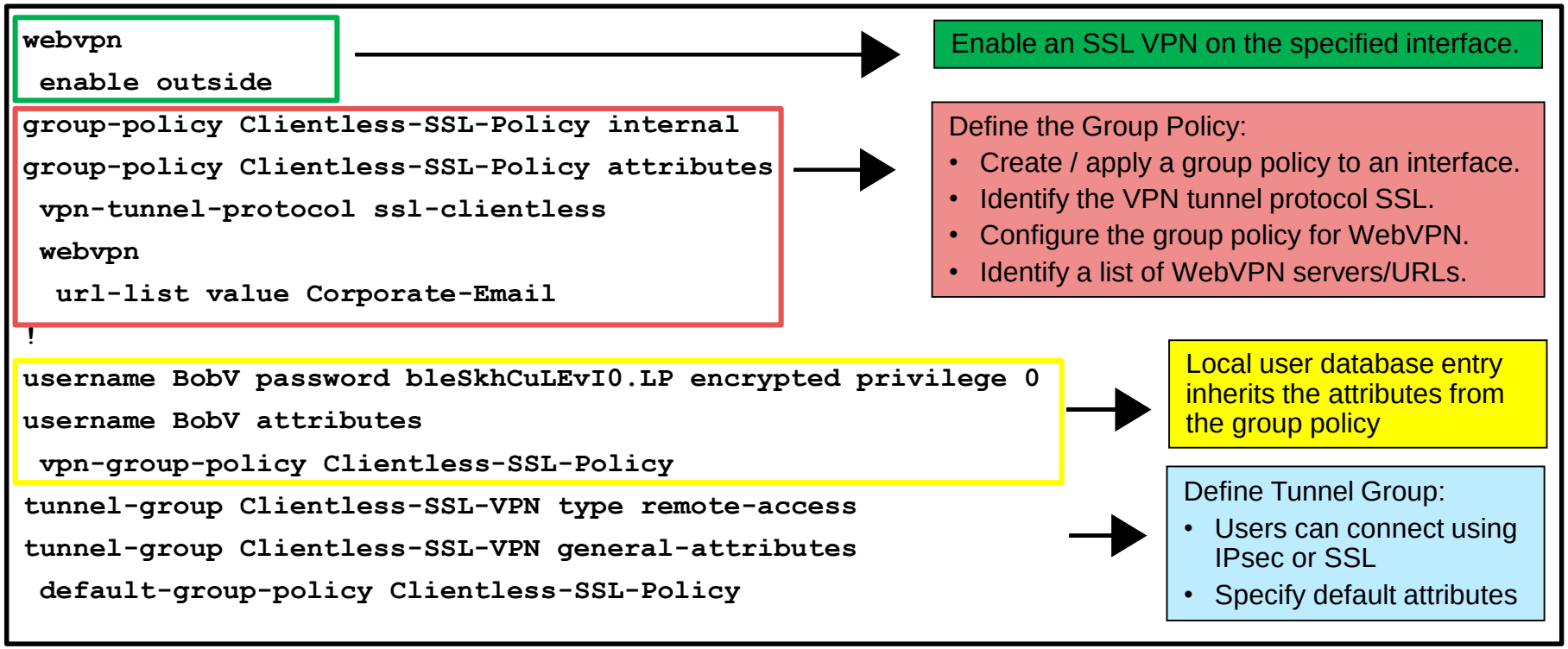

Web Portal File Access Page




Log Out of the Web Portal

# Generated CLI Commands

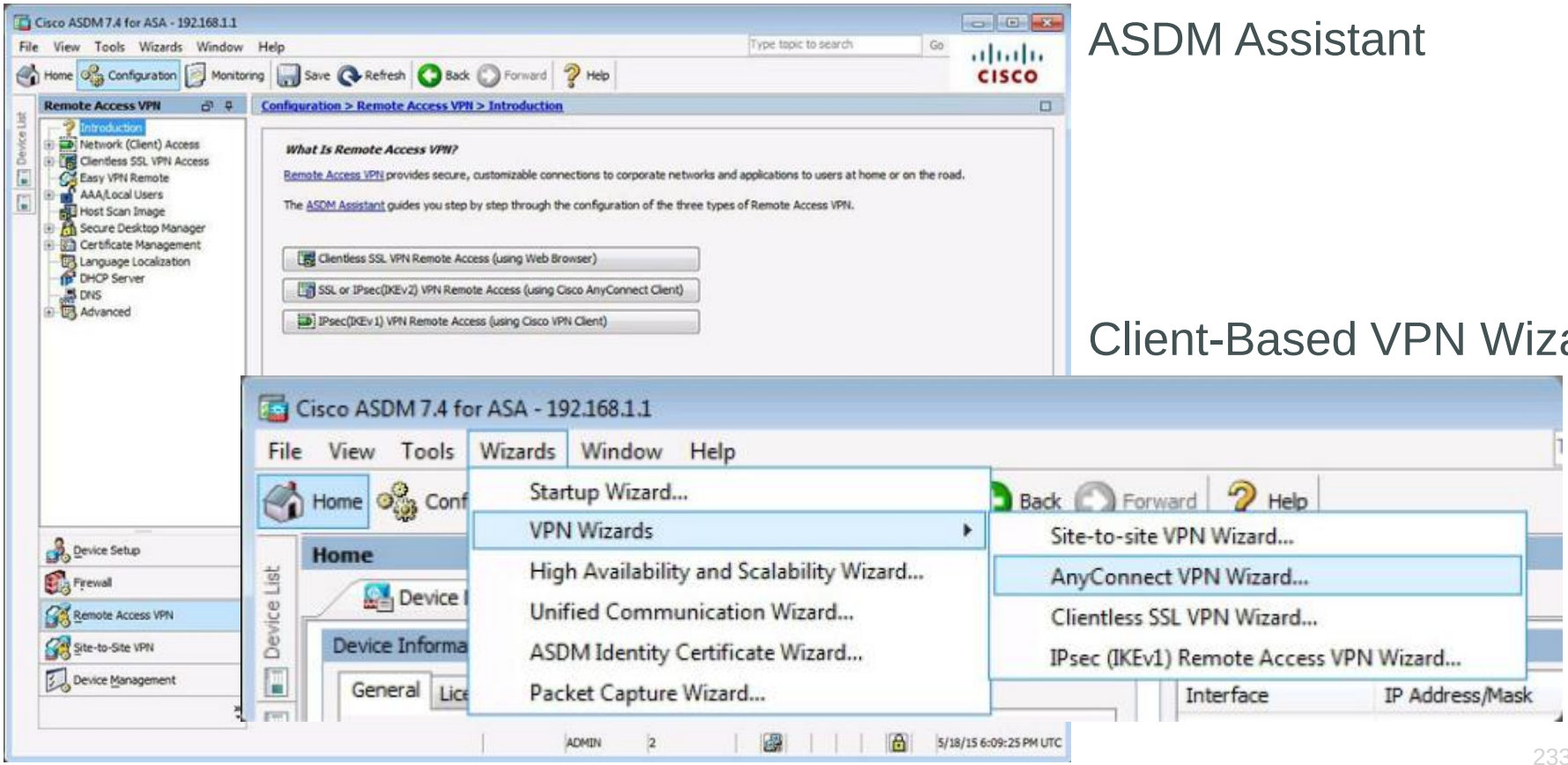
- The clientless SSL VPN wizard generates configuration settings for the following:



# AnyConnect VPN Wizard

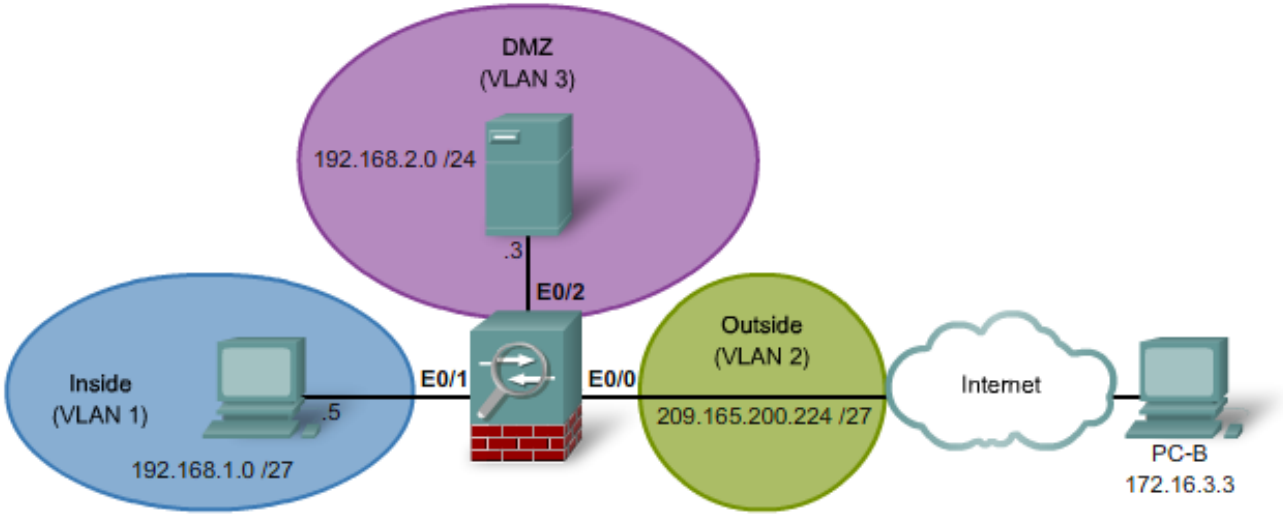
# ASDM Assistant

- **Configurations** > **Remote-Access VPN** > **Introduction**
  - Click **SSL or IPsec(IKEv2) VPN Remote Access (using Cisco AnyConnect Client)**.
- **Wizards** > **VPN Wizards** > **AnyConnect VPN Wizard**



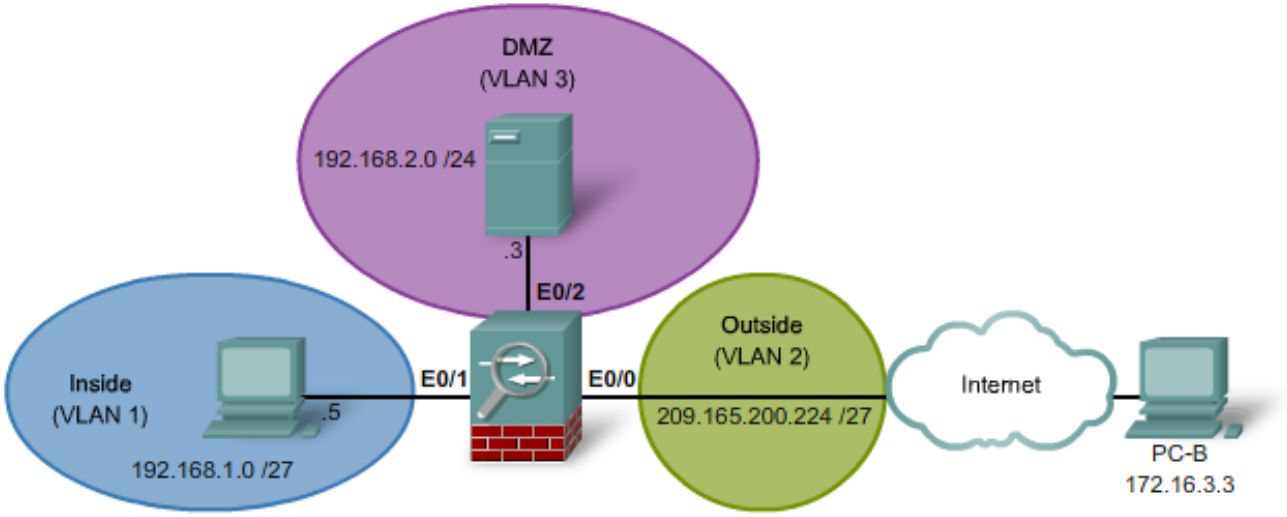
# AnyConnect VPN Wizard Example

- The topology in this example is as follows:
  - An inside network with security level 100
  - A DMZ with security level 50
  - An outside network with a security level of 0
- Access to the DMZ server is already provided using static NAT.

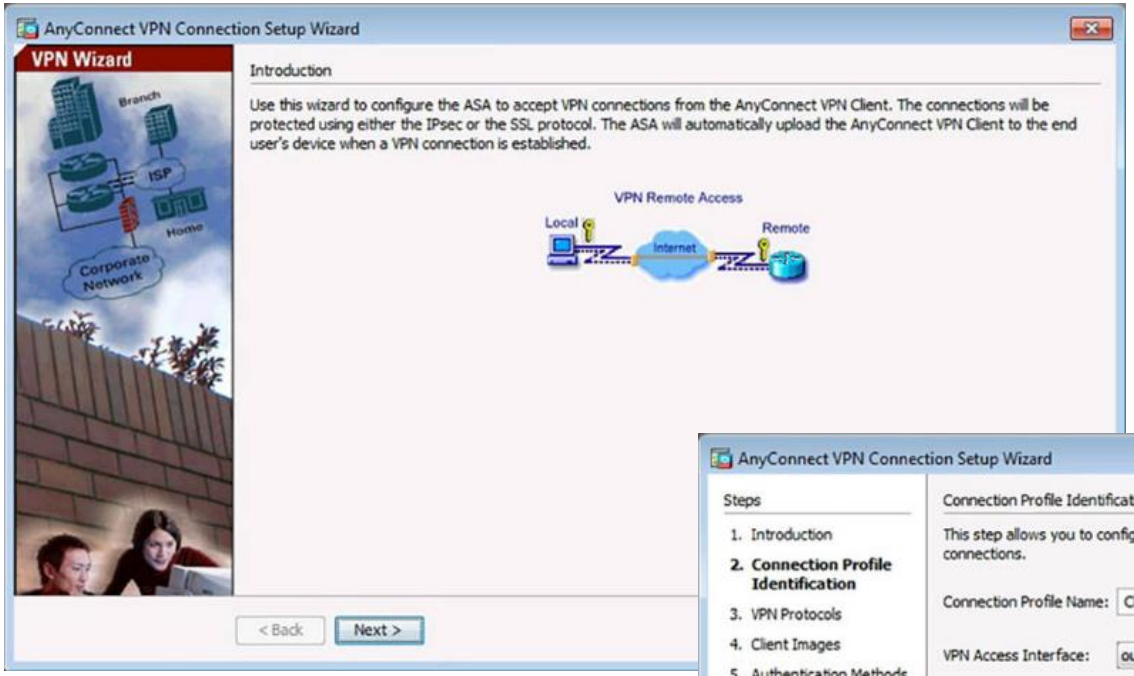


# AnyConnect VPN Wizard Example

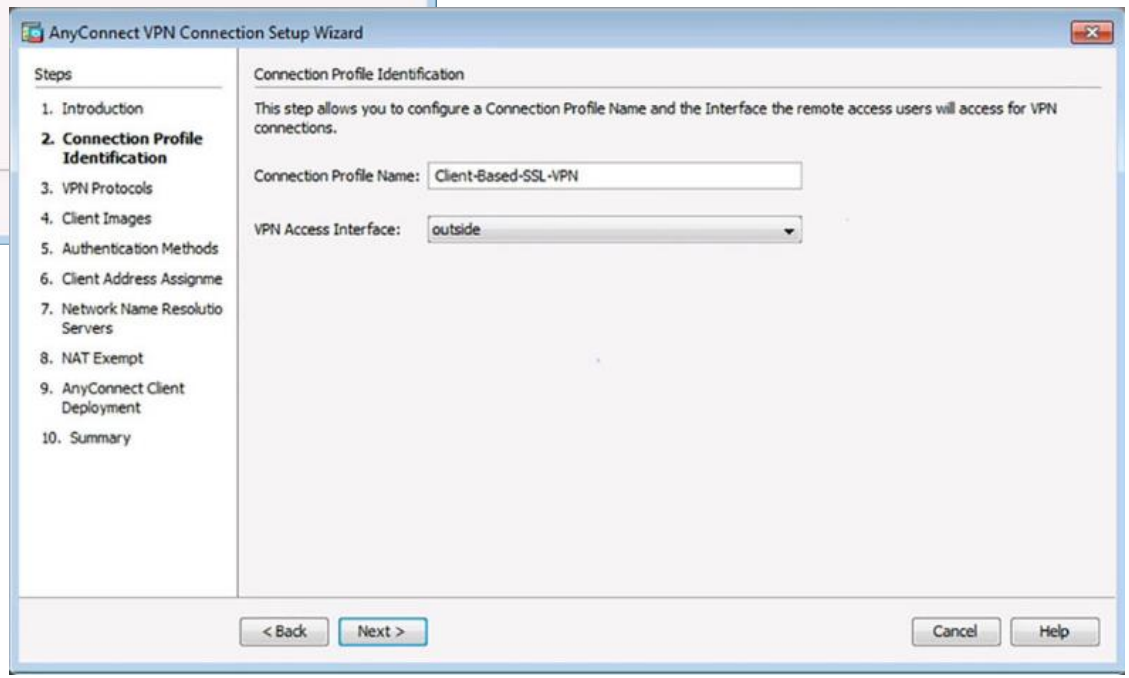
- The outside host does not have the Cisco AnyConnect client pre-installed.
  - Therefore, the remote user will have to initiate a clientless SSL VPN connection using a web browser, and then download and install the AnyConnect client on the remote host.
- Once installed, the host can exchange traffic with the ASA using a full tunnel SSL VPN connection.



# AnyConnect SSL VPN




AnyConnect VPN Wizard Introduction Window

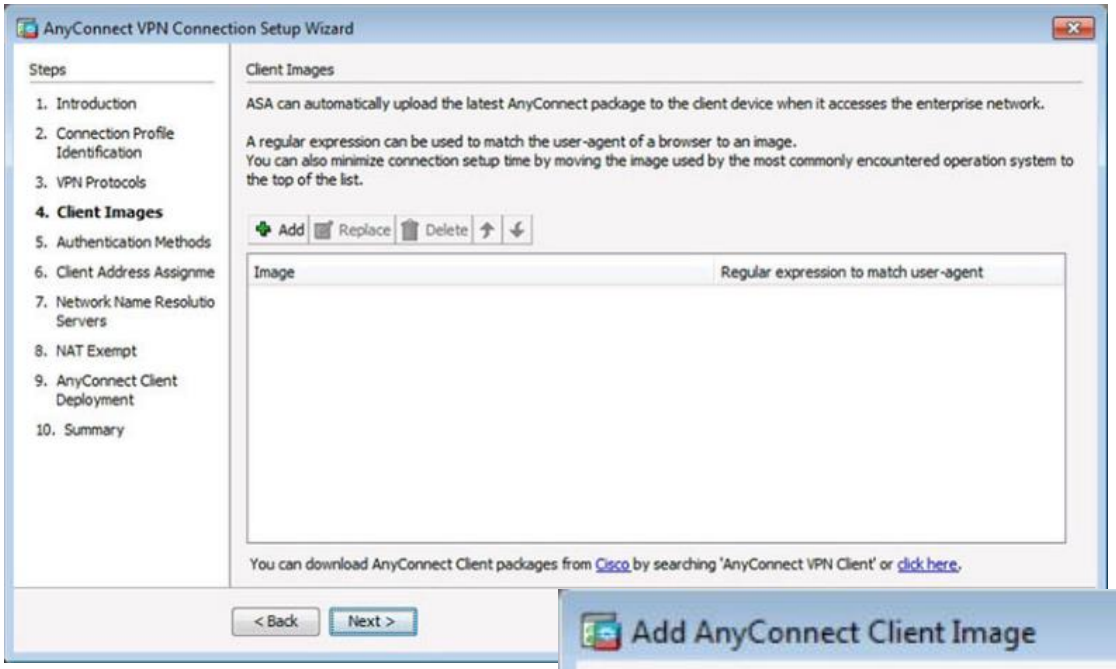



Connection Profile Identification Window

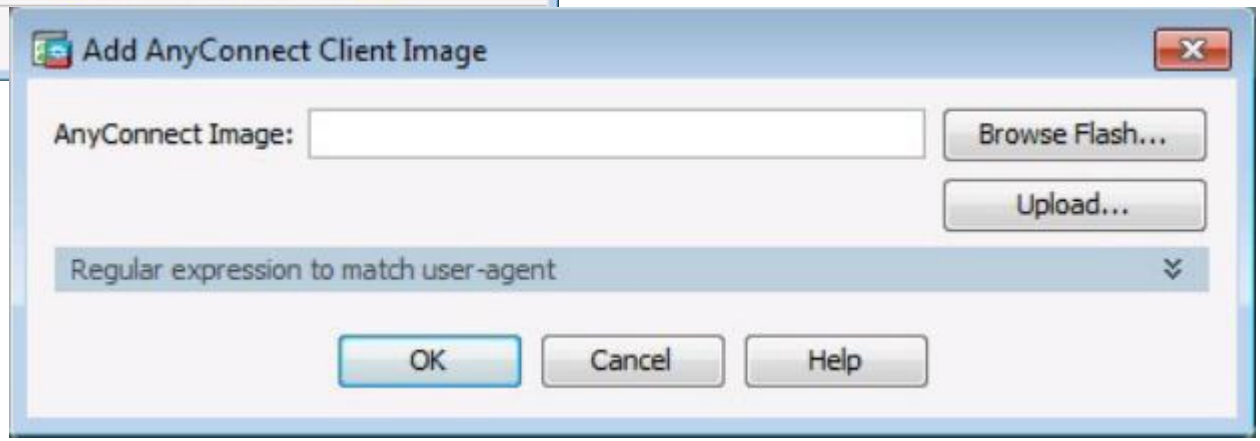
# AnyConnect SSL VPN (Cont.)

VPN Protocols Window

# AnyConnect SSL VPN (Cont.)

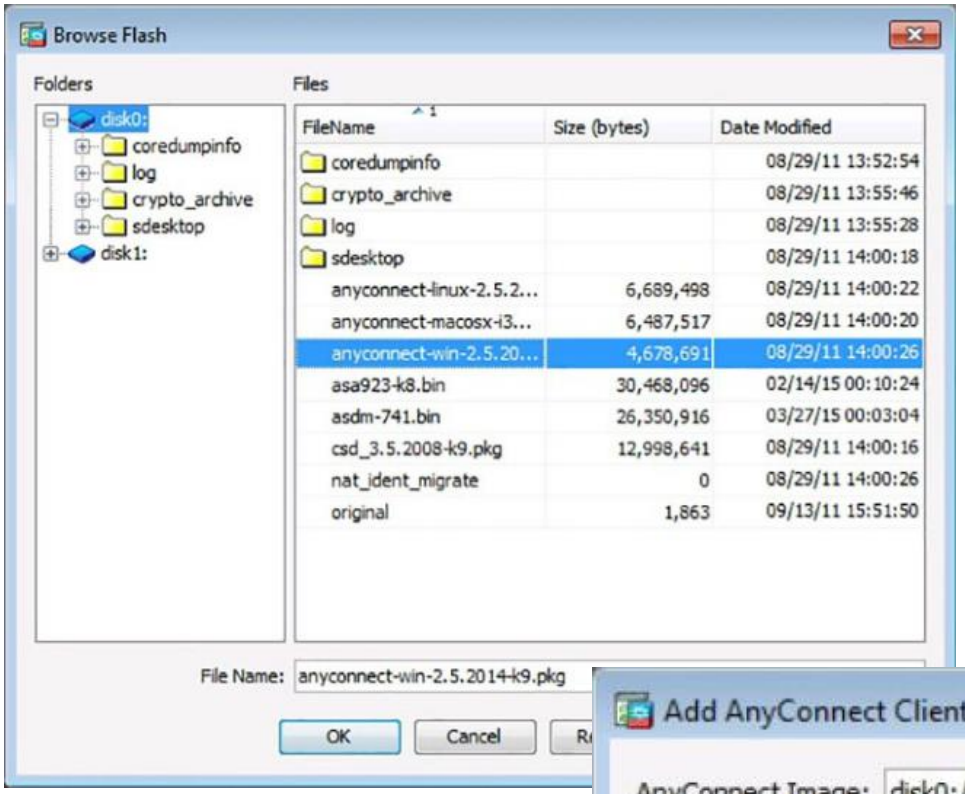



Client Images Window

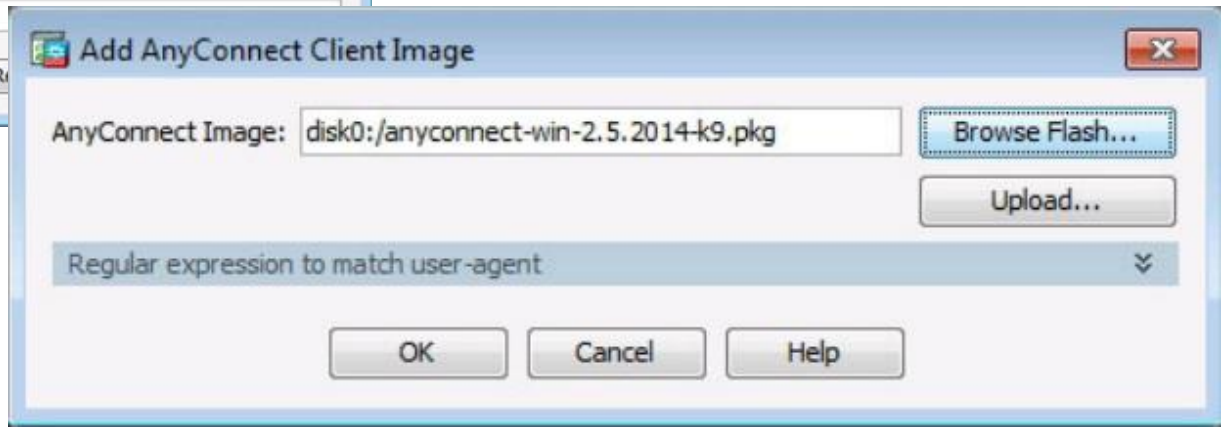



Add AnyConnect Client Image Window

# AnyConnect SSL VPN (Cont.)



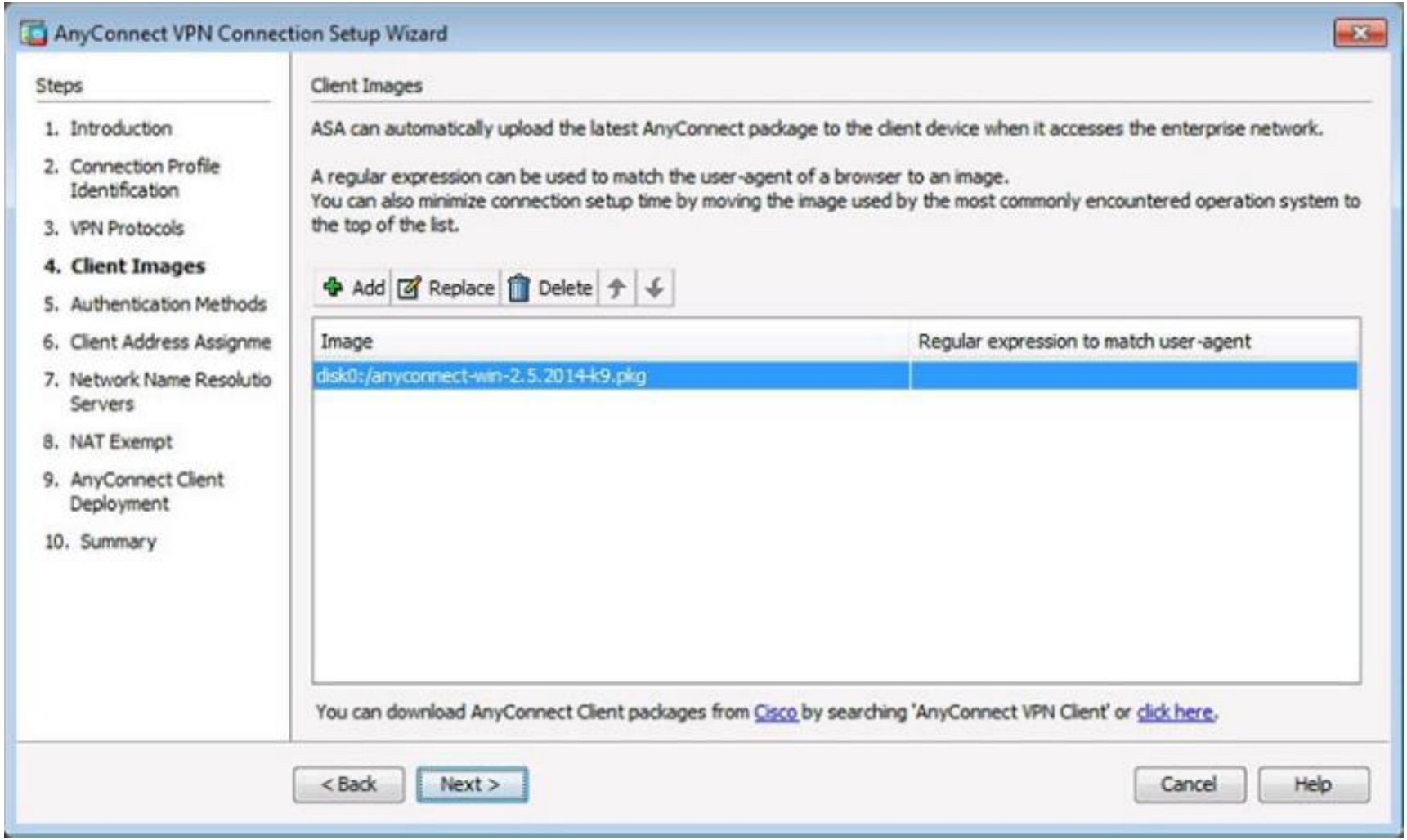

Browse Flash Window




Add AnyConnect Client Image Window

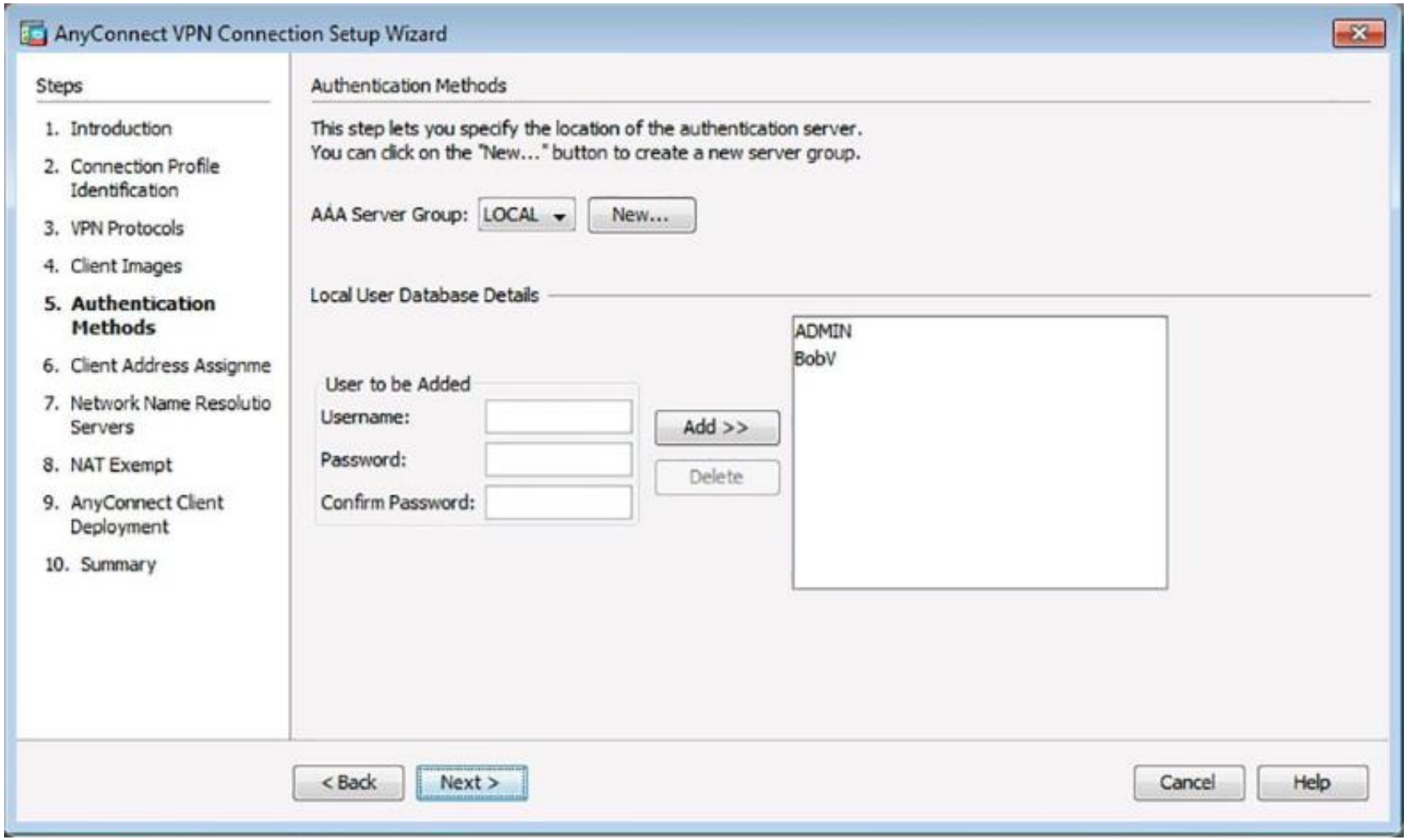
# AnyConnect SSL VPN (Cont.)

Completed Client Images Window

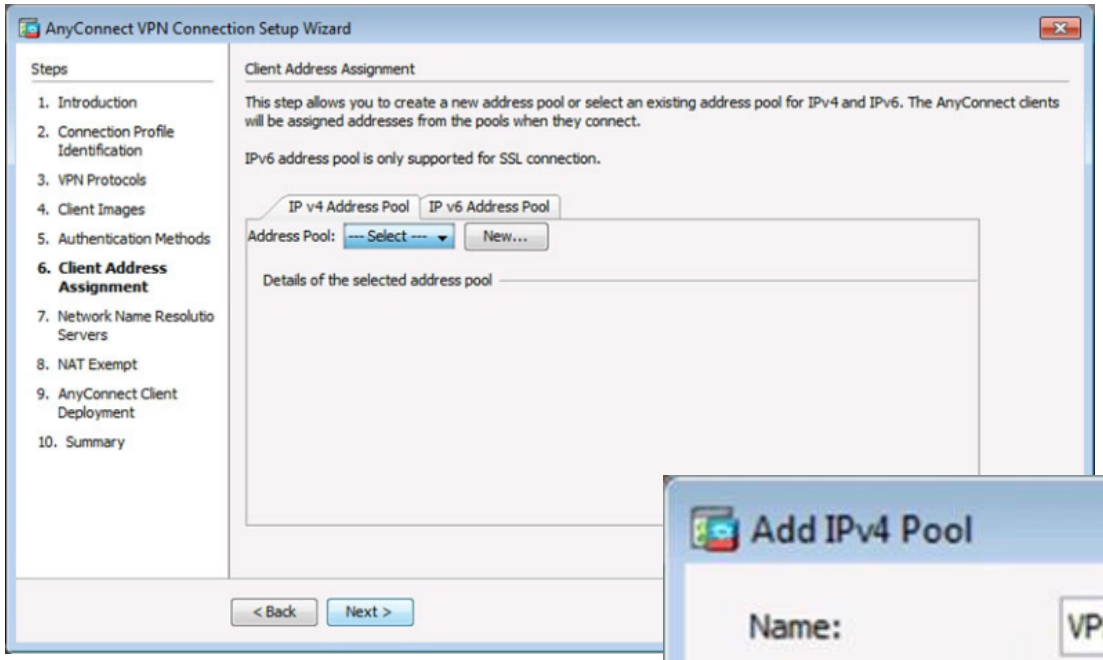


# AnyConnect SSL VPN (Cont.)

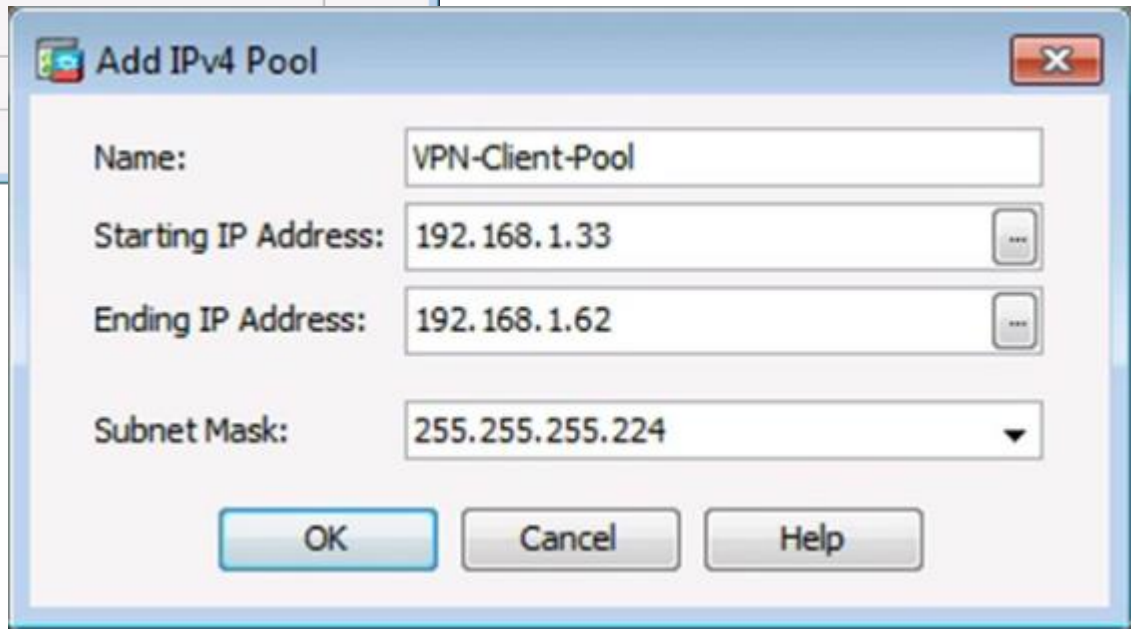
## Authentication Methods Window



# AnyConnect SSL VPN (Cont.)

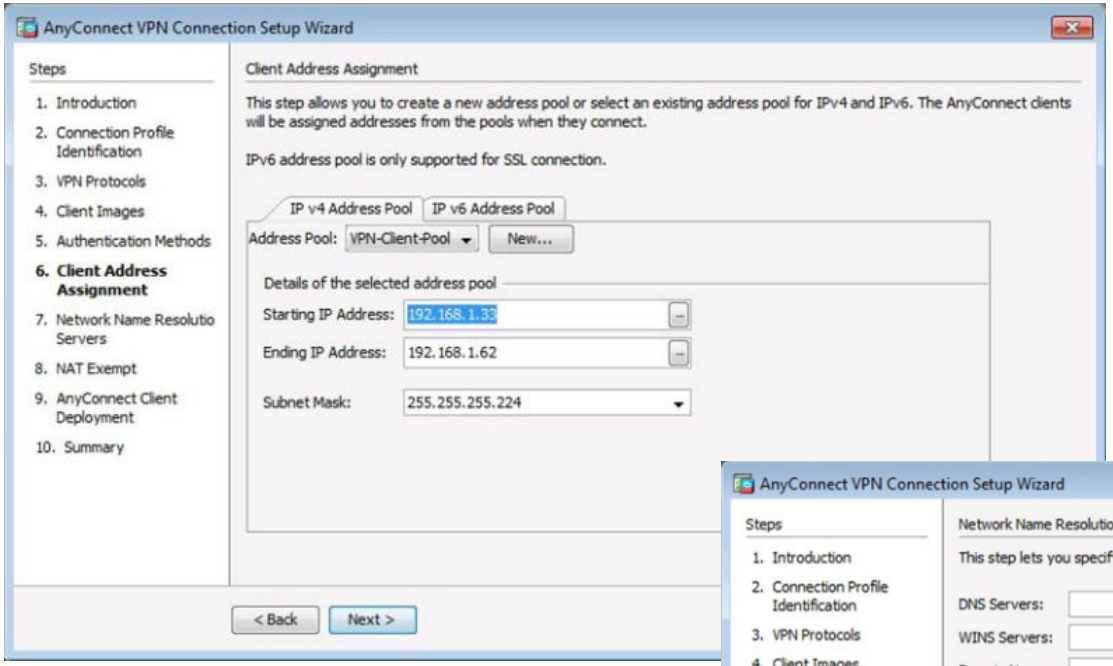



Client Address Management Window

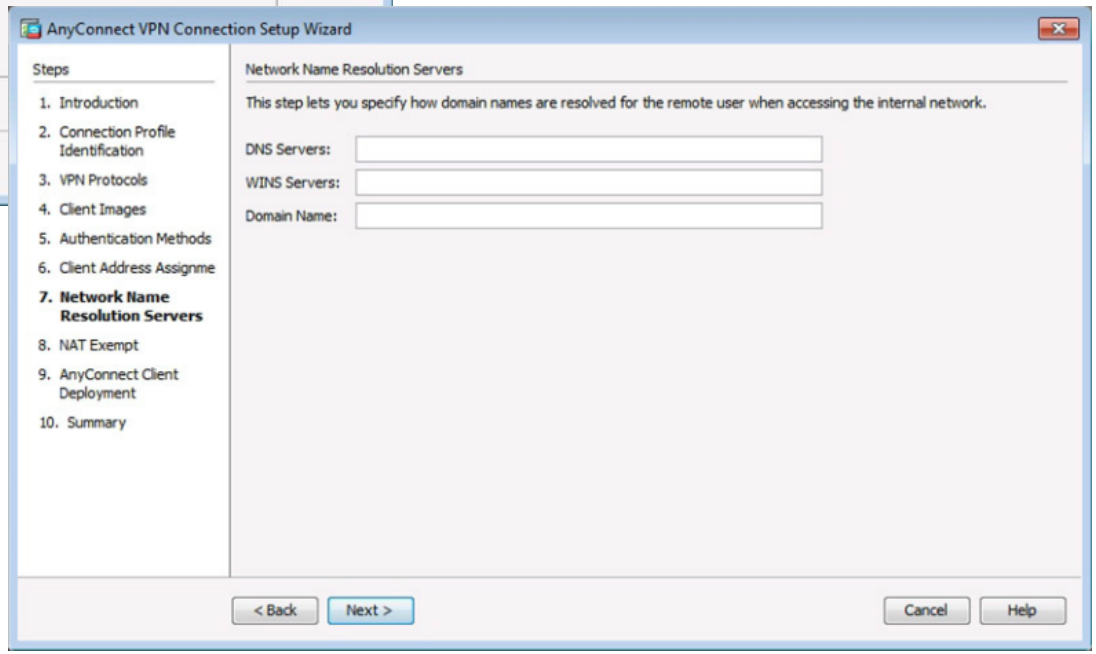



Add IPv4 Window

# AnyConnect SSL VPN (Cont.)



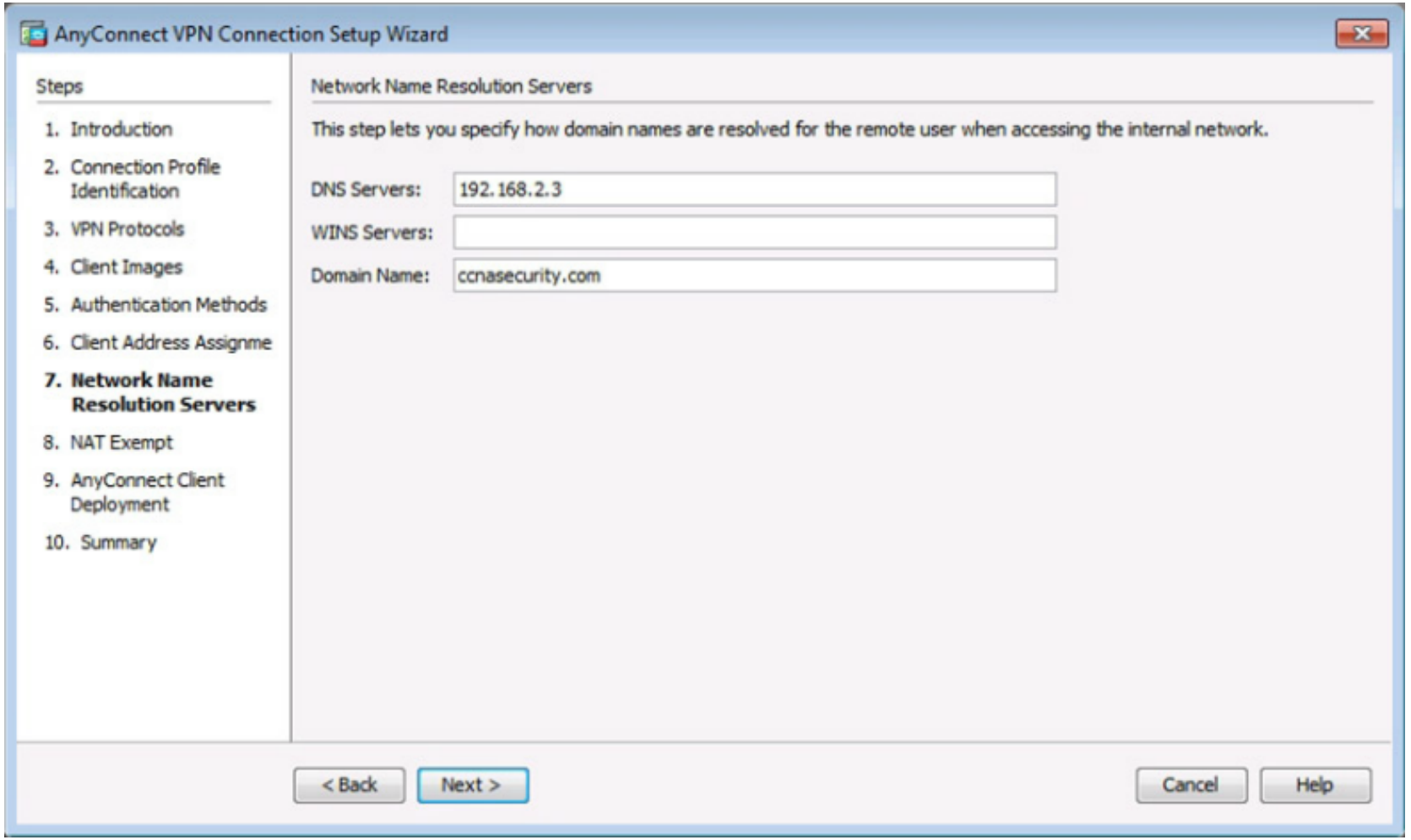

Completed Client Address Management Window



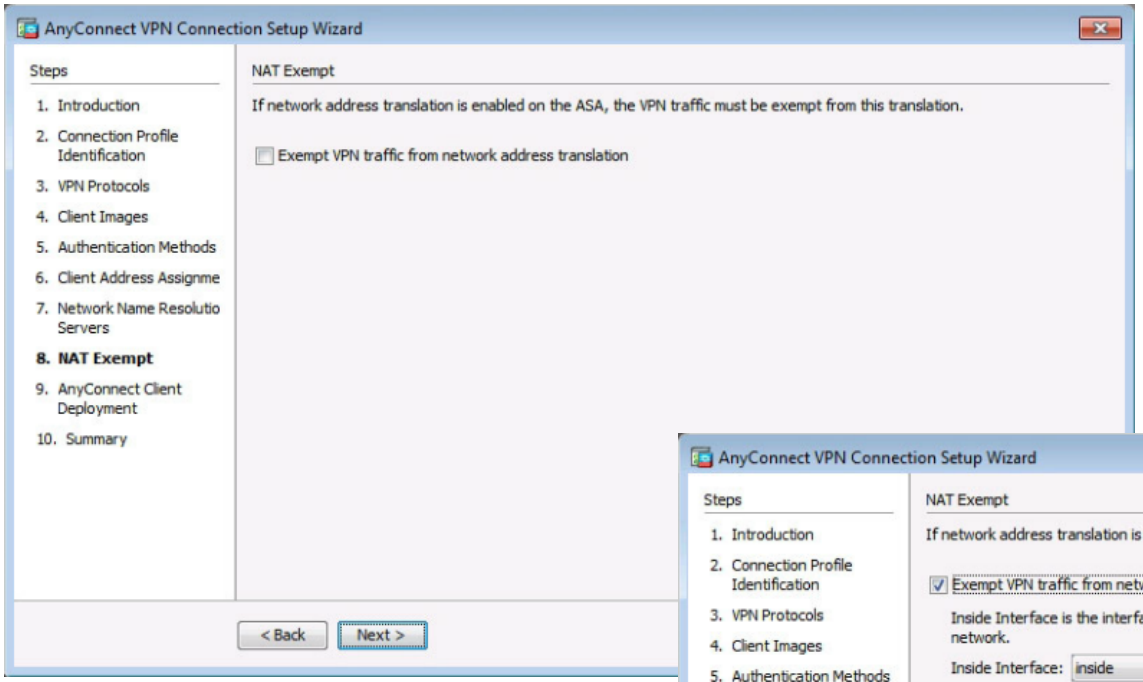

Network Name Resolution Servers Window

# AnyConnect SSL VPN (Cont.)

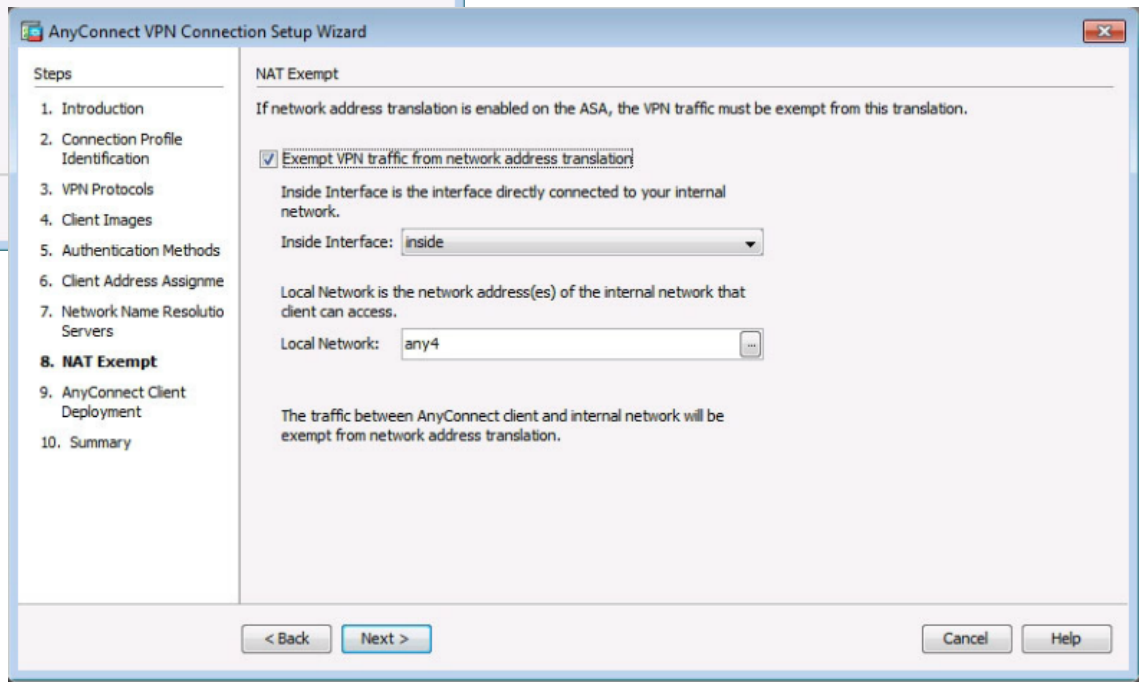
Completed Network Name Resolution Servers Window



# AnyConnect SSL VPN (Cont.)

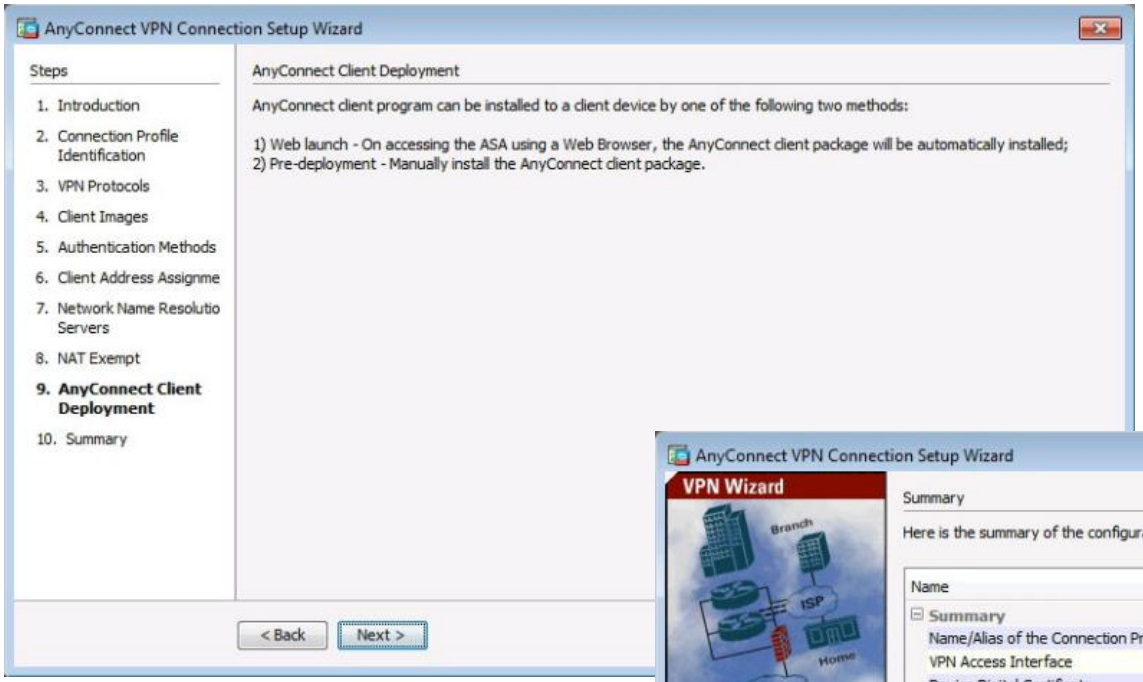



NAT Exempt Window

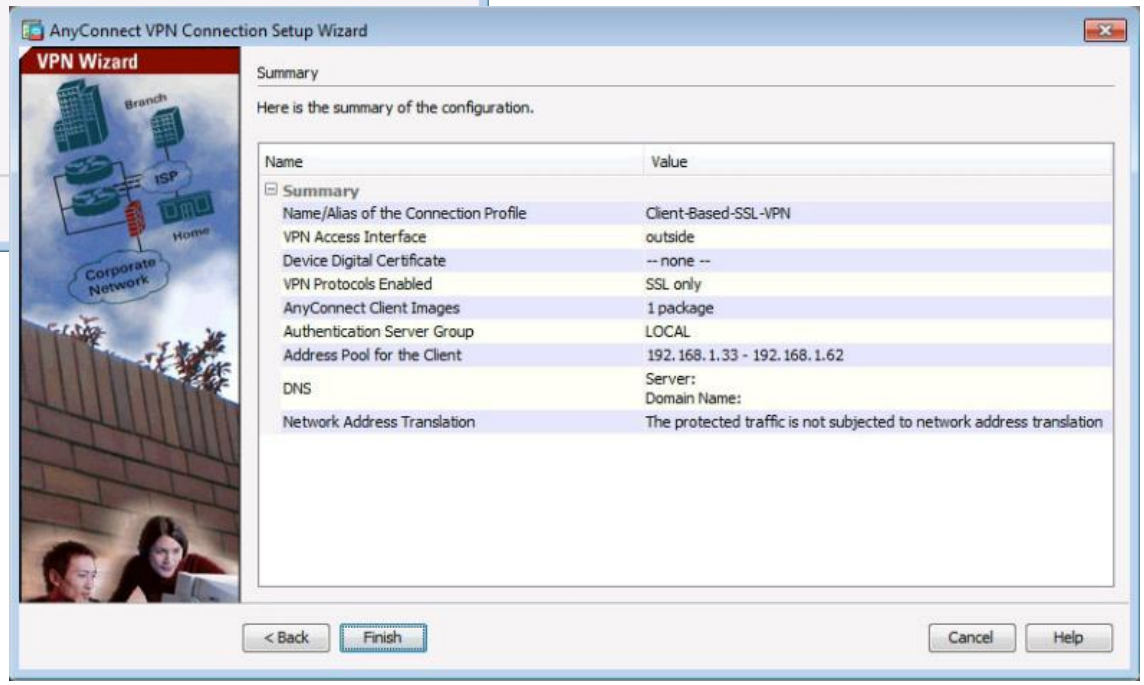



Completed NAT Exempt Window

# AnyConnect SSL VPN (Cont.)



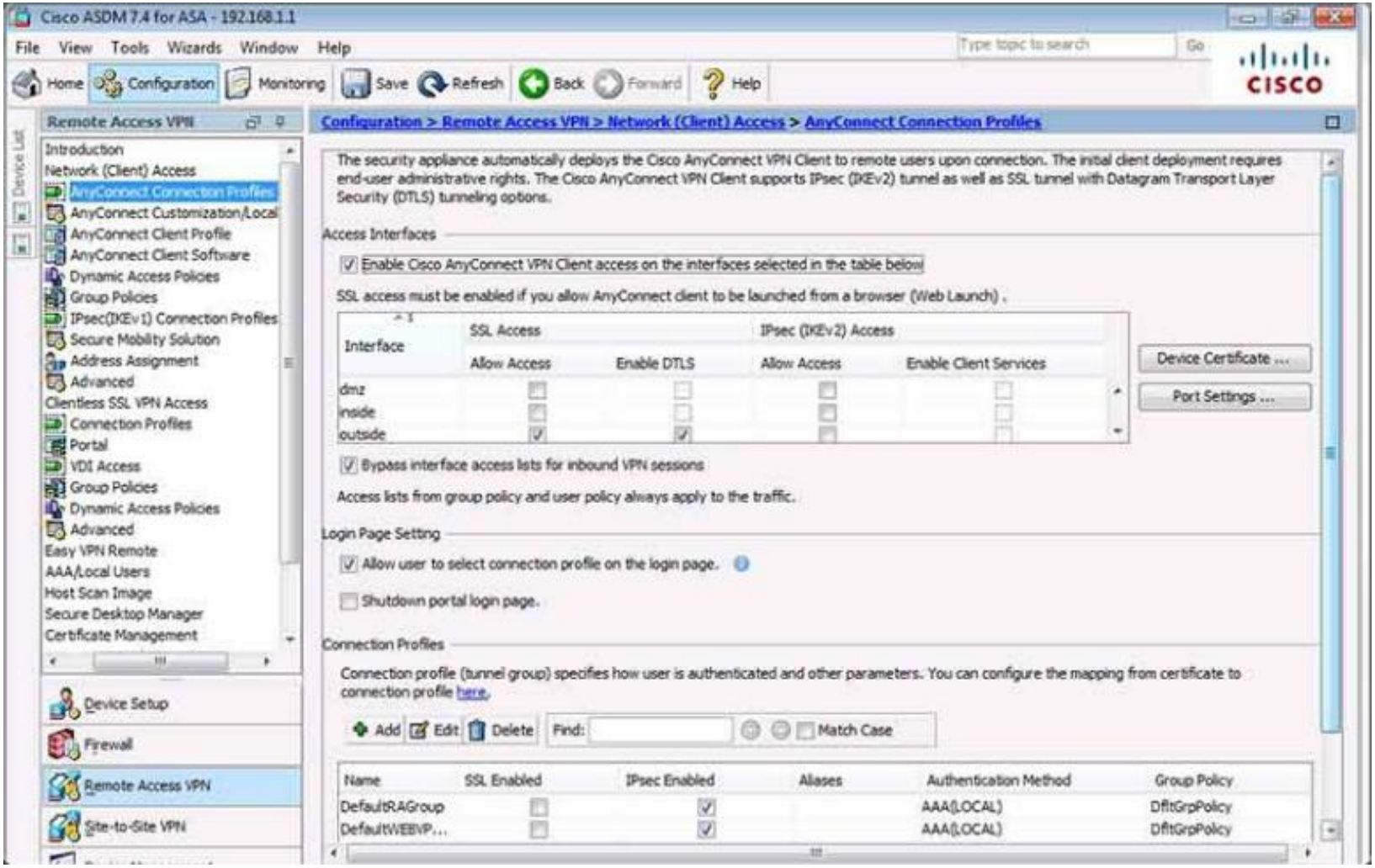

AnyConnect Client Deployment




Summary Window

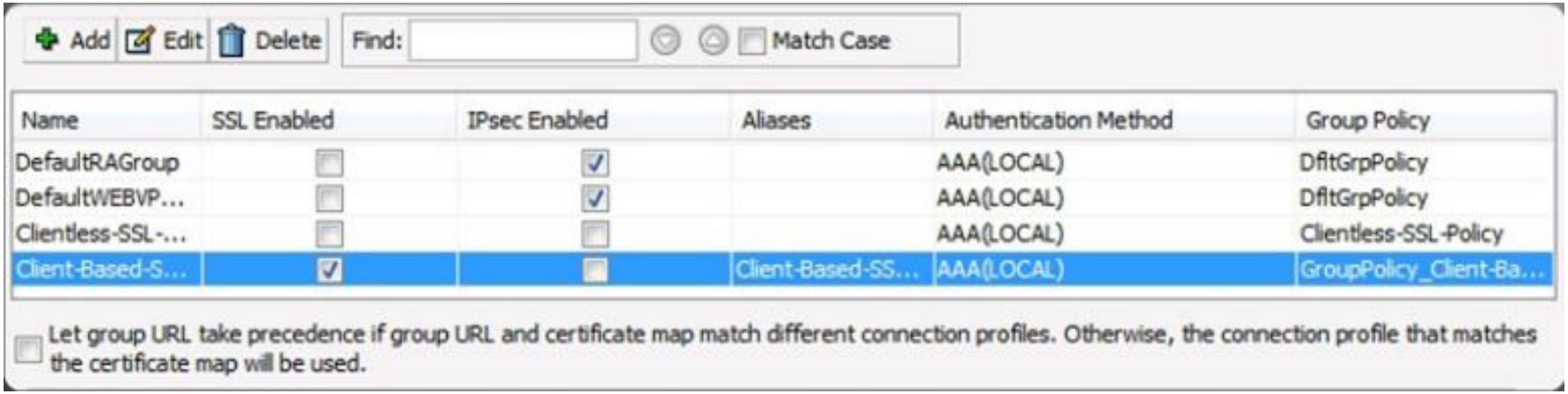
# Verifying AnyConnect Connection

AnyConnect Connection Profiles Page

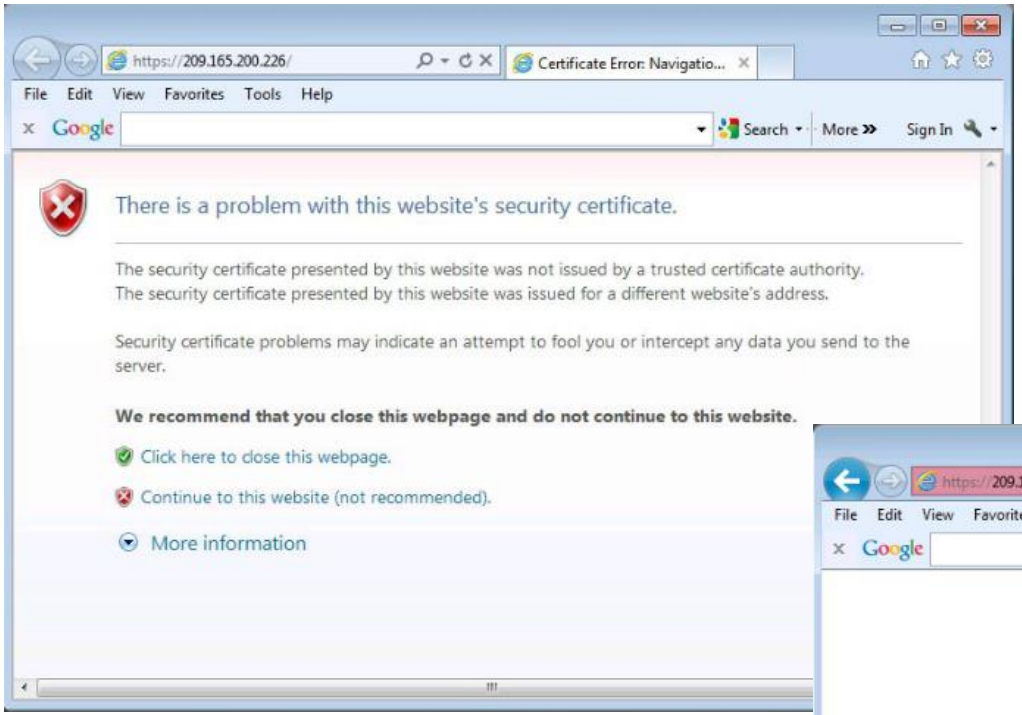


# Verifying AnyConnect Connection (Cont.)

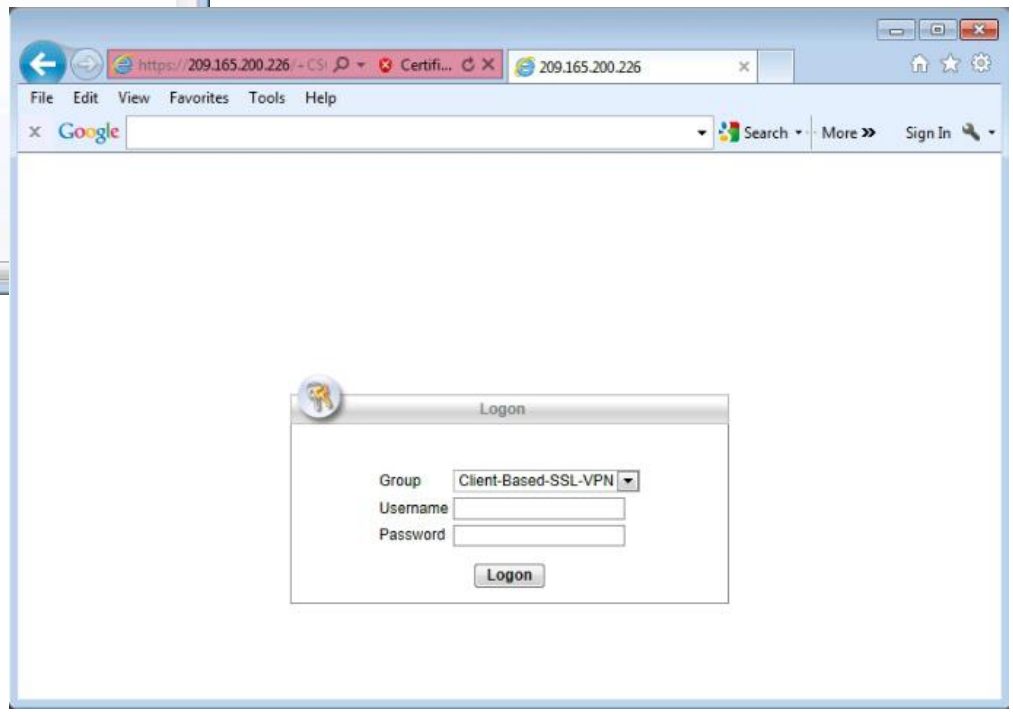
Verifying the Client-Based Configuration



# Install the AnyConnect Client

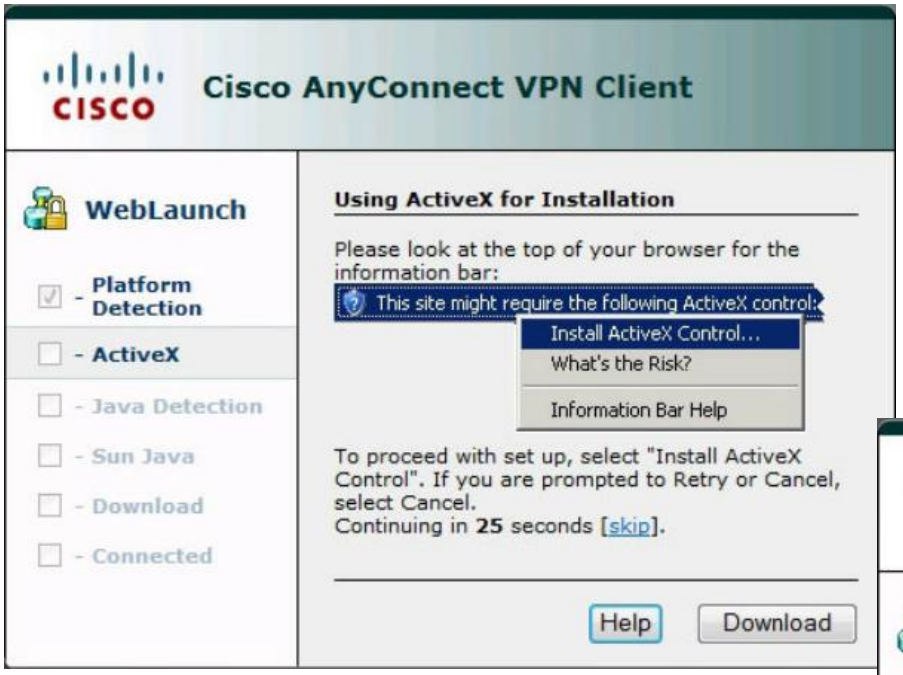



Security Certificate Window

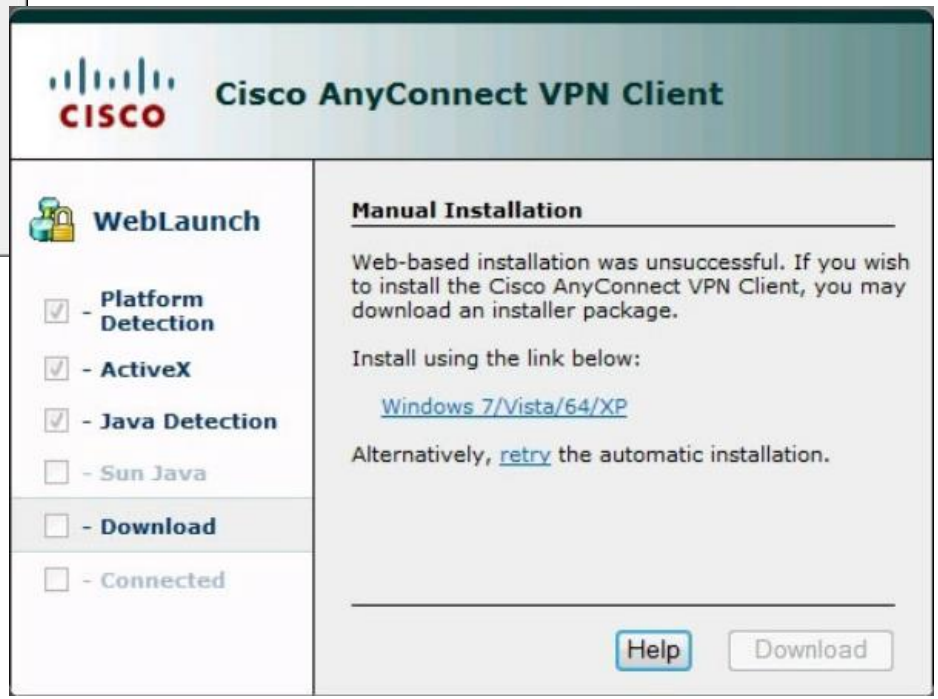



Logon Window

# Install the AnyConnect Client (Cont.)




Cisco AnyConnect VPN Client Window



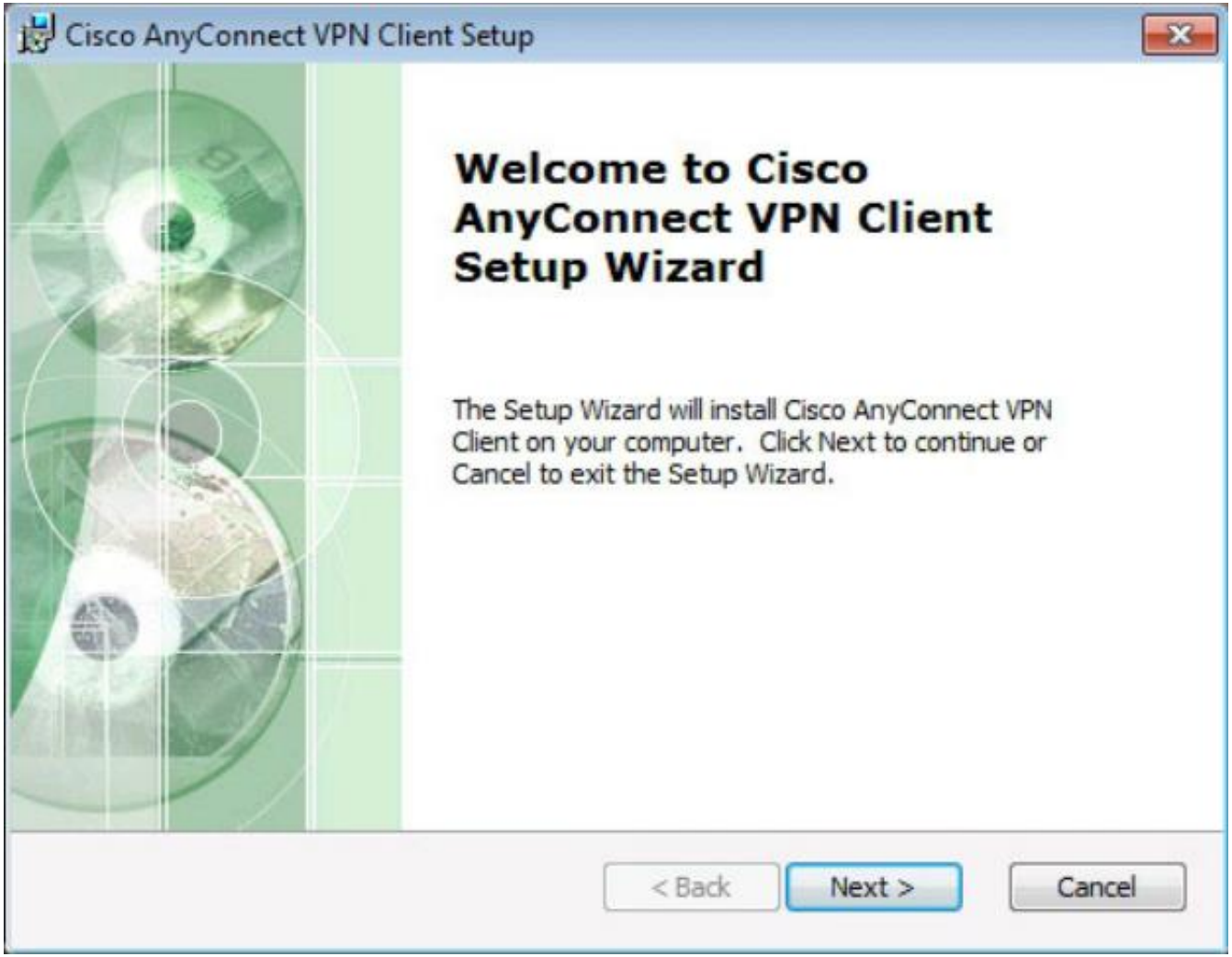

Manual Installation Window

# Install the AnyConnect Client (Cont.)

Run Installer Window

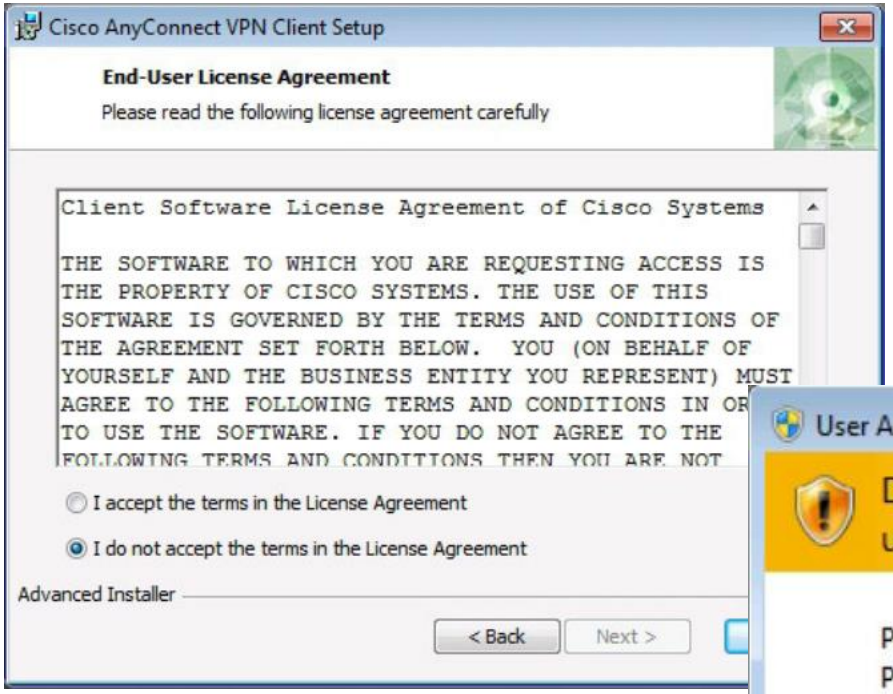
# Install the AnyConnect Client (Cont.)

Cisco AnyConnect VPN Client Setup Window

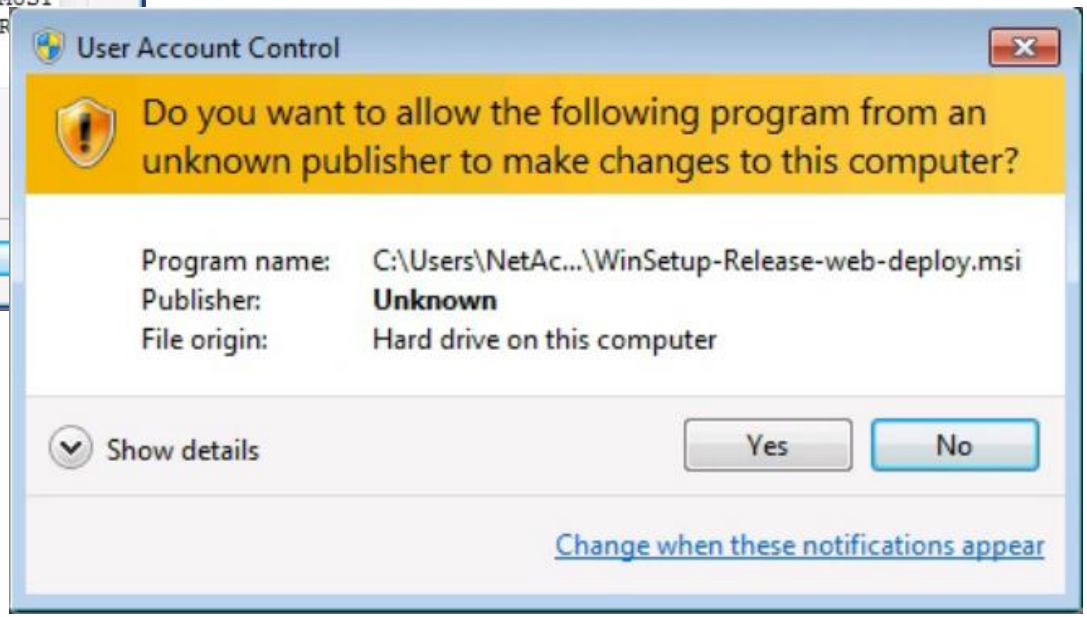


# Install the AnyConnect Client (Cont.)

End-User Agreement Window

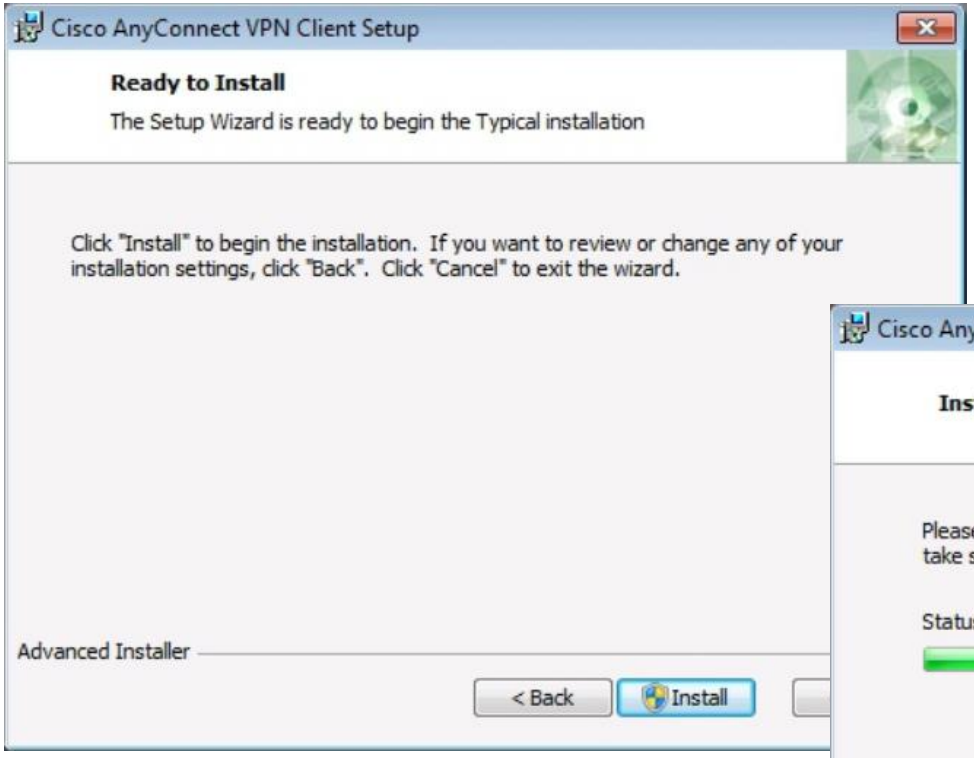



User Account Control Security Window

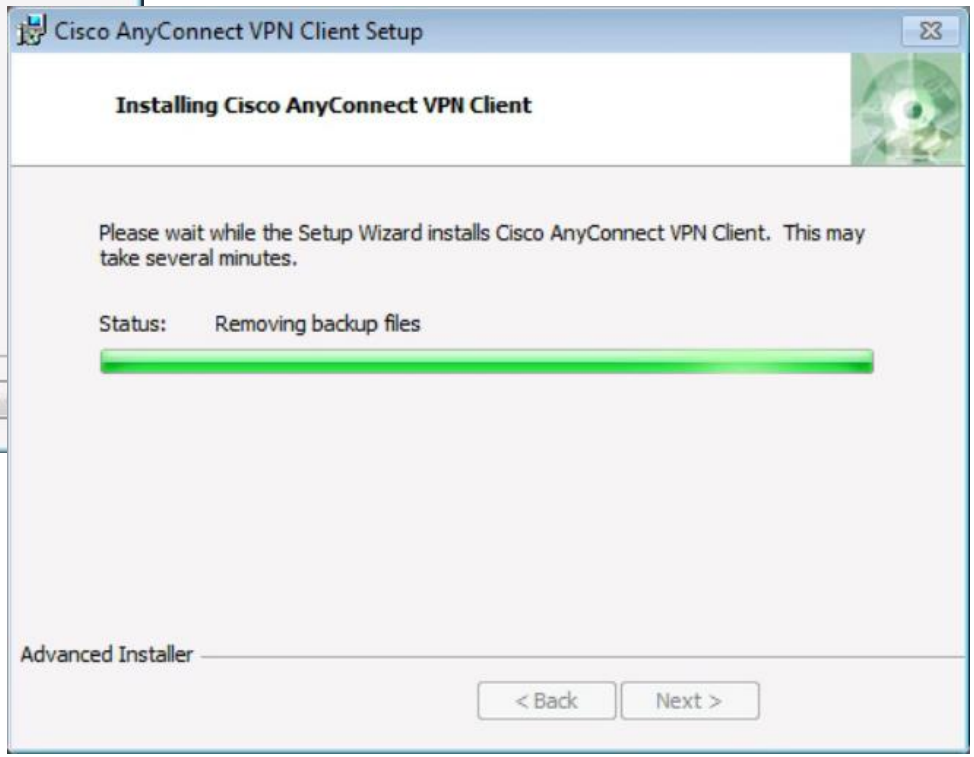


# Install the AnyConnect Client (Cont.)

Ready to Install AnyConnect Client

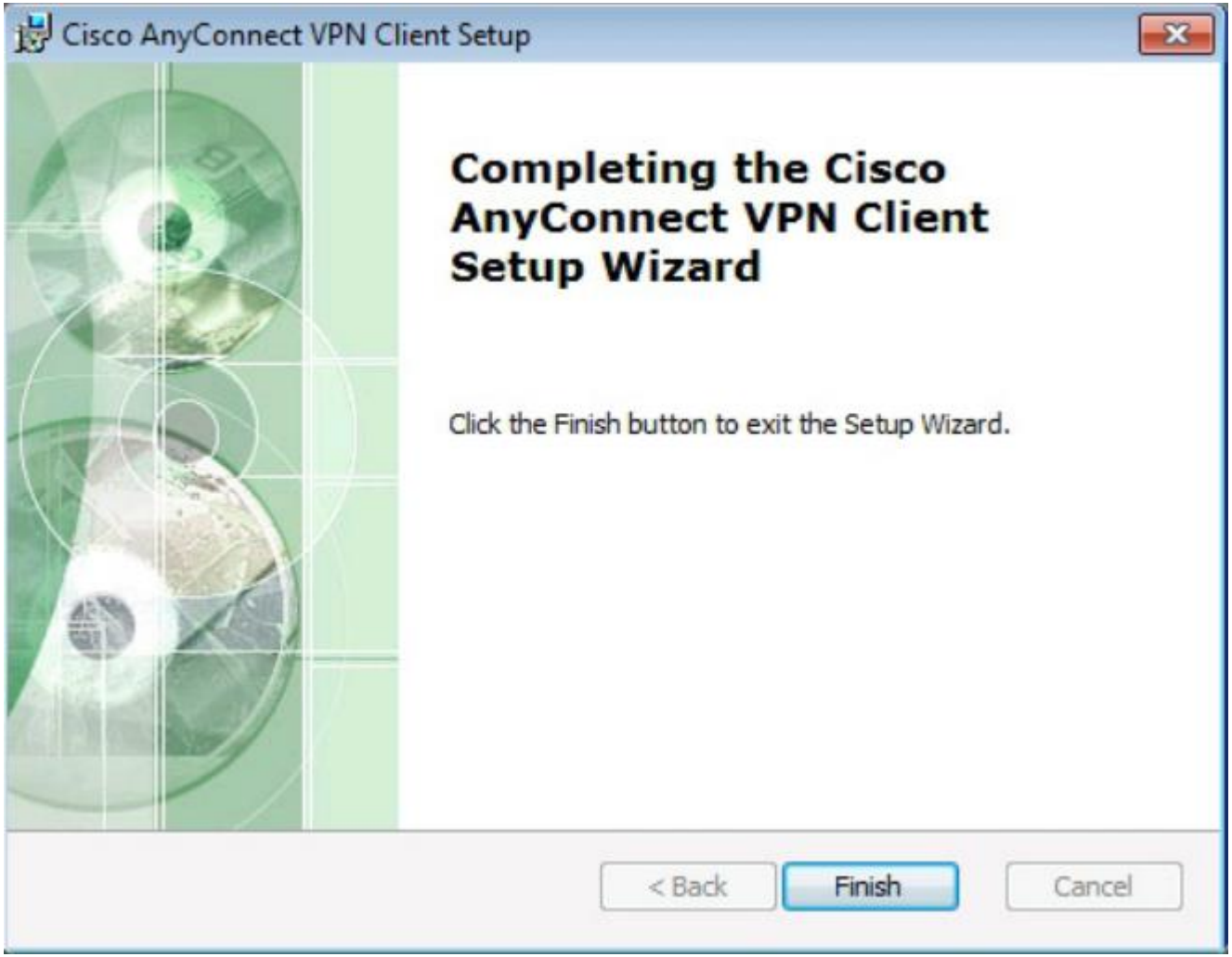



Installing the AnyConnect Client



# Install the AnyConnect Client (Cont.)

Complete Cisco AnyConnect VPN Installation



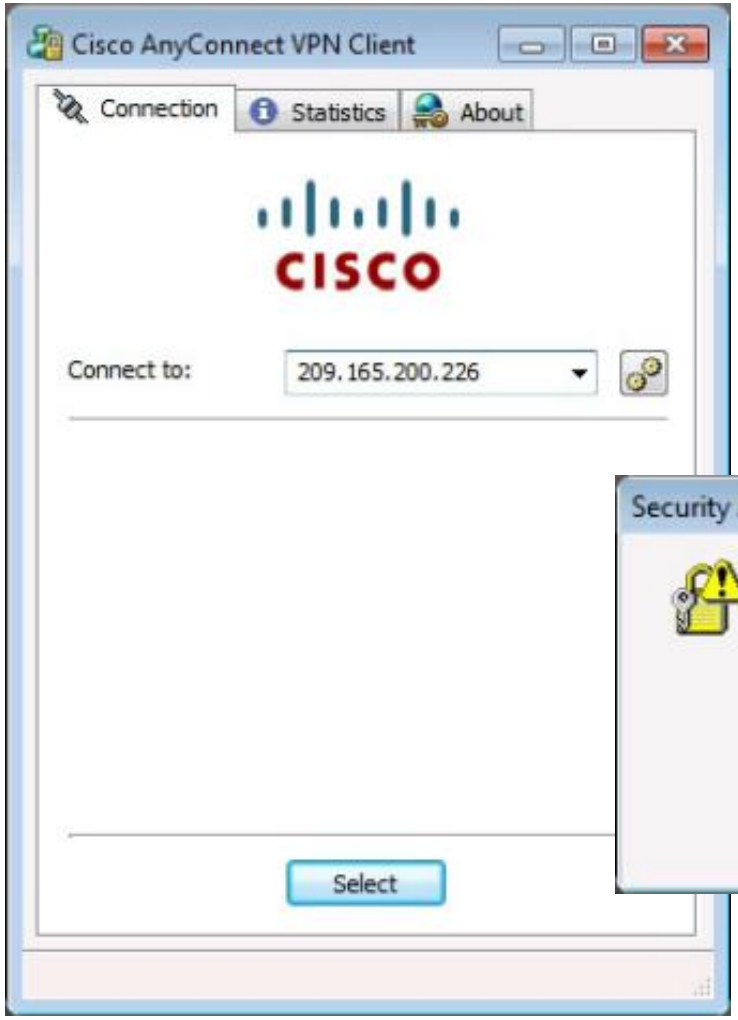
# Install the AnyConnect Client (Cont.)

Start the Cisco AnyConnect VPN 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

```
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>
```

# AnyConnect Wizard Generated Output

- The generated output from the AnyConnect VPN Wizard.

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

# AnyConnect Wizard Generated Output

- NAT configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK OBJ 192.168.1.32 27 NETWORK OBJ 192.168.1.32 27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

# AnyConnect Wizard Generated Output

- WebVPN Configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK OBJ 192.168.1.32 27 NETWORK OBJ 192.168.1.32 27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

# AnyConnect Wizard Generated Output

- Group Policy configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

# AnyConnect Wizard Generated Output

- Tunnel Group configuration

```
CCNAS-ASA(config)# object network NETWORK_OBJ_192.168.1.32_27
CCNAS-ASA(config-network-object)# subnet 192.168.1.32 255.255.255.224
CCNAS-ASA(config-network-object)# ip local pool VPN-Client-Pool 192.168.1.33-1192.168.1.62
mask 255.255.255.224
CCNAS-ASA(config-network-object)# exit
CCNAS-ASA(config)# nat (inside,outside) source static any any destination static
NETWORK_OBJ_192.168.1.32_27 NETWORK_OBJ_192.168.1.32_27 no-proxy-arp route-lookup
CCNAS-ASA(config)# webvpn
CCNAS-ASA(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'outside'.
CCNAS-ASA(config-webvpn)# anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 1
CCNAS-ASA(config-webvpn)# anyconnect enable
CCNAS-ASA(config-webvpn)# tunnel-group-list enable
CCNAS-ASA(config-webvpn)# exit
CCNAS-ASA(config)# group-policy GroupPolicy_AnyConnect-VPN internal
CCNAS-ASA(config-group-policy)# group-policy GroupPolicy_AnyConnect-VPN attributes
CCNAS-ASA(config-group-policy)# wins-server none
CCNAS-ASA(config-group-policy)# dns-server value 192.168.2.3
CCNAS-ASA(config-group-policy)# vpn-tunnel-protocol ssl-client
CCNAS-ASA(config-group-policy)# default-domain value ccnasecurity.com
CCNAS-ASA(config-group-policy)# exit
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN type remote-access
CCNAS-ASA(config)# tunnel-group AnyConnect-VPN general-attributes
CCNAS-ASA(config-tunnel-general)# address-pool VPN-Client-Pool
CCNAS-ASA(config-tunnel-general)# default-group-policy GroupPolicy_AnyConnect-VPN
CCNAS-ASA(config-tunnel-general)# tunnel-group AnyConnect-VPN webvpn-attributes
CCNAS-ASA(config-tunnel-webvpn)#  group-alias AnyConnect-VPN enable
```

# Multimode

# Config

## Configuring Multiple Mode

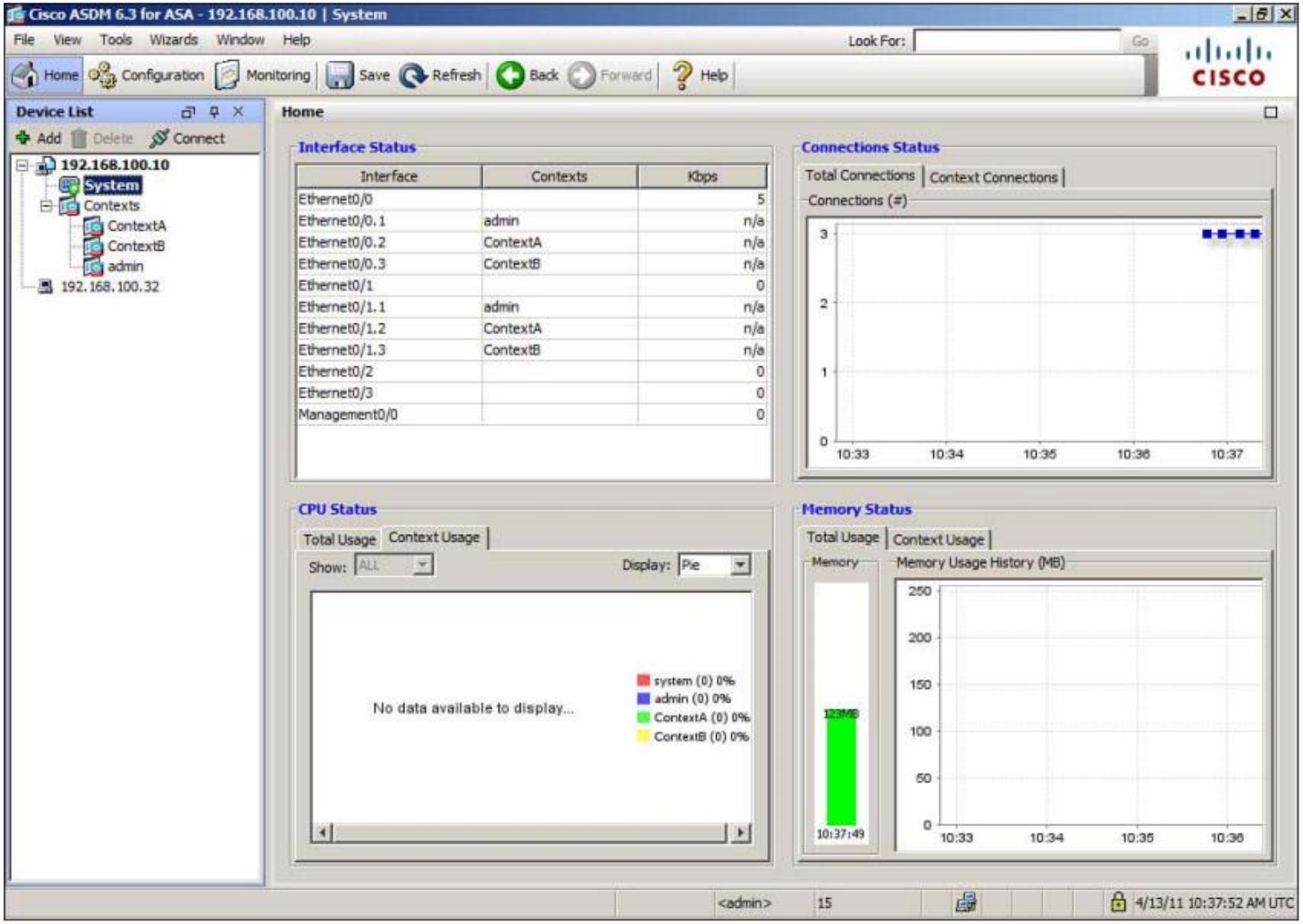
The switch to multiple mode is one of those unique configurations on the Cisco ASA that can be accomplished only by using the command-line interface (CLI). Use the **mode** command in global configuration mode. There is a **noconfirm** keyword option that makes the change without a confirmation request. This option is useful for automating the process with a script.

Here is an example of using the command:

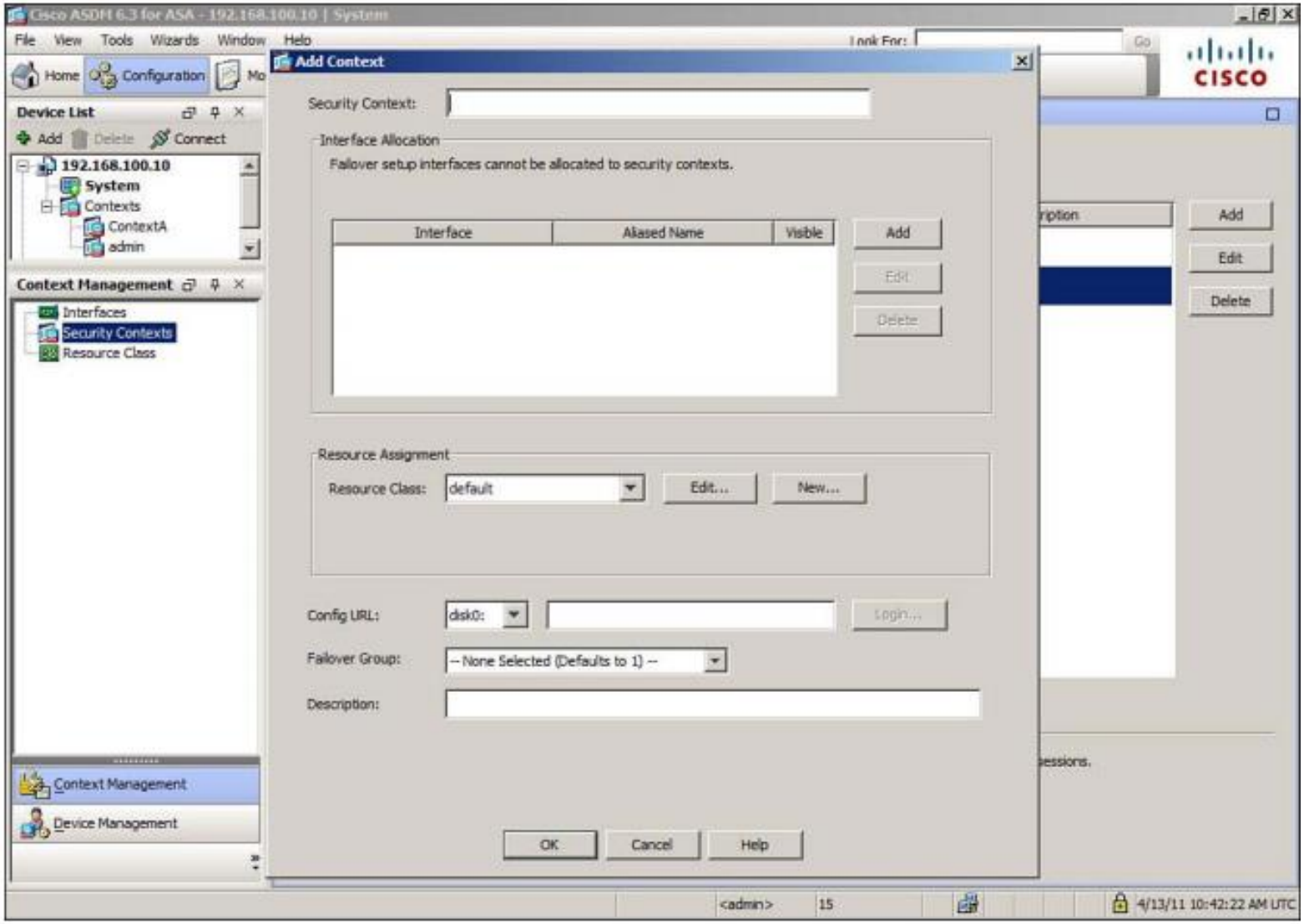
```
ciscoasa(config)# mode multiple noconfirm
```

**Note:** This change requires a reboot of the Cisco ASA.

# Contexts Overview



# Create Context



# Verifying

```
CiscoASA# show context
Context Name          Interfaces                          URL
*admin                GigabitEthernet0/1.100              disk0:/admin.cfg
                      GigabitEthernet0/1.101
contexta              GigabitEthernet0/1.200              disk0:/contexta.cfg
                      GigabitEthernet0/1.201
contextb              GigabitEthernet0/1.300              disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

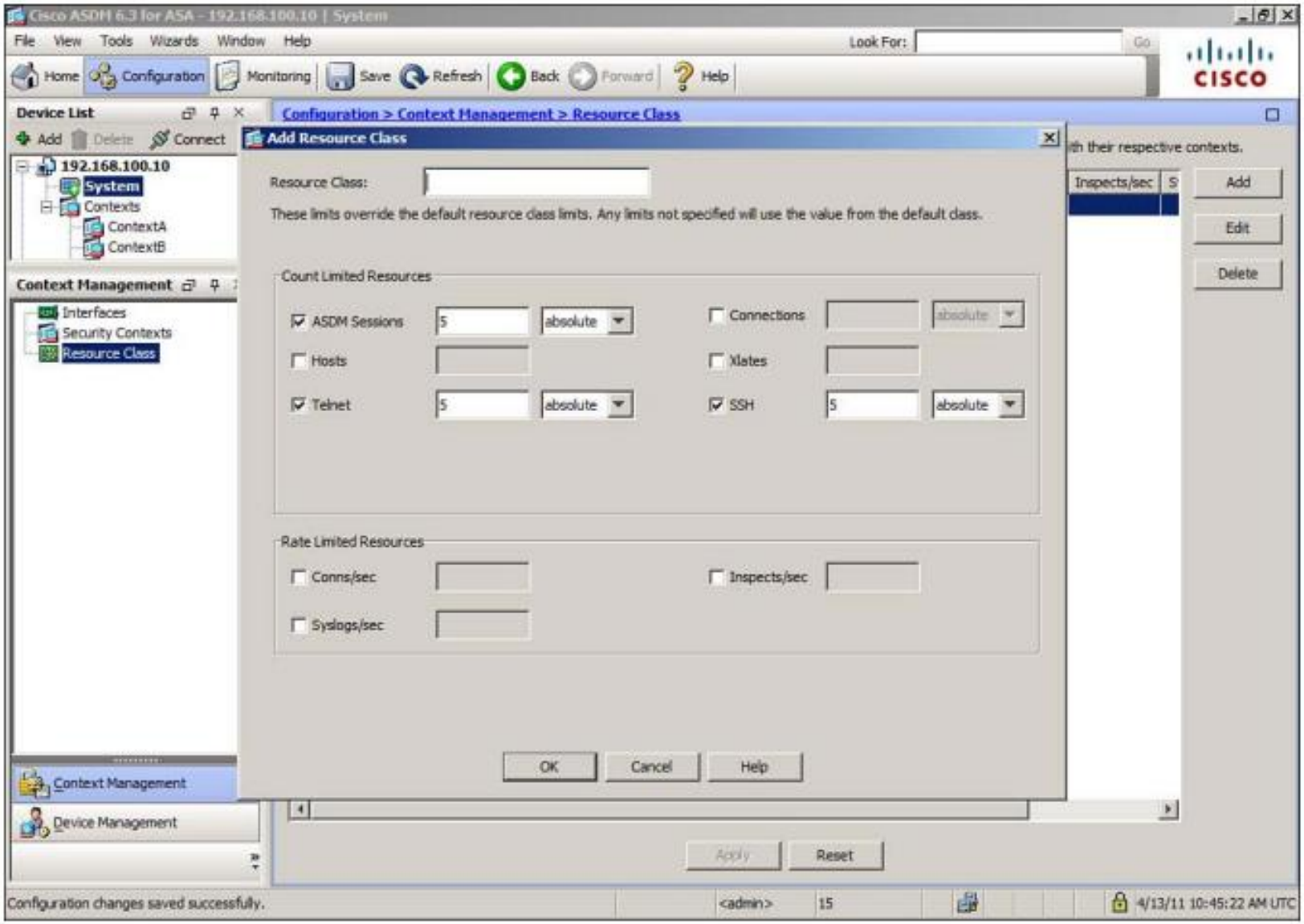
To change between contexts using the CLI, use the **changeto** command in privileged mode. For example:

```
ciscoasa# changeto MYCONTEXT
```

or

```
ciscoasa# changeto system
```

# Managing Resources



# Managing Resources

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
! And then later to make the context a member of the class:
hostname(config-ctx)# member gold
```

# Failover

# Types

- **Active-standby:** One ASA takes on the active role, handling all the normal security functions. The other ASA stays in standby mode, ready to take over the active role in the event of a failure. The active-standby failover mode provides device redundancy.
- **Active-active:** When the ASAs are running multiple security contexts, the contexts can be organized into groups. One ASA is active for one group of contexts, and the other ASA is active for another group. In effect, both ASAs are actively involved in providing security functions, but not in the same security context simultaneously. The active-active failover mode provides both device redundancy and load balancing across contexts.

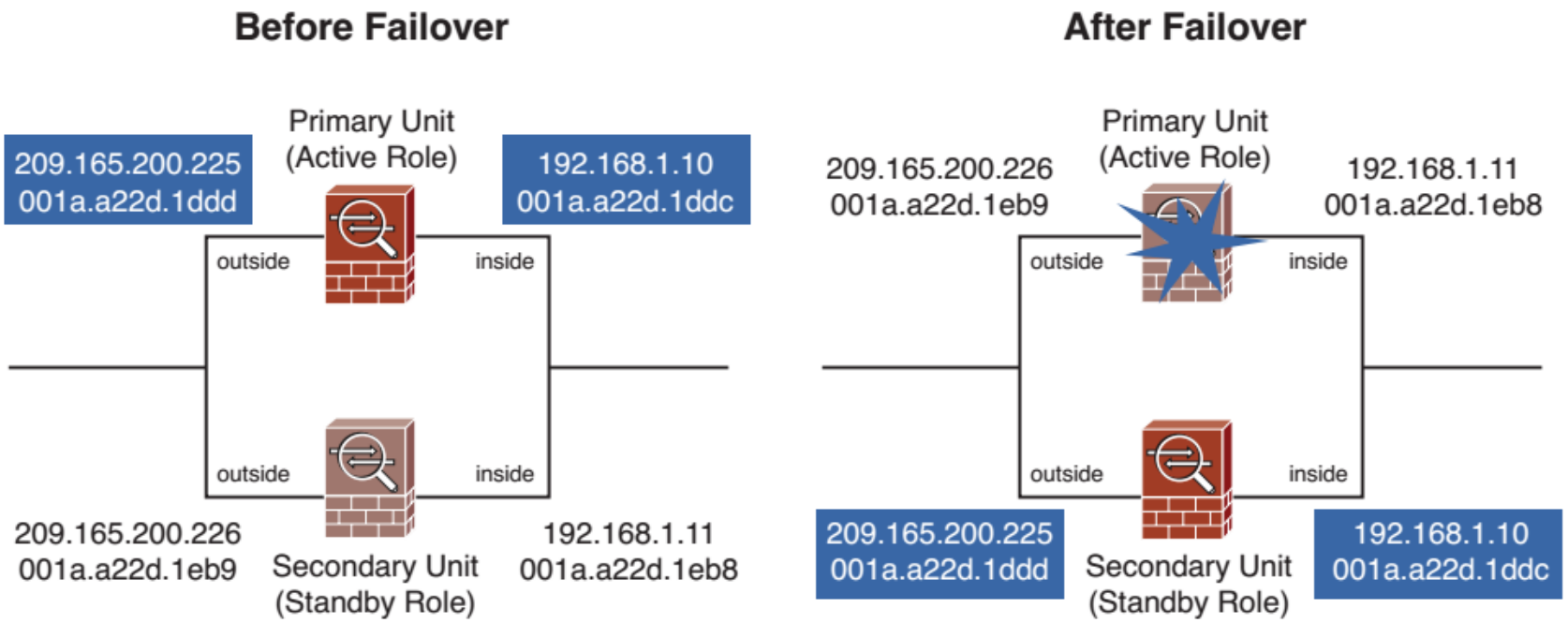
| Failover Group | Primary ASA | Secondary ASA |
|---|---|---|
| 1 | Active role | Standby role |
| 2 | Standby role | Active role |

# Conditions

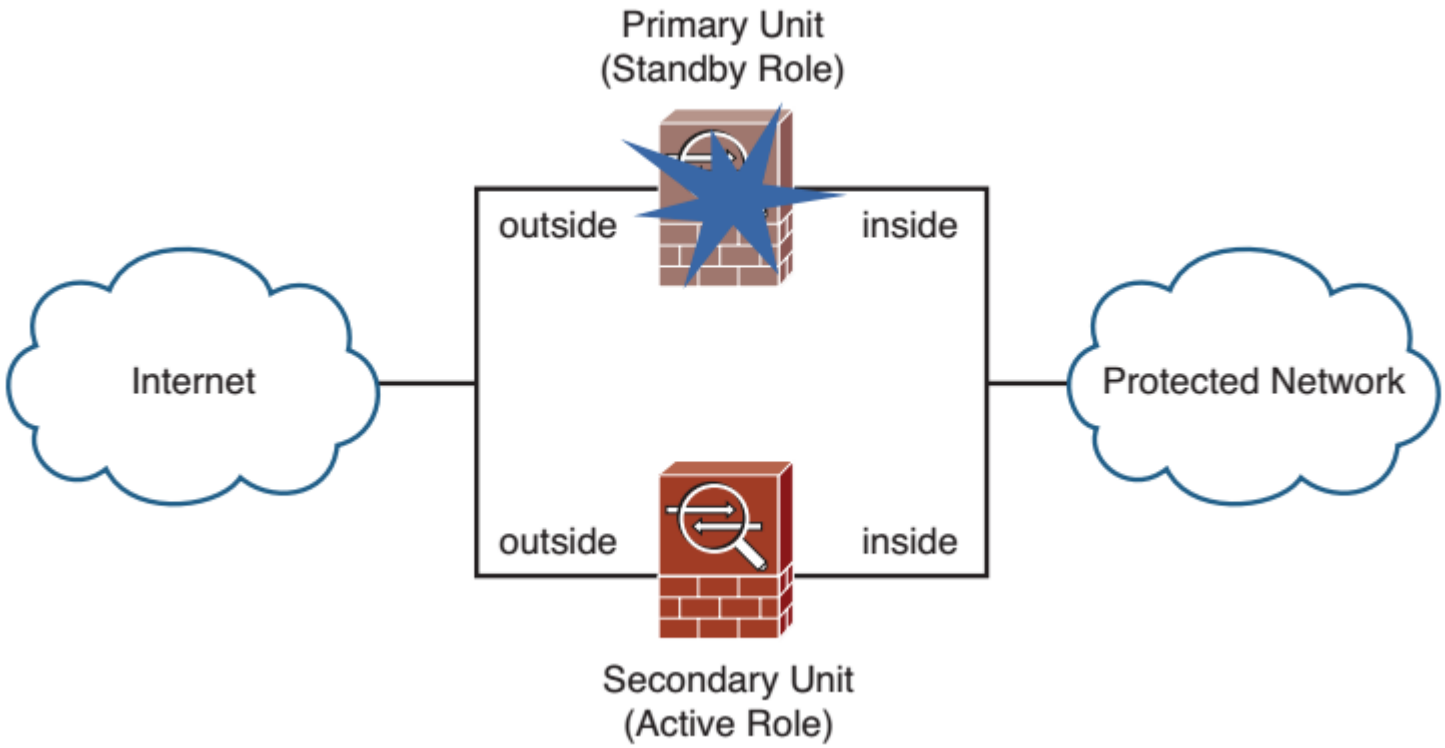
Notice that the ASA pair must share identical sets of interfaces. For example, each unit has an inside and an outside interface, and the similar interfaces must be connected together. This is for two reasons:

- The standby unit must be ready to take over handling traffic at any time, so its interfaces must be connected and ready to use.
- The two ASAs monitor each other's health by communicating over each of their interfaces.

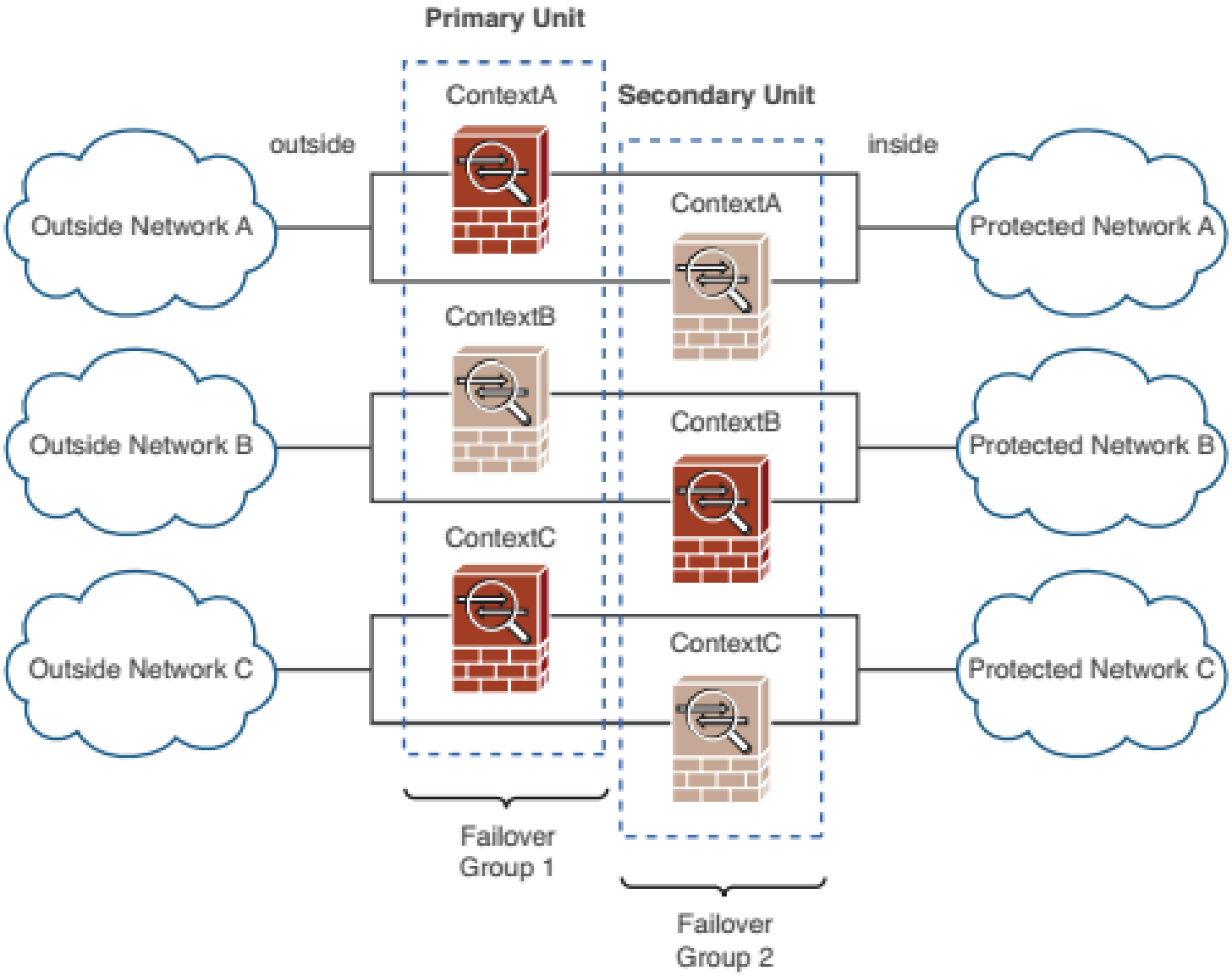
# MAC and IP


Before Failover
Primary Unit
(Active Role)
209.165.200.225
001a.a22d.1ddd
192.168.1.10
001a.a22d.1ddc
outside
inside
outside
inside
209.165.200.226
001a.a22d.1eb9
Secondary Unit
(Standby Role)
192.168.1.11
001a.a22d.1eb8
After Failover
Primary Unit
(Active Role)
209.165.200.226
001a.a22d.1eb9
192.168.1.11
001a.a22d.1eb8
outside
inside
outside
inside
209.165.200.225
001a.a22d.1ddd
Secondary Unit
(Standby Role)
192.168.1.10
001a.a22d.1ddc

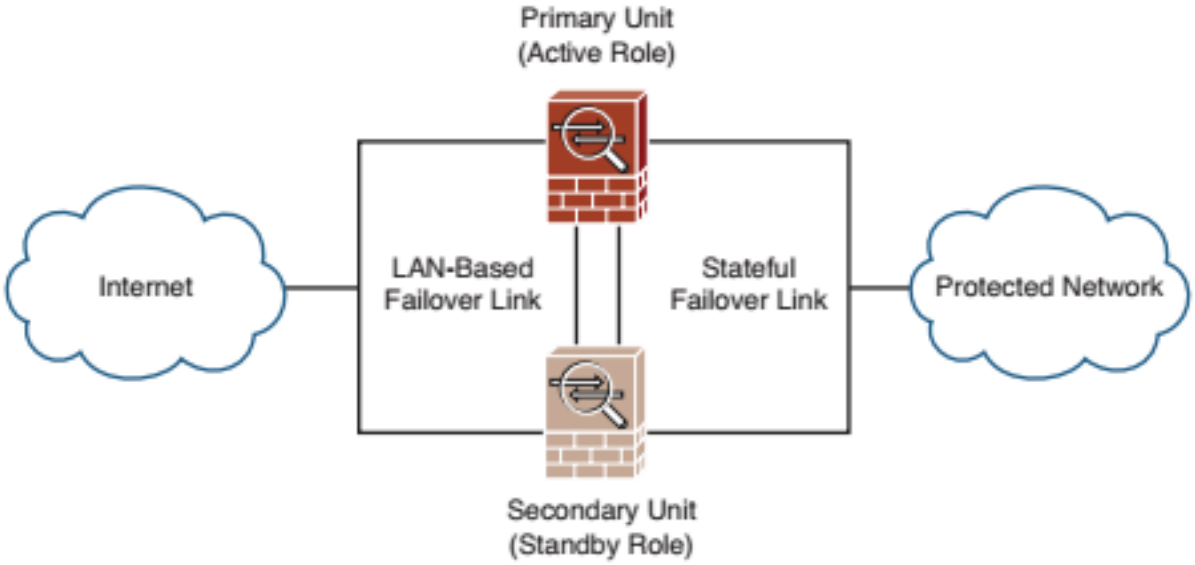
# Example Active-Standby



# Example Active-Active



# Links




| State Information Replicated | State Information Not Replicated |
|---|---|
| NAT table entries | User authentication Cut-through Proxy |
| ARP table entries | DHCP server address leases |
| MAC address table entries | Phone proxy information |
| UDP connections | Security Services Module activity |
| TCP connections | |
| H.323 and SIP signaling sessions | |
| MGCP connections | |
| HTTP connections (if explicitly enabled) | |

# Health Monitoring

An ASA monitors the health of its peer according to the following rules:

- As long as hellos are received over the LAN failover interface, the peer must be alive and no failover occurs.
- If hellos are not received over the LAN failover interface, but hellos are received on other monitored interfaces, the peer must be alive and no failover occurs. Only the LAN failover interface is declared to be "failed" and should be repaired as soon as possible.
- If no hellos are received on any interface for a hold time interval, the peer is declared to be "failed" and failover occurs.

By default, hello packets are sent over the LAN failover interface every 1 second. The default hold timer is 15 seconds. You can shorten the failover unit poll (hello) and hold timers so that a failure is detected sooner, if desired. The failover timers are covered in more detail in the section, "Tuning Failover Operation."

Each interface of one ASA must connect to the same network as the corresponding interface of the peer ASA. Hello packets are also sent on all interfaces that are configured to be monitored for failover, so that an ASA can determine the health of each interface on its peer.

# Interface Testing

Interfaces in the "testing" mode are moved through the following sequence of tests:

1. **Interface status:** The interface is failed if the link status is down.
2. **Network activity:** If no packets are received over a 5-second interval, the next testing phase begins; otherwise, the interface can still be used.
3. **ARP:** The interface stimulates received traffic by sending ARP requests for the ten newest entries in the ASA's ARP table. If no traffic is received in 5 seconds, the next testing phase begins.
4. **Broadcast ping:** Traffic is stimulated by sending an ICMP echo request to the broadcast address on the interface. If no replies are received over a 5-second interval, the interface is marked in a "failed" state; however, if the same interface on the peer ASA also fails the test, then the interface is marked in an "unknown" state because an actual failure cannot be determined.

At the conclusion of the tests, the two ASAs attempt to compare their status. If the active unit has more failed interfaces than a configured threshold, a failover occurs.

Once a monitored interface is marked as "failed," it will become operational again as soon as any traffic is received on it.

# Configuration: A-S

```
ciscoasa(config)# failover lan unit primary
ciscoasa(config)# failover lan interface LANfo Ethernet0/2
ciscoasa(config)# failover interface ip LANfo 192.168.200.1 255.255.255.0 standby
  192.168.200.2
ciscoasa(config)# failover key B1gs3cr3tk3y
ciscoasa(config)# failover
!
ciscoasa(config)# failover link stateful Ethernet0/3
ciscoasa(config)# failover interface ip stateful 192.168.201.1 255.255.255.0
  standby 192.168.201.2
ciscoasa(config)# failover replication http
!
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 209.165.200.226 255.255.255.0 standby
  209.165.200.227
ciscoasa(config-if)# exit
!
ciscoasa(config)# interface Ethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.1.10 255.255.255.0 standby 192.168.1.11
ciscoasa(config-if)# exit
ciscoasa(config)# failover mac address inside 001a.a22d.1ddd 001a.a22d.1eb9
ciscoasa(config)# failover mac address outside 001a.a22d.1ddc 001a.a22d.1eb8
ciscoasa(config)# no monitor-interface management0/0
```

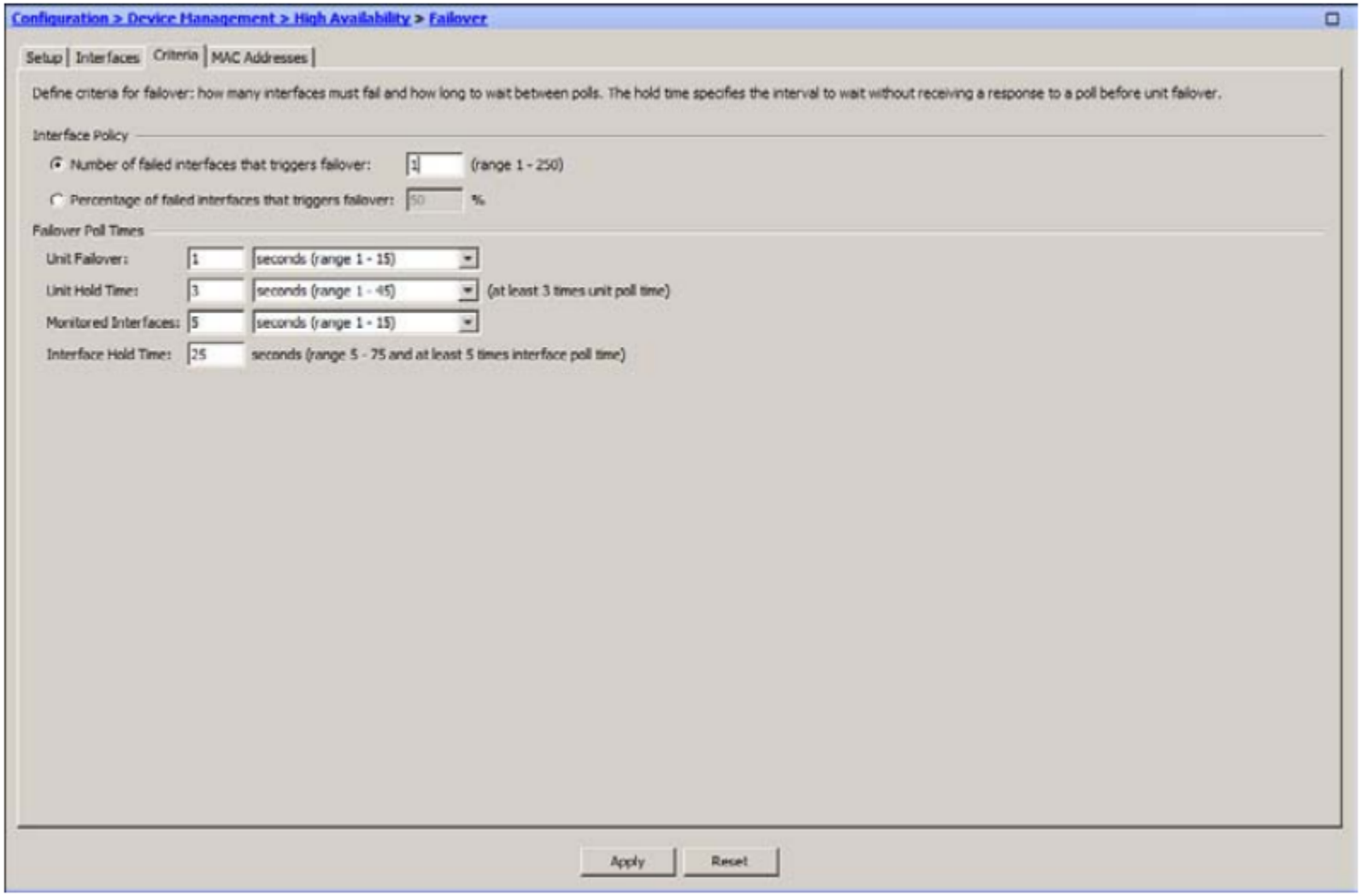
# Configuration: A-S

```
ciscoasa(config)# failover lan unit secondary
ciscoasa(config)# failover lan interface LANfo Ethernet0/2
ciscoasa(config)# failover interface ip LANfo 192.168.200.1 255.255.255.0 standby
  192.168.200.2
ciscoasa(config)# failover key B1gs3cr3tk3y
ciscoasa(config)# failover
```

# Configuration: A-A

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)#  preempt
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface Ethernet0/0.1
ciscoasa(config-ctx)# allocate-interface Ethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg
ciscoasa(config-ctx)# join-failover-group 1
ciscoasa(config-ctx)# exit
!
ciscoasa(config)# context ContextA
ciscoasa(config-ctx)# allocate-interface Ethernet0/0.2
ciscoasa(config-ctx)#  allocate-interface Ethernet0/1.2
ciscoasa(config-ctx)# config-url disk0:/contexta.cfg
ciscoasa(config-ctx)# join-failover-group 2
ciscoasa(config-ctx)# exit
!
ciscoasa(config)# context ContextB
ciscoasa(config-ctx)# allocate-interface Ethernet0/0.3
ciscoasa(config-ctx)# allocate-interface Ethernet0/1.3
ciscoasa(config-ctx)# config-url disk0:/contextb.cfg
ciscoasa(config-ctx)# join-failover-group 1
```

# Tuning


Configuration > Device Management > High Availability > Failover
Setup
Interfaces
Criteria
MAC Addresses
Define criteria for failover: how many interfaces must fail and how long to wait between polls. The hold time specifies the interval to wait without receiving a response to a poll before unit failover.
Interface Policy
Number of failed interfaces that triggers failover: 1 (range 1 - 250)
Percentage of failed interfaces that triggers failover: 50 %
Failover Poll Times
Unit Failover: 1 seconds (range 1 - 15)
Unit Hold Time: 3 seconds (range 1 - 45) (at least 3 times unit poll time)
Monitored Interfaces: 5 seconds (range 1 - 15)
Interface Hold Time: 25 seconds (range 5 - 75 and at least 5 times interface poll time)
Apply
Reset