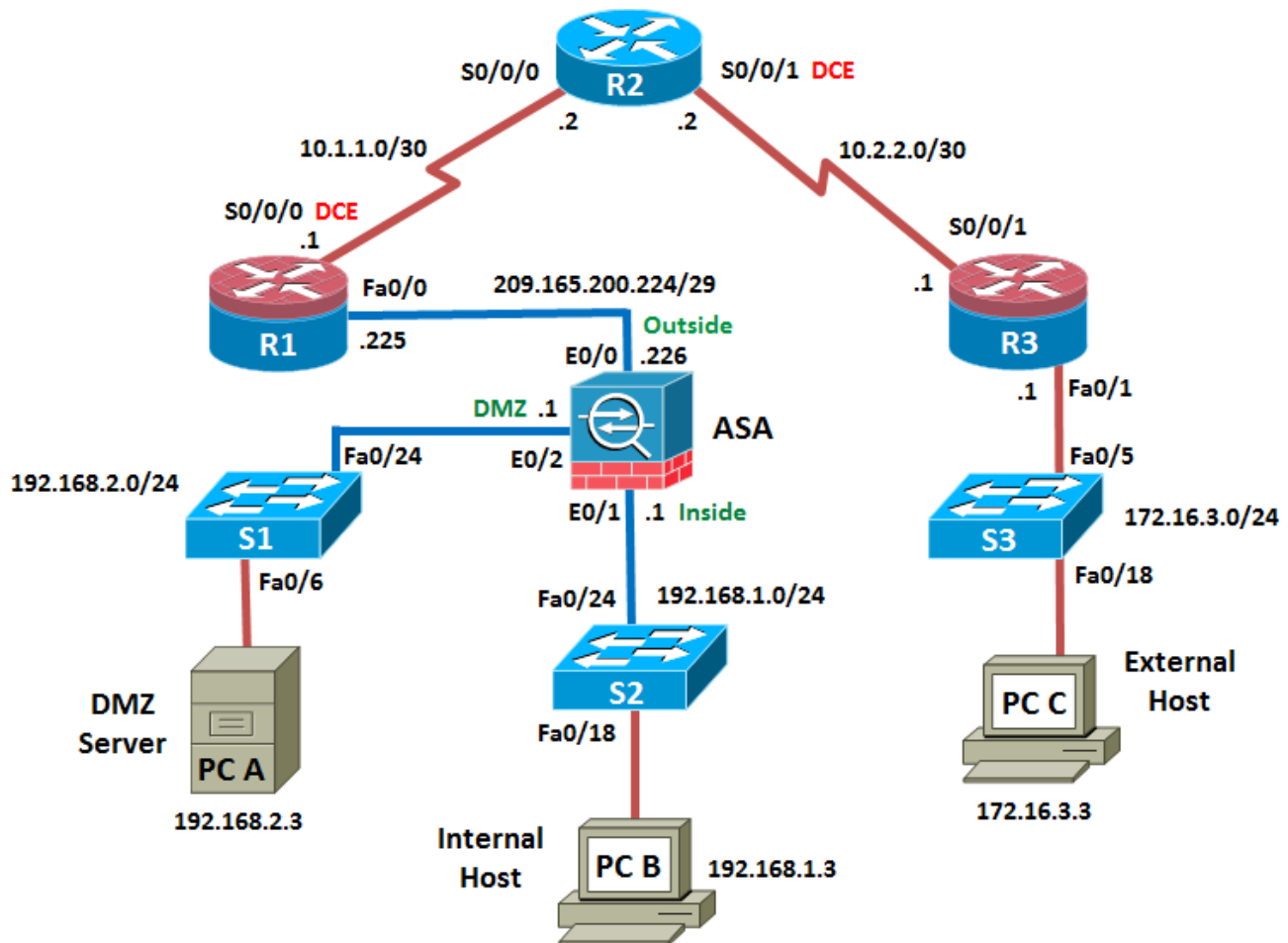


Chapter 10 Lab F: Configuring ASA 5510 Basic Settings and Firewall Using ASDM

Topology



Note: ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet interfaces.

IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	172.16.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	E0/0 (outside)	209.165.200.226	255.255.255.248	NA	R1 FA0/0
	E0/1 (inside)	192.168.1.1	255.255.255.0	NA	S2 FA0/24
	E0/2 (dmz)	192.168.2.1	255.255.255.0	NA	S1 FA0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 FA0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 FA0/18

Objectives

Part 1: Lab Setup

- Cable the network as shown in the topology.
- Configure hostnames and interface IP addresses for routers, switches, and PCs.
- Configure static routing, including default routes, between R1, R2, and R3.
- Configure HTTP and Telnet access for R1.
- Verify connectivity between hosts, switches, and routers.

Part 2: Accessing the ASA Console and ASDM

- Access the ASA console and view hardware, software, and configuration settings.
- Clear previous configuration settings.
- Use CLI to configure settings for ASDM access.
- Test Ethernet and Layer 3 connectivity to the ASA.
- Access the ASDM GUI and explore major windows and options.

Part 3: Configuring ASA Settings and Firewall Using the ASDM Startup Wizard

- Configure the hostname, domain name, and enable password.
- Configure the inside and outside interfaces.
- Configure DHCP for the inside network.
- Configure port address translation (PAT) for the inside network.
- Configure Telnet and SSH administrative access.

Part 4: Configuring ASA Settings from the ASDM Configuration Menu

- Set the date and time.
- Configure a static default route for the ASA.
- Test connectivity using ASDM Ping and Traceroute.

- Configure Local AAA user authentication.
- Modify the MPF application inspection policy.

Part 5: Configuring a DMZ, Static NAT and ACLs

- Configure static NAT for the DMZ server.
- Configure an ACL on the ASA to allow access to the DMZ for Internet users.
- Verify access to the DMZ server for external and internal users.
- Use ASDM Monitor to graph traffic.

Background / Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall as well as VPN and other capabilities. This lab employs an ASA 5510 to create a firewall and protect an internal corporate network from external intruders while allowing internal hosts access to the Internet. The ASA creates three security interfaces: Outside, Inside and DMZ. It provides outside users limited access to the DMZ and no access to internal resources. Inside users can access the DMZ and outside resources.

The focus of this lab is on the configuration of the ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of the lab. This lab uses the ASA GUI interface ASDM, which is similar to the SDM and CCP used with Cisco ISRs, to configure basic device and security settings.

In Part 1 of the lab you will configure the topology and non-ASA devices. In Part 2 you will prepare the ASA for ASDM access. In Part 3 you will use the ASDM Startup wizard to configure basic ASA settings and the firewall between the inside and outside networks. In Part 4 you will configure additional settings via the ASDM configuration menu. In Part 5 you will configure a DMZ on the ASA and provide access to a server in the DMZ.

Your company has one location connected to an ISP. Router R1 represents a CPE device managed by the ISP. Router R2 represents an intermediate Internet router. Router R3 connects an administrator from a network management company, who has been hired to manage your network remotely. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network as well as the remote administrator. ASA Layer 3 routed interfaces provide access to the three areas created in the lab: Inside, Outside, and DMZ. The ISP has assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

Note: The routers used with this lab are Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). The switches are Cisco WS-C2960-24TT-L with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). Other routers, switches, and Cisco IOS versions can be used. However, results and output may vary.

The ASA used with this lab is a Cisco model 5510 with four FastEthernet routed interfaces, running OS version 8.4(2) and ASDM version 6.4(5), and comes with a Base license that allows a maximum of 50 VLANs.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 3 switches (Cisco 2960 or comparable)
- 1 ASA 5510 (OS version 8.4(2) and ASDM version 6.4(5) and Base license or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with CCP, PuTTY SSH client (Web and FTP server optional)
- PC-B: Windows XP, Vista, or Windows 7 with PuTTY SSH client and Java version 6.x or higher (ASDM loaded on the PC is optional)
- PC-C: Windows XP, Vista, or Windows 7 with CCP, PuTTY SSH client
- Serial and Ethernet cables as shown in the topology

- Rollover cables to configure the routers and ASA via the console

Part 1: Basic Router/Switch/PC Configuration

In Part 1 of this lab, you will set up the network topology and configure basic settings on the routers such as interface IP addresses and static routing.

Note: Do not configure any ASA settings at this time.

Step 1: Cable the network and clear previous device settings.

Attach the devices that are shown in the topology diagram and cable as necessary. Make sure that the routers and switches have been erased and have no startup configurations.

Step 2: Configure basic settings for routers and switches.

- Configure host names as shown in the topology for each router.
- Configure router interface IP addresses as shown in the IP Addressing Table.
- Configure a clock rate for routers with a DCE serial cable attached to the serial interface.
- Configure the host name for the switches. With the exception of the host name, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

Step 3: Configure static routing on the routers.

- Configure a static default route from R1 to R2 and from R3 to R2.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```
- Configure a static route from R2 to the R1 Fa0/0 subnet (connected to ASA interface E0/0) and a static route from R2 to the R3 LAN.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

Step 4: Enable the HTTP server on R1 and set the enable and vty passwords.

- Enable HTTP access to R1 using the `ip http server` command in global config mode. Configure an enable password of **class**. Also set the vty and console passwords to **cisco**. This will provide web and Telnet targets for testing later in the lab.

```
R1(config)# ip http server
R1(config)# enable password class
```

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

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

- On routers R2 and R3, set the same enable, console and vty passwords as with R1.

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing Table.

Step 6: Verify connectivity.

Because the ASA is the focal point for the network zones and it has not yet been configured, there will be no connectivity between devices that are connected to it. However, PC-C should be able to ping the Fa0/0 interface of R1. From PC-C, **ping** the R1 Fa0/0 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

Note: If you can ping from PC-C to R1 Fa0/0 and S0/0/0 you have demonstrated that static routing is configured and functioning correctly.

Step 7: Save the basic running configuration for each router and switch.**Part 2: Accessing the ASA Console and ASDM**

In Part 2 of this lab, you will access the ASA via the console and use various **show** commands to determine hardware, software, and configuration settings. You will prepare the ASA for ASDM access and explore some of the ASDM screens and options.

Step 1: Access the ASA console.

- Accessing the ASA via the console port is the same as with a Cisco router or switch. Connect to the ASA console port with a rollover cable.
- Use a terminal emulation program such as TeraTerm or HyperTerminal to access the CLI. Use the Serial port settings of 9600 baud, eight data bits, no parity, one stop bit, and no flow control.
- If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.
- Enter privileged mode with the **enable** command and password (if set). By default the password is blank so you can just press **Enter**. If the password has been changed to that specified in this lab, the password will be **class**. In addition, the hostname and prompt will be **CCNAS-ASA>**, as shown here. The default ASA hostname and prompt is **ciscoasa>**.

```
CCNAS-ASA> enable
Password: class (or press Enter if none set)
```

Step 2: Determine the ASA version, interfaces, and license.

The ASA 5510 used in this lab has four integrated 10/100 FastEthernet interfaces (E0/0 – E0/3). Unlike the 5505 model, these are Layer 3 routed interfaces similar to those in an ISR. In addition, a special Management FastEthernet interface (M0/0) is also provided, which is not present on the ASA 5505.

Use the **show version** command to determine various aspects of this ASA device.

```
CCNAS-ASA# show version

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 15-Jun-11 18:17 by builders
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

CCNAS-ASA up 24 mins 5 secs

Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1599 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                          Boot microcode       : CN1000-MC-BOOT-2.00
                          SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                          IPSec microcode       : CNlite-MC-IPSECm-MAIN-2.06
```

Number of accelerators: 1

```

0: Ext: Ethernet0/0      : address is 44d3.cafd.986c, irq 9
1: Ext: Ethernet0/1      : address is 44d3.cafd.986d, irq 9
2: Ext: Ethernet0/2      : address is 44d3.cafd.986e, irq 9
3: Ext: Ethernet0/3      : address is 44d3.cafd.986f, irq 9
4: Ext: Management0/0    : address is 44d3.cafd.986b, irq 11
5: Int: Not used         : irq 11
6: Int: Not used         : irq 5

```

Licensed features for this platform:

Maximum Physical Interfaces	: Unlimited	perpetual
Maximum VLANs	: 50	perpetual
Inside Hosts	: Unlimited	perpetual
Failover	: Disabled	perpetual
VPN-DES	: Enabled	perpetual
VPN-3DES-AES	: Enabled	perpetual
Security Contexts	: 0	perpetual
GTP/GPRS	: Disabled	perpetual
AnyConnect Premium Peers	: 2	perpetual
AnyConnect Essentials	: Disabled	perpetual
Other VPN Peers	: 250	perpetual
Total VPN Peers	: 250	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.

<output omitted>

What software version is this ASA 5510 running? _____

What is the name of the system image file and from where was it loaded?

The ASA can be managed using a built-in GUI known as the Adaptive Security Device Manager (ASDM). What version of ASDM is this ASA running? _____

How much RAM does this ASA have? _____

How much flash memory does this ASA have? _____

How many Ethernet interfaces does this ASA have? _____

What type of license does this ASA have? _____

How many VLANs can be created with this license? _____

Step 3: Determine the file system and contents of flash memory.

- Display the ASA file system using the **show file system** command to determine what prefixes are supported.

CCNAS-ASA# **show file system**

File Systems:

	Size(b)	Free(b)	Type	Flags	Prefixes
* 260034560		198070272	disk	rw	disk0: flash:

```

-          - disk      rw      disk1:
-          - network   rw      tftp:
-          - opaque    rw      system:
-          - network   ro      http:
-          - network   ro      https:
-          - network   rw      ftp:
-          - network   rw      smb:

```

What is another name for flash: ? _____

- b. Display the contents of flash memory using one of these commands: **show flash**, **show disk0**, **dir flash:** or **dir disk0:**

CCNAS-ASA# **show flash:**

```

--#--  --length--  -----date/time-----  path
124  15390720      Oct 19 2011 15:49:48  asa842-k8.bin
125  16280544      Oct 19 2011 18:22:24  asdm-645.bin
   3   4096         Jan 01 2003 00:03:32  log
  10   4096         Jan 01 2003 00:04:00  crypto_archive
  11   4096         Jan 01 2003 00:04:04  coredumpinfo
  12    43          Jan 01 2003 00:04:04  coredumpinfo/coredump.cfg
127  12105313      Oct 19 2011 18:07:50  csd_3.5.841-k9.pkg
128   4096         Oct 19 2011 18:07:52  sdesktop
135   1462         Oct 19 2011 18:07:52  sdesktop/data.xml
129  2857568       Oct 19 2011 18:07:54  anyconnect-wince-ARMv4I-2.4.1012-k9.pkg
130  3203909       Oct 19 2011 18:07:54  anyconnect-win-2.4.1012-k9.pkg
131  4832344       Oct 19 2011 18:07:58  anyconnect-macosx-i386-2.4.1012-k9.pkg
132  5209423       Oct 19 2011 18:08:00  anyconnect-linux-2.4.1012-k9.pkg

```

260034560 bytes total (198070272 bytes free)

What is the name of the ASDM file in flash: ? _____

Step 4: Determine the current running configuration.

The ASA 5510 is commonly used as an edge security device that connects a medium -sized business to an ISP for access to the Internet. The default factory configuration for the ASA 5510 includes the following:

- The management interface, Management 0/0, is configured. If you did not set the IP address using the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.

Note: The Management 0/0 interface is a separate physical FastEthernet interface on the ASA 5510. This interface is not present on the ASA 5505.

- The DHCP server is enabled on the security appliance, so a PC connecting to the Management 0/0 interface receives an address between 192.168.1.2 and 192.168.1.254.

Note: With the default factory configuration, it is assumed that the PC connected to Management 0/0 is a DHCP client and will be used to configure the 5510 using the ASDM GUI imbedded in flash.

- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.
- No console or enable passwords are required and the default host name is **ciscoasa**.

Note: The default factory configuration only configures the Management 0/0 interface and does not configure an inside or outside network interface.

The configuration consists of the commands listed below.

Note: Do not use these commands to configure the ASA at this time.

```
interface management 0/0
```

```
ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown
logging asdm informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

- a. Display the current running configuration using the **show running-config** command. Output will vary depending on the current state of the ASA configuration

```
CCNAS-ASA# show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
  no nameif
  no security-level
  no ip address
!
<output omitted>
```

Tip: To stop the output from a command using the CLI, press the letter **Q**.

If you see the Management interface configured, and other settings as described previously, the device is most likely configured with the default factory configuration. You may also see other security features such as a global policy that inspects selected application traffic, which the ASA inserts by default, if the original startup configuration has been erased. The actual output will vary depending on the ASA model, version and configuration status.

- b. You can restore the ASA to its factory default settings by using the command **configure factory-default** from global configuration mode as shown here.

```
CCNAS-ASA# conf t
CCNAS-ASA(config)# configure factory-default
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 192.168.1.1 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
```



```

Executing command: exit
Executing command: http server enable
Executing command: http 192.168.1.0 255.255.255.0 management
Executing command: dhcpd address 192.168.1.2-192.168.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed

```

- c. Review this output. You may wish to capture and print the factory-default configuration as a reference.

Note: Restoring the ASA to factory default settings resets the hostname and prompt to **ciscoasa>**.

Step 5: Clear the previous ASA configuration settings.

- a. Use the **write erase** command to remove the **startup-config** file from flash memory.

```

ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK]
ciscoasa#

ciscoasa# show start
No Configuration

```

Note: The IOS command **erase startup-config** is not supported on the ASA.

- b. Use the **reload** command to restart the ASA. If prompted to save the configuration, respond with **"no"**.

```

ciscoasa# reload
Proceed with reload? [confirm] <Enter>
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
<output omitted>

```

Step 6: Bypass setup mode and configure the ASA interfaces.

When the ASA completes the reload process, it should detect that the **startup-config** file is missing and present a series of interactive prompts to configure basic ASA settings. If it does not come up in this mode, repeat Step 5.

- a. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with **"no."**

```
Pre-configure Firewall now through interactive prompts [yes]? no
```
- b. Enter privileged EXEC mode with the **enable** command and press <Enter>. The password should be blank (no password) at this point.
- c. Enter global configuration mode using the command **config t**. The first time you enter configuration mode after reloading you will be asked if you wish to enable anonymous reporting. Respond with **"no."**

ASA 5510 interface notes:

The 5510 and other higher-end 5500 series ASA models are different from the ASA 5505. With the 5510 a physical FastEthernet interface can be assigned a Layer 3 IP address directly, much like a Cisco router. With the ASA 5505, the eight integrated switch ports are Layer 2 ports and VLANs must be created. This is not the case with the 5510. The four FastEthernet interfaces on the 5510 are routed interfaces.

Note: If you completed the initial configuration **Setup** utility, Management interface M0/0 is configured with an IP address of 192.168.1.1. You will need to remove the IP address from the M0/0 interface in order to assign it to the inside interface E0/1. Instructions are provide here to configure both the inside (E0/1) and outside interface (E0/0) at this time. The DMZ interface (E0/2) will be configured in Part 6 of the lab.

- d. Remove the configuration from the M0/0 interface and shut it down (if required).

```
ciscoasa(config)# interface m0/0
ciscoasa(config-if)# shutdown
ciscoasa(config-if)# no nameif
ciscoasa(config-if)# no security-level
ciscoasa(config-if)# no ip address
```

- e. Configure interface E0/1 for the inside network, 192.168.1.0/24. Name the interface **inside**, set the security level to the highest setting of **100** and bring it up.

```
ciscoasa(config)# interface e0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
```

- f. Configure interface E0/0 for the outside network, 209.165.200.224/29. Name the interface **outside**, set the security level to the lowest setting of **0** and bring it up.

```
ciscoasa(config-if)# interface e0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# no shutdown
```

Interface security level notes:

You may receive a message that the security level for the inside interface was set automatically to 100 and the outside interface was set to 0. The ASA uses interface security levels from 0 to 100 to enforce the security policy. Security Level 100 (inside) is the most secure and level 0 (outside) is the least secure.

By default, the ASA applies a policy where traffic from a higher security level interface to one with a lower level is permitted and traffic from a lower security level interface to one with a higher security level is denied. The ASA default security policy permits outbound traffic, which is inspected by default. Returning traffic is allowed because of stateful packet inspection. This default “routed mode” firewall behavior of the ASA allows packets to be routed from the inside network to the outside network but not vice versa. In Part 3 of this lab you will configure NAT to increase the firewall protection.

- g. Use the **show interface ip brief** command to ensure that ASA interfaces E0/0 and E0/1 are both up/up. Note that this command is different from the IOS command **show ip interface brief**. If either port is shown as down/down, check the physical connections. If either port is administratively down, bring it up with the **no shutdown** command.

```
ciscoasa(config-if)# show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	209.165.200.226	YES	manual	up	up
Ethernet0/1	192.168.1.1	YES	manual	up	up
Ethernet0/2	unassigned	YES	unset	administratively down	up
Ethernet0/3	unassigned	YES	unset	administratively down	down
Management0/0	unassigned	YES	unset	administratively down	down

Tip: Most ASA **show** commands, as well as **ping**, **copy** and others, can be issued from within any config mode prompt without the “do” command required with IOS.

- h. Display the Layer 3 interface information using the **show ip address** command.

```
ciscoasa(config)# show ip address
```

<output omitted>

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Ethernet0/0	outside	209.165.200.226	255.255.255.248	manual
Ethernet0/1	inside	192.168.1.1	255.255.255.0	Manual

- i. You may also use the command **show running-config interface** to display the configuration for a particular interface from the running-config.

```
ciscoasa# show run interface e0/0
!
interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 209.165.200.226 255.255.255.248
```

- j. Test basic connectivity to the ASA by pinging from PC-B to ASA interface E0/1 IP address 192.168.1.1. The pings should be successful.

Step 7: Configure HTTP and verify ASDM access to the ASA.

- a. Configure the ASA to accept HTTPS connections using the **http** command to allow access to ASDM from any host on the inside network 192.168.1.0/24.

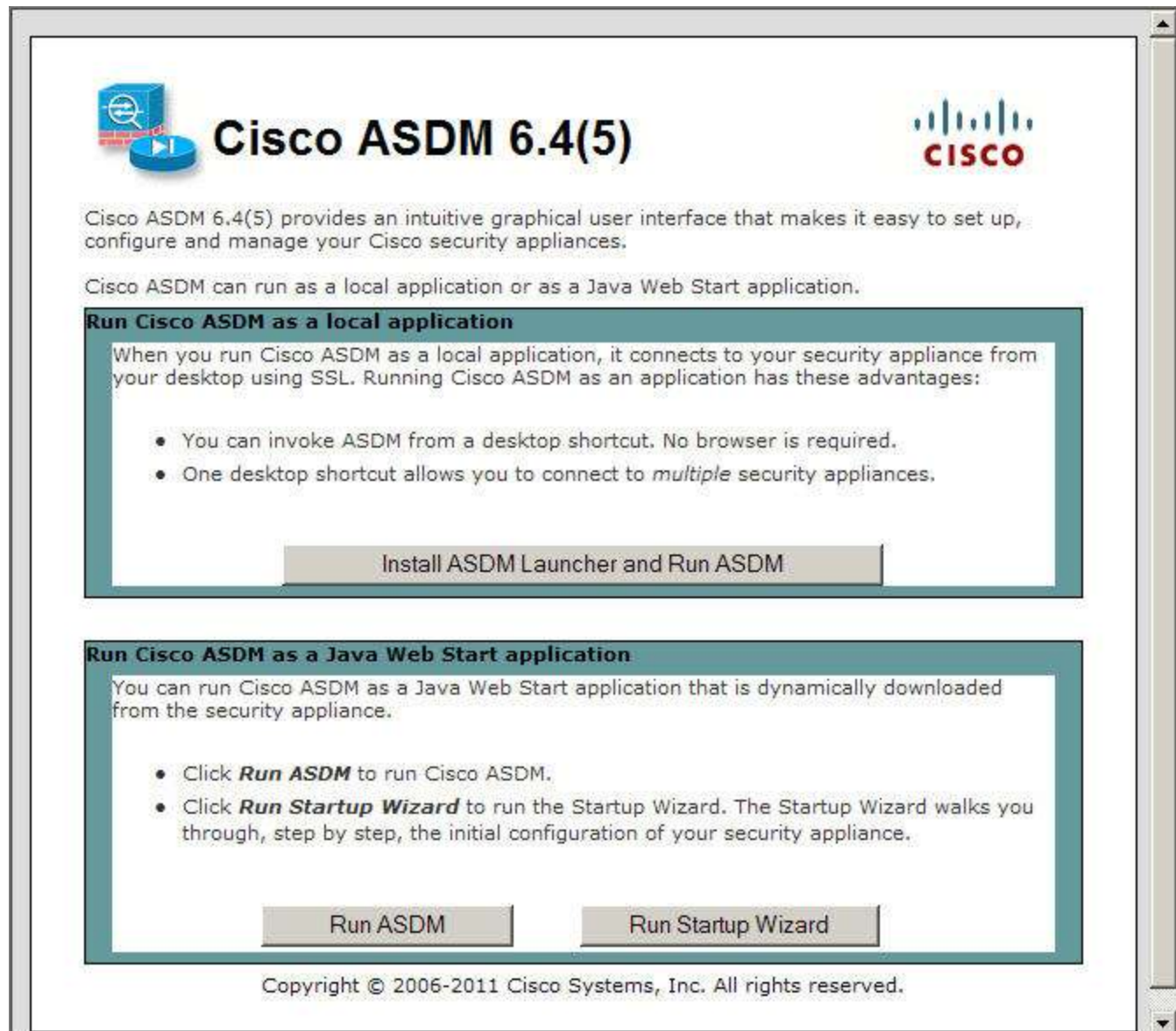
```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

- b. Open a browser on PC-B and test the HTTPS access to the ASA by entering <https://192.168.1.1>.

Note: Be sure to specify the HTTPS protocol in the URL.

Step 8: Access ASDM and explore the GUI.

- a. After entering the URL above, you should see a security warning about the website security certificate. Click **Continue to this website**. The ASDM Welcome page will display. From this screen, you can run ASDM as a local application on the PC (installs ASDM on the PC), run ASDM as a browser-based Java applet directly from the ASA, or run the Startup wizard.



The screenshot shows the Cisco ASDM 6.4(5) interface. At the top left is a logo with a blue cube and a play button. To its right is the text "Cisco ASDM 6.4(5)". At the top right is the Cisco logo. Below the title, a paragraph states: "Cisco ASDM 6.4(5) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances." Another paragraph follows: "Cisco ASDM can run as a local application or as a Java Web Start application." There are two main sections, each with a teal header. The first section is titled "Run Cisco ASDM as a local application" and contains text about connecting via SSL and a list of advantages: "You can invoke ASDM from a desktop shortcut. No browser is required." and "One desktop shortcut allows you to connect to *multiple* security appliances." Below this list is a button labeled "Install ASDM Launcher and Run ASDM". The second section is titled "Run Cisco ASDM as a Java Web Start application" and contains text about dynamically downloading the application. It lists two options: "Click **Run ASDM** to run Cisco ASDM." and "Click **Run Startup Wizard** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance." Below these options are two buttons: "Run ASDM" and "Run Startup Wizard". At the bottom of the window, a copyright notice reads: "Copyright © 2006-2011 Cisco Systems, Inc. All rights reserved."

Cisco ASDM 6.4(5)

Cisco ASDM 6.4(5) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

Install ASDM Launcher and Run ASDM

Run Cisco ASDM as a Java Web Start application

You can run Cisco ASDM as a Java Web Start application that is dynamically downloaded from the security appliance.

- Click **Run ASDM** to run Cisco ASDM.
- Click **Run Startup Wizard** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

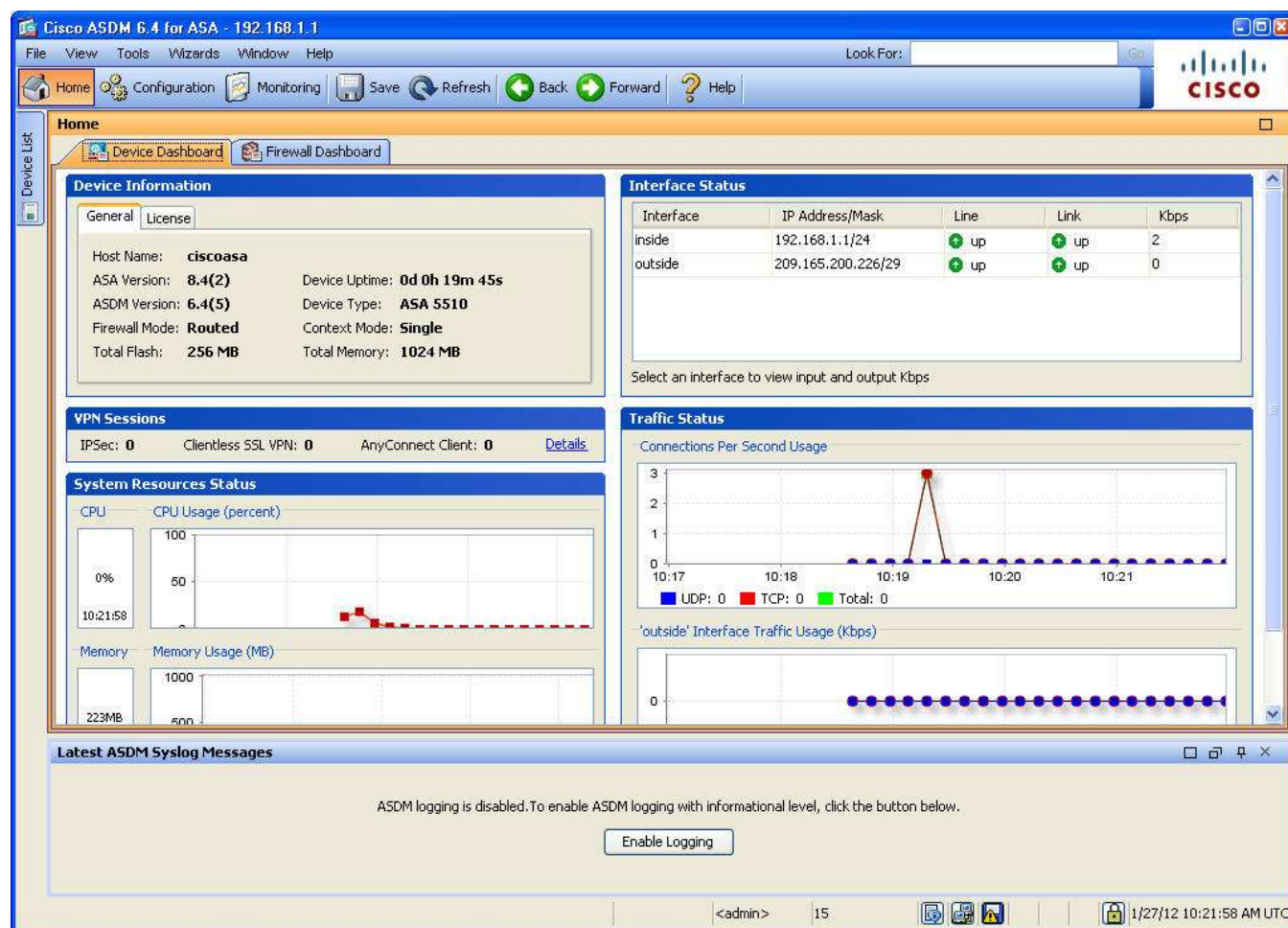
Run ASDM Run Startup Wizard

Copyright © 2006-2011 Cisco Systems, Inc. All rights reserved.

- b. Click the **Run ASDM** button.
- c. Click **Yes** for any other security warnings. You should see the **Cisco ASDM-IDM Launcher** dialog box where you can enter a username and password. Leave these fields blank as they have not yet been configured.



- d. Click **OK** to continue. ASDM will load the current configuration into the GUI.
- e. The initial GUI screen is displayed with various areas and options. The main menu at the top left of the screen contains three main sections; Home, Configuration, and Monitoring. The Home section is the default and has two dashboards: Device and Firewall. The Device dashboard is the default screen and shows device information such as Type (ASA 5510), ASA and ASDM version, amount of memory and firewall mode (routed). There are five areas on the Device Dashboard.
 - **Device Information**
 - **Interface Status**
 - **VPN Sessions**
 - **System Resources Status**
 - **Traffic Status**

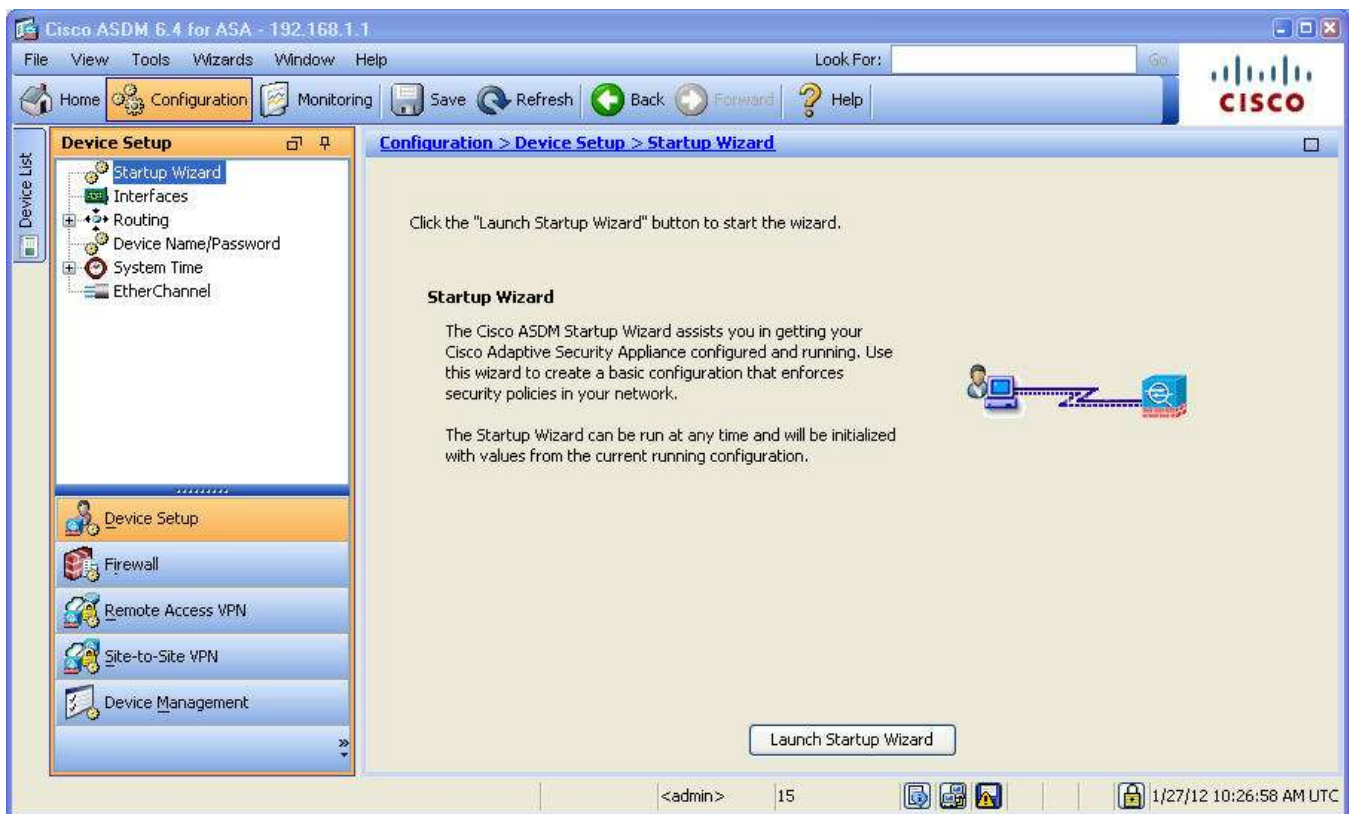


- f. Click the **Configuration** and **Monitoring** tabs to become familiar with their layout and to see what options are available.

Part 3: Configuring Basic ASA Settings and Firewall Using the ASDM Startup Wizard

Step 1: Access the Configuration menu and launch the Startup wizard.

- a. Click the **Configuration** button at the top left of the screen. There are five main configuration areas:
 - **Device Setup**
 - **Firewall**
 - **Remote Access VPN**
 - **Site-to-Site VPN**
 - **Device Management**
- b. The Device Setup Startup wizard is the first option available and displays by default. Read through the on-screen text describing the Startup wizard and then click the **Launch Startup Wizard** button.



Step 2: Configure hostname, domain name, and enable password.

- a. On the first Startup Wizard screen, you have a choice of modifying the existing configuration or resetting the ASA to the factory defaults. With the **Modify Existing Configuration** option selected, click **Next** to continue.
- b. On the Startup Wizard Step 2 screen, **Basic Configuration**, configure the ASA host name **CCNAS-ASA** and domain name of **ccna.security.com**. Click the checkbox for changing the enable mode password and change it from blank (no password) to **class** and enter it again to confirm. When the entries are completed, click **Next** to continue.

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Basic Configuration (Step 2 of ...)

☐ Configure the device for Teleworker usage

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

ASA Host Name:

Domain Name:

Privileged Mode (Enable) Password

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

☒ Change privileged mode (enable) password

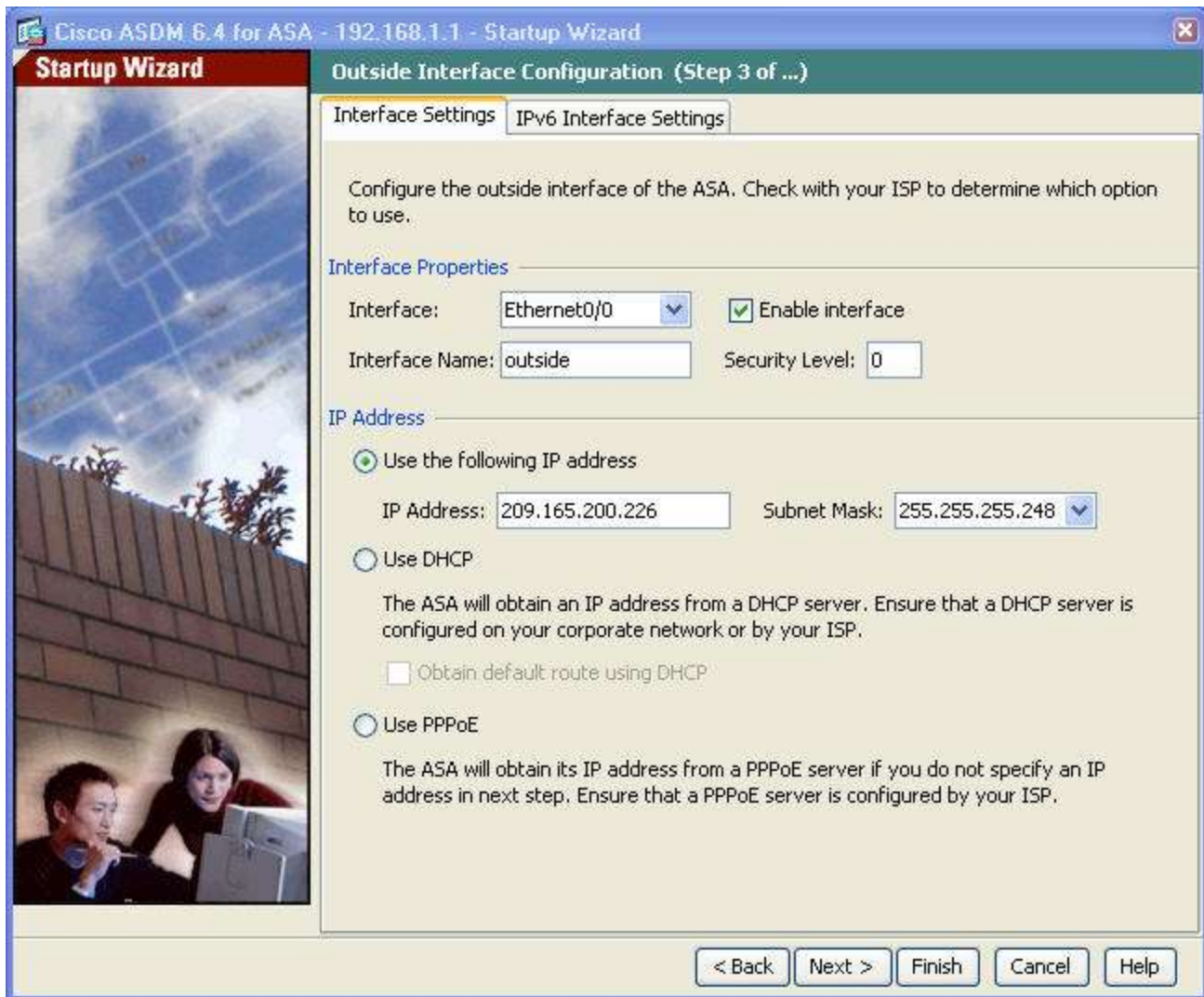
Old Password:

New Password:

Confirm New Password:

Step 3: Configure the outside interface.

- a. On the Startup Wizard Step 3 screen – **Outside Interface Configuration, Interface Settings** tab, review the interface properties shown. Do not change the current settings because these were previously defined using the CLI. Click **Next** to continue.



- b. On the Startup Wizard Step 4 screen – **Other Interface Configuration**, verify the settings for the inside interface, which were previously configured via the CLI. You can edit the settings for any of the interfaces from this screen.

Note: Do not check the two boxes for enabling traffic between interfaces of the same security level and hosts on the same interface.

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Other Interface Configuration (Step 4 of 11)

Configure the remaining interfaces of the ASA. To configure an interface, select it in the list below and click Edit.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask/ Prefix Length
Ethernet0/1	inside	Yes	100	192.168.1.1	255.255.255.0
Ethernet0/0	outside	Yes	0	209.165.200.226	255.255.255.248
Ethernet0/2		No			
Ethernet0/3		No			
Management0/0		No			

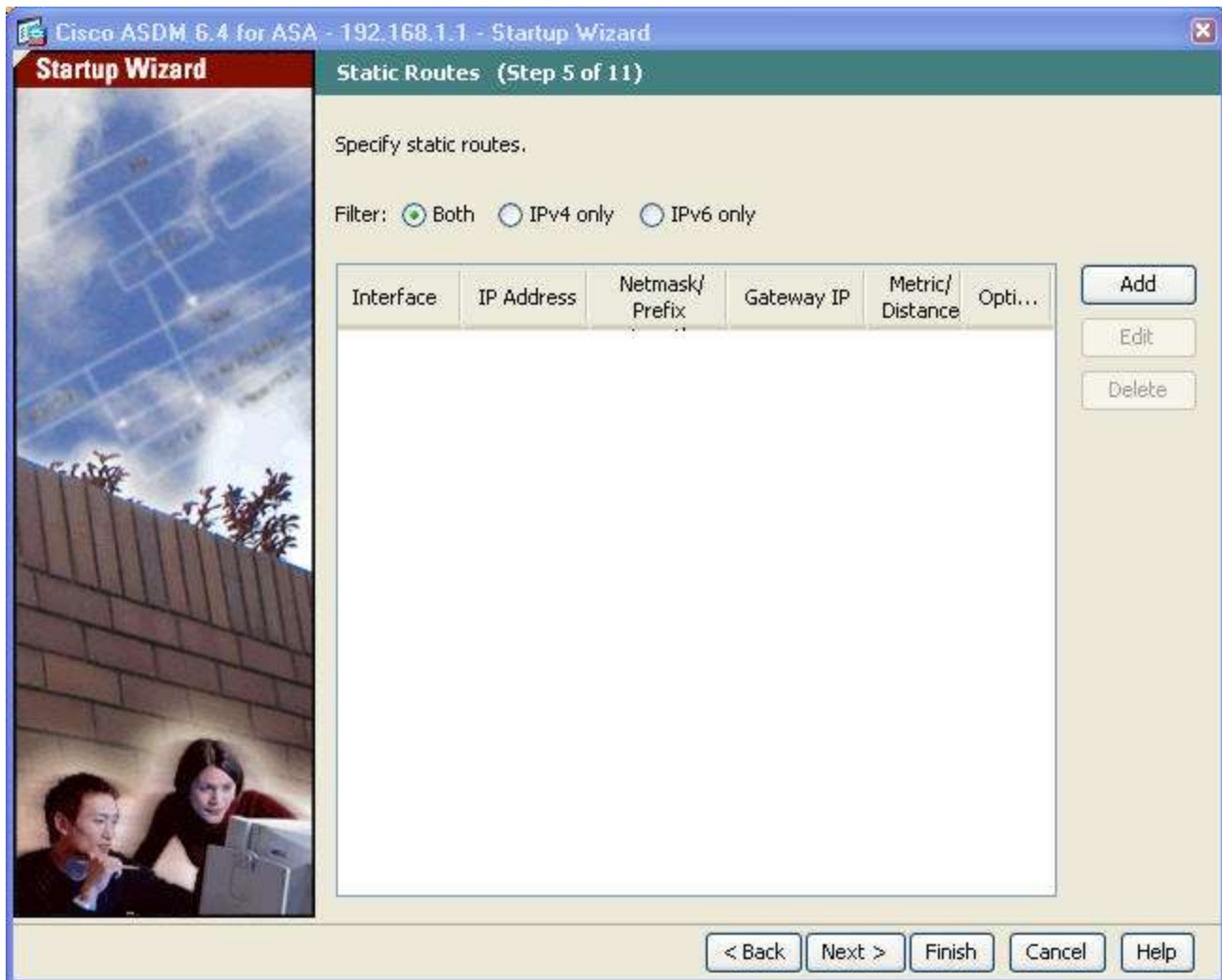
[Edit](#)

☐ Enable traffic between two or more interfaces with the same security levels

☐ Enable traffic between two or more hosts connected to the same interface

[< Back](#) [Next >](#) [Finish](#) [Cancel](#) [Help](#)

- c. On the Startup Wizard Step 5 screen – **Static Routes**, click **Next** to bypass this wizard option at this time. You will configure a static route for the ASA later using the Configuration menu.



Step 4: Configure DHCP, address translation and administrative access.

- a. On the Startup Wizard Step 6 screen – **DHCP Server**, select the checkbox to **Enable DHCP server on the inside interface**. Enter a Starting IP Address of **192.168.1.5** and Ending IP Address of **192.168.1.50**. Enter the DNS Server 1 address of **10.20.30.40** and Domain Name **ccna.security.com**. Do **NOT** check the box to Enable autoconfiguration from interface. Click **Next** to continue.

The screenshot shows the Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard window. The title bar indicates the interface is 192.168.1.1. The window is titled "Startup Wizard" and "DHCP Server (Step 6 of 11)".

The main content area contains the following information:

- A text box explaining that the ASA can act as a DHCP server and provide IP addresses to the hosts on the Inside network. It also mentions that to configure a DHCP server on an interface other than the inside interface, the user should go to Configuration > Device Management > DHCP > DHCP Server in the main ASDM window.
- A checkbox labeled "Enable DHCP server on the inside interface" which is checked.
- A section titled "DHCP Address Pool" with two input fields: "Starting IP Address" (192.168.1.5) and "Ending IP Address" (192.168.1.50).
- A section titled "DHCP Parameters" with several input fields:
 - DNS Server 1: 10.20.30.40
 - DNS Server 2: (empty)
 - WINS Server 1: (empty)
 - WINS Server 2: (empty)
 - Lease Length: (empty) sec
 - Ping Timeout: (empty) ms
 - Domain Name: ccnasecurity.com
- A text box explaining that enabling auto-configuration causes the DHCP server to automatically configure DNS, WINS and domain name. The values in the fields above take precedence over the auto-configured values.
- A checkbox labeled "Enable auto-configuration from interface:" which is unchecked.
- A dropdown menu showing "outside".

At the bottom of the window, there are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

- b. On the Startup Wizard Step 7 screen – **Address Translation (NAT/PAT)**, click the button **Use Port Address Translation (PAT)**. The default is to use the IP address of the outside interface. Note that you can also specify a particular IP address for PAT or a range of addresses with NAT. Click **Next** to continue.

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Address Translation (NAT/PAT) (Step 7 of 11)

Select Port Address Translation (PAT) to share a single external IP address for devices on the inside interface. Select Network Address Translation (NAT) to share several external IP addresses for devices on the inside interface. Select the first option, if no address translation is desired between the inside and outside interfaces.

This NAT configuration applies to all the traffic from the inside interface to the outside interface.

☐ No Address Translation

☒ Use Port Address Translation (PAT)

☒ Use the IP address on the outside interface

☐ Specify an IP address

IP Address:

☐ Use Network Address Translation (NAT)

IP Address Range:

< Back Next > Finish Cancel Help

- c. On the Startup Wizard Step 8 screen – **Administrative Access**, HTTPS/ASDM access is currently configured for hosts on inside network 192.168.1.0/24. Add Telnet access to the ASA for the inside network 192.168.1.0 with a subnet mask of 255.255.255.0. Add SSH access to the ASA from host 172.16.3.3 on the outside network. Make sure the checkbox **Enable HTTP server for HTTPS/ASDM access** is checked. Click **Next** to continue.

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Administrative Access (Step 8 of 11)

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

Type	Interface	IP Address	Mask/ Prefix Length
HTTPS/ASDM	inside	192.168.1.0	255.255.255.0
Telnet	inside	192.168.1.0	255.255.255.0
SSH	outside	172.16.3.3	255.255.255.255

☒ Enable HTTP server for HTTPS/ASDM access
Disabling HTTP server will prevent HTTPS/ASDM access to this ASA.

☐ Enable ASDM history metrics

< Back Next > Finish Cancel Help

- d. On the Startup Wizard Step 9 screen – **Auto Update Server**, review the on-screen text describing the function of Auto Update but do not check the box to Enable Auto Update ASA. Click **Next** to continue.

Cisco ASDM 6.4 for ASA - 192.168.1.1 - Startup Wizard

Startup Wizard

Auto Update Server (Step 9 of 11)

The ASA can be remotely managed from an Auto Update Server. This includes automatically updating the ASA configuration, ASA image, and ASDM image as needed.

☐ Enable Auto Update for ASA

Server

Server URL: :// /

☐ Verify server's SSL certificate

User

Specify the username and password to login to the auto update server.

Username:

Password: Confirm Password:

Device Identity

Specify the device ID to uniquely identify the ASA.

Device ID Type:

Device ID:

< Back Next > Finish Cancel Help

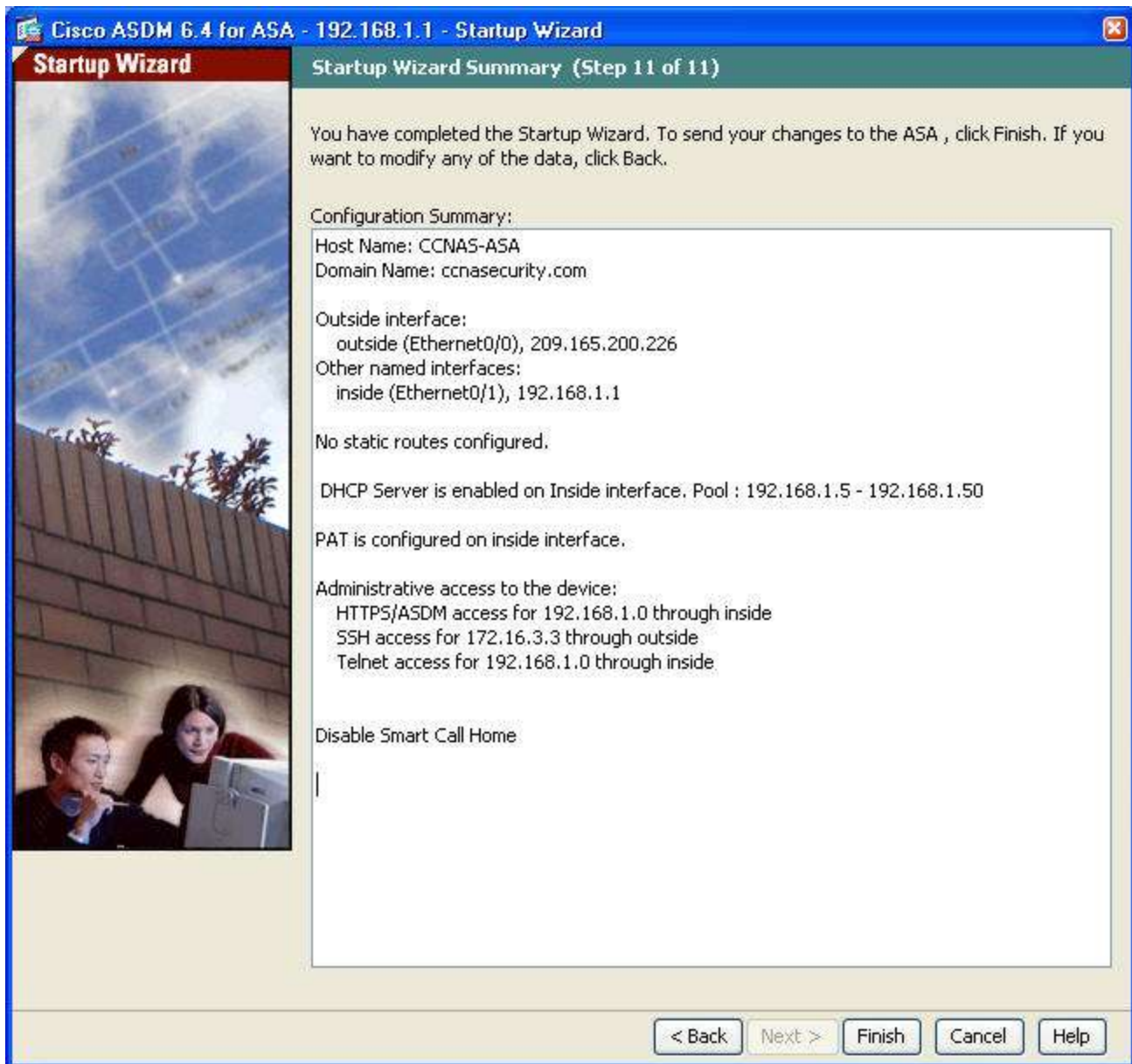
- e. On the Startup Wizard Step 10 screen – **Cisco Smart Call Home Enrollment**, review the on-screen text describing the function of Smart Call Home and leave the default radio button selected to not enable this feature. Click **Next** to continue.



Step 5: Review the summary and deliver the commands to the ASA

- On the Startup Wizard Step 11 screen – **Startup Wizard Summary**, review the Configuration Summary and click **Finish**. ASDM will deliver the commands to the ASA device and then reload the modified configuration.

Note: If the GUI dialogue box stops responding during the reload process, close it, exit ASDM, and restart the browser and ASDM. If prompted to save the configuration to flash memory, respond with **Yes**. Even though ASDM may not appear to have reloaded the configuration, the commands were delivered. If there are errors encountered as ASDM delivers the commands, you will be notified with a list of commands that succeeded and those that failed.



- b. Restart ASDM and provide the new enable password **class** with no username. Return to the Device Dashboard and check the Interface Status window. You should see the inside and outside interfaces with IP address and status. The inside interface should show some number of Kb/s. The Traffic Status window may show the ASDM access as TCP traffic spike.

Step 6: Test Telnet and SSH access to the ASA.

- a. From a command prompt or GUI Telnet client on PC-B, Telnet to the ASA inside interface at IP address 192.168.1.1.
- b. Login to the ASA using the default login password of **cisco**. Enter privileged EXEC mode by using the **enable** command and provide the password **class**. Exit the Telnet session by using the **quit** command.
- c. In Part 3, Step 4, SSH access was configured using the Startup wizard to allow access to the ASA from outside PC-C (172.16.3.3). From PC-C, open an SSH client such as PuTTY and attempt to connect to the ASA outside interface at 209.165.200.226. You will not be able to establish the

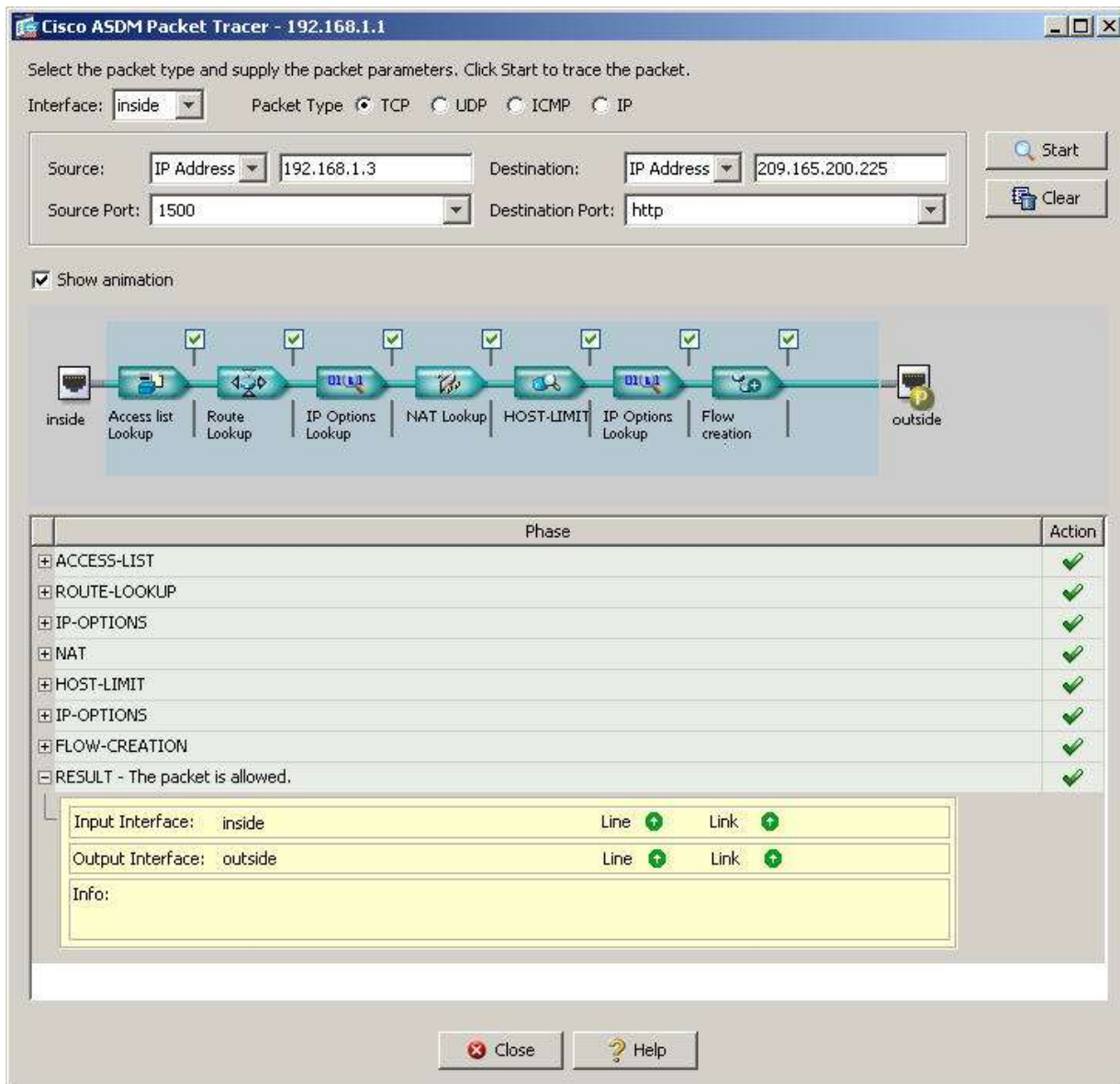
connection because SSH access (ASA version 8.4(2) and later) requires that you also configure AAA and provide an authenticated user name. AAA will be configured in the Part 4 of the lab.

Step 7: Test access to an external website from PC-B.

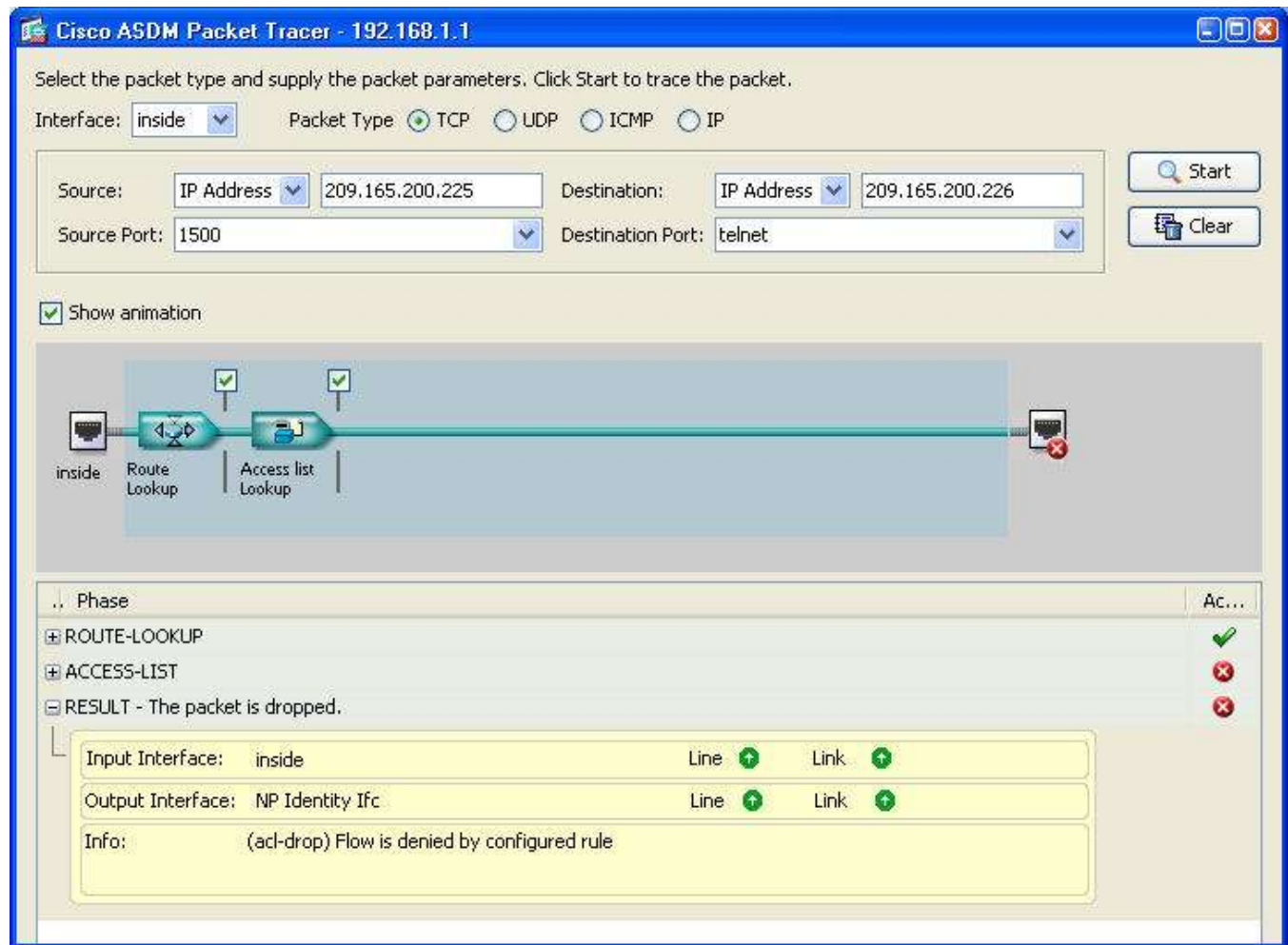
- a. Open a browser on PC-B and enter the IP address of the R1 Fa0/0 interface (209.165.200.225) to simulate access to an external website.
- b. The R1 HTTP server was enabled in Part 1 of the lab so you should be prompted with a user authentication login dialog box from the R1 GUI device manger. Leave the username blank and enter the password of **class**. Exit the browser. You should see TCP activity in the ASDM Device Dashboard Traffic Status window.

Step 8: Test access to an external website using the ASDM Packet Tracer utility.

- a. From the ASDM Home page, choose **Tools > Packet Tracer**.
- b. Choose the **Inside** interface from the Interface drop down menu and click **TCP** from the Packet Type radio buttons. From the Source drop down menu, choose IP Address and enter the address **192.168.1.3** (PC-B) with a source port of **1500**. From the Destination drop down menu, choose IP Address and enter **209.165.200.225** (R1 Fa0/0) with a Destination Port of **HTTP**. Click **Start** to begin the trace of the packet. The packet should be permitted.



- c. Reset the entries by clicking the **Clear** button. Try another trace and choose **Outside** from the Interface drop down menu and leave **TCP** as the packet type. From the Source drop down menu, choose IP Address and enter **209.165.200.225** (R1 Fa0/0) and a Source Port of **1500**. From the Destination drop down menu, choose IP Address and enter the address **209.165.200.226** (ASA outside interface) with a Destination Port of telnet. Click **Start** to begin the trace of the packet. The packet should be dropped. Click **Close** to continue.

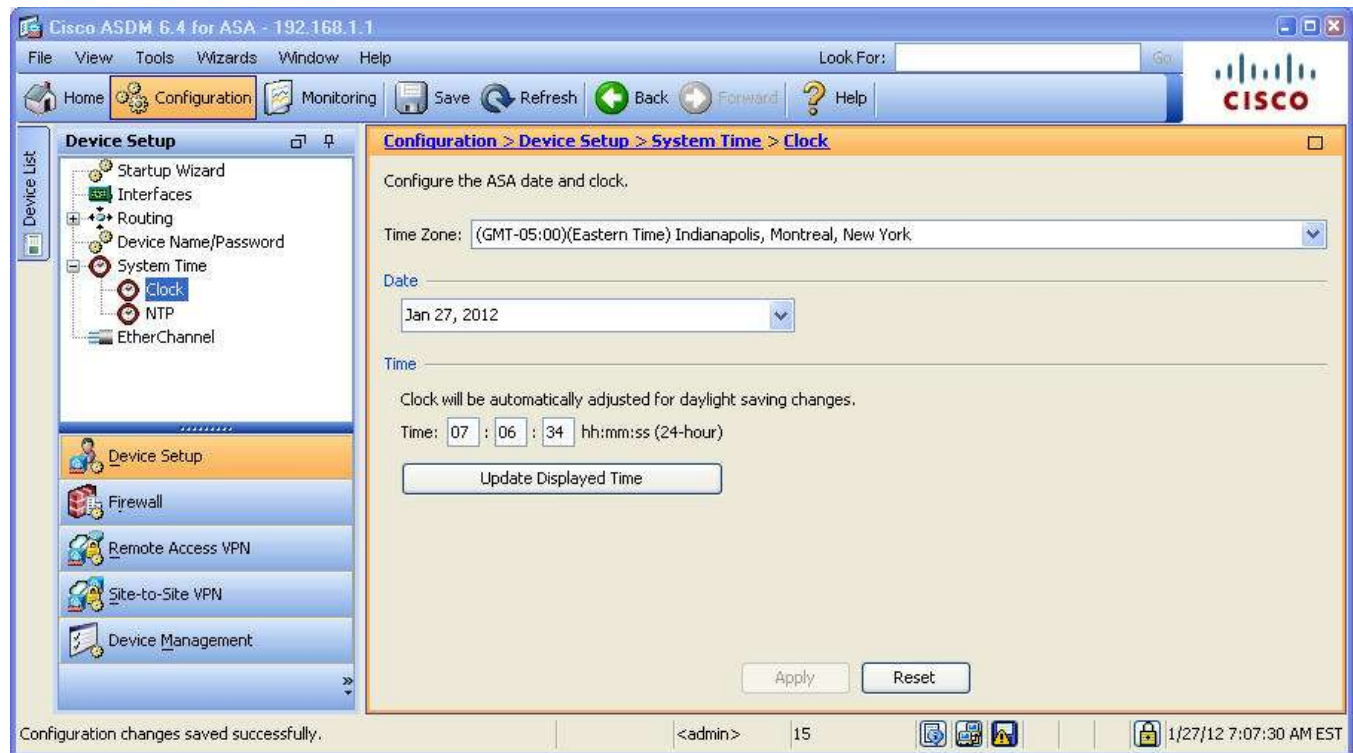


Part 4: Configuring ASA Settings from the ASDM Configuration Menu

In Part 4, you will set the ASA clock, configure a default route, test connectivity using ASDM tools Ping and Traceroute, configure Local AAA user authentication, and modify the MPF application inspection policy.

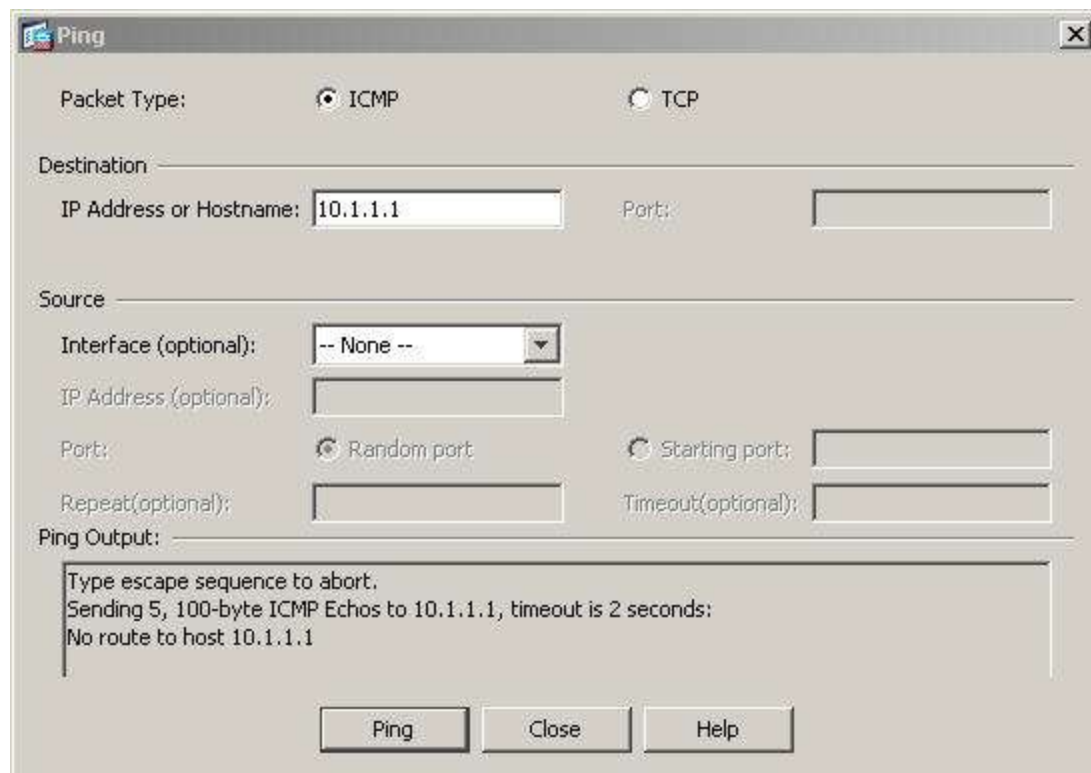
Step 1: Set the ASA date and time.

- From the Configuration screen, Device Setup menu, choose **System Time > Clock**.
- Select your Time Zone from the drop-down menu and enter the current date and time in the fields provided. The clock is a 24-hour clock. Click **Apply** to send the commands to the ASA.



Step 2: Configure a static default route for the ASA.

- a. From the ASDM Tools menu, select **Ping** and enter the IP address of router R1 S0/0/0 (10.1.1.1). The ASA does not have a default route to unknown external networks. The ping should fail because the ASA has no route to 10.1.1.1. Click **Close** to continue.



- b. From the Configuration screen, Device Setup menu, choose **Routing > Static Routes**. Click the **IPv4 Only** button and click **Add** to add a new static route.
- c. In the Add Static Route dialogue box, choose the **outside** interface from the drop down menu. Click the ellipsis button to the right of **Network** and select **any** from the list of network objects, then click **OK**. The selection of **any** translates to a “quad zero” (0.0.0.0 0.0.0.0) route. For the Gateway IP, enter **209.165.200.225** (R1 Fa0/0).

Add Static Route

Interface:

Network:

Gateway IP: Metric:

Options

☒ None

☐ Tunneled (Default tunnel gateway for VPN traffic)

☐ Tracked

Track ID: Track IP Address:

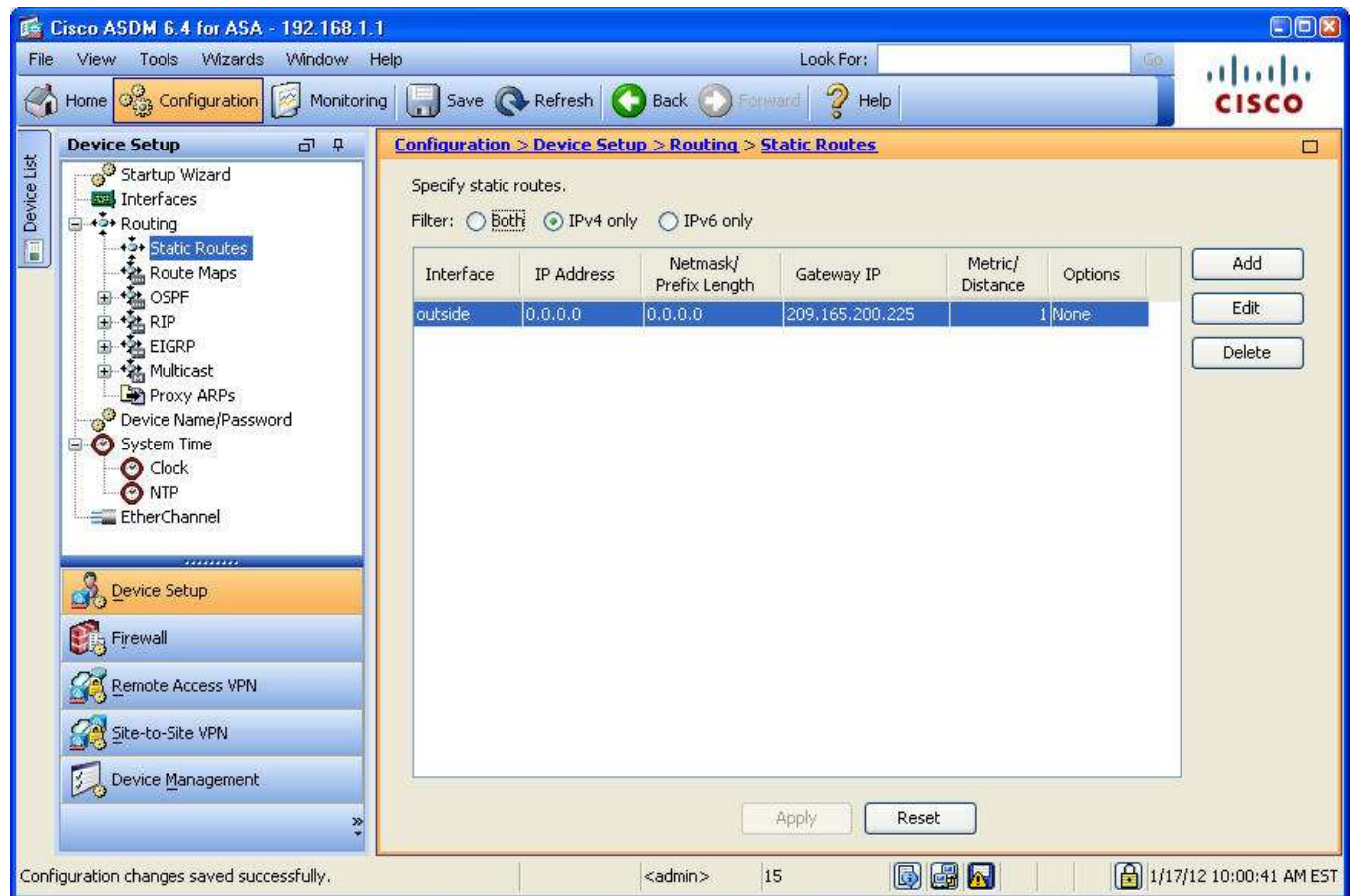
SLA ID: Target Interface:

Monitoring Options

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

OK Cancel Help

- d. Click **OK** and click **Apply** to send the commands to the ASA.



- e. From the ASDM **Tools** menu, select **Ping** and enter the IP address of router R1 S0/0/0 (10.1.1.1). The ping should succeed this time. Click **Close** to continue.
- f. From the ASDM **Tools** menu, select **Traceroute** and enter the IP address of external host PC-C (172.16.3.3). Click on **Trace Route**. The traceroute should succeed and show the hops from the ASA through R1, R2, and R3 to host PC-C. Click **Close** to continue.

The image shows a 'Traceroute' utility window. At the top, the title bar says 'Traceroute'. Below it, the 'Host Name or IP Address' field contains '172.16.3.3'. Under the 'Optional Parameters' section, there are several fields: 'Timeout' (empty, default 3 sec), 'Port' (empty, default 33434), 'Probe' (empty, default 3), and 'Min. & Max. TTL' (empty, defaults 1 and 30). There are also checkboxes for 'Specify source interface or IP address' (unchecked), 'Source Interface' (selected, dropdown shows 'inside'), 'Source IP' (unchecked, empty field), 'Reverse resolve' (checked), and 'Use ICMP' (unchecked). The 'Traceroute Output' section contains a text area with the following text: 'Type escape sequence to abort.', 'Tracing the route to 172.16.3.3', and a list of hops: '1 209.165.200.225 10 msec 0 msec 0 msec', '2 10.1.1.2 10 msec 0 msec 0 msec', '3 10.2.2.1 0 msec 0 msec 0 msec', and '4 172.16.3.3 10 msec 0 msec 0 msec'. At the bottom, there are three buttons: 'Trace Route', 'Close', and 'Help'.

Host Name or IP Address: 172.16.3.3

Optional Parameters

Timeout: (default: 3 sec) ☐ Specify source interface or IP address

Port: (default: 33434) ☒ Source Interface inside

Probe: (default: 3) ☐ Source IP

Min. & Max. TTL: (defaults: 1 and 30) ☒ Reverse resolve ☐ Use ICMP

Traceroute Output

Type escape sequence to abort.
Tracing the route to 172.16.3.3

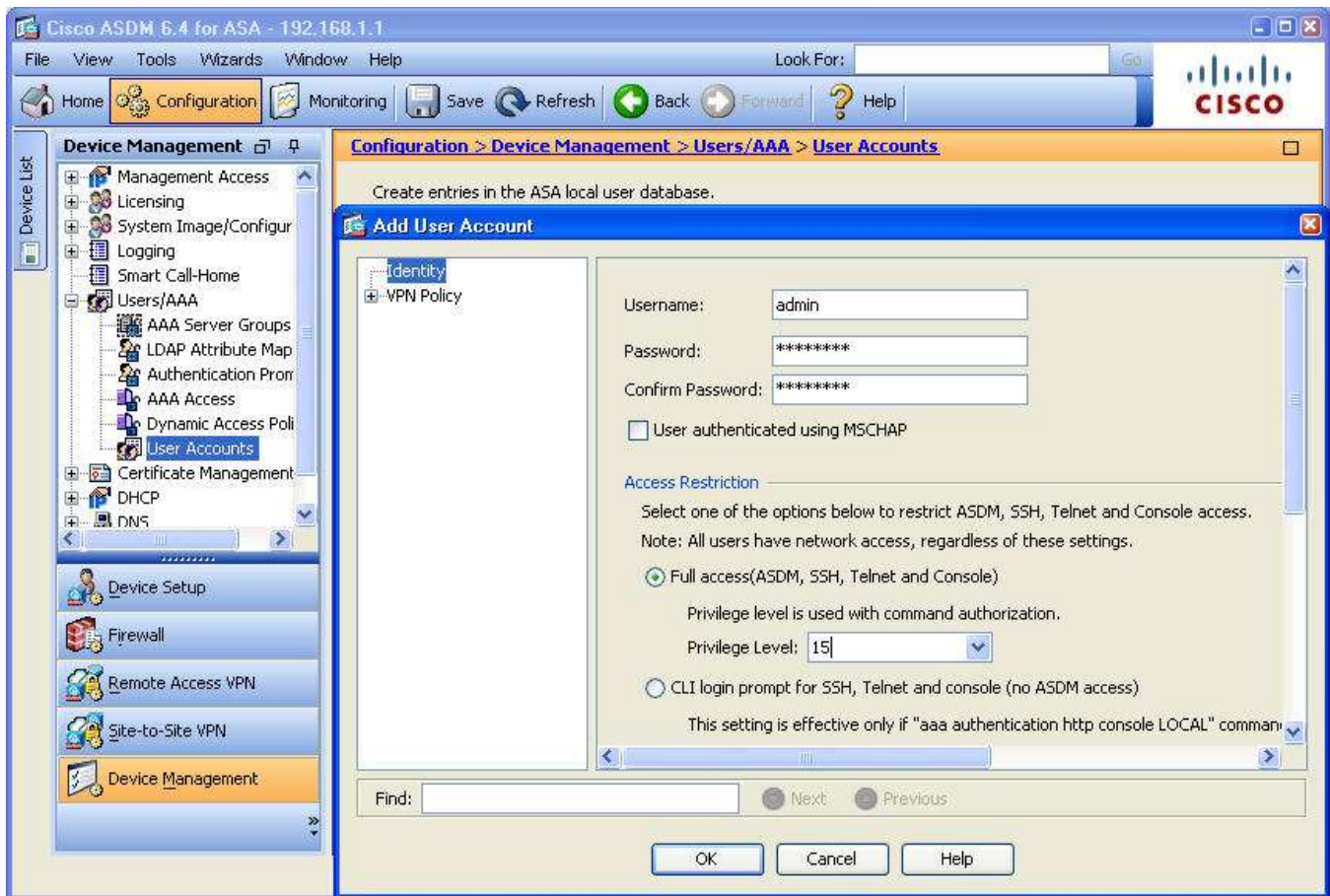
1 209.165.200.225 10 msec 0 msec 0 msec
2 10.1.1.2 10 msec 0 msec 0 msec
3 10.2.2.1 0 msec 0 msec 0 msec
4 172.16.3.3 10 msec 0 msec 0 msec

Trace Route Close Help

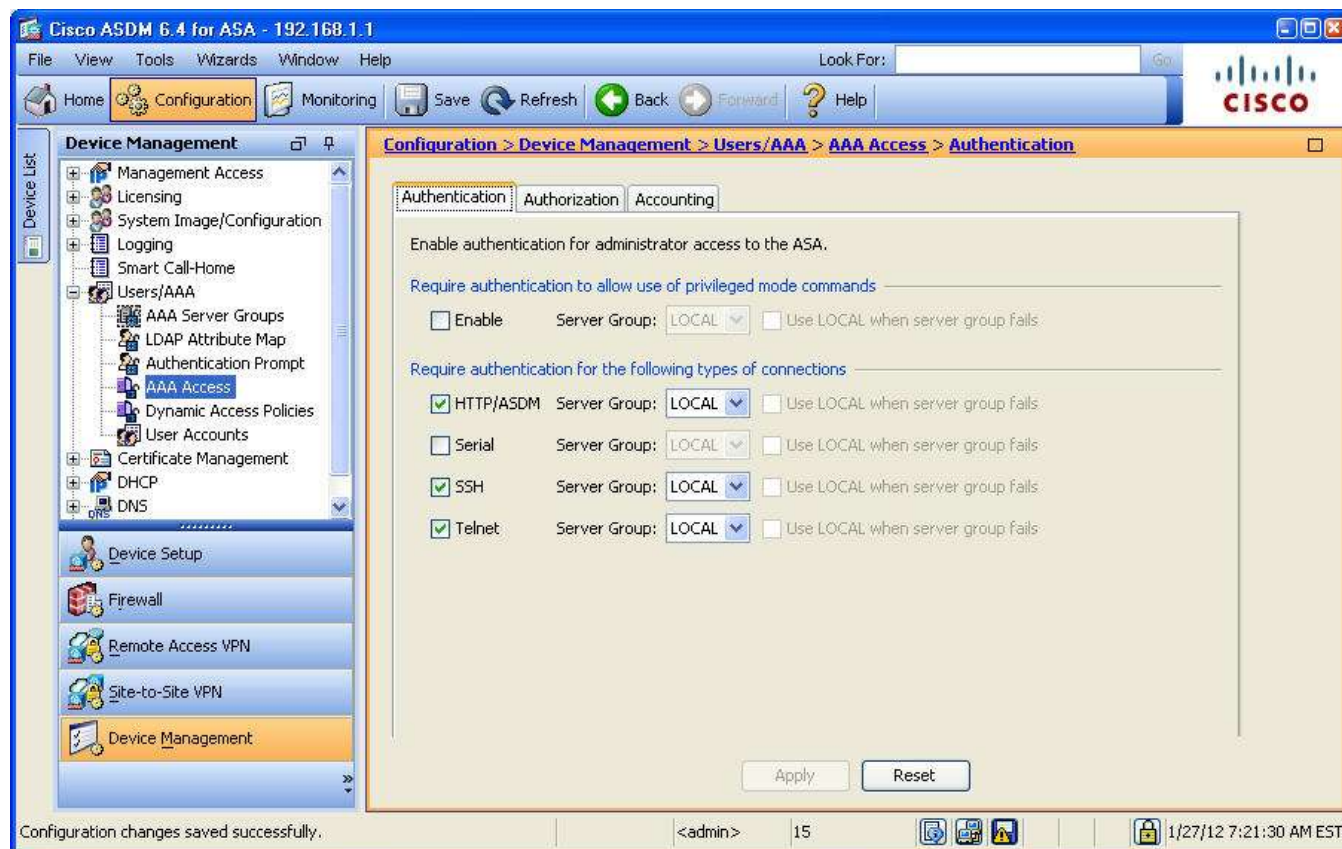
Step 3: Configure AAA user authentication using the local ASA database.

It is necessary to enable AAA user authentication in order to access the ASA using SSH. You allowed SSH access to the ASA from the outside host PC-C when the **Startup wizard** was run. To allow the remote network administrator at PC-C to have SSH access to the ASA, you will create a user in the local database.

- a. From the Configuration screen, Device Management area, click **Users/AAA**. Click **User Accounts** and then **Add**. Create a new user named **admin** with a password of **cisco123** and enter the password again to confirm it. Allow this user **Full access** (ASDM, SSH, Telnet, and console) and set the privilege level to **15**. Click **OK** to add the user and click **Apply** to send the commands to the ASA.



- b. From the Configuration screen, Device Management area, click **Users/AAA**. Click **AAA Access**. On the Authentication tab, select the checkboxes to require authentication for **HTTP/ASDM**, **SSH** and **Telnet** connections and specify the “LOCAL” server group for each connection type. Click **Apply** to send the commands to the ASA.



Note: The next action you attempt within ASDM will require you to login as **admin** with password **cisco123**.

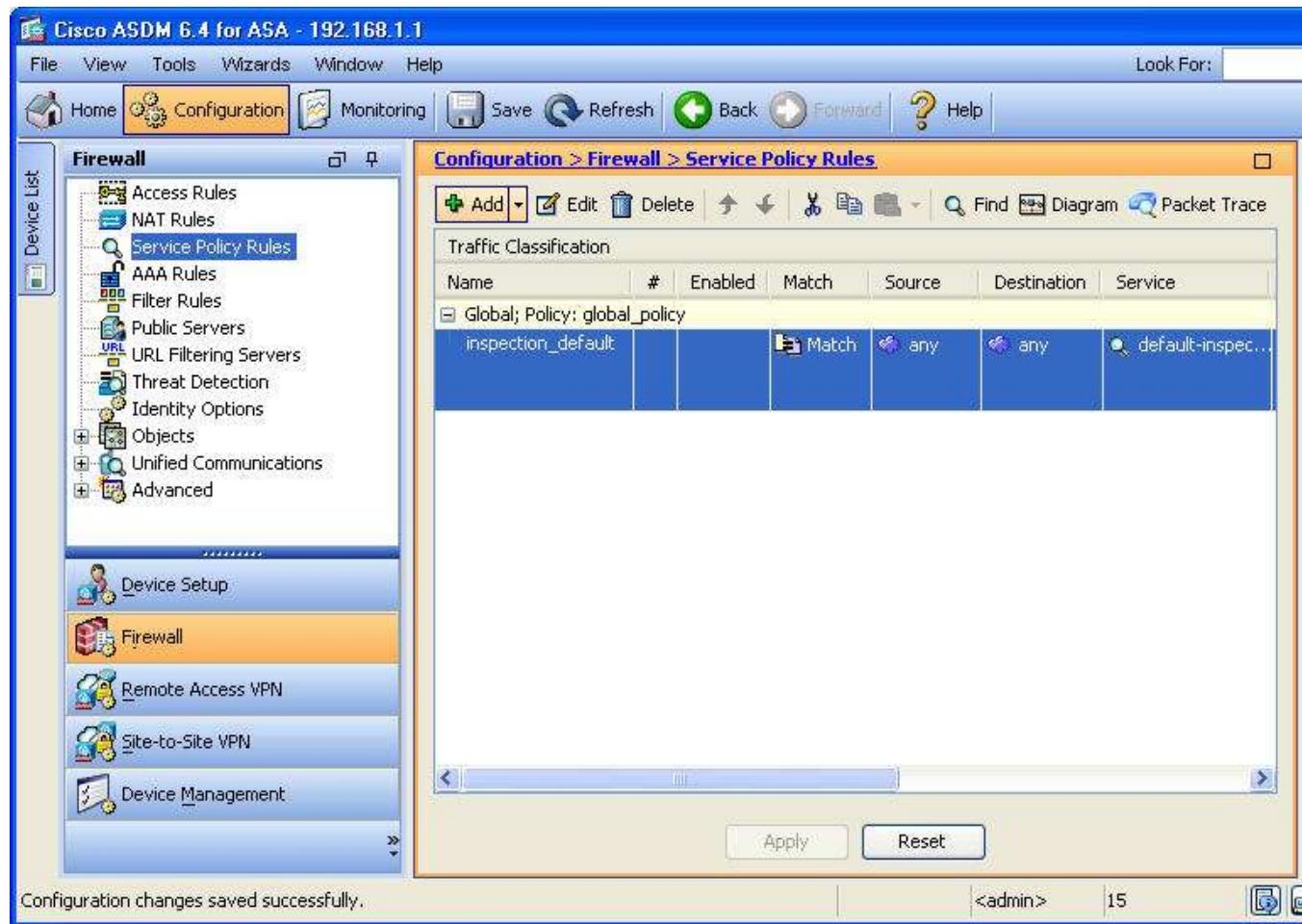
- c. From PC-C, open an SSH client such as PuTTY and attempt to access the ASA outside interface at 209.165.200.226. You should be able to establish the connection. When prompted to login, enter user name **admin** and password **cisco123**.
- d. After logging in to the ASA using SSH, enter the **enable** command and provide the password **class**. Issue the **show run** command to display the current configuration you have created using ASDM.

Note: The default timeout for Telnet and SSH is 5 minutes. You can increase this setting using the CLI as described in Lab 10A or go to ASDM **Device Management > Management Access > ASDM/HTTP/Telnet/SSH**.

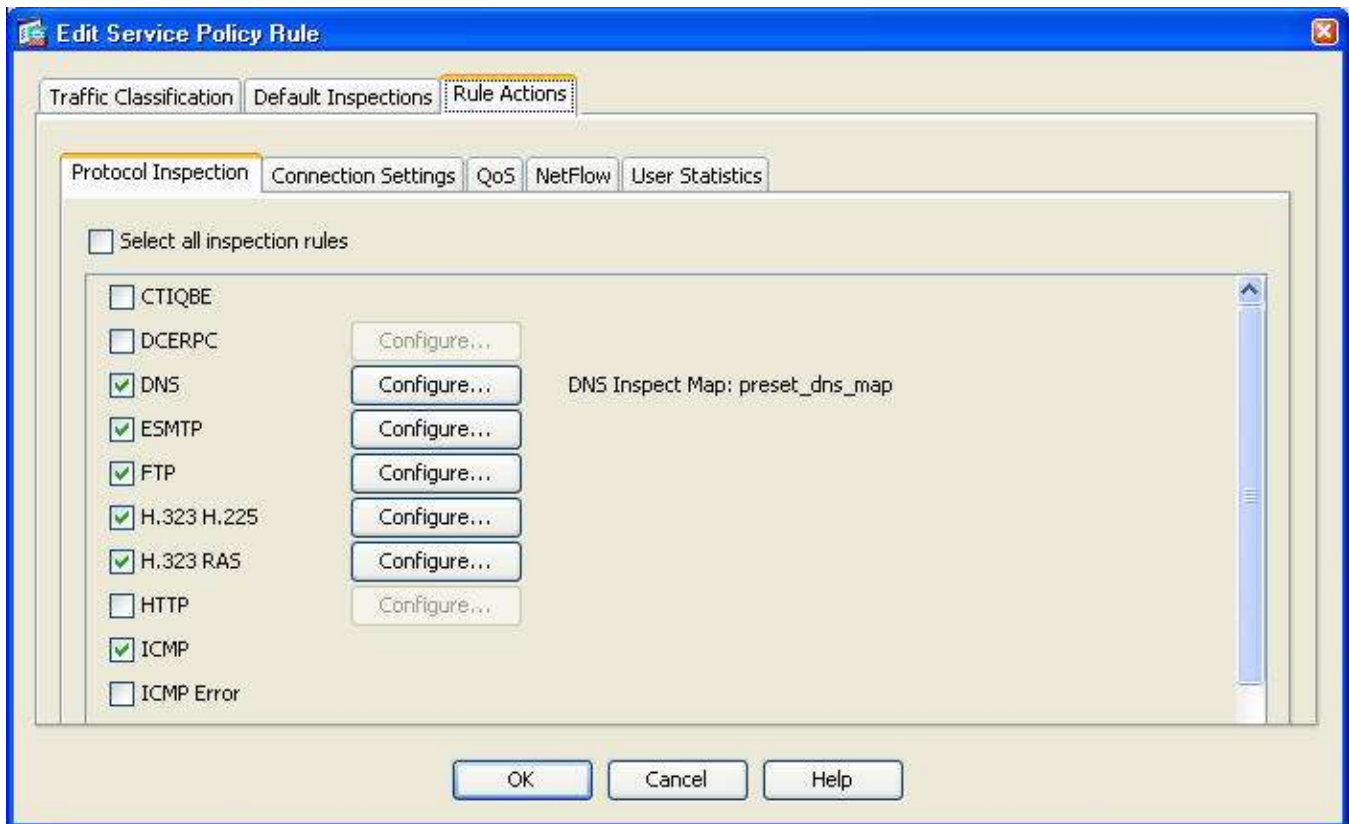
Step 4: Modify the MPF application inspection policy.

For application layer inspection, as well as other advanced options, the Cisco Modular Policy Framework (MPF) is available on ASAs.

- a. The default global inspection policy does not inspect ICMP. To enable hosts on the internal network to ping external hosts and receive replies, ICMP traffic must be inspected. From the **Configuration** screen, Firewall area menu, click **Service Policy Rules**.



- b. Select the **inspection_default** policy and click **Edit** to modify the default inspection rules. On the Edit Service Policy Rule window, click the **Rule Actions** tab and select the checkbox for **ICMP**. Do not change the other default protocols that are checked. Click **OK** and then click **Apply** to send the commands to the ASA. If prompted, login as again **admin** with a password of **cisco123**.



- c. From PC-B, **ping** the external interface of R1 S0/0/0 (10.1.1.1). The pings should be successful.

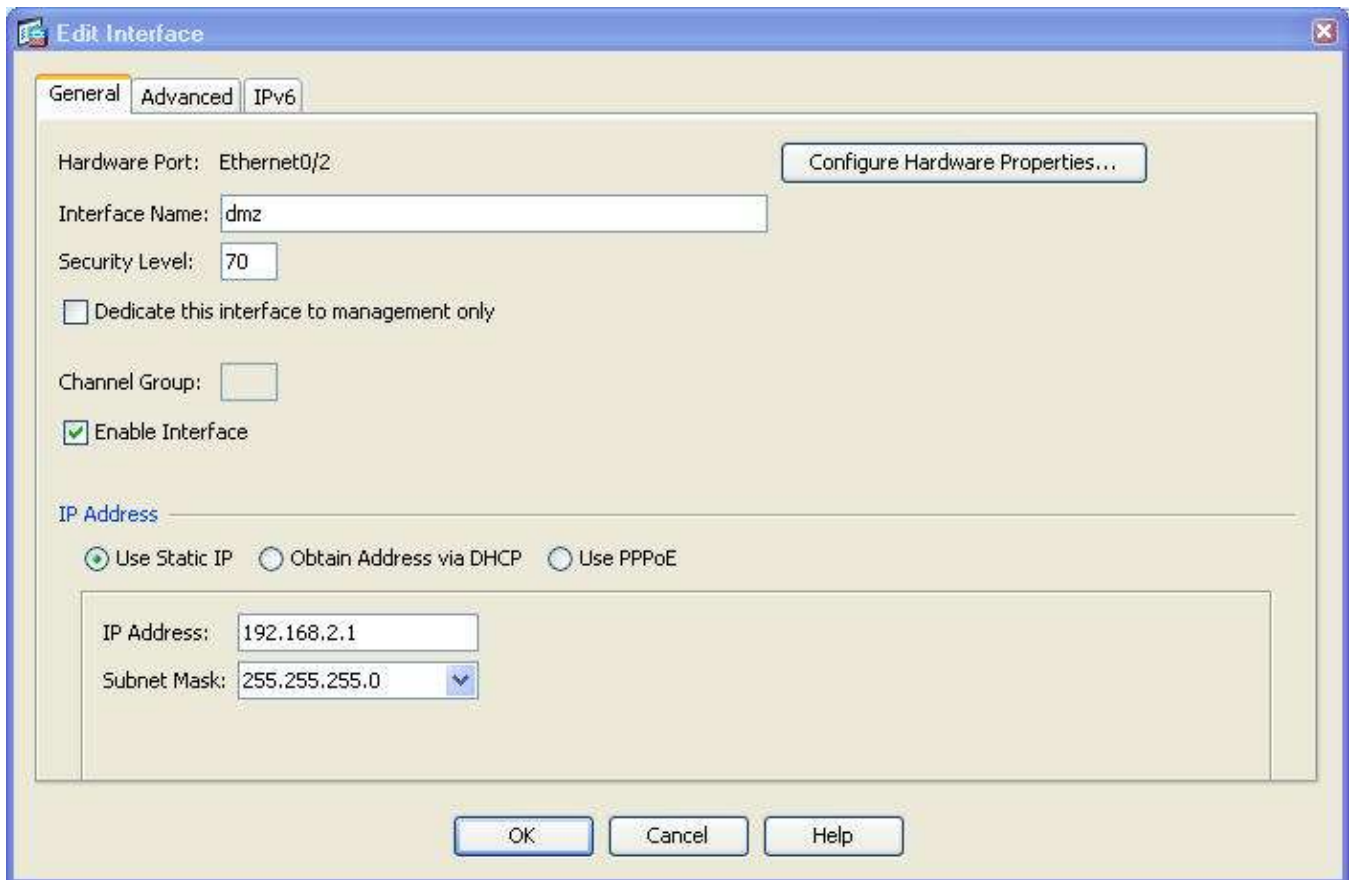
Part 5: Configuring a DMZ, Static NAT and ACLs

In Part 3 of this lab, you configured address translation using PAT for the inside network. In this part, you create a DMZ on the ASA, configure static NAT to a DMZ server, and apply an ACL to control access to the server.

Step 1: Configure the ASA DMZ interface.

In this step you will configure a new interface E0/2 named **dmz**, set the security level to 70, and bring the interface up.

- From the Configuration screen, Device Setup menu, click **Interfaces**. Select interface Ethernet0/2 and click **Edit**.
- In the Edit Interface dialog box, the General tab is displayed by default. Name the interface **dmz**, assign it a security level of **70**, and make sure the **Enable Interface** checkbox is checked.
- Ensure that the **Use Static IP** button is selected and enter an IP address of **192.168.2.1** with a subnet mask of **255.255.255.0**. Click **OK**. When the Security Level Change warning is displayed, read it and then click **OK** again. On the Interfaces screen, click **Apply** to send the commands to the ASA.



Edit Interface

General | Advanced | IPv6

Hardware Port: Ethernet0/2 Configure Hardware Properties...

Interface Name:

Security Level:

☐ Dedicate this interface to management only

Channel Group:

☒ Enable Interface

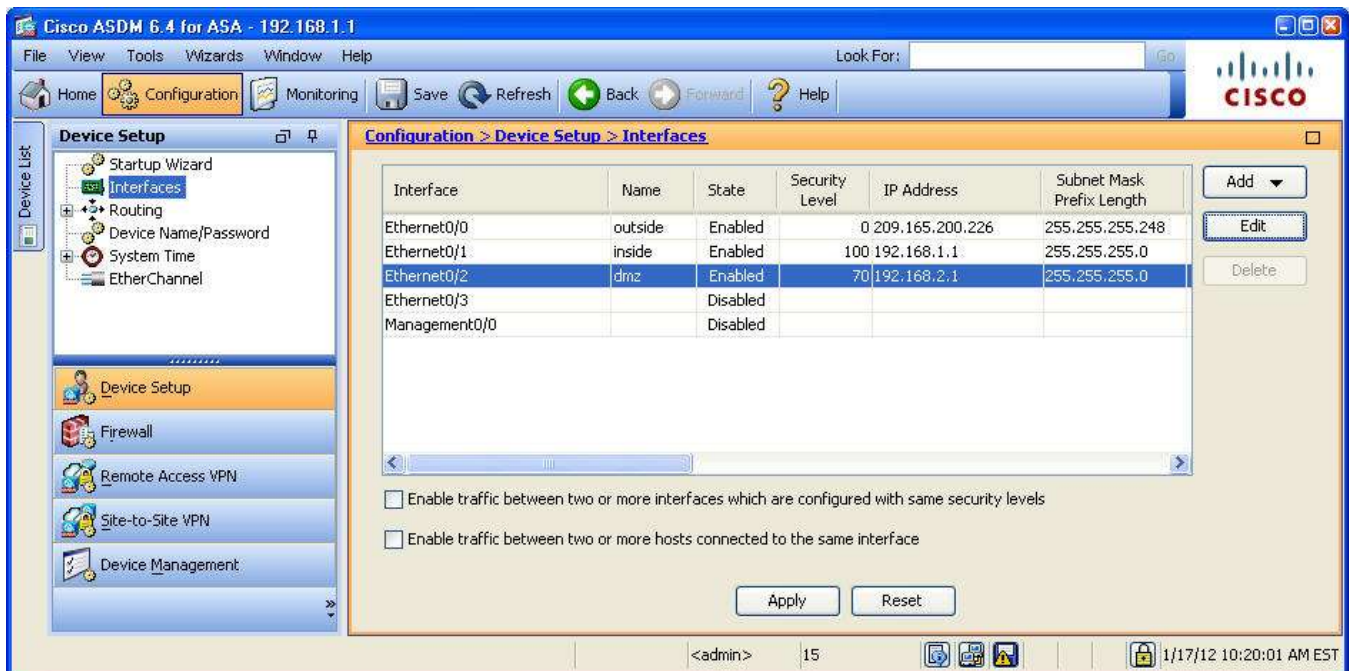
IP Address

☒ Use Static IP ☐ Obtain Address via DHCP ☐ Use PPPoE

IP Address:

Subnet Mask:

OK Cancel Help



Cisco ASDM 6.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Look For: Go

Home Configuration Monitoring Save Refresh Back Forward ? Help

Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length
Ethernet0/0	outside	Enabled	0	209.165.200.226	255.255.255.248
Ethernet0/1	inside	Enabled	100	192.168.1.1	255.255.255.0
Ethernet0/2	dmz	Enabled	70	192.168.2.1	255.255.255.0
Ethernet0/3		Disabled			
Management0/0		Disabled			

☐ Enable traffic between two or more interfaces which are configured with same security levels

☐ Enable traffic between two or more hosts connected to the same interface

Apply Reset

<admin> 15 1/17/12 10:20:01 AM EST

Step 2: Configure the DMZ server and static NAT.

To accommodate the addition of a DMZ and a web server, you will use another address from the ISP range assigned, 209.165.200.224/29 (.224-.231). Router R1 Fa0/0 and the ASA outside interface are

already using 209.165.200.225 and .226, respectively. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

- a. From the Configuration screen, Firewall menu, click the **Public Servers** option and click **Add** to define the DMZ server and services offered. In the Add Public Server dialog box, specify the Private Interface as **dmz**, the Public Interface as **outside** and the Public IP address as **209.165.200.227**.

Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.

Private Interface:

Private IP Address:

Private Service:

Public Interface:

Public IP Address:

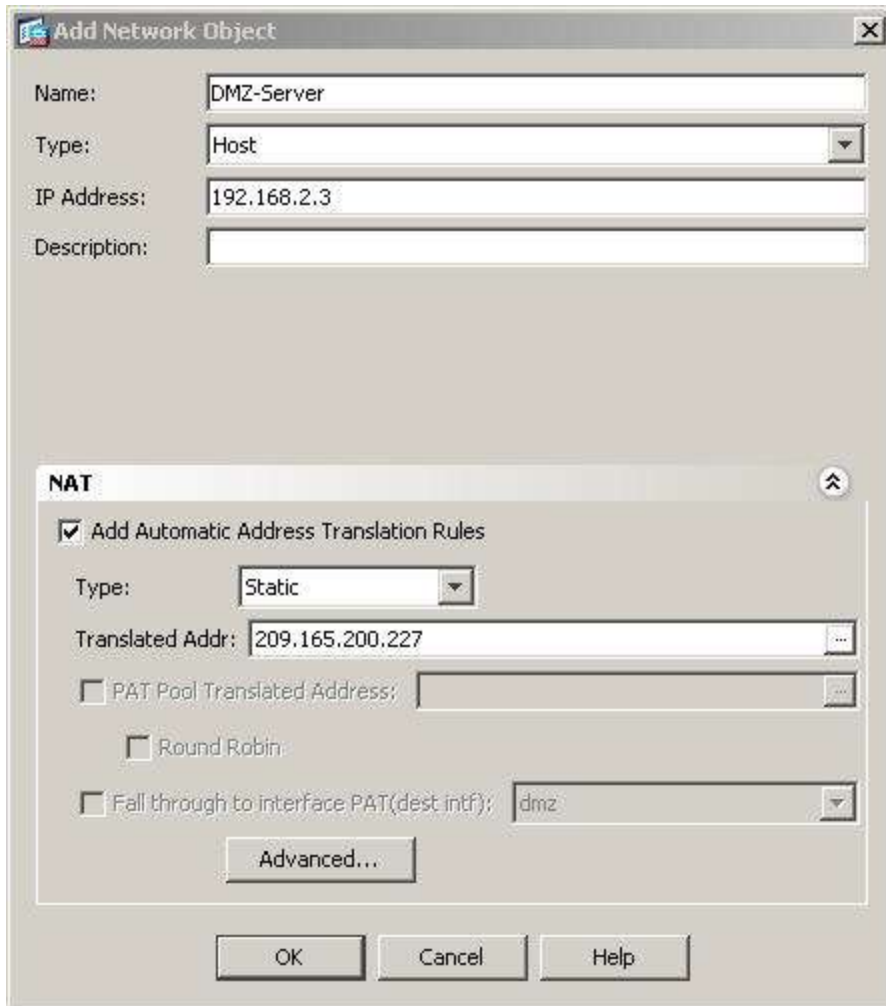
Options

☐ Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only)

OK Cancel Help

- b. Click the ellipsis button to the right of Private IP Address. In the Browse Private IP Address window, click **Add** to define the server as a **Network Object**. Enter the name **DMZ-Server**, with a Type of **Host** and the Private IP Address of **192.168.2.3**.
- c. While in the Add Network Object dialog box, click the double down arrow button for **NAT**. Click the checkbox for **Add Automatic Address Translation Rules** and enter the type as **Static**. Enter Translated Addr: **209.165.200.227**. When the screen looks like the following, click **OK** to add the server network object. From the Browse Private IP Address window, click **OK**. You will return to the Add Public Server dialog box.



The image shows a screenshot of the 'Add Network Object' dialog box in a network configuration tool. The dialog has a title bar with a close button. It contains several input fields: 'Name' with the value 'DMZ-Server', 'Type' with a dropdown menu showing 'Host', 'IP Address' with the value '192.168.2.3', and an empty 'Description' field. Below these fields is a section titled 'NAT' with an expand/collapse arrow. Inside the NAT section, there is a checked checkbox for 'Add Automatic Address Translation Rules'. Below this, there is a 'Type' dropdown menu showing 'Static', a 'Translated Addr' field with the value '209.165.200.227' and an ellipsis button, a disabled 'PAT Pool Translated Address' field, a disabled 'Round Robin' checkbox, and a disabled 'Fall through to interface PAT(dest intf):' dropdown menu showing 'dmz'. There is an 'Advanced...' button below the NAT section. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Add Network Object

Name: DMZ-Server

Type: Host

IP Address: 192.168.2.3

Description:

NAT

☒ Add Automatic Address Translation Rules

Type: Static

Translated Addr: 209.165.200.227

☐ PAT Pool Translated Address:

☐ Round Robin

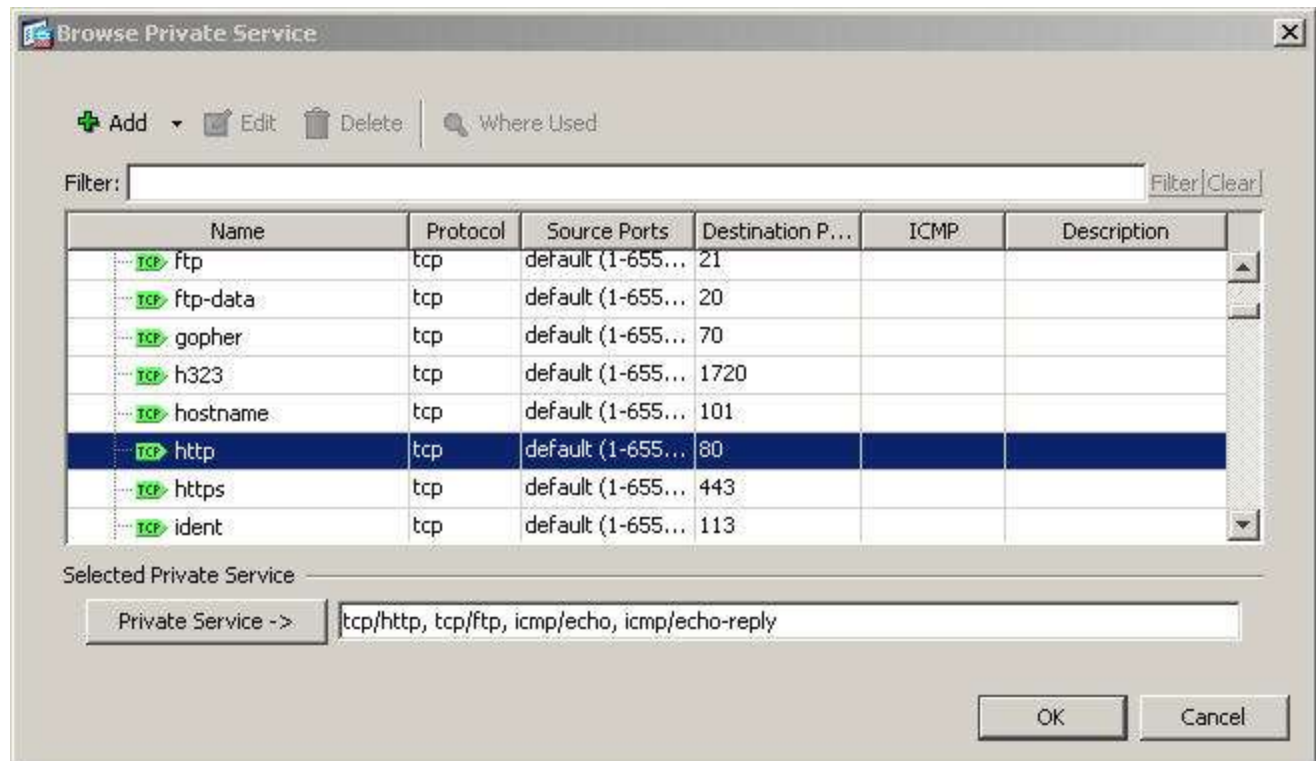
☐ Fall through to interface PAT(dest intf): dmz

Advanced...

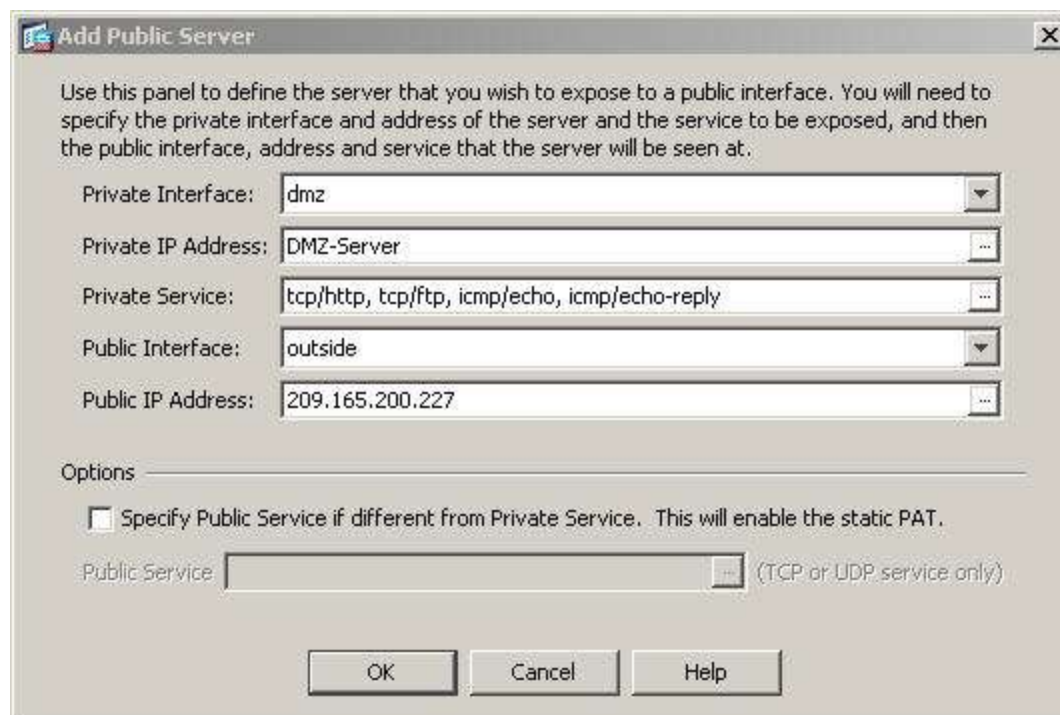
OK Cancel Help

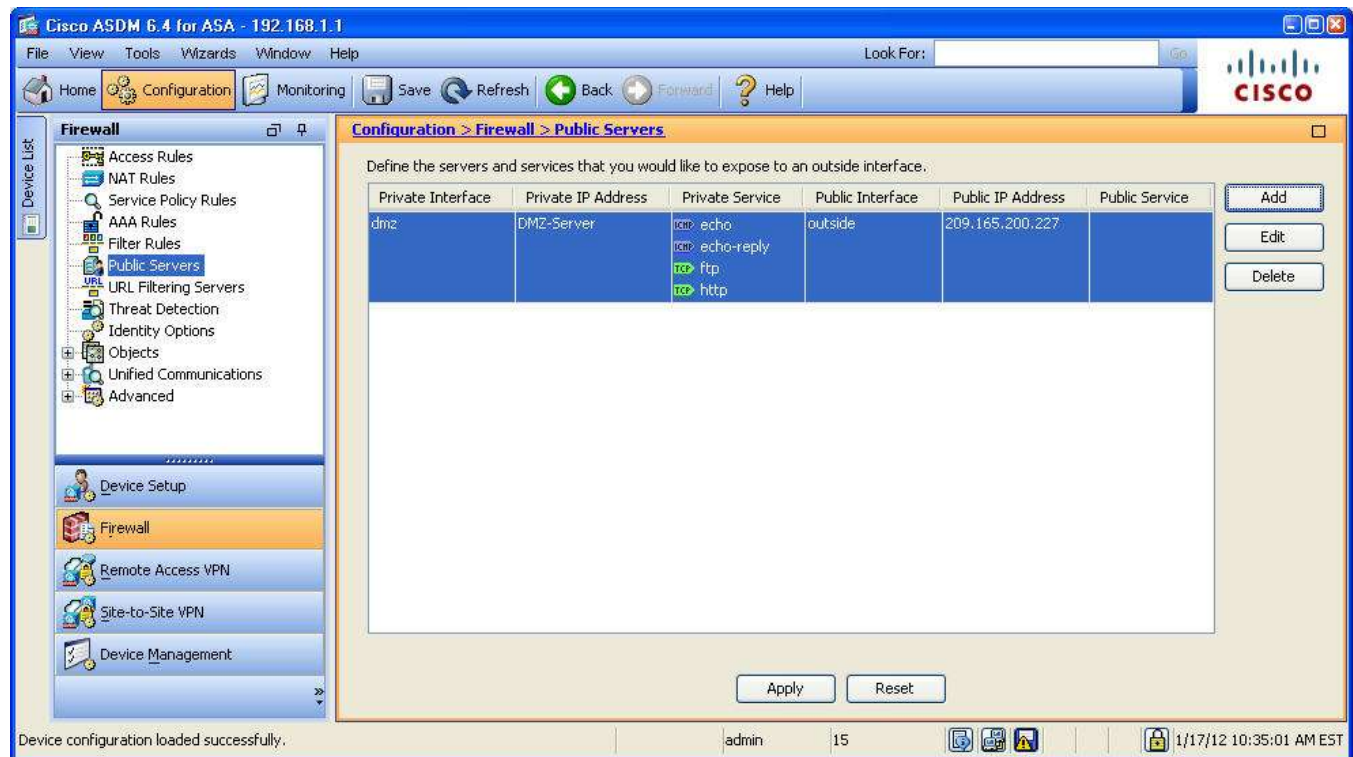
- d. In the Add Public Server dialog, click the ellipsis button to the right of Private Service. In the Browse Private Service window, double click to select the following services: **tcp/http**, **tcp/ftp**, **icmp/echo** and **icmp/echo-reply** (scroll down to see all services). Click **OK** to continue and return to the **Add Public Server** dialog.

Note: You can specify Public services if different from the Private services, using the option on this screen.



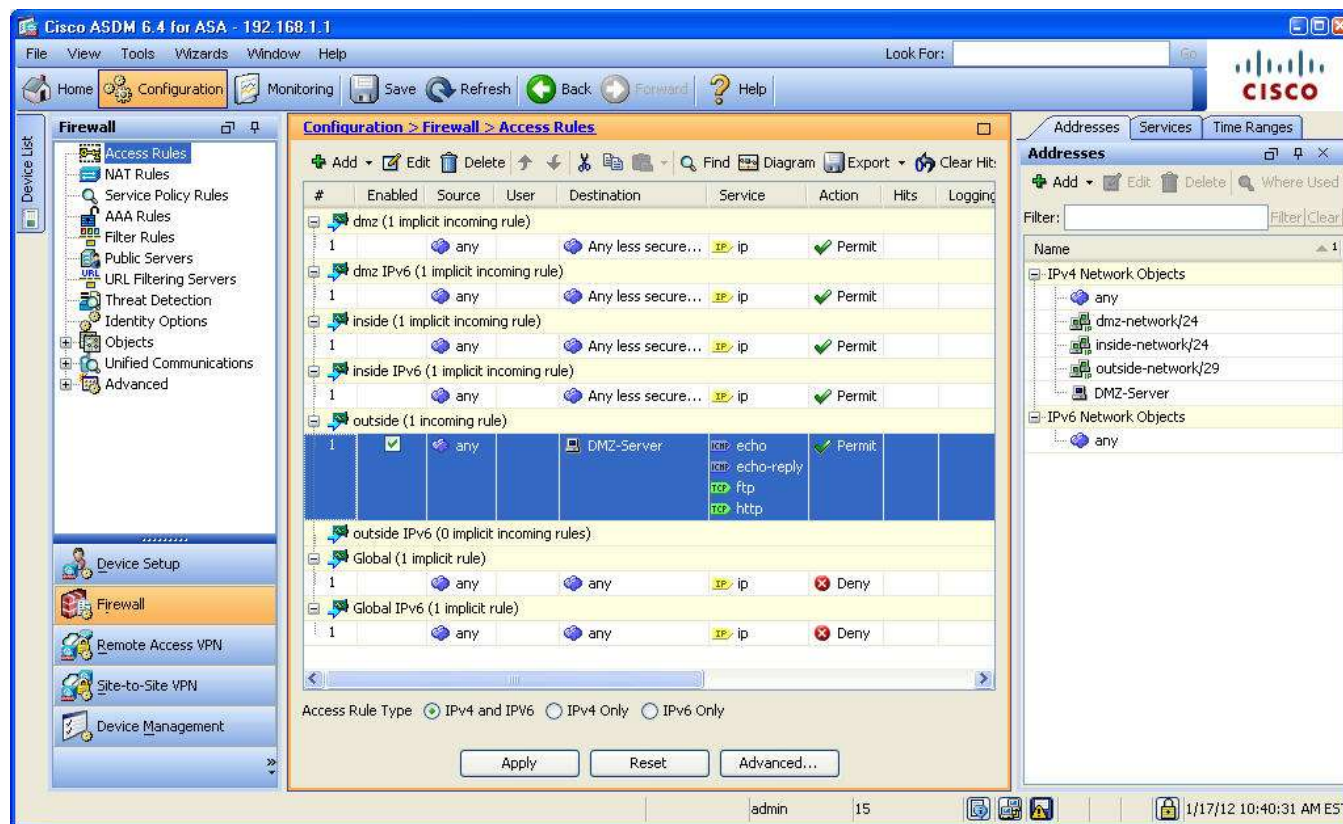
- e. When you have completed all information in the Add Public Server dialog box, it should look like the one shown below. Click **OK** to add the server. Click **Apply** at the Public Servers screen to send the commands to the ASA.





Step 3: View the DMZ Access Rule (ACL) generated by ASDM.

- With the creation of the DMZ server object and selection of services, ASDM automatically generates an Access Rule (ACL) to permit the appropriate access to the server and applies it to the outside interface in the incoming direction.
- View this Access Rule in ASDM by choosing **Configuration > Firewall > Access Rules**. It appears as an outside incoming rule. You can select the rule and use the horizontal scroll bar to see all of the components.



- c. **Note:** You can also see the actual IOS commands generated using the **ASDM Tools > Command Line Interface** and entering the command **show run**.

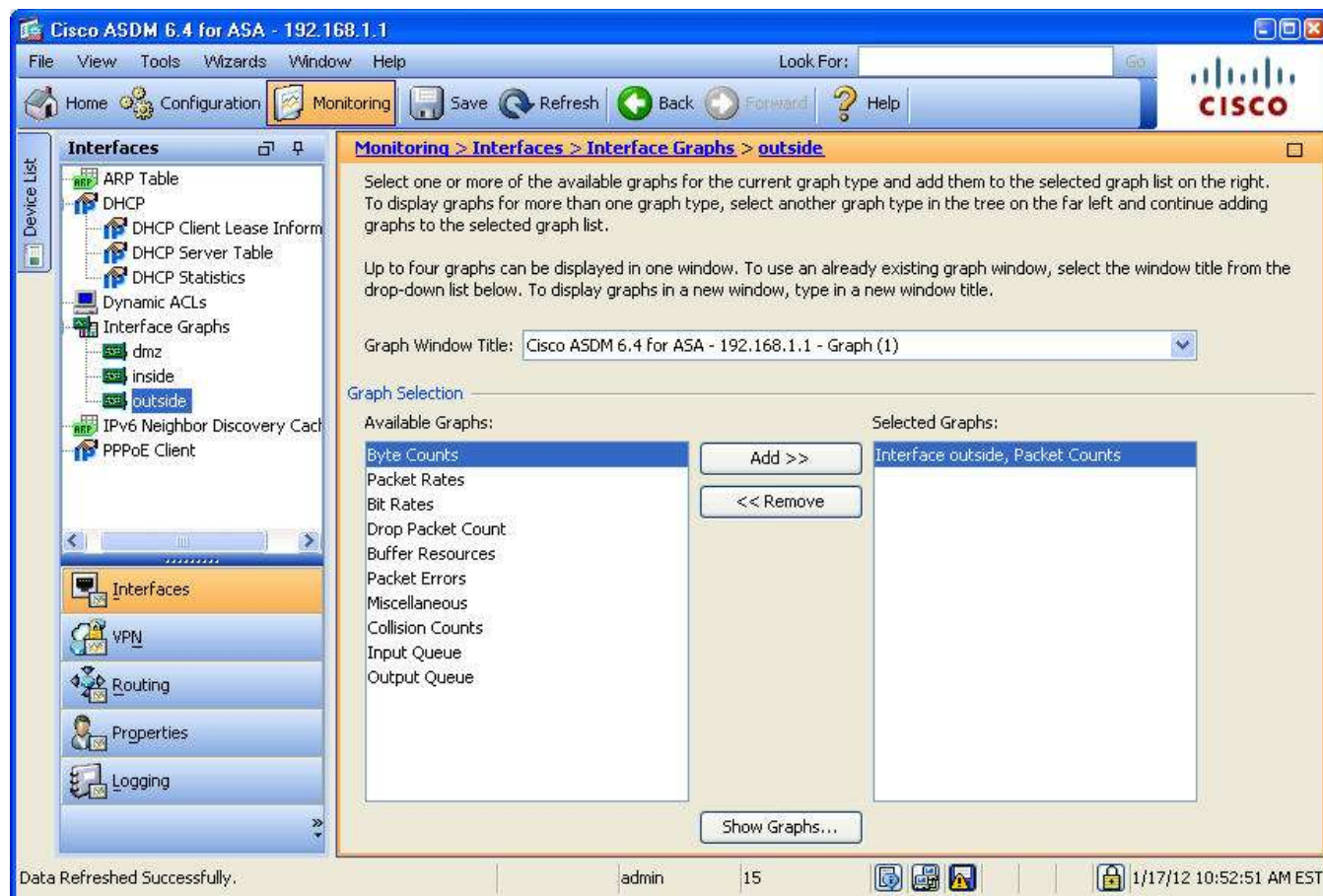
Step 4: Test access to the DMZ server from the outside network.

- From PC-C, ping the IP address of the static NAT public server address (209.165.200.227). The pings should be successful.
- Because the ASA inside interface E0/1 is set to security level 100 (the highest) and the DMZ interface E0/2 is set to 70, you can also access the DMZ server from a host on the inside network. The ASA acts like a router between the two networks. Ping the DMZ server (PC-A) internal address (192.168.2.3) from inside network host PC-B (192.168.1.3 or DHCP assigned address). The pings should be successful due to interface security level and the fact that ICMP is being inspected on the inside interface by the global inspection policy.
- The DMZ server cannot ping PC-B on the inside network. This is because the DMZ interface E0/2 has a lower security level (70) than inside interface E0/1 (100). Try to ping from the DMZ server PC-A to PC-B at IP address 192.168.1.X. The pings should not be successful.

Step 5: Use ASDM Monitoring to graph packet activity.

There are a number of aspects of the ASA that can be monitored using the **Monitoring** screen. The main categories on this screen are **Interfaces**, **VPN**, **Routing**, **Properties**, and **Logging**. In this step you will create a graph to monitor packet activity for the ASA outside interface.

- From the Monitoring screen, Interfaces menu, click **Interface Graphs > outside**. Select **Packet Counts** and click **Add** to add the graph. The exhibit below shows Packet Counts added.



- b. Click the **Show Graphs** button to display the graph. Initially there is no traffic displayed.
- c. From a privileged mode command prompt on R2, simulate Internet traffic to the ASA by pinging the DMZ server public address with a repeat count of 1000. You can increase the number of pings if desired.

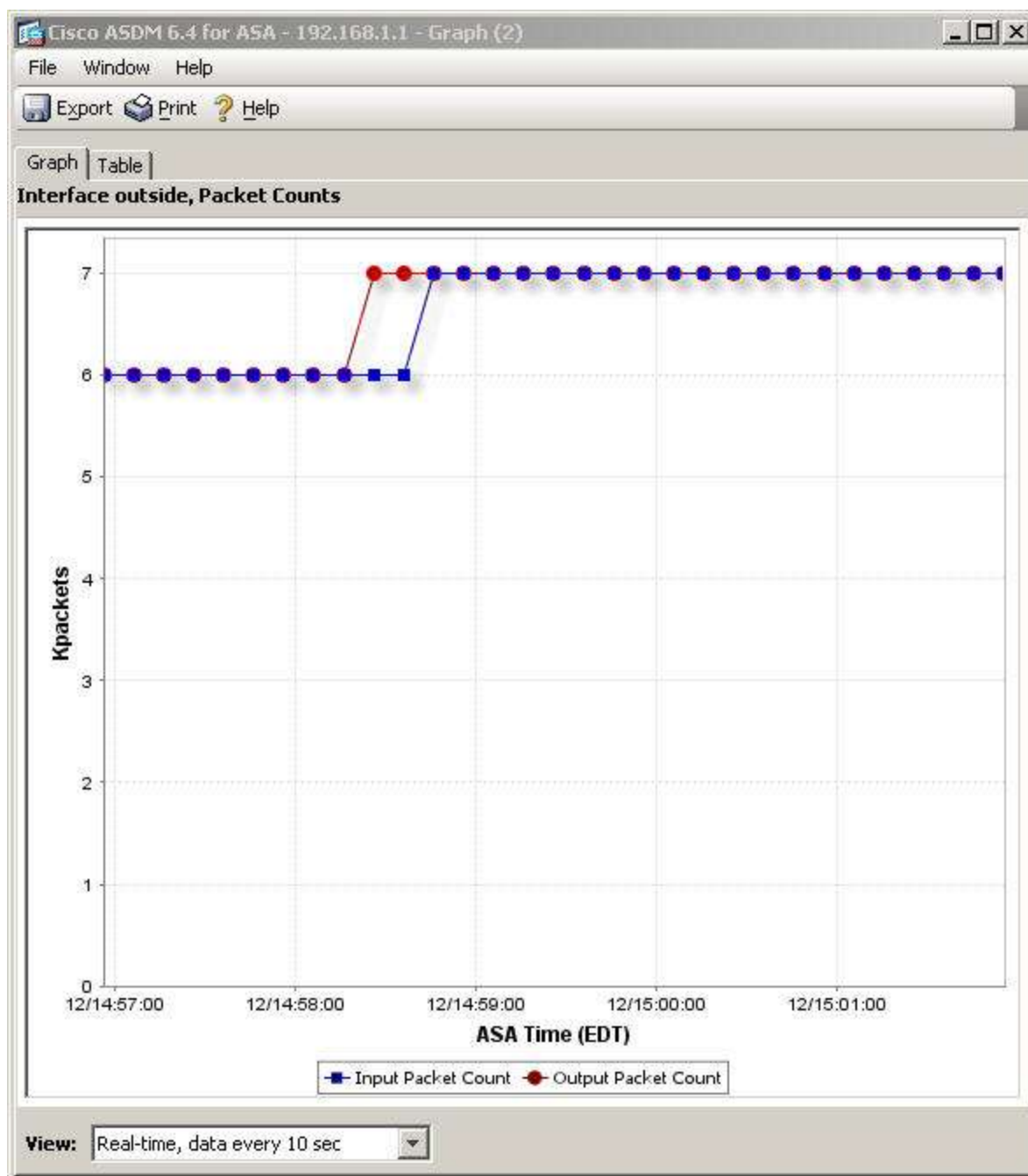
R2# **ping 209.165.200.227 repeat 1000**

```
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/12 ms
```

- d. You should see the results of the pings from R2 on the graph as an Input Packet Count. The scale of the graph is automatically adjusted depending on the volume of traffic. You can also view the data in tabular form by clicking the **Table** tab. Notice that the View selected at the bottom left of the Graph screen is Real-time, data every 10 seconds. Click the pull-down menu to see the other options available.
- e. Ping from PC-B to R1 Fa0/0 at 209.165.200.225 using the **-n** option (number of packets) to specify 1000 packets.

C:\> **ping 209.165.200.225 -n 1000**

Note: The response from the PC is relatively slow and it may take a while to show up on the graph as Output Packet Count. The graph below shows an additional 5000 input packets as well as both input and output packet counts.



Reflection:

1. What are some benefits to using ASDM over the CLI?

2. What are some benefits to using the CLI over ASDM?

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				