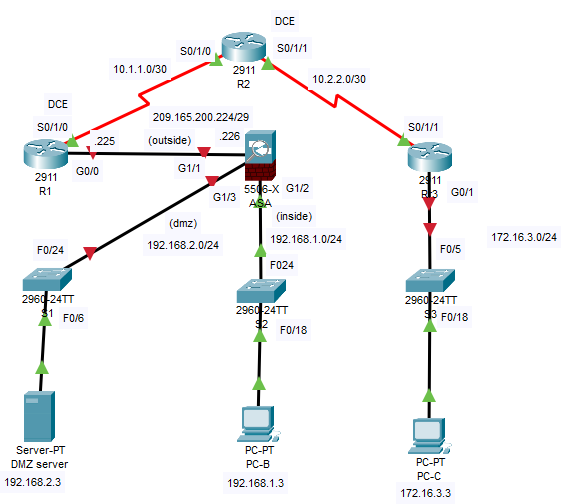
Packet Tracer - Configuring ASA Basic Settings and Firewall Using CLI (ASA-5506-X)

1. Topology



1. IP Addressing Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway | Switch Port |
| R1 | G0/0 | 209.165.200.225 | 255.255.255.248 | N/A | ASA G1/1 |
| S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A | N/A |
| R2 | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A | N/A |
| S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A | N/A |
| R3 | G0/1 | 172.16.3.1 | 255.255.255.0 | N/A | S3 F0/5 |
| S0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A | N/A |
| ASA | G1/2 | 192.168.1.1 | 255.255.255.0 | NA | S2 F0/24 |
| ASA | G1/1 | 209.165.200.226 | 255.255.255.248 | NA | R1 G0/0 |
| ASA | G1/3 | 192.168.2.1 | 255.255.255.0 | NA | S1 F0/24 |
| DMZ Server | NIC | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | S1 F0/6 |
| PC-B | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | S2 F0/18 |
| PC-C | NIC | 172.16.3.3 | 255.255.255.0 | 172.16.3.1 | S3 F0/18 |

1. Objectives

Part 1: Basic Router/Switch/PC Configuration

* Configure hostnames and interface IP addresses for routers, switches, and PCs.
* Configure static routing, including default routes, between R1, R2, and R3.
* Enable SSH access for R1.
* Configure PC host IP settings.
* Verify connectivity between hosts, switches, and routers.
* Save the basic running configuration for each router and switch.

. Part 2: Accessing the ASA Console and Using CLI Setup Mode to Configure Basic Settings

* Access the ASA console and view hardware, software, and configuration settings.
* Determine the ASA version, interfaces, and license.
* Determine the file system and contents of flash memory.

Part 3: Configuring Basic ASA Settings and Interface Security Levels Using the CLI.

* Configure the hostname and domain name.
* Configure the login and enable passwords.
* Set the date and time.
* Configure the inside and outside interfaces.
* Test connectivity to the ASA.
* Configure SSH access to the ASA.
* Configure HTTPS access on the ASA for ASDM.

Part 4: Configuring Routing, Address Translation, and Inspection Policy Using the CLI

* Configure a static default route for the ASA.
* Configure PAT and network objects.
* Modify the MPF application inspection global service policy.

**Part 5: Configuring DHCP, AAA, and SSH**

* Configure the ASA as a DHCP server/client.
* Configure Local AAA user authentication.
* Configure SSH remote access to the AAA.

Part 6: Configuring DMZ, Static NAT, and ACLs

* Configure the DMZ interface VLAN 3 on the ASA.
* Configure static NAT for the DMZ server using a network object.
* Configure an ACL to allow access to the DMZ for Internet users.
* Verify access to the DMZ server for external and internal users.

1. Scenario

Your company has one location connected to an ISP. R1 represents a CPE device managed by the ISP. R2 represents an intermediate Internet router. R3 represents an ISP that connects an administrator from a network management company, who has been hired to remotely manage your network. 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 and by the remote administrator. Layer 3 VLAN interfaces provide access to the three areas created in the activity: Inside, Outside, and DMZ. The ISP assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA.

**Note**: This Packet Tracer activity is not a substitute for the ASA labs. This activity provides additional practice and simulates most of the ASA 5506 configurations. When compared to a real ASA 5506, there may be slight differences in command output or commands that are not yet supported in Packet Tracer.

1. Configure Basic Device Settings

In Part 1, 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 ASA settings at this time.

* + 1. Configure basic settings for routers and switches.
       1. Configure hostnames, as shown in the topology, for each router.
       2. Configure router interface IP addresses, as shown in the IP Addressing table.
       3. Configure a clock rate for routers with a DCE serial cable attached to the serial interface. R1 is shown here as an example.

R1(config)# **interface S0/1/0**

R1(config-if)# **clock rate 128000**

* + - 1. Configure the hostname for the switches. With the exception of the hostname, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.
    1. Configure static routing on the routers.
       1. 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 10.1.1.2**

R3(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

* + - 1. Configure a static route from R2 to the R1 G0/0/1 subnet (connected to ASA interface G1/5) and a static route from R2 to the R3 LAN.

R2(config)# **ip route 209.165.200.224 255.255.255.248 10.1.1.1**

R2(config)# **ip route 172.16.3.0 255.255.255.0 10.2.2.1**

* + 1. Enable the HTTP server and configure a user account, encrypted passwords, and crypto keys for SSH.

**Note**: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the purposes of this lab. More complex passwords are recommended in a production network.

* + - 1. Enable HTTP access to R1 using the **ip http server** command in global config mode. Set the console and VTY passwords to cisco. This will provide web and SSH targets for testing later in the lab.

R1(config)# **ip http server (Cannot do this in PT)**

Configure a minimum password length of 10 characters using the **security passwords** command.

R1(config)# **security passwords min-length 10**

* + - 1. Configure a domain name.

R1(config)# **ip domain-name ccnasecurity.com**

* + - 1. Configure crypto keys for SSH.

R1(config)# **crypto key generate rsa general-keys modulus 1024**

* + - 1. Configure an admin01 user account using algorithm-type scrypt for encryption and a password of admin01pass.

R1(config)# **username admin01 algorithm-type scrypt secret admin01pass**

* + - 1. Configure line console 0 to use the local user database for logins. For additional security, the **exec-timeout** command causes the line to log out after five minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.

**Note**: To avoid repetitive logins during this lab, the **exec-timeout** command can be set to 0 0, which prevents it from expiring. However, this is not considered to be a good security practice.

R1(config)# **line console 0**

R1(config-line)# **login local**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **logging synchronous**

* + - 1. Configure line vty 0 4 to use the local user database for logins and restrict access to only SSH connections.

R1(config)# **line vty 0 4**

R1(config-line)# **login local**

R1(config-line)# **transport input ssh**

R1(config-line)# **exec-timeout 5 0**

* + - 1. Configure the enable password with strong encryption.

R1(config)# **enable algorithm-type scrypt secret admin01pass**

* + 1. Configure PC host IP settings.

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

* + 1. Verify connectivity.

There will be no connectivity between devices that are connected to the ASA because the ASA is the focal point for the network zones and it has not been configured. However, PC-C should be able to ping the R1 interface G0/0. From PC-C, ping the R1 G0/0 IP address (**209.165.200.225**). If these pings are unsuccessful, troubleshoot the basic device configurations before continuing.

**Note**: If you can ping from PC-C to R1 G0/0 and S0/1/0, you have demonstrated that addressing has been configured properly, and static routing is configured and functioning correctly.

* + 1. Save the basic running configuration for each router and switch.

1. Accessing the ASA Console and Using CLI Setup to Configure Basic Settings

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 clear the current configuration and use the CLI interactive setup utility to configure basic ASA settings.

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

* + 1. Access the ASA console.
       1. Enter privileged mode with the **enable** command and password (if a password has been set). The password is blank by default. Press **Enter**. If the password has been changed to what is specified in this lab, enter the word **class**. The default ASA hostname and prompt is *ciscoasa>*.

ciscoasa> **enable**

Password: **class** (or press **Enter** if none set)

* + 1. Determine the ASA version, interfaces, and license.

The ASA 5506 comes with eight Gigabit Ethernet ports.

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

ciscoasa# **show version**

Cisco Adaptive Security Appliance Software Version 9.8(2)

Firepower Extensible Operating System Version 2.2(2.52)

Device Manager Version 7.8(1)

Compiled on Sun 27-Aug-17 13:06 PDT by builders

System image file is "disk0:/asa982-lfbff-k8.SPA"

Config file at boot was "startup-config"

ciscoasa up 10 mins 59 secs

Hardware: ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)

Internal ATA Compact Flash, 8000MB

BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)

Number of accelerators: 1

1: Ext: GigabitEthernet1/1 : address is 00f2.8b8e.69ef, irq 255

2: Ext: GigabitEthernet1/2 : address is 00f2.8b8e.69f0, irq 255

3: Ext: GigabitEthernet1/3 : address is 00f2.8b8e.69f1, irq 255

4: Ext: GigabitEthernet1/4 : address is 00f2.8b8e.69f2, irq 255

5: Ext: GigabitEthernet1/5 : address is 00f2.8b8e.69f3, irq 255

6: Ext: GigabitEthernet1/6 : address is 00f2.8b8e.69f4, irq 255

7: Ext: GigabitEthernet1/7 : address is 00f2.8b8e.69f5, irq 255

8: Ext: GigabitEthernet1/8 : address is 00f2.8b8e.69f6, irq 255  
<output omitted>

What software version is this ASA running?

\_ Cisco Adaptive Security Appliance Software Version 9.6(1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

System image file is "disk0:/asa961-lfbff-k8.SPA"

Config file at boot was "startup-config"

The ASA can be managed using a built-in GUI known as ASDM. What version of ASDM is this ASA running?

\_\_\_\_Not available on Packet tracer\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How much RAM does this ASA have?

\_\_\_\_\_\_\_\_ 4096 MB\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How much flash memory does this ASA have?

\_\_\_\_\_\_ 16384KB \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How many network ports does this ASA have?

\_\_\_\_\_\_\_8\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What type of license does this ASA have?

\_\_\_\_ ASA 5506 Security Plus license \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How many VLANs can be created with this license?

\_\_\_30\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Determine the file system and contents of flash memory.
       1. Display the ASA file system using the **show file system** command. Determine what prefixes are supported.

ciscoasa# **show file system**

File Systems:

Size(b) Free(b) Type Flags Prefixes

\* 7859437568 4465147904 disk rw disk0: flash:

- - disk rw disk1:

- - network rw tftp:

- - opaque rw system:

- - network ro http:

- - network ro https:

- - network rw scp:

- - network rw ftp:

- - network wo

What is another name for flash:?\_\_ \_Disk0\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Display the contents of flash memory using one of these commands: **show flash**, **show disk0**, **dir flash:**, or **dir disk0:**.
      2. ciscoasa# **show flash**

--#-- --length-- -----date/time------ path

1. 33 Nov 29 2017 10:34:52 .boot\_string

11 4096 Jan 09 2016 19:43:02 log

1. 65486 Nov 29 2017 11:28:45 log/asa-appagent.log

20 4096 Jan 09 2016 19:43:52 crypto\_archive

1. 4096 Jan 09 2016 19:43:56 coredumpinfo
2. 59 Jan 09 2016 19:43:56 coredumpinfo/coredump.cfg
3. 08563072 Nov 24 2017 14:55:22 asa982-lfbff-k8.SPA
4. 5209829 Oct 17 2017 21:50:48 anyconnect-win-4.5.02033-webdeploy-k9.pkg
5. 26916068 Nov 24 2017 15:22:28 asdm-781.bin

7859437568 bytes total (4465147904 bytes free)

What is the name of the ASDM file in flash:? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PT version does not have ASDM

* + 1. Determine the current running configuration.

The ASA 5506 is commonly used as an edge security device that connects a small business or teleworker to an ISP device, such as a DSL or cable modem, for access to the Internet.

Display the current running configuration using the **show running-config** command.

ciscoasa# **show running-config**

: Saved

: Serial Number: JAD2002064E

: Hardware: ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)

:

ASA Version 9.8(2)

!

hostname ciscoasa

enable password $sha512$5000$ftqbmZLcP1yvT9in1bvjlg==$+GU2ZHobKrNifvyb45nWEQ== pbkdf2

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

names

!

interface GigabitEthernet1/1

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/2

shutdown

no nameif

no security-level

no ip address

!

<output omitted>

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

* + 2. Clear the previous ASA configuration settings.

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.

Use the **reload** command to restart the ASA. This causes the ASA to come up in CLI Setup mode. If prompted that the config has been modified and needs to be saved, respond with **N**, and then press **Enter** to proceed with the reload.

ciscoasa# **reload**

Proceed with reload? [confirm]

ciscoasa#

\*\*\* --- START GRACEFUL SHUTDOWN ---

Shutting down isakmp

Shutting down webvpn

Shutting down sw-module

Shutting down License Controller

Shutting down File system   
\*\*\* --- SHUTDOWN NOW ---

Process shutdown finished

Rebooting.....

CISCO SYSTEMS

Cisco Systems ROMMON, Version 1.1.8, RELEASE SOFTWARE<output omitted>

1. Configure ASA Settings and Interface Security Using the CLI

**Tip**: Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and submodes is essentially the same.

* + 1. Configure the hostname and domain name.
       1. Configure the ASA hostname as **CCNAS-ASA**.

Ciscoasa(config)# hostname CCNAS-ASA

* + - 1. Configure the domain name as **ccnasecurity.com**.

CCNAS-ASA(config)# domain-name ccnasecurity.com

* + 1. Configure the login and enable mode passwords.
       1. The login password is used for Telnet connections (and SSH prior to ASA version 8.4). By default, it is set to cisco, but since the default startup configuration was erased you have the option to configure the login password using the **passwd** or **password** command. This command is optional because later in the lab we will configure the ASA for SSH, and not Telnet access.

CCNAS-ASA(config)# **passwd cisco**

* + - 1. Configure the privileged EXEC mode (enable) password using the **enable password** command.

CCNAS-ASA(config)# **enable password class**

* + 1. Set the date and time.

The date and time can be set manually using the **clock set** command. The syntax for the **clock set** command is **clock set** *hh:mm:ss {month day | day month} year*. The following example shows how to set the date and time using a 24-hour clock:

CCNAS-ASA(config)# **clock set 11:14:00 April 28 2020**

* + 1. Configure the inside and outside interfaces.

ASA 5506 interface notes:

The 5506 is different than the 5505 ASA model. With the 5506 ASA, the physical ports can be assigned a Layer 3 IP address directly, much like a Cisco router. In this step, you will configure internal and external interfaces, name them, assign IP addresses, and set the interface security level.

If you completed the initial configuration Setup utility, the MGMT interface is configured with an IP address of 192.168.100.1. You will configure another interface as the inside interface for this lab. You will only configure the inside and outside interfaces at this time. The dmz interface will be configured in Part 5 of the lab.

* + - 1. Configure the Gi1/2 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100.

CCNAS-ASA(config)# **interface gi1/2**

CCNAS-ASA(config-if)# **nameif inside**

CCNAS-ASA(config-if)# **ip address 192.168.1.1 255.255.255.0**

CCNAS-ASA(config-if)# **security-level 100**CCNAS-ASA(config-if)# **no shutdown**

Configure the G1/1 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and access the Gi1/1 interface.

CCNAS-ASA(config-if)# **interface G1/1**

CCNAS-ASA(config-if)# **nameif outside**

INFO: Security level for "outside" set to 0 by default.

CCNAS-ASA(config-if)# **ip address 209.165.200.226 255.255.255.248**

CCNAS-ASA(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 due to 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 4 of this lab, you will configure NAT to increase the firewall protection.

* + - 1. Display the status for all ASA interfaces using the **show interface ip brief** command.

**Note:** This command is different from the **show ip interface brief** IOS command. If any of the physical or logical interfaces previously configured are not up/up, troubleshoot as necessary before continuing.

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

CCNAS-ASA# **show interface ip brief**

Interface IP-Address OK? Method Status Protocol

Virtual0 127.1.0.1 YES unset up up

GigabitEthernet1/1 209.165.200.226 YES manual up up

GigabitEthernet1/2 192.168.1.1 YES manual up up GigabitEthernet1/3 unassigned YES unset administratively down down

GigabitEthernet1/4 unassigned YES unset administratively down down

GigabitEthernet1/5 unassigned YES unset administratively down down

GigabitEthernet1/6 unassigned YES unset administratively down down

GigabitEthernet1/7 unassigned YES unset administratively down down

GigabitEthernet1/8 unassigned YES unset administratively down down

Internal-Control1/1 127.0.1.1 YES unset up up

Internal-Data1/1 unassigned YES unset up down

Internal-Data1/2 unassigned YES unset up up

Internal-Data1/3 unassigned YES unset up up

Management1/1 192.168.100.1 YES manual down down

* + - 1. Display the information for the Layer 3 interfaces using the **show ip address** command.

CCNAS-ASA#

System IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet1/1 outside 209.165.200.226 255.255.255.248 manual

GigabitEthernet1/2 inside 192.168.1.1 255.255.255.0 manual

Management1/1 management 192.168.100.1 255.255.255.0 manual

Current IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet1/1 outside 209.165.200.226 255.255.255.248 manual

GigabitEthernet1/2 inside 192.168.1.1 255.255.255.0 manual

Management1/1 management 192.168.100.1 255.255.255.0 manual

* + - 1. You may also use the **show running-config interface type/number** command to display the configuration for a particular interface from the running configuration.

CCNAS-ASA# **show running-config interface gig1/1**

!

interface GigabitEthernet1/1

nameif outside

security-level 0  
ip address 209.165.200.226 255.255.255.248

* + 1. Test connectivity to the ASA.
       1. Ensure that PC-B has a static IP address of 192.168.1.3, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1 (the IP address of the Gi1/2 inside interface).
       2. You should be able to ping from PC-B to the ASA inside interface address and ping from the ASA to PC-B. If the pings fail, troubleshoot the configuration as necessary.

CCNAS-ASA# **ping 192.168.1.3**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

* + - 1. From PC-C, ping the Gi1/1 (outside) interface at IP address 209.165.200.226. You should **Not** be able to ping this address.

1. Configure Routing, Address Translation, and Inspection Policy Using the CLI
   * 1. Configure a static default route for the ASA.

In Part 3, you configured the ASA outside interface with a static IP address and subnet mask. However, the ASA does not have a gateway of last resort defined. To enable the ASA to reach external networks, you will configure a default static route on the ASA outside interface.

**Note**: If the ASA outside interface was configured as a DHCP client, it could obtain a default gateway IP address from the ISP. However, in this lab, the outside interface is configured with a static address.

* + - 1. Ping from the ASA to R1 G0/0 at IP address 209.165.200.225. Was the ping successful?

\_\_\_Yes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Ping from the ASA to R1 S0/1/0 at IP address 10.1.1.1. Was the ping successful?

\_\_No\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + - 1. Create a “quad zero” default route using the **route** command, associate it with the ASA outside interface, and point to the R1 G0/0 at IP address 209.165.200.225 as the gateway of last resort. The default administrative distance is one by default.

CCNAS-ASA(config)# **route outside 0.0.0.0 0.0.0.0 209.165.200.225**

* + - 1. Issue the **show route** command to display the ASA routing table and the static default route you just created.

CCNAS-ASA# **show route**

Codes: L - local, C - connected, S - static, 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

i - IS-IS, su - IS-IS summary, 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, + - replicated route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S\* 0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside

C 192.168.1.0 255.255.255.0 is directly connected, inside

L 192.168.1.1 255.255.255.255 is directly connected, inside

C 209.165.200.224 255.255.255.248 is directly connected, outside

L 209.165.200.226 255.255.255.255 is directly connected, outside

* + - 1. Ping from the ASA to R1 S0/1/0 IP address 10.1.1.1. Was the ping successful?

\_\_\_\_\_\_Yes\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Configure address translation using PAT and network objects.

**Note**: Beginning with ASA version 8.3, network objects are used to configure all forms of NAT. A network object is created, and it is within this object that NAT is configured. In Step 2a, the network object **INSIDE-NET** is used to translate the inside network addresses (192.168.10.0/24) to the global address of the outside ASA interface. This type of object configuration is called Auto-NAT.

* + - 1. Create the network object **INSIDE-NET** and assign attributes to it using the **subnet** and **nat** commands.

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)# **end**

* + - 1. The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run object** and **show run nat** commands.

CCNAS-ASA# **show run object**

object network INSIDE-NET

subnet 192.168.1.0 255.255.255.0

CCNAS-ASA# **show run nat**

!

object network INSIDE-NET

nat (inside,outside) dynamic interface

* + - 1. From PC-B, attempt to ping the R1 G0/0 interface at IP address **209.165.200.225**. Notice the pings are not successful at this time as the default inspection policy does not allow ICMP to pass through the firewall.
      2. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, three were translated and three were not because ICMP is not being inspected by the global inspection policy. The outgoing pings (echoes) were translated, and the returning echo replies were blocked by the firewall policy. You will configure the default inspection policy to allow ICMP in the next step. **Note:** Depending on the processes and daemons running on the particular computer used as PC-B, you may see more translated and untranslated hits than the three echo requests and echo replies.

CCNAS-ASA# **show nat**

Auto NAT Policies (Section 2)

1 (inside) to (outside) source dynamic INSIDE-NET interface

translate\_hits = 3, untranslate\_hits = 3

* + - 1. Ping from PC-B to R1 again and quickly issue the **show xlate** command to see the addresses being translated.

CCNAS-ASA# show xlate

1 in use, 1 most used

Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.3/1 to outside:209.165.200.226/1 flags ri idle 0:00:01 timeout 0:00:30

**Note**: The flags (r and i) indicate that the translation was based on a port map (r) and was done dynamically (i).

* + - 1. Open a browser on PC-B and enter the IP address of R1 G0/0 (209.165.200.225). In a pop-up window, you should be prompted by R1 that authentication is required. TCP-based HTTP traffic is permitted, by default, by the firewall inspection policy.

Note: Because we can not set up the ip http server on the routers you will get a Request Timeout. However when you issue the commands below you will see tcp traffic leaving the ASA

* + - 1. On the ASA, reissue the **show nat** and **show xlate** commands to see the hits and addresses being translated for the HTTP connection.
    1. Modify the default MPF application inspection global service policy.

For application layer inspection and other advanced options, the Cisco MPF is available on ASAs.

Cisco MPF uses three configuration objects to define modular, object-oriented, and hierarchical policies:

* **Class maps** - Define a match criterion.
* **Policy maps** - Associate actions to the match criteria.
* **Service policies** - Attach the policy map to an interface, or globally to all interfaces of the appliance.

The Packet Tracer ASA device does not have an MPF policy map in place by default. As a modification, we can create the default policy map that will perform the inspection on inside-to-outside traffic. When configured correctly only traffic initiated from the inside is allowed back in to the outside interface. You will need to add ICMP to the inspection list.

Issue the command

CCNA-ASA# **show run | begin class**

You will see there is no default MPF policy

* + - 1. Create the class-map, policy-map, and service-policy. Add the inspection of ICMP traffic to the policy map list using the following commands:

CCNAS-ASA(config)# **class-map inspection\_default**

CCNAS-ASA(config-cmap)# **match default-inspection-traffic**

CCNAS-ASA(config-cmap)# **exit**

CCNAS-ASA(config)# **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)# **service-policy global\_policy global**

* + - 1. From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being allowed. If the pings fail, troubleshoot your configurations.

1. Configure DHCP, AAA, and SSH
   * 1. Configure the ASA as a DHCP server.
        1. Configure a DHCP address pool and enable it on the ASA inside interface.

CCNAS-ASA(config)# **dhcpd address 192.168.1.5-192.168.1.36 inside**

* + - 1. (Optional) Specify the IP address of the DNS server to be given to clients.

CCNAS-ASA(config)# **dhcpd dns 209.165.201.2 interface inside**

* + - 1. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

CCNAS-ASA(config)# **dhcpd enable inside**

* + - 1. Verify the DHCP daemon configuration by using the **show run dhcpd** command.

CCNA-ASA#show run dhcpd

dhcpd address 192.168.1.5-192.168.1.36 inside

dhcpd dns 209.165.201.2 interface inside

dhcpd enable inside

* + - 1. Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing information. Troubleshoot, as necessary to resolve any problems.
    1. Configure AAA to use the local database for authentication.
       1. Define a local user named **admin** by entering the **username** command. Specify a password of **admin01pass**

CCNAS-ASA(config)# **username admin password admin01pass**

* + - 1. Configure AAA to use the local ASA database for SSH user authentication.

CCNAS-ASA(config)# **aaa authentication ssh console LOCAL**

* + 1. Configure remote access to the ASA.

The ASA can be configured to accept connections from a single host or a range of hosts on the inside or outside network. In this step, hosts from the outside network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network.

* + - 1. Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter **no** when prompted to replace them.

CCNAS-ASA(config)# **crypto key generate rsa modulus 1024**

WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: **no**

ERROR: Failed to create new RSA keys named <Default-RSA-Key>

* + - 1. Configure the ASA to allow SSH connections from any host on the inside network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the outside network. Set the SSH timeout to 10 minutes (the default is 5 minutes).

CCNAS-ASA(config)# **ssh 192.168.1.0 255.255.255.0 inside**

CCNAS-ASA(config)# **ssh 172.16.3.3 255.255.255.255 outside**

CCNAS-ASA(config)# **ssh timeout 10**

* + - 1. Establish an SSH session from PC-C to the ASA (209.165.200.226). Troubleshoot if it is not successful.

PC> **ssh -l admin 209.165.200.226**

* + - 1. Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

PC> **ssh -l admin 192.168.1.1**

1. Configuring DMZ, Static NAT, and ACLs

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

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 G0/0 and the ASA outside interface are already using 209.165.200.225 and .226. You will use the public address 209.165.200.227 and static NAT to provide address translation access to the server.

* + 1. Configure the DMZ interface Gi1/3 on the ASA.
       1. Configure DMZ interface Gi1/3, which is where the public access web server will reside. Assign Gi1/3 the IP address **192.168.2.1/24**, name it **dmz**, and assign a security level of **70**.

CCNAS-ASA(config)# **int gi1/3**

CCNAS-ASA(config-if)# **ip address 192.168.2.1 255.255.255.0**

CCNAS-ASA(config-if)# **nameif dmz**

INFO: Security level for "dmz" set to 0 by default.INFO: Security level for "dmz" set to 0 by default.

CCNAS-ASA(config-if)# **security-level 70**

CCNAS-ASA(config-if)# **no shut**

* + - 1. Display the status for all ASA interfaces using the **show interface ip brief** command.

CCNAS-ASA# **show int ip brief**

Interface IP-Address OK? Method Status Protocol

Virtual0 127.1.0.1 YES unset up up

GigabitEthernet1/1 209.165.200.226 YES manual up up

GigabitEthernet1/2 192.168.1.1 YES manual up up

GigabitEthernet1/3 192.168.2.1 YES manual up up

GigabitEthernet1/4 unassigned YES unset administratively down down

GigabitEthernet1/5 unassigned YES unset administratively down down

GigabitEthernet1/6 unassigned YES unset administratively down down

GigabitEthernet1/7 unassigned YES unset administratively down down

GigabitEthernet1/8 unassigned YES unset administratively down down

Management1/1 192.168.100.1 YES manual down down

<output omitted>

* + - 1. Display the information for the interfaces using the **show ip address** command.

CCNAS-ASA# **show ip address**

System IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet1/1 outside 209.165.200.226 255.255.255.248 manual

GigabitEthernet1/2 inside 192.168.1.1 255.255.255.0 manual

GigabitEthernet1/3 dmz 192.168.2.1 255.255.255.0 manual

Management1/1 management 192.168.100.1 255.255.255.0 manual

Current IP Addresses:

Interface Name IP address Subnet mask Method

GigabitEthernet1/1 outside 209.165.200.226 255.255.255.248 manual

GigabitEthernet1/2 inside 192.168.1.1 255.255.255.0 manual

GigabitEthernet1/3 dmz 192.168.2.1 255.255.255.0 manual

Management1/1 management 192.168.100.1 255.255.255.0 manual

<output omitted>

* + 1. Configure static NAT to the DMZ server using a network object.

Configure a network object named **dmz-server** and assign it the static IP address of the DMZ server (**192.168.2.3**). While in object definition mode, use the **nat** command to specify that this object is used to translate a DMZ address to an outside address using static NAT, and specify a public translated address of **209.165.200.227**.

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 209.165.200.227**

* + 1. Configure an ACL to allow access to the DMZ server from the Internet.

Configure a named access list (**OUTSIDE-DMZ**) that permits any IP protocol from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the **IN** direction.

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**

**Note**: Unlike IOS ACLs, the ASA ACL **permit** statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.

You can modify this ACL to allow only services that you want to be exposed to external hosts, such as web (HTTP) or file transfer (FTP).

* + 1. Test access to the DMZ server.

At the time this Packet Tracer activity was created, the ability to successfully test outside access to the DMZ web server was not in place; therefore, successful testing is not required.

1. Reflection
   1. How does the configuration of the ASA firewall differ from that of an ISR?

There are more security features and default settings, such as interface security levels, built-in ACLs, and default inspection policies.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. What does the ASA use to define address translation and what is the benefit?

\_\_ Objects and groups allow the creation of modular structures and the configuration of attributes.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. How does the ASA 5506 use physical interfaces to manage security and how does this differ from other ASA models?

\_\_The 5506 its physical interfaces assigned security levels to control traffic from one interface to another \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Paste a copy of your ASA show run here.

CCNAS-ASA(config)#sh run

: Saved

:

ASA Version 9.6(1)

!

hostname CCNAS-ASA

domain-name ccnasecurity.com

enable password Qa8ENuiyPgE/u.0d encrypted

passwd 4IncP7vTjpaba2aF encrypted

names

!

interface GigabitEthernet1/1

nameif outside

security-level 0

ip address 209.165.200.226 255.255.255.248

!

interface GigabitEthernet1/2

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0

!

interface GigabitEthernet1/3

nameif dmz

security-level 70

ip address 192.168.2.1 255.255.255.0

!

interface GigabitEthernet1/4

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/5

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/6

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/7

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/8

no nameif

no security-level

no ip address

!

interface Management1/1

no nameif

no security-level

no ip address

!

object network INSIDE-NET

subnet 192.168.1.0 255.255.255.0

object network dmz-server

host 192.168.2.3

!

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

!

access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3

!

!

access-group OUTSIDE-DMZ in interface outside

object network INSIDE-NET

nat (inside,outside) dynamic interface

object network dmz-server

nat (dmz,outside) static 209.165.200.227

!

aaa authentication ssh console LOCAL

!

!

username admin password zKlkq7CT0mv7eALP encrypted

!

class-map inspection\_default

match default-inspection-traffic

!

policy-map global\_policy

class inspection\_default

inspect icmp

!

service-policy global\_policy global

!

telnet timeout 5

ssh 192.168.1.0 255.255.255.0 inside

ssh 172.16.3.3 255.255.255.255 outside

ssh timeout 10

!

dhcpd address 192.168.1.5-192.168.1.36 inside

dhcpd dns 209.165.201.2 interface inside

dhcpd enable inside

!

!

!

!

!