

9.3.1.2 Lab – Configure ASA 5506-X Basic Settings and Firewall Using CLI Answers

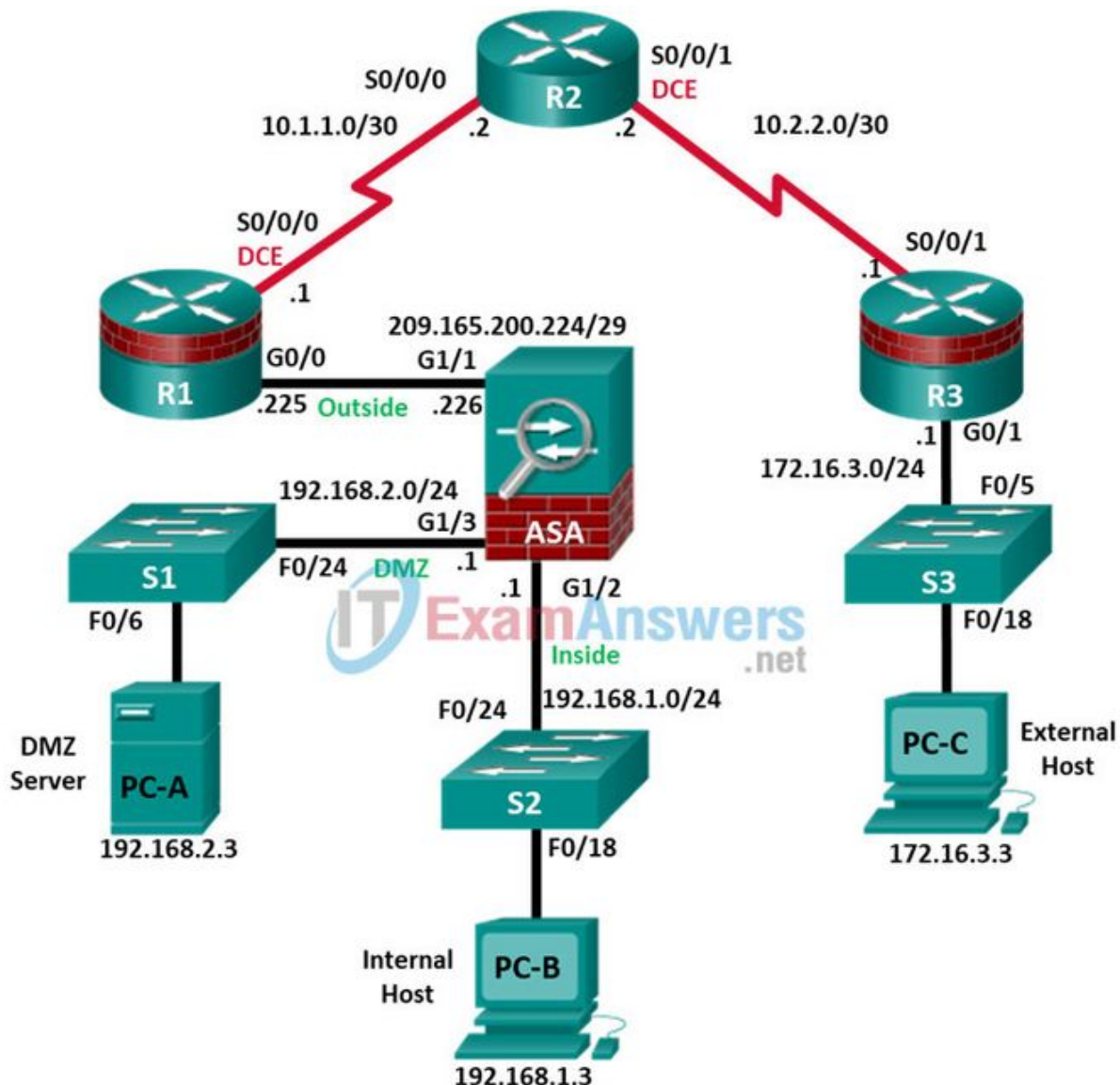
itexamanswers.net/9-3-1-2-lab-configure-asa-5506-x-basic-settings-and-firewall-using-cli-answers.html

June 6, 2022

9.3.1.2 Lab – Configure ASA 5506-X Basic Settings and Firewall Using CLI (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Note: ISR G2 devices use GigabitEthernet interfaces instead of FastEthernet interfaces.

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
R1	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
R2	S0/0/1 (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
R3	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	G1/1 (outside)	209.165.200.226	255.255.255.248	NA	R1 G0/0
ASA	G1/2 (inside)	192.168.1.1	255.255.255.0	NA	S2 F0/24
ASA	G1/3 (dmz)	192.168.2.1	255.255.255.0	NA	S1 F0/24
PC-A	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

Objectives

Part 1: Configure Basic Device Settings

- Cable the network as shown in the topology.
- Configure hostnames and interface IP addresses for routers, switches, and PCs.
- Configure static routes on R2 and default routes on R1 and R3.
- Enable HTTP and SSH access for R1.
- Configure PC host IP settings.
- Verify connectivity between hosts 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.

- Use CLI Setup mode to configure basic settings (hostname, passwords, clock, etc.).

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 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.

Background/Scenario

The Cisco Adaptive Security Appliance (ASA) is an advanced network security device that integrates a stateful firewall, VPN, and FirePOWER services. This lab employs an ASA 5506-X 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 inside resources. Inside users can access the DMZ and outside resources.

The focus of this lab is to configure the ASA as a basic firewall. Other devices will receive minimal configuration to support the ASA portion of this lab. This lab uses the ASA CLI, which is similar to the IOS CLI, to configure basic device and security settings.

In Part 1 of this lab, you will configure the topology and non-ASA devices. In Parts 2 through 4 you will configure basic ASA settings and the firewall between the inside and outside networks. In part 5 you will configure the ASA for additional services, such as DHCP, AAA, and SSH. In Part 6, you will configure a DMZ on the ASA and provide access to a server in the DMZ.

The scenario for this lab assumes your company has a location connected to an ISP. R1 is 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 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 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 router commands and output in this lab are from a Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology license. Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of this lab to determine which interface identifiers to use based on the equipment in your class. Depending on the router model and Cisco IOS version, the available commands and output produced might vary from what is shown in this lab.

The ASA used with this lab is a Cisco model 5506-X with an 8-port integrated switch, running OS version 9.10(1), Adaptive Security Device Manager (ASDM) version 7.10(1), and comes with a Base license that allows a maximum of five VLANs.

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

Instructor Note: Instructions for initializing the network devices are provided in the Chapter 0.0.0.0 Instructions for erasing the ASA and accessing the console are provided in this lab.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology Package license)
- 3 Switches (Cisco 2960 with cryptography IOS image for SSH support – Release 15.0(2)SE7 or comparable) (not required)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1)) and Base license or comparable)
- 3 PCs (Windows with SSH client software)

- Serial and Ethernet cables as shown in the topology
- Console cables to configure Cisco networking devices

Instructor Note:

- This lab is divided into six parts. Part 1 can be performed separately, but must be performed before parts 2 through 6. Part 2 uses the CLI Setup mode. Parts 3 through 6 can be performed individually or in combination with other parts as time permits, but should be performed sequentially. In some cases, a task assumes the configuration of certain features in a prior task.
- The goal is to use an ASA to implement firewall and other services that might previously have been configured on an ISR. In this lab, the student configures the most common basic ASA settings and services, such as NAT, ACL, DHCP, AAA, and SSH.
- The final running configurations for all devices are found at the end of this lab. The ASA factory default configuration is also provided.

Part 1: Configure Basic Device Settings

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 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.

- a. Configure hostnames as shown in the topology for each router.
- b. Configure router interface IP addresses as shown in the IP Addressing Table.
- c. Set the clock rate of 64000 for routers with a DCE serial cable attached.
- d. Configure the host name for the switches. Other than the host name, the switches can be left in their default configuration state.

Step 3: Configure static routing on the routers.

- a. 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
```

b. Configure a static route from R2 to the R1 G0/0 subnet (connected to ASA interface G1/1) 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 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.

a. 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
```

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

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

c. Configure a domain name.

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

d. Configure crypto keys for SSH.

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

e. Configure an admin01 user account using algorithm-type scrypt for encryption and a password of cisco12345.

```
R1(config)# username admin01 algorithm-type scrypt secret cisco12345
```

f. 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, 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
```

g. 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
```

h. Configure the enable password with strong encryption.

```
R1(config)# enable algorithm-type scrypt secret class12345
```

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 R1 interface. From PC-C, ping the R1 Go/o 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 Go/o and So/o/o 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 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.

Step 1: Access the ASA console.

a. 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 and use a terminal emulation program, such as TeraTerm or PuTTY to open a serial connection and access the CLI.

b. The ASA initially prompts you to pre-configure the firewall using an interactive prompt. We will not be configuring the ASA this way, therefore enter no and press **Enter**. If you have inadvertently started the setup wizard, press **CTRL-Z** to exit it. The terminal screen should display the default ASA user EXEC hostname and prompt ciscoasa>.

c. Enter privileged mode with the **enable** command. The password is blank by default therefore press **Enter**. If the password has been changed to what is specified in this lab, enter the word **class**.

```
ciscoasa> enable
Password: class (or press Enter if none set)
```

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

The ASA 5506-X comes with an integrated eight-port Ethernet switch. Ports G1/1 to G1/8 are normal GigabitEthernet ports.

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

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 9.10(1)
Firepower Extensible Operating System Version 2.4(1.103)
Device Manager Version 7.10(1)

Compiled on Wed 24-Oct-18 16:22 PDT by builders
System image file is "disk0:/asa9101-lfbff-k8.SPA"
Config file at boot was "startup-config"

ciscoasa up 16 mins 27 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 00a3.8ecd.0ed2, irq 255
 2: Ext: GigabitEthernet1/2  : address is 00a3.8ecd.0ed3, irq 255
 3: Ext: GigabitEthernet1/3  : address is 00a3.8ecd.0ed4, irq 255
<output omitted>
```

What software version is this ASA running?

The ASA in this lab uses version 9.10(1).

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

The system image file in the ASA for this lab is asa9101-lfbff-k8.SPA, and it was loaded from disk0: (or flash:).

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

The ASA in this lab uses ASDM version 7.10(1).

What is the Firepower Extension Operating System version?

The Firepower-X version in this lab is 2.4(1.103).

How much RAM does this ASA have?

The ASA in this lab has 4096 MB RAM.

How much flash memory does this ASA have?

The ASA in this lab has 8000 MB RAM.

How many Ethernet ports does this ASA have?

The ASA in this lab has eight GigabitEthernet ports and a Management port.

What type of license does this ASA have?

The ASA has either Base or the Security Plus license.

How many VLANs can be created with this license?

Five VLANs can be created with the Base license or 30 with the Security Plus license.

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

a. 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
* 7365472256	3902828544	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	cluster:
-	-	- stub	ro	cluster_trace:
-	-	- network	rw	smb

What is another name for flash:?

disk0:

b. Display the contents of flash memory using either the **show flash**, **show disk0**, **dir flash:**, or **dir disk0:** command. These commands display similar output.

```
ciscoasa# show flash
--#--  --length--  -----date/time-----  path
107  4096          Jan 01 1980 00:00:00  FSCK0000.REC
108  28672         Jan 01 1980 00:00:00  FSCK0001.REC
109   33           Feb 21 2019 23:24:58  .boot_string
11  4096           Aug 29 2017 14:25:32  log
13  25250          Feb 25 2019 22:13:00  log/asa-appagent.log
20  4096           Aug 29 2017 14:26:24  crypto_archive
21  4096           Aug 29 2017 14:26:28  coredumpinfo
22   59           Aug 29 2017 14:26:28  coredumpinfo/coredump.cfg
110  4096          Jan 01 1980 00:00:00  FSCK0002.REC
111  34143680       Feb 20 2019 01:53:30  asdm-7101.bin
113  115316320      Feb 20 2019 02:28:44  asa9101-lfbff-k8.SPA
114  35209829       Oct 04 2017 03:17:02  anyconnect-win-4.5.02033-webdeploy-k9.pkg
<output omitted>
```

c. What is the name of the ASDM file in flash:?
asdm-7101.bin

Instructor Note: Your ASA may display other files. Check the content of flash memory occasionally to see if there are FSCK*.REC files. These files are generated automatically by the ASA when it runs the file system check (fsck). You can delete these files by issuing the command **delete flash:FSCK*.REC** from the privileged EXEC prompt. Press **Enter** at each prompt to confirm the deletion.

```
ciscoasa# delete flash:FSCK*.REC
Delete filename [FSCK*.REC]? <Enter>

Delete disk0:/FSCK0000.REC? [confirm]
<output omitted>
```

Step 4: Determine the current running configuration.

The ASA 5506-X 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.

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

```
ciscoasa# show running-config
: Saved

:
: Serial Number: JAD21140GC5
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.10(1)
!
hostname ciscoasa
enable password ***** pbkdf2
names
no mac-address auto

!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
```

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

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 varies depending on the ASA model, version, and configuration status.

b. You can restore the ASA to its factory default settings by using the **configure factory-default** global configuration command. When entering global configuration, you will initially be prompted to enable anonymous error reporting. Enter **A** to be prompted for this at a later date.

```
ciscoasa# conf t
ciscoasa(config)#
```

***** NOTICE *****

Help to improve the ASA platform by enabling anonymous reporting, which allows Cisco to securely receive minimal error and health information from the device. To learn more about this feature, please visit: <http://www.cisco.com/go/smartcall>

Would you like to enable anonymous error reporting to help improve the product? [Y]es, [N]o, [A]sk later: A
You will be reminded again in 7 days.

If you would like to enable this feature, issue the command "call-home reporting anonymous".

Please remember to save your configuration.

```
ciscoasa(config)# configure factory-default
Based on the inside IP address and mask, the DHCP address pool size is reduced to 250 from the platform limit 256
```

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

WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.

Executing command: !

Executing command: interface Management1/1

Executing command: management-only

Executing command: no nameif

Executing command: no security-level

Executing command: no ip address

Executing command: no shutdown

Executing command: exit

Executing command: !

Executing command: interface GigabitEthernet1/1

Executing command: nameif outside

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

Executing command: security-level 0

Executing command: no shutdown

Executing command: ip address dhcp setroute

Executing command: exit

<output omitted>

c. Review this output and pay particular attention to the interfaces, NAT-related, and DHCP-related sections. These will be configured later in this lab using the CLI.

d. You may want to capture and print the factory-default configuration as a reference. Use the terminal emulation program to copy it from the ASA and paste it into a text document. You can then edit this file if desired, so that it contains only valid commands. You should remove password commands and enter the **no shut** command to enable the desired interfaces.

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. 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
System config has been modified. Save? [Y]es/[N]o: n
Proceed with reload? [confirm]
ciscoasa(config)#
```

```
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down webvpn
Shutting down sw-module
Shutting down License Controller
Shutting down File system
<output omitted>
```

Step 6: Use the Setup interactive CLI mode to configure basic settings.

When the ASA completes the reload process, it should detect that the startup-config file is missing and prompt you to pre-configure the firewall using interactive prompts. This presents a series of interactive prompts to configure basic ASA settings.

Note: The interactive prompt mode does not configure the ASA with factory defaults as described in Step 4. This mode can be used to configure minimal basic settings, such as hostname, clock, and passwords. You can also go directly to the CLI to configure the ASA settings, as described in Part 3.

a. Respond to the Setup interactive prompts as shown here, after the ASA reloads.

```
Pre-configure Firewall now through interactive prompts [yes]? <Enter>
Firewall Mode [Routed]: <Enter>
Enable password [<use current password>]: class
Allow password recovery [yes]? <Enter>
Clock (UTC):
  Year [2019]: <Enter>
  Month [Mar]: <Enter>
  Day [19]: <Enter>
  Time [23:32:19]: <Enter>
Management IP address: 192.168.100.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com
IP address of host running Device Manager: <Enter>
```

The following configuration will be used:

```
Enable password: class
Allow password recovery: yes
Clock (UTC): 07:29:14 Mar 19 2019
Firewall Mode: Routed
Management IP address: 192.168.100.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com
```

```
Use this configuration and save to flash? [yes] <Enter>
INFO: Security level for "management" set to 0 by default.
Cryptochecksum: d0b22e76 5178e9e6 0a6bc590 5f5e5a3d
```

3958 bytes copied in 0.80 secs

```
User enable_1 logged in to ASA-Init
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ASA-Init>
```

Note: In the above configuration, the IP address of the host running ASDM was left blank. It is not necessary to install ASDM on a host. It can be run from the flash memory of the ASA device itself using the browser of the host.

Note: The responses to the prompts are automatically stored in the startup-config and the running config. However, additional security-related commands, such as a global default inspection service policy, are inserted into the running-config by the ASA OS.

b. Enter privileged EXEC mode with the **enable** command. Enter **class** for the password.

- c. Issue the **show run** command to see the additional security-related configuration commands that are inserted by the ASA.
- d. Issue the **write memory** command to capture the additional security-related commands in the startup-config file.

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

In Part 3, you will configure basic settings by using the ASA CLI, even though some of them were already configured using the Setup mode interactive prompts in Part 2. In this part, you will start with the settings configured in Part 2 and then add to or modify them to create a complete basic configuration.

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 sub-modes is essentially the same.

Note: You must complete Part 2 before beginning Part 3.

Step 1: Configure the hostname and domain name.

- a. Enter global configuration mode using the **config t** command. The first time you enter configuration mode after running Setup, you will be prompted to enable anonymous reporting. Respond with no.

```
ASA-Init# config t
ASA-Init(config)#
```

```
***** NOTICE *****
```

```
Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall
```

```
Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: n
```

```
In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".
```

```
Please remember to save your configuration.
```

- b. Configure the ASA hostname using the **hostname** command.

```
ASA-Init(config)# hostname CCNAS-ASA
```

- c. Configure the domain name using the **domain-name** command.

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

Step 2: Configure the login and enable mode passwords.

a. 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
```

b. Configure the privileged EXEC mode (enable) password using the **enable password** command.

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

Step 3: 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 19:09:00 april 19 2019
```

Step 4: Configure the inside and outside interfaces.

In this step, you will configure internal and external interfaces, name them, assign IP addresses, and set the interface security level.

ASA 5506-X interface notes:

The ASA 5506-X is different than the 5505 ASA model. The ASA 5506-X has eight integrated switch ports that are routed interfaces. Like a Cisco router, the routed interfaces on the 5506-X can be assigned a Layer 3 IP address.

If you completed the initial configuration Setup utility, the MGMT interface was 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 6 of the lab.

a. Configure interface G1/2 for the inside network, 192.168.1.0/24. Name the interface **inside**, set the security level to the highest setting of **100** and enable it.


```
CCNAS-ASA(config)# interface g1/2
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
```

b. Configure interface G1/1 for the outside network, 209.165.200.224/29. Name the interface **outside**, set the security level to the lowest setting of 0 and enable it.

```
CCNAS-ASA(config-if)# interface g1/1
CCNAS-ASA(config-if)# nameif outside
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# security-level 0
CCNAS-ASA(config-if)# no shutdown
```

c. Remove the configuration from the M1/1 interface and shut it down (if required).

```
CCNAS-ASA(config)# interface m1/1
CCNAS-ASA(config-if)# shutdown
CCNAS-ASA(config-if)# no ip address
```

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.

d. Display the status for all ASA interfaces using the **show interface ip brief** command.

Note: The command syntax 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(config-if)# 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	down	down
Internal-Data1/2	unassigned	YES	unset	up	up
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	administratively down	down

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

```
CCNAS-ASA(config-if)# show ip address
```

System IP Addresses:

Interface	Name	IP address	Subnet mask
GigabitEthernet1/1	outside	209.165.200.226	255.255.255.248
GigabitEthernet1/2	inside	192.168.1.1	255.255.255.0

Current IP Addresses:

Interface	Name	IP address	Subnet mask
GigabitEthernet1/1	outside	209.165.200.226	255.255.255.248
GigabitEthernet1/2	inside	192.168.1.1	255.255.255.0

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

```
CCNAS-ASA(config-if)# show run interface g1/1
!
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address 209.165.200.226 255.255.255.248
```

Step 5: Test connectivity to the ASA.

a. 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.

b. 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(config-if)# 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 = 1/2/10 ms
```

c. From PC-C, ping the outside interface IP address **209.165.200.226**. You should not be able to ping this address.

Step 6: Configure ASDM access to the ASA.

a. You can configure the ASA to accept HTTPS connections using the **http server enable** command. This allows access to the ASA GUI (ASDM). Configure the ASA to allow HTTPS connections from any host on the inside network (192.168.1.0/24).

```
CCNAS-ASA(config-if)# http server enable
CCNAS-ASA(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**. You will be prompted that the connection is not secure. Select **Advanced > Add Exception > Confirm Security Exemption**.

You should then be required to authenticate to the ASA. Because no username was specified, simply enter the enable password **class** in the password field.

You should then see Cisco ASDM Welcome screen that allows you to: Install ASDM Launcher or run ASDM as a Java Web start application.

c. Close the browser. In the next lab, you will use ASDM extensively to configure the ASA. The objective here is not to use the ASDM configuration screens, but to verify HTTP/ASDM connectivity to the ASA. If you are unable to access ASDM, check your configurations. If the configurations are correct contact your instructor for further assistance.

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

In Part 4 of this lab, you will provide a default route for the ASA to reach external networks. You will configure address translation using network objects to enhance firewall security. You will then modify the default application inspection policy to allow specific traffic.

Note: You must complete Part 3 before proceeding to Part 4.

Step 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.

a. Ping from the ASA to R1 Go/o at IP address 209.165.200.225. Was the ping successful?
Yes, 209.165.200.224/248 is a directly connected network for both R1 and the ASA.

b. Ping from the ASA to R1 So/o/o at IP address 10.1.1.1. Was the ping successful?
No, the ASA does not have a route to 10.1.1.0/30.

c. Create a “quad zero” default route using the **route** command, associate it with the ASA outside interface, and point to the R1 Go/o 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
```

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

```
CCNAS-ASA(config)# 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, V - VPN
       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
```

e. Ping from the ASA to R1 So/o/o IP address 10.1.1.1. Was the ping successful?
Yes. The ASA now has a default route to unknown networks.

Step 2: Configure address translation using PAT and network objects.

Instructor Notes:

Pre-ASA 8.3 NAT configuration:

Prior to ASA version 8.3, NAT configuration from the CLI was the same as the older PIX firewalls. Configuration was performed using the **nat**, **global**, and **static** commands. These commands have been deprecated with 8.3 and newer versions and are no longer supported, with the exception of the **nat** command under certain circumstances.

An example of configuring PAT using the old commands is presented here for historical reference. In the example, inside addresses from the 192.168.1.0/24 network are being translated using the address of the outside interface.

If you use the older commands as shown in the example with ASA version 8.3 and newer you will receive the error result shown here.

```
CCNAS-ASA(config)# nat (inside) 1 192.168.10.0 255.255.255.0
ERROR: This syntax of nat command has been deprecated.
Please refer to "help nat" command for more details.
```

```
CCNAS-ASA(config)# global (outside) 1 interface
ERROR: This syntax of nat command has been deprecated.
Please refer to "help nat" command for more details.
```

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.

a. 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
```

b. 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
```

c. From PC-B, attempt to ping the R1 Go/o interface at IP address **209.165.200.225**. Were the pings successful?

No.

d. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four 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 four 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 = 4, untranslate_hits = 4
```

e. 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 0:00:02
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).

f. Open a browser on PC-B and enter the IP address of R1 Go/o (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.

g. On the ASA, reissue the **show nat** and **show xlate** commands to see the hits and addresses being translated for the HTTP connection.

Step 3: Modify the default MPF application inspection global service policy.

For application layer inspection, as well as 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.

a. Display the default MPF policy map that performs the inspection on inside-to-outside traffic. Only traffic that was initiated from the inside is allowed back in to the outside interface. Notice that the ICMP protocol is missing.

```
CCNAS-ASA# show run | begin class
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
<output omitted>
```

b. Add the inspection of ICMP traffic to the policy map list using the following commands:

```
CCNAS-ASA# configure terminal
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
```

c. Display the default MPF policy map to verify ICMP is now listed in the inspection rules.

```
CCNAS-ASA(config-pmap-c)# show run policy-map
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect icmp
<output omitted>
```

d. From PC-B, attempt to ping the R1 Go/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.

Part 5: Configuring DHCP, AAA, and SSH

In Part 5, you will configure ASA features, such as DHCP and enhanced login security, using AAA and SSH.

Note: You must complete Part 4 before beginning Part 5.

Step 1: Configure the ASA as a DHCP server.

The ASA can be both a DHCP server and a DHCP client. In this step, you will configure the ASA as a DHCP server to dynamically assign IP addresses for DHCP clients on the inside network.

a. Configure a DHCP address pool and enable it on the ASA inside interface. This is the range of addresses to be assigned to inside DHCP clients. Set the range from 192.168.1.5 through 192.168.1.100.

```
CCNAS-ASA(config-pmap-c)# dhcpd address 192.168.1.5-192.168.1.100 inside
```


b. (Optional) Specify the IP address of the DNS server to be given to clients.

```
CCNAS-ASA(config)# dhcpd dns 209.165.201.2
```

Note: Other parameters can be specified for clients, such as WINS server, lease length, and domain name. By default, the ASA sets its own IP address as the DHCP default gateway, so there is no need to configure it. However, to manually configure the default gateway, or set it to a different networking device's IP address, use the following command:

```
CCNAS-ASA(config)# dhcpd option 3 ip 192.168.1.1
```

c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

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

d. Verify the DHCP daemon configuration by using the **show run dhcpd** command.

```
CCNAS-ASA(config)# show run dhcpd
dhcpd dns 209.165.201.2
dhcpd option 3 ip 192.168.1.1
!
dhcpd address 192.168.1.5-192.168.1.100 inside
dhcpd enable inside
```

e. Access the Network Connection IP Properties for PC-B, and change it from a static IP address to a DHCP client so that it obtains an IP address automatically from the ASA DHCP server. The procedure to do this varies depending on the PC operating system. It may be necessary to issue the **ipconfig /renew** command on PC-B to force it to obtain a new IP address from the ASA.

Instructor Notes: Configuring the ASA as a DHCP client (informational only).

These instructions are provided to configure the outside interface as a DHCP client in the event the ASA needs to obtain its public IP address from an ISP. This is not performed as part of the lab. Optionally, you may wish to configure router R1 as a DHCP server to provide the necessary information to the ASA.

The following command configures the ASA outside interface VLAN 2 to receive its IP address information via a DHCP server and sets the default route using the default gateway parameter provided by the ISP DHCP server.

```
CCNAS-ASA(config)# interface g1/1
CCNAS-ASA(config-if)# ip address dhcp setroute
```

Step 2: Configure AAA to use the local database for authentication.

a. Define a local user named admin by entering the **username** command. Specify a password of **cisco12345**.

```
CCNAS-ASA(config)# username admin password cisco12345
```

b. Configure AAA to use the local ASA database for SSH user authentication.

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

Note: For added security, starting with ASA version 8.4(2), configure AAA authentication to support SSH connections. The Telnet/SSH default login is not supported. You can no longer connect to the ASA using SSH with the default username and the login password.

Step 3: Configure SSH remote access to the ASA.

You can configure the ASA to accept SSH connections from a single host or a range of hosts on the inside or outside network.

a. Generate an **RSA** key pair, which is required to support SSH connections. The modulus (in bits) can be 512, 768, 1024, or 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA. Specify a modulus of **1024** using the **crypto key** command.

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
INFO: The name for the keys will be:
Keypair generation process begin. Please wait...
```

Note: You may receive a message that a RSA key pair is already defined. To replace the RSA key pair enter yes at the prompt.

b. Save the RSA keys to persistent flash memory using either the **copy run start** or **write mem** command.

```
CCNAS-ASA# write mem
Building configuration...
Cryptochecksum: 3c845d0f b6b8839a f9e43be0 33feb4ef
3270 bytes copied in 0.890 secs
[OK]
```

c. 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
```

d. On PC-C, use an SSH client (such as PuTTY) to connect to the ASA outside interface at the IP address **209.165.200.226**. The first time you connect you may be prompted by the SSH client to accept the RSA host key of the ASA SSH server. Log in as user **admin** and provide the password **cisco12345**.

e. You can also connect to the ASA inside interface from a PC-B SSH client using the IP address **192.168.1.1**.

Part 6: 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 Go/o 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.

Step 1: Configure the DMZ interface G1/3 on the ASA.

a. Configure DMZ interface G1/3 which is on the LAN where the public access web server will reside. Assign the interface IP address **192.168.2.1/24**, name it **dmz**, assign it a security level of **70** and enable the interface.

```
CCNAS-ASA(config)# interface g1/3
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.
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# no shut
```

b. Display the status for all ASA interfaces using the **show interface ip brief** command.

```
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	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
Internal-Control1/1	127.0.1.1	YES	unset	up	up
Internal-Data1/1	unassigned	YES	unset	down	down
Internal-Data1/2	unassigned	YES	unset	up	up
Internal-Data1/3	unassigned	YES	unset	up	up
Internal-Data1/4	169.254.1.1	YES	unset	up	up
Management1/1	unassigned	YES	unset	administratively down	down

c. 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			

```
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			

Step 2: 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-if)# 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
```

Step 3: 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).

Step 4: Test access to the DMZ server.

a. Create a loopback 0 interface on Internet R2 representing an external host. Assign Lo0 IP address **172.30.1.1** and a mask of **255.255.255.0**. Ping the DMZ server public address from R2 using the loopback interface as the source of the ping. The pings should be successful.

```
R2(config-if)# interface lo0
R2(config-if)# ip address 172.30.1.1 255.255.255.0
R2(config-if)# end
R2# ping 209.165.200.227 source lo0
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:

Packet sent with a source address of 172.30.1.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

b. Clear the NAT counters using the **clear nat counters** command.

```
CCNAS-ASA# clear nat counters
```

c. Ping from PC-C to the DMZ server at the public address **209.165.200.227**. The pings should be successful.

d. Issue the **show nat** and **show xlate** commands on the ASA to see the effect of the pings. Both the PAT (inside to outside) and static NAT (dmz to outside) policies are shown.

```
CCNAS-ASA# show nat
```

Auto NAT Policies (Section 2)

```
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 4
2 (inside) to (outside) source dynamic INSIDE-NET interface
    translate_hits = 1, untranslate_hits = 3
```

Note: Pings from inside to outside are translated hits. Pings from outside host PC-C to the DMZ are considered untranslated hits.

```
CCNAS-ASA# show xlate
```

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

Note: This time the flag is “s”, which indicates a static translation.

e. You can also access the DMZ server from a host on the inside network because the ASA inside interface (G1/2) is set to a security level of 100 (the highest) and the DMZ interface (G1/3) is set to 70. 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.X). The pings should be successful because of the interface security level and the fact that ICMP is being inspected on the inside interface by the global inspection policy. The pings from PC-B to PC-A will not affect the NAT translation counts because both PC-B and PC-A are behind the firewall, and no translation takes place.

The DMZ server cannot ping PC-B on the inside network because the DMZ interface VLAN 3 has a lower security level and because the **no forward** command was specified when the VLAN 3 interface was created. Try to ping from the DMZ server PC-A to PC-B at IP address **192.168.1.3**. The pings should not be successful.

Use the **show run** command to display the configuration for VLAN 3.

```
CCNAS-ASA# show run interface g1/3
!
interface g1/3
nameif dmz
    security-level 70
    ip address 192.168.2.1 255.255.255.0
```

Note: An access list can be applied to the inside interface to control the type of access to be permitted or denied to the DMZ server from inside hosts.

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.

2. 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.

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 (F0/0)	Fast Ethernet 0/1 (F0/1)	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)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	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.

Device Configs

Note: ISR G2 devices have GigabitEthernet interfaces instead of FastEthernet Interfaces.

ASA 5506-X Final Config

```

CCNAS-ASA# show run
: Saved

:
: Hardware:   ASA5506, 4096 MB RAM, CPU Atom C2000 series 1250 MHz, 1 CPU (4 cores)
:
ASA Version 9.8(2)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password $sha512$5000$moS4D9cvXZnHdxzLcQZ5cA==$NUhzP1Ut5xeeMv+z6hA60w== 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
passwd 2KFQnbNIdI.2KY0U 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
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet1/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet1/6
  shutdown

```



```

no nameif
no security-level
no ip address
!
interface GigabitEthernet1/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet1/8
shutdown
no nameif
no security-level
no ip address
!
interface Management1/1
management-only
shutdown
nameif management
security-level 0
no ip address
!
ftp mode passive
dns server-group DefaultDNS
domain-name ccnasecurity.com
object network INSIDE-NET
subnet 192.168.1.0 255.255.255.0
object network dmz-server
host 192.168.2.3
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
pager lines 24
mtu management 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network INSIDE-NET
nat (inside,outside) dynamic interface
object network dmz-server
nat (dmz,outside) static 209.165.200.227
access-group OUTSIDE-DMZ in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00

```

```

timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 10
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd dns 209.165.201.2
dhcpd option 3 ip 192.168.1.1
!
dhcpd address 192.168.1.5-192.168.1.100 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
username admin password
$sha512$5000$Wu07KpWYaLIbNvYnvYbrQ==$bAb/djgPtJy01MTr1u32HA== pbkdf2
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options

```

```

inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect dns preset_dns_map
inspect icmp
policy-map type inspect dns migrated_dns_map_2
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect dns migrated_dns_map_1
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:a1d22f5c946cb489c715c247a64bbc9c
: end

```

ASA 5506-X Factory Default Config

```

ciscoasa# show run
: Saved

:
: 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$31khKufWlikvKuwNFuthGA==$4ECChj3TUbwBATa+tpH6FQ== pbkdf2
names

!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface GigabitEthernet1/2
 bridge-group 1
 nameif inside_1
 security-level 100
!
interface GigabitEthernet1/3
 bridge-group 1
 nameif inside_2
 security-level 100
!
interface GigabitEthernet1/4
 bridge-group 1
 nameif inside_3
 security-level 100
!
interface GigabitEthernet1/5
 bridge-group 1
 nameif inside_4
 security-level 100
!
interface GigabitEthernet1/6
 bridge-group 1
 nameif inside_5
 security-level 100
!
interface GigabitEthernet1/7
 bridge-group 1
 nameif inside_6
 security-level 100
!
interface GigabitEthernet1/8
 bridge-group 1
 nameif inside_7
 security-level 100

```

```

!
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
!
interface BVI1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
ftp mode passive
same-security-traffic permit inter-interface
object network obj_any1
  subnet 0.0.0.0 0.0.0.0
object network obj_any2
  subnet 0.0.0.0 0.0.0.0
object network obj_any3
  subnet 0.0.0.0 0.0.0.0
object network obj_any4
  subnet 0.0.0.0 0.0.0.0
object network obj_any5
  subnet 0.0.0.0 0.0.0.0
object network obj_any6
  subnet 0.0.0.0 0.0.0.0
object network obj_any7
  subnet 0.0.0.0 0.0.0.0
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside_1 1500
mtu inside_2 1500
mtu inside_3 1500
mtu inside_4 1500
mtu inside_5 1500
mtu inside_6 1500
mtu inside_7 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 16384
!
object network obj_any1
  nat (inside_1,outside) dynamic interface
object network obj_any2
  nat (inside_2,outside) dynamic interface
object network obj_any3
  nat (inside_3,outside) dynamic interface
object network obj_any4
  nat (inside_4,outside) dynamic interface

```

```

object network obj_any5
  nat (inside_5,outside) dynamic interface
object network obj_any6
  nat (inside_6,outside) dynamic interface
object network obj_any7
  nat (inside_7,outside) dynamic interface
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
no snmp-server location
no snmp-server contact
service sw-reset-button
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map

```

```
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:41b85e17968fd3f025d888e36ed8c016
: end
```

Router R1

```
R1# show run
Building configuration...

Current configuration : 1626 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 9 $9$ClZUh5YnAAiTdE$DAuM/C/VKMJPCKKfM17JBC1l.2zs4XXF84M15EophQk
!
no aaa new-model
!
!
ip domain name ccnasecurity.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
username admin01 secret 9
$9$QyoiaBEQk.ewRE$6KLtQh25dXf3xiiGN87zBZfT6dtLMRlAi2L5vxFsKgM
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.248
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
```



```

    clock rate 64000
    !
interface Serial0/0/1
    no ip address
    shutdown
    clock rate 2000000
    !
ip forward-protocol nd
    !
ip http server
no ip http secure-server
    !
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
    !
control-plane
    !
line con 0
    exec-timeout 0 0
    logging synchronous
    login local
line aux 0
line 2
    no activation-character
    no exec
    transport preferred none
    transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
    stopbits 1
line vty 0 4
    exec-timeout 0 0
    login local
    transport input ssh
    !
scheduler allocate 20000 1000
    !
end

```

Router R2

```
R2# show run
Building configuration...

Current configuration : 1327 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
!
redundancy
!
interface Loopback0
 ip address 172.30.1.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 64000
```

```
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
ip route 172.16.3.0 255.255.255.0 Serial0/0/1  
ip route 209.165.200.224 255.255.255.248 Serial0/0/0  
!  
control-plane  
!  
line con 0  
line aux 0  
line 2  
    no activation-character  
    no exec  
    transport preferred none  
    transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
    stopbits 1  
line vty 0 4  
    login  
    transport input none  
!  
scheduler allocate 20000 1000  
!  
end
```

Router R3

```
R3# show run
Building configuration...

Current configuration : 1298 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
```

```
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
control-plane
!
line con 0
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  login
  transport input none
!
scheduler allocate 20000 1000
!
end
```

Switches S1, S2, and S3 – Use default configs, except for host name