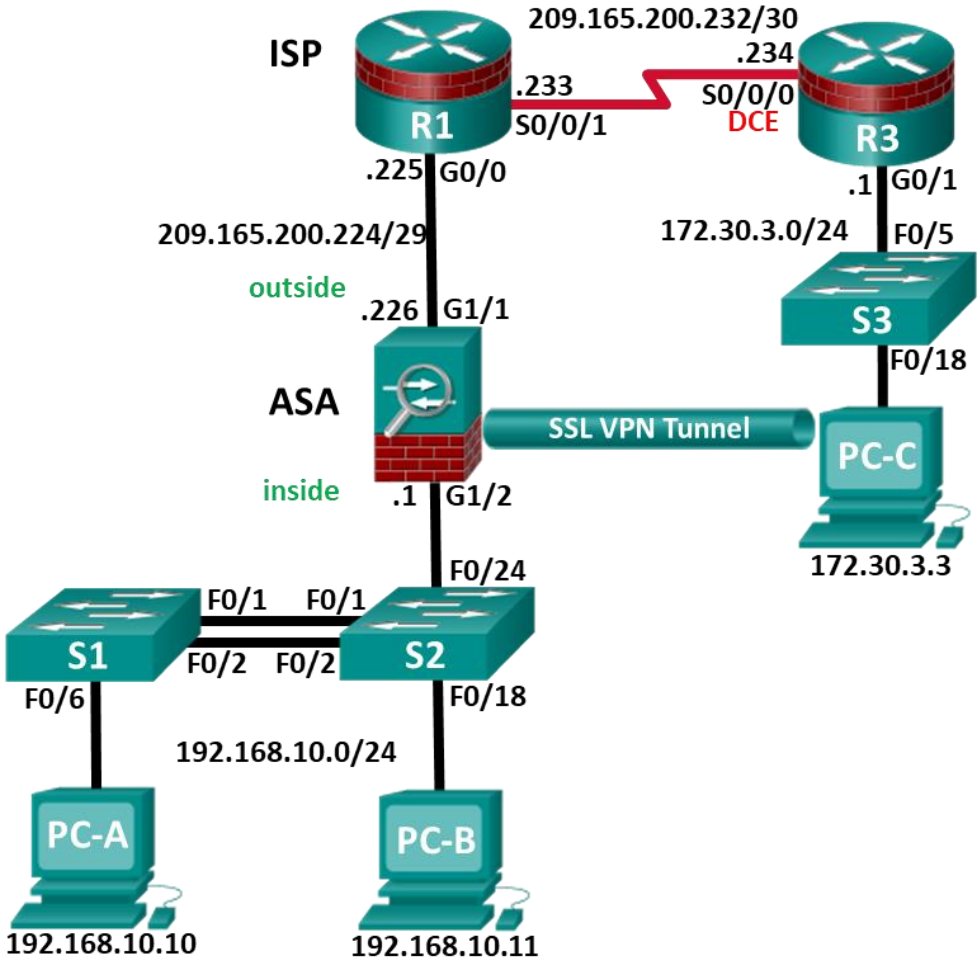
Skills Assessment Using ASA-5506-X – Form A

Topology



Assessment Objectives

- **Part 1: Verify Network Connectivity (**1 points, 5 minutes**)**
- **Part 2: Configure Secure Router Administrative Access** (17 points, 15 minutes)
- **Part 3: Configure a Zone-Based Policy Firewall** (14 points, 10 minutes)
- **Part 4: Configure an Intrusion Prevention System** (15 points, 10 minutes)
- **Part 5: Secure Layer 2 Switches** (22 points, 20 minutes)
- **Part 6: Configure ASA Basic Management and Firewall Settings** (17 points, 15 minutes)
- **Part 7: Configure the ASA for SSL VPN Remote Access Using ASDM** (14 points, 15 minutes)

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Scenario

This Skills Assessment (SA) is the final practical exam of student training for the CCNA Security course. The exam is divided into seven parts. The parts should be completed sequentially, and signed off by your instructor before moving on to the next part. In Part 1, you will verify that the basic device settings have been preconfigured by the instructor. In Part 2, you will secure a network router using the command line interface (CLI) to configure various IOS features including AAA and SSH. In Part 3 and 4, you will configure a zone-based policy firewall (ZPF) and intrusion prevention using the Cisco IOS intrusion prevention system (IPS) on an integrated service router (ISR) using the CLI. In Part 5, you will configure and secure layer 2 switches using the CLI. In Parts 6 and 7, you will configure the ASA management and firewall settings using the CLI and implement an SSL Remote Access VPN using ASDM.

Required Resources

- 2 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)
- 1 ASA 5506-X (OS version 9.10(1) and ASDM version 7.10(1) and Base license or comparable)
- 3 PCs (Windows, SSH Client and Java version compatible with installed ASDM version)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Verify Network Connectivity

Total points: 17

Time: 15 minutes

In the interest of time, your instructor has pre-configured basic settings on R1 and R3 and configured the static IP address information for the PC hosts in the topology. In Part 1, you will verify that PC-C can ping the G0/1 interface on R3.

Configuration Task	Specification	Points
Ping the G0/1 interface on R3 from PC-C.	See Topology for specific settings.	1/2
Ping interface S0/0/1 on R1 from R3.	See Topology for specific settings.	1/2

Instructor Sign-Off Part 1: _____

Points: _____ **of 1**

Note: Do not proceed to Part 2 until your instructor has signed off on Part 1.

Part 2: Configure Secure Router Administrative Access

Total points: 17

Time: 15 minutes

In Part 2, you will secure administrative access on R3 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification	Points
Set minimum password length.	Minimum Length: **10** characters	1

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuration Item or Task	Specification	Points
Assign and encrypt a privileged EXEC password.	Password: **cisco12345** Encryption type: 9 (**scrypt**)	1
Add a user in the local database for administrator access.	Username: **Admin01** Privilege level: **15** Encryption type: 9 (**scrypt**) Password: **admin01pass**	1
Configure an MOTD banner.	**Unauthorized Access is Prohibited!**	1/2
Disable HTTP server services.		1/2
Configure SSH.	Domain name: **ccnassecurity.com** RSA keys size: **1024** Version: **2** Timeout: **90** seconds Authentication retries: **2**	4
Configure VTY lines to allow SSH access.	Allow only **SSH** access	1
Configure the AAA authentication and authorization settings.	Enable AAA Use **local database** as default setting.	2
Configure NTP.	Authentication key: **NTPpassword** Encryption: **MD5** Key: **1** NTP server: **209.165.200.233** Configure for periodic calendar updates.	4
Configure syslog.	Enable timestamp service to log the date and time in milliseconds. Send syslog messages to: **172.30.3.3**. Set message logging severity level to: **Warnings**.	2

Note: Before proceeding to Part 3, ask your instructor to verify R3's configuration and functionality.

Instructor Sign-Off Part 2: _____

Points: _____ **of 17**

Part 3: Configure a Zone-Based Policy Firewall

Total points: 14

Time: 10 minutes

In Part 3, you will configure a ZPF on R3 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification	Points
Create security zone names.	Inside zone name: **INSIDE** Outside zone name: **INTERNET**	2

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Create an inspect class map.	Class map name: **INSIDE_PROTOCOLS** Inspection type: **match-any** Protocols allowed: **tcp, udp, icmp**	3
Create an inspect policy map.	Policy map name: **INSIDE_TO_INTERNET** Bind the class map to the policy map. Matched packets should be inspected.	3
Create a zone pair.	Zone pair name: **IN_TO_OUT_ZONE** Source zone: **INSIDE** Destination zone: **INTERNET**	2
Apply the policy map to the zone pair.	Zone pair name: **IN_TO_OUT_ZONE** Policy map name: **INSIDE_TO_INTERNET**	2
Assign interfaces to the proper security zones.	Interface G0/1: **INSIDE** Interface S0/0/0: **INTERNET**	2

Troubleshoot as necessary to correct any issues.

Note: Before proceeding to Part 4, ask your instructor to verify your ZPF configuration and functionality.

Instructor Sign-Off Part 2: _____

Points: _____ of 14

Part 4: Configure an Intrusion Prevention System

Total points: 15

Time: 10 minutes

In Part 4, you will configure an IPS on R3 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification	Points
Create an IPS directory on flash.	Directory name: **IPSDIR** **Note**: If the directory already exists, delete the directory and recreate it.	1

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuration Item or Task	Specification	Points
Copy and paste the crypto key file into R3's running-configuration.	crypto key pubkey-chain rsa named-key realm-cisco.pub signature key-string 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128 B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3 F3020301 0001 quit	1
Create an IPS rule.	IPS rule name: **IOSIPS**	1
Set the storage location for the IPS signatures.	Location: **IPSDIR on flash**	1
Enable IPS SDEE event notification.	Enable HTTP server services. Enable SDEE notification services.	1
Enable IPS syslog support.		1
Retire all signatures in the all category.	Category: **all**	2
Un-retire the ios_ips basic category signatures.	Category: **ios_ips basic**	2
Apply the IPS rule to the interface.	Interface: **S0/0/0** Direction: **in**	2
Copy the S854 signature from PC-C.	Protocol: **TFTP** IP Address of TFTP server: **172.30.3.3** Signature: **IOS-S854-CLI.pkg** Compile signatures after they are loaded: **idconf**	3

Note: Before attempting the TFTP copy, the TFTP server software on PC-C needs to be running with the directory set to the location of the file: **IOS-S854-CLI.pkg**.

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Troubleshoot as necessary to correct any issues.

Note: Before proceeding to Part 5, ask your instructor to verify your IPS configuration and functionality.

Instructor Sign-Off Part 4: _____

Points: _____ **of 15**

Part 5: Secure Layer 2 Switches

Total points: 22

Time: 20 minutes

Note: Not all security features in this part of the exam will be configured on all switches. However, in a production network, all security features will be configured on all switches. In the interest of time, the security features are configured on only S2, except where noted.

In Part 5, you will configure security settings on S2 using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification	Points
Assign and encrypt a privileged EXEC password.	Switch: **S2** Password: **cisco12345** Encryption type: 9 (**scrypt**)	1/2
Add a user in the local database for administrator access.	Switch: **S2** Username: **Admin01** Privilege level: **15** Encryption type: 9 (**scrypt**) Password: **admin01pass**	1
Configure an MOTD banner.	Switch: **S2** Banner: **Unauthorized Access is Prohibited!**	1/2
Disable HTTP and HTTP secure server.	Switch: **S2**	1
Configure SSH.	Switch: **S2** Domain name: **ccnassecurity.com** RSA keys size: **1024** Version: **2** Timeout: **90** seconds Authentication retries: **2**	2
Configure the VTY lines to allow SSH access.	Switch: **S2** Allow only **SSH** access.	1/2
Configure the AAA authentication and authorization settings.	Switch: **S2** Enable **AAA** Use **local database** as default setting.	2
Create the VLAN list.	Switches: **S1 & S2** VLAN: **2,** Name: **NewNative** VLAN: **10,** Name: **LAN** VLAN: **99,** Name: **Blackhole**	1/2

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuration Item or Task	Specification	Points
Configure the trunk ports.	Switches: **S1 & S2** Interfaces: **F0/1, F0/2** Native VLAN: **2** Prevent DTP.	2
Disable trunking.	Switch: **S2** Ports: **F0/18, F0/24** VLAN assignment: **10**	2
Enable PortFast and BPDU guard.	Switch: **S2** Ports: **F0/18, F0/24**	2
Configure basic port security.	Switch: **S2** Port: **F0/18** Maximum limit: **1** Remember the MAC address. Violation Action: **Shutdown**	3
Disable unused ports on S2, and assign ports to VLAN 99.	Switch: **S2** Ports: **F0/3-17, F0/19-23, G0/1-2**	1
Configure Loop guard.	Switch: **S2** Loop guard: **Default**	1
Configure DHCP snooping.	Enable DHCP snooping globally Enable DHCP for VLAN: **10** DHCP trusted interface: **F0/24**	3

NETLAB+ Note: Use a Maximum limit of **2** when configuring basic port security. Otherwise, the hidden Control Switch will cause a violation to occur and the port will be shutdown.

Troubleshoot as necessary to correct any issues.

Note: Before proceeding to Part 6, ask your instructor to verify your switch configuration and functionality.

Instructor Sign-Off Part 5: _____

Points: _____ **of 22**

Part 6: Configure ASA Basic Management and Firewall Settings

Total points: 17

Time: 15 minutes

Note: By default, the privileged EXEC password is blank. Press **Enter** at the password prompt.

In Part 6, you will configure the ASA's basic setting and firewall using the CLI. Configuration tasks include the following:

Configuration Item or Task	Specification	Points
Configure the ASA hostname.	Name: **CCNAS-ASA**	1/2
Configure the domain name.	Domain name: **ccnasecurity.com**	1/2

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Configuration Item or Task	Specification	Points
Configure the privileged EXEC password.	Password: **cisco12345**	1/2
Add a user in the local database with administrator console access.	User: **Admin01** Password: **admin01pass**	1/2
Configure interface G1/2.	Name: **inside** IP address: **192.168.10.1** Subnet mask: **255.255.255.0** Security level: **100**	3
Configure interface G1/1.	Name: **outside** IP address: **209.165.200.226** Subnet mask: **255.255.255.248** Security level: **0**	3
Configure the AAA to use the local database for SSH user authentication.		1
Generate an RSA key pair to support the SSH connections.	Key: **RSA** Modulus size: **1024**	1
Configure the ASA to accept SSH connections from hosts on the inside LAN.	Inside network: **192.168.10.0/24** Timeout: **10** minutes Version: **2**	2
Configure the default route.	Default route IP address: **209.165.200.225**	1
Configure the ASDM access to the ASA.	Enable HTTPS server services. Enable HTTPS on the inside network.	2
Create a network object to identify internal addresses for PAT. Dynamically bind interfaces by using the interface address as the mapped IP.	Object name: **INSIDE-NET** Subnet: **192.168.10.0/24** Interfaces: **inside, outside**	2
Modify the default global policy to allow returning ICMP traffic through the firewall.	Policy-map: **global_policy** Class: **inspection_default** Inspect: **icmp**	1

Troubleshoot as necessary to correct any issues.

Note: Before proceeding to Part 7, ask your instructor to verify your ASA configuration and functionality.

Instructor Sign-Off Part 6: _____

Points: _____ **of 17**

Part 7: Configure the ASA for SSL VPN Remote Access Using ASDM

Total points: 14

Time: 15 minutes

In Part 7, you will configure an AnyConnect SSL remote access VPN on the ASA using ASDM. You will then use a browser on PC-C to connect and download the Cisco AnyConnect Secure Mobility Client software

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

located on the ASA. After the software has downloaded, you will manually install the AnyConnect software to PC-C and use it to establish a remote SSL VPN connection to the ASA.

Step 1: Configure SSL VPN settings on the ASA using the ASDM from PC-B.

Use a browser on PC-B to establish an ASDM session to the ASA. After the session is established, use the **AnyConnect VPN Wizard** to configure the ASA to allow SSL VPN client connections. Configuration parameters include the following:

Configuration Item or Task	Specification	Points
Use a browser on PC-B, and connect to the ASA.	Connection: **HTTPS** IP address: **192.168.10.1** Username: **Admin01** Password: **admin01pass** **Note:** You will need to accept all security messages.	1
Use the AnyConnect VPN Wizard to configure the ASA to accept SSL VPN connections from the Cisco AnyConnect Secure Mobility Client.	Connection profile name: **ANYCONNECT-SSL-VPN** VPN access interface: **outside** VPN protocols: **SSL** only. Client images: **anyconnect-win-4.1.00028-k9.pkg** or **equivalent** Username: **VPNuser** Password: **VPNuserpa55** IP address pool name: **VPN-POOL** IP address pool starting address: **192.168.10.201** IP address pool ending address: **192.168.10.210** IP address pool subnet mask: **255.255.255.0** DNS server: **10.20.30.40** Domain name: **ccnasecurity.com** Exempt VPN traffic from NAT: **Enable** Inside interface: **inside** Local network: **any4**	7

Step 2: Establish an SSL VPN connection to the ASA from PC-C

To establish an SSL VPN connection to the ASA, you will need to use a browser on PC-C to download the Cisco AnyConnect Secure Mobility Client software from the ASA. After the software is downloaded, you will install the AnyConnect software to PC-C and then establish an SSL VPN connection to the ASA. The steps required are as follows:

Configuration Item or Task	Specification	Points
Use a browser on PC-C. Connect to the ASA. Download the Cisco AnyConnect Secure Mobility Client software to the PC.	Connection: **HTTPS** IP address: **209.165.200.226** Username: **VPNuser** Password: **VPNuserpa55**	2

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Download and install the Cisco AnyConnect Secure Mobility Client. After installation is complete the AnyConnect SSL VPN session should be established automatically.	Accept all security warning messages. If the **Untrusted Server Blocked!** window appears. Click **Change Setting** to allow the connection to the ASA. When asked to change PC settings to allow AnyConnect Client to be installed, click **Yes**.	2
Verify that an SSL VPN session has been established to the ASA using ASDM from PC-B.		2

Troubleshoot as necessary to correct any issues.

Instructor Sign-Off Part 7: _____

Points: _____ **of 14**

Router Interface Summary

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 (S0/0/1)
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, identify the type of router, and how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. This 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.

© 2015 - 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public