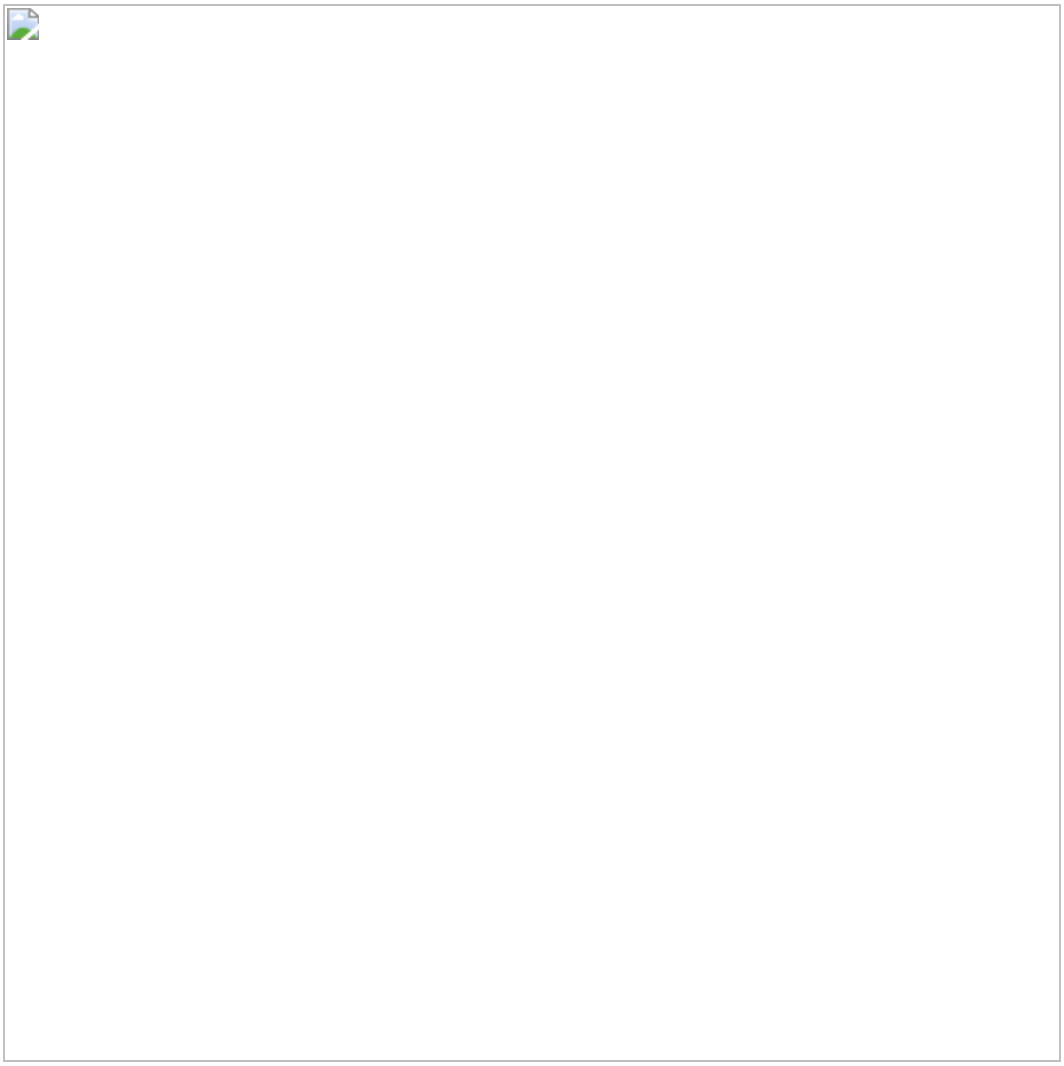
CCNA Security v2.0 Skills Assessment – A (Answer Key)

July 6, 2021

CCNA Security v2.0 Skills Assessment – Type A

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

Topology



Assessment Objectives

- **Part 1: Configure PCs and Verify Network Connectivity** (5 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** (18 points, 15 minutes)
- **Part 7: Configure the ASA for SSL VPN Remote Access Using ASDM** (14 points, 15 minutes)

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.

Instructor Note: The routers used in this SA are Cisco 1941 ISRs with Cisco IOS Release 15.4(3)M2 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this SA. Refer to the Router Interface Summary table at the end of this SA for the correct interface identifiers.

Instructor Note: Sample scoring and estimated times for each exam are provided. These can be adjusted by the instructor as necessary to suit the testing environment. Total points for the exam are 100 and the total time is estimated at 90 minutes. The instructor may choose to deduct points if excessive time is taken for a part of the assessment.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.4(3)M2 image with a Security Technology package license or comparable)
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 ASA 5506 (OS version 9.8(1) and ASDM version 7.8(1) and Base license or comparable)
- 3 PCs (Windows 7 or Windows 8.1, with SSH Client software installed)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Instructor Notes:

Router Resource Requirements:

Note: The following requirements are critical to successful completion of this SA.

• The router that runs IPS (R3) requires a minimum of 192 MB of DRAM and at least 2 MB of free flash memory. It must also be running T-Train Cisco IOS Release 12.4(11)T1 or later (preferably 12.4(24)T8 or later) to support the version 5.x format signature package.

• This SA uses the newer Version 5.x signature files, which are independent of the Cisco IOS software. Prior to Cisco IOS release 12.4(11)T, Cisco IOS IPS had 132 built-in signatures available in the Cisco IOS software image. The built-in signatures are hard-coded into the Cisco IOS software image for backward compatibility. Starting with Cisco IOS release 12.4(11)T, there are no built-in (hard-coded) signatures within Cisco IOS software. Support for signatures and signature definition files (SDFs) in Cisco IPS version 4.x is discontinued in 12.4(11)T1 and subsequent Cisco IOS T-Train software releases.

• To configure IOS IPS for 12.4(11)T and later, a signature package in Cisco IPS version 5.x format is required to load signatures on an ISR. Cisco provides a version 5.x format signature package for CLI users.

• To download the latest IPS signature package and public crypto key files, you need a valid CCO (Cisco.com) account.

• Download the signature package (IOS-Sxxx-CLI.pkg) from:
http://www.cisco.com/cisco/software/type.html?mdfid=281442967&catid=268438162

Note: It is recommended that you use the latest signature file available. However, if the amount of router flash memory is an issue, consider downloading an older version 5.x signature file, which requires less memory.
The S854 file is used with this SA, although newer versions are available. Consult CCO to determine the latest version for use in a production environment.

• Create the following public crypto key text file and name it **realm-cisco.pub.key.txt**, for use with IOS IPS:

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub
  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
```

Note: The signature package file should be in the TFTP default directory for PC-C. The public key file should be available on the desktop or other known location.

Refer to the Chapter 5 Lab titled “Configuring an IPS Using the CLI” for additional details on IPS requirements.

Router and Switch Preparation

Erase the router and switch startup configurations. Before interconnecting the switches, delete the **vlan.dat** file from each switch. If the file is not deleted, VLAN information from one switch may be transferred to the other via VTP.

The IPS signature (.xml) file for R3 is in the **flash:/ipsdir/** directory. If the file is in the flash directory, delete the file and the directory before starting the SA. Use the following procedure.

```
R3# show flash
-#- --length-- -----date/time   path

1       0       Jan     30      2015    00:24:58        +00:00  IPSDIR
2       1628152 Jan     30      2015    00:42:10        +00:00  IPSDIR/iosips-sig-
default.xmz
3       835     Jan     30      2015    00:39:42        +00:00  IPSDIR/iosips-seap-
typedef.xmz
4       304     Jan     30      2015    00:39:40        +00:00  IPSDIR/iosips-seap-
delta.xmz
5       143447  Jan     30      2015    00:40:56        +00:00  IPSDIR/iosips-sig-
category.xmz
6       16625   Jan     30      2015    00:40:52        +00:00  IPSDIR/iosips-sig-
typedef.xmz
7       255     Jan     30      2015    00:39:40        +00:00  IPSDIR/iosips-sig-
delta.xmz
9       2903    Aug     9 2012 16:07:28 +00:00 cpconfig-19xx.cfg
10      3000320 Aug     9 2012 16:07:42 +00:00 cpexpress.tar
11      1038    Aug     9       2012    16:07:50        +00:00  home.shtml
12      122880  Aug     9       2012    16:07:58        +00:00  home.tar
13      1697952 Aug     9       2012    16:08:12        +00:00  securedesktop-ios-
3.1.1.45-k9.pkg
14      415956  Aug     9       2012    16:08:26        +00:00  sslclient-win-
1.1.4.176.pkg
15      75551300 Feb 17 2015 00:52:42 +00:00 c1900-universalk9-mz.SPA.154-3.M2.bin

173850624 bytes available (82636800 bytes used)
R3# delete /force /recursive flash:IPSDIR
Remove directory filename [IPSDIR]?
Delete flash:IPSDIR? [confirm]
```

Instructor Note: In the interest of time, the instructor should pre-configure the basic device settings. Basic configurations are provided below for R1 and R3.

R1 Startup Configuration

```
hostname R1
no ip domain lookup interface GigabitEthernet0/0
ip address 209.165.200.225 255.255.255.248
no shutdown interface Serial0/0/1
ip address 209.165.200.233 255.255.255.252
no shutdown
ip route 192.168.10.0 255.255.255.0 209.165.200.226
ip route 172.30.3.0 255.255.255.0 209.165.200.234
ntp authentication-key 1 md5 NTPpassword ntp trusted-key 1
ntp authenticate ntp master 3
end
```

R3 Startup Configuration

```
hostname R3
no ip domain lookup interface G0/1
ip address 172.30.3.1 255.255.255.0
no shut int S0/0/0
ip address 209.165.200.234 255.255.255.252
no shutdown
ip route 0.0.0.0 0.0.0.0 209.165.200.233
end
```

S1 Startup Configuration

```
hostname S1
no ip domain lookup
spanning-tree vlan 1 root primary
interface range f0/3-5, f0/7-24, g0/1-2
shutdown
end
```

S2 Startup Configuration

```
hostname S2
no ip domain lookup
spanning-tree vlan 1 root secondary
end
```

S3 Startup Configuration

```
hostname S3
no ip domain lookup
interface range f0/1-4, f0/6-17, f0/19-24, g0/1-2 shutdown
end
```

PC-A

```
IP Address: 192.168.10.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.1
```

PC-B

```
IP Address: 192.168.10.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.1
```

PC-C

```
IP Address: 172.30.3.3
Subnet Mask: 255.255.255.0
Default Gateway: 172.30.3.1
```

Intructions

Part 1: Configure PCs and Verify Network Connectivity

Total points: 5

Time: 5 minutes

In the interest of time, R1 and R3 are pre-configured for basic connectivity. You must configure the static IP address information for the PC hosts using the addressing in the topology. You will then verify connectivity.

Configuration Task	Specification	Points
Configure Static IP Addressing on PC-A, PC- B, and PC-C	See Topology for specific settings.	3
See Topology for specific settings.	3	1/2
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
Ping interface G0/0 on R1 from PC-C.	See Topology for specific settings.	1

Instructor Sign-Off Part 1: _____

Points: _____ of 5

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
Assign and encrypt a privileged EXEC password.	Password: **cisco12345** Encryption type: 9 (**scrypt**)	1

Configuration Item or Task	Specification	Points
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

Configuration Item or Task	Configuration Commands	Verification Commands
Set minimum password length.	security passwords min-length 10	show run | inc passwords
Assign and encrypt a privileged EXEC password.	enable algorithm-type scrypt secret cisco12345	show run | inc enable Verify encryption type 9. Exit global EXEC mode and enable to verify the password is correct.
Add a user in the local database for administrator access.	username Admin01 privilege 15 algorithm-type scrypt secret admin01pass	show run | include username

Configuration Item or Task	Configuration Commands	Verification Commands
Configure an MOTD banner.	banner motd $Unauthorized Access is Prohibited!$	show run | inc banner
Disable HTTP server services.	no ip http server	show run | inc http
Configure SSH.	ip domain-name ccnasecurity.com crypto key generate rsa general- keys modulus 1024 ip ssh version 2 ip ssh time-out 90 ip ssh authentication-retries 2	show ip ssh
Configure VTY lines to allow SSH access.	line vty 0 4 transport input ssh exit	show run | sec vty
Configure the AAA authentication and authorization settings.	aaa new-model aaa authentication login default local aaa authorization exec default local	show run | inc aaa
Configure NTP.	ntp authentication-key 1 md5 NTPpassword ntp authenticate ntp server 209.165.200.233 ntp update-calendar	show ntp associations show run | sec ntp
Configure syslog.	service timestamps log datetime msec logging 172.30.3.3 logging trap warnings	show run | inc timestamps show run | sec logging show logging

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
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

Configuration Item or Task	Configuration Commands	Verification Commands
Create security zone names.	zone security INSIDE zone security INTERNET	show run | section zone security
Create an inspect class map.	class-map type inspect match- any INSIDE_PROTOCOLS match protocol tcp match protocol udp match protocol icmp	show class-map type inspect
Create an inspect policy map.	policy-map type inspect INSIDE_TO_INTERNET class type inspect INSIDE_PROTOCOLS inspect	show policy-map type inspect

Configuration Item or Task	Configuration Commands	Verification Commands
Create a zone pair.	zone-pair security IN_TO_OUT_ZONE source INSIDE destination INTERNET	show zone-pair security
Apply the policy map to the zone pair.	zone-pair security IN_TO_OUT_ZONE service-policy type inspect INSIDE_TO_INTERNET	show zone-pair security
Assign interfaces to the proper security zones.	interface g0/1 zone-member security INSIDE interface s0/0/0 zone-member security INTERNET	show zone security

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: **IPSDIRNote:** If the directory already exists, delete the directory and recreate it.	1

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**	2

Note: Before attempting the TFTP copy, the **Tftpd32** software on PC-C needs to be running with the directory set to the location of the file: **IOS-S854-CLI.pkg**.

Configuration Item or Task	Configuration Commands	Verification Commands
Create an IPS directory on flash.	mkdir IPSDIR (Note: If the directory already exists: del /force /recursive flash:IPSDIR)	show flash (Look for the IPSDIR directory.)
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	show crypto key pubkey- chain rsa name realm- cisco.pub
Create an IPS rule.	ip ips name IOSIPS	show ip ips name IOSIPS

Configuration Item or Task	Configuration Commands	Verification Commands
Set the storage location for the IPS signatures.	ip ips config location flash:IPSDIR	show run | sec ips
Enable IPS SDEE event notification.	ip http server ip ips notify sdee	show run | inc http show run | inc notify show ip ips all | inc Event
Enable IPS syslog support.	ip ips notify log	show run | sec ips show ip ips all | inc Event
Retire all signatures in the all category.	ip ips signature-category category all retired true exit	show ip ips signature-category config
Un-retire the ios_ips basic category signatures.	ip ips signature-category category ios_ips basic retired false exit exit Do you want to accept these changes? [confirm]	show ip ips signature-category config
Apply the IPS rule to the interface.	interface s0/0/0 ip ips IOSIPS in exit	show run interface s0/0/0 show ip ips interface
Copy the S854 signature from PC-C.	copy tftp://172.30.3.3/IOS-S854-CLI.pkg idconf	show ip ips signatures

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: S2Allow 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
Configure the trunk ports.	Switches: **S1 & S2** Interfaces: **F0/1, F0/2** Native VLAN: **2** Prevent DTP.	2

Configuration Item or Task	Specification	Points
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.

Configuration Item or Task	Configuration Commands	Verification Commands
Assign and encrypt a privileged EXEC password. (Switch: S2 only)	enable algorithm-type scrypt secret cisco12345	show run | inc enable Verify encryption type 9.
Add a user in the local database for administrator access. (Switch: S2 only)	username Admin01 privilege 15 algorithm-type scrypt secret admin01pass	show run | include username Verify username, privilege level, and encryption type. The password can be verified.
Configure an MOTD banner. (Switch: S2 only)	banner motd $Unauthorized Access is Prohibited!$	show run | inc banner
Disable the HTTP and HTTP secure server. (Switch: S2 only)	no ip http server no ip http secure-server	show run | inc http

Configuration Item or Task	Configuration Commands	Verification Commands
Configure SSH. (Switch: S2 only)	ip domain-name ccnasecurity.com crypto key generate rsa general-keys modulus 1024 ip ssh version 2 ip ssh time-out 90 ip ssh authentication-retries 2	show ip ssh
Configure the VTY lines to allow SSH access. (Switch: S2 only)	line vty 0 15 transport input ssh exit	show run | sec vty
Configure the AAA authentication and authorization settings. (Switch: S2 only)	aaa new-model aaa authentication login default local aaa authorization exec default local	show run | inc aaa
Create the VLAN list. (Switch: S1 & S2)	vlan 2 name NewNative vlan 10 name LAN vlan 99 name Blackhole exit	show vlan
Configure the trunk ports. (Switch: S1 & S2)	interface range f0/1-2 switchport mode trunk switchport trunk native vlan 2 switchport nonegotiate	show run | beg interface
Disable trunking. (Switch: S2 only)	interface ran f0/18, f0/24 switchport mode access switchport access vlan 10	show run interface f0/18 show run interface f0/24
Enable PortFast and BPDU guard. (Switch: S2 only)	interface ran f0/18, f0/24 spanning-tree portfast spanning-tree bpduguard enable	show run interface f0/18 show run interface f0/24

Configuration Item or Task	Configuration Commands	Verification Commands
Configure basic port security. (Switch: S2 only)	interface f0/18 switchport port-security switchport port-security maximum 1 switchport port-security mac-address sticky switchport port-security violation shutdown	show run interface f0/18 show port-security interface fa0/18
Disable the unused ports on S2. (Switch: S2 only)	interface range f0/3-17, f0/19-23, g0/1-2 switchport mode access switchport access vlan 99 shutdown	show ip interface brief (Determine whether interfaces are administratively down.)
Configure Loop guard. (Switch: S2 only)	spanning-tree loopguard default	show spanning-tree summary (Determine whether Loopguard Default is enabled.)
Configure DHCP snooping. (Switch: S2 only)	ip dhcp snooping ip dhcp snooping vlan 10 int f0/24 ip dhcp snooping trust end	show ip dhcp snooping

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: 18

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
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 Gig1/2	Gig1/2 Name: **inside** IP address: **192.168.10.1** Subnet mask: **255.255.255.0** Security level: **100**	3
Configure Interface Gig1/1	Gig1/1 Name: **outside** IP address: **209.165.200.226** Subnet mask: **255.255.255.248** Security level: **0**	4
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**	1
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

Configuration Item or Task	Specification	Points
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

Configuration Item or Task	Configuration Commands	Verification Commands
Configure the ASA hostname.	hostname CCNAS-ASA	(View the command prompt to verify the CCNAS-ASA name.)
Configure the domain name.	domain-name ccnasecurity.com	show run domain
Configure the privileged EXEC password.	enable password cisco12345	show run enable
Add a user in the local database with administrator console access.	username Admin01 password admin01pass	show run username
Configure Gig1/2	interface gig1/2 nameif inside ip add 192.168.10.1 255.255.255.0 security-level 100 no shutdown	show run interface vlan 1
Configure Gig1/1	interface gig1/1 nameif outside ip add 209.165.200.226 255.255.255.248 security-level 0 no shutdown	show run interface vlan 2

Configuration Item or Task	Configuration Commands	Verification Commands
Configure the AAA to use the local database for SSH user authentication.	aaa authentication ssh console LOCAL	show run aaa
Generate an RSA key pair to support the SSH connections.	crypto key generate rsa modulus 1024 (if asked to replace a current keypair, Yes)	show crypto key mypubkey rsa
Configure the ASA to accept SSH connections from hosts on the inside LAN.	ssh 192.168.10.0 255.255.255.0 inside ssh timeout 10 ssh version 2	show ssh
Configure the default route.	route outside 0.0.0.0 0.0.0.0 209.165.200.225	show route (Look for the quad-zero static route.)
Configure the ASDM access to the ASA.	http server enable http 192.168.10.0 255.255.255.0 inside	show run http
Create a network object to identify internal addresses for PAT. Dynamically bind the interfaces by using the interface address as the mapped IP.	object network INSIDE-NET subnet 192.168.10.0 255.255.255.0 nat (inside,outside) dynamic interface	show nat show run object
Modify the default global policy to allow returning ICMP traffic through the firewall.	policy-map global_policy class inspection_default inspect icmp	show run policy-map

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 18

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 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 and/or add the ASA IP address to the allowed list of IP addresses in Java. If the “Run ASDM” button via Java is not accessible, access your ASA via **https://<ip_address>/admin/public/asdm.jnlp** to download the JNLP file and then open the file to continue using ASDM.	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** 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

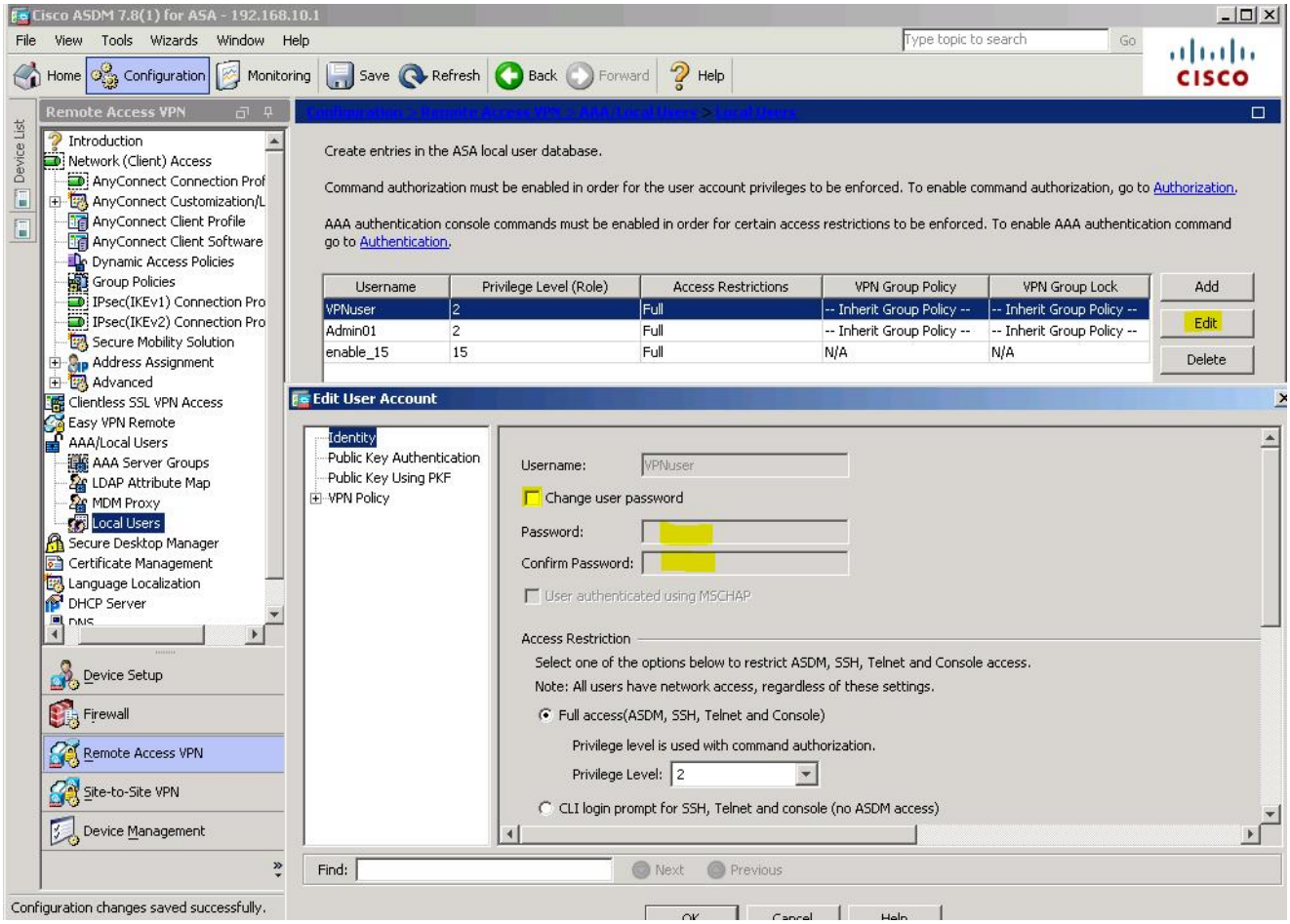
To establish an SSL VPN connection to the ASA, you will need to use a browser on PC-C to download the Cisco AnyConnect Secure Mobility Client software from the ASA. After the software is downloaded, you will install the AnyConnect software to PC-C and then establish an SSL VPN connection to the ASA. 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** **Note:** You will need to accept all security messages. If authentication fails troubleshoot below.	2
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.	ASDM **Monitoring** **VPN** tab Filter by: **AnyConnect Client**	2

Troubleshoot as necessary to correct any issues.

Note: If the AnyConnect client fails authentication, reset the password.

Configuration > Remote Access VPN > Local Users > REMOTEuser > Edit > Identity > Change user password (retype in the correct username and password combo). Click **OK** followed by clicking **Apply**.



Instructor Sign-Off Part 7: _____

Points: _____ of 14

Instructor Note: Have student demonstrate that PC-C has established an SSL VPN connection to the ASA by pinging PC-B. The student should also be able to display the established VPN session using the ASDM on PC-B.

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 (S0/0/0)	Serial 0/1/1 (S0/0/1)

Router Interface Summary

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.