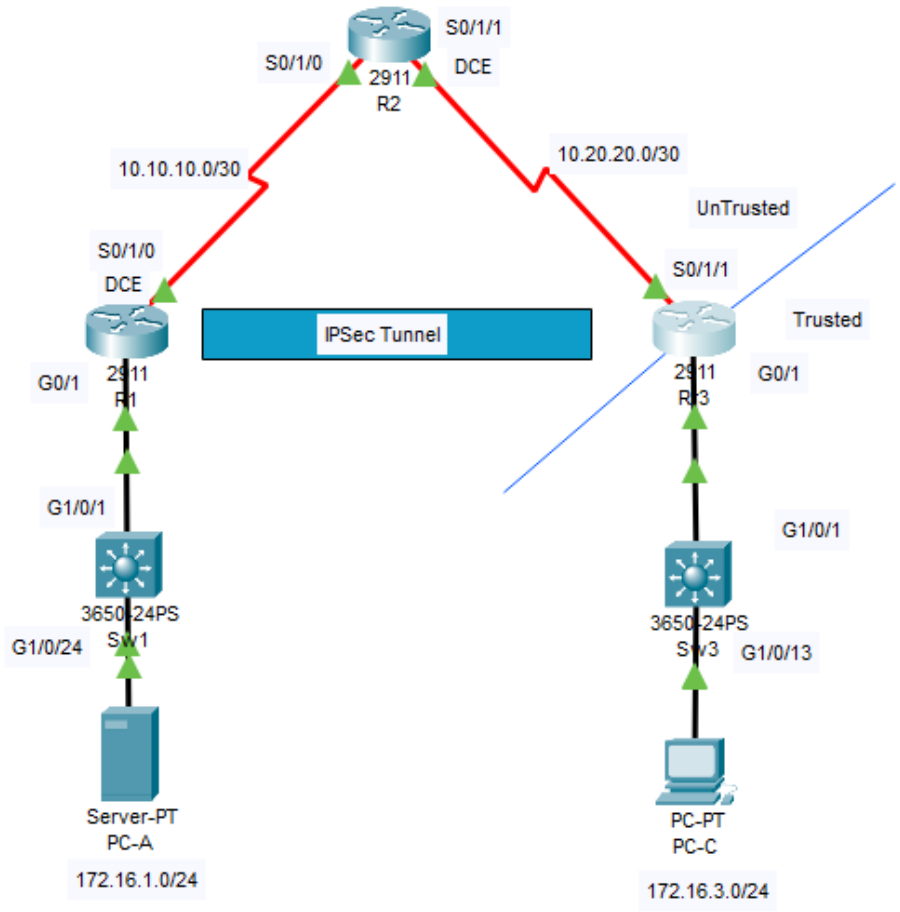
CCNA Security

Skills-Based Assessment PT v1

Topology

Total Exam Marks 62 Marks



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	172.16.1.1	255.255.255.0	N/A	Sw1 G1/0/1
	S0/1/0 (DCE)	10.10.10.1	255.255.255.252	N/A	N/A
R2	S0/1/0	10.10.10.2	255.255.255.252	N/A	N/A
	S0/1/1 (DCE)	10.20.20.2	255.255.255.252	N/A	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A	Sw3 G1/0/1
	S0/1/1	10.20.20.1	255.255.255.252	N/A	N/A
Sw1	VLAN 1	172.16.1.11	255.255.255.0	172.16.1.1	N/A
Sw3	VLAN 1	172.16.3.11	255.255.255.0	172.16.3.1	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1	Sw1 G1/0/24
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	Sw3 G1/0/13

Objectives

Part 1: Configure basic device settings

Part 2: Secure Network Routers

- Configure encrypted passwords and a login banner.
- Configure EXEC timeout on console and VTY lines.
- Configure login failure rates and virtual login enhancements
- Configure SSH access and disable Telnet.
- Configure local AAA authentication.
- Configure a zone-based policy firewall (ZPF)

Part 3: Configure a Site-to-Site VPN

- Configure a Site-to-Site VPN using CLI.

Part 4: Secure Network Switches

- Configure passwords, and a login banner.
- Configure management VLAN access.
- Secure access ports.
- Protect against STP attacks.
- Configure port security and disable unused ports.

Exam Overview

This skills-based assessment is the final practical exam for the course CCNA Security. The exam is divided into four parts. The parts should be completed sequentially. In Part 1, you configure the basic device settings. Static routing is used between the networks. In Part 2 you secure network routers using CLI to configure various IOS features including AAA, ZPF, In Part 3 you configure a Site-to-Site VPN between R1 and R3 through the ISP router (Rtr2). In Part 4 you configure switch security features.

Part 1: Build the Network and Configure Basic Settings to Create the Testing Environment. (3 marks)

In Part 1, you configure basic settings, such as the hostname, interface IP addresses and static routing. Perform steps on routers and switches as indicated.

Step 1: Configure basic settings for all routers.

a. Configure host names as shown in the topology.

b. Configure the interface IP addresses as shown in the IP addressing table.

c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.

d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

Step 2: Configure static default routes on edge routers (R1 and R3).

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

Step 3: Configure static routes on the ISP router (R2).

Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

Step 4: Configure basic settings for each switch.

a. Configure host names as shown in the topology.

b. Configure the VLAN 1 management address on each switch as shown in the IP Addressing table.

c. Configure the IP default gateway for each switch. The gateway for the Sw1 switch is the R1 G0/1 interface IP address. The gateway for the Sw3 switch is the R3 G0/1 interface IP address.

d. Disable DNS lookup to prevent the switches from attempting to translate incorrectly entered commands as though they were host names.

Step 5: Configure PC host IP settings.

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

Step 6: Verify connectivity between PC-A and PC-C.

Step 7: Save the basic running configuration for each router and switch.

Part 2: Secure Network Routers (23 marks)

In Part 2, you configure device access, passwords, firewalls. Perform steps on routers as indicated.

Task 1: Configure Passwords and a Login Banner.

Step 1: Configure a minimum password length of 10 characters on R1 and R3.

Step 2: Configure the enable secret password on R1 and R3

Use an enable secret password type 9 of **ciscoenapa55**

Step 3: Encrypt plaintext passwords.

Step 4: Configure the console lines on R1 and R3.

Configure a console password of **ciscoconpa55** and enable login. Set the exec-timeout to 0 0.

Prevent console messages from interrupting command entry.

Step 5: Configure a login warning banner on routers R1 and R3.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says: "**Unauthorized access strictly prohibited and prosecuted to the full extent of the law!**".

Task 2: Configure Local Authentication Using AAA on R1 and R3.

Step 1: Configure the local user database on R1.

Create a local user account of **Admin01** with a secret password of **Admin01pa55**.

Step 2: Enable AAA services on R1.

Step 3: Implement AAA services using the local database on R1.

a. Create the default login authentication method list using local authentication as the first option and the enable password as the backup option.

b. Exit to the initial router screen that displays: **Rtr1 con0 is now available, Press RETURN to get started**.

c. Log in to the console as **Admin01** with a password of **Admin01pa55** to verify that AAA with local authentication is functioning correctly.

Step 4: Repeat Steps 1 through 3 to configure AAA with local authentication on R3.

Task 3: Configure the SSH Server on R2.

Step 1: Configure the domain name ccnasecurity.com and force the use of version 2

Step 2: Configure a privileged user for login

Username :**SSHUser** password **cisco12345** with privilege level 15

Step 3: Configure the incoming vty lines on R2.

Specify that the vty lines will accept only SSH connections, and login local.

Step 4: Generate the RSA encryption key pair

Configure the RSA keys with 1024 as the number of modulus bits.

Step 5: Verify SSH connectivity to R2 from PC-A.

Launch the SSH client on PC-A, enter the S0/1/0 IP address, and login in as **SSHUser** with the password **cisco12345.**

Task 4: Secure against login attacks on R1

Step 1: Configure the following parameters on R1 to provide enhanced login security for virtual logins.

- Blocking period when login attack detected: 60
- Maximum login failures with the device: 2
- Maximum time period for crossing the failed login attempts: 30
- Log all failed login attempts

Step 2: Save the running configuration to the startup configuration for R1 and R2.

Task 5: Configure a Zone-based Policy Firewall (ZPF) Firewall on R3.

Step 1:

a. Create Security zones names **TRUSTED,** and **UNTRUSTED**

b. Create an inspection class map, with class map name **INSIDE_PROTOCOLS**

c. Inspect the following protocols as they exit from the trusted side of the firewall: **FTP, TFTP, ICMP, TCP** and **UDP**.

d. Create the policy map **INSIDE_TO_INTERNET**

e. Create the Zone Pair **IN_TO_OUT_ZONE**, source **TRUSTED**, destination **UNTRUSTED**

f. Apply zone pairs to appropriate interfaces

Step 2: Verify ZPF functionality.

a. From PC-C, **ping** PC-A at the address **172.16.1.3**. The pings should be successful.

b. From PC-A, **ping** PC-C at IP address **172.16.3.3**. The pings should NOT be successful.

c. From PC-C on the R3 internal LAN, ssh to R2 at IP address **10.20.20.2** and username **SSHUser** password **cisco12345** This should be successful

d. Run the command R3#**show policy-map type inspect zone-pair session.**

e. **Paste your response from the verification step b and d above into your OUTPUT file**

Step 3: Save the running configuration to the startup configuration.

Part 3: Configure a Site-to-Site IPsec VPN between R1 and R3 using CLI

(21 marks)

In Part 3 of this exam, you configure an IPsec VPN tunnel between R1 and R3 that passes through R2.

Task 1: Configure the site-to-site VPN on R1 and R3.

Step 1: Create the IPsec VPN using the following parameters

a. IsaKMP Policy – **Authentication Pre-share, Encryption aes 256, DH group 5, hash sha, Lifetime 86400 seconds.**

b. Pre-share key – **ciscokey**

c. IPSec Transform set – **esp-aes 256.**

d. Traffic to encypt – **PC-A subnet going to PC-C subnet and vice-versa**.

e. Crypto map to include **pfs group 5**, **security association 1 hour.**

Step 2: Save the running-config to the startup-config.

Task 2: Test the VPN between R1 and R3

Note: In this exam you should only be able to create the tunnel for ICMP traffic originated on R3. This is because the Firewall you created on R3 should block ICMP traffic from the untrusted side. Thus, the tunnel will not form if initiated from PC-A but will form if initiated from PC-C

a. On PC-C **ping** the IP address of PC-A at **172.16.1.3**

b. Issue the **`show crypto isakmp sa`** command on R1 to view the security association created.

c. Issue the **`show crypto ipsec sa`** command. How many packets have been received from R3 and decrypted by R1? _____

d. Paste the above responses from b and c into the OUTPUT file.

Part 4: Secure Network Switches

(15 marks)

Task 1: Configure Passwords and a Login Banner on Switches Sw1, and Sw3.

Step 1: Configure the enable secret password.

Use an enable secret password type 9 of **ciscoenapa55**

Step 2: Encrypt plaintext passwords.

Step 3: Configure the console and VTY lines.

a. Configure a console password of **ciscoconpa55** and enable login. Set the exec-timeout to never logout with the exec-timeout 0 0 command.

b. Prevent console messages from interrupting command entry.

c. Configure a vty lines password of **ciscovtypa55** and enable login. Set the exec-timeout to log out after 5 minutes of inactivity.

Step 4: Configure a login warning banner.

Configure a warning to unauthorized users with a message-of-the-day (MOTD) banner that says "**Unauthorized access strictly prohibited and prosecuted to the full extent of the law!**".

Step 5: Repeat Steps 1 through 5 to configure basic settings on switch Sw3.

Task 2: Secure Access Ports

Step 1: Disable trunking on Sw1, and Sw3 access ports.

a. On Sw1, configure ports **G1/0/1** and **G1/0/24** as access mode only.

b. On Sw3, configure ports **G1/0/1** and **G1/0/13** as access mode only.

Task 3: Protect Against STP Attacks

Step 1: Enable PortFast on Sw1, and Sw3 access ports.

PortFast is configured on access ports that connect to a single workstation or server to enable them to become active more quickly.

a. Enable **PortFast** on the Sw1 **G1/0/1** and **G1/0/24** access ports.

b. Enable **PortFast** on the Sw3 **G1/0/1** and **G1/0/13** access ports.

Step 2: Enable BPDU guard on Sw1, and Sw3 access ports.

Enable **BPDU guard** on the switch ports previously configured as access only.

Task 4: Configure Port Security and Disable Unused Ports

Step 1: Configure basic port security for Sw1 G1/0/24, and Sw3 G1/0/13

Set the **maximum MAC addresses to 2** and the violation action to **shutdown.**

Use the **`sticky`** option to allow the secure MAC address that is dynamically learned on a port to the switch running configuration.

Run show port-security on both switches and paste to your OUTPUT file

Step 2: Disable unused ports on Sw1, and Sw3.

As a further security measure, disable any ports not being used on the switch.

a. Ports **G1/0/1** and **G1/0/24** are used on switch Sw1. Shut down the remaining ports

b. Ports **G1/0/1** and **G1/0/13** are used on switch Sw3. Shut down the remaining ports.

Run sh ip int brie on both switches and paste to your OUTPUT file

Step 3: Save the running-config to the startup-config for each switch.

Required output for marking.

Save the output file **SRAN_Skills_OUTPUT_StudentId**
Do a sh run on each device and copy to a single file **SRAN_Skills_sh_run_StudentId**
Save you PT file and save as **SRAN_Skills_PT_studentId**

Upload the three files into Canvas.