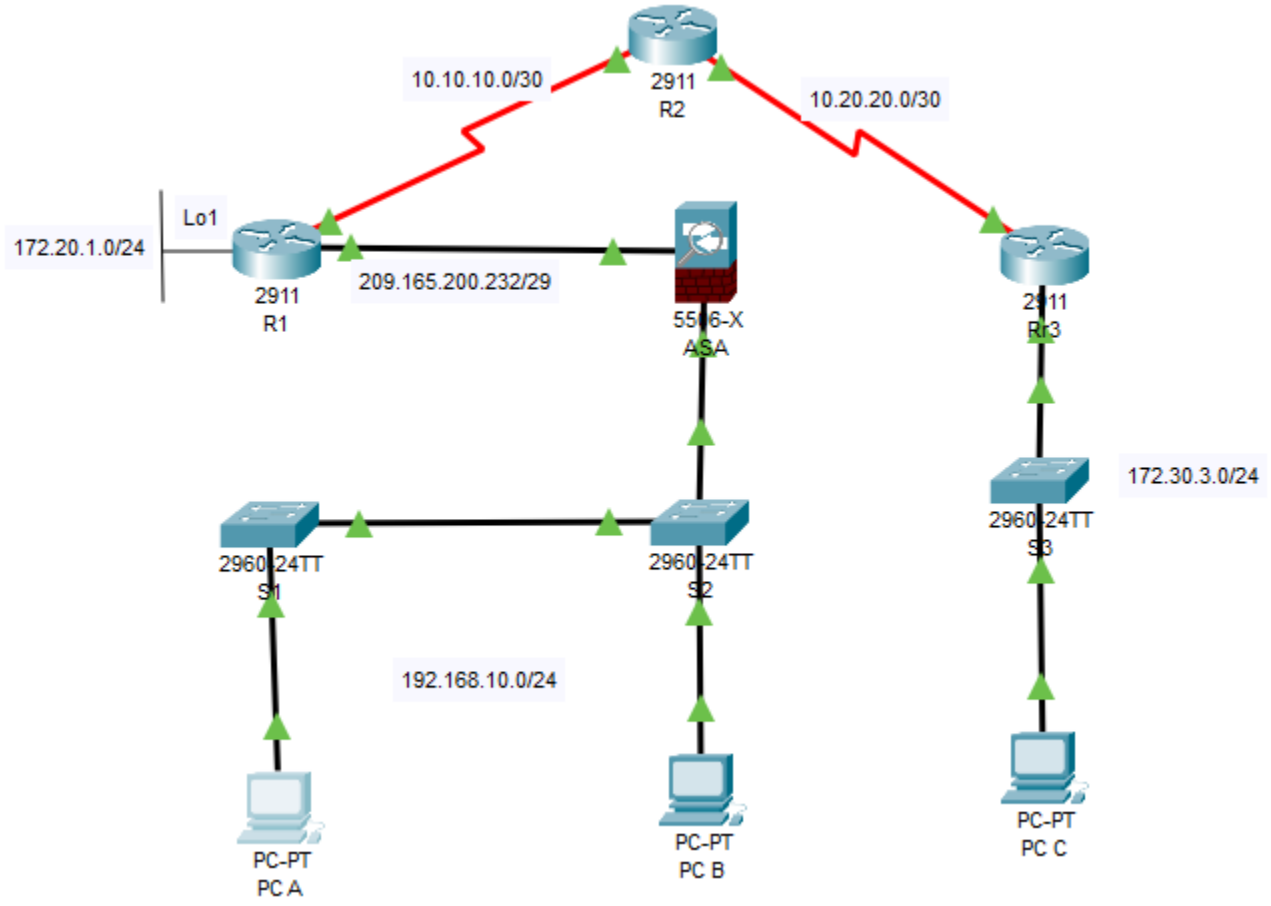
Packet Tracer - Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.233	255.255.255.248	N/A
	S0/1/0 (DCE)	10.10.10.1	255.255.255.252	N/A
	Loopback 1	172.20.1.1	255.255.255.0	N/A
R2	S0/1/0	10.10.10.2	255.255.255.252	N/A
	S0/1/1 (DCE)	10.20.20.2	255.255.255.252	N/A
R3	G0/1	172.30.3.1	255.255.255.0	N/A
	S0/1/1	10.20.20.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN 1	172.30.3.11	255.255.255.0	172.30.3.1
ASA	G1/1	209.165.200.234	255.255.255.248	N/A
	G1/2	192.168.10.1	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	172.30.3.3	255.255.255.0	172.30.3.1

Objectives

- Configure basic router security
- Configure basic switch security
- Configure AAA local authentication
- Configure SSH
- Secure against login attacks
- Configure site-to-site IPsec VPNs
- Configure firewall and IPS settings
- Configure ASA basic security and firewall settings

Scenario

This culminating activity includes many of the skills that you have acquired during this course. The routers and switches are preconfigured with the basic device settings, such as IP addressing and routing. You will secure routers using the CLI to configure various IOS features, including AAA, SSH, and Zone-Based Policy Firewall (ZPF). You will configure a site-to-site VPN between R1 and R3. You will secure the switches on the network. In addition, you will also configure firewall functionality on the ASA.

Requirements

Note: Not all security features will be configured on all devices, however, they would be in a production network.

Configure Basic Router Security

- Configure the following on R1:
  - Minimum password length is 10 characters.
  - Encrypt plaintext passwords.
  - Privileged EXEC mode secret password is **ciscoenapa55**.
  - Console line password is **ciscoconpa55**, timeout is **15** minutes, and console messages should not interrupt command entry.
  - A message-of-the-day (MOTD) banner should include the word **unauthorized**.
- Configure the following on R2:
  - Privileged EXEC mode secret password is **ciscoenapa55**.
  - Password for the VTY lines is **ciscovtypa55**, timeout is **15** minutes, and login is required.

Configure Basic Switch Security

- Configure the following on S1:
  - Encrypt plaintext passwords.
  - Privileged EXEC mode secret password is **ciscoenapa55**.
  - Console line password is **ciscoconpa55**, timeout is **5** minutes, and consoles messages should not interrupt command entry.
  - Password for the VTY lines is **ciscovtypa55**, timeout is **5** minutes, and login is required.
  - An MOTD banner should include the word **unauthorized**.
- Configure trunking between S1 and S2 with the following settings:
  - Set the mode to **trunk** and assign VLAN **99** as the native VLAN.
  - Disable the generation of DTP frames.
- Configure the S1 with the following port settings:
  - F0/6 should only allow access mode, set to **PortFast**, and enable BPDU guard.
  - F0/6 uses basic default port security with dynamically learned MAC addresses added to the running configuration.
  - All other ports should be disabled.

Note: Although not all ports are checked, your instructor may want to verify that all unused ports are disabled.

Configure AAA Local Authentication

- Configure the following on R1:
  - Create a local user account of **Admin01**, a secret password of **Admin01pa55**, and a privilege level of **15**.
  - Enable AAA services.
  - Implement AAA services using the local database as the first option and then the **enable** password as the backup option.

Configure SSH

- Configure the following on R1:
  - The domain name is **ccnasecurity.com**

- The RSA key should be generated with **1024** modulus bits.
- Only SSH version 2 is allowed.
- Only SSH is allowed on VTY lines.

- Verify that PC-C can remotely access R1 (209.165.200.233) using SSH.

Secure Against Login Attacks

- Configure the following on R1:
  - If a user fails to log in twice within a 30-second time span, disable logins for one minute.
  - Log all failed login attempts.

Configure Site-to-Site IPsec VPNs

Note: Some VPN configurations are not scored. However, you should be able to verify connectivity across the IPsec VPN tunnel.

- Enable the Security Technology package license on R1.
  - Save the running configuration before reloading.
- Configure the following on R1:
  - Create an access list to identify interesting traffic on R1.
  - Configure ACL **101** to allow traffic from the R1 Lo1 network to the R3 G0/1 LAN.
- Configure the **crypto isakmp policy 10** Phase 1 properties on R1 and the shared crypto key **ciscovpnpa55**. Use the following parameters:
  - Key distribution method: **ISAKMP**
  - Encryption: **aes 256**
  - Hash: **sha**
  - Authentication method: **pre-shared**
  - Key exchange: **DH Group 5**
  - IKE SA lifetime: **3600**
  - ISAKMP key: **ciscovpnpa55**
- Create the transform set **VPN-SET** to use **esp-aes 256** and **esp-sha-hmac**. Then create the crypto map **CMAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map. Use the following parameters:
  - Transform set: **VPN-SET**
  - Transform encryption: **esp-aes 256**
  - Transform authentication: **esp-sha-hmac**
  - Perfect Forward Secrecy (PFS): **group5**
  - Crypto map name: **CMAP**
  - SA establishment: **ipsec-isakmp**
  - Bind the crypto map (**CMAP**) to the outgoing interface.
- Verify that the Security Technology package license is enabled. Repeat the site-to-site VPN configurations on R3 so that they mirror all configurations from R1.
- Ping the Lo1 interface (172.20.1.1) on R1 from PC-C. On R3, use the **show crypto ipsec sa** command to verify that the number of packets is more than 0, which indicates that the IPsec VPN tunnel is working.

Configure Firewall and IPS Settings

- Configure a ZPF on R3 using the following requirements:
  - Create zones named **IN-ZONE** and **OUT-ZONE**.
  - Create an ACL number **110** that defines internal traffic, which permits all IP protocols from the **172.30.3.0/24** source network to **any** destination.
- Create a class map named **INTERNAL-CLASS-MAP** that uses the **match-all** option and ACL **110**.
- Create a policy map named **IN-2-OUT-PMAP** that uses the class map **INTERNAL-CLASS-MAP** to **inspect** all matched traffic.
- Create a zone pair named **IN-2-OUT-ZPAIR** that identifies **IN-ZONE** as the source zone and **OUT-ZONE** as the destination zone.
  - Specify that the **IN-2-OUT-PMAP** policy map is to be used to **inspect** traffic between the two zones.
  - Assign G0/1 as an **IN-ZONE** member and S0/1/1 as an **OUT-ZONE** member.
- Configure an IPS on R3 using the following requirements:

Note: Within Packet Tracer, the routers already have the signature files imported and in place. They are the default XML files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.

  - Create a directory in flash named **ipsdir** and set it as the location for IPS signature storage.
  - Create an IPS rule named **IPS-RULE**.
  - Retire the **all** signature category with the **retired true** command (all signatures within the signature release).
  - Unretire the **IOS_IPS Basic** category with the **retired false** command.
  - Apply the rule inbound on the S0/1/1 interface.

Configure ASA Basic Security and Firewall Settings

- Configure VLAN interfaces with the following settings:
  - For the G1/2 interface, configure the addressing to use **192.168.10.1/24**.
  - For the G1/1 interface, remove the default DHCP setting and configure the addressing to use **209.165.200.234/29**.
- Configure hostname, domain name, enable password, and console password using the following settings:
  - The ASA hostname is **CCNAS-ASA**.
  - The domain name is **ccnasecurity.com**.
  - The enable mode password is **ciscoenapa55**.
- Create a user and configure AAA to use the local database for remote authentication.
  - Configure a local user account named **admin** with the password **adminpa55**. Do not use the **encrypted** attribute.
  - Configure AAA to use the local ASA database for SSH user authentication.
  - Allow SSH access from the outside host **172.30.3.3** with a timeout of **10** minutes.
- Configure the ASA as a DHCP server using the following settings:
  - Assign IP addresses to inside DHCP clients from 192.168.10.5 to 192.168.10.30.
  - Enable DHCP to listen for DHCP client requests.

- Configure static routing and NAT.
  - Create a static default route to the next hop router (R1) IP address.
  - Create a network object named **inside-net** and assign attributes to it using the **subnet** and **nat** commands.
  - Create a dynamic NAT translation to the outside interface.
- Modify the Cisco Modular Policy Framework (MPF) on the ASA using the following settings:
  - Configure **class-map inspection_default** to **match default-inspection-traffic**, and then exit to global configuration mode.
  - Configure the **policy-map** list **global_policy**. Enter the **class inspection_default** and enter the command to **inspect icmp**. Then exit to global config mode.
  - Configure the MPF **service-policy** to make the **global_policy** apply globally.

Testing.

From PC-C ping 172.20.1.1	should have reply
On R3 do a show crypto ipsec sa	should have evidence of encryption
From PC-C ssh into ASA 209.165.200.234	should be able to ssh into ASA
From R1 do an extended ping 172.30.3.3 from 172.20.1.1	This should fail
From R1 do an extended ping 172.30.3.1 from 172.20.1.1	This should have reply
On R1 do a show crypto ipsec sa	Encryption counter should increase
On PC-A change to DHCP. What is the IP address?	
On PC-B change to DHCP. What is the IP address?	
From PC-A ping 172.20.1.1	should have a reply
From PC-A ping 172.30.3.1	should have a reply
From PC-A ping 172.30.3.3	should fail
On R3 do a show ip ips all	
On R3 do a show zone-pair security	
On R3 do a show policy-map type inspect zone-pair sessions	

For marking you need to paste all of the results from the above testing and capture a show run from each device.