Module 3 Mastery Assessment

Course Competency(s)

CC3.1 Fortify network perimeter to provide an integrated defense

LO3.1.1 Implement best practices to secure network router and switch devices
LO3.1.2 Implement network firewall technologies to secure network communications and protect internal network

Course Outcome(s)

CO1: Demonstrate system security skills through firewall implementation and testing
CO2: Use system tools, practices, and relevant technologies to implement a security plan
CO5: Use relevant tools to secure a network
CO6: Respond to and follow up on various types of attacks
CO12: CAE2Y-CORE-KU 1.3 CYBER DEFENSE. (3) Apply cyber defense methods to prepare a system to repel attacks

Equipment/Supplies Needed

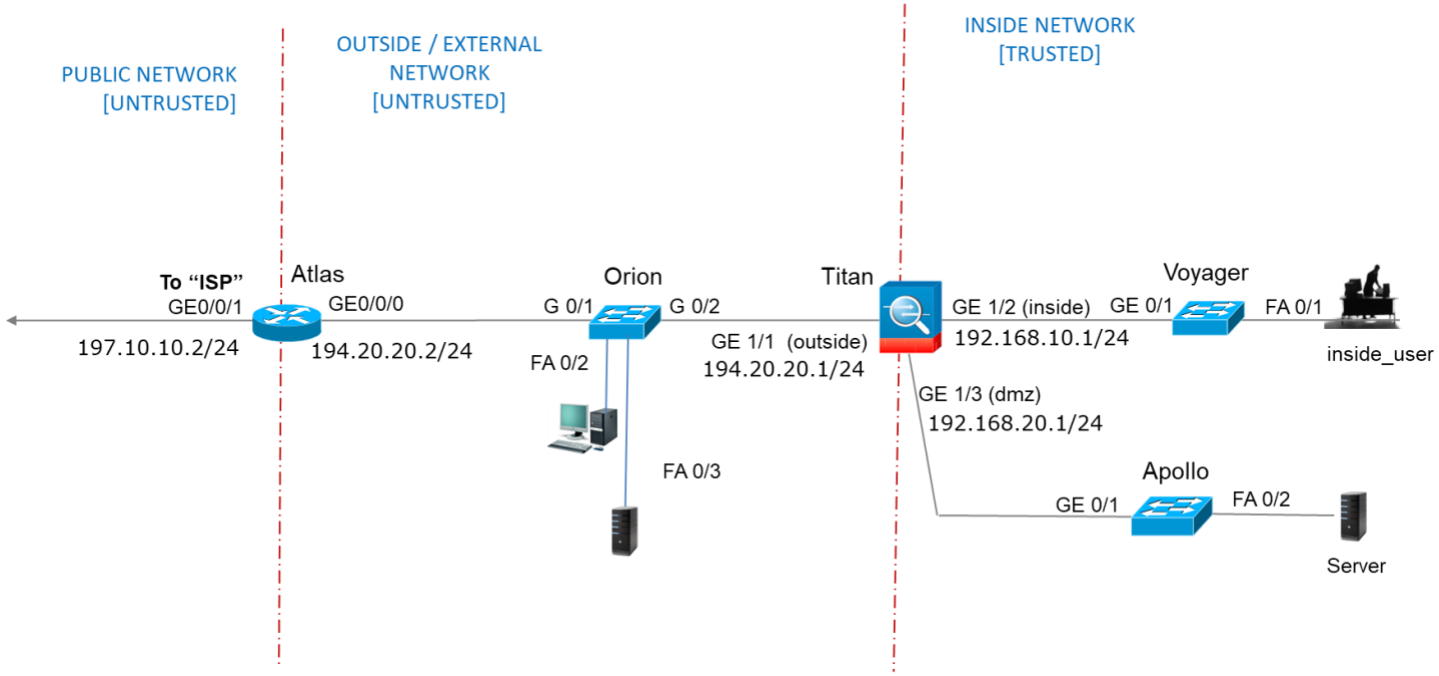
- Computers (2)
- Router (2) [4321 ISR]
- Switch (2) [Catalyst 2960]
- Firewall (1) [ASA 5506-X]
- Cable(s) [if working in physical environment]
- Cisco Packet Tracer (working online)
- Terminal Emulation Software: Putty / Tera Term/ Hyperterm

Procedure

Perform the steps in the order they are presented to you. Answer all questions and record the requested information.

Network Setup

Configure the Network as shown.



Configure hostnames and interface IP addresses for routers, switches, and PCs.

Router Security

*On **Atlas** Router*

1. Disable unused router interfaces (verify shut down interfaces). Verify configuration with following command

   show run | begin interface

2. Encrypt the enable passwords on the router. Verify configuration with following command

   show run | include password

3. Harden the router using autosecure. Verify autosecure using the following command

   show auto secure config

4. Configure a local administrator account Username: **Navigator**
   secret password: **SpaceOut**

5. Verify account/username and password by exiting and logging back into the router. (save configuration before exiting) Obtain a screenshot.

6. Configure Router for SSH access [Replace XXXX with course section number [example: 10Z3]

   Domain name: **MercuryXXXX**.local
   ssh version: 2
   modulus: 1024

7. Verify SSH Verify the SSH configuration with **show ip ssh** command
   Record output in text file.

8. Configure line vty **0 4** to use the local user database for logins and restrict access to only **SSH** connections, with a timeout of **60 seconds** and **3 authentication retries.** Verify using the following command. Record the output.

   show run | begin line vty
   show run | section vty

9. Create the MOTD Warning Banner. Use your last name for the company name

   Warning: By using this "COMPANY" System, you are acknowledging consent to monitoring. All activities performed on this device are logged and monitored.

   Verify using the following command. Record the output.

   show run | include motd

10. Configure the router for TCP and UDP [CBAC] inspection with the following settings:

    Alert: on
    Audit-trail: on
    Timeout: 30 seconds
    Activate the inspection on interface ge 0/0/0

Router Network Address Translation

*On **Atlas** Router*

1. Configure/Define the inside (private network) and outside (public) interfaces

2. Configure Port Address Translations (PAT) using the first 20 ip addresses from the 197.10.10.0/24 network for the pool (PatPool) for external ip addresses.

3. Configure the associated ip access list.

4. Verify configuration using the following commands. Record the output.

   show run | include ip nat
   Show ip nat translation
   show ip access-list

5. Ping to create/verify translations

Switch Security

*On **Orion** Switch*

1. On Orion switch, configure port security on interface FA 0/2 with **sticky MAC addresses** and **protect** mode on interface FA 0/3.

2. Verify with **show port-security** and **show port-security address** commands. Record output in text file.

3. Configure a vlan, **VLAN 10** as a **Native** vlan on the switch.

4. Implement **802.1Q** trunking on **FA 0/2** to use the native VLAN. Verify that trunking is configured on the switch with the **show interface trunk** command. Record the output in the text file.

5. Shut down all **unused physical ports** on the switch. Verify that unused ports are disabled with the **show interfaces status** command. Record the output in the text file.

6. Configure DHCP snooping on **VLAN 20**, interface **FA 0/10**

7. Configure the port FA 0/3 to which the trusted DHCP server is directly connected.

8. Verify configuration with the **show ip dhcp snooping** command

Firewall

*On **Titan** Firewall*

1. Configure the ASA hostname
2. Configure the domain name as **Galaxy.local**
3. Configure the inside and outside interfaces as shown in diagram with appropriate security levels.
4. Verify with the **show interface ip brief** command. Record the output in the text file.
5. configure a **default route** for all firewall internal traffic out to the router.
6. Verify with the **show route** command. Record the output in the text file.
7. Configure the global_policy MFP to allow icmp traffic through the ASA. Verify with **show run policy-map** command. Record the output in the text file.
8. Configure PAT and associated objects. Name the network object **Going-Out**
9. Verify PAT configuration with **show run object** and **show run nat** commands.
10. Configure NAT for DMZ traffic to a web server named **DMZ-Web**.
11. Configure an Access List to allow access to the DMZ server from the outside. Verify configuration with **show ip access-list.**
12. Verify configuration with **show run object** and **show run nat** commands.

Submit a copy of running configurations (text file) and packet tracer file, along with recorded output to Instructor for grading.

Rubric -
Checklist/Single Point Mastery

Criteria Standards for This Competency	Evidence of Mastering Competency 1- yes; 0 = no
Router Security	
1. Verify shut down interfaces **show run | begin interface** command output	
2. Encrypt password **show run | include password** command output	
3. **show auto secure config** command output	
5. account/username and password screenshot	
7. **show ip ssh** command output	
8. **show run | begin line vty** command output	
9. **show run | include motd** command output	
Router NAT	
4. NAT configuration **show run | include ip nat** command output **show ip access-list** command output	
4. NAT configuration **Show ip nat translation** command output	
Switch Security	
2. **show port-security** command output **show port-security address** command output	
Native vlan 4. **show interface trunk** command output 5. **show interfaces status** command output	

8. DHCP snooping on **VLAN 20**, interface **FA 0/10** **show ip dhcp snooping** command output	
Firewall Security	
4. **show interface ip brief** command output	
6. **show route** command output	
7. **show run policy-map** command output	
9. PAT configuration **show run object** command output **show run nat** command output	
11. NAT ACL **show ip access-list** command output	
12. NAT configuration **show run object** command output **show run nat** command output	
Grade [Total Met/18 *100] =	
Comment:	