Module 4 Mastery Assessment - Secure Remote Access

Course Competency(s)

CC4.1 Identify cryptography principles and techniques for secure network communications

LO4.1.2 Implement virtual private networks (VPNs) for secure communications across a 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

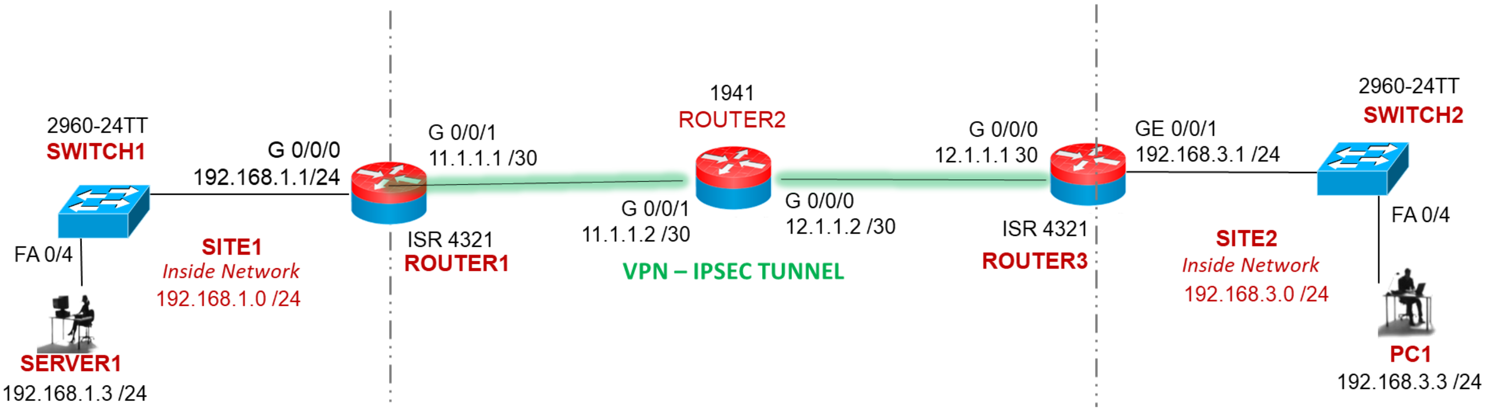
- Cisco Packet Tracer (online)

Procedure

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

Network Setup

1. Configure the network as shown in the diagram below.



   a. Configure hostnames, router interfaces, and PCs as shown in the diagram.

   b. Configure the network for **Static Routing**.

   c. Confirm **network connectivity** by pinging from the PC to the Server. Record successful ping(s).

2. Enable IKE Policies on

   Policy: **10**
   Hash: **sha**
   Authentication: **pre-share**
   Group: **2**
   Lifetime: **3600**
   Encryption: **aes**

3. Configure the pre-shared keys for ROUTER1 and ROUTER3

   a. ROUTER1
   pre-shared key: **cyber123**
   Remote peer: **ROUTER3**

   b. ROUTER2
   pre-shared key: **cyber123**
   Remote peer: **ROUTER1**

4. Configure the Ipsec Transform Set and Lifetime. Create the following transform set on both ROUTER1 and ROUTER3
   a. Transform set tag: **50, ESP transform, AES cipher, ESP and SHA hash function**

5. Define interesting traffic
   a. ROUTER1. Create extended **ACL 101** that permits all IP-related services from the 192.168.1.0 network to the 192.168.3.0 network (don’t forget to put in the Wildcard Masks).

   b. Apply the ACL to the appropriate interface.

   c. ROUTER3. Create extended **ACL 101** that permits all IP-related services from the 192.168.3.0 network to the 192.168.1.0 network (don’t forget to put in the Wildcard Masks).

   d. Apply the ACL to the appropriate interface.

6. Create and Apply a Crypto Maps

   a. ROUTER1
      crypto map: **CMAP 10 ipsec-isakmp**
      match address: **101**
      peer: **ROUTER3**
      pfs: **group2**
      transform-set: **50**
      security-association lifetime seconds: **900**

   b. ROUTER3

      crypto map: **CMAP 10 ipsec-isakmp**
      match address: **101**
      peer: ROUTER1
      pfs: **group2**
      transform-set: **50**
      security-association lifetime seconds: **900**

7. Apply the Crypto Maps on ROUTER1 AND ROUTER2

8. Generate traffic for the VPN with a continuous ping from ROUTER1 to ROUTER3

9. Verify tunnel is built with the following commands. Record the results of each command.

   Show crypto map
   Show crypto isakmp sa
   Show crypto ipsec sa

10. Copy the routers' configuration to a text file.

11. Save packet tracer file.

Rubric -
Checklist/Single Point Mastery

Criteria Standards for This Competency		Evidence of Mastering Competency 1- yes; 0 = no
	Network Setup	
1a	Hostnames Interface Addressing [PCs, Routers, Switches]	
1b	Static Routing	
1c	Successful ping — PC to Server	
	VPN	
14	Show crypto map command output	
14	Show crypto isakmp sa command output	
14	Show crypto ipsec sa command output	
	Grade [Total Met/ Total *100] =	
Comment:		