PT Activity:  Configure and Verify a Site-to-Site IPsec VPN using CLI

**Addressing Table**

| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| --- | --- | --- | --- |
| R1 | Fa0/0 | 192.168.1.1 | 255.255.255.0 |
| S0/0/0 | 10.1.1.2 | 255.255.255.252 |
| R2 | S0/0/0 | 10.1.1.1 | 255.255.255.252 |
| Fa0/0 | 192.168.2.1 | 255.255.255.0 |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 |
| R3 | S0/0/1 | 10.2.2.2 | 255.255.255.252 |
| Fa0/0 | 192.168.3.1 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 |
| PC-B | NIC | 192.168.2.3 | 255.255.255.0 |
| PC-C | NIC | 192.168.3.3 | 255.255.255.0 |

**Learning Objectives**

·         Verify connectivity throughout the network.

·         Configure router R1 to support a site-to-site IPsec VPN with R3.

**Introduction**

The network topology shows three routers. Your task is to configure routers R1 and R3 to support a site-to-site IPsec VPN when traffic flows from their respective LANs. The IPsec VPN tunnel is from router R1 to router R3 via R2. R2 acts as a pass-through and has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

**ISAKMP Phase 1 Policy Parameters**

| **Parameters** | | **R1** | **R3** |
| --- | --- | --- | --- |
| **Key distribution method** | Manual or **ISAKMP** | **ISAKMP** | **ISAKMP** |
| **Encryption algorithm** | **DES**, 3DES, or AES | AES | AES |
| **Hash algorithm** | MD5 or **SHA-1** | **SHA-1** | **SHA-1** |
| **Authentication method** | Pre-shared keys or **RSA** | pre-share | pre-share |
| **Key exchange** | DH Group **1**, 2, or 5 | DH 2 | DH 2 |
| **IKE SA Lifetime** | 86400 seconds or less | **86400** | **86400** |
| **ISAKMP Key** |  | vpnpa55 | vpnpa55 |

**Note:**Bolded parameters are defaults. Only unbolded parameters have to be explicitly configured.

**IPsec Phase 2 Policy Parameters**

| **Parameters** | **R1** | **R3** |
| --- | --- | --- |
| **Transform Set** | VPN-SET | VPN-SET |
| **Peer Hostname** | R3 | R1 |
| **Peer IP Address** | 10.2.2.2 | 10.1.1.2 |
| **Network to be encrypted** | 192.168.1.0/24 | 192.168.3.0/24 |
| **Crypto Map name** | VPN-MAP | VPN-MAP |
| **SA Establishment** | ipsec-isakmp | ipsec-isakmp |

The routers have been pre-configured with the following:

·         Password for console line: **ciscoconpa55**

·         Password for vty lines: **ciscovtypa55**

·         Enable password: **ciscoenpa55**

·         RIP version 2

**Task 1: Configure IPsec parameters on R1**

**Step 1. Test connectivity.**

**Ping** from PC-A to PC-C.

**Step 2. Identify interesting traffic on R1.**

Configure ACL **110** to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny all, there is no need to configure a **deny any any** statement.

**Step 3. Configure the ISAKMP Phase 1 properties on R1.**

Configure the crypto ISAKMP policy **10** properties on R1 along with the shared crypto key **vpnpa55**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

**Step 4. Configure the ISAKMP Phase 2 properties on R1.**

Create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10**and identify it as an **ipsec-isakmp**map.

**Step 5. Configure the crypto map on the outgoing interface.**

Finally, bind the **VPN-MAP** crypto map to the outgoing **Serial 0/0/0** interface. Note: This is not graded.

R1(config)# **interface S0/0/0**

R1(config-if)# **crypto map VPN-MAP**

**Task 2: Configure IPsec Parameters on R3**

**Step 1. Configure router R3 to support a site-to-site VPN with R1.**

Now configure reciprocating parameters on R3. Configure ACL **110** identifying the traffic from the LAN on R3 to the LAN on R1 as interesting.

**Step 2. Configure the ISAKMP Phase 1 properties on R3.**

Configure the crypto ISAKMP policy **10** properties on R3 along with the shared crypto key **vpnpa55**.

**Step 3. Configure the ISAKMP Phase 2 properties on R3.**

Like you did on R1, create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

**Step 4. Configure the crypto map on the outgoing interface.**

Finally, bind the **VPN-MAP** crypto map to the outgoing **Serial 0/0/1** interface. Note: This is not graded.

R1(config)# **interface S0/0/1**

R1(config-if)# **crypto map VPN-MAP**

**Task 3: Verify the IPsec VPN**

**Verify the tunnel prior to interesting traffic.**

Issue the **show crypto ipsec sa** command on R1. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.

**Step 2. Create interesting traffic.**

From PC-A, **ping** PC-C.

**Step 3. Verify the tunnel after interesting traffic.**

On R1, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

**Step 4. Create uninteresting traffic.**

From PC-A, **ping** PC-B.

**Step 5. Verify the tunnel.**

On R1, re-issue the **show crypto ipsec sa** command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted.

**Step 6. Check results.**

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

All contents are Copyright © 1992–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.