Packet Tracer - Configure a Site-to-Site VPN

Objectives

Part 1: Verify Connectivity between Branch and HQ

Part 2: Create and Verify Site-to-Site VPN

Background / Scenario

In this Packet Tracer activity, you will add the commands required to configure a site-to-site IPsec VPN between Branch to HQ. The ISP 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. The Internet Security Association and Key Management Protocol (ISAKMP) is part of IPsec protocol suite and will be used to negotiate the parameters and keys to establish a security association (SA) between the two sites.

Instructions

Part 1: Verify Connectivity between Branch and HQ

In this part, you will verify that devices in the Branch and HQ networks can send and receiving email. You will also use a network sniffer to view the contents of the sent email

Step 1: Configure the HQ Sniffer to filter specific protocol traffic.

You will use the **HQ Sniffer** to capture email traffic that is unencrypted. Later in the activity, you will capture email traffic that is encapsulated and encrypted in an IPsec packet.

a. Click **HQ Sniffer** > **GUI** tab.

b. Click **Show All/None** to clear the filters, and then click **Edit Filters**.

c. In the **Misc** tab, select **IPsec**, **ISAKMP**, and **SMTP**, and then close the window.

d. Click **Clear** to empty the buffer.

Step 2: Send an email between Branch and HQ.

a. Click **Branch**, and then **PC-BR1**.

b. Click **Desktop** tab > **Email**. The **Configure Mail** settings open.

c. Enter the following configurations:

- Your Name: **BRuser1**
- Email address: **BRuser1@mail.cyberhq.com**
- Incoming and Outgoing Mail Server: **mail.cyberhq.com**
- User Name: **BRuser1**
- Password: **Cisco123-** (note that a hyphen is the last character in the password)

d. Click **Save**.

Step 3: Compose and send an email.

a. Click **Compose**.

b. Compose an email to **HQuser1@mail.cyberhq.com**. Use a subject and text of your choice. Click **Send** when finished.

Note: Packet Tracer may take several seconds to converge before you see a **Send Success** message at the bottom of the window.

Step 4: Verify that the email is received.

a. Navigate to **HQ** and click PC **2-1**, which is located in the top right room with the water cooler.

b. Click **Desktop** tab > **Email**.

c. Click **Receive** and open the email you just sent.

Step 5: View protocols used for transmission.

a. Navigate to **Greenville** and click the **HQ Sniffer**.

b. In the buffer, click an SMTP packet, and the scroll to the bottom of the packet to see the field where the SMTP data would be visible to anyone who captured the packet.

Part 2: Create a Site-to-Site VPN

In this Part, you copy and paste the commands necessary to configure the Branch side of the site-to-site VPN to match the already configured HQ router.

Step 1: Add the crypto commands to the Branch router.

a. Navigate to **Branch** > **Branch Wiring Closet** > **BRouter1**.

b. Press the **Enter** key and enter **BRsecurity** as the password.

```
Authorized Access Only!


User Access Verification


Password: BRsecurity
```

c. Enter the **enable** command, and then **BRc1sc0@!** as the enable password.

```
Branch> enable
Password: BRc1sc0@!
Branch#
```

d. Enter global configuration mode.

```
Branch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#
```

e. Copy the following commands and paste them into **BRouter1**. The comments are there for your information and will not impact the configuration.

```
!Comment: Configure an ISAKMP policy with a priority of 10, 256 bit AES
encryption, pre-shared authentication key, D-H group 5, and a lifetime of 900
seconds
!
crypto isakmp policy 10
```

```
 encr aes 256
 authentication pre-share
 group 5
 lifetime 900
 exit
!
! Comment: Configure cisco123 as the pre-shared key and identify the IP
address of the remote endpoint HQ-Edge router.
!
crypto isakmp key cisco123 address 10.0.0.50
!
!Comment: Create an IPsec transform set that is used in negotiations of the
security association (SA)
!
crypto ipsec transform-set Branch-HQ esp-aes esp-sha-hmac
!
!Comment: Create a crypto map that associates traffic that matches an access
list to a peer and various IKE and IPsec settings
!
crypto map CMAP 10 ipsec-isakmp
 set peer 10.0.0.50
 set pfs group5
 set security-association lifetime seconds 1800
 set transform-set Branch-HQ
 match address 101
 exit
```

f. If you check the running configuration with the show run command, you will notice an "Incomplete" comment under the **crypto map** command. This message will disappear after the crypto map is applied to an interface and interesting traffic is defined by an access control list (ACL).

```
Branch(config-if)# end
Branch# show run
Building configuration...
<output omitted>
!
crypto map CMAP 10 ipsec-isakmp
 ! Incomplete
 set peer 10.0.0.50
<output omitted>
!
Branch#
```

Step 2: Associate the crypto map to the router interface.

Apply the crypto map to the **G0/0/0** interface on **BRouter1**. This identifies the endpoint of the tunnel.

```
Branch(config)# interface g0/0/0
Branch(config-if)# crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
Branch(config-if)#
```

Note: The router generates a notification that crypto is now on. However, the SAs are not established until the crypto map has been activated by interesting traffic.

Step 3: Network Address Translation on Branch.

a. Copy and paste the following ACL statements to identify the interesting traffic that will use the tunnel. These ACL statements identify traffic sourced from the Branch network to subnets in the HQ network.

```
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.75.0 0.0.0.255
access-list 101 permit ip 10.0.3.0 0.0.0.255 192.168.99.0 0.0.0.255
access-list 101 permit icmp 10.0.3.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit icmp 10.0.3.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit icmp 10.0.3.0 0.0.0.255 192.168.75.0 0.0.0.255
access-list 101 permit icmp 10.0.3.0 0.0.0.255 192.168.99.0 0.0.0.255
```

b. Check the running configuration to verify that the “incomplete” warning is gone.

Step 4: Configure the NAT ACL to define interesting traffic that is not using the VPN tunnel.

a. Network Address Translation (NAT) will not be executed for traffic that is travelling through the tunnel. Remove ACL 102 from the current configuration.

```
Branch(config)# no access-list 102
```

b. NAT will be used on all traffic that is NOT travelling through the tunnel. Add the following ACL commands to the configuration to identify traffic that will go through network address translation.

Note: The ACL will include access to servers at the ISP.

```
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.3.0.0 0.0.255.255
```

Step 5: Verify the site-to-site VPN configuration.

In this step, you will send another email which will qualify as interesting traffic and initiate the VPN tunnel between **Branch** and **HQ**.

a. Navigate to **PC-BR1** and send another new email to **HQuser1@mail.cyberhq.com**.

b. Navigate to the **HQ Sniffer** and click an IPsec packet. In the packet details window, scroll down to the TCP header and locate the destination port number. Notice that it is 25, which is SMTP, the Simple Mail Transfer Protocol.