**ITT-216 VPN Configuration**

So far, we have new locations, security, and internal routing and servers for the intranet and internet. Now, we want to set up a VPN for the new location sites. The finished network will look something like this:

Graphical user interface, diagram, application

Description automatically generated

Steps:

1. In Packet Tracer, open the **firstInitialLastNameT6ManagmntServer** and save it as **firstInitialLastNameT6VPNConfig**.
2. The Home-Office-Router is being relegated to covering just the internet, remote offices, and home office networks. A new Cisco 2811 [Main-Office-VPN-Router] is taking over the NewLocation connections. In addition, NewLocation routers are being replaced with Cisco 1941 routers so VPNs can be configured between the VPN router and NewLocation routers. Save the old routers off to the side, in case they are needed in the future, and configure the new routers with the same addresses and routing protocol(s). 1941 routers will need to be updated with the IOS 15-k9.
3. Move the serial connections from the Main-Office-Router to the Main-Office-VPN-Router. Use one of the serial ports to connect the Main-Office-Router to the Main-Office-VPN-Router [192.168.255.248 subnet – update EIGRP on both routers!]. Test to make sure the new connections from NewLocation workstations to the Sales workstation work.
4. Configure a VPN form NewLocation1 to Main-Office-VPN-Router, with the other end configured on that router. Ping from all locations to make sure the configuration works for everyone. Copy-paste screenshots of the pings to a Microsoft Word document, to be added to in step 5. Replicate this for each of the other NewLocation routers.
5. Write a summary of network changes for management, including rationales for each change. Copy-paste the configs of the routers, showing the adjacencies and the crypto ISAKMP sa <cr> of the previous steps, along with the report, to a Word document saved as **firstInitialLastNameT6VPNConfig**.

Deliverables:

In a zipped folder named **firstInitialLastNameT6VPNConfig**, include the following items to turn in through the digital classroom:

1. The Word document containing the summary of network changes for management, list of pings, configurations, a screenshot of the workstation window doing the pings, and the screenshot of Packet Tracer showing the completed network.
2. The Packet Tracer file.

Resources:

!--- Create an ISAKMP policy for Phase 1 - Main-Office-VPN-Router to NewLocation routers  
!--- negotiations for the L2L tunnels.

crypto isakmp policy 10

hash md5

authentication pre-share

!--- Specify the pre-shared key and the remote peer address   
!--- to match for the L2L tunnel.

crypto isakmp key vpnuser address 192.168.255.10

crypto isakmp key vpnuser address 192.168.255.14

crypto isakmp key vpnuser address 192.168.255.18

crypto isakmp key vpnuser address 192.168.255.22

crypto isakmp key vpnuser address 192.168.255.26

!

!--- Create the Phase 2 policy for actual data encryption.

crypto ipsec transform-set myset esp-des esp-md5-hmac

!

!--- Create the actual crypto map. Specify   
!--- the peer IP address, transform   
!--- set, and an access control list (ACL) for the split tunneling.

crypto map mymap10 10 ipsec-isakmp

set peer 192.168.255.10

set transform-set myset

match address 101

!

!

crypto map mymap14 10 ipsec-isakmp

set peer 192.168.255.14

set transform-set myset

match address 101

!

!

crypto map mymap18 10 ipsec-isakmp

set peer 192.168.255.18

set transform-set myset

match address 101

!

!

crypto map mymap22 10 ipsec-isakmp

set peer 192.168.255.22

set transform-set myset

match address 101

!

!

crypto map mymap26 10 ipsec-isakmp

set peer 192.168.255.26

set transform-set myset

match address 101

!

!

!

!

!--- Apply the crypto map on the outgoing interface.

!--- DON'T PUT THE MAPS ON UNTIL THE ROUTERS HAVE THE NEW IOS!!

!interface Serial1/1

! crypto map mymap10

!

interface Serial1/2

crypto map mymap14

!

!interface Serial1/3

! crypto map mymap18

!

!interface Serial1/4

! crypto map mymap22

!

!interface Serial1/5

! crypto map mymap26

!

!--- Create an ACL for the traffic to   
!--- be encrypted. In this example,   
!--- the traffic from 192.168.255.9/30 to 192.168.255.10/30   
!--- is encrypted. The traffic that does not match the access list   
!--- is unencrypted for the internet.

access-list 101 permit ip any any

!

!--- Create an ISAKMP policy for Phase 1 - NewLocation1  
!--- negotiations for the L2L tunnels. This is the same for other locations, except peer addresses.

crypto isakmp policy 10

hash md5

authentication pre-share

!--- Specify the pre-shared key and the remote peer address   
!--- to match for the L2L tunnel. Per VPN.

crypto isakmp key vpnuser address 192.168.255.9

!

!--- Create the Phase 2 policy for actual data encryption. Once for all VPNs.

crypto ipsec transform-set myset esp-des esp-md5-hmac

!

!--- Create the actual crypto map. Specify   
!--- the peer IP address, transform   
!--- set, and an access control list (ACL) for the split tunneling.

crypto map mymap 10 ipsec-isakmp

set peer 192.168.255.9

set transform-set myset

match address 100

!

!

!

!

!--- Apply the crypto map on the outgoing interface.

interface Serial0/0/0

crypto map mymap

!

!--- Create an ACL for the traffic to   
!--- be encrypted. In this example,   
!--- the traffic from 192.168.255.9/30 to 192.168.255.10/30   
!--- is encrypted. The traffic that does not match the access list   
!--- is unencrypted for the internet.

access-list 100 permit ip any any

!