**Pacific Tech Center**

Today’s topic: Cisco Lab - DMVPN

Goals: Our current goal today is to create and protect a DMVPN tunnel.

1. Setup the basic VPN Router lab

Diagram

Description automatically generated

1. Validate that the lab is working correctly
   1. The DMVPN cloud is represented by a switch, the IP address of the switch is .10 for any of the segments.
   2. The basic lab only has static routes for the different segments, you should not be able to reach the loopback addresses of the opposite routes at first.

R1: ***ping 200.1.2.2***

R1: ***ping 200.1.3.3***

R2: ***ping 200.1.3.3***

Note: If any of the above ping attempts do not work, try to ping the switch IP from each router and make sure that’s working.

1. Setup GRE based DMVPN tunnels
   1. Create a tunnel interface for each router

***Interface tunnel 123***

***ip address 10.1.1.{Router} 255.255.255.0***

***tunnel source Gi0/0***

***tunnel mode gre multipoint***

***ip nhrp network-id {Router 3 times is a good example, such as 111} each network should have it’s own id***

* 1. Router 1 will have a slightly different configuration then the other routers since this will be the HUB and the other routers will be the spoke. Here is the HUB part of the tunnel configuration.

***ip nhrp map multicast dynamic***

* 1. The SPOKE routers will need to be configured to point to the HUB router as the source of truth for all network connections. And here we will explicitly map the link address for this source of truth as well.

***ip nhrp nhs 10.1.1.1***

***ip nhrp map 10.1.1.1 200.1.1.1***

1. Validate the tunnels, and DMVPN is working as expected on Router1

***show ip nhrp***

***show dmvpn detail***

***ping 10.1.1.2***

***ping 10.1.1.3***

1. Setup EIGRP
   1. First setup eigrp like you would normally, this is for both the HUB and the SPOKE routers

***router eigrp 100***

***network {loopback ip address, such as 1.1.1.1 0.0.0.0}***

***network {tunnel ip address, such as 10.1.1.1 0.0.0.0}***

* 1. Because are goal is to allow each of the nodes to be able to communicate with each other directly without going to us (after the initial setup), we need to modify eigrp a little bit. We will need to first disable split horizon so we can advertise routes coming from let’s say HUB1 over to HUB2 which by default would be blocked on the same interface to prevent loop situations. In addition, we do not want to be the middleman for their communications so we will not advertise ourselves as the next hop.

***interface tunnel 123***

***no ip split-horizon eigrp 100***

***no ip next-hop-self eigrp 100***

* 1. For the SPOKE routers we will need to setup multicast mapping on the tunnel going to the HUB router.

***interface tunnel 123***

***ip nhrp map multicast 200.1.1.1***

1. Validate that you can reach from router 2 to router 1 and router 3 loop back addresses

***show ip route eigrp | begin Gate***

***ping 1.1.1.1***

***ping 3.3.3.3***

1. Now let’s protect the tunnels behind IPSEC, first setup the ISAKMP and IPSEC policies for each router. For simplicity of this lab, we will use the same information for all routers.

***crypto isakmp policy 10***

***hash md5***

***authentication pre-share***

***group 2***

***encryption 3des***

***crypto isakmp key cisco address 0.0.0.0***

***crypto ipsec transform-set TSET esp-des esp-md5-hmac***

***mode transport***

***crypto ipsec profile TST***

***set transform-set TSET***

***interface tunnel 123***

***tunnel protection ipsec profile TST***

1. Now let’s validate that the encryption/decryption is functional

***show crypto ipsec sa***

***show crypto isakmp sa***

***ping 3.3.3.3 source loopback 0***

***show crypto ipsec sa | include local|remote|#pkts***

1. This completes this lab