**Pacific Tech Center**

Today’s topic: Cisco Lab – FLEXVPN Lab 1

Goals: Our current goal today is to create a FLEXVPN configuration.

1. Setup a dual Data Center lab

Diagram

Description automatically generated

1. Validate that the lab is working correctly
   1. The FLEXVPN cloud is represented by a router, the IP address of the switch is .10 for any of the segments.
   2. Also note that for the branches the router gateway address will always be .1 (example 10.112.1.1/24)
   3. The lab only has the Data Centers the basic parts pre-configured; you will need to setup routing for the MPLS, but other protocols will be used for future labs. And any additional tasks will be part of the lab(s) as well.
2. Time to configure the Site-to-Site configuration between the Data Centers.

Let’s setup the configuratoin, with version 2 they consider it smart-defaults let’s use that for now. We can modify the default configuration anytime and will later on.

***crypto ikev2 keyring Flex-Keys***

***peer HUB***

***address {other router IP address, ex., 172.16.31.2}***

***pre-shared-key HUB-Routers***

***crypto ikev2 profile hubIKEProfile***

***match identity remote fqdn {other DC router, ex. dc2.testlab}***

***identity local fqdn {this router, ex. dc1.testlab}***

***authentication remote pre-share***

***authentication local pre-share***

***keyring local Flex-Keys***

***crypto ipsec transform-set xf1Hub esp-aes 256 esp-sha512-hmac***

***mode transport***

***crypto ipsec profile pf1Hub***

***set transform-set xf1Hub***

***set ikev2-profile hubIKEProfile***

***int tunnel30***

***ip address 172.16.32.1 255.255.255.0***

***tunnel source GigabitEthernet0/1***

***tunnel destination {other DC router link address, ex. 172.16.31.2}***

***tunnel path-mtu-discovery***

***tunnel protection ipsec profile pf1Hub***

1. Now that you have the two Data Centers communicating with Site-to-Site, it’s time to configure the data center routers to support spoke to hub communications with the branches.

***aaa new-model***

***aaa authorization network FLEXVPN local***

***ip local pool FlexPool 10.1.1.2 10.1.1.254 (for dc1, 10.2.1.x for dc2)***

***crypto ikev2 name-mangler DomainName***

***fqdn domain***

***crypto ikev2 authorization policy branch10m.testlab***

***aaa attribute list 10M-Branch***

***pool FlexPool***

***route set interface  
crypto ikev2 authorization policy branch25m.testlab***

***aaa attribute list 25M-Branch***

***pool FlexPool***

***route set interface***

***crypto ikev2 authorization policy testlab***

***route set interface***

***aaa attribute list 10M-Branch***

***attribute type interface-config “bandwidth 10000” protocol ip***

***aaa attribute list 25M-Branch***

***attribute type interface-config “bandwidth 25000” protocol ip***

***int Loopback0***

***ip address 10.1.1.1 255.255.255.255 (10.2.1.1 for dc2)***

***crypto ikev2 keyring Flex-Keys***

***peer Branches***

***address 200.0.0.0 255.0.0.0***

***pre-shared-key Branch-Keys***

***crypto ikev2 profile spokeIKEProfile***

***match identity remote fqdn domain branch10m.testlab***

***match identity remote fqdn domain branch25m.testlab***

***match identity remote fqdn domain testlab***

***identity local fqdn {routerName}***

***authentication remote pre-share***

***authentication local pre-share***

***keyring local Flex-Keys***

***aaa authorization group psk list FLEXVPN name-mangler DomainName***

***virtual-template 1***

***crypto ipsec transform-set xf1Spoke esp-aes 256 esp-sha-hmac***

***mode transport***

***crypto ipsec profile pf1Spoke***

***set transform-set xf1Spoke***

***set ikev2-profile spokeIKEProfile***

***interface Virtual-Template1 type tunnel***

***ip unnumbered Loopback0***

***tunnel source Gi0/2***

***tunnel path-mtu-discovery***

***tunnel protection ipsec profile pf1Spoke***

***ip nhrp network-id 1***

***ip nhrp redirect timeout 3***

***ip nhrp shortcut virtual-template 1***

1. Time to configure the Branch Routers, don’t forget to check to make sure that the tunnel is up before going to the next step

***aaa new-model***

***aaa authorization network FLEXVPN local***

***crypto ikev2 authorization policy Flex-IKEv2-Policy***

***route set interface***

***crypto ikev2 keyring Flex-Keys***

***peer FlexPeers***

***address 200.0.0.0 255.0.0.0***

***pre-share-key Branch-Keys***

***crypto ikev2 profile spokeIKEProfile***

***match identity remote fqdn dc1.testlab***

***identity local fqdn {routerName}***

***authentication remote pre-share***

***authentication local pre-share***

***keyring local Flex-Keys***

***aaa authorization group psk list FLEXVPN Flex-IKEv2-Policy***

***crypto ipsec transform-set xf1Flex esp-aes 256 esp-sha-hmac***

***mode transport***

***crypto ipsec profile pf1Flex***

***set transform-set xf1Flex***

***set ikev2-profile spokeIKEProfile***

***int Tunnel200***

***shut***

***ip address negotiated***

***bandwidth 10000 (for the 10m branches, 25000 for the 25m branches)***

***tunnel source GigabitEthernet0/0***

***tunnel destination dc1.testlab***

***tunnel protection ipsec profile pf1Flex***

***tunnel path-mtu-discovery***

***ip nhrp network-id 1***

***no shut***

1. Setup the branch routers to connect to the dc2 router

***crypto ikev2 profile spokeIKEProfile***

***match identity remote fqdn dc2.testlab***

***int Tunnel201***

***shut***

***ip address negotiated***

***bandwidth 10000 (for the 10m branches, 25000 for the 25m branches)***

***tunnel source GigabitEthernet0/0***

***tunnel destination dc2.testlab***

***tunnel protection ipsec profile pf1Flex***

***tunnel path-mtu-discovery***

***ip nhrp network-id 1***

***no shut***

1. Now let’s setup a simple dynamic routing configuration for all routers (except for the MPLS which is supposed to be a carrier)

***router eigrp 50***

***network 10.0.0.0***

1. Try pinging from any host computer to another and if everything works, we can move to the next step which is optimizing the connection between the peers.

Prior to making these changes, baseline the traceroute so you can tell the difference.

(From router br1 perform the following from the User1 to User2, User2 to User1)

***traceroute -n 10.112.2.100 (or 10.112.1.100 if from User2)***

(Now go ahead and make the configuration changes on both branch routers)

***crypto ikev2 name-mangler DomainName***

***fqdn domain***

***crypto ikev2 authorization policy branch10m.testlab***

***route set interface***

***crypto ikev2 authorization policy branch25m.testlab***

***route set interface***

***crypto ikev2 authorization policy testlab***

***route set interface***

***no crypto ikev2 authorization policy Flex-IKEv2-Policy***

***crypto ikev2 profile spokeIKEProfile***

***match identity remote fqdn domain branch10m.testlab***

***match identity remote fqdn domain branch25m.testlab***

***match identity remote fqdn domain testlab***

***no match identity remote fqdn dc1.testlab***

***no match identity remote fqdn dc2.testlab***

***aaa authorization group psk list FLEXVPN name-mangler DomainName***

***virtual-template 1***

***interface Tunnel200***

***shut***

***ip nhrp shortcut virtual-template 1***

***interface Virtual-Template1 type tunnel***

***bandwidth 10000***

***ip unnumbered Tunnel200***

***ip nhrp network-id 1***

***ip nhrp shortcut virtual-template 1***

***tunnel source GigabitEthernet0/0***

***tunnel destination dc1.testlab***

***tunnel path-mtu-discovery***

***tunnel protection ipsec profile pf1Flex***

***interface Tunnel200***

***no shut***

(Notice that we did not modify the bandwidth of the virtual interface based on the circuit, we will address that in a later lab involving QoS)

(Now perform the following commands to see the difference from when you baselined, since you need to initiate the spoke-to-spoke communications before the tunnel will try to come up, we will have to ping prior to traceroute from User1 to User2 and then try it from User2 to User1)

***(User1) traceroute -n 10.112.2.100***

***(User2) traceroute -n 10.112.1.100***

1. Troubleshooting tools

*ping … source …*

*traceroute source … numeric*

*show ip route*

*show ip int brief*

*show interface …*

*show access-list*

Live debugging can really make a difference in figuring out the issue

*debug crypto ikev2 error*

*debug crypto ikev2 internal*

Note that you can speed up getting the debug messages by bouncing the tunnel in question

Don’t forget to look at the syslog messages, if you see things like not receiving IPsec type of messages, you know the other side of the tunnel is missing something.

*show log*

*show crypto ikev2 authorization policy*

*show crypto ikev2 sa*

*show crypto ikev2 sa detail*

*show crypto ikev2 sa remote … detail*

*show crypto session brief*

*show crypto ipsec sa*

1. This completes this lab