Lab 8

1. Setting up vpn part 1
    a. Create ISAKMP policy on each router (IKE phase 1 and 2)
        i. global conf
            1. crypto isakmp policy 1
                a. encryption aes 128
                b. authentication pre-share
                c. group 2
            2. crypto ipsec transform-set ____ (name) esp-aes esp-sha-hmac
    b. Specifics of each VPN
        i. define pre-shared ISAKMP key
            1. global conf
                a. crypto isskmp key 0 ___ (password) address ____ (end-point of vpn)
                b. ip route ____ (destination subnet and mask) ____ (next hop ip)
                c. access-list 101 permit ip host ____ (source) host ____ (destinatoin)
                d. crypto map ____ (name) ____ (number) ipsec-isakmp
                    i. *** if more than one vpn give different crypto map number ***
                    ii. set peer ____ (end-point)
                    iii. set transform -set _____ (name define before)
                    iv. match address ____ (access list name)

            2. interface conf
                - a. crypto map ____ (name)

    - c. Troubleshooting
        - i. sh crypto isakmp sa
        - ii. to clear SAs
            1. clear crypto sa

2. Nat: Part 2
    - a. picture
3. Easy VPN: Part 4
    - a. Enable AAA for authentication
        - i. global conf of router with network we are vpning to
            1. aaa new-model
            2. aaa authentication login ____ (name) local
            3. aaa authorization network ____ (name) local
            4. aaa session-id common
    - b. Specify Username and Password users should use
        - i. global conf
            1. username ___ (name) password 0 _____ (name)
            2. crypto isakmp policy 3
                - a. hash md5
                - b. authentication pre-share
                - c. group 2
    - c. specify how server will recognize clients (group username and password)
        - i. crypto isakmp client configuration group ____ (name)

    ii. key ___ (name)
    iii. pool ____ (name)

d. IPsec transform set
    i. crypto ipsec transform-set ___ (name) esp-des esp-md5-hmac
    ii. crypto dynamic-map dynmap 10
        1. set transform-set ___ (name)
        2. reverse-route

e. Assign features to crypto map
    i. crypto map ____ (name) client authentication list ___ (aaa authentication login)
    ii. crypto map ___ (name) isakmp authorization list ___ (aaa authentication network)
    iii. crypto map ____ (name) client configuration address initiate
    iv. crypto map ____ (name) client configuration address respond
    v. crypto map ___ (name) ___ (dynamic-map number) dynamic ____ (dynamic-map name)

f. Associate crypto map with public interface
    i. interface conf
        1. crypto map ____ (name)

g. Assign IP pool to be used by remote users
    i. global conf
        1. ip local pool ____ (group pool name) ____ (address range)

h. Configure pat
    i. interface conf

1. public facing interface
   a. ip nat outside
2. inside facing interface
   a. ip nat inside
3. global conf
   a. access-list ___ (number) permit _____ (permitted inside addresses)
   b. ip nat inside source list ___ (number) interface ____ (interface number) overload

4. DMVPN: Part 5
   a. Step 1: Achieve connectivity of routers through switch
      i. add ip address within the same subnet to the interfaces facing the other routers
   b. Step 2: Configure mGRE and NHRP on hub router
      i. interface tunnel 1
         1. tunnel mode gre multipoint
         2. tunnel source ____ (interface type and number)
         3. ip nhrp map multicast dynamic
         4. ip nhrp network-id ____ (number)
         5. ip nhrp authentication ____ (password)
         6. ip address ______ (virtual ip address of tunnel)
   c. Step 3: Configure spoke routers with mGRE and NHRP
      i. interface tunnel 1
         1. ip address ____

        2. tunnel mode gre multipoint
        3. ip nhrp map multicast dynamic
        4. ip nhrp map ____ (virtual ip of next hop in tunnel) _____ (public ip of next hop)
        5. ip nhrp map multicast ____ (public ip of next hop)
        6. ip nhrp network-id ___ (number)
        7. ip nhrp nhs ____ (virtual ip of next hop in tunnel)
        8. tunnel source ____ (interface and number)
        9. ip nhrp authentication ____ (password)

    ii. Step 3a: Configure ospf to route loopbacks

        1. global conf

            a. router ospf ___ (number)

                i. network ____ (virtual ip network)_____ (wildcard mask) area _____ (number)

                ii. network _____ (other networks)

        2. interface conf

            a. ip ospf network broadcast

            b. ip ospf priority ___ (number; 0 for spokes)

d. Step 4: Configure Ipsec

    i. global conf

        1. crypto isakmp policy ___ (number)

            a. encryption aes 128

            b. authentication pre-share

            c. group 2

2. crypto ipsec transform-set ____ (name) esp-aes esp-sha-hmac
3. crypto isakmp key 0 ___ (password) address 0.0.0.0 (all addresses)
4. crypto ipsec profile mgre
    a. set transform-set ____ (name)

ii. interface conf on tunnel

1. tunnel protection ipsec profile mgre

iii. troubleshooting tunnel ipsec

1. sh crypto session

iv. picture