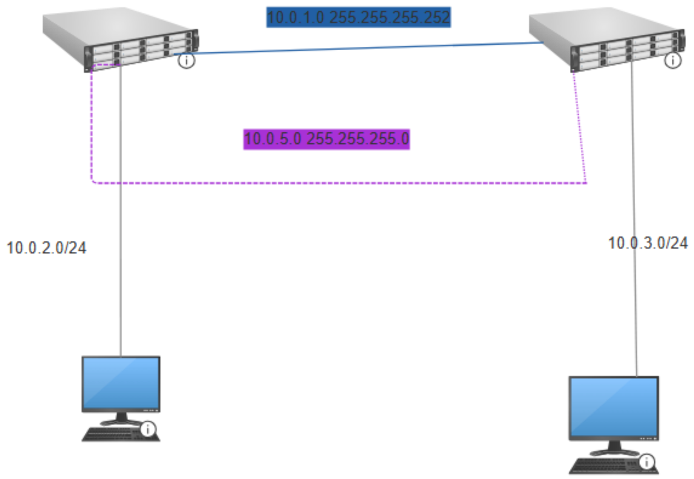
Policy-based R1-ASA vpn



Lets assume R1 is on the left and Asa is on the right. They have ospf configured

ASA

```
interface GigabitEthernet1/1
        nameif OUTSIDE


interface GigabitEthernet1/2
        nameif INSIDE
```

Step 1. Crypto set + access-list

ASA

```
crypto ipsec transform-set VPN-TRANSFORM-SET esp-aes esp-sha-hmac


access-list 101 extended permit ip 10.0.3.0 255.255.255.0 10.0.2.0 255.255.255.0
```

R1

```
access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.3.0 0.0.0.255
```

```
crypto ipsec transform-set vpn esp-aes esp-sha-hmac

    mode tunnel
```

Step 2. Crypto map

ASA

```
crypto map VPN-CRYPTO-MAP 10 match address 101

crypto map VPN-CRYPTO-MAP 10 set peer [R1->ASA address] 10.0.1.1

crypto map VPN-CRYPTO-MAP 10 set transform-set VPN-TRANSFORM-SET

crypto map VPN-CRYPTO-MAP 10 set security-association lifetime seconds 3600

crypto map VPN-CRYPTO-MAP interface OUTSIDE
```

R1

```
crypto map vpn 10 ipsec-isakmp

    set peer [ASA->R1 ip address] 10.2.2.1

     match address [name of the access list] 101

    set transform-set [name of the crypto set] vpn
```

Step 3. Isakmp policy

ASA

```
crypto ikev1 enable OUTSIDE

crypto ikev1 policy 10

    authentication pre-share

    encryption aes

    hash sha

    group 2

    lifetime 86400

    exit
```

R1

isakmp

crypto ~~ikev1~~ policy 10

```
        authentication pre-share
        encryption aes
        hash sha
        group 2
        lifetime 86400
        exit
```

Step 4. Keys + other changes

ASA

```
tunnel-group [R1-ASA ip] 10.0.1.1 type ipsec-l2l
tunnel-group 10.0.1.1 ipsec-attributes
        pre-shared-key cisco
policy-map global_policy
        class inspection_default
                inspect icmp
end
```

R1

```
crypto isakmp key cisco address [ASA->R1 ip] 10.0.1.2
interface [R1-ASA] GigabitEthernet0/0
        crypto map VPN-CRYPTO-MAP
```

Final:

Ping from PC-A and PC-B and vice versa

Show crypto ipsec sa and see if the number of packets encry/decry is increasing

Bonus: Joining VPN + Nat to work together

IF YOU HAVE NAT SET UP and have to also set up VPN THIS IS VERY MUCH NEEDED

```
! 1. Create an object for the remote network

object network REMOTE_VPN_NET

 subnet 10.0.2.0 255.255.255.0

 exit


! 2. Create the NAT exemption rule (Identity NAT)

!   We use '1' to place this rule at the top of the manual NAT rules,

!   ensuring it's processed before the auto/object NAT rule.

nat (INSIDE,OUTSIDE) 1 source static INSIDE INSIDE destination static REMOTE_VPN_NET REMOTE_VPN_NET


! 3. Save your configuration

write memory
```