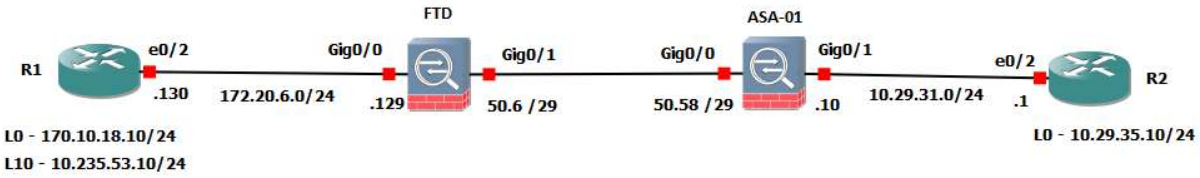
Site-to-Site VPN with NAT

There is a requirement where we have to create a VPN tunnel with one network subnet from each site are allowed and other network subnet / endpoints needs to go through the VPN tunnel with NAT translation.

Topology is



Requirements

1. If traffic sourced from 10.235.53.0/24 and destined to 10.29.35.0/24 and vice versa it should use the VPN tunnel.
2. If traffic sourced from 170.10.18.0/24 and destined to 10.29.35.024(here in this scenario, I have taken only 10.29.35.10) then the traffic shall be NAT with some specific IP address from the subnet 10.235.53.0/24

Firstly, need to make sure that there IP reachability of R1 Loopbacks to FTD and R2 Loopback to ASA.

From FTD towards R1 loopbacks

```
> ping 10.235.53.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.235.53.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
> ping 170.10.18.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 170.10.18.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/10 ms
```

```
ASA-01# ping 10.29.35.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.29.35.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Secondly, we need to test the IP reachability between FTD and ASA and vice versa

```
> ping 10.235.50.58
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.235.50.58, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
>
```

```
ASA-01# ping 10.235.50.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.235.50.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASA-01#
```

IP address summary on the devices

R1

```
R1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       172.20.6.130    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet4       unassigned      YES NVRAM  administratively down down
Loopback0              170.10.18.10    YES NVRAM  up                    up
Loopback10             10.235.53.10    YES NVRAM  up                    up
```

R2

```
R2#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.29.31.1      YES manual up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Loopback10             10.29.35.10     YES manual up                    up
R2#
```

ASA-01

```
ASA-01# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.235.50.58    YES manual up                    up
GigabitEthernet0/1         10.29.31.10     YES manual up                    up
```

FTD

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         172.20.6.129    YES CONFIG up                    up
GigabitEthernet0/1         10.235.50.6     YES manual up                    up
```

Now let's create the VPN tunnel, (please note that due to limitation of demo license on FTD, I have selected DES which is not recommended) and to keep it simple I have used Ikev1.

On ASA,

Phase 1

crypto ikev1 enable out

crypto ikev1 policy 10
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400

tunnel-group 10.235.50.6 type ipsec-l2l
tunnel-group 10.235.50.6 ipsec-attributes
ikev1 pre-shared-key ***

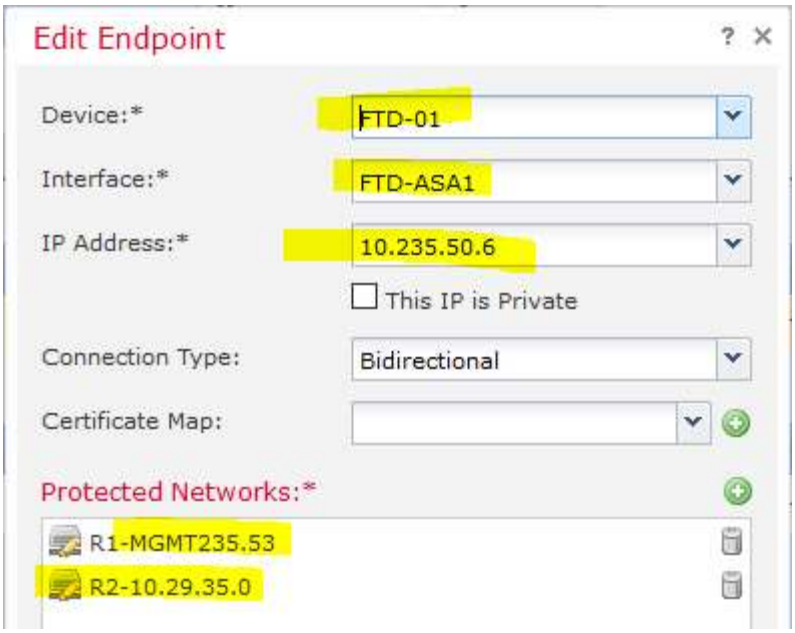
Phase 2

access-list ACL-VPN extended permit ip 10.29.35.0 255.255.255.0 10.235.53.0 255.255.255.0

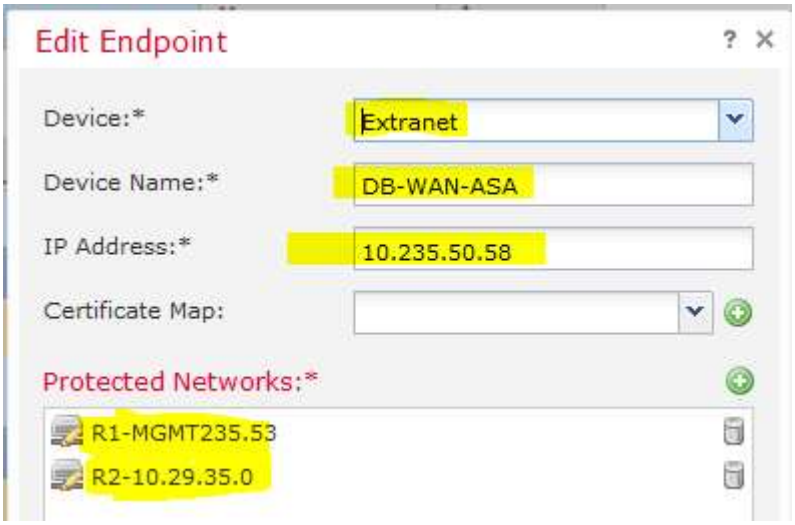
crypto ipsec ikev1 transform-set TSET esp-des esp-sha-hmac

crypto map OUT_MAP 10 match address ACL-VPN
crypto map OUT_MAP 10 set peer 10.235.50.6
crypto map OUT_MAP 10 set ikev1 transform-set TSET
crypto map OUT_MAP 10 set reverse-route
crypto map OUT_MAP interface out

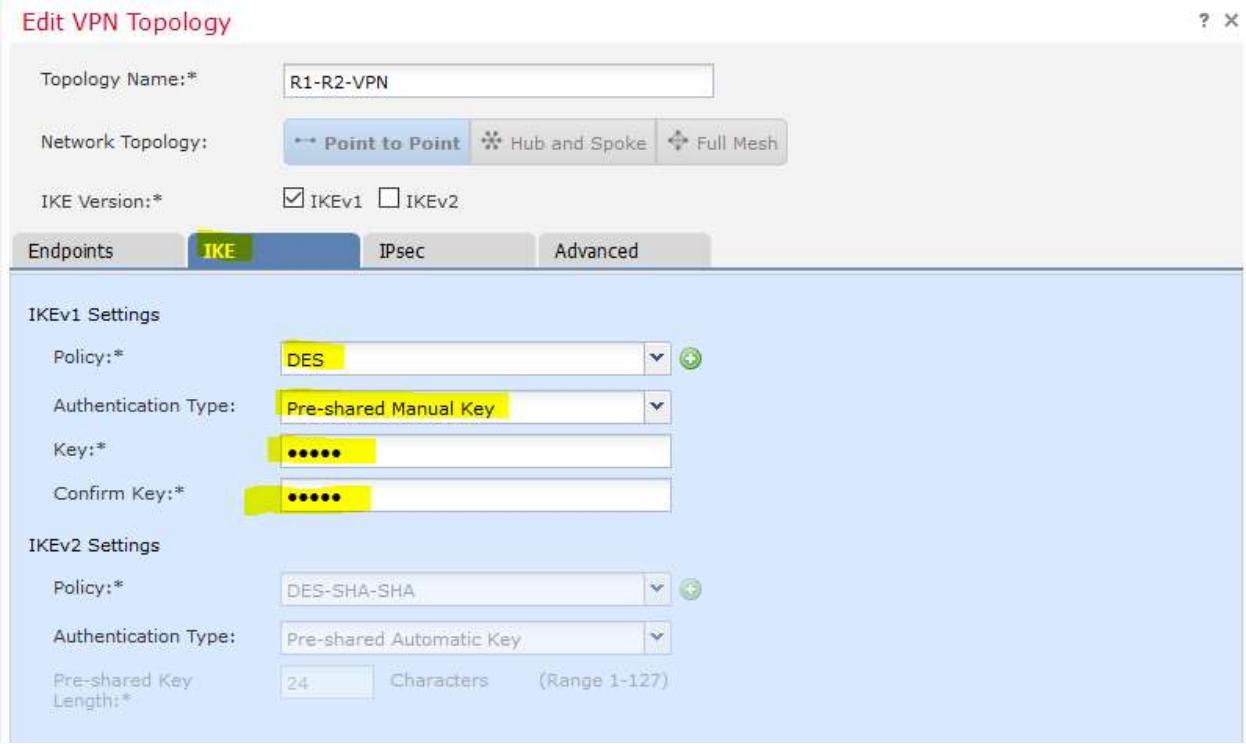
On FTD



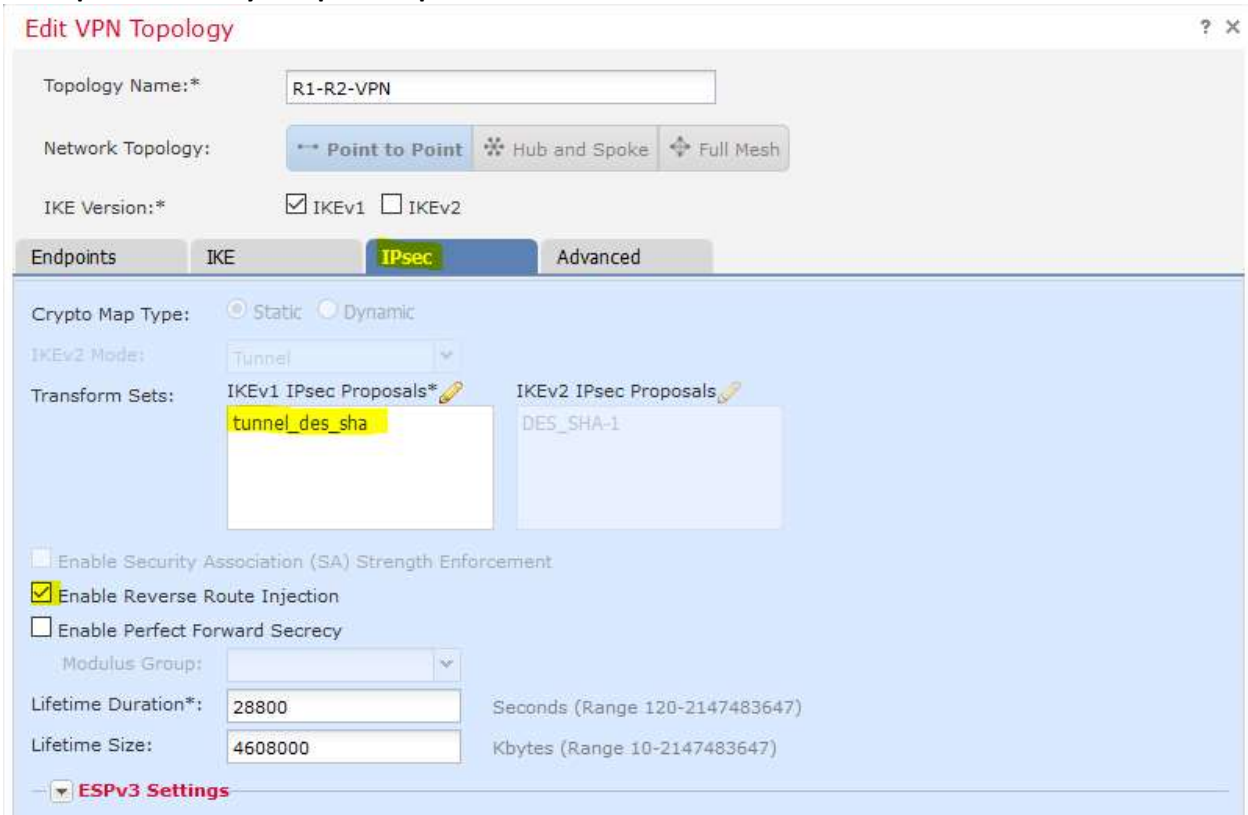
Node A
Device: This will be FTD itself
Interface: This will the interface facing ASA-01
IP Address: Automatically selected by FTD
Connection Type: Can be Bidirectional or Unidirectional
Protected Networks: Same as ASA we allowed only 10.29.35.0/24 and 10.235.53.0/24



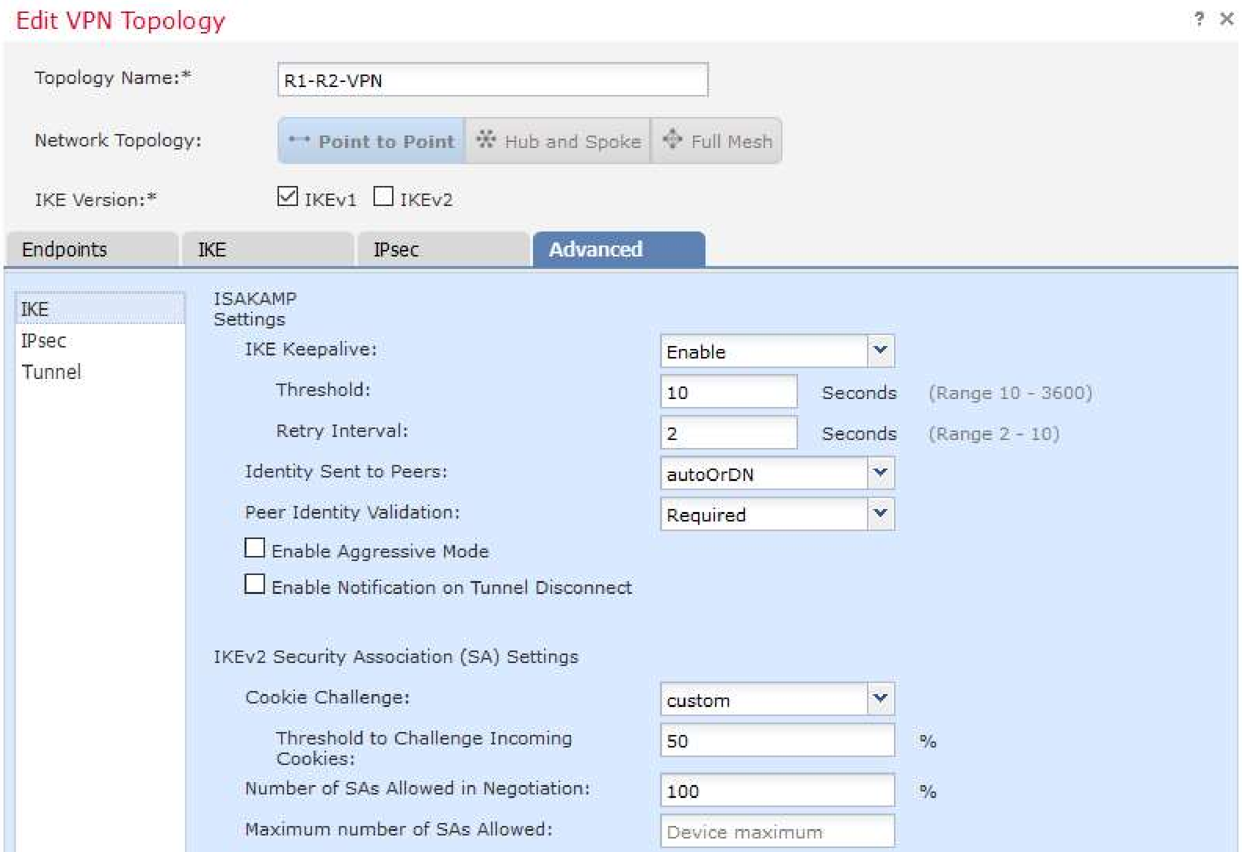
Node B
Device: This will be extranet means any other device
Device Name: Any name
IP Address: Manually type the other end IP address.



Same pre-shared key and phase 1 policies as ASA.



Same Phase2 policies as ASA



Kept the default settings as it is.

Now we will do ping from R1 source Lo 10 – 10.235.53.10 to R2 Lo 10 – 10.29.35.10

```
R1#ping 10.29.35.10 source lo 10 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.29.35.10, timeout is 2 seconds:
Packet sent with a source address of 10.235.53.10
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 2/24/43 ms
R1#
```

Notice, 1st packet got dropped.

Now let us check ASA and FTD, If tunnel is created or not.

```
ASA-01# show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection    : 10.235.50.6
Index         : 20                       IP Addr       : 10.235.50.6
Protocol      : IKEv1 IPsec
Encryption    : IKEv1: (1)DES  IPsec: (1)DES
Hashing       : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx      : 9900                     Bytes Rx      : 9900
Login Time    : 20:07:23 UTC Thu Jul 11 2019
Duration      : 0h:02m:15s
```

FTD

```
> show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection    : 10.235.50.58
Index         : 20                       IP Addr       : 10.235.50.58
Protocol      : IKEv1 IPsec
Encryption    : IKEv1: (1)DES  IPsec: (1)DES
Hashing       : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx      : 9900                     Bytes Rx      : 9900
Login Time    : 20:07:23 UTC Thu Jul 11 2019
Duration      : 0h:02m:28s
Tunnel Zone   : 0
```

```
ASA-01# show crypto ipsec sa
interface: out
    Crypto map tag: OUT_MAP, seq num: 10, local addr: 10.235.50.58

      access-list ACL-VPN extended permit ip 10.29.35.0 255.255.255.0 10.235.53.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.29.35.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.235.53.0/255.255.255.0/0/0)
      current_peer: 10.235.50.6


      #pkts encaps: 99, #pkts encrypt: 99, #pkts digest: 99
      #pkts decaps: 99, #pkts decrypt: 99, #pkts verify: 99
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 99, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.235.50.58/0, remote crypto endpt.: 10.235.50.6/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D1AC66E1
      current inbound spi : BCC860BF

    inbound esp sas:
      spi: 0xBCC860BF (3167248575)
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 81920, crypto-map: OUT_MAP
         sa timing: remaining key lifetime (kB/sec): (4373990/28682)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD1AC66E1 (3517736673)
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 81920, crypto-map: OUT_MAP
         sa timing: remaining key lifetime (kB/sec): (4373990/28682)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
```

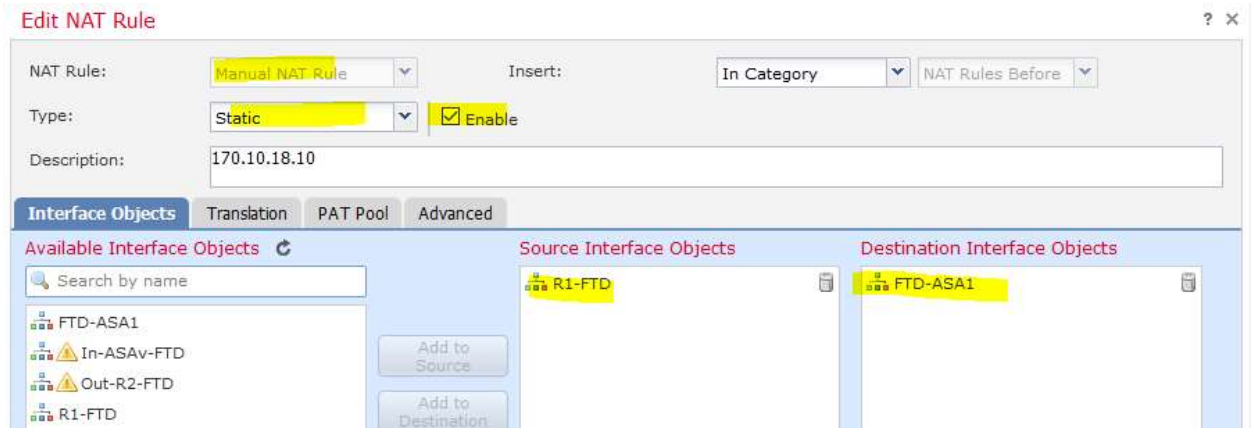
FTD

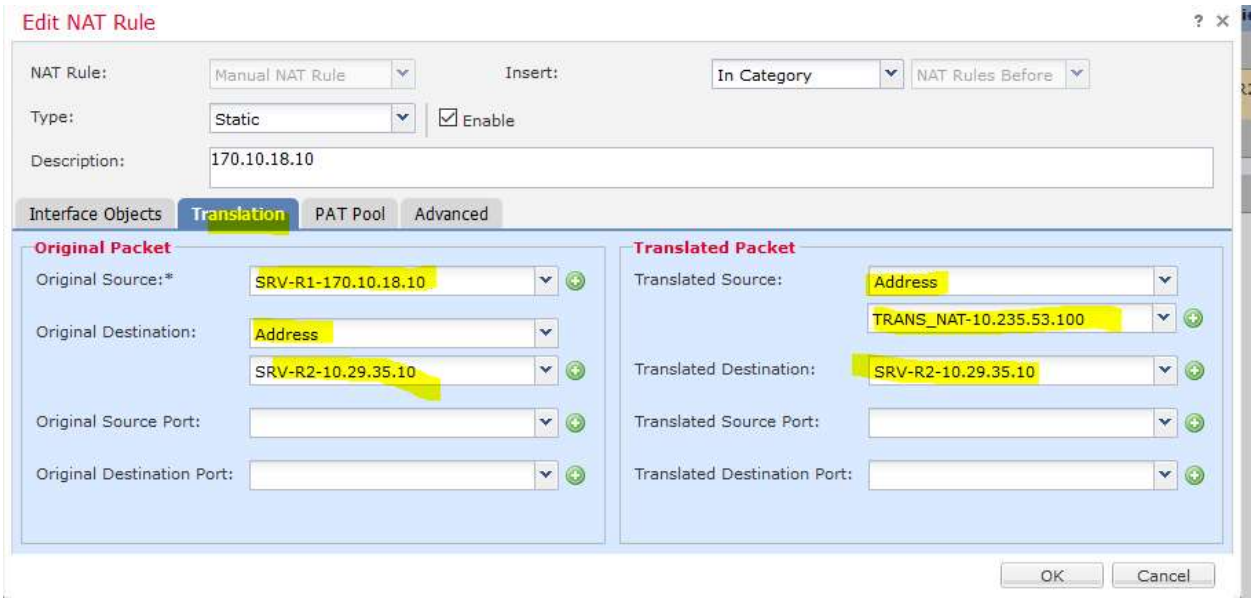
```
> show crypto ipsec sa
interface: FTD-ASA1
    Crypto map tag: CSM_FTD-ASA1_map, seq num: 1, local addr: 10.235.50.6

      access-list CSM_IPSEC_ACL_2 extended permit ip 10.235.53.0 255.255.255.0 10.29.35.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.235.53.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.29.35.0/255.255.255.0/0/0)
      current_peer: 10.235.50.58


      #pkts encaps: 99, #pkts encrypt: 99, #pkts digest: 99
      #pkts decaps: 99, #pkts decrypt: 99, #pkts verify: 99
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 99, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.235.50.6/0, remote crypto endpt.: 10.235.50.58/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: BCC860BF
      current inbound spi : D1AC66E1

    inbound esp sas:
      spi: 0xD1AC66E1 (3517736673)
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 81920, crypto-map: CSM_FTD-ASA1_map
         sa timing: remaining key lifetime (kB/sec): (3914990/28462)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xBCC860BF (3167248575)
         transform: esp-des esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 81920, crypto-map: CSM_FTD-ASA1_map
         sa timing: remaining key lifetime (kB/sec): (3914990/28462)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Now let's try from R2 to R1

```
R2#ping 10.235.53.10 source lo 10 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.235.53.10, timeout is 2 seconds:
Packet sent with a source address of 10.29.35.10
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 7/24/42 ms
R2#
```

Now our 2 requirement comes in where we need to NAT 170.10.18.10 to 10.235.53.100.
We will do twice NAT to achieve the solution. Manual NAT





Now let us give a try

Ping from R1 loopback 0 to R2 Loopback 10

FTD NAT Counters before ping

```
> show nat
Manual NAT Policies (Section 1)
1 (R1-FTD) to (FTD-ASA1) source static SRV-R1-170.10.18.10 TRANS_NAT-10.235.53.100  destination static SRV-R2-10.29.35.10 SRV-R2-10.29.35.10 description 170.10.18.10
    translate_hits = 0, untranslate_hits = 0
```

```
R1#ping 10.29.35.10 source lo 0 re 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.29.35.10, timeout is 2 seconds:
Packet sent with a source address of 170.10.18.10
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 2/24/34 ms
R1#
```

Now NAT Counters

```
> show nat
Manual NAT Policies (Section 1)
1 (R1-FTD) to (FTD-ASA1) source static SRV-R1-170.10.18.10 TRANS_NAT-10.235.53.100  destination static SRV-R2-10.29.35.10 SRV-R2-10.29.35.10 description 170.10.18.10
    translate_hits = 2, untranslate_hits = 2
```

Let us try in opposite way.

```
R2#ping 10.235.53.100 source lo 10 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 10.235.53.100, timeout is 2 seconds:
Packet sent with a source address of 10.29.35.10
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 7/28/49 ms
R2#
```

```
> show nat
Manual NAT Policies (Section 1)
1 (R1-FTD) to (FTD-ASA1) source static SRV-R1-170.10.18.10 TRANS_NAT-10.235.53.100  destination static SRV-R2-10.29.35.10 SRV-R2-10.29.35.10 description 170.10.18.10
    translate_hits = 4, untranslate_hits = 4
>
```

---------------- THANKS---------------------