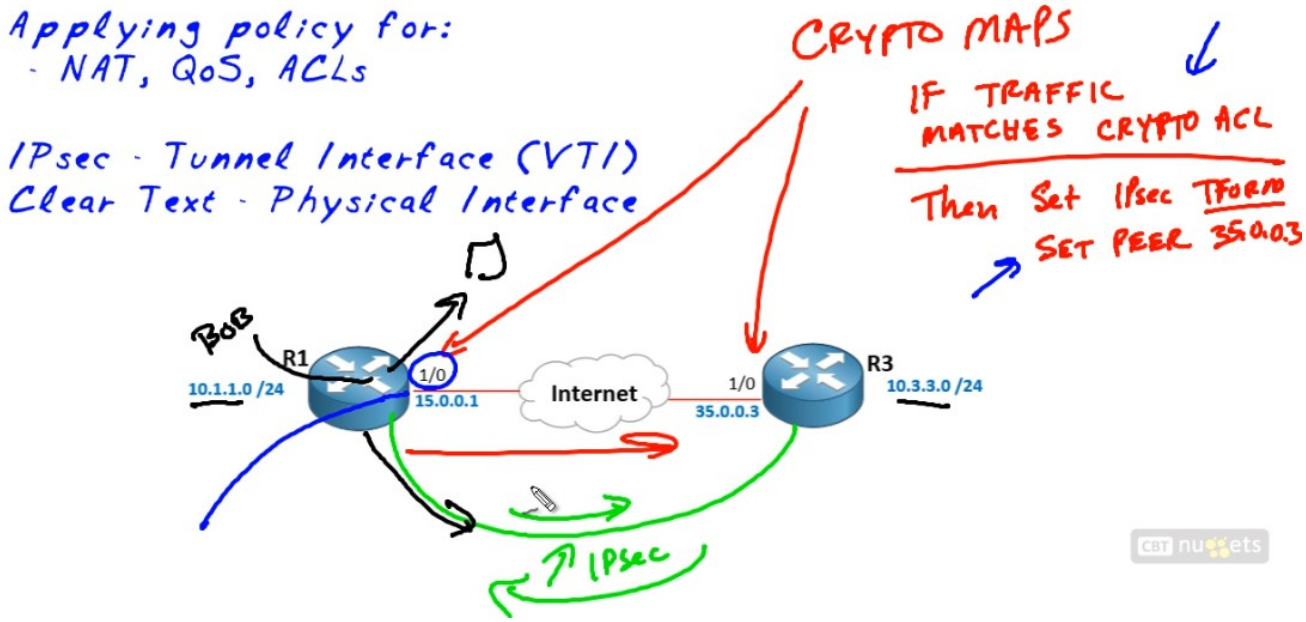
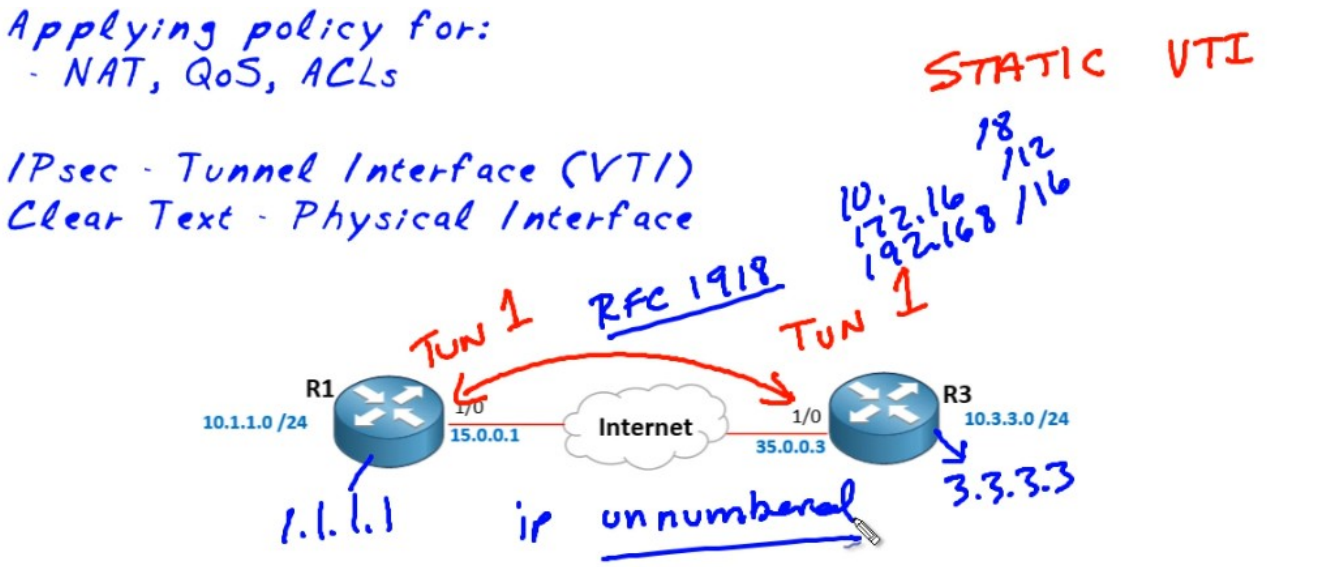
IPsec Virtual Tunnel Interfaces (VTIs)

Using Point to Point VPNs



VTI is used when you need to apply different policies to the actual external interface and the tunnel, so you create virtual tunnel interface for that VPN traffic.



Static VTI

R1:

(previous tunnel 0 config remains the same)

crypto ipsec transform-set P2P-SET esp-aes 256 esp-sha-hmac
mode tunnel
exit
crypto ipsec profile P2P-PROFILE
set transform-set P2P-SET
exit

```
interface tunnel 1
ip unnumbered loopback 0
tunnel source serial 1/0
tunnel destination 35.0.0.3
tunnel mode ipsec ipv4
tunnel protection ipsec profile P2P-PROFILE
exit

router eigrp 777
network 1.1.1.1 0.0.0.0
end
```

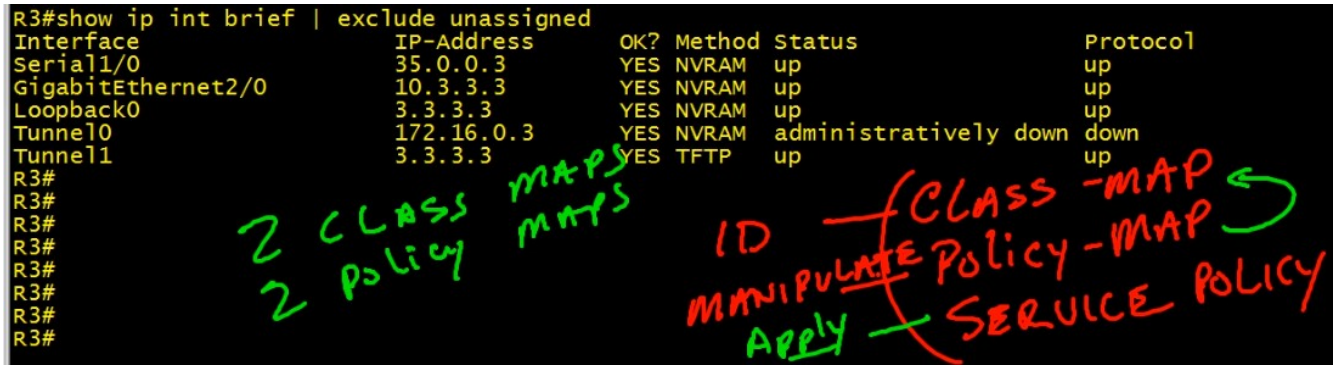
R3:

(previous tunnel 0 config remains the same)

```
crypto ipsec transform-set P2P-SET esp-aes 256 esp-sha-hmac
mode tunnel
exit
crypto ipsec profile P2P-PROFILE
set transform-set P2P-SET
exit

interface tunnel 1
ip unnumbered loopback 0
tunnel source serial 1/0
tunnel destination 15.0.0.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile P2P-PROFILE
exit

router eigrp 777
network 3.3.3.3 0.0.0.0
end
```

Verification Commands:

```
show run | section crypto
show crypto isakmp sa
show crypto ipsec sa
show crypto engine connection active
show ip eigrp neighbors
show ip route eigrp
```



Example Policies applied to the VTI and the external interface:

R3:

class-map match-all VTI-CLASS
match any
class-map match-all Serial-CLASSS
match any

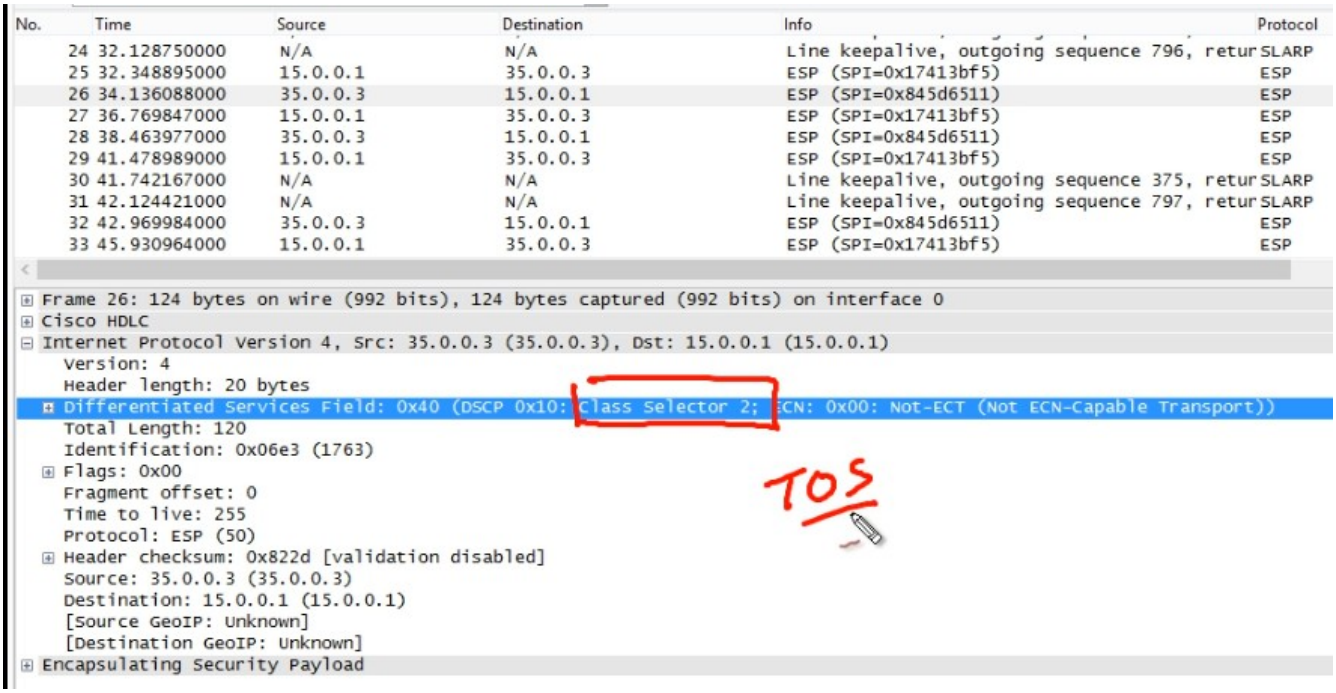
policy-map VTI-MAP
class VTI-CLASS
set precedence 2
exit
exit
policy-map Serial-MAP
class Serial-CLASS
set precedence 4
exit
exit

interface tunnel 1
service-policy output VTI-MAP
exit
interface serial 1/0
service-policy output Serial-MAP
end

Verification Commands:

show class-map (default calss map already exists)
show poliy-map
show policy-map interface tunnel 1
show policy-map interface serial 1/0

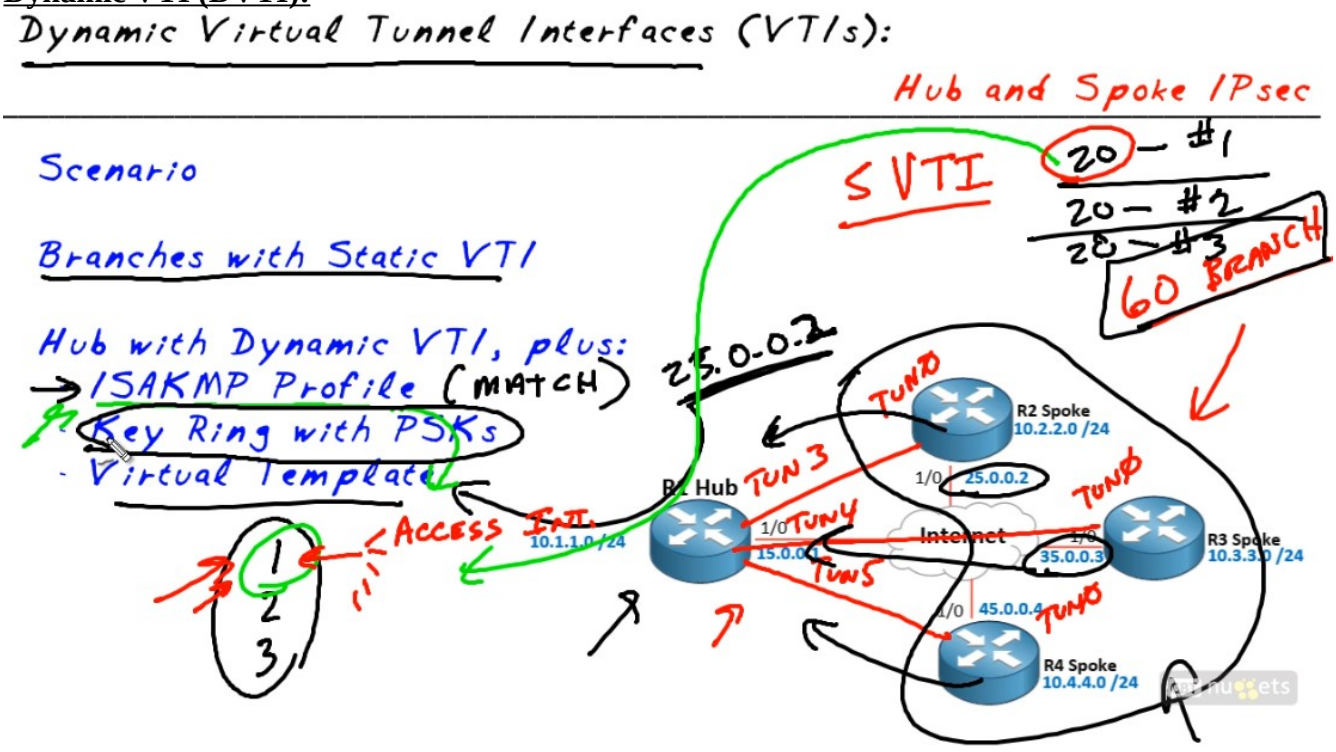
```
R3#show policy-map interface tunnel 1
 Tunnel1

  Service-policy output: VTI-MAP

    Class-map: VTI-CLASS (match-all)
      27 packets, 1618 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence 2
          Packets marked 27

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```



No.	Time	Source	Destination	Info	Protocol
10	13.912872000	35.0.0.3	15.0.0.1	ESP (SPI=0x845d6511)	ESP
11	14.228083000	35.0.0.3	15.0.0.1	Echo (ping) request id=0x0006, seq=0/0, ttl	ICMP
12	14.281118000	15.0.0.1	35.0.0.3	Echo (ping) reply id=0x0006, seq=0/0, ttl	ICMP
13	14.313141000	35.0.0.3	15.0.0.1	Echo (ping) request id=0x0006, seq=1/256, t	ICMP
14	14.347162000	15.0.0.1	35.0.0.3	Echo (ping) reply id=0x0006, seq=1/256, t	ICMP
15	14.377184000	35.0.0.3	15.0.0.1	Echo (ping) request id=0x0006, seq=2/512, t	ICMP
16	14.408203000	15.0.0.1	35.0.0.3	Echo (ping) reply id=0x0006, seq=2/512, t	ICMP
17	15.215741000	15.0.0.1	35.0.0.3	ESP (SPI=0x17413bf5)	ESP
18	15.418880000	N/A	N/A	Line keepalive, outgoing sequence 405, retur	SLARP
19	15.796129000	N/A	N/A	Line keepalive, outgoing sequence 827, retur	SLARP

```
Frame 13: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
Cisco HDLC
Internet Protocol Version 4, Src: 35.0.0.3 (35.0.0.3), Dst: 15.0.0.1 (15.0.0.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x80 (DSCP 0x20: Class Selector 4; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0x0017 (23)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x88fe [validation disabled]
    Source: 35.0.0.3 (35.0.0.3)
    Destination: 15.0.0.1 (15.0.0.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

Dynamic VTI (DVTI):



R1:

crypto isakmp policy 1
encr aes 192
authentication pre-share
group 5
exit

```
crypto keyring OUR-PSKs
pre-shared-key address 0.0.0.0 key cisco123
exit

crypto ipsec transform-set OUR-SET esp-aes 128 esp-md5-hmac
exit
crypto ipsec profile OUR-IPSec-PROFILE
set transform-set OUR-SET
exit

interface virtual-template 1 type tunnel
ip unnumbered loop 0
tunnel mode ipsec ipv4
tunnel protection ipsec profile OUR-IPSec-PROFILE

crypto isakmp profile OUR-IKE-PROFILE
match identity address 25.0.0.2 255.255.255.255
match identity address 0.0.0.0  (don't do it in production)
virtual-template 1
keyring OUR-PSKs
exit

router eigrp 777
no auto-summary
network 1.0.0.0
network 10.0.0.0
end
```

R2:

```
crypto isakmp policy 1
encr aes 192
authentication pre-share
group 5
exit

crypto isakmp key cisco123 adress 0.0.0.0
exit

crypto ipsec transform-set OUR-SET esp-aes 128 esp-md5-hmac
exit
crypto ipsec profile OUR-IPSec-PROFILE
set transform-set OUR-SET
exit

interface tunnel 2
tunnel mode ipsec ipv4
ip unnumbered loopback 0
tunnel source serial 1/0
tunel destination 15.0.0.1
```

tunnel protection ipsec profile OUR-IPSec-PROFILE
exit

router eigrp 777
no auto-summary
network 10.0.0.0
network 2.0.0.0

R3:
crypto isakmp policy 1
encr aes 192
authentication pre-share
group 5
exit

crypto isakmp key cisco123 adress 0.0.0.0
exit

crypto ipsec transform-set OUR-SET esp-aes 128 esp-md5-hmac
exit
crypto ipsec profile OUR-IPSec-PROFILE
set transform-set OUR-SET
exit

interface tunnel 2
tunnel mode ipsec ipv4
ip unnumbered loopback 0
tunnel source serial 1/0
tunel destination 15.0.0.1
tunnel protection ipsec profile OUR-IPSec-PROFILE
exit

router eigrp 777
no auto-summary
network 10.0.0.0
network 3.0.0.0

R4:
crypto isakmp policy 1
encr aes 192
authentication pre-share
group 5
exit

crypto isakmp key cisco123 adress 0.0.0.0
exit

crypto ipsec transform-set OUR-SET esp-aes 128 esp-md5-hmac
exit

crypto ipsec profile OUR-IPSec-PROFILE
set transform-set OUR-SET
exit

interface tunnel 2
tunnel mode ipsec ipv4
ip unnumbered loopback 0
tunnel source serial 1/0
tunel destination 15.0.0.1
tunnel protection ipsec profile OUR-IPSec-PROFILE
exit

router eigrp 777
no auto-summary
network 10.0.0.0
network 4.0.0.0

Verification commands:
show crypto isakmp sa
show crypto engine connections active
show ip int bri | exclude unassigned
show ip route eigrp

```
R1#show ip int brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
Serial1/0                  15.0.0.1        YES NVRAM  up                    up
FastEthernet2/0            10.1.1.1        YES NVRAM  up                    up
Virtual-Template1          1.1.1.1         YES TFTP   down                  down
Virtual-Access2            1.1.1.1         YES TFTP   up                    up
Virtual-Access3            1.1.1.1         YES TFTP   up                    up
Virtual-Access4            1.1.1.1         YES TFTP   up                    up
Loopback0                  1.1.1.1         YES NVRAM  up                    up
R1#
R1#
```

```
R2#show ip route eigrp
     1.0.0.0/32 is subnetted, 1 subnets
D       1.1.1.1 [90/297372416] via 1.1.1.1, 00:08:21, Tunnel2
     3.0.0.0/32 is subnetted, 1 subnets
D       3.3.3.3 [90/310172416] via 1.1.1.1, 00:05:41, Tunnel2
     4.0.0.0/32 is subnetted, 1 subnets
D       4.4.4.4 [90/310172416] via 1.1.1.1, 00:05:29, Tunnel2
     10.0.0.0/24 is subnetted, 4 subnets
D       10.4.4.0 [90/310046976] via 1.1.1.1, 00:05:28, Tunnel2
D       10.3.3.0 [90/310046976] via 1.1.1.1, 00:05:41, Tunnel2
D       10.1.1.0 [90/297246976] via 1.1.1.1, 00:08:21, Tunnel2
R2#
R2#
```

```
R2#traceroute 10.3.3.3

Type escape sequence to abort.
Tracing the route to 10.3.3.3

  1 1.1.1.1 76 msec 64 msec 52 msec
  2 3.3.3.3 88 msec 132 msec 88 msec
R2#
```