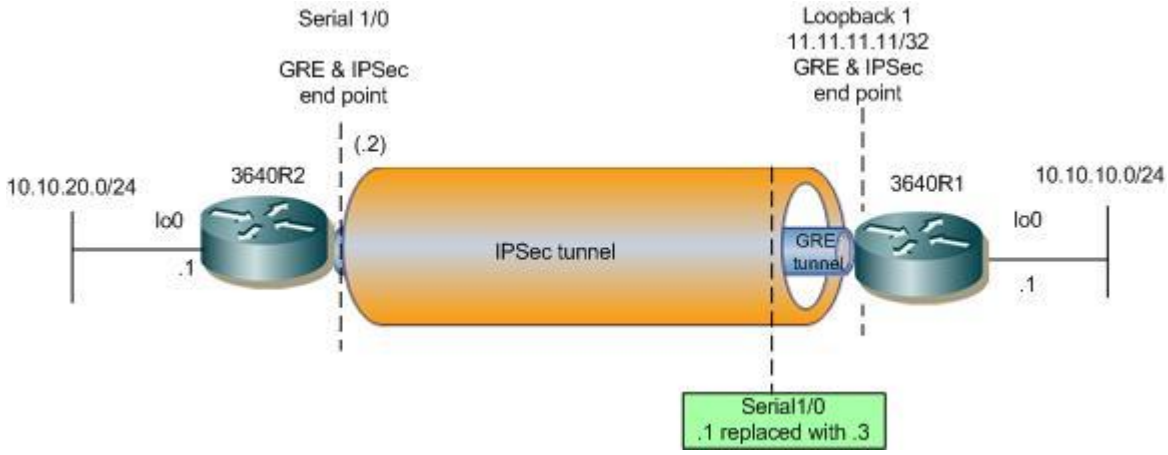

ISAKMP Policy	
Notice that router 3440R1 is identified only by its loopback int (not serial)	

`crypto isakmp policy 10`
`authentication pre-share`
`crypto isakmp key cisco address 11.11.11.11`
`crypto isakmp keepalive 10`
	`crypto isakmp policy 10`
	`authentication pre-share`
	`crypto isakmp key cisco address 192.168.10.2`
	`crypto isakmp keepalive 10`

IPSec policy	
`crypto ipsec security-association idle-time 120` `crypto ipsec transform-set 10 esp-3des esp-sha-hmac`	`crypto ipsec security-association idle-time 120` `crypto ipsec transform-set 10 esp-3des esp-sha-hmac`

IPSec crypto map	
Notice that the tunne l interfaces in both sides will not turn to up until tunnel destination addresses are available for each other (reachable by routing)	
crypto map tor1 1 ipsec-isakmp set peer 11.11.11.11 set transform-set 10 set pfs group1 match address 100	crypto map tor2 local-address Loopback1 crypto map tor2 1 ipsec-isakmp set peer 192.168.10.2 set transform-set 10 set pfs group1 match address 100

First the tunnel is formed between the two routers	
interface Tunnel0 ip address 192.168.20.2 255.255.255.0 keepalive 5 4 tunnel source Serial1/0 tunnel destination 11.11.11.11	interface Tunnel0 ip address 192.168.20.1 255.255.255.0 keepalive 5 4 tunnel source Loopback1 tunnel destination 192.168.10.2
Then crypto maps will be solicited, triggered by GRE traffic. Crypto maps still bound to physical interface.	Crypto maps still bound to physical interface.
interface Serial1/0 ip address 192.168.10.2 255.255.255.0 crypto map tor1	interface Serial1/0 ip address 192.168.10.1 255.255.255.0 crypto map tor2
	interface Loopback1 ip address 11.11.11.11 255.255.255.255
Static routing	
-Interesting traffic will be directed to tunnel interface. -Router 3640R1 address 11.11.11.11 will be used by GRE traffic as dst ip, so will be reachable via serial 1/0	-Interesting traffic will be directed to tunnel interface.
ip route 10.10.10.0 255.255.255.0 Tunnel0 ip route 11.11.11.11 255.255.255.255 Serial1/0	ip route 10.10.20.0 255.255.255.0 Tunnel0

This is the interresting traffic (GRE) that will trigger the crypto map which is bound to the physical interfaces

access-list 100 permit gre host 192.168.10.2 host 11.11.11.11	access-list 100 permit gre host 11.11.11.11 host 192.168.10.2

Troubleshooting:

ISAKMP & IPSEC SAs	
3640R2#sh cry isa sa dst src state conn-id slot 11.11.11.11 192.168.10.2 QM_IDLE 2 0	3640R1#sh cry isa sa dst src state conn-id slot 11.11.11.11 192.168.10.2 QM_IDLE 2 0
3640R2#sh cry ips sa interface: Serial1/0 Crypto map tag: tor1, local addr. 192.168.10.2 protected vrf: local ident (addr/mask/prot/port): (192.168.10.2/255.255.255.255/47/0) remote ident (addr/mask/prot/port):	3640R1#sh cry ips sa interface: Serial1/0 Crypto map tag: tor2, local addr. 11.11.11.11 protected vrf: local ident (addr/mask/prot/port): (11.11.11.11/255.255.255.255/47/0) remote ident (addr/mask/prot/port):

```
(11.11.11.11/255.255.255.255/47/0)

   current_peer: 11.11.11.11:500

     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 1212, #pkts encrypt: 1212, #pkts digest
1212

    #pkts decaps: 1212, #pkts decrypt: 1212, #pkts verify
1212

    #pkts compressed: 0, #pkts decompressed: 0

    #pkts not compressed: 0, #pkts compr. failed: 0

    #pkts not decompressed: 0, #pkts decompress failed: 0

    #send errors 18, #recv errors 0


     local crypto endpt.: 192.168.10.2, remote crypto
endpt.: 11.11.11.11

     path mtu 1500, media mtu 1500

     current outbound spi: 8DDD86EB


     inbound esp sas:
```

```
(192.168.10.2/255.255.255.255/47/0)

   current_peer: 192.168.10.2:500

     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 1240, #pkts encrypt: 1240, #pkts digest
1240

    #pkts decaps: 1240, #pkts decrypt: 1240, #pkts verify
1240

    #pkts compressed: 0, #pkts decompressed: 0

    #pkts not compressed: 0, #pkts compr. failed: 0

    #pkts not decompressed: 0, #pkts decompress failed: 0

    #send errors 2, #recv errors 0


     local crypto endpt.: 11.11.11.11, remote crypto
endpt.: 192.168.10.2

     path mtu 1500, media mtu 1500

     current outbound spi: 868FB46A


     inbound esp sas:
```

```
      spi: 0x868FB46A(2257564778)

        transform: esp-3des esp-sha-hmac ,

        in use settings ={Tunnel, }

        slot: 0, conn id: 2000, flow_id: 1, crypto map:
tor1

        sa timing: remaining key lifetime (k/sec):
(4421374/616)

        IV size: 8 bytes

        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:

      spi: 0x8DDD86EB(2380105451)

        transform: esp-3des esp-sha-hmac ,

        in use settings ={Tunnel, }
```

```
      spi: 0x8DDD86EB(2380105451)

        transform: esp-3des esp-sha-hmac ,

        in use settings ={Tunnel, }

        slot: 0, conn id: 2000, flow_id: 1, crypto map:
tor2

        sa timing: remaining key lifetime (k/sec):
(4387948/550)

        IV size: 8 bytes

        replay detection support: Y


     inbound ah sas:


     inbound pcp sas:


     outbound esp sas:

      spi: 0x868FB46A(2257564778)

        transform: esp-3des esp-sha-hmac ,

        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 2001, flow_id: 2, crypto map:
tor1

        sa timing: remaining key lifetime (k/sec):
(4421374/616)

        IV size: 8 bytes

        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:


3640R2#
```

```
        slot: 0, conn id: 2001, flow_id: 2, crypto map:
tor2

        sa timing: remaining key lifetime (k/sec):
(4387948/550)

        IV size: 8 bytes

        replay detection support: Y


     outbound ah sas:


     outbound pcp sas:


3640R1#
```

GRE Tunnel	
3640R2#ping Protocol [ip]: Target IP address: 10.10.10.1 Repeat count [5]:	3640R1#debug tunnel Tunnel Interface debugging is on 3640R1# *Mar 1 02:40:25.627: Tunnel0: GRE/IP encapsulated

```
Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 10.10.20.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is
2 seconds:

Packet sent with a source address of 10.10.20.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max
= 12/52/104 ms

3640R2#
```

```
11.11.11.11->192.168.10.2 (linktype=7, len=48)

*Mar  1 02:40:25.759: Tunnel0: GRE/IP to decaps
192.168.10.2->11.11.11.11 (len=24 ttl=253)

*Mar  1 02:40:25.971: Tunnel0: GRE decapsulated IP
10.10.20.1->10.10.10.1 (len=100, ttl=254)

*Mar  1 02:40:25.975: Tunnel0: GRE/IP encapsulated
11.11.11.11->192.168.10.2 (linktype=7, len=124)

*Mar  1 02:40:26.067: Tunnel0: GRE decapsulated IP
10.10.20.1->10.10.10.1 (len=100, ttl=254)

*Mar  1 02:40:26.067: Tunnel0: GRE/IP encapsulated
11.11.11.11->192.168.10.2 (linktype=7, len=124)

…
```