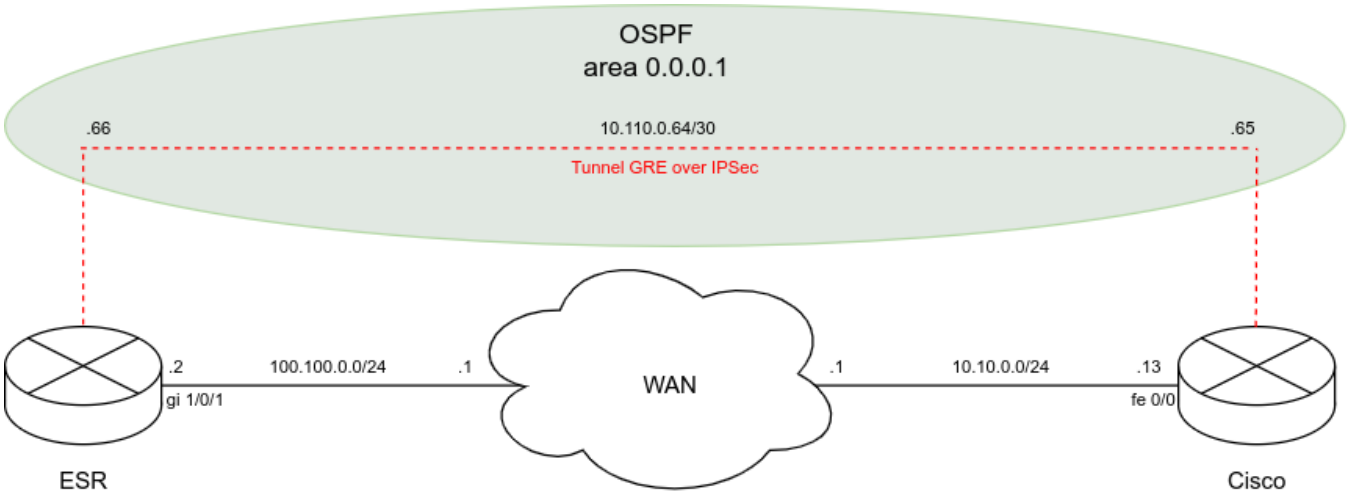
GRE over IPSec ESR Cisco

:



:

GRE over IPSec ESR Cisco. OSPF.

> ⚠ IPSec ESR **ike establish-tunnel route**, IPSec . Loopback IPSec ( ) .

ESR:

1) :

```
esr# show running-config
router ospf log-adjacency-changes
router ospf 1
  router-id 10.110.0.66
  area 0.0.0.1
    enable
  exit
  enable
exit

interface gigabitethernet 1/0/1
  ip firewall disable
  ip address 100.100.0.2/24
exit
interface loopback 1
  ip address 2.2.2.2/32
exit
tunnel gre 1
  mtu 1476
  ip firewall disable
  local address 100.100.0.2
  remote address 10.10.0.13
  ip address 10.110.0.66/30
  ip ospf instance 1
  ip ospf area 0.0.0.1
  ip ospf
  enable
exit

security ike proposal IKEPROP
  encryption algorithm aes128
  dh-group 2
exit

security ike policy IKEPOL
  lifetime seconds 86400
  pre-shared-key ascii-text encrypted 8CB5107EA7005AFF
  proposal IKEPROP
exit

security ike gateway IKEGW
  ike-policy IKEPOL
  local address 100.100.0.2
  local network 100.100.0.2/32 protocol gre
  remote address 10.10.0.13
  remote network 10.10.0.13/32 protocol gre
  mode policy-based
exit

security ipsec proposal IPPROP
  encryption algorithm aes128
exit

security ipsec policy IPPOL
  proposal IPPROP
exit

security ipsec vpn IPSEC
  mode ike
  ike establish-tunnel route
  ike gateway IKEGW
  ike ipsec-policy IPPOL
  enable
exit

ip route 0.0.0.0/0 tunnel gre 1
ip route 10.10.0.0/24 100.100.0.1
```

2) OSPF IPSec :

```
esr# show ip ospf neighbors
Router ID        Pri  State          DTime  Interface          Router IP
---------        ---  -----          -----  -----------------  ---------
10.110.0.65      1    Full/BDR       00:36  gre 1              10.110.0.65
esr# show security ipsec vpn status IPSEC
Currently active IKE SA:
    Name:                       IPSEC
    State:                      Established
    Version:                    v1-only
    Unique ID:                  1
    Local host:                 100.100.0.2
    Remote host:                10.10.0.13
    Role:                       Responder
    Initiator spi:              0xc6518822b67d5635
    Responder spi:              0x8f9084d1b93f1ccc
    Encryption algorithm:       aes128
    Authentication algorithm:   sha1
    Diffie-Hellman group:       2
    Established:                1 minute and 21 seconds ago
    Rekey time:                 1 minute and 21 seconds
    Reauthentication time:      23 hours, 43 minutes and 35 seconds
    Child IPsec SAs:
        Name:                       IPSEC-2
        State:                      Installed
        Protocol:                   esp
        Mode:                       Tunnel
        Encryption algorithm:       aes128
        Authentication algorithm:   sha1
        Rekey time:                 45 minutes and 53 seconds
        Life time:                  58 minutes and 39 seconds
        Established:                1 minute and 21 seconds ago
        Traffic statistics:
            Input bytes:            832
            Output bytes:           736
            Input packets:          8
            Output packets:         8
        ------------------------------------------------------------
```

Cisco:

1) :

```
crypto isakmp policy 2
 encr aes
 authentication pre-share
 group 2
crypto isakmp key password address 100.100.0.2
!
!
crypto ipsec transform-set IPsec esp-aes esp-sha-hmac
!
crypto ipsec profile IPsec_profile
 set transform-set IPsec
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel2
 ip address 10.110.0.65 255.255.255.252
 ip ospf network broadcast
 ip ospf 1 area 0.0.0.1
 tunnel source 10.10.0.13
 tunnel destination 100.100.0.2
 tunnel protection ipsec profile IPsec_profile
!
interface FastEthernet0/0
 ip address 10.10.0.13 255.255.255.0
 speed auto
 full-duplex
!
router ospf 1
router-id 10.110.0.65
log-adjacency-changes
!
ip route 100.100.0.0 255.255.255.0 10.10.0.1
ip route 0.0.0.0 0.0.0.0 Tunnel2
```

2) OSPF IPSec :

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.110.0.66     128   FULL/DR         00:00:33    10.110.0.66     Tunnel2

Router#show crypto ipsec sa

interface: Tunnel2
    Crypto map tag: Tunnel2-head-0, local addr 10.10.0.13

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.0.13/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (100.100.0.2/255.255.255.255/47/0)
   current_peer 100.100.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 31, #pkts encrypt: 31, #pkts digest: 31
    #pkts decaps: 28, #pkts decrypt: 28, #pkts verify: 28
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 7, #recv errors 0

     local crypto endpt.: 10.10.0.13, remote crypto endpt.: 100.100.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xC9AC095C(3383495004)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x5F736BDD(1601399773)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:7, sibling_flags 80000046, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4410255/3460)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC9AC095C(3383495004)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:8, sibling_flags 80000046, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4410255/3460)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```