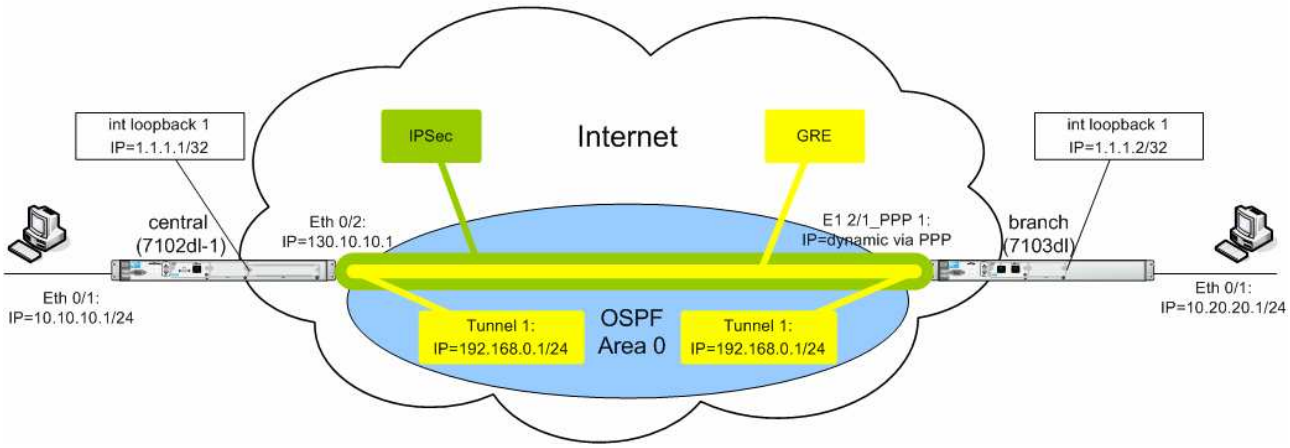
GRE tunnel over IPSec with OSPF



This example illustrates the connection of two sites over the Internet and their interconnection via a site-to-site IPSec VPN. The IP address on the public interface eth0/2 on the central router is fixed. The IP address on the public interface ppp1 on the branch router is dynamically learned.

As the public IP address at the branch side is not known in advance, therefore it is required to make sure that:

- the branch router will always try to initiate the IPSec tunnel
- the central router will accept and process the incoming IPSec (IKE) packets

Inside the IPSec tunnel there is a GRE tunnel used for the following purposes:

- the GRE keepalives or the LLDP frames on the GRE tunnel will always try to open the tunnel
- for OSPF to run between the router we need to have a common IP subnet

Configuration of router central:

```
hostname "central"
!
!
ip subnet-zero
ip classless
ip routing
!
!
```

```
ip crypto
!
crypto ike policy 100
  initiate main
  respond anymode
  local-id fqdn central
  peer any
  attribute 1
    encryption aes-256-cbc
    authentication pre-share
    group 2
!
crypto ike remote-id fqdn branch preshared-key my_shared_secret ike-
policy 100 crypto map VPN 10 no-mode-config no-xauth
crypto ike remote-id any preshared-key my_shared_secret ike-policy 100
crypto map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-aes-256-cbc-esp-sha-hmac esp-aes-256-cbc
esp-sha-hmac
  mode tunnel
!
crypto map VPN 10 ipsec-ike
  description VPN_connection_to_branch
  match address VPN-10-vpn-selectors
  set transform-set esp-aes-256-cbc-esp-sha-hmac
  ike-policy 100
!
!
!
interface loop 1
  ip address  1.1.1.1  255.255.255.255
  no shutdown
!
interface eth 0/1
  ip address  10.10.10.1  255.255.255.0
  no shutdown
!
interface eth 0/2
  ip address  130.10.10.1  255.255.255.0
  ip access-group allow_only_VPN_traffic in
  crypto map VPN
  no shutdown
!
interface tunnel 1
  ip address  192.168.0.1  255.255.255.0
  tunnel mode gre
  tunnel source loop 1
  tunnel destination 1.1.1.2
  keepalive
  mtu 1460
  no shutdown
!
!
!
router ospf
  network 192.168.0.0 0.0.0.255 area 0
  network 10.10.10.0 0.0.0.255 area 0
```

```
!
ip access-list extended allow_only_VPN_traffic
  permit udp any eq isakmp host 130.10.10.1 eq isakmp
  permit esp any  host 130.10.10.1
!
ip access-list extended ISDN_intrest
  permit ip any  10.20.20.0 0.0.0.255
!
ip access-list extended VPN-10-vpn-selectors
  permit ip 10.10.10.0 0.0.0.255  10.20.20.0 0.0.0.255
  permit gre host 1.1.1.1  host 1.1.1.2
!
!
!
ip route 0.0.0.0 0.0.0.0 130.10.10.2
```

Configuration of router branch:

```
hostname "branch"
enable password hp
!
!
ip subnet-zero
ip classless
ip routing
!
!
ip crypto
!
crypto ike policy 100
  initiate main
  respond anymode
  local-id fqdn branch
  peer 130.10.10.1
  attribute 1
    encryption aes-256-cbc
    authentication pre-share
    group 2
!
crypto ike remote-id fqdn central preshared-key my_shared_secret ike-
policy 100 crypto map VPN 10 no-mode-config no-xauth
crypto ike remote-id address 130.10.10.1 preshared-key my_shared_secret
ike-policy 100 crypto map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-aes-256-cbc-esp-sha-hmac esp-aes-256-cbc
esp-sha-hmac
  mode tunnel
!
crypto map VPN 10 ipsec-ike
  description VPN_connection_to_central
  match address VPN-10-vpn-selectors
  set peer 130.10.10.1
  set transform-set esp-aes-256-cbc-esp-sha-hmac
  ike-policy 100
```

```
!
interface loop 1
  ip address  1.1.1.2  255.255.255.255
  no shutdown
!
interface eth 0/1
  ip address  10.20.20.1  255.255.255.0
  no shutdown
!
interface eth 0/2
  no ip address
  shutdown
!
interface e1 3/1
  tdm-group 1 timeslots 1-8 speed 64
  no shutdown
!
interface ppp 1
  ip address negotiated
  ip access-group allow_only_VPN_traffic in
  crypto map VPN
  ppp authentication chap
  username branch password hp
  ppp chap hostname branch
  ppp chap password hp
  no shutdown
  bind 1 e1 3/1 1 ppp 1
!
interface tunnel 1
  ip address  192.168.0.2  255.255.255.0
  tunnel mode gre
  tunnel source loop 1
  tunnel destination 1.1.1.1
  keepalive
  mtu 1460
  bandwidth 1000000
  no shutdown
!
!
router ospf
  network 192.168.0.0 0.0.0.255 area 0
  network 10.20.20.0 0.0.0.255 area 0
!
!
ip access-list extended allow_only_VPN_traffic
  permit esp host 130.10.10.1  any
  permit udp host 130.10.10.1 eq isakmp any eq isakmp
!
ip access-list extended ISDN_intrest
  permit ip any  10.10.10.0 0.0.0.255
!
ip access-list extended VPN-10-vpn-selectors
  permit ip 10.20.20.0 0.0.0.255  10.10.10.0 0.0.0.255
  permit gre host 1.1.1.2  host 1.1.1.1
!
!
ip route 10.10.10.0 255.255.255.0 demand 1
```

show Command outputs:

```
central#sh ip int brie
  Interface            IP Address          Status      Protocol
   demand 1            30.30.30.1          UP          SPOOFING
   eth 0/1             10.10.10.1          UP          UP
   eth 0/2             130.10.10.1         UP          UP
   loop 1              1.1.1.1             UP          UP
   tunnel 1            192.168.0.1         UP          UP

central#sh ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2

Gateway of last resort is 130.10.10.2 to network 0.0.0.0

S    0.0.0.0/0 [1/0] via 130.10.10.2, eth 0/2
C    1.1.1.1/32 is directly connected, loop 1
C    10.10.10.0/24 is directly connected, eth 0/1
O    10.20.20.0/24 [110/2] via 192.168.0.2, tunnel 1
C    30.30.30.0/30 is directly connected, demand 1
C    130.10.10.0/24 is directly connected, eth 0/2
C    192.168.0.0/24 is directly connected, tunnel 1

central#sh lldp neigh
Capability Codes: R - Router, B - Bridge, H - Host, D - DOCSIS Device,
                  W - WLAN Access Point, r - Repeater, T - Telephone

System Name     Port ID        TTL    Cap.     Platform       Local Int
--------------- -------------- ------ -------- -------------- ---------
branch          tunnel 1       106    ----R--- ProCurve Secu  tunnel 1

central#sh crypto ike sa
IKE Security Associations
Total IKE SAs: 1

  Peer IP Address: 199.1.1.2
  Remote ID: branch
  Lifetime: 25932
  Status: SA_MATURE
  IKE Policy: 100
  NAT-traversal: V2
  Detected NAT: No
  Dead Peer Detection: Yes

central#sh crypto ipsec sa
IPSec Security Associations: Total IPSec SAs: 2

  Peer IP Address: 130.10.10.1
  Direction: Inbound
  SPI: 0xF822FB59 (4163042137)
  Encapsulation: ESP
  RX Bytes: 71612
  Selectors: Src:1.1.1.2/255.255.255.255  Port:ANY  Proto:47
```

```
            Dst:1.1.1.1/255.255.255.255  Port:ANY  Proto:47
  Hard Lifetime: 25930
  Soft Lifetime: 0
  Crypto Map: VPN 10

  Peer IP Address: 199.1.1.2
  Direction: Outbound
  SPI: 0xB8500959 (3092253017)
  Encapsulation: ESP
  TX Bytes: 72244
  Selectors: Src:1.1.1.1/255.255.255.255  Port:ANY  Proto:47
             Dst:1.1.1.2/255.255.255.255  Port:ANY  Proto:47
  Hard Lifetime: 25930
  Soft Lifetime: 25900
  Crypto Map: VPN 10
```

central#sh int tunnel 1

```
tunnel 1 is UP
  IP address 192.168.0.1, netmask 255.255.255.0
  MTU 1460 bytes, BW 1000000 Kbit
  Tunnel mode GRE, keepalive enabled (10 seconds, 3 retries)
  Tunnel source 1.1.1.1 (loop 1), destination 1.1.1.2
  Key not set, packet checksumming disabled, sequencing disabled
  0 invalid checksums,  0 invalid seq.
  Previous seq. numbers: 4294967295/0 (rx/tx)
    28643 packets input, 1326228 bytes
    33393 packets output, 2335337 bytes
    0 rx broadcast pkts, 0 tx broadcast pkts
```

---

branch#sh ip int brie

```
  Interface            IP Address          Status      Protocol
   demand 1            30.30.30.2          UP          SPOOFING
   eth 0/1             10.20.20.1          UP          UP
   loop 1              1.1.1.2             UP          UP
   ppp 1               199.1.1.2           UP          UP
   tunnel 1            192.168.0.2         UP          UP
```

branch#sh ip route

```
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S    0.0.0.0/0 [1/0] via 0.0.0.0, ppp 1
C    1.1.1.2/32 is directly connected, loop 1
S    10.10.10.0/24 [1/0] via 0.0.0.0, demand 1
C    10.20.20.0/24 is directly connected, eth 0/1
C    30.30.30.0/30 is directly connected, demand 1
C    192.168.0.0/24 is directly connected, tunnel 1
C    199.1.1.1/32 is directly connected, ppp 1
C    199.1.1.2/32 is directly connected, ppp 1
```

```
branch#sh lldp neigh remote
Capability Codes: R - Router, B - Bridge, H - Host, D - DOCSIS Device,
                  W - WLAN Access Point, r - Repeater, T - Telephone
System Name     Port ID        TTL    Cap.     Platform       Local Int
--------------- -------------- ------ -------- -------------- --------
central         tunnel 1       115    ----R--- ProCurve Secu  tunnel 1

branch#sh crypto ike sa
IKE Security Associations
Total IKE SAs: 1

  Peer IP Address: 130.10.10.1
  Remote ID: central
  Lifetime: 26449
  Status: SA_MATURE
  IKE Policy: 100
  NAT-traversal: V2
  Detected NAT: No
  Dead Peer Detection: Yes

branch#sh crypto ipsec sa
IPSec Security Associations: Total IPSec SAs: 2

  Peer IP Address: 199.1.1.2
  Direction: Inbound
  SPI: 0xB8500959 (3092253017)
  Encapsulation: ESP
  RX Bytes: 60416
  Selectors: Src:1.1.1.1/255.255.255.255  Port:ANY  Proto:47
             Dst:1.1.1.2/255.255.255.255  Port:ANY  Proto:47
  Hard Lifetime: 26430
  Soft Lifetime: 0
  Crypto Map: VPN 10

  Peer IP Address: 130.10.10.1
  Direction: Outbound
  SPI: 0xF822FB59 (4163042137)
  Encapsulation: ESP
  TX Bytes: 59564
  Selectors: Src:1.1.1.2/255.255.255.255  Port:ANY  Proto:47
             Dst:1.1.1.1/255.255.255.255  Port:ANY  Proto:47
  Hard Lifetime: 26430
  Soft Lifetime: 26340
  Crypto Map: VPN 10

branch#sh int tunnel 1
tunnel 1 is UP
  IP address 192.168.0.2, netmask 255.255.255.0
  MTU 1460 bytes, BW 1000000 Kbit
  Tunnel mode GRE, keepalive enabled (10 seconds, 3 retries)
  Tunnel source 1.1.1.2 (loop 1), destination 1.1.1.1
  Key not set, packet checksumming disabled, sequencing disabled
  0 invalid checksums,  0 invalid seq.
  Previous seq. numbers: 4294967295/0 (rx/tx)
    28541 packets input, 1320512 bytes
    33276 packets output, 2323688 bytes
    0 rx broadcast pkts, 0 tx broadcast pkts
```