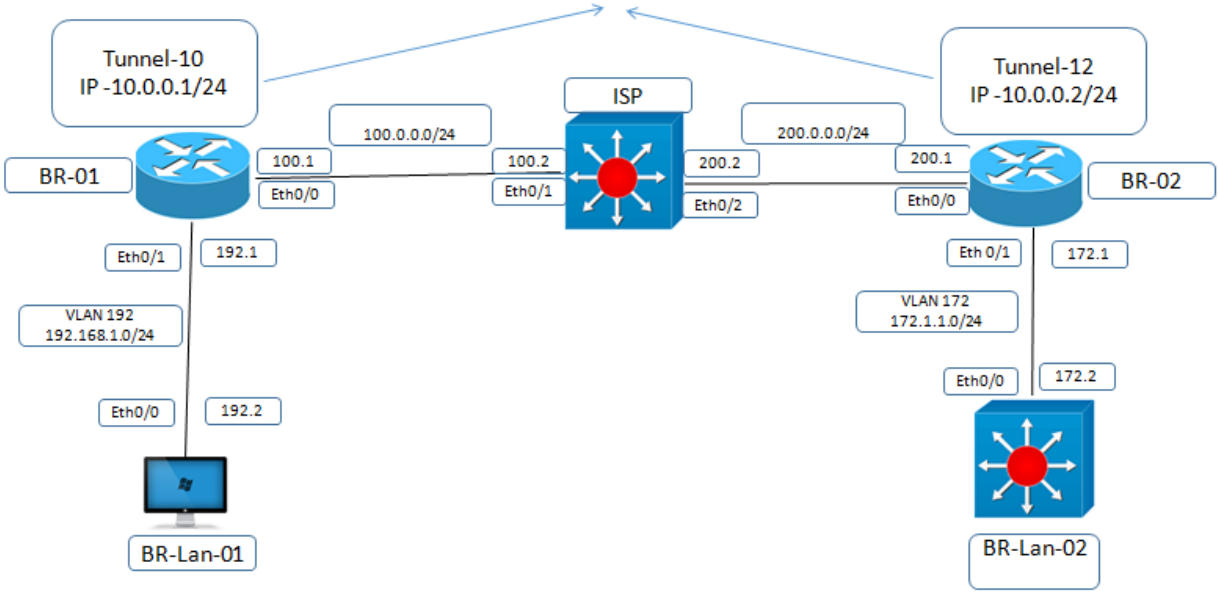
IPSec over GRE Tunnel on IOS

Platform: https://racks.uninets.com
Lab Name: CCNP Security SIMOS

Topology

IPSec over GRE Tunnel on IOS



Task

- Configure R1 AS Branch-01 router with ip address of 100.0.0.1/24 and 192.168.1.1/24 on 0/1 and create tunnel interface 10 with ip address 10.0.0.1/24 and tunnel destination would be 200.0.0.1
- Configure R2 AS Branch-02 router with ip address of 200.0.0.1/24 and 172.1.1.1/24 on 0/1 and create tunnel interface 12 with ip address 10.0.0.2/24 and tunnel destination would be 100.0.0.1
- Create site to site VPN tunnel b/w gre tunnel 10 and gre tunnel 12 using pre shared key unnets@123
- Verify from tunnel 10 to tunnel 12

Explanation

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

This article will show how to setup and configure two Cisco routers to create a permanent secure site-to-site VPN tunnel over the Internet, using the P Security (IPSec) protocol. In this article we assume both Cisco routers have a static public IP address. Readers interested in configuring support for dynamic public IP address endpoint routers can refer to our Configuring Site to Site IPSec VPN with Dynamic IP Endpoint Cisco Routers article.

IPSec VPN tunnels can also be configured using GRE (Generic Routing Encapsulation) Tunnels with IPSec. GRE tunnels greatly simply the configuration and administration of VPN tunnels and are covered in our Configuring Point-to-Point GRE VPN Tunnels article. Lastly, DMVPNs – a new VPN trend that provide major flexibility and almost no administration overhead can also be examined by reading our Understanding Cisco Dynamic Multipoint VPN (DMVPN), Dynamic Multipoint VPN (DMVPN) Deployment Models & Architectures and Configuring Cisco Dynamic Multipoint VPN (DMVPN) - Hub, Spokes , m GRE Protection and Routing - DMVPN Configuration articles.

ISAKMP (Internet Security Association and Key Management Protocol) and IPSec are essential to building and encrypting the VPN tunnel. ISAKMP, also called IKE (Internet Key Exchange), is the negotiation protocol that allows two hosts to agree on how to build an IPSec security association. ISAKMP negotiation consists of two phases: Phase 1 and Phase 2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data. IPSec then comes into play to encrypt the data using encryption algorithms and provides authentication, encryption and anti-replay services.

As GRE does not have its own mechanism to encrypt traffic it depends on IPSec for getting the encryption job done. As opposed to GRE over IPSec, which encrypts anything that is encapsulated by GRE, IPSec over GRE encrypts only the payload and not the routing protocols running over a GRE tunnel.

In IPSec over GRE, the GRE tunnel is established over the internet, neighbor ship is formed and routes are exchanged and all of this is in clear text. We are only concerned with encrypting the interesting traffic flowing between the two peers. When securing the routing updates and routes isn't a requirement and the major concern is to encrypt the information/payload flowing between the peers we use IPSec over GRE.

IPSec over GRE eliminates the additional overhead of encrypting the GRE header.

Configuration

Configuration on ISP (Sw02)

```
interface Ethernet0/2
 no switchport
 ip address 100.0.0.2 255.255.255.0
No shutdown
Exit
interface Ethernet0/3
```

```
 no switchport
 ip address 200.0.0.2 255.255.255.0
No shutdown
end
```

Configuration on Branch-01(R1)

```
interface Ethernet0/0
 ip address 100.0.0.1 255.255.255.0
No shutdown
exit
interface Ethernet0/1
 ip address 192.168.1.1 255.255.255.0
No shutdown
end
```

```
ip route 0.0.0.0 0.0.0.0 100.0.0.2
```

```
interface Tunnel10
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 200.0.0.1
end
```

Configuration on Branch-02(R2)

```
interface Ethernet0/0
 ip address 200.0.0.1 255.255.255.0
No shutdown
exit
interface Ethernet0/1
 ip address 172.1.1.1 255.255.255.0
no shutdown

exit
```

```
ip route 0.0.0.0 0.0.0.0 200.0.0.2
```

```
interface Tunnel12
 ip address 10.0.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 100.0.0.1
end
```

S2S GRE OVER IPSEC VPN tunnel configuration on Branch-01

```
crypto isakmp policy 10
hash sha
authentication pre-share
group 2
lifetime 86400
encryption aes
exit

crypto isakmp key uninets@123 address 200.0.0.1
```

Configuring IPSec Phase 2 (Transform Set)

```
crypto ipsec transform-set MY-SET esp-aes 128 esp-md5-hmac
crypto ipsec security-association lifetime seconds 3600
```

Configuring Tunnel profile

```
crypto ipsec profile MyProfile
set transform-set MY-SET
EXIT
```

Apply IPSec profile on tunnel interface

```
interface Tunnel10
 tunnel protection ipsec profile MyProfile
end
```

S2S GRE OVER IPSEC VPN configuration on Branch-02

```
crypto isakmp policy 10
hash sha
authentication pre-share
group 2
lifetime 86400
encryption aes
exit

crypto isakmp key uninets@123 address 100.0.0.1
```

Configuring IPSec Phase 2 (Transform Set)

```
crypto ipsec transform-set MY-SET esp-aes 128 esp-md5-hmac
crypto ipsec security-association lifetime seconds 3600
```

Configuring Tunnel profile

```
crypto ipsec profile MyProfile
set transform-set MY-SET
EXIT
```

Apply IPSec profile on tunnel interface

```
interface Tunnel12
 tunnel protection ipsec profile MyProfile
end
```

Verification

```
Branch-01#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

```
Branch-01#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
200.0.0.1       100.0.0.1       QM_IDLE           1002 ACTIVE
100.0.0.1       200.0.0.1       QM_IDLE           1001 ACTIVE
```

```
Branch-01#show crypto ipsec sa
interface: Tunnel10
    Crypto map tag: Tunnel10-head-0, local addr 100.0.0.1
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (100.0.0.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (200.0.0.1/255.255.255.255/47/0)
   current_peer 200.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
  local crypto endpt.: 100.0.0.1, remote crypto endpt.: 200.0.0.1
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
 current outbound spi: 0xAD32CD9A(2905787802)
PFS (Y/N): N, DH group: none
    inbound esp sas:
     spi: 0x4EA85CC7(1319656647)
       transform: esp-aes esp-md5-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: SW:3, sibling_flags 80004040, crypto map: Tunnel10-head-0
       sa timing: remaining key lifetime (k/sec): (4326091/3450)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
```