
```
! This is a template for IPSec/GRE on a Cisco router.  In this example, two routers will connect
! to each other using IPSec over the Internet and allow GRE traffic within the encrypted tunnel.
!
!
!
!           - Example design using two routers:
!
!             - ROUTER_A (1.1.1.1) will connect to ROUTER_B (2.2.2.2) using IPSec over the
!             public Internet.
!             - A GRE tunnel will be setup between the two routers using the IPSec tunnel for
!             protection.
!             - ROUTER_A local LAN is 6.6.6.0.24
!             - ROUTER_B local LAN is 7.7.7.0/24
!             - Note: We used very simple IP addressing to make reading the config easier.
!             - Email info@configtoolbox.com if you have any questions.
!
!
!
! hostname ROUTER_A
!
clock timezone ET -5 0
clock summer-time ET recurring
! >>>>>>>>>> Ensure your router clock is correct with the proper time zone.  We suggest using NTP.
!
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
!
crypto isakmp key 12345678912345678912345678 address 2.2.2.2
! >>>>>>>>>> In this example, 2.2.2.2 is the public address of ROUTER_B
! >>>>>>>>>> Use 25 characters or more on your preshared key for best security
!
crypto isakmp keepalive 15
crypto isakmp aggressive-mode disable
!
crypto ipsec transform-set STRONG esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec df-bit clear
! >>>>>>>>>> This will clear the "don't fragment" bit in the IP header
!
crypto map MAP_1 10 ipsec-isakmp
 description IPSec to ROUTER_B
 set peer 2.2.2.2
```

```
 set transform-set STRONG
 set pfs group5
 match address MAP_1_ACL
!
interface Loopback1
 description Loopback for GRE Tunnel1 to ROUTER_B
 ip address 3.3.3.3 255.255.255.255
! >>>>>>>>>> This can be any available /32 private address within your network
!
interface Tunnel1
 description GRE Tunnel to ROUTER_B
 ip address 5.5.5.5 255.255.255.252
! >>>>>>>>>> This can be any available /30 subnet within your network
 ip mtu 1400
 ip tcp adjust-mss 1360
 ip policy route-map DF_BIT_CLEAR
! >>>>>>>>>> This will clear the "don't fragment" bit in the IP header
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination 4.4.4.4
! >>>>>>>>>> This will be the Loopback1 interface on ROUTER_B
!
interface GigabitEthernet0/0/0
 description Interface connecting to your ISP
 ip address 1.1.1.1 255.255.255.252
! >>>>>>>>>> This will be the public address assigned by your ISP
 ip nat outside
 crypto map MAP_1
 ip virtual-reassembly
! >>>>>>>>> Note: We highly recommend you put a strong ACL on the outside interface of your router
to ensure proper security.  Contact us if you need additional help with that.
!
interface GigabitEthernet0/0/1
 description Interface connecting to your inside switch
 ip address 6.6.6.6 255.255.255.0
! >>>>>>>>>> This will be the private address you assigned to this router
 ip nat inside
 ip virtual-reassembly
!
ip nat inside source route-map NAT_OVERLOAD interface Gi0/0/0 overload
!
ip route 0.0.0.0 0.0.0.0 1.1.1.2
! >>>>>>>>>> This will be the peer address assigned by your ISP (your gateway)
ip route 4.4.4.4 255.255.255.255 1.1.1.2
! >>>>>>>>>> This route is for the GRE tunnel to ROUTER_B
ip route 7.7.7.0 255.255.255.0 Tunnel1
! >>>>>>>>>> This is a route so you can get to the private subnet of ROUTER_B
!
ip access-list extended 100
10 permit ip any any
! >>>>>>>>>> This ACL will be used with the route map to disable Path MTU Discovery
!
ip access-list extended NAT_ACL
! >>>>>>>>>> This ACL will be used for the NAT configuration
10 deny   ip host 3.3.3.3 host 4.4.4.4
! >>>>>>>>>> This ensures your GRE setup doesn't get NAT'ed
```

```
 10 permit ip 10.0.0.0 0.255.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
 20 permit ip 172.16.0.0 0.15.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
 30 permit ip 192.168.0.0 0.0.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
 40 deny   ip any any
! >>>>>>>>>> This will NAT all remaining traffic to the Internet
!
ip access-list extended MAP_1_ACL
! >>>>>>>>>> This allows the GRE Loopback interfaces to see each other within IPSec tunnel
 10 permit gre host 3.3.3.3 host 4.4.4.4
!
route-map DF_BIT_CLEAR permit 10
 match ip address 100
 set ip df 0
!
route-map NAT_OVERLOAD permit 10
 match ip address NAT_ACL
!
end
! End of IPSec/GRE config for ROUTER_A
!
!
!
!
!
!
hostname ROUTER_B
!
clock timezone ET -5 0
! >>>>>>>>>> Ensure your router clock is correct with the proper time zone.  We suggest using NTP.
clock summer-time ET recurring
!
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 5
!
crypto isakmp key 123456789123456789123456 address 1.1.1.1
! >>>>>>>>>> Use the same key here that entered on ROUTER_A
crypto isakmp keepalive 15
! >>>>>>>>>> In this example, 1.1.1.1 is the public address of ROUTER_A
crypto isakmp aggressive-mode disable
!
crypto ipsec transform-set STRONG esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec df-bit clear
!
crypto map MAP_1 10 ipsec-isakmp
 description IPSec to ROUTER_A
 set peer 1.1.1.1
! >>>>>>>>>> This will be the public IP address of ROUTER_B
 set transform-set STRONG
 set pfs group5
```

```
 match address MAP_1_ACL
!
interface Loopback1
 description Loopback for GRE Tunnel1 to ROUTER_A
 ip address 4.4.4.4 255.255.255.255
! >>>>>>>>>> This can be any available /32 private address within your network
!
interface Tunnel1
 description GRE Tunnel to ROUTER_A
 ip address 5.5.5.6 255.255.255.252
! >>>>>>>>>> This will be on the same subnet assigned to Tunnel1 on Router_A (5.5.5.5)
 ip mtu 1400
 ip tcp adjust-mss 1360
 ip policy route-map DF_BIT_CLEAR
! >>>>>>>>>> This will clear the "don't fragment" bit in the IP header
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination 3.3.3.3
! >>>>>>>>> This will be the Loopback1 interface on ROUTER_A
!
interface GigabitEthernet0/0/0
 description Interface connecting to your ISP
 ip address 2.2.2.2 255.255.255.252
! >>>>>>>>>> This will be the public address assigned by your ISP
 ip nat outside
 crypto map MAP_1
 ip virtual-reassembly
! >>>>>>>>> Note: We highly recommend you put a strong ACL on the outside interface of your router
to ensure proper security.  Contact us if you need additional help with that.
!
interface GigabitEthernet0/0/1
 description Interface connecting to your inside switch
 ip address 7.7.7.7 255.255.255.0
! >>>>>>>>>> This will be the private address you assigned to this router
 ip nat inside
 ip virtual-reassembly
!
ip nat inside source route-map NAT_OVERLOAD interface Gi0/0/0 overload
!
ip route 0.0.0.0 0.0.0.0 2.2.2.2
! >>>>>>>>>> This will be the peer address assigned by your ISP (your gateway)
ip route 3.3.3.3 255.255.255.255 2.2.2.2
! >>>>>>>>>> This route is for the GRE tunnel to ROUTER_A
ip route 6.6.6.0 255.255.255.0 Tunnel1
! >>>>>>>>>> This is a route so you can get to the private subnet of ROUTER_A
!
ip access-list extended 100
! >>>>>>>>>> This ACL will be used with the route map to disable Path MTU Discovery
 10 permit ip any any
!
ip access-list extended NAT_ACL
! >>>>>>>>>> This ACL will be used for the NAT configuration
 10 deny   ip host 3.3.3.3 host 4.4.4.4
! >>>>>>>>>> This ensures your GRE setup doesn't get NAT'ed
 10 permit ip 10.0.0.0 0.255.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
```

```
 20 permit ip 172.16.0.0 0.15.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
 30 permit ip 192.168.0.0 0.0.255.255 any
! >>>>>>>>>> This will allow private subnets to pass over GRE without NAT'ing
 40 deny   ip any any
! >>>>>>>>>> This will NAT all remaining traffic to the Internet
!
ip access-list extended MAP_1_ACL
! >>>>>>>>>> This allows the GRE Loopback interfaces to see each other within IPSec tunnel
 10 permit gre host 3.3.3.3 host 4.4.4.4
!
route-map DF_BIT_CLEAR permit 10
 match ip address 100
 set ip df 0
!
route-map NAT_OVERLOAD permit 10
 match ip address NAT_ACL
!
end
! End of IPSec/GRE config for ROUTER_B
!
!
! Here are some show commands to verify function:
show crypto isa sa
show crypto ipsec sa
show interface Tunnel1
```