Massimiliano Sbaraglia Network Engineer

Configurazione di un Tunnel GRE over IPSEC

1.

```
interface Tunnel0
ip address < ip address > < subnet mask >
tunnel source
tunnel destination
```

2.

```
crypto isakmp policy 1
authentication pre-share
crypto isakmp key < password > address < remote outside interface IP address >
```

3.

```
crypto ipsec transform-set strong esp-3des esp-md5-hmac
```

4.

```
access-list < number_acl > permit gre host < local outside interface ip > host < remote
outside interface IP >
```

5.

```
crypto map vpn < number > ipsec-isakmp
set peer
set transform-set strong
match address < number_acl >
```

Bind crypto map to the physical (outside) interface if you are running Cisco IOS Software Release 12.2.15 or later. If not, then the crypto map must be applied to the tunnel interface as well as the physical interace, as shown:

```
interface < interface_if >
ip address
half-duplex
crypto map vpn < number >
```

Configure Network Address Traslation (NAT) bypass if needed, as shown:

```
access-list < number_acl > deny ip < local private network > < subnet mask > < remote
private network > < subnet mask >
access-list < number_acl > permit ip < local private network > < subnet mask > any
!
route-map nonat permit < number >
match ip address < number_acl >
exit
!
ip nat inside source route-map nonat interface < outside interface name > overload
!
!
```

Configure the remote router the same way. Once configured try passing traffic. If it does not, then add IP routes for the remote networks pointing to the tunnel interface IP address.