How to configure a Cisco IOS Remote Access IPSEC VPN - Alfred Tong

How to configure Cisco IOS Remote Access IPSEC VPN

June 17, 2011

Here’s how to setup a Remote Access IPsec VPN on the Cisco Router IOS platform

Step1. Define the authentication and authorization methods used.

In this case, we’re defining a new group called VPN which will use the local database for authenticating and authorizing the user.

```
aaa authorization login VPN local
aaa authorization network VPN local
```

Step2. Define the isakmp phase 1 policy to use.

We will be using pre-shared key for the phase 1 authentication.

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

Step 3. Define the VPN client group profile.

We are going to name the group VPNGROUP. This is the group name that will be entered in the VPN client. Enter the preshared secret here, and a POOL name, which defines what IPs that will be handed out to the VPN clients. Then assign the name of the ACL that will be used to define the encrypted traffic that will be allowed through the VPN.

```
crypto isakmp client configuration group VPNGROUP
 key secret
 dns 8.8.8.8
 pool VPNRAPOOL
 acl VPN_SPLIT
```

Step 4. Create a the address Pool and the access-list used for traffic encryption

Setup the IP ranged to be assigned to the address pool. In this case the starting IP is 10.100.3.1 and the last IP that can be assigned is 10.100.3.254

```
ip local pool VPNRAPOOL 10.100.3.1 10.100.3.254
```

Define the IP subnet that can be reached behind the VPN. Take special note on the direction of the traffic. You need to specify the traffic behind the router as the source address and the ip used in the VPN Pool as the destination.

```
ip access-list extended VPN_SPLIT
  permit ip 10.100.0.0 0.0.255.255 10.100.3.0 0.0.0.255
```

Step 5. Define the phase 2 encryption parameters ad assign it to the crypto dynamic-map<

Make sure to put in the reverse-route entry so that a static route is inserted into the router.

```
crypto ipsec transform-set T1 esp-3des esp-sha-hmac

crypto dynamic-map DYNMAP 10
 set transform-set T1
 reverse-route
```

Step 6. Create a crypto map.

```
crypto map VPN client authentication list VPN
crypto map VPN isakmp authorization list VPN
crypto map VPN client configuration address respond
crypto map VPN 10 ipsec-isakmp dynamic DYNMAP
```

Step 7. Lastly, assign the crypto map to the internet interface

```
interface FastEthernet0/0
 description Internet
 ip address dhcp
 speed auto
 crypto map VPN
```

- 2

  Shares

- 0
- 1
- 1
- 0
- 0