CCBOOTCAMP
A Division of Network Learning Inc.

GET Protected DMVPN

January 18, 2010
By Steve Means

GET VPN is a new technology released by Cisco that greatly simplifies key management and encryption policy for VPN. It does this by having group members (routers that want to participate in the VPN) register to a key server. This registration is done using a version of IKE/ISAKMP called GDOI. Once the group members register, the key server pushes down IPsec parameters to the group member, including the encryption protocols, crypto ACLs, etc…. the group members are then free to communicate with each other without needing to negotiate IKE phase 1 and 2, all of that is already done during the registration process.

So, what does this have to do with DMVPN? Well, one of the issues with DMVPN is that it is IPsec tunnel based. When dynamic spoke to spoke traffic is necessary, the spokes always have to go through standard IPsec negotiation and this introduces a delay. You may have noticed this when pinging spoke to spoke in a DMVPN network. You'll often see a few of the pings go through (these took the path through the hub), then a dropped packet and finally a few more pings. The drop occurred while the tunnel was being built between the spokes.

GET can eliminate this delay since the IPsec parameters are already set up. The spoke will simply need to send an NHRP query to the hub for the destination address and then send the packets encapsulated within GRE as normal. Now that you understand the theory, here is how you set it up.

We won't be going in to setting up key servers, group members, etc… for GET. Cisco already has excellent documentation for that in their online documentation. As far as the GET portion of our configuration is concerned, we simply need to decide what traffic is going to be encrypted. DMVPN is based on encapsulating with GRE, so we only need to worry about GRE between the group members. This is done with an ACL on the key server like so:

```
access-list 101 permit gre any any
!
crypto gdoi group dmvpn
server local
sa ipsec 1
match address ipv4 101
```

In a standard DMVPN implementation the GRE tunnels are encrypted using tunnel protection with an IPsec profile. Since GET has already taken care of the encryption we can simply remove (or not include) the tunnel protection command. Here is a sample tunnel configuration for the hub.

```
interface Tunnel0
 bandwidth 1000
 ip address 192.168.1.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 no ip split-horizon eigrp 1
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 1
```

Configured this way, you will have eliminated the IPsec negotiation delay and built a better DMVPN!