

Re: Cisco ASA IPSEC Tunnelling

Source: <http://newsgroups.derkeiler.com/Archive/Comp/comp.dcom.sys.cisco/2007-12/msg00307.html>

- *From:* "Scott Perry" <scottperry@aciscocompany.com>
 - *Date:* Mon, 17 Dec 2007 10:58:44 -0500
-

I suggest creating a GRE tunnel between the MPLS connecting routers. You need to already be using a dynamic routing protocol in your environment (RIP, EIGRP, OSPF, etc.). If you are not, please do not read further and get used to binding static routes to interfaces.

If a router, for example "Router-Houston" in Houston with a 10.10.20.X/24 network, normally sends 10.10.10.X/24 traffic towards the California router, "Router-California", then make a GRE tunnel from Router-Houston to Router-California.

- (1) Create a loopback interface on both Router-Houston and Router-California. Do not advertise this loopback interface through your dynamic routing protocol.
- (2) Configure the GRE tunnel to go from a loopback IP address on one router to a loopback IP address on the other router.
- (3) Configure non-redistributed static routes on these GRE terminating routers and also on any routers between them and their site ASA to send traffic destined to the other router's loopback interface towards the ASA.
- (4) On the ASA, configure an IPsec LAN-to-LAN tunnel with the tunnel traffic access-list permitting IP protocol GRE for traffic from host Router-Houston's loopback IP address to Router-California's loopback IP address. If you get stuck, just permit all IP from Router-Houston's loopback IP address to Router-California's loopback IP address. It is more specific to allow protocol GRE and also ICMP for testing.
- (5) This step will take a while. Test connectivity using an extended PING and TRACEROUTE command on both routers which is sourced from the loopback IP address of one router to the loopback IP address of the other. If your configuration was correct, the GRE tunnels will connect over the IPsec tunnel that will connect. Your TRACEROUTE will show the traffic not going directly over the MPLS cloud but instead over the path across the IPsec tunnel. The hops inside of the IPsec tunnel will not show.
- (6) When the PING works, you will have a connection between routers which is a GRE tunnel. A GRE tunnel acts like a point-to-point interface like a DS-1/T-1 or similar connection. As the GRE tunnel traffic crosses the

Re: Cisco ASA IPSEC Tunnelling

Intenet, the ASA will encrypt the traffic using IPsec. Sure, this will reduce overall MTU, but this makes it like one router is directly connected to the other. This is VPN.

(7) Configure the GRE tunnel interface with your dynamic routing protocol with a lesser preference. The interface should remain up all of the time.

(8) Test. Drop the MPLS connection and watch traffic go over the VPN to the other site.

I have used this and it works. There are some headaches along the way, but it is inexpensive and effective.

--

=====
Scott Perry

=====
Indianapolis, Indiana

"Jimsu" <jimsu1973@xxxxxxxx> wrote in message
news:2bc41c97-3257-44c6-a4a7-3eef9b0fd601@xx

Hello,

I am trying to engineer a solution that will meet our needs. I've come into a network, and am having to figure it all out as I go. We currently have a site in Houston. This site serves the public as well as our branch offices.

Currently, we connect to remote offices using an IPSEC tunnel initiated and landing on Cisco ASA5510's. Each of the branch offices have their own independent internet connections whether it be a T3 with ATT or 384k dsl with mom/pop telco.

Well the company has decided to go with an MPLS network for all locations. They will drop all of their independent uplinks, and do everything over the MPLS, with a split off of it for their internet access. The hub location (houston) will connect to both MPLS connection AND the normal internet connection. Each location, including houston, received a routeable address which is natted to an internal address at each location.

For redundancy, we want to make it so that if the MPLS link in houston fails, we can still create tunnels into/outof the branch offices utilizing the internet connection.

The way that I had envisioned this is to setup the tunnels on the ASA to land on the new ip address. This address is both internet routeable, and if it's a destination sent out to the MPLS router, it will ride the MPLS network to the other end. And then I could setup

Re: Cisco ASA IPSEC Tunnelling

trackrouting on my router which looked to get to that address over the MPLS link, and if that failed, it would change the route to send the traffic over the internet link instead.

Unfortunately, this does not seem to be working. The other options I have are dropping doing ipsec over MPLS (which I'm not too terribly thrilled about, but that's a whole other debate) moving the MPLS router behind our firewall with another router in front of it, doing the same tracked route idea, and having the devices use this router as a default gateway.

Is there a better way of doing what I'd like to do? The ASA doesn't seem to deal well with multiple routes, and I'm curious about possibly creating a tunnel on the inside interface to encrypt over the MPLS, but if you have two tunnels routing for the same addresses I'm sure it wouldn't like that.. unless there's some way to determin if a tunnel should be up or down based on another tunnel.. or something being up (eg pingable ip).

any information would be appreciated.