

A Cisco ASA Site to Site VPN in 4 pages or Less!

By S. Bondy

Revised 8/9/2009

Setting up a site-to-site VPN between two ASA devices can be a challenge. Even more so because the web interface usually produces configurations that – to be blunt – just don't work. (I've actually had Cisco support tell me NOT to use the web interface for VPN setups because the configs it builds are usually wrong.)

So, because the task can be daunting, I've decide to write this howto for those of you that may have to do it.

Let's begin.

A VPN needs three components to work – authentication, encryption, and tunneling.

Who are you?

Because the first thing we have to do is authenticate, let's begin there. To authenticate, we'll set up ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP can use one of three methods for mutual authentication. These are RADIUS, certificates and a pre-shared key. In my opinion, certificates are hardest to set up, and pre-shared keys are easiest. Let's be lazy and use the easiest option. Here is what we will set up:

```
crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash md5
group 2
lifetime 86400
```

Let's dissect this. The first line sets the identity to be the IP address of the outside interface – think of this as the “username”.

The second line enables the ISAKMP protocol on the outside interface. On a Cisco firewall device, nothing is enabled by default, so you have to turn everything on.

The third line begins setting policy options for policy number 10. We can have multiple policies, identified by different policy numbers. For this policy, we are using a “pre-shared” key. Think of this as the “password”. The other options we have on the policy are that the password will be encrypted with 3des, that we will use a md5 hash, a Diffie-

Helman group of 2, and that the “lifetime” of the connection will be 86400 seconds – or 24 hours. After 24 hours, the systems will “re-authenticate”.

This is a simplified explanation. But our goal is to get something WORKING! If you want to know more, check the Cisco documentation. You can change the encryption to AES if you like, and the hash to SHA1, which are considered more secure. In fact, you can also shorten the lifetime. But the important thing to remember is that your ISAKMP settings have to be THE SAME on both ends of the tunnel.

I've got a secret

Now that we have an authentication method, let's set up how the data will be encrypted. Here is a sample:

```
crypto ipsec transform-set MY-CRYPTO-SET esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 3600
```

This sets an encryption transformation – a set of rules used to encrypt data. In this case, we are setting the encryption to 3DES, and the hashing to MD5-HMAC.

WARNING: look out for transform sets that use AH instead of ESP. AH is NOT COMPATIBLE with network address translation. If you are using NAT, DON'T USE AH!

Now - the next step, telling the ASA what we want to encrypt. To do that, we'll use an access list:

```
access-list IPSEC-LIST extended permit ip 10.1.10.0 255.255.255.0 192.168.1.0
255.255.255.0
```

Our local private network is 10.1.10.0/24. The remote office is using the private network 192.168.1.0/24. All traffic with this source and destination should be encrypted.

Now that we know HOW to encrypt, and WHAT to encrypt, we need to combine those two things:

```
crypto map CRYPTO-MAP 20 match address IPSEC-LIST
crypto map CRYPTO-MAP 20 set peer 1.2.3.4
crypto map CRYPTO-MAP 20 set transform-set MY-CRYPTO-SET
crypto map CRYPTO-MAP interface outside
```

Basically this says, encrypt the traffic that matches the access list, the destination for the encryption is 1.2.3.4, use the transform set already defined above, and do all of this on the outside interface.

Which way to the office?

One more thing to do. We need to define the tunnel.. What we've done so far is set source and destination networks to be encrypted, but we have to "directly" connect those networks – especially if they are private networks (BOGON addresses) as we used in these examples. To define the tunnel, we need to set the type of tunnel, and other attributes:

```
tunnel-group 1.2.3.4 type ipsec-l2l  
tunnel-group 1.2.3.4 ipsec-attributes  
pre-shared-key mysharedkey
```

This says that the tunnel is a LAN to LAN (l2l) and that the authentication key is the static string "mysharedkey".

As with the transform set, the tunnel characteristics must be the same on both ends, but obviously the target IP addresses will change in your implementation.

With these items in place the tunnel will come up once some traffic passes that matches the access-list and you can verify this by using the commands:

```
show crypto isakmp sa  
And  
show crypto ipsec sa
```

These will show the security associations. Note that a "ping" or other ICMP based command may not work correctly, since the access-list is passing IP, not ICMP.

There are two reasons this setup may not work. The first is if NAT is being used. This is because NAT is processed BEFORE the tunnel. So we need to prevent this. We will use the same access list we used to specify "interesting traffic" – that is, traffic to be tunneled – to exclude that traffic from NAT.

```
nat (inside) 0 access-list IPSEC-LIST
```

We've just told the ASA not to NAT ("0") anything in the IPSEC-LIST.

The second reason we may have a problem is that, like any good firewall, an ASA doesn't let anything in by default. We either have to allow VPN traffic in an inbound access list, or set a global option to allow it. Since the goal of this HOWTO is an easy setup, let's do the second option:

```
sysopt connection permit-vpn
```

We've just told the ASA to allow any VPN connections to occur. Note that they still need to be authenticated, and to match our transform set. In some versions of Cisco software this is on by default, so you may not need it.

Final words

Presto! A point to point encrypted VPN, in 4 pages!

And now some disclaimers.

A hard core security person would fault my setup on several points. First, using an IP address as the identity in the ISAKMP setup could be penetrated by IP spoofing. Also, pre-shared keys are a risk since they are a fairly simple authentication mechanism. Certificates are a vastly superior authentication method. And AES is better encryption than 3DES. But the goal here is simplicity, and being able to get a secured tunnel working quickly, and easily.

Remember in all cases that network security must balance the risks, threats, and rewards that various security methods bring with them. If this simple method is not appropriate for your environment, don't use it!