SITE-TO-SITE VPNS PART II: CISCO IOS

Now that the theory has been explained, on to the first S2S VPN configuration. This example will use 3DES and MD5, DH Group 2, and some default lifetimes.

In Cisco terminology, 'isakmp' is used for Phase 1, and 'ipsec' for Phase 2 (many systems refer to it this way). VPN uses encryption, so most commands are done using the 'crypto' engine. The config for the first Phase is logical:

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#lifetime 86400
Router(config-isakmp)#exit
```

The policy number does not have to match with the rest of the upcoming configuration. In fact, the IOS tries to use all Phase 1 proposals configured for all VPN peers until a matching one is found, e.g. if policy 1 matches, then it will be used, if it doesn't, policy 2 will be tried, and so on.

This is not a complete Phase 1 configuration: though pre-shared key authentication is specified, no key is entered. A key needs to be entered on a per-peer basis using the following command:

Router(config)#crypto isakmp key 0 *key* address *peer-ip-address*

For Phase 2, some more parameters are required. First the 'transform set', which is how the packets will actually be encrypted.

```
Router(config)#crypto ipsec transform-set VPN-1 esp-3des esp-md5-hmac
Router(cfg-crypto-trans)#exit
```

This needs some more explaining:

- The name is free to choose. Try to keep it consistent, I usually start the name with ‘VPN-’ here.
- The ‘esp’ in ‘esp-3des’ means the use of the Encapsulating Security Payload (ESP) header. The other option, Authentication Header (AH) is rarely, if ever, used.
- HMAC, or Hash-based message authentication code, specifies the mathematics for the encryption, and it’s the only available option.
- You can set transport or tunnel mode in the configuration. It defaults to tunnel mode and unless transport mode is needed for a specific reason, it’s the best way.

  Next the encryption domain. Not surprisingly, IOS uses an extended access-list for this.

  Router(config)#ip access-list extended AL4-VPN-1

  Router(config-ext-nacl)#*number* permit ip *source-network wildcardmask destination-network wildcardmask*

  Router(config-ext-nacl)#exit

  I like to use naming conventions and best practices. My encryption domain access-lists are usually named ‘AL4-VPN-…’ and use sequence numbers for clarity. Also, it’s perfectly possible to use single hosts in an accesslist (wildcard 0.0.0.0 or ‘host’ keyword), and you can use multiple lines to send multiple subnets through the tunnel. Of course, the remote peer should have the same encryption domain, but his source subnets should be your destination subnets, and vice versa.

  The above two parts of the Phase 2 now need to be connected together, and the remaining parameters (lifetime, peer IP, optionally PFS with a DH group) need to be added. Then, an interface has to be selected that will form the VPN. This is the final step, and it’s all done inside a crypto map:

  Router(config)#crypto map VPNMAP 1 ipsec-isakmp

  % NOTE: This new crypto map will remain disabled until a peer

  and a valid access list have been configured.

  Router(config-crypto-map)# set security-association lifetime seconds 3600

Router(config-crypto-map)# set transform-set VPN-1

Router(config-crypto-map)# set pfs group2

Router(config-crypto-map)# set peer *peer-ip-address*

Router(config-crypto-map)# match address AL4-VPN-1

Router(config-crypto-map)# exit

Router(config)#interface *interface*

Router(config-if)#crypto map VPNMAP

Router(config-if)#exit

The ’1′ used above is the sequence number. You can only assign one crypto map name per interface. To have multiple VPNs through the same interface, create crypto maps with the same name, but different sequence numbers.

Also, depending on the platform, sometimes a (static) route out of the VPN enabled interface for the remote subnet is needed, although usually a default route will do. Either add the static routes manually, or issue ‘reverse-route static’ under the crypto map configuration, after which the routes will automatically be created.

The VPN is now configured but will not come up until it is triggered by ‘interesting traffic’, traffic matching the access list that needs to be encrypted. Troubleshooting is done using ‘show crypto isakmp sa’ for Phase 1 and ‘show crypto ipsec sa’ for Phase 2. These commands and their subcommands give an indication if the VPN is up.

That concludes the Cisco IOS VPN configuration. Other platforms will be described in upcoming parts!

Source : http://reggle.wordpress.com/2012/10/29/site-to-site-vpns-part-ii-cisco-ios/