Configuring a Site-to-Site VPN between Two Cisco Routers

A site-to-site virtual private network (VPN) allows you to maintain a secure "always-on" connection between two physically separate sites using an existing non-secure network such as the public Internet. Traffic between the two sites is transmitted over an encrypted tunnel to prevent snooping or other types of data attacks.

There are several protocols used in creating the VPN including protocols used for a key exchange between the peers, those used to encrypt the tunnel, and hashing technologies which produce message digests.

VPN Protocols

IPSec: Internet Protocol Security (IPSec) is a suite of protocols that are used to secure IP communications. IPSec involves both key exchanges and tunnel encryption. You can think of IPSec as a framework for implementing security. When creating an IPSec VPN, you can choose from a variety of security technologies to implement the tunnel.

- ISAKMP (IKE): Internet Security Association and Key Management Protocol (ISAKMP) provides a means for authenticating the peers in a secure communication. It typically uses Internet Key Exchange (IKE), but other technologies can also be used. Public keys or a pre-shared key are used to authenticate the parties to the communication.
- MD5: Message-Digest algorithm 5 (MD5) is an often used, but partially insecure cryptographic hash function with a 128-bit hash value. A cryptographic hash function is a way of taking an arbitrary block of data and returning a fixed-size bit string, the hash value based on the original block of data. The hashing process is designed so that a change to the data will also change the hash value. The hash value is also called the message digest.
- SHA: Secure Hash Algorithm (SHA) is a set of cryptographic hash functions designed by the National Security Agency (NSA). The three SHA algorithms are structured differently and are distinguished as SHA-0,SHA-1, and SHA-2. SHA-1 is a commonly used hashing algorithm with a standard key length of 160 bits.
- ESP: Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite that provides origin authenticity, integrity, and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure. Unlike the other IPsec protocol, Authentication Header (AH), ESP does not protect the IP packet header. This difference makes ESP preferred for use in a Network Address Translation configuration. ESP operates directly on top of IP, using IP protocol number 50.
- DES: The Data Encryption Standard (DES) provides 56-bit encryption. It is no longer considered a secure protocol because its short key-length makes it vulnerable to brute-force attacks.
- 3DES: Three DES was designed to overcome the limitations and weaknesses of DES by using three different 56-bit keys in a encrypting, decrypting, and re-encrypting operation. 3DES keys are 168 bits in length. When using 3DES, the data is first encrypted with one

56-bit key, then decrypted with a different 56-bit key, the output of which is then re-encrypted with a third 56-bit key.

- AES: The Advanced Encryption Standard (AES) was designed as a replacement for DES and 3DES. It is available in varying key lengths and is generally considered to be about six times faster than 3DES.
- HMAC: The Hashing Message Authentication Code (HMAC) is a type of message authentication code (MAC). HMAC is calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.

Configuring a Site-to-Site VPN

The process of configuring a site-to-site VPN involves several steps:

1. Phase One configuration involves configuring the key exchange. This process uses ISAKMP to identify the hashing algorithm and authentication method. It is also one of two places where you must identify the peer at the opposite end of the tunnel. In this example, we chose SHA as the hashing algorithm due to its more robust nature, including its 160-bit key. The key "vpnuser" must be identical on both ends of the tunnel. The address "192.168.16.25" is the outside interface of the router at the opposite end of the tunnel.

```
Athens#
Athens#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Athens(config)#crypto isakmp policy 10
Athens(config-isakmp)#hash sha
Athens(config-isakmp)#authentication pre-share
Athens(config-isakmp)#crypto isakmp key vpnuser address 192.168.16.25
Athens(config)#
```

2. Phase Two configuration involves configuring the encrypted tunnel. In Phase Two configuration, you create and name a transform set which identifies the encrypting protocols used to create the secure tunnel. You must also create a crypto map in which you identify the peer at the opposite end of the tunnel, specify the transform-set to be used, and specify which access control list will identify permitted traffic flows. In this example, we chose AES due to its heightened security and enhanced performance. The statement "set peer 192.168.16.25" identifies the outside interface of the router at the opposite end of the tunnel. The statement "set transform-set vpnset" tells the router to use the parameters specified in the transform-set vpnset in this tunnel. The "match address 100" statement is used to associate the tunnel with access-list 100 which will be defined later.

```
Athens(config)#
Athens(config)#crypto ipsec transform-set vpnset esp-aes esp-sha-hmac
Athens(cfg-crypto-trans)#exit
Athens(config)#crypto map vpnset 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Athens(config-crypto-map)#set peer 192.168.16.25
Athens(config-crypto-map)#set transform-set vpnset
Athens(config-crypto-map)#match address 100
Athens(config-crypto-map)#
```

3. The crypto map must be applied to your outside interface (in this example, interface FastEthernet 4).

```
Athens(config)#
Athens(config)#int f4
Athens(config-if)#crypto map vpnset
Athens(config-if)#
```

4. You must create an access control list to explicitly allow certain traffic across the tunnel.

```
Athens(config)#
Athens(config)#access-list 100 permit ip 10.10.10.0 0.0.0.255 172.16.2.0 0.0.0.255
Athens(config)#
```

5. You must also create a default gateway (also known as the "gateway of last resort").

```
Athens(config)#
Athens(config)#ip route 0.0.0.0 0.0.0.0 192.168.16.1
Athens(config)#
```

Verifying VPN Connections

The following two commands can be used to verify VPN connections:

- Router#**show crypto ipsec sa** displays the settings used by the current Security Associations (SAs)
- Router#**show crypto isakmp sa** displays current IKE Security Associations.

Troubleshooting VPN Connections

After confirming physical connectivity, audit both ends of the VPN connection to ensure they mirror each other.
Use debugging to analyze VPN connection difficulties:

- Router#**debug crypto isakmp** allows you to observe Phase 1 ISAKMP negotiations.
- Router#**debug crypto ipsec** allows you to observe Phase 2 IPSec negotiations.