Global Information Assurance Certification Paper

Building Virtual Private Networks with Cisco Devices

David Templeton
GSEC
Dec 20, 2001
Login:datc001

Introduction

The Internet contains a vast wealth of information, services and resources for any group that would chose to use it. It may have started as a modest collection of four computers connected together by members of the Advance Research Projects Agency (ARPA) but today there are million of computers connected together sharing information. This huge infrastructure can be tapped into for the mire cost of connecting to a local service provider.

Now what if you could securely send information to your branch offices or road warriors through the Internet, then you could capitalize on the size and reach of the Internet and make the Internet your Infrastructure for connecting your private sites. Instead of building you own private worldwide network, you could use the worldwide network of the Internet. You would then be using the Internet as a Virtual Private Network (VPN). This solution can realize large savings on monthly line costs not to mention the training and salaries of all those network engineers required to maintain that private infrastructure.

A VPN is a network service over a public infrastructure (i.e. the Internet) with the privacy and security policies of a private network. There are three main categories of VPNs:

- Remote Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

- Intranet VPNs Link corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Internet VPNs differ from extranet VPNs in that they allow access only to the enterprise customer's employees.

- Extranet VPNs link customers, suppliers, partners, or communities of interest to a corporate Intranet over a shared infrastructure using dedicated connections. Extranet VPNs differ from Internet VPNs in that they allow access to users outside the enterprise.[6]

This paper is an introduction to Cisco components and devices used to build a secure Virtual Private Network. I will Provide a brief summary and explanation of the framework and protocols supporting IPSec as well as give an example of how to terminate an IPSec tunnel using some of these appliances.

Cisco's VPN Components

The following are the main components that make up Cisco's VPN devices.

- Cisco VPN Routers-Use Cisco IOS software IPSec support to enable a secure VPN.
- Cisco Secure PIX Firewall-Act's as a VPN gateway when the security group controls the VPN.
- Cisco VPN Concentrator series-Offers remote access and site-to-site VPN capability.
- Cisco Secure VPN Client-Enables secure remote access to Cisco router and PIX Firewalls and runs on the Windows operating system.
- Cisco UNITY Client-Enables secure remote access to Cisco VPN 3000 Concentrators.
- Cisco 3002 Hardware Client-A new VPN appliance that connects SOHO computers to the VPN using a hardware-based version of the UNITY Client.
- Cisco Secure Intrusion Detection System (CSIDS) and Cisco Secure Scanner can be used to monitor and audit the security of the VPN.
- Cisco Secure Policy Manager and Cisco Works 2000 provide VPN-wide system management.

Cisco provides a suite of VPN-optimized routers. These routers range from the Cisco 800 providing telecommuter applications over IDSN to head-end connectivity with the Cisco 7100,7200,and 7500 series. The Cisco 7100 Series VPN Router provides solutions where WAN density requirements are lower, where only one or two connections to the VPN cloud are required for VPN connectivity.

The Cisco PIX 535 Firewall Supports both site-to-site and remote access VPN applications via 56-bit DES or 168-bit 3DES, the integrated VPN functionality of the PIX 535 can be supplemented with a VPN Accelerator card to deliver 100 Mbps throughput and 2,000 IPsec tunnels.

The Cisco VPN 3000 Series Concentrator includes models to support a range of enterprise customers, from small businesses with 100 or fewer remote access users to large organizations with up to 10,000 simultaneous remote users. The Cisco VPN 3000 is available in redundant or load balancing configurations, allowing for robust, reliable, and cost-effective VPNs.

The new 3002 Hardware client is a network appliance used to connect small office/ home office (SOHO) local area networks to the VPN. The device comes in ether a single port or 8-port (hub) version The 3002 replaces traditional VPN client application on individual computers

Cisco VPNs employ IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) for tunnel support, as well as the strongest standard encryption technologies available—Data Encryption Standard (DES), 3DES, and 40/128-bit RC4 for Microsoft Point-to-Point Encryption (MPPE). Cisco VPN solutions support major certificate authority vendors, such as Verisign and Entrust, for managing security/encryption administration.

We have began our discussion by introducing the concepts of a Virtual Private Network design and we've looked at some of the products that Cisco offers to provide these services. Next we will spend some time looking at the standards and protocols required to build a VPN.

IPSec Overview

IP Security (IPSec) is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec is a network layer protocol, protecting and authenticating IP packets between participating IPSec devices ("peers"), such as Cisco routers, concentrators, and firewalls. IPSec provides the following network security services.

- Data Confidentiality---The IPSec sender can encrypt packets before transmitting them across a network.
- Data Integrity---The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication---The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-Replay---The IPSec receiver can detect and reject replayed packets.

IPSec consists of the following two main protocols:

- Authentication Header
- Encapsulating Security Payload

Authentication Header (AH) provides data authentication and integrity for packets passed between two systems. AH does not provide data confidentiality (encryption) of packets. Authentication is achieved by applying a keyed one-way hash function to the packet to create a message digest. Changes in any part of the packet that occur during transit are detected by the receiver when it performs the same one-way hash function on the packet and compares the value of the message digest that the sender has supplied.

Encapsulation Security Payload (ESP) is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional anti-replay service, and limited traffic flow confidentiality by defeating traffic flow analysis. ESP provides confidentiality by performing encryption at the IP packet layer. It supports a variety of symmetric encryption algorithms. Cisco VPN devices support use of 3DES for strong encryption. Confidentiality may be selected independent of all other services.[3]

IPSec also uses encryption standards to make a protocol suite. IPSec has several standards that are supported by Cisco IOS and the PIX Firewall.

DES Algorithm uses a 56-bit key. DES is used to encrypt and decrypt packet data. It is not considered a strong enough standard at this time. The 3DES algorithm is a variant of the 56-bit DES. 3DES then operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES.

Diffies-Hellman (DH) is a public-key cryptography protocol. It allows two parties to establish a shared secret key used by encryption algorithms over as insecure communications channel. DH

is used within Internet Key Exchange (IKE) to establish session keys. 768-bit (Group 1) and 1024-bit (Group 2) DH groups are supported in the Cisco router and PIX Firewall.

Secure Hash Algorithm-1 (SHA-1) is a hash algorithm used to authenticate packet data. A hash is a one-way encryption algorithm that takes an input message of arbitrary length and produces a fixed length output message. Cisco routers and the PIX Firewall uses the SHA-1 HMAC variant which provides an additional level of hashing. IKE, AH, and ESP use SHA-1 for authentication.

Message Digest 5 (MD5) is a hashing algorithm used to authenticate packet data. Cisco routers and the PIX Firewall use the MD5 HMAC variant, which provides an additional level of hashing. IKE, AH, and ESP use MD5 for authentication.

Internet Key Exchange (IKE) is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec peers, negotiation of IKE and IPSec security associations, and establishment of keys for encryption algorithms used by IPSec. IKE is synonymous with ISAKMP in Cisco router or PIX Firewall configurations.

When two IPSec peers want to communicate, they exchange digital certificates to prove their identities. The digital certificates are obtained from a Certificate Authority (CA). CA support on Cisco products uses Rivest, Shamir, and Adelman Signatures (RSA) signatures to authenticate the CA exchange. RSA is a public-key cryptographic system used for authentication. IKE on the Cisco router and PIX Firewall uses a DH exchange to determine secret keys on each IPSec peer used by encryption algorithm. The DH exchange can be authenticated with RSA signatures or pre-shared keys.

IPSec provides secure tunnels between two peers, such as two PIX Firewalls, VPN routers, or in the case of remote access, between client software on a PC and the VPN gateway. You define which packets are considered interesting and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets, by specifying the characteristics of these tunnels. Then, when the IPSec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. In the case of remote access the Client software request initiates the process to create the tunnel. These tunnels are sets of security associations that are established between two remote IPSec peers. The security associations define which protocols and algorithms should be applied to sensitive packets, and also specify the keying material to be used by the two peers. Security associations are uni-directional and are established per security protocol (AH or ESP).[2]

IKE Overview

No matter which protocols or component technologies are used IPSec's operation can be broken into five basic steps.

Step 1. Interesting traffic initiates the IPSec process-Your security policy should be the starting point for determining the type of traffic that will cause the start of the IKE process. For Cisco routers and PIX firewalls, access lists are used to determine the traffic to encrypt. With the Cisco VPN client, you use menu windows to select connections to be secured.

Step 2. IKE Phase one-The purpose of IKE phase is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. The following tasks are performed during the phase.

- Authenticates IPSec peers
- Establishes an IKE sa policy between peers to protect the IKE exchange
- Performs Diffie-Hellman exchange producing matching shared secret keys
- Sets up a secure tunnel to negotiate IKE phase two parameters

IKE phase one uses two modes: Main mode and aggressive mode.
Main Mode has three two-way exchanges between the initiator and receiver:

In the first exchange the algorithms and hashes used to secure the IKE communications are agreed upon. The second exchange is the Diffie-Hellman exchange used to generate shared secret keying material used to generate shared secret keys. The third exchange verifies the other side's identity. The identity value is the IPSec peers IP address in encrypted form. The main purpose of main mode is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers.

In Aggressive mode, fewer exchange are done and with fewer packets. On the first exchange almost everything is squeezed in the proposed IKE SA values. The receiver sends everything back that is needed to complete the exchange. The weakness of using the aggressive mode is that both sides have exchanged information before there is a secure channel.

Step 3. IKE phase two-Negotiate IPSec SAs to set up the IPSec tunnel. IKE performs the following tasks during this phase.

- Negotiates IPSec SA parameters protected by an existing IKE SA
- Establishes IPSec security associations
- Periodically renegotiates IPSec
- Optionally performs an additional Diffie-Hellman exchange

IKE phase two negotiates a shared IPSec policy, derived shared secret keying materials used for the IPSec security algorithms, and establishes IPSec SAs.

Step 4. Data transfer-Information is transferred via an IPSec tunnel. Packets are encrypted and decrypted using the encryption specified in the IPSec SA.

Step 5. Tunnel Termination-IPSec terminates by deletion or by timing out. An SA can time out by reaching a specified number of seconds or bytes. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new phase two and, if necessary, a new phase one negotiation. [4]

IKE configuration on a Cisco router.

Ensure you are in global configuration mode:

Router# **config terminal**

Enable IKE/ISAKMP on the router:

Router(config)# **crypto isakmp enable**

Create an IKE policy to use pre-shared keys.

1. Set the policy to use pre-shared keys:
   Router(config)# **crypto isakmp policy 101**

2. Set authentication to use pre-shared keys:

   Router(config-isakmp)# **authentication pre-share**

3. **Set IKE encryption:**

   Router(config-isakmp)# **encryption des**

4. **Set the Diffie-Hellman group:**

   Router(config-isakmp)# **group 1**

5. **Set the hash algorithm:**

   Router(config-isakmp)# **hash md5**

6. **Set the IKE SA lifetime:**

   Router(config-isakmp)# **lifetime 86400**

7. Exit the config-isakmp mode:

   Router(config-isakmp)# **exit**

8. Set up the pre-shared key and peer address:

   Router(config)# **crypto isakmp key *cisco_test* address xxx.xxx.xxx.xxx**

9. **Exit config mode:**

   Router(config)# **exit**

10. **Examine the crypto is akmp policy**

    Router # **show crypto isakmp policy**

    Protection suite of priority 101

encryption algorithm	DES – Data Encryption Standard (56 bit keys)
hash	Message Digest 5
authentication method:	Pre-Shard Key

Diffie-Hellman group:	#1 (768 bit)
lifetime	86400 seconds, no volume limit Router

IPSec Configuration Task List

Ensuring Access Lists Are Compatible with IPSec

With IPSec, you define what traffic should be protected between two remote IPSec peers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected on the basis of source and destination address. (Access lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface or inbound and outbound from the PIX Firewall.)

IKE uses UDP port 500. The IPSec ESP and AH protocols use protocol numbers 50 and 51. Ensure that your access lists are configured so that protocol 50, 51, and UDP port 500 traffic is not blocked at interfaces used by IPSec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.[4]

Setting Global Lifetimes for IPSec Security Associations

You can change the global lifetime values, which are used when negotiating new IPSec security associations. These lifetimes only apply to security associations established via IKE. The default lifetimes are 3600 seconds (one hour) and 4,608,000 kilobytes (10 megabytes per second for one hour). If you change a global lifetime, the new lifetime value will not be applied to currently existing security associations, but will be used in the negotiation of subsequently established security associations. If you wish to use the new values immediately, you can clear all or part of the security association database. Refer to the **clear crypto sa** command for more details. IPSec security associations use one or more shared secret keys. These keys and their security associations time out together. The following is an example for the commands for configuring lifetimes on the router.

Router (config)# **crypto ipsec security-association lifetime seconds** *seconds*
Or
Router (config)# **crypto ipsec security-association lifetime kilobytes** *kilobytes*

Creating Crypto Access Lists

Crypto access lists are used to define which IP traffic will be protected by crypto and which traffic will not be protected by crypto. For example, access lists can be created to protect all IP traffic between Subnet A and Subnet B or Telnet traffic between Host A and Host B.
Crypto access lists associated with IPSec crypto map entries have four primary functions:

- Select outbound traffic to be protected by IPSec.
- Indicate the data flow to be protected by the new security associations (specified by a single **permit** entry) when initiating negotiations for IPSec security associations.

- Process inbound traffic in order to filter out and discard traffic that should have been protected by IPSec.
- Determine whether or not to accept requests for IPSec security associations on behalf of the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is only done for **ipsec-isakmp** crypto map entries.) In order to be accepted, if the peer initiates the IPSec negotiation, it must specify a data flow that is "permitted" by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries, which specify different IPSec policies. Cisco recommends that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

Router (config)# **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**log**]

Defining Transform Sets

A transform set represents a combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow you can specify multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry's access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peers' IPSec security associations.
With manually established security associations, there is no negotiation with the peer, so both sides must specify the same transform set. If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

To define a transform set, use the following commands starting in global configuration mode:

Step 1 Router (config)# **crypto ipsec**
transform-set
transform-set-name transform1 [*transform2*
[*transform3*]]

Step 2 Router (cfg-crypto-tran)# **mode** [**tunnel** | **transport**]

Step 3 Router (cfg-crypto-tran)# **exit**

Step 4 Router (config)# **clear crypto sa**

The table shows the transform combinations to choose from.

Transform Type	Transform	Description
AH Transform (choose one)	**Ah-md5-hmac**	AH with the MD5 (HMAC variant) authentication algorithm
	Ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm
ESP Encryption Transform (Choose one)	**esp-des**	ESP with the 56-bit DES encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm
	esp-null	Null encryption algorithm
ESP Authentication Transform (Choose one)	**esp-md5-hmac**	ESP with the MD5(HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA(HMAC variant) authentication algorithm
IP Compression Transform	**Comp-lzs**	IP compression with the LZS algorithm

Formatted

Formatted

Creating Crypto Map Entries

When IKE is used to establish security associations, the IPSec peers can negotiate the settings they will use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

The following commands will configure the crypto map to Establish an IKE Security Associations.

Router (config) # **crypto map** *map-name seq-num* **ipsec-isakmp**
Router (config-crypto-m) # **match address** *access-list-id*
Router (config-crypto-m) # **set peer** {hostname}
Router (config-crypto-m) # **set security-association lifetime seconds** *seconds*
Router (config-crypto-m) # **set security-association level per-host**

Router (config-crypto-m) # **set pfs [group1 | group2]**
Router (config-crypto-m) # **exit**

Applying Crypto Map Sets to interfaces

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Applying the crypto map set to an interface instructs the router to evaluate all the interface's traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.[1]

The following commands will apply a crypto map set to an interface, use the following command in interface configuration mode.

Router (config-if) # **crypto map** map-name

This concludes the basic configuration to terminate an IPSec tunnel on a router. We have briefly covered the Cisco equipment offered to support the Virtual Private Networking solution, defined the protocols involved with IPSec and shown a minimal IPSEC configuration.

Bibliography

1. VPN Configuration Guide/12 Dec 2001
   url: http://www.cisco.com/univercd/cc/td/doc/product/core/7100/swcg/

2. SAFE: A Security Blueprint for Enterprise Networks/13 Dec 2001
   url:http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.ht

3. SAFE VPN: IPSec Virtual Private Networks in Depth/12 Dec 2001
   url: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

4. Security Architecture for the Internet Protocol (RFC 1825)/12 Dec 2001
   url: http://www.ietf.org/rfc/rfc1825.txt?number=1825

5. The Internet Key Exchange (IKE)(RFC 2409)/13 Dec 2001
   url: http://www.ietf.org/rfc/rfc2409.txt?number=2409

6. Lee Donald / Enhanced IP Services for Cisco Networks/Indianapolis, IN/Cisco Press/, 1999