GLOSSARY

A

Access Virtual Private Network — See Access VPN.

Access VPN — Access Virtual Private Network. A Virtual Private Network (VPN) that provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

AH — Authentication Header. A security protocol which provides data authentication, data integrity, and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).

AH does not provide confidentiality. AH does not provide encryption, only authentication.

Both the older RFC1828 AH and the updated AH protocol are implemented.
RFC 1828 specifies the HMAC variant algorithm; it does not provide anti-replay services.
RFC 2402 is the latest version of AH.

The updated AH protocol is per the latest version of the “IP Authentication Header” Internet Draft (draft-ietf-ipsec-auth-header-xx.txt). The updated AH protocol allows for the use of various authentication algorithms; Cisco IOS software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms.

The updated AH protocol provides anti-replay services.

AH (HMAC-MD5) — AH (HMAC-MD5). Authentication Header (Keyed-Hashing for Message Authentication-Message Digest 5). See AH.

MD5 provides source authentication for each network packet using the HMAC-MD5 hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

MD5 performs faster and provides less secure authentication than does SHA.

RFC 2402 is the latest version of AH.
RFC 2403 is the latest version of MD5.

A (continued)

AH (HMAC-SHA) AH (HMAC-SHA). Authentication Header (Keyed-Hashing for Message Authentication-Secure Hash Algorithm). See AH.

Provides source authentication for each network packet using the HMAC-SHA hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

SHA provides more secure authentication and performs slower than does MD5.

RFC 2402 is the latest version of AH.
RFC 2404 is the latest version of SHA.

Aggressive Mode This mode during IKE negotiation is quicker than Main Mode because it eliminates several steps when the communicating parties are negotiating authentication (Phase 1).

anti-replay A security service where the receiver can reject old or duplicate packets to protect itself against replay attacks. IPSec provides this optional service by use of a sequence number combined with the use of data authentication. This service is not available for manually established security associations (that is, security associations established by manual configuration and not by IKE).

authentication The method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication establishes data integrity and ensures no one tampers with the data in transit. It also provides data origin authentication.

Authentication Header See AH.

C

CA certification authority. A service responsible for managing certificate requests and issuing certificates to participating IPSec network devices. This service is explicitly entrusted by the receiver to validate identities and to create digital certificates. This service provides centralized key management for the participating devices.

CBC Cipher Block Chaining. A component that requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

certification authority See CA.

Certificate Manager A dialog box in Cisco Secure VPN Client that allows you to request, import, and store the digital certificates you receive from certification authorities (CAs).

Certificate Signing Request See CSR.

Cipher Block Chaining See CBC.

client A node or software program (front-end device) that requests services from a server.

Client-initiated Virtual Private Network See Client-initiated VPN.

Client-initiated VPN Client-initiated Virtual Private Network. A Virtual Private Network (VPN) in which users establish an encrypted IP tunnel across the Internet service provider (ISP)’s shared network to the enterprise customer's network. The enterprise manages the client software that initiates the tunnel.

crypto map A command that filters traffic to be protected and defines the policy to be applied to that traffic.

CSR Certificate Signing Request. An electronic request you send to the certification authority for a digital certificate signature. A digital certificate must be verified and signed by a certification authority to be valid.

D

D&B D-U-N-S number Dun & Bradstreet Data Universal Numbering System. The D&B D-U-N-S number is D&B's distinctive nine-digit identification sequence, which links to a many quality information products and services originating from D&B. The D&B D-U-N-S Number is an internationally recognized common company identifier in EDI and global electronic commerce transactions.

DNS Domain Name System. System used in the Internet for translating names of network nodes into addresses.

D (continued)

data confidentiality The ability to encrypt packets before transmitting them across a network. With confidentiality, the designated recipient can decrypt and read data, while those without authorization cannot decrypt and read this data. It is provided by encryption algorithms such as Data Encryption Standard (DES).

Method where protected data is manipulated so that no attacker can read it. This is commonly provided by data encryption and keys that are only available to the parties involved in the communication.

Data Encryption Standard See DES.

data integrity Verification for the recipient that data has not been modified during transmission. This is provided by secret-key, public-key, and hashing algorithms.

data origin authentication A security service where the receiver can verify that protected data could have originated only from the sender. This service requires a data integrity service plus a key distribution mechanism, where a secret key is shared only between the sender and receiver. Also, see authentication.

DES Data Encryption Standard. A standard that encrypts packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard.

DH A public key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange. Cisco IOS software supports 768-bit and 1024-bit Diffie-Hellman groups.

With Diffie- Hellman key exchange, a public and private key can be combined to create a shared secret between two peers. Using Diffie-Hellman, you can establish session keys for IKE negotiation. Valid values for this setting are as follows:

Diffie-Hellman Group 1 enables 768-bit encryption, which requires less processing time than does Diffie-Hellman Group 2.

Diffie-Hellman Group 2 enables 1024-bit encryption, which is more secure than Diffie-Hellman Group 1.

You should choose either option based on compatibility, available processing power, and security concerns. Not all vendors support Diffie-Hellman group 2. Diffie-Hellman group 2 is also significantly more CPU intensive than Diffie-Hellman group 1; therefore, you would not want to use Diffie-Hellman group 2 on low-end devices. Diffie-Hellman group 2 is more secure than Diffie-Hellman group 1.

Diffie-Hellman See DH.

digital certificate A digital certificate contains information to identify a user or device, such as the name, serial number, company, department or IP address. It also contains a copy of the entity's public key. The certificate is signed by a certification authority (CA).

digital signature A digital signature is enabled by public key cryptography. It provides a means to digitally authenticate devices and individual users. A signature is formed when data is encrypted with a user's private key. A digital certificate receives its signature when it is signed by a certification authority (CA).

Domain Name System See DNS.

D (continued)

Dun & Bradstreet Data Universal Numbering System See D&B D-U-N-S number.

dynamic IP address A dynamic IP address is an IP address that is temporarily assigned as part of a login session, to be returned to an IP pool at the end of the session. Dynamic addresses are obtained by devices when they attach to a network, by means of some protocol-specific process. A device using a dynamic address often has a different address each time it connects to the network.

E

Encapsulating Security Payload See ESP.

encapsulation The tunneling of data in a particular protocol header. For example, Ethernet data is tunneled in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

encryption The application of a specific algorithm to data to scramble its appearance, making the data incomprehensible to those who are not authorized to see the information.

ESP Encapsulating Security Payload. A security protocol which provides data confidentiality, data integrity, and protection services, optional data origin authentication, and anti-replay services. ESP encapsulates the data to be protected. ESP can be used either by itself or in conjunction with AH. ESP can be configured with DES or Triple DES.

Both the older RFC 1829 ESP and the updated ESP protocol are implemented.
RFC 1829 specifies DES-CBC as the encryption algorithm; it does not provide data authentication or anti-replay services.
RFC 2406 documents the latest version of ESP.

The updated ESP protocol is per the latest version of the “IP Encapsulating Security Payload” Internet Draft (draft-ietf-ipsec-esp-v2-xx.txt). The updated ESP protocol allows for the use of various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS software implements the mandatory 56-bit DES-CBC with Explicit IV as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides anti-replay services.

ESP (DES-CBC) ESP (DES-CBC). Encapsulation (Data Encryption Standard-Cipher Block Chaining) encryption algorithm. See ESP.

DES-CBC provides 56-bit basic encryption with the updated ESP protocol, anti-replay services, and can be used with various cipher and authentication algorithms.

DES performs faster and provides less secure encryption than does Triple DES.

Supported combined with HMAC-MD5 or HMAC-SHA.

RFC 2406 documents the latest version of ESP.
RFC 2405 documents the latest version of ESP CBC.

E (continued)

ESP (HMAC-MD5) ESP (HMAC-MD5). Encapsulation with Authentication Header (Keyed-Hashing for Message Authentication-Message Digest 5) encryption and authentication algorithm. See ESP and AH.

HMAC-MD5 provides source authentication for each network packet using the HMAC-MD5 hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

MD5 performs faster and provides less secure authentication than does SHA.

Supported combined with DES-CBC.

RFC 2406 documents the latest version of ESP.
RFC 2403 documents the latest version of MD5.

ESP (HMAC-SHA) ESP(HMAC-SHA). Encapsulation with Authentication Header (Keyed-Hashing for Message Authentication-Secure Hash Algorithm) encryption and authentication algorithm. See ESP and AH.

SHA provides source authentication for each network packet using the HMAC-SHA hash algorithm. Also, provides optional anti-replay services, in which a receiving peer can protect itself against replay attacks by denying old or duplicate packets.

SHA provides more secure authentication and performs slower than does MD5.

Supported combined with DES-CBC and Triple-DES.

RFC 2406 documents the latest version of ESP.
RFC 2404 documents the latest version of SHA.

ESP (Triple DES) ESP (Triple DES). Encapsulation (Triple Data Encryption Standard) encryption algorithm. See ESP.

Triple DES provides 168-bit encryption and processes each cipher block three times with three different keys to increase encryption strength.

Triple DES provides more secure encryption and performs slower than does DES-CBC.

Supported combined with HMAC-MD5 or HMAC-SHA.

RFC 2406 documents the latest version of ESP.

Extranet Virtual Private Network See Extranet VPN.

Extranet VPN Extranet Virtual Private Network. A private communications channel between two or more separate entities that may involve data traversing the Internet or some other Wide Area Network (WAN). An extranet VPN links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections.

G

gateway A device that performs an application layer conversion from one protocol stack to another.

H

hash algorithm A mechanism for data authentication and maintenance of data integrity as packets are transmitted. This one way function takes an input message of arbitrary length and produces a fixed length digest. Cisco uses both Secure Hash Algorithm (SHA) and Message Digest 5 (MD5) hashes in the implementation of the IPSec framework.

SHA produces a 160-bit digest, which is more resistant to brute-force attacks than MD5. It is recommended that you use SHA for a more secure authentication.

MD5 produces a 128-bit digest, which uses less processing time than does SHA. It is recommended that you use SHA for a more secure authentication.

See HMAC variant.

HMAC variant Keyed-Hashing for Message Authentication. A mechanism for message authentication using cryptographic hashes such as SHA and MD5. See RFC 2104.

Keyed-Hashing for Message Authentication See HMAC variant.

I

IKE Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

Internet Engineering Task Force Task force consisting of over 80 working groups responsible for developing Internet standards.

Internet Key Exchange See IKE.

Internet Security Association and Key Management Protocol See ISAKMP.

I (continued)

Internet Virtual Private Network See Internet VPN.

Internet VPN Internet Virtual Private Network. A private communications channel over the public access Internet that connects remote offices across the Internet and remote dial users to their home gateway via an ISP.

Intranet Virtual Private Network See Intranet VPN.

Intranet VPN Intranet Virtual Private Network. A private communications channel within an enterprise or organization that may or may not involve traffic traversing a Wide Area Network (WAN). An intranet VPN links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections.

IP Security Protocol See IPSec.

IPSec IP Security Protocol. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

RFC 2401 documents IP Security Architecture.

ISAKMP Internet Security Association and Key Management Protocol. A protocol framework which defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of an SA.

M

MD5 Message Digest 5. One way hash that combines a shared secret and the message (the header and payload) to produce a 128-bit value. The recipient of the message runs the same hash of the message and compares it with the inserted hash value to yield the same result, which indicates that nothing in the packet has been changed in transit.

SHA is more secure than MD4 and MD5. Cisco uses hashes for authentication within the IPSec framework.

RFC 2403 documents the latest version of MD5.

Main Mode This mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1).

Manual Keys This mode requires no negotiations; it is available for troubleshooting only.

Message Digest 5 See MD5.

N

NAS network access server. Cisco platform (or collection of platforms such as an AccessPath system which interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).

NAS-Initiated VPN network access server-initiated Virtual Private Network. Users dial in to the ISP's network access server, which establishes an encrypted tunnel to the enterprise's private network.

network access server See NAS.

network access server-initiated Virtual Private Network See NAS-Initiated VPN.

non-repudiation A quality where a third party can prove that a communication between two other parties took place. Non-repudiation is desirable if you want to be able to trace your communications and prove that they occurred.

See also repudiation.

O

Oakley key exchange A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the Diffie-Hellman key exchange algorithm (DH).

P

peer A router or device that participates as an endpoint in IPSec and IKE.

peer authentication methods Methods required to authenticate the data flows between peers. Also used to generate a shared secret key to protect the IKE channel via DES-CBC. This shared secret key is also used as a basis for creating the IPSec shared secret encryption key by combining it with a random value.

Perfect Forward Secrecy Perfect forward secrecy (PFS) is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

PKI Public Key Infrastructure. Software, encryption and authentication technologies, and services that allows secure communications for enterprises over the Internet.

Plain Old Telephone System See PSTN.

POTS See PSTN.

pre-shared keys An authentication method in a policy. A given pre-shared key is shared between two peers. Pre-shared keys are simpler to configure, but less scalable than digital certification.

P (continued)

PSTN Public Switched Telephone Network. General term referring to the variety of telephone networks and services in place worldwide. Sometimes called Plain Old Telephone System (POTS).

public key cryptography Each user has a key-pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. Public key cryptography is the same as public/private key system.

public key infrastructure See PKI.

Public Switched Telephone Network See PSTN.

public/private key system See public key cryptography.

Q

QoS quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

quality of service See QoS.

R

RA Registration Authority. A server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

Registration Authority See RA.

replay-detection A security service where the receiver can reject old or duplicate packets in order to defeat replay attacks (replay attacks rely on the attacker sending out older or duplicate packets to the receiver and the receiver thinking that the bogus traffic is legitimate). Replay-detection is done by using sequence numbers combined with authentication, and is a standard feature of IPSec.

repudiation A quality that prevents a third party from being able to prove that a communication between two other parties ever took place. This is a desirable quality if you do not want your communications to be traceable.

See also non-repudiation.

Rivest, Shamir and Adleman See RSA.

RSA Rivest, Shamir and Adleman algorithm. A public key cryptographic algorithm (named after its inventors, Rivest, Shamir and Adleman) with a variable key length. Cisco's IKE implementation uses a Diffie-Hellman (DH) exchange to get the secret keys. This exchange can be authenticated with RSA (or pre-shared keys). With the Diffie-Hellman exchange, the DES key never crosses the network (not even in encrypted form), which is not the case with the RSA encrypt and sign technique. RSA is not public domain, and must be licensed from RSA Data Security.

S

SA Security Association. An instance of security policy and keying material applied to a data flow. Both IKE and IPSec use SAs, although SAs are independent of one another. IPSec SAs are unidirectional and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

SCEP Simple Certificate Enrollment Protocol. A PKI communication protocol which leverages existing technology by using PKCS #7 and PKCS #10.

Secure Hash Algorithm See SHA.

Security Association See SA.

Security Parameter Index See SPI.

security policy The means to configure the Policy Enforcement Points (PEPs) to accept or deny network traffic. These rules allow a network service to originate from a specific source.

Security Policy Editor A dialog box in Cisco Secure VPN Client that allows you to establish connections and associated authentication and key exchange proposals, then list them in hierarchical order for defining an IP data communications security policy.

SHA A one way hash put forth by NIST. SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to attacks than 128-bit hashes (such as MD5), but it is slower.

RFC 2404 documents the latest version of SHA.

Simple Certificate Enrollment Protocol See SCEP.

Skeme key exchange A key exchange protocol which defines how to derive authenticated keying material, with rapid key refreshment.

SPI Security Parameter Index. This is a number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association. SPI has a 32-bit value.

static IP address A static IP address is a unique IP address that is assigned to a client for an extended period of time, to be used by only that client. Static addresses are assigned by a network administrator according to a preconceived Internetwork addressing plan. A static address does not change until the network administrator manually changes it.

T

3DES A variant of the DES, which iterates three times with three separate keys, effectively doubling the strength of DES.

transform A transform describes a security protocol (AH or ESP) with its corresponding algorithms. For example, ESP with the DES cipher algorithm and HMAC variant-SHA for authentication.

transform set A grouping of IPSec algorithms to negotiate with IKE. A transform set specifies one or two IPSec security protocols (either ESP or AH or both) and specifies which algorithms to use with the selected security protocol.

transport mode A mode in which the IP payload is encrypted, and the original IP headers are left intact. It adds only a few bytes to each packet and allows devices on the public network to see the final source and destination of the packet. This capability allows one to enable special processing (for example, quality of service) in the intermediate network based on the information on the IP header. However, the Layer 4 header will be encrypted, limiting the examination of the packet. The opposite of transport mode is tunnel mode. Transport mode is typically used in a host-to-host connection.

Triple DES See 3DES.

tunnel A secure communication path between two peers, such as a client and a router.

tunnel mode Encapsulation in which the entire original IP datagram is encrypted, and it becomes the payload in a new IP packet. This mode allows a network device, such as a router, to act as an IPSec proxy. The router performs encryption on behalf of the hosts. The source's router encrypts packets and forwards them along the IPSec tunnel. The destination's router decrypts the original IP datagram and forwards it on to the destination system. Tunnel mode is typically used in a gateway-to-gateway connection.

V

Virtual Private Network See VPN.

VPN Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.