



## GLOSSARY

[Numerics](#) | [A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#)

---

### Numerics

**3DES** See [DES](#).

---

### A

**AAA** Authentication, authorization, and accounting. See also [TACACS+](#) and [RADIUS](#).

**ABR** Area Border Router. In [OSPF](#), a router with interfaces in multiple areas.

**ACE** Access Control Entry. Information entered into the configuration that lets you specify what type of traffic to permit or deny on an [interface](#). By default, traffic that is not explicitly permitted is denied.

**Access Modes** The security appliance CLI uses several command modes. The commands available in each mode vary. See also [user EXEC mode](#), [privileged EXEC mode](#), [global configuration mode](#), [command-specific configuration mode](#).

**ACL** Access Control List. A collection of [ACEs](#). An ACL lets you specify what type of traffic to allow on an interface. By default, traffic that is not explicitly permitted is denied. ACLs are usually applied to the [interface](#) which is the source of inbound traffic. See also [rule](#), [outbound ACL](#).

**ActiveX** A set of object-oriented programming technologies and tools used to create mobile or portable programs. An ActiveX program is roughly equivalent to a Java applet.

**Address Resolution Protocol** See [ARP](#).

**address translation** The translation of a network address and/or port to another network address/or port. See also [IP address](#), [interface PAT](#), [NAT](#), [PAT](#), [Static PAT](#), [xlate](#).

**AES** Advanced Encryption Standard. A symmetric block cipher that can encrypt and decrypt information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. See also [DES](#).

**AH** Authentication Header. An IP protocol (type 51) that can ensure data integrity, authentication, and replay detection. AH is embedded in the data to be protected (a full IP datagram, for example). AH can be used either by itself or with [ESP](#). This is an older [IPSec](#) protocol that is less important in most networks than [ESP](#). AH provides authentication services but does not provide encryption services. It is provided to ensure compatibility with [IPSec](#) peers that do not support [ESP](#), which provides both [authentication](#) and [encryption](#). See also [encryption](#) and [VPN](#). Refer to the RFC 2402.

**A record address** “A” stands for address, and refers to name-to-address mapped records in [DNS](#).

<b>APCF</b>	Application Profile Customization Framework. Lets the security appliance handle non-standard applications so that they render correctly over a WebVPN connection.
<b>ARP</b>	Address Resolution Protocol. A low-level TCP/IP protocol that maps a hardware address, or MAC address, to an IP address. An example hardware address is 00:00:a6:00:01:ba. The first three groups of characters (00:00:a6) identify the manufacturer; the rest of the characters (00:01:ba) identify the system card. ARP is defined in RFC 826.
<b>ASA</b>	Adaptive Security Algorithm. Used by the security appliance to perform inspections. ASA allows one-way (inside to outside) connections without an explicit configuration for each internal system and application. See also <a href="#">inspection engine</a> .
<b>ASA</b>	adaptive security appliance.
<b>ASDM</b>	Adaptive Security Device Manager. An application for managing and configuring a single security appliance.
<b>asymmetric encryption</b>	Also called public key systems, asymmetric encryption allows anyone to obtain access to the public key of anyone else. Once the public key is accessed, one can send an encrypted message to that person using the public key. See also <a href="#">encryption</a> , <a href="#">public key</a> .
<b>authentication</b>	Cryptographic protocols and services that verify the identity of users and the integrity of data. One of the functions of the <a href="#">IPSec</a> framework. Authentication establishes the integrity of datastream and ensures that it is not tampered with in transit. It also provides confirmation about the origin of the datastream. See also <a href="#">AAA</a> , <a href="#">encryption</a> , and <a href="#">VPN</a> .
<b>Auto Applet Download</b>	Automatically downloads the WebVPN port-forwarding applet when the user first logs in to WebVPN.
<b>auto-signon</b>	This command provides a single sign-on method for WebVPN users. It passes the WebVPN login credentials (username and password) to internal servers for authentication using NTLM authentication, basic authentication, or both.

---

## B

<b>Backup Server</b>	IPSec backup servers let a VPN client connect to the central site when the primary security appliance is unavailable.
<b>BGP</b>	Border Gateway Protocol. BGP performs interdomain routing in TCP/IP networks. BGP is an Exterior Gateway Protocol, which means that it performs routing between multiple autonomous systems or domains and exchanges routing and access information with other BGP systems. The security appliance does not support BGP. See also <a href="#">EGP</a> .
<b>BLT stream</b>	Bandwidth Limited Traffic stream. Stream or flow of packets whose bandwidth is constrained.
<b>BOOTP</b>	Bootstrap Protocol. Lets diskless workstations boot over the network as is described in RFC 951 and RFC 1542.
<b>BPDU</b>	Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network. Protocol data unit is the OSI term for packet.

---

**C**

<b>CA</b>	Certificate Authority, Certification Authority. A third-party entity that is responsible for issuing and revoking certificates. Each device with the public key of the CA can authenticate a device that has a certificate issued by the CA. The term CA also refers to software that provides CA services. See also <a href="#">certificate</a> , <a href="#">CRL</a> , <a href="#">public key</a> , <a href="#">RA</a> .
<b>cache</b>	A temporary repository of information accumulated from previous task executions that can be reused, decreasing the time required to perform the tasks. Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content.
<b>CBC</b>	Cipher Block Chaining. A cryptographic technique that increases the encryption strength of an algorithm. CBC requires an initialization vector (IV) to start encryption. The IV is explicitly given in the <a href="#">IPSec</a> packet.
<b>certificate</b>	A signed cryptographic object that contains the identity of a user or device and the public key of the <a href="#">CA</a> that issued the certificate. Certificates have an expiration date and may also be placed on a <a href="#">CRL</a> if known to be compromised. Certificates also establish non-repudiation for <a href="#">IKE</a> negotiation, which means that you can prove to a third party that <a href="#">IKE</a> negotiation was completed with a specific peer.
<b>CHAP</b>	Challenge Handshake Authentication Protocol.
<b>CIFS</b>	Common Internet File System. It is a platform-independent file sharing system that provides users with network access to files, printers, and other machine resources. Microsoft implemented CIFS for networks of Windows computers, however, open source implementations of CIFS provide file access to servers running other operating systems, such as Linux, UNIX, and Mac OS X.
<b>Citrix</b>	An application that virtualizes client-server applications and optimizes web applications.
<b>CLI</b>	command line interface. The primary interface for entering configuration and monitoring commands to the security appliance.
<b>client/server computing</b>	Distributed computing (processing) network systems in which transaction responsibilities are divided into two parts: client (front end) and server (back end). Also called distributed computing. See also <a href="#">RPC</a> .
<b>Client update</b>	Lets you update revisions of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version.
<b>command-specific configuration mode</b>	From global configuration mode, some commands enter a command-specific configuration mode. All user EXEC, privileged EXEC, global configuration, and command-specific configuration commands are available in this mode. See also <a href="#">global configuration mode</a> , <a href="#">privileged EXEC mode</a> , <a href="#">user EXEC mode</a> .
<b>Compression</b>	The process of encoding information using fewer bits or other information-bearing units than an unencoded representation would use. Compression can reduce the size of transferring packets and increase communication performance.
<b>configuration, config, config file</b>	A file on the security appliance that represents the equivalent of settings, preferences, and properties administered by <a href="#">ASDM</a> or the <a href="#">CLI</a> .

<b>Content Rewriting/Transformation</b>	Interprets and modifies applications so that they render correctly over a WebVPN connection.
<b>cookie</b>	A cookie is a object stored by a browser. Cookies contain information, such as user preferences, to persistent storage.
<b>CPU</b>	Central Processing Unit. Main processor.
<b>CRC</b>	Cyclical Redundancy Check. Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.
<b>CRL</b>	Certificate Revocation List. A digitally signed message that lists all of the current but revoked certificates listed by a given <a href="#">CA</a> . This is analogous to a book of stolen charge card numbers that allow stores to reject bad credit cards. When certificates are revoked, they are added to a CRL. When you implement authentication using certificates, you can choose to use CRLs or not. Using CRLs lets you easily revoke certificates before they expire, but the CRL is generally only maintained by the <a href="#">CA</a> or an <a href="#">RA</a> . If you are using CRLs and the connection to the <a href="#">CA</a> or <a href="#">RA</a> is not available when authentication is requested, the authentication request will fail. See also <a href="#">CA</a> , <a href="#">certificate</a> , <a href="#">public key</a> , <a href="#">RA</a> .
<b>CRV</b>	Call Reference Value. Used by <a href="#">H.225.0</a> to distinguish call legs signalled between two entities.
<b>cryptography</b>	Encryption, authentication, integrity, keys and other services used for secure communication over networks. See also <a href="#">VPN</a> and <a href="#">IPSec</a> .
<b>crypto map</b>	A data structure with a unique name and sequence number that is used for configuring VPNs on the security appliance. A crypto map selects data flows that need security processing and defines the policy for these flows and the crypto peer that traffic needs to go to. A crypto map is applied to an interface. Crypto maps contain the <a href="#">ACLs</a> , encryption standards, peers, and other parameters necessary to specify security policies for <a href="#">VPNs</a> using <a href="#">IKE</a> and <a href="#">IPSec</a> . See also <a href="#">VPN</a> .
<b>CTIQBE</b>	Computer Telephony Interface Quick Buffer Encoding. A protocol used in IP telephony between the Cisco CallManager and CTI <a href="#">TAPI</a> and <a href="#">JTAPI</a> applications. CTIQBE is used by the TAPI/JTAPI protocol inspection module and supports <a href="#">NAT</a> , <a href="#">PAT</a> , and bi-directional <a href="#">NAT</a> . This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to communicate with Cisco CallManager for call setup and voice traffic across the security appliance.
<b>cut-through proxy</b>	Enables the security appliance to provide faster traffic flow after user authentication. The cut-through proxy challenges a user initially at the application layer. After the security appliance authenticates the user, it shifts the session flow and all traffic flows directly and quickly between the source and destination while maintaining session state information.

---

## D

<b>data confidentiality</b>	Describes any method that manipulates data so that no attacker can read it. This is commonly achieved by data encryption and <a href="#">keys</a> that are only available to the parties involved in the communication.
<b>data integrity</b>	Describes mechanisms that, through the use of encryption based on <a href="#">secret key</a> or <a href="#">public key</a> algorithms, allow the recipient of a piece of protected data to verify that the data has not been modified in transit.

<b>data origin authentication</b>	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 <a href="#">key</a> distribution mechanism, where a <a href="#">secret key</a> is shared only between the sender and receiver.
<b>decryption</b>	Application of a specific algorithm or cipher to encrypted data so as to render the data comprehensible to those who are authorized to see the information. See also <a href="#">encryption</a> .
<b>DES</b>	Data encryption standard. DES was published in 1977 by the National Bureau of Standards and is a secret key encryption scheme based on the Lucifer algorithm from IBM. Cisco uses DES in classic crypto (40-bit and 56-bit key lengths), <a href="#">IPSec</a> crypto (56-bit key), and 3DES (triple DES), which performs encryption three times using a 56-bit key. 3DES is more secure than DES but requires more processing for encryption and decryption. See also <a href="#">AES</a> , <a href="#">ESP</a> .
<b>DHCP</b>	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses to hosts dynamically, so that addresses can be reused when hosts no longer need them and so that mobile computers, such as laptops, receive an IP address applicable to the <a href="#">LAN</a> to which it is connected.
<b>Diffie-Hellman</b>	A public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within <a href="#">IKE</a> to establish session keys. Diffie-Hellman is a component of <a href="#">Oakley</a> key exchange.
<b>Diffie-Hellman Group 1, Group 2, Group 5, Group 7</b>	Diffie-Hellman refers to a type of public key cryptography using asymmetric encryption based on large prime numbers to establish both Phase 1 and Phase 2 <a href="#">SAs</a> . Group 1 provides a smaller prime number than Group 2 but may be the only version supported by some <a href="#">IPSec</a> peers. Diffie-Hellman Group 5 uses a 1536-bit prime number, is the most secure, and is recommended for use with <a href="#">AES</a> . Group 7 has an elliptical curve field size of 163 bits and is for use with the Movian VPN client, but works with any peer that supports Group 7 (ECC). See also <a href="#">VPN</a> and <a href="#">encryption</a> .
<b>digital certificate</b>	See <a href="#">certificate</a> .
<b>DMZ</b>	See <a href="#">interface</a> .
<b>DN</b>	Distinguished Name. Global, authoritative name of an entry in the OSI Directory (X.500).
<b>DNS</b>	Domain Name System (or Service). An Internet service that translates domain names into IP addresses.
<b>DoS</b>	Denial of Service. A type of network attack in which the goal is to render a network service unavailable.
<b>DSL</b>	digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. DSL is provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.
<b>DSP</b>	digital signal processor. A DSP segments a voice signal into frames and stores them in voice packets.
<b>DSS</b>	Digital Signature Standard. A digital signature algorithm designed by The US National Institute of Standards and Technology and based on public-key cryptography. DSS does not do user datagram encryption. DSS is a component in classic crypto, as well as the Redcreek <a href="#">IPSec</a> card, but not in <a href="#">IPSec</a> implemented in Cisco IOS software.

**Dynamic NAT** See [NAT](#) and [address translation](#).

**Dynamic PAT** Dynamic Port Address Translation. Dynamic PAT lets multiple outbound sessions appear to originate from a single IP address. With PAT enabled, the security appliance chooses a unique port number from the PAT IP address for each outbound translation slot ([xlate](#)). This feature is valuable when an [ISP](#) cannot allocate enough unique IP addresses for your outbound connections. The global pool addresses always come first, before a PAT address is used. See also [NAT](#), [Static PAT](#), and [xlate](#).

---

## E

**ECHO** See [Ping](#), [ICMP](#). See also [inspection engine](#).

**EGP** Exterior Gateway Protocol. Replaced by BGP. The security appliance does not support EGP. See also [BGP](#).

**EIGRP** Enhanced Interior Gateway Routing Protocol. The security appliance does not support EIGRP.

**EMBLEM** Enterprise Management BaseLine Embedded Manageability. A syslog format designed to be consistent with the Cisco IOS system log format and is more compatible with CiscoWorks management applications.

**encryption** Application of a specific algorithm or cipher to data so as to render the data incomprehensible to those unauthorized to see the information. See also [decryption](#).

**ESMTP** Extended [SMTP](#). Extended version of [SMTP](#) that includes additional functionality, such as delivery notification and session delivery. ESMTP is described in RFC 1869, SMTP Service Extensions.

**ESP** Encapsulating Security Payload. An [IPSec](#) protocol, ESP provides authentication and encryption services for establishing a secure tunnel over an insecure network. For more information, refer to RFCs 2406 and 1827.

---

## F

**failover, failover mode** Failover lets you configure two security appliances so that one will take over operation if the other one fails. The security appliance supports two failover configurations, Active/Active failover and Active/Standby failover. Each failover configuration has its own method for determining and performing failover. With Active/Active failover, both units can pass network traffic. This lets you configure load balancing on your network. Active/Active failover is only available on units running in multiple context mode. With Active/Standby failover, only one unit passes traffic while the other unit waits in a standby state. Active/Standby failover is available on units running in either single or multiple context mode.

**Fixup** See [inspection engine](#).

**Flash, Flash memory** A nonvolatile storage device used to store the configuration file when the security appliance is powered down.

**FQDN/IP** Fully qualified domain name/IP address. [IPSec](#) parameter that identifies peers that are security gateways.

**FragGuard** Provides IP fragment protection and performs full reassembly of all [ICMP](#) error messages and virtual reassembly of the remaining IP fragments that are routed through the security appliance.

**FTP** File Transfer Protocol. Part of the TCP/IP protocol stack, used for transferring files between hosts.

---

## G

**GGSN** gateway [GPRS](#) support node. A wireless gateway that allows mobile cell phone users to access the public data network or specified private IP networks.

**global configuration mode** Global configuration mode lets you to change the security appliance configuration. All user EXEC, privileged EXEC, and global configuration commands are available in this mode. See also [user EXEC mode](#), [privileged EXEC mode](#), [command-specific configuration mode](#).

**GMT** Greenwich Mean Time. Replaced by UTC (Coordinated Universal Time) in 1967 as the world time standard.

**GPRS** general packet radio service. A service defined and standardized by the European Telecommunication Standards Institute. GPRS is an IP-packet-based extension of [GSM](#) networks and provides mobile, wireless, data communications

**GRE** Generic Routing Encapsulation described in RFCs 1701 and 1702. GRE is a tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to routers at remote points over an IP network. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single protocol backbone environment.

**GSM** Global System for Mobile Communication. A digital, mobile, radio standard developed for mobile, wireless, voice communications.

**GTP** GPRS tunneling protocol. GTP handles the flow of user packet data and signaling information between the [SGSN](#) and [GGSN](#) in a [GPRS](#) network. GTP is defined on both the Gn and Gp interfaces of a [GPRS](#) network.

---

## H

**H.225** A protocol used for TCP signalling in applications such as video conferencing. See also [H.323](#) and [inspection engine](#).

**H.225.0** An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of [RTP](#).

**H.245** An ITU standard that governs H.245 endpoint control.

**H.320** Suite of ITU-T standard specifications for video conferencing over circuit-switched media, such as ISDN, fractional T-1, and switched-56 lines. Extensions of ITU-T standard H.320 enable video conferencing over LANs and other packet-switched networks, as well as video over the [Internet](#).



<b>H.323</b>	Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.
<b>H.323 RAS</b>	Registration, admission, and status signaling protocol. Enables devices to perform registration, admissions, bandwidth changes, and status and disengage procedures between <a href="#">VoIP</a> gateway and the gatekeeper.
<b>H.450.2</b>	Call transfer supplementary service for <a href="#">H.323</a> .
<b>H.450.3</b>	Call diversion supplementary service for <a href="#">H.323</a> .
<b>Hash, Hash Algorithm</b>	A hash algorithm is a one way function that operates on a message of arbitrary length to create a fixed-length message digest used by cryptographic services to ensure its data integrity. MD5 has a smaller digest and is considered to be slightly faster than <a href="#">SHA-1</a> . Cisco uses both <a href="#">SHA-1</a> and <a href="#">MD5</a> hashes within our implementation of the <a href="#">IPSec</a> framework. See also <a href="#">encryption</a> , <a href="#">HMAC</a> , and <a href="#">VPN</a> .
<b>headend</b>	A firewall, concentrator, or other host that serves as the entry point into a private network for <a href="#">VPN</a> client connections over the public network. See also <a href="#">ISP</a> and <a href="#">VPN</a> .
<b>HMAC</b>	A mechanism for message authentication using cryptographic hashes such as <a href="#">SHA-1</a> and <a href="#">MD5</a> .
<b>host</b>	The name for any device on a TCP/IP network that has an IP address. See also <a href="#">network</a> and <a href="#">node</a> .
<b>host/network</b>	An IP address and netmask used with other information to identify a single host or network subnet for security appliance configuration, such as an address translation ( <a href="#">xlate</a> ) or <a href="#">ACE</a> .
<b>HTTP</b>	Hypertext Transfer Protocol. A protocol used by browsers and web servers to transfer files. When a user views a web page, the browser can use HTTP to request and receive the files used by the web page. HTTP transmissions are not encrypted.
<b>HTTPS</b>	Hypertext Transfer Protocol Secure. An <a href="#">SSL</a> -encrypted version of HTTP.

---

<b>IANA</b>	Internet Assigned Number Authority. Assigns all port and protocol numbers for use on the <a href="#">Internet</a> .
<b>ICMP</b>	Internet Control Message Protocol. Network-layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
<b>IDS</b>	Intrusion Detection System. A method of detecting malicious network activity by signatures and then implementing a policy for that signature.
<b>IETF</b>	The Internet Engineering Task Force. A technical standards organization that develops <a href="#">RFC</a> documents defining protocols for the <a href="#">Internet</a> .
<b>IGMP</b>	Internet Group Management Protocol. IGMP is a protocol used by IPv4 systems to report IP <a href="#">multicast</a> memberships to neighboring multicast routers.



<b>IKE</b>	Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as <a href="#">IPSec</a> ) that require keys. Before any <a href="#">IPSec</a> traffic can be passed, each security appliance must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a <a href="#">CA</a> service. IKE is a hybrid protocol that uses part <a href="#">Oakley</a> and part of another protocol suite called <a href="#">SKEME</a> inside <a href="#">ISAKMP</a> framework. This is the protocol formerly known as ISAKMP/Oakley, and is defined in RFC 2409.
<b>IKE Extended Authentication</b>	IKE Extended Authenticate (Xauth) is implemented per the IETF draft-ietf-ipsec-isakmp-xauth-04.txt (“extended authentication” draft). This protocol provides the capability of authenticating a user within IKE using <a href="#">TACACS+</a> or <a href="#">RADIUS</a> .
<b>IKE Mode Configuration</b>	IKE Mode Configuration is implemented per the IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt. IKE Mode Configuration provides a method for a security gateway to download an IP address (and other network level configuration) to the VPN client as part of an IKE negotiation.
<b>ILS</b>	Internet Locator Service. ILS is based on LDAP and is ILSv2 compliant. ILS was developed by Microsoft for use with its NetMeeting, SiteServer, and Active Directory products.
<b>IMAP</b>	Internet Message Access Protocol. Method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.
<b>implicit rule</b>	An access rule automatically created by the security appliance based on default rules or as a result of user-defined rules.
<b>IMSI</b>	International Mobile Subscriber Identity. One of two components of a <a href="#">GTP</a> tunnel ID, the other being the <a href="#">NSAPI</a> . See also <a href="#">NSAPI</a> .
<b>inside</b>	The first interface, usually port 1, that connects your internal, “trusted” network protected by the security appliance. See also <a href="#">interface</a> , <a href="#">interface names</a> .
<b>inspection engine</b>	The security appliance inspects certain application-level protocols to identify the location of embedded addressing information in traffic. This allows <a href="#">NAT</a> to translate these embedded addresses and to update any checksum or other fields that are affected by the translation. Because many protocols open secondary <a href="#">TCP</a> or <a href="#">UDP</a> ports, each application inspection engine also monitors sessions to determine the port numbers for secondary channels. The initial session on a well-known port is used to negotiate dynamically assigned port numbers. The application inspection engine monitors these sessions, identifies the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session. Some of the protocols that the security appliance can inspect are <a href="#">CTIQBE</a> , <a href="#">FTP</a> , <a href="#">H.323</a> , <a href="#">HTTP</a> , <a href="#">MGCP</a> , <a href="#">SMTP</a> , and <a href="#">SNMP</a> .
<b>interface</b>	The physical connection between a particular network and a security appliance.
<b>interface ip_address</b>	The IP address of a security appliance network interface. Each interface IP address must be unique. Two or more interfaces must not be given the same IP address or IP addresses that are on the same IP network.
<b>interface names</b>	Human readable name assigned to a security appliance network interface. The inside interface default name is “inside” and the outside interface default name is “outside.” Any perimeter interface default names are “intf <i>n</i> ”, such as intf2 for the first perimeter interface, intf3 for the second perimeter interface, and so on to the last interface. The numbers in the intf string corresponds to the position of the interface card in the security appliance. You can use the default names or, if you are an experienced user, give each interface a more meaningful name. See also <a href="#">inside</a> , <a href="#">intf<i>n</i></a> , <a href="#">outside</a> .

<b>intfn</b>	Any interface, usually beginning with port 2, that connects to a subset network of your design that you can custom name and configure.
<b>interface PAT</b>	The use of <a href="#">PAT</a> where the <a href="#">PAT</a> IP address is also the IP address of the outside interface. See <a href="#">Dynamic PAT</a> , <a href="#">Static PAT</a> .
<b>Internet</b>	The global network that uses <a href="#">IP</a> . Not a <a href="#">LAN</a> . See also <a href="#">intranet</a> .
<b>intranet</b>	Intranetwork. A LAN that uses <a href="#">IP</a> . See also <a href="#">network</a> and <a href="#">Internet</a> .
<b>IP</b>	Internet Protocol. IP protocols are the most popular nonproprietary protocols because they can be used to communicate across any set of interconnected networks and are equally well suited for <a href="#">LAN</a> and <a href="#">WAN</a> communications.
<b>IPS</b>	Intrusion Prevention Service. An in-line, deep-packet inspection-based solution that helps mitigate a wide range of network attacks.
<b>IP address</b>	An IP protocol address. A security appliance interface <code>ip_address</code> . IP version 4 addresses are 32 bits in length. This address space is used to designate the network number, optional subnetwork number, and a host number. The 32 bits are grouped into four octets (8 binary bits), represented by 4 decimal numbers separated by periods, or dots. The meaning of each of the four octets is determined by their use in a particular network.
<b>IP pool</b>	A range of local IP addresses specified by a name, and a range with a starting IP address and an ending address. IP Pools are used by <a href="#">DHCP</a> and <a href="#">VPNs</a> to assign local IP addresses to clients on the inside interface.
<b>IPSec</b>	IP Security. 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. IPSec uses <a href="#">IKE</a> to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can 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.
<b>IPSec Phase 1</b>	The first phase of negotiating <a href="#">IPSec</a> , includes the key exchange and the <a href="#">ISAKMP</a> portions of <a href="#">IPSec</a> .
<b>IPSec Phase 2</b>	The second phase of negotiating <a href="#">IPSec</a> . Phase two determines the type of encryption rules used for payload, the source and destination that will be used for encryption, the definition of interesting traffic according to access lists, and the <a href="#">IPSec</a> peer. <a href="#">IPSec</a> is applied to the interface in Phase 2.
<b>IPSec transform set</b>	A transform set specifies the <a href="#">IPSec</a> protocol, encryption algorithm, and hash algorithm to use on traffic matching the <a href="#">IPSec</a> policy. A transform describes a security protocol ( <a href="#">AH</a> or <a href="#">ESP</a> ) with its corresponding algorithms. The <a href="#">IPSec</a> protocol used in almost all transform sets is <a href="#">ESP</a> with the <a href="#">DES</a> algorithm and HMAC-SHA for authentication.
<b>ISAKMP</b>	Internet Security Association and Key Management Protocol. A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association. See <a href="#">IKE</a> .
<b>ISP</b>	Internet Service Provider. An organization that provides connection to the <a href="#">Internet</a> via their services, such as modem dial in over telephone voice lines or <a href="#">DSL</a> .

---

**J**

**JTAPI** Java Telephony Application Programming Interface. A Java-based API supporting telephony functions. See also [TAPI](#).

---

**K**

**key** A data object used for [encryption](#), [decryption](#), or [authentication](#).

---

**L**

**LAN** Local area network. A network residing in one location, such as a single building or campus. See also [Internet](#), [intranet](#), and [network](#).

**layer, layers** Networking models implement layers with which different protocols are associated. The most common networking model is the OSI model, which consists of the following 7 layers, in order: physical, data link, network, transport, session, presentation, and application.

**LCN** Logical channel number.

**LDAP** Lightweight Directory Access Protocol. LDAP provides management and browser applications with access to X.500 directories.

---

**M**

**mask** A 32-bit mask that shows how an [Internet](#) address is divided into network, subnet, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

**MCR** See [multicast](#).

**MC router** Multicast (MC) routers route multicast data transmissions to the hosts on each LAN in an internetwork that are registered to receive specific multimedia or other broadcasts. See also [multicast](#).

**MD5** Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and [SHA-1](#) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. [SHA-1](#) is more secure than MD4 and MD5. Cisco uses hashes for authentication within the [IPSec](#) framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. [MD5](#) has a smaller digest and is considered to be slightly faster than [SHA-1](#).

**MDI** Media dependent interface.

**MDIX** Media dependent interface crossover.

<b>Message Digest</b>	A message digest is created by a hash algorithm, such as <a href="#">MD5</a> or <a href="#">SHA-1</a> , that is used for ensuring message integrity.
<b>MGCP</b>	Media Gateway Control Protocol. Media Gateway Control Protocol is a protocol for the control of VoIP calls by external call-control elements known as media gateway controllers or call agents. MGCP merges the IPDC and <a href="#">SGCP</a> protocols.
<b>Mode</b>	See <a href="#">Access Modes</a> .
<b>Mode Config</b>	See <a href="#">IKE Mode Configuration</a> .
<b>Modular Policy Framework</b>	Modular Policy Framework. A means of configuring security appliance features in a manner to similar to Cisco IOS software Modular <a href="#">QoS</a> CLI.
<b>MS</b>	mobile station. Refers generically to any mobile device, such as a mobile handset or computer, that is used to access network services. <a href="#">GPRS</a> networks support three classes of MS, which describe the type of operation supported within the <a href="#">GPRS</a> and the <a href="#">GSM</a> mobile wireless networks. For example, a Class A MS supports simultaneous operation of <a href="#">GPRS</a> and <a href="#">GSM</a> services.
<b>MS-CHAP</b>	Microsoft <a href="#">CHAP</a> .
<b>MTU</b>	Maximum transmission unit, the maximum number of bytes in a packet that can flow efficiently across the network with best response time. For Ethernet, the default MTU is 1500 bytes, but each network can have different values, with serial connections having the smallest values. The MTU is described in RFC 1191.
<b>multicast</b>	Multicast refers to a network addressing method in which the source transmits a packet to multiple destinations, a multicast group, simultaneously. See also <a href="#">PIM</a> , <a href="#">SMR</a> .

---

<b>N</b>	
<b>N2H2</b>	A third-party, policy-oriented filtering application that works with the security appliance to control user web access. N2H2 can filter <a href="#">HTTP</a> requests based on destination host name, destination IP address, and username and password. The N2H2 corporation was acquired by Secure Computing in October, 2003.
<b>NAT</b>	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the <a href="#">Internet</a> by translating those addresses into a globally routable address space.
<b>NEM</b>	Network Extension Mode. Lets <a href="#">VPN</a> hardware clients present a single, routable network to the remote private network over the <a href="#">VPN</a> tunnel.
<b>NetBIOS</b>	Network Basic Input/Output System. A Microsoft protocol that supports Windows host name registration, session management, and data transfer. The security appliance supports NetBIOS by performing <a href="#">NAT</a> of the packets for NBNS UDP port 137 and NBDS UDP port 138.
<b>netmask</b>	See <a href="#">mask</a> .
<b>network</b>	In the context of security appliance configuration, a network is a group of computing devices that share part of an IP address space and not a single host. A network consists of multiple nodes or hosts. See also <a href="#">host</a> , <a href="#">Internet</a> , <a href="#">intranet</a> , <a href="#">IP</a> , <a href="#">LAN</a> , and <a href="#">node</a> .

<b>NMS</b>	network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
<b>node</b>	Devices such as routers and printers that would not normally be called hosts. See also <a href="#">host</a> , <a href="#">network</a> .
<b>nonvolatile storage, memory</b>	Storage or memory that, unlike RAM, retains its contents without power. Data in a nonvolatile storage device survives a power-off, power-on cycle or reboot.
<b>NSAPI</b>	Network service access point identifier. One of two components of a <a href="#">GTP</a> tunnel ID, the other component being the <a href="#">IMSI</a> . See also <a href="#">IMSI</a> .
<b>NSSA</b>	Not-so-stubby-area. An OSPF feature described by RFC 1587. NSSA was first introduced in Cisco IOS software release 11.2. It is a non-proprietary extension of the existing stub area feature that allows the injection of external routes in a limited fashion into the stub area.
<b>NTLM</b>	NT Lan Manager. A Microsoft Windows challenge-response authentication method.
<b>NTP</b>	Network time protocol.

---

**O**

<b>Oakley</b>	A key exchange protocol that defines how to acquire authenticated keying material. The basic mechanism for Oakley is the <a href="#">Diffie-Hellman</a> key exchange algorithm. Oakley is defined in RFC 2412.
<b>object grouping</b>	Simplifies access control by letting you apply access control statements to groups of network objects, such as protocol, services, hosts, and networks.
<b>OSPF</b>	Open Shortest Path First. OSPF is a routing protocol for IP networks. OSPF is a routing protocol widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. The security appliance supports OSPF.
<b>OU</b>	Organizational Unit. An X.500 directory attribute.
<b>outbound</b>	Refers to traffic whose destination is on an interface with lower security than the source interface.
<b>outbound ACL</b>	An <a href="#">ACL</a> applied to outbound traffic.
<b>outside</b>	The first interface, usually port 0, that connects to other “untrusted” networks outside the security appliance; the <a href="#">Internet</a> . See also <a href="#">interface</a> , <a href="#">interface names</a> , <a href="#">outbound</a> .

---

**P**

<b>PAC</b>	<a href="#">PPTP</a> Access Concentrator. A device attached to one or more PSTN or ISDN lines capable of <a href="#">PPP</a> operation and of handling the <a href="#">PPTP</a> protocol. The PAC need only implement TCP/IP to pass traffic to one or more <a href="#">PNSs</a> . It may also tunnel non-IP protocols.
<b>PAT</b>	See <a href="#">Dynamic PAT</a> , <a href="#">interface PAT</a> , and <a href="#">Static PAT</a> .
<b>PDP</b>	Packet Data Protocol.

<b>Perfmon</b>	The security appliance feature that gathers and reports a wide variety of feature statistics, such as connections/second, xlates/second, etc.
<b>PFS</b>	Perfect Forwarding Secrecy. PFS enhances security by using different security key for the <a href="#">IPSec</a> Phase 1 and Phase 2 <a href="#">SAs</a> . Without PFS, the same security key is used to establish <a href="#">SAs</a> in both phases. PFS ensures that a given <a href="#">IPSec SA</a> key was not derived from any other secret (like some other keys). In other words, if someone were to break a key, PFS ensures that the attacker would not be able to derive any other key. If PFS were not enabled, someone could hypothetically break the <a href="#">IKE SA</a> secret key, copy all the <a href="#">IPSec</a> protected data, and then use knowledge of the <a href="#">IKE SA</a> secret to compromise the <a href="#">IPSec SA</a> setup by this <a href="#">IKE SA</a> . With PFS, breaking <a href="#">IKE</a> would not give an attacker immediate access to <a href="#">IPSec</a> . The attacker would have to break each <a href="#">IPSec SA</a> individually.
<b>Phase 1</b>	See <a href="#">IPSec Phase 1</a> .
<b>Phase 2</b>	See <a href="#">IPSec Phase 2</a> .
<b>PIM</b>	Protocol Independent Multicast. PIM provides a scalable method for determining the best paths for distributing a specific multicast transmission to a group of hosts. Each host has registered using IGMP to receive the transmission. See also <a href="#">PIM-SM</a> .
<b>PIM-SM</b>	Protocol Independent Multicast-Sparse Mode. With PIM-SM, which is the default for Cisco routers, when the source of a multicast transmission begins broadcasting, the traffic is forwarded from one MC router to the next, until the packets reach every registered host. See also <a href="#">PIM</a> .
<b>Ping</b>	An <a href="#">ICMP</a> request sent by a host to determine if a second host is accessible.
<b>PIX</b>	Private Internet eXchange. The Cisco PIX 500-series security appliances range from compact, plug-and-play desktop models for small/home offices to carrier-class gigabit models for the most demanding enterprise and service provider environments. Cisco PIX security appliances provide robust, enterprise-class integrated network security services to create a strong multilayered defense for fast changing network environments.
<b>PKCS12</b>	A standard for the transfer of PKI-related data, such as private keys, certificates, and other data. Devices supporting this standard let administrators maintain a single set of personal identity information.
<b>PNS</b>	<a href="#">PPTP</a> Network Server. A PNS is envisioned to operate on general-purpose computing/server platforms. The PNS handles the server side of <a href="#">PPTP</a> . Because <a href="#">PPTP</a> relies completely on TCP/IP and is independent of the interface hardware, the PNS may use any combination of IP interface hardware including <a href="#">LAN</a> and <a href="#">WAN</a> devices.
<b>Policy NAT</b>	Lets you identify local traffic for address translation by specifying the source and destination addresses (or ports) in an access list.
<b>POP</b>	Post Office Protocol. Protocol that client e-mail applications use to retrieve mail from a mail server.
<b>Pool</b>	See <a href="#">IP pool</a> .
<b>Port</b>	A field in the packet headers of <a href="#">TCP</a> and <a href="#">UDP</a> protocols that identifies the higher level service which is the source or destination of the packet.
<b>PPP</b>	Point-to-Point Protocol. Developed for dial-up <a href="#">ISP</a> access using analog phone lines and modems.

<b>PPTP</b>	Point-to-Point Tunneling Protocol. PPTP was introduced by Microsoft to provide secure remote access to Windows networks; however, because it is vulnerable to attack, PPTP is commonly used only when stronger security methods are not available or are not required. PPTP Ports are pptp, 1723/tcp, 1723/udp, and pptp. For more information about PPTP, see RFC 2637. See also <a href="#">PAC</a> , <a href="#">PPTP GRE</a> , <a href="#">PPTP GRE tunnel</a> , <a href="#">PNS</a> , <a href="#">PPTP session</a> , and <a href="#">PPTP TCP</a> .
<b>PPTP GRE</b>	Version 1 of GRE for encapsulating PPP traffic.
<b>PPTP GRE tunnel</b>	A tunnel defined by a <a href="#">PNS-PAC</a> pair. The tunnel protocol is defined by a modified version of <a href="#">GRE</a> . The tunnel carries <a href="#">PPP</a> datagrams between the <a href="#">PAC</a> and the <a href="#">PNS</a> . Many sessions are multiplexed on a single tunnel. A control connection operating over <a href="#">TCP</a> controls the establishment, release, and maintenance of sessions and of the tunnel itself.
<b>PPTP session</b>	<a href="#">PPTP</a> is connection-oriented. The <a href="#">PNS</a> and <a href="#">PAC</a> maintain state for each user that is attached to a <a href="#">PAC</a> . A session is created when end-to-end <a href="#">PPP</a> connection is attempted between a dial user and the <a href="#">PNS</a> . The datagrams related to a session are sent over the tunnel between the <a href="#">PAC</a> and <a href="#">PNS</a> .
<b>PPTP TCP</b>	Standard <a href="#">TCP</a> session over which <a href="#">PPTP</a> call control and management information is passed. The control session is logically associated with, but separate from, the sessions being tunneled through a <a href="#">PPTP</a> tunnel.
<b>preshared key</b>	A preshared key provides a method of <a href="#">IKE</a> authentication that is suitable for networks with a limited, static number of <a href="#">IPSec</a> peers. This method is limited in scalability because the key must be configured for each pair of <a href="#">IPSec</a> peers. When a new <a href="#">IPSec</a> peer is added to the network, the preshared key must be configured for every <a href="#">IPSec</a> peer with which it communicates. Using <a href="#">certificates</a> and <a href="#">CAs</a> provides a more scalable method of <a href="#">IKE</a> authentication.
<b>primary, primary unit</b>	The security appliance normally operating when two units, a primary and secondary, are operating in failover mode.
<b>privileged EXEC mode</b>	Privileged EXEC mode lets you to change current settings. Any user EXEC mode command will work in privileged EXEC mode. See also <a href="#">command-specific configuration mode</a> , <a href="#">global configuration mode</a> , <a href="#">user EXEC mode</a> .
<b>protocol, protocol literals</b>	A standard that defines the exchange of packets between network nodes for communication. Protocols work together in layers. Protocols are specified in a security appliance configuration as part of defining a security policy by their literal values or port numbers. Possible security appliance protocol literal values are ahp, eigrp, esp, gre, icmp, igmp, igmp, ip, ipinip, ipsec, nos, ospf, pcp, snp, tcp, and udp.
<b>Proxy-ARP</b>	Enables the security appliance to reply to an <a href="#">ARP</a> request for IP addresses in the global pool. See also <a href="#">ARP</a> .
<b>public key</b>	A public key is one of a pair of keys that are generated by devices involved in public key infrastructure. Data encrypted with a public key can only be decrypted using the associated private key. When a private key is used to produce a digital signature, the receiver can use the public key of the sender to verify that the message was signed by the sender. These characteristics of key pairs provide a scalable and secure method of authentication over an insecure media, such as the <a href="#">Internet</a> .



---

**Q**

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

---

**R**

**RA** Registration Authority. An authorized proxy for a [CA](#). RAs can perform certificate enrollment and can issue [CRLs](#). See also [CA](#), [certificate](#), [public key](#).

**RADIUS** Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. RFC 2058 and RFC 2059 define the RADIUS protocol standard. See also [AAA](#) and [TACACS+](#).

**Refresh** Retrieve the running configuration from the security appliance and update the screen. The icon and the button perform the same function.

**registration authority** See [RA](#).

**replay-detection** A security service where the receiver can reject old or duplicate packets 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](#).

**RFC** Request for Comments. RFC documents define protocols and standards for communications over the [Internet](#). RFCs are developed and published by [IETF](#).

**RIP** Routing Information Protocol. Interior gateway protocol (IGP) supplied with UNIX BSD systems. The most common IGP in the [Internet](#). RIP uses hop count as a routing metric.

**RLLA** Reserved Link Local Address. Multicast addresses range from 224.0.0.0 to 239.255.255.255, however only the range 224.0.1.0 to 239.255.255.255 is available to us. The first part of the multicast address range, 224.0.0.0 to 224.0.0.255, is reserved and referred to as the RLLA. These addresses are unavailable. We can exclude the RLLA range by specifying: 224.0.1.0 to 239.255.255.255. 224.0.0.0 to 239.255.255.255 excluding 224.0.0.0 to 224.0.0.255. This is the same as specifying: 224.0.1.0 to 239.255.255.255.

**route, routing** The path through a [network](#).

**routed firewall mode** In routed firewall mode, the security appliance is counted as a router hop in the network. It performs [NAT](#) between connected networks and can use [OSPF](#) or [RIP](#). See also [transparent firewall mode](#).

**RPC** Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the clients.

<b>RSA</b>	A <a href="#">public key</a> cryptographic algorithm (named after its inventors, Rivest, Shamir, and Adelman) with a variable key length. The main weakness of RSA is that it is significantly slow to compute compared to popular secret-key algorithms, such as <a href="#">DES</a> . The Cisco implementation of <a href="#">IKE</a> uses a <a href="#">Diffie-Hellman</a> exchange to get the secret keys. This exchange can be authenticated with RSA (or preshared keys). With the <a href="#">Diffie-Hellman</a> exchange, the <a href="#">DES</a> 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.
<b>RSH</b>	Remote Shell. A protocol that allows a user to execute commands on a remote system without having to log in to the system. For example, RSH can be used to remotely examine the status of a number of access servers without connecting to each communication server, executing the command, and then disconnecting from the communication server.
<b>RTCP</b>	RTP Control Protocol. Protocol that monitors the <a href="#">QoS</a> of an IPv6 <a href="#">RTP</a> connection and conveys information about the on-going session. See also <a href="#">RTP</a> .
<b>RTP</b>	Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.
<b>RTSP</b>	Real Time Streaming Protocol. Enables the controlled delivery of real-time data, such as audio and video. RTSP is designed to work with established protocols, such as <a href="#">RTP</a> and <a href="#">HTTP</a> .
<b>rule</b>	Conditional statements added to the security appliance configuration to define security policy for a particular situation. See also <a href="#">ACE</a> , <a href="#">ACL</a> , <a href="#">NAT</a> .
<b>running configuration</b>	The configuration currently running in RAM on the security appliance. The configuration that determines the operational characteristics of the security appliance.

---

## S

<b>SA</b>	security association. An instance of security policy and keying material applied to a data flow. SAs are established in pairs by <a href="#">IPSec</a> peers during both phases of <a href="#">IPSec</a> . SAs specify the encryption algorithms and other security parameters used to create a secure tunnel. Phase 1 SAs ( <a href="#">IKE</a> SAs) establish a secure tunnel for negotiating Phase 2 SAs. Phase 2 SAs ( <a href="#">IPSec</a> SAs) establish the secure tunnel used for sending user data. Both <a href="#">IKE</a> and <a href="#">IPSec</a> use SAs, although SAs are independent of one another. <a href="#">IPSec</a> SAs are unidirectional and they are unique in each security protocol. 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 <a href="#">ESP</a> between peers, one <a href="#">ESP</a> SA is required for each direction. SAs are uniquely identified by destination ( <a href="#">IPSec</a> endpoint) address, security protocol ( <a href="#">AH</a> or <a href="#">ESP</a> ), and Security Parameter Index. <a href="#">IKE</a> negotiates and establishes SAs on behalf of <a href="#">IPSec</a> . A user can also establish <a href="#">IPSec</a> SAs manually. An <a href="#">IKE</a> SA is used by <a href="#">IKE</a> only, and unlike the <a href="#">IPSec</a> SA, it is bidirectional.
<b>SCCP</b>	Skinny Client Control Protocol. A Cisco-proprietary protocol used between Cisco Call Manager and Cisco <a href="#">VoIP</a> phones.
<b>SCEP</b>	Simple Certificate Enrollment Protocol. A method of requesting and receiving (also known as enrolling) certificates from <a href="#">CAs</a> .

<b>SDP</b>	Session Definition Protocol. An <a href="#">IETF</a> protocol for the definition of Multimedia Services. SDP messages can be part of <a href="#">SGCP</a> and <a href="#">MGCP</a> messages.
<b>secondary unit</b>	The backup security appliance when two are operating in failover mode.
<b>secret key</b>	A secret key is a key shared only between the sender and receiver. See <a href="#">key</a> , <a href="#">public key</a> .
<b>security context</b>	You can partition a single security appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple stand-alone firewalls.
<b>security services</b>	See <a href="#">cryptography</a> .
<b>serial transmission</b>	A method of data transmission in which the bits of a data character are transmitted sequentially over a single channel.
<b>SGCP</b>	Simple Gateway Control Protocol. Controls <a href="#">VoIP</a> gateways by an external call control element (called a call-agent).
<b>SGSN</b>	Serving GPRS Support Node. The SGSN ensures mobility management, session management and packet relaying functions.
<b>SHA-1</b>	Secure Hash Algorithm 1. SHA-1 [NIS94c] is a revision to SHA that was published in 1994. SHA is closely modeled after MD4 and produces a 160-bit digest. Because SHA produces a 160-bit digest, it is more resistant to brute-force attacks than 128-bit hashes (such as <a href="#">MD5</a> ), but it is slower. Secure Hash Algorithm 1 is a joint creation of the National Institute of Standards and Technology and the National Security Agency. This algorithm, like other hash algorithms, is used to generate a hash value, also known as a message digest, that acts like a <a href="#">CRC</a> used in lower-layer protocols to ensure that message contents are not changed during transmission. SHA-1 is generally considered more secure than <a href="#">MD5</a> .
<b>SIP</b>	Session Initiation Protocol. Enables call handling sessions, particularly two-party audio conferences, or “calls.” SIP works with <a href="#">SDP</a> for call signaling. <a href="#">SDP</a> specifies the ports for the media stream. Using SIP, the security appliance can support any SIP <a href="#">VoIP</a> gateways and <a href="#">VoIP</a> proxy servers.
<b>site-to-site VPN</b>	A site-to-site <a href="#">VPN</a> is established between two <a href="#">IPSec</a> peers that connect remote networks into a single <a href="#">VPN</a> . In this type of <a href="#">VPN</a> , neither <a href="#">IPSec</a> peer is the destination or source of user traffic. Instead, each <a href="#">IPSec</a> peer provides encryption and authentication services for hosts on the <a href="#">LAN</a> s connected to each <a href="#">IPSec</a> peer. The hosts on each <a href="#">LAN</a> send and receive data through the secure tunnel established by the pair of <a href="#">IPSec</a> peers.
<b>SKEME</b>	A key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.
<b>SMR</b>	Stub Multicast Routing. SMR allows the security appliance to function as a “stub router.” A stub router is a device that acts as an <a href="#">IGMP</a> proxy agent. <a href="#">IGMP</a> is used to dynamically register specific hosts in a multicast group on a particular <a href="#">LAN</a> with a multicast router. Multicast routers route multicast data transmissions to hosts that are registered to receive specific multimedia or other broadcasts. A stub router forwards <a href="#">IGMP</a> messages between hosts and <a href="#">MC routers</a> .
<b>SMTP</b>	Simple Mail Transfer Protocol. SMTP is an Internet protocol that supports email services.
<b>SNMP</b>	Simple Network Management Protocol. A standard method for managing network devices using data structures called Management Information Bases.

<b>split tunneling</b>	Allows a remote <a href="#">VPN</a> client simultaneous encrypted access to a private network and clear unencrypted access to the <a href="#">Internet</a> . If you do not enable split tunneling, all traffic between the <a href="#">VPN</a> client and the security appliance is sent through an <a href="#">IPSec</a> tunnel. All traffic originating from the <a href="#">VPN</a> client is sent to the outside interface through a tunnel, and client access to the <a href="#">Internet</a> from its remote site is denied.
<b>spoofing</b>	A type of attack designed to foil network security mechanisms such as filters and access lists. A spoofing attack sends a packet that claims to be from an address from which it was not actually sent.
<b>SQL*Net</b>	Structured Query Language Protocol. An Oracle protocol used to communicate between client and server processes.
<b>SSH</b>	Secure Shell. An application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities.
<b>SSL</b>	Secure Sockets Layer. A protocol that resides between the application layer and TCP/IP to provide transparent encryption of data traffic.
<b>standby unit</b>	See <a href="#">secondary unit</a> .
<b>stateful inspection</b>	Network protocols maintain certain data, called state information, at each end of a network connection between two hosts. State information is necessary to implement the features of a protocol, such as guaranteed packet delivery, data sequencing, flow control, and transaction or session IDs. Some of the protocol state information is sent in each packet while each protocol is being used. For example, a browser connected to a web server uses <a href="#">HTTP</a> and supporting TCP/IP protocols. Each protocol layer maintains state information in the packets it sends and receives. The security appliance and some other firewalls inspect the state information in each packet to verify that it is current and valid for every protocol it contains. This is called stateful inspection and is designed to create a powerful barrier to certain types of computer security threats.
<b>Static PAT</b>	Static Port Address Translation. Static PAT is a static address that also maps a local port to a global port. See also <a href="#">Dynamic PAT</a> , <a href="#">NAT</a> .
<b>subnetmask</b>	See <a href="#">mask</a> .

---

## T

<b>TACACS+</b>	Terminal Access Controller Access Control System Plus. A client-server protocol that supports <a href="#">AAA</a> services, including command authorization. See also <a href="#">AAA</a> , <a href="#">RADIUS</a> .
<b>TAPI</b>	Telephony Application Programming Interface. A programming interface in Microsoft Windows that supports telephony functions.
<b>TCP</b>	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.

<b>TCP Intercept</b>	With the TCP intercept feature, once the optional embryonic connection limit is reached, and until the embryonic connection count falls below this threshold, every SYN bound for the effected server is intercepted. For each SYN, the security appliance responds on behalf of the server with an empty SYN/ACK segment. The security appliance retains pertinent state information, drops the packet, and waits for the client acknowledgment. If the ACK is received, then a copy of the client SYN segment is sent to the server and the <a href="#">TCP</a> three-way handshake is performed between the security appliance and the server. If this three-way handshake completes, may the connection resume as normal. If the client does not respond during any part of the connection phase, then the security appliance retransmits the necessary segment using exponential back-offs.
<b>TDP</b>	Tag Distribution Protocol. TDP is used by tag switching devices to distribute, request, and release tag binding information for multiple network layer protocols in a tag switching network. TDP does not replace routing protocols. Instead, it uses information learned from routing protocols to create tag bindings. TDP is also used to open, monitor, and close TDP sessions and to indicate errors that occur during those sessions. TDP operates over a connection-oriented transport layer protocol with guaranteed sequential delivery (such as <a href="#">TCP</a> ). The use of TDP does not preclude the use of other mechanisms to distribute tag binding information, such as piggybacking information on other protocols.
<b>Telnet</b>	A terminal emulation protocol for TCP/IP networks such as the <a href="#">Internet</a> . Telnet is a common way to control web servers remotely; however, its security vulnerabilities have led to its replacement by <a href="#">SSH</a> .
<b>TFTP</b>	Trivial File Transfer Protocol. TFTP is a simple protocol used to transfer files. It runs on UDP and is explained in depth in RFC 1350.
<b>TID</b>	Tunnel Identifier.
<b>TLS</b>	Transport Layer Security. A future IETF protocol to replace <a href="#">SSL</a> .
<b>traffic policing</b>	The traffic policing feature ensures that no traffic exceeds the maximum rate (bits per second) that you configure, thus ensuring that no one traffic flow can take over the entire resource.
<b>transform set</b>	See <a href="#">IPSec transform set</a> .
<b>translate, translation</b>	See <a href="#">xlate</a> .
<b>transparent firewall mode</b>	A mode in which the security appliance is not a router hop. You can use transparent firewall mode to simplify your network configuration or to make the security appliance invisible to attackers. You can also use transparent firewall mode to allow traffic through that would otherwise be blocked in <a href="#">routed firewall mode</a> . See also <a href="#">routed firewall mode</a> .
<b>transport mode</b>	An <a href="#">IPSec</a> encryption mode that encrypts only the data portion (payload) of each packet, but leaves the header untouched. Transport mode is less secure than tunnel mode.
<b>TSP</b>	TAPI Service Provider. See also <a href="#">TAPI</a> .
<b>tunnel mode</b>	An <a href="#">IPSec</a> encryption mode that encrypts both the header and data portion (payload) of each packet. Tunnel mode is more secure than transport mode.

<b>tunnel</b>	A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote <a href="#">VPN</a> client have encrypted access to a private network.
<b>Turbo ACL</b>	Increases <a href="#">ACL</a> lookup speeds by compiling them into a set of lookup tables. Packet headers are used to access the tables in a small, fixed number of lookups, independent of the existing number of <a href="#">ACL</a> entries.

---

## U

<b>UDP</b>	User Datagram Protocol. A connectionless transport layer protocol in the IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, which requires other protocols to handle error processing and retransmission. UDP is defined in RFC 768.
<b>UMTS</b>	Universal Mobile Telecommunication System. An extension of <a href="#">GPRS</a> networks that moves toward an all-IP network by delivering broadband information, including commerce and entertainment services, to mobile users via fixed, wireless, and satellite networks
<b>Unicast RPF</b>	Unicast Reverse Path Forwarding. Unicast RPF guards against spoofing by ensuring that packets have a source IP address that matches the correct source interface according to the routing table.
<b>URL</b>	Uniform Resource Locator. A standardized addressing scheme for accessing hypertext documents and other services using a browser. For example, <a href="http://www.cisco.com">http://www.cisco.com</a> .
<b>user EXEC mode</b>	User EXEC mode lets you to see the security appliance settings. The user EXEC mode prompt appears as follows when you first access the security appliance. See also <a href="#">command-specific configuration mode</a> , <a href="#">global configuration mode</a> , and <a href="#">privileged EXEC mode</a> .
<b>UTC</b>	Coordinated Universal Time. The time zone at zero degrees longitude, previously called Greenwich Mean Time (GMT) and Zulu time. UTC replaced GMT in 1967 as the world time standard. UTC is based on an atomic time scale rather than an astronomical time scale.
<b>UTRAN</b>	Universal Terrestrial Radio Access Network. Networking protocol used for implementing wireless networks in UMTS. GTP allows multi-protocol packets to be tunneled through a UMTS/GPRS backbone between a <a href="#">GGSN</a> , an <a href="#">SGSN</a> and the <a href="#">UTRAN</a> .
<b>UUIE</b>	User-User Information Element. An element of an <a href="#">H.225</a> packet that identifies the users implicated in the message.

---

## V

<b>VLAN</b>	Virtual <a href="#">LAN</a> . A group of devices on one or more <a href="#">LANs</a> that are configured (using management software) so that they can communicate as if they were attached to the same physical network cable, when in fact they are located on a number of different <a href="#">LAN</a> segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
<b>VoIP</b>	Voice over IP. VoIP carries normal voice traffic, such as telephone calls and faxes, over an IP-based network. DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification <a href="#">H.323</a> .

**VPN** Virtual Private Network. A network connection between two peers over the public network that is made private by strict authentication of users and the encryption of all data traffic. You can establish VPNs between clients, such as PCs, or a [headend](#), such as the security appliance.

**virtual firewall** See [security context](#).

**VSA** Vendor-specific attribute. An attribute in a [RADIUS](#) packet that is defined by a vendor rather than by [RADIUS](#) RFCs. The [RADIUS](#) protocol uses IANA-assigned vendor numbers to help identify VSAs. This lets different vendors have VSAs of the same number. The combination of a vendor number and a VSA number makes a VSA unique. For example, the cisco-av-pair VSA is attribute 1 in the set of VSAs related to vendor number 9. Each vendor can define up to 256 VSAs. A [RADIUS](#) packet contains any VSAs attribute 26, named Vendor-specific. VSAs are sometimes referred to as subattributes.

---

## W

**WAN** wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers.

**WCCP** Web Cache Communication Protocol. Transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.

**Websense** A content filtering solution that manages employee access to the [Internet](#). Websense uses a policy engine and a [URL](#) database to control user access to websites.

**WEP** Wired Equivalent Privacy. A security protocol for wireless [LANs](#), defined in the IEEE 802.11b standard.

**WINS** Windows Internet Naming Service. A Windows system that determines the IP address associated with a particular network device, also known as “name resolution.” WINS uses a distributed database that is automatically updated with the [NetBIOS](#) names of network devices currently available and the IP address assigned to each one. WINS provides a distributed database for registering and querying dynamic [NetBIOS](#) names to IP address mapping in a routed network environment. It is the best choice for [NetBIOS](#) name resolution in such a routed network because it is designed to solve the problems that occur with name resolution in complex networks.

---

## X

**X.509** A widely used standard for defining digital certificates. X.509 is actually an ITU recommendation, which means that it has not yet been officially defined or approved for standardized usage.

**xauth** See [IKE Extended Authentication](#).

**xlate** An xlate, also referred to as a translation entry, represents the mapping of one IP address to another, or the mapping of one IP address/port pair to another.