CRS Glossary

A

AAA	Authentication, Authorization, Accounting. Allows all facets of user security to be defined on a central server.
ABEND	Abnormal END. Abnormal termination of software.
Access	1.) In dealing with network security it is an all-encompassing term that refers to unauthorized data manipulation, system access, or privileged escalation.
Access attacks	An all-encompassing term that refers to unauthorized data manipulation, system access, or privileged escalation. Unauthorized data retrieval is simply reading, writing, copying, or moving files that are not intended to be accessible to the intruder.
access control	Limiting the flow of information from the resources of a system to only the authorized persons or systems in the network.
Access Control Entry	See ACE.
access control list	See ACL.
access device	Hardware component used in your signaling controller system: access server or mux.
access layer	The point at which local end users are allowed into the network.
Access Method	1.) Generally, the way in which network devices access the network medium. 2.) Software within an SNA processor that controls the flow of information through a network.
access policy	Defines access rights and privileges for the network users. The access policy should provide guidelines for connecting external networks, connecting devices to a network, and adding new software to systems.
Access Provider	The remote computer system which connects a personal computer to the Internet.
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.
accounting	The action of recording what a user is doing or has done. See also auditing.
ACE	An entry in an access-control list (ACL) that contains a set of access rights and a security identifier (SID) that identifies who is allowed, denied, or audited.
ACF	Advanced Communications Function. A group of SNA products that provides distributed processing and resource sharing.
ACK packets	See acknowledgement.
acknowledgement	Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) occurred. Sometimes abbreviated ACK.
ACL	List kept by routers to control access to or from the router for a number of services. Can be used for security purposes by denying entry to a host accessing the network with a certain IP address, through a certain port, or through other upper layer protocols.
ACS	Allows an administrator to control who can access the network, authorize what types of network services and network access each per user or group, and keep an accounting record of all user actions in the network.
Action	An action is a component of a security policy that resolves a condition. It is a terminal node in a condition branch. The firewall will enforce a specific action against any session requests that satisfy the condition branch leading to that action. Only two actions exist: ACCEPT and REJECT.

Active Hub	Multiported device that amplifies LAN transmission signals.
Active port monitor	A type of monitoring supported by the Switched Port Analyzer (SPAN) that allows you to monitor traffic using a customer-supplied monitoring device, such as an RMON probe, or a trace tool, such as a Network General Sniffer. The trace tool monitors only the LLC traffic that is switched by the monitored port. The MAC frames are not monitored. See also SPAN.
ActiveX	Formerly known as Object Linking and Embedding (OLE) or Object Linking and Embedding control (OCX). Applets that can be inserted in web pages—often used in animations—or in other applications. ActiveX controls create a potential security problem because they can provide a way for someone to attack servers.
adaptive cut-through switching	A switching feature that alternates between cut-through and store-and-forward switching modes based on preset, user-defined error thresholds to optimize performance while providing protection from network errors.
address	Data structure or logical convention used to identify a unique entity, such as a particular process or network device.
Address classes	Predefined groupings of Internet addresses, with each class defining networks of a certain size. The range of numbers that can be assigned for the first octet in the IP address is based on the address class. Class A networks (values 1-126) are the largest, with over 16 million hosts per network. Class B networks (128-191) have up to 65,534 hosts per network, and Class C networks (192-223) can have up to 254 hosts per network. See also octet.
Address Harvester	A robot that searches the internet looking for valid e-mail addresses, usually for compiling address lists for spam. See also spam.
Address hiding	The process of converting between IP addresses used within an intranet or other private network (called a subdomain) and Internet IP addresses (or external IP addresses on a PEP). This makes it possible for internal networks to use a large number of addresses without depleting the limited number of available Internet IP addresses assigned to the external network.
address mask	Bit combination used to describe which portion of an address refers to the network or subnet and which part refers to the host. Sometimes referred to simply as mask. See also subnet mask.
Administrative Model	The model by which a system is administered. It specifies the abilities of the system to separate administrative actions into different administrative roles. An administrative model is made up of nodes (taken from graph theory), where each node has administrative actions associated with it and those nodes may differ. See also hierarchical administrative model and strict adherence administrative model.
admission concrol	See traffic policing.
AES	Advanced Encryption Standard.
Agent	The fundamental building blocks of the firewall. Agents are designed to perform a specific task or collection of tasks. They provide specific services to other agents within the system.
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).
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 transform	A mechanism for payload authentication.
Airplane rule	The rule in software and hardware that simplicity increases robustness, such that complexity increases the chances of a failure.
alarm	Message notifying an operator or administrator of a network problem. See also event and trap.
Alderson loop	A version of an infinite loop where an exit condition is available but not accessible.

Anonymous FTP	The File Transfer Protocol (FTP) can be set up for anonymous access. Anonymous ftp allows any user on the network who does not have access to an account on your computer to access its files and databases using the account named "anonymous". See also FTP.
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.
Applet	Refers specifically to a Java-based program that requires a just-in-time compiler to operate correctly. Generically, an applet is a component of an application (e.g., the control panel is an application, all of the things in the control panel are applets.)
AppleTalk Remote Access	See ARA.
application layer	Layer 7 of the OSI reference model. This layer provides services to application processes (such as electronic mail, file transfer, and terminal emulation) that are outside of the OSI model. The application layer identifies and establishes the availability of intended communication partners (and the resources required to connect with them), synchronizes cooperating applications, and establishes agreement on procedures for error recovery and control of data integrity.
application layer	Layer 7 of the OSI reference model. This layer provides services to application processes (such as e-mail, file transfer, and terminal emulation) that are outside of the OSI model. The application layer identifies and establishes the availability of intended communication partners (and the resources required to connect with them), synchronizes cooperating applications, and establishes agreement on procedures for error recovery and control of data integrity.
Application Layer Firewall	An application layer firewall is a third-generation firewall technology that evaluates network packets for valid data at the application layer before allowing a connection. It examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. In addition, an application layer firewall can validate other security items that only appear within the application layer, such as user passwords and service requests. Most application layer firewalls include specialized application software and proxy services. See also proxy services.
Application Proxy	The combination of a client proxy and a server proxy that both reside on an application layer firewall. See also proxy server and proxy client.
Application Service Provider	See ASP.
ARA	
Archie	A software utility for searching through millions of files on the internet and finding a specific one. The software's database is made up of names and the more specific your request the more likely you are to find the file.
Architecture	The design and structure of specific components of a computer system and how they connect and interact with one another.
ARP	Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.
ARPANET	Developed in the 1970's and funded by the Advanced Research Projects Agency, ARPANET is the network for which TCP/IP was originally developed. It is primarily used for military research and communications. See also DoD Internet.
ASA	Adaptive Security Algorithm.
ASCII	American Standard Code for Information Interchange. 8-bit code for character representation (7 bits plus parity).
ASN.1	H.323 protocol. See H.323.
ASP	
Asynchronous Communications Server	See ACS.

Asynchronous transmission	Term describing digital signals that are transmitted without precise clocking. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and end of each character.
Attachments	A file that is attached to an e-mail message as a "rider" which is not seen in the written text but is displayed in the Attached field of the header.
attribute-value pair	A generic pair of values passed from a AAA server to a AAA client. For example, in the AV pair user = bill, "user" is the attribute and "bill" is the value.
Audit Event	An action that causes an audit record to be recorded in the Windows NT Event Log.
Audit Policy	Defines the types of events that will be recorded for the purpose of improving security.
Audit Record	The information recorded in the Windows NT event log that describes an audit event including the user's ID, time of the event, session identifier, local port number, and other identifying information.
Audit Trail	Also referred to as audit logs, audit trails provide a method of accountability within a network application. It identifies who performed what tasks and when they did it. Audit events and audit records are instrumental to providing thorough audit trails. The more events that cause audit records to be recorded as well as the better the detail provided by an audit record, then the better the audit trail.
Auditing	Tracking activities of users by recording selected types of events in the security log of a server or workstation.
AUP	Acceptable Use Policy. A written agreement outlining terms of use of the Internet for parents, teachers, and students at the school.
Authentication	Gives access to authorized users only (for example, using one-time passwords).
Autonomous Agent	An autonomous agent implies that it does not communicate directly with any other agent. Instead, an agent communicates only with the Security Knowledge Base. Agents communicate with each other indirectly by writing into and reading from the Security Knowledge Base data store. Agents only interact with the Security Knowledge Base. Because all interactions are well understood, this knowledge isolation facilitates rapid subsystem development. In addition, it lessens integration errors by isolating an agent's constraints. See also fixed agent and mobile agent.
Availability	High availability is defined as the continuous operation of computing systems. Applications require differing availability levels depending on the business impact of down time. For an application to be available, all components-including application and database servers, storage devices, and the end-to-end network-must provide continuous service.

B

Back door	A hole deliberately left in a system by the designers intended for use by service technicians.
Back Orifice	A program that can give unwanted access and control of a system by way of its Internet link. It runs on Windows 95/98 systems.
Backup Domain Controller	See BDC.
BAD	Broken As Designed. In hacker terms, a program that is "bogus" not because of bugs but because of bad design and misfeatures.
bagbiter	In hacker terms, a computer or program that does not work in an acceptable manner.
bandwidth	The amount of information that a computer or transmission medium can hande in a unit of time.

Bastion Host	A bastion host is a computer that is critical to enforcing your organization's network security policy. Bastion hosts must be highly secured as they are vulnerable to attacks due to the fact that they are exposed to untrusted or unknown networks and are main points of contact for users of trusted networks. Often, bastion hosts provide services to external users, such as Web services and public access systems. Because these computers are very likely to be attacked, they are often referred to as sacrificial hosts.
BBS	Bulletin Board System. A database of messages where people can leave broadcast messages for others grouped into "topic groups". In other words, an electronic bulletin board.
BDC	Backup Domain Controller. In a Windows NT Server domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the primary domain controller (PDC). BDCs also authenticate user's logons and can be promoted to function as PDCs as needed. Multiple BDCs can exist on a domain. See also primary domain controller.
BGP	Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems.
big-endian	A computer architecture where the most significant byte has the lowest address (big-end-first). Also called "network order".
BIND	Berkeley Internet Name Domain. Implementation of DNS developed and distributed by the University of California at Berkeley (United States). Many Internet hosts run BIND, which is the ancestor of many commercial BIND implementations.
bit bucket	The "place" where lost, discarded, or destroyed data is sent.
BOOTP	Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.
Break-in	A successful intrusion or attack on a computer that resides on your network.
Breidbart Index	Invented by the long-time hacker Seth Breidbart, a measurement of the severity of spam messages. See also spam attack.
Bridge	A device used at the data link layer that selectively copies packets between networks of the same type.
broadcast storm	In hacker usage, a packet that causes other hosts to respond all at once, typically with packets that cause the process to start over again.
brute force	A programming style that relies on the computer's processing power to simplify a problem.
bug	An unwanted and unintended property of a program that often causes it to malfunction.

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.
CA Interoperability	CA interoperability permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA with SCEP provides manageability and scalability for IPSec.
CBAC	Context-based Access Control. Protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC enhances security by scrutinizing both source and destination addresses and by tracking each application's connection status.

CBC	Cipher Block Chaining. A component that requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
CCO	Provides online access to glossaries of networking terminology and acronyms translated into 28 languages and regional dialects.
CDP	Cisco Discovery Protocol. Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.
CEF	Cisco Express Forwarding. An advanced Layer 3 IP switching technology designed for high-performance, highly resilient Layer 3 IP backbone switching. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications or interactive sessions.
Central Processing Unit	See CPU.
CEP	Certificate Enrollment Protocol. See SCEP.
CERT	Computer Emergency Response Team. Chartered to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. The U.S. CERT is based at Carnegie Mellon University in Pittsburgh (United States), Regional CERTs are, like NICs, springing up in different parts of the world.
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).
CET	
CHAP	Challenge Handshake Authentication Protocol. A PPP cryptographic challenge/response authentication protocol in which the cleartext password is not passed over the line. CHAP allows the secure exchange of a shared secret between the two endpoints of a connection.
chargen attack	Establishes a connection between UDP services, producing a high character output. The host chargen service is connected to the echo service on the same or different systems, which causes congestion on the network with echoed chargen traffic.
ciphertext	Encrypting plaintext, results in unreadable data.
Circuit Level Firewall	A circuit level firewall is a second-generation firewall technology which validates the fact that a packet is either a connection request, or a data packet belonging to a connection, or virtual circuit, between two peer transport layers.
Cisco Connection Online	See CCO.
Cisco Encryption Technology	See CET.
Cisco IOS Firewall	A security-specific option for Cisco IOS software. It integrates robust firewall functionality, authentication proxy, and intrusion detection for every network perimeter, and enriches existing Cisco IOS security capabilities. It adds greater depth and flexibility to existing Cisco IOS security solutions, such as authentication, encryption, and failover, by delivering state-of-the-art security features such as stateful, application-based filtering; dynamic per-user authentication and authorization; defense against network attacks; Java blocking; and real-time alerts.
Cisco Secure Intrusion Detection System.	See CSIDS.

Cisco Secure PIX Firewall	Offers a VPN gateway alternative when the security group “owns” the VPN.
Cisco Secure Policy Manager	See CSPM.
Cisco Secure Scanner	Identifies the security posture of the network with respect to the security procedures that form the hub of the Security Wheel.
Cisco Secure VPN client	The VPN client enables secure remote access to Cisco router and PIX Firewalls and runs on the Windows operating system.
Cisco Systems TAC	
Cisco VPN Concentrator series	Offers powerful remote access and site-to-site VPN capability, easy-to-use management interface, and a VPN client.
Cisco VPN routers	Use Cisco IOS software IPSec support to enable a secure VPN. VPN optimized routers leverage existing Cisco investment; perfect for the hybrid WAN.
cleartext	Data that can be read and understood without any special tools.
CLI	command line interface. Interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CLID	Calling Line Identification. A unique number that informs the called party of the phone number of the calling party.
Client	1.) A system that uses NIS, NFS, or other services provided by another system. Web browsers, such as Netscape Navigator and Microsoft Internet Explorer, are also clients for Web servers. 2.) A node or software program (front-end device) that requests services from a server.
Client Application	A networked application that requests network services directly from a server application.
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.
Client Server	A program that has a client application and a server application. The server application presents network or information services to a client application upon request.
cloning	Creating and configuring a virtual access interface by applying a specific virtual template interface. The template is the source of the generic user and router-dependent information. The result of cloning is a virtual access interface configured with all the commands in the template.
cloud	Clouds are time-saving features in CSPM. You can define an entire subnet as a cloud, and apply policy to its outside interface, just as if it were a single host. This saves time by allowing you to treat a multitude of hosts as a single entity.
Command Line Interface	See CLI.
Compression	The running of a data set through an algorithm that reduces the space required to store or the bandwidth required to transmit the data set
Computer Emergency Response Team	See CERT.
Computer Security Institute	See CSI.
Condition	A comparative test between user-defined values and the actual values of a session request. See also condition branch.

Condition Branch	A condition branch is one or more conditions terminated by two terminal nodes. Depending on whether the session request parameters satisfy the condition, the request is either accepted, rejected, processed by the next condition branch, or passed up to the next security policy for evaluation to find a condition that more closely matches the parameters of a particular session request.
Conduit	A pathway through a firewall or other security device.
Confidentiality	Confidentiality is the protection of data from unauthorized disclosure to a third party. Whether it is customer data or internal company data, a business is responsible for protecting the privacy of its data.
Configuration mode	This mode displays the (config)# prompt and enables you to change system configurations. All privileged, unprivileged, and configuration commands work in this mode. Applicable to both Cisco routers and PIX Firewalls.
control messages	Exchange messages between the NAS and home gateway pairs, operating in-band within the tunnel protocol. Control messages govern the aspects of the tunnel and sessions within the tunnel.
Controlled Host	Controlled hosts are computers that are the object of the activities of the agents. These hosts are controlled by decisions made by other agents. Computers executing product instances are examples of controlled hosts. Generally, fixed agents run on controlled hosts. See also controlling host.
Controlling Host	Controlling hosts are computers that run agents, but are not directly affected by the actions of the agents. Computers that run the administration agent are examples of controlling hosts. Generally mobile agents execute on controlling hosts. See also controlled host.
core layer	A high-speed switching backbone that is designed to switch packets as fast as possible.
CPU	Central Processing Unit.
CPU hogging	Programs such as Trojan horses or viruses that tie up CPU cycles, memory, or other resources, denying computer resources to legitimate users.
Cracker	Someone who breaks through the security on a system. A term used by hackers to describe themselves.
cracking	Generally, the act of breaching a security system with malicious intent.
CRC	cyclic redundancy check. Packets that contain corrupted data (checksum error).
CRL	Certificate Revocation List. A method of certificate revocation. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPSec peers on a regular periodic basis (for example, hourly, daily, or weekly). Each revoked certificate is identified in a CRL by its certificate serial number. When a participating peer device uses a certificate, that system not only checks the certificate signature and validity but also acquires a most recently issued CRL and checks that the certificate serial number is not on that CRL.
Crypto access lists	Traffic selection access lists that are used to define which IP traffic is interesting and will be protected by IPSec and which traffic will not be protected by IPSec.
Crypto ACL	Used to define which IP traffic is or is not protected by IPSec.
crypto map	A command that filters traffic to be protected and defines the policy to be applied to that traffic.
cryptography	The mathematical science that deals with transforming data to render its meaning unintelligible (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form. *(RFC 2828)*
CSACS	Cisco Secure Asynchronous Communications Server. See ACS.
CSCS team	Cisco Secure Consulting Services team. A team of white-hat hackers whose mission is to discover vulnerabilities in their clients' networks and recommend ways to secure them
CSI	Computer Security Institute. A company dedicated to serving and training the information, computer and network security professional.

CSIDS	Cisco Secure Intrusion Detection System. Detects security violations in real time and can be configured to automatically respond before any damage is done by an intruder.
CSIS	Cisco Secure Integrated Software. See Cisco IOS Firewall.
CSPM	A scalable, powerful security policy management system for Cisco firewalls and Virtual Private Network (VPN) gateways.
CSPM Topology Wizard	Automatically discovers the interfaces and settings of a managed device.
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.
Cut-Through Proxy	Transparently verifies user identity. The user is challenged first at the application layer. After successful authentication, the session is shifted to a lower layer for better performance.
CWI	Catalyst Web Interface. A browser-based tool that you can use to configure the Catalyst 6000, 5000, and 4000 Family Switches. It consists of a graphical user interface (GUI) that runs on the client, Catalyst CV 5.0 (Catalyst version of CiscoView 5.0), and an HTTP server that runs on the switch.

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 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.
Daemon	In UNIX, a server program. The term is from the Old English daemon meaning deified being, not demon meaning evil spirit.
DARPANET	The network used/created by the Department of Defense's Advanced Research Projects Agency.
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).
Data Encryption Standard	See DES.
data flow	A grouping of traffic, identified by a combination of source address/netmask, destination address/netmask, IP next protocol field, and source and destination ports, where the protocol and port fields can have the values of any. In effect, all traffic matching a specific combination of these values is logically grouped together into a data flow. A data flow can represent a single TCP connection between two hosts, or it can represent all traffic between two subnets. IPSec protection is applied to data flows.
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 Link Layer	Layer 2 of the OSI reference model. Provides reliable transit of data across a physical link. The data-link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE divided this layer into two sublayers: the MAC sublayer and the LLC sublayer. Sometimes simply called link layer.
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.

Data Privacy Directives	Passed by the European Union in 1998 concerning privacy issues, they provide consumers with strong control over their personal data.
Datagram	1.) Non-sequenced, self-contained network transmission unit at the IP level. The datagram is the fundamental unit for IP and UDP. 2.) A packet of data and other delivery information that is routed through a packet-switched network or transmitted on a local area network.
DDOS	Distributed Denial of Service. Attacks that are designed to saturate network links with spurious data which can overwhelm a bussiness' link and causing legitimate traffic to be dropped.
Decapsulation	The process of removing headers and trailers from an incoming datagram as it travels up a network stack. It is the opposite process to encapsulation. Each layer strips off its header and/or trailer before passing the data up to the layer above. As information flows back up the network stack, information received from a lower layer is interpreted as both a header/trailer and data.
Decision Tree	A decision tree comprises one or more condition branches. See also condition branch.
dedicated firewall	An individual appliance much like a router, or a software solution running on a server that sits behind the perimeter router. Since these firewalls are dedicated to examining inbound and outbound traffic, services and performance of these firewalls are generally superior. A dedicated firewall can be designed as a stand-alone appliance that contains both hardware and software, like the Cisco PIX Firewall, or a software solution that is installed on a server sitting behind the perimeter router, like Microsoft’s Proxy Server.
Deep Magic	An arcane technique specific to a program or system. Examples: cryptography, signal processing, graphics and artificial intelligence.
Default gateway	See gateway.
Defense Information Infrastructure	See DII.
Denial of Service	See DoS.
DER	A subset of the Basic Encoding Rules, which gives exactly one way to represent any ASN.1 value as an octet string [X690]. *(RFC 2828)*
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.
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
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).
Digital Signature Standard	See DSS.
DII	

Directory Database	A database of security information, such as user account names and passwords, and the security policy settings. For Windows NT Workstation, the directory database is managed using User Manager. For a Windows NT Server domain, it is managed using User Manager for Domains. Other Windows NT documentation may refer to the directory database as the Security Accounts Manager (SAM) database.
Directory Information Tree	See DIT.
Directory System Agent signing	See DSA signing.
Distinguished Encoding Rules	See DER.
Distinguished Name	See DN.
Distributed Computing Environment (DCE)	A set of distributed computing technologies that provide security services to protect and control access to data; name services that make it easy to find distributed resources; and a highly scalable model for organizing widely scattered users, services, and data.
Distributed DoS	See DDOS.
distribution layer	The demarcation point between the access and core layers; this layer helps to define and differentiate the core.
DIT	
DMZ	De-Militarized Zone. See perimeter network.
DN	An identifier that uniquely represents an object in the X.500 Directory Information Tree (DIT). *(RFC 2828)*
DNIS	Dialed Number Identification Service. The called party number used by call centers or a central office where different numbers are assigned to a specific service.
DNS	Domain Name System. System used in the Internet for translating names of network nodes into addresses.
DNS Guard	Identifies an outbound DNS query request and only allows a single DNS response back to the sender. A host may query several servers for a response in case the first server is slow in responding; however, only the first answer to the specific question will be allowed back in. All the additional answers from other servers will be dropped.
DNSSEC	DNS Security Charter. Specifies enhancements to the DNS protocol to protect the DNS against unauthorized modification of data and against masquerading of data origin.
DoD Internet	Department of Defense (DoD) Internet. A wide area network to which the ARPANET belongs. See also Internet.
DoS	When an attacker disables or corrupts networks, systems, or services with the intent to deny the service to intended users. It usually involves either crashing the system or slowing it down to the point that it is unusable.
Downstream	Toward the edge or away from the inside of the network.
DSA signing	A public algorithm backed by the U.S. government. DSA signing is supported by a limited number of PKI vendors (for example, NAI and Baltimore are two who support DSA signing).
DSL	Digital Subscriber Link.
DSP	Digita Signal Processor.
DSS	The U.S. Government standard [FP186] that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography. *(RFC 2828)*

Dual-Homed Bastion Station	A dual-homed or multi-homed bastion host. A computer with two (dual-homed) or more (multi-homed) network interface cards connecting it to two or more physical networks (see Figure C-2). This computer evaluates each network packet that it receives against a security policy definition file. A multi-homed bastion host can translate between two network access layer protocols (e.g., Ethernet to Token Ring) and check for IP spoofing attacks using trust tables. If positioned between two routers (an internal and external network pair), dual-homed bastion hosts allow for less complex rules in the routers, which increases performance. However, routers are not required with a dual-homed bastion host if it can provide the necessary routing and security functions.
dumpacl	
dynamic crypto map	A crypto map entry without all of the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a peer's requirements. This allows peers to exchange IPSec traffic with the PIX Firewall or Cisco IOS even if they do not have a crypto map entry specifically configured to meet all the peer's requirements.
Dynamic Host Configuration Protocol	See DHCP.
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.
Dynamic Packet Filter	A dynamic packet filtering firewall is a fourth-generation firewall technology that allows the modification of the firewall security rule base on the fly. This type of technology is most useful for providing limited support for the UDP transport protocol. The UDP transport protocol is typically used for limited information requests and queries for exchanges by application layer protocols.
Dynamic Stack	Within Cisco Centri Firewall, a custom network stack comprising only applicable kernel proxies is dynamically constructed for each session. See also Kernel Proxy.
Dynamic Tunnel Endpoint Discovery	Allows IPSec to scale to large networks by reducing multiple encryptions, reducing the setup time, and allowing for simple configurations on participating peer routers. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

E

EAP	A general protocol for PPP authentication that supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at the link control phase; rather, it postpones this until the authentication phase so that the authenticator can request more information before determining the specific authen-tication mechanism.
EBCDIC	extended binary coded decimal interchange code. Any of a number of coded character sets developed by IBM consisting of 8-bit coded characters. This character code is used by older IBM systems and telex machines.
e-business	A secure, flexible and integrated approach to delivering differentiated business value by combining the systems and processes that run core business operations with the simplicity and reach made possible by Internet Technology. *(consider revision, IBM's definition)*
EDI	Electronic Data Interchange. Computer-to-computer exchange, between trading partners, of business data in standardized document formats. *(RFC 2828)*

EIGRP	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
Electronic Data Interchange	See EDI.
e-mail bombs	Programs that send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.
Embryonic	Term meaning "not yet established".
Encapsulation	The process by which each layer in a network stack adds control information to an outgoing datagram (such as destination address, routing controls, and checksum) to ensure proper delivery. This control information is called a header and/or a trailer because it is placed in front of or behind the data to be transmitted. Each layer treats all of the information that it receives from the layer above it as data, and it places its own header and/or trailer around that information.
Encryption	The transformation of a message into another type of message, using a mathematical function and an encryption password, called a key. The purpose of encryption is to make information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.
Enterprise network	A large scale network belonging to a business or organization.
Entrust/PKI	Software that is installed and administered by the user. The Cisco IOS interoperates with the Entrust/PKI 4.0 CA server. Entrust/PKI(tm) delivers the ability to issue digital IDs to any device or application supporting the X.509 certificate standard, meeting the need for security, flexibility and low cost by supporting all devices and applications from one PKI.
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 and can be configured with DES or Triple DES.
ESP transform	A mechanism for payload encryption.
Ethernet	A 10-megabit-per-second standard for local area networks (LANs) initially developed by Xerox. All hosts are connected by coaxial cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm.
event logging	Automatically logs output from system error messages and other events to the console terminal.
extended ACL	An access list that is placed close to the source. Extended ACL's can block by source and destination address, network layer protocols, and other upper layer protocols.
Extended Authentication	See Xauth.
Extensible Authentication Protocol	See EAP.
External Network	Generally, a network outside of the internal (trusted) network. (i.e. the Internet)
External Threats	Individuals or organizations working from outside of your company who do not have authorized access and work their way in mainly through the Internet or dial-up access servers. See also Internal Threats.
extranet	The use of Internet technologies to connect internal business processes to external ones.

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.

F

failover	Provides a safeguard in case a PIX Firewall fails. Specifically, when one PIX Firewall fails, another immediately takes its place.
Fast Ethernet	Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase ten times that of the 10BaseT Ethernet specification, while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.
FDDI	Fiber Distributed Data Interface. LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbps token-passing network using fiber-optic cable, with transmission distances of up to 2 km. FDDI uses a dual-ring architecture to provide redundancy.
File Explorer	
FIN packets	Packets used to conceal a reconnaissance sweep.
Finger	Used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker. The "finger" service may be disabled with the command no service finger.
Finger of Death	These attacks involve sending a finger request to a specific computer every minute, but never disconnecting. Program failure to terminate the connection can quickly overload a UNIX server "process tables" and bring the Internet service provider's (ISP's) services to a standstill for hours.
firewall	A system or group of systems that enforces an access control policy between two more networks.
Firewall Server	The firewall server is the actual computer on which the firewall software is running.
Fixed Agent	Fixed agents execute on a particular computer. For example, agents that are tightly integrated with a product instance are fixed to the same computer that is executing the product instance.
Flood Guard	Allows an administrator to reclaim firewall resources if the user authentication (uauth) subsystem runs out of resources.
flow restriction	Prevents any network packet from taking a specified path, just as if the network media along that path were not connected. In other words, if a network packet can take more than one path to reach a specific destination, you can eliminate some of those possible paths by defining a flow restriction.
FORTEZZA	A registered trademark of NSA, used for a family of interoperable security products that implement a NIST/NSA-approved suite of cryptographic algorithms for digital signature, hash, encryption, and key exchange. The products include a PC card that contains a CAPSTONE chip, serial port modems, server boards, smart cards, and software implementations. *(RFC 2828)*
FQDN	The host name and IP domain name you assign to the PIX Firewall.
FTP	File Transfer Protocol. A protocol that allows a user on one host to access and transfer files to and from another host over a network.
Fully Qualified Domain Name	See FQDN.

G

Gateway	A *gateway* is a protocol converter between two peer network layers. Also commonly misused as a synonym for *firewall*.
giant	A packet with more information than expected.
GID	Group ID.
Gopher	distributed document delivery system. The Internet Gopher allows a neophyte user to access various types of data residing on multiple hosts in a seamless fashion.
GUI	graphical user interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.

H

H.323	Extension of ITU-T standard H.320 that enables videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.
H.225	Standard that defines Registration, Admission, and Status (RAS), and Call signaling.
H.245	Standard that defines Control signaling.
Hacker	Someone with a strong interest in computers, who enjoys learning about them and experimenting with them. *(RFC 2828)*
Handshake	A handshake is the exchange of control information during the session setup. A connectionless protocol, such as UDP, does not exchange control information (called a handshake) to establish an end-to-end connection before transmitting data. In contrast, a connection-oriented protocol, such as TCP, exchanges control information with the remote peer network layer to verify that it is ready to receive data before sending it. When the handshaking is successful, the peer network layers are said to have established a connection.
hash	An algorithm that computes a value based on a data object (such as a message or file; usually variable-length; possibly very large), thereby mapping the data object to a smaller data object (the "hash result") which is usually a fixed-size value. See also Hash Algorithm. *(RFC 2828)*
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.
hashing	The act of executing a hash function. See hash.
Header	Information attached to the beginning of a datagram. Headers usually contain information about the following data to aid in processing it.
Hierarchical Administrative Model	Within this administrative model, each higher-level node assumes the privileges and administrative authority of all lower-level nodes. This model allows for the "inheritance" of privileges as you move toward the top of the administrative domain.
Hijacking Tool	Once an intruder has root access on a system, they can use a tool to dynamically modify the kernel. This modification allows them to hijack existing terminal and login connections for any user on the system.
HMAC variant	Keyed-Hashing for Message Authentication. A mechanism for message authentication using cryptographic hashes such as SHA and MD5. See RFC 2104.
home gateway	The device, maintained by the enterprise customer, where a tunnel terminates. A home gateway is analogous to the L2TP network server.
Hop Count	A measure of distance between two points on the Internet.

Host	A host is network object (such as a computer or network printer) attached to a network that is addressable on that network. As a host, it has the ability to process network packets at the Internet layer. The features of routers confuse this definition because they can act as both hosts (because they are addressable network objects when you are applying new routing tables) and network devices that translate between two peer network access layers. When translating between peer network access layers, routers do not process the network packets at the Internet layer. However, when you are configuring the routers, they act as hosts processing IP-based protocols (such as RIP) so that they can maintain information stored in their routing tables.
Host ID	The portion of the IP address that identifies a computer within a particular network ID. See also IP address and network ID.
Host-based Firewall	A firewall where the security is implemented in software running on a general-purpose computer of some sort. Security in host-based firewalls is generally at the application level, rather than at a network level.
hot standby	See stateful failover.
HTML	Hypertext Markup Language. Simple hypertext document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a Web browser.
HTTP	Hypertext Transfer Protocol. The communication protocol used for transmitting data between servers and clients (browsers) on the World Wide Web. It also has variants, such as Secure HyperText Transfer Protocol (SHTTP) and one based on the Secure Sockets Layer (SLL) where URLs are addressed HTTPS.
HTTP fixup	Logs all URLs accessed in HTTP traffic (when syslog is enabled). It also enables URL-based filtering.

I

ICMP	Internet Control Message Protocol. A network protocol that handles network errors and error messages. The **ping** command uses ICMP.
IDEA	A patented, symmetric block cipher that uses a 128-bit key and operates on 64-bit blocks. *(RFC 2828)*
Identity certificate	The identity certificate is used to identify the Concentrator. A copy of this certificate is sent to the remote Concentrator during IKE negotiations. You have the option to view, delete, and enable or disable CRL lookup.
idle timeout	If a user is logged into a switch and performs no keystrokes (remains idle) for 5 minutes, the switch will automatically log the user out.
IDS	Intrusion Detection System. Monitors and responds to security events as they occur. See CSIDS.
IDS Module	See IDSM.
IDSM	Designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch back-plane, thus bringing both switching and security functionality into the same chassis.
IETF	Internet Engineering Task Force. A loosely associated collection of individuals and organizations who are the protocol engineering and development arm of the Internet. It publishes specifications on Internet protocols, such as TCP/IP, using specifications and RFC (Request for Comment) documents.
IGRP	Interior Gateway Routing Protocol. IGP developed by Cisco to address the problems associated with routing in large, heterogeneous networks.
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 policy	Defines a combination of security parameters used during the IKE negotiation. A group of policies makes up a “protection suite” of multiple policies that enable IPSec peers to establish IKE sessions and establish SAs with a minimal configuration.
IMAP	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 electronic mail applications to access remote message stores as if they were local without actually transferring the message.
Integrity	Integrity refers to the assurance that data is not altered or destroyed in an unauthorized manner. Integrity is maintained when the message sent is identical to the message received.
Internal Threats	Individuals or organizations working from outside of your company; typically disgruntled former or current employees or contractors. See also External Threats.
Internet	A wide area network originally funded by the Department of Defense, which uses TCP/IP for data interchange. The term *Internet* is used to refer to any and all of ARPANET, DARPANET, DDN, or DoD Internets.
Internet Protocol	See IP.
Internet Service Provider	See ISP.
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.
Internetwork	A group of networks connected by routers.
Internetwork Operating System	See IOS.
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.
intrusion detection	Refers to the real-time monitoring of network activity and the analyzing of data for potential vulnerabilities and attacks in progress.
Intrusion Detection System	See IDS.
IOS	Internetwork Operating System. See NOS.
IP	Internet Protocol. The network layer for the TCP/IP protocol suite. It is a connectionless, packet-switching protocol that allows host-to-host datagram delivery.
IP Address	A unique number that identifies each node on a network and to specify routing information. Each node must be assigned a unique IP address. The address is made up of two distinct parts: a network ID, which identifies the network; and a host ID, which is typically assigned by the administrator. These addresses are typically represented in dotted-decimal notation, such as 138.58.11.27.
IP Network	A unique number that identifies each IP network. IP network numbers are generalizations of IP addresses.
IP Range	An IP range is useful for identifying a collection of hosts to which you want to apply a special network policy. Typically, IP ranges are used to apply policies to a specific range of host addresses on a particular network.
IP Spoofing	To gain access, intruders create packets with spoofed source IP addresses. This attack exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker.

IP Spoofing Protection	*IP spoofing protection* is a firewall feature that verifies that the source address of a network packet that originates on an untrusted network does not match a valid address or range of addresses that are reserved for a trusted network. It also verifies that trusted addresses do not match untrusted addresses or addresses of other trusted networks. However, IP spoofing protection does not prevent IP spoofing on the same network. In addition, it does not prevent other forms of packet spoofing, such as modifying user data.
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.
IPSec client	An IPSec host that establishes IPSec tunnel(s) between itself and a Security gateway/IPSec client to protect traffic for itself.
IPSec transform	Specifies a single IPSec security protocol (either AH or ESP) with its corresponding security algorithms and mode.
IPX	Internetwork Packet Exchange. NetWare network layer (Layer 3) protocol used for transferring data from servers to workstations. IPX is similar to IP and XNS.
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.
ISDN	Communication protocols offered by telephone companies that permit telephone networks to carry date, voice, and other source traffic.
IS-IS	Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, whereby ISs (routers) exchange routing information based on a single metric, to determine network topology.
ISP	Internet service provider. Company that provides Internet access to other companies and individuals.

J

Java	Object-oriented programming language developed at Sun Microsystems to solve a number of problems in modern programming practice. The Java language is used extensively on World-Wide Web, particularly for applets. See also Java applet, Java script.
Java Applet	A small program written in the Java programming language that can be included in an HTML page. Applets can cause security breaches in a network and are often blocked by administrators.
Java Script	A separate programming language closely related to Java that can be written in HTML.
JDBC	Java specification for connecting to SQL-based databases. *(http://java.about.com/compute/java/library/glossary/bldef-JDBC.htm)*

K

KDC	Key Distribution Center. A type of key center (used in symmetric cryptography) that implements a key distribution protocol to provide keys (usually, session keys) to two (or more) entities that wish to communicate securely. *(RFC 2828)*

Kerberos	A secret-key network authentication protocol implemented through AAA that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism.
Kernel Mode	The privileged processor mode in which Windows NT system code runs. A thread running in kernel mode has access to system memory and to hardware.
Kernel Proxy	Kernel Proxy is a fifth generation firewall architecture that provides modular, kernel-based, multi-layer session evaluation and runs in the Windows NT Executive, which is the kernel mode of Windows NT.
Key Distribution Center	See KDC.

L

L2F	Layer 2 Forwarding. A Layer 2 tunneling protocol that establishes a secure tunnel across a public infrastructure (such as the Internet) that connects an ISP POP to a enterprise home gateway. This tunnel creates a virtual point-to-point connection between the user and the enterprise customer's network. L2F is the most established and stable Layer 2 tunneling protocol.
L2TP	Layer 2 Tunnel Protocol. A Layer 2 tunneling protocol that is an extension of the PPP protocol used for virtual private networks (VPNs). L2TP merges the best features of two existing tunneling protocols: Microsoft's PPTP and Cisco's L2F. L2TP is the emerging IETF standard, currently being drafted by participants from Ascend, Cisco Systems, Copper Mountain Networks, IBM, Microsoft, and 3Com.
LAC	L2TP access controller. In L2TP technology, a device that the client directly connects to and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server (NAS).
LAN	local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.
land.c	This program sends a TCP SYN packet that specifies the target host's address as both source and destination. The program also uses the same port (such as 113 or 139) on the target host as both source and destination, which causes the target system to stop functioning. See also SYN packet.
LAT	local-area transport. A network virtual terminal protocol developed by Digital Equipment Corporation.
LCB	Local Communications Bus. Within Cisco Centri Firewall, a secure application-layer communications channel used to quickly and efficiently exchange system data among application-layer agents of the security system.
LCC	Local Communications Channel. Within Cisco Centri Firewall, a secure kernel-layer communications channel used to quickly and efficiently exchange system data between kernel-layer agents and application-layer agents of the security system.

LCP	A protocol that establishes, configures, and tests data link connections used by the PPP.
LDAP	Used for accessing online directory services. LDAP was developed by the University of Michigan in 1995 to make it easier to access X.500 directories.
Lightweight Directory Access Protocol	See LDAP.
LLC	Logical Link Control. Higher of the two data link layer sublayers defined by the IEEE. The LLC sublayer handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants.
LNS	L2TP network server. In L2TP technology, a termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single media over which L2TP tunnels arrive. The LNS may have a single LAN or WAN interface---yet it can terminate calls arriving at any of the LAC's full range of PPP interfaces (asynchronous, synchronous, ISDN, V.120, etc.). The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.
Lock-and-Key	A customized firewall security feature commonly called a dynamic access list.
Logical Link Controller	See LLC.

M

MAC address	A unique 49-bit number assigned to the network interface card (NIC) by the manufacturer. MAC addresses, which are physical addresses, are used for mapping in TCP/IP network communications.
MAC layer	MAC is a layer in the network architecture that deals with network access and collision detection.
MacOS	Macintosh Operating System.
Mail Guard	Provides a safe conduit for Simple Mail Transfer Protocol (SMTP) connections from the outside to an inside electronic mail server. It allows a mail server to be deployed within the internal network without exposing it to known mail-server implementation security problems.
Main Mode	This mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1).
Malicious applets	Java, JavaScript, or ActiveX programs that act as Trojan horses or viruses to cause destruction or tie up computer resources.
MAN	metropolitan-area network. Network that spans a metropolitan area. Generally, a MAN spans a larger geographic area than a LAN, but a smaller geographic area than a WAN. Compare with LAN and WAN.
Management Information Base	See MIB.
Manual Keys	This mode requires no negotiations; it is available for troubleshooting only.
MD4	Message Digest 4. A cryptographic hash that produces a 128-bit hash result and was designed by Ron Rivest. *(RFC 2828)*
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.

media	Plural of medium. Various physical environments through which transmission signals pass. Common network media include twisted-pair, coaxial, and fiber-optic cable, and the atmosphere (through which microwave, laser, and infrared transmission occurs). Sometimes called *physical media*.
Media Access Control	See MAC address.
Message Authentication Code (MAC)	"(The) Message Authentication Code" refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES. (Also known as the U.S. Government standard Data Authentication Code.) *(RFC 2828)*
MIB	Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
MISSI	Provides a framework for the development and evolution of interoperable, complementary security products to provide flexible, modular security for networked information systems across the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII). See also DII, NII.
MLP	Multilink PPP Protocol. A protocol that splits and recombines packets to a single end system across a logical pipe (also called a bundle) formed by multiple links. Multilink PPP provides bandwidth on demand and reduces transmission latency across WAN links.
Mobile Agent	A free agent that can execute on any computer that matches its resource and security requirements.
Monitor mode	The PIX Firewall 515 has a special mode called the monitor mode that lets you update the image over the network. While in the monitor mode you can enter commands that let you specify the location of the TFTP server and the binary image to download.
MOP	Maintenance Operation Protocol. Digital Equipment Corporation protocol that provides a way to perform primitive maintenance operations on DECnet systems. For example, MOP can be used to download a system image to a diskless station.
Mp3	A music compression file type used to pass music files easily and quickly between host computers.
MSFC	
MTU	Maximum Transmission Unit. Maximum packet size, in bytes, that a particular interface can handle.
Multi-layer Switch Feature Card	See MSFC.
Multilevel Information Systems Security Initiative	See MISSI.
multiplex identifier	The number associated with a specific user's L2TP/L2F session.

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).
nameif command	Assigns a name to each perimeter interface on the PIX Firewall and specifies its security level (except for the inside and outside PIX Firewall interfaces, which are named by default).

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.
NAT	Network Address Translation.
National Information Infrastructure	See NII.
NCP	Network Control Protocol. A PPP protocol for negotiating OSI Layer 3 (the network layer) parameters.
NDIS	Network Device Interface Specification. In Windows networking, the Microsoft/3Com specification for the interface of network device drivers. All transport drivers call the NDIS interface to access network adapter cards. All network drivers and protocol drivers that are shipped with Windows NT Workstation and Windows NT Server conform to NDIS.
Nessus	
Netcat	
NetCom Systems	NetForensics.com's flagship product. NetCom Systems connects to firewalls, intrusion detection systems, Web servers and VPNs to bring the information into a single console. The tool also provides realtime alarms that can be viewed from any intranet browser, while a back-end database collects data or evidence from the security devices. *(consider revision)*
NetForensics	A web-based security infrastructure platform that collates information from disparate network and host security devices, such as Cisco Secure IDS, Cisco Secure PIX firewalls and Entercept Security Technologies Entercept host IDS, and provides detailed access, intrusion analysis and correlation and real-time event notification using a powerful enterprise database.
Netiquette	Conventions of politeness such as avoidance of cross-pointing to inappropriate groups or commercial pluggery.
Network	A *network* is a group of two or more network objects connected to each other by a cable, over telephone lines, or through wireless communication.
Network Adapter	A physical adapter that allows a host to use network services.
Network Adapter Card	A physical piece of hardware that is installed in a computer and allows that computer to connect to a network via a physical wire or dialup connection. For the purposes of the Cisco Centri Firewall, network adapter cards include Ethernet cards, modems, Token Ring cards, etc.
Network Administrator	The person in charge of operations on either a wide area network or local area network. The duties of a network administrator (also called a system administrator) can be broad and might include such tasks as installing new workstations and other devices, adding and removing authorized users, archiving files, overseeing passwords and other security measures, monitoring usage of shared resources, and handling multifunctioning equipment.
Network Application	A program that is primary to the network. It was designed specifically for the network, such as FTP. Within Cisco Centri Firewall, network applications are constructed using other networked applications and/or network services that define the services required to support a specific networked application. They serve as usable wrappers for a collection of services and network applications that collectively define the services required for a specific user application.
Network File System	See NFS.
Network ID	The portion of the *ip* address that identifies a group of computers and devices located along the same logical network.
Network Interface	A combination of the hardware and software that is required to communicate across a physical network medium.
Network Interface Card	See NIC.

Network layer	Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two end systems. The network layer is the layer at which routing occurs. Corresponds roughly with the path control layer of the SNA model.
Network Mask	A number used by software applications to separate additional network information (called the "subnet") from the host part of an IP address. The network mask is also referred to as a subnet mask or netmask.
Network Number	A number that InterNIC assigns to your network. The net number forms the first part of a host's IP address. Also referred to as a registered IP address.
Network Object	A *network object* is an entity on a network that is addressable via an *ip* address, an *ip* address and subnet mask, or a hostname. An address is similar to phone numbers for people on the global telephone network. If you dial a phone number, you can contact the person to whom that number belongs. Likewise, a network object can be contacted using its address.
Network Object Groups	A logical collection of objects from your NTT. They are one of the many components that you can use in the construction of security policy abstracts, and are important components in the construction of scalable security policies.
Network Operations Center	See NOC.
Network Packet	A *network packet* is the fundamental unit of communication on the network. It is a transmission unit of fixed maximum size that consists of binary information representing both data and a header containing an ID number, source and destination addresses, and error-control data.
Network Packet Header	The part of a network packet that contains an identification number, source and destination addresses, and sometimes, error control data. See also network packet.
Network Protocol	Sets of rules that explain how software and hardware should interact within a network to transmit information.
Network Security Database	See NSDB.
Network Security Perimeter	A typical network security perimeter includes a collection of trusted networks, or intranetworks, and a collection of perimeter networks, or De-Militarized Zones (DMZs). Any networks that are not classified as trusted or perimeter networks should be classified as either untrusted networks or unknown networks (a term used to indicate remaining networks on the Internet).
Network Security Policy	A *network security policy* focuses on controlling the network traffic and usage. It identifies a network's resources and threats, defines network use and responsibilities, and details action plans for when the security policy is violated. When you deploy a network security policy, you want to strategically enforce them at defensible boundaries within your network. These strategic boundaries are called *perimeter networks*.
Network Security Stance	A network security stance is a high-level statement on the security policies and procedures that are enforced for a network of systems.
Network Service	Most often, a *network service* defines the particular properties of a network protocol and port mappings that satisfies the requirements of a specific service, such as Domain Name Server TCP Service, which is well defined at port 53 on TCP. Within Cisco Centri Firewall, a network service is a descriptive wrapper for the actual configuration details of a protocol-to-port mapping.
Network Service Bundles	Groupings of network services that can be referenced as a whole from a service condition node within a security policy abstract. The Network Service Bundles branch of the Tools and Services tree is where they are created, stored, and modified.
Network Session	A complete communication exchange between two network objects. *See also* session.
Network Time Protocol	See NTP.

network topography	The physical path of the network media.
Network Topology Tree	See NTT.
NFS	Network File System. As commonly used, a distributed file system protocol suite developed by Sun Microsystems that allows remote file access across a network. In actuality, NFS is simply one protocol in the suite. NFS protocols include NFS, RPC, XDR, and others. These protocols are part of a larger architecture that Sun refers to as ONC.
NIC	network interface card. Board that provides network communication capabilities to and from a computer system. Also called an *adapter*.
NII	
NMAP	A utility for port scanning single hosts and large networks.
NMS	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.
NNTP	Network News Transfer Protocol. The standard protocol used for transferring Usenet news from machine to machine. *(http://usenet.about.com/internet/usenet/library/glossary/bldef-nntp.htm?rnk=r1&terms=NNTP)*
NOC	
nonce	A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks. *(RFC 2828)*
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.
NSDB	Cisco's HTML-based encyclopedia of network vulnerability information.
Nslookup	
NT Executive	The portion of the Windows NT operating system that run in kernel mode. It provides process structure, interprocess communication, memory management, object management, thread scheduling, intercept processing, I/O capabilities, networking, and object security.
NT Kernel	The component of the NT executive that manages the processor. It performs thread scheduling and dispatching, interrupt and exception handling, and multiprocessor synchronization and provides primitive objects that the NT executive uses to create user-mode objects.
NTP	The Network Time Protocol (NTP) isn't especially dangerous, but any unneeded service may represent a path for penetration. If NTP is actually used, it's important to explicitly configure trusted time source, and to use proper authentication, since corrupting the time base is a good way to subvert certain security protocols.
NTT	Identifies the important components of a network infrastructure. It also identifies network objects that enable the Policy Enforcement Points to protect other network objects, such as authentication servers, syslog servers, and CSPM hosts that distribute the policies to the Policy Enforcement Points. Because the NTT identifies these components, it is also the location for specifying the physical descriptions of those components, and defining "device-centric" settings and rules, such as NAT and routing rules.
NVRAM	nonvolatile RAM. RAM that retains its contents when a unit is powered off.

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).
Object	A single runtime instance of an NT-defined object type. It contains data that can be manipulated only by using a set of services provided for the objects of its type.
Octet	In programming, an octet refers to eight bits or one byte. For example, IP addresses are typically represented in dotted-decimal notation, where the decimal value of each octet of the address is separated by a period. *See also* IP address.
OCX	Object Linking and Embedding control. See ActiveX.
ODBC	Open Database Connectivity. A standard method of sharing data between databases and other programs. ODBC drivers use the standard Structured Query Language (SQL) to store data in sources outside of Cisco Centri Firewall's Security Knowledge Base. Cisco Centri Firewall supports any ODBC 2.0 compliant drivers for popular database formats.
OLE	Object Linking and Embedding. See ActiveX.
One-Time Password	See OTP.
Open Software Foundation	See OSF.
Operating System	Software that controls the input and output and that loads and runs other programs
Optical Time Domain Reflectometer	See OTDR.
ORA	An RA for an organization. *(RFC 2828)*
Organizational Registration Authority	See ORA.
OSF	Open Software Foundation. Group responsible for the Distributed Computing Environment (DCE) and the Distributed Management Environment (DME). See DCE.
OSI	Open System Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.
OSPF	Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol. See also IGP, IS-IS, and RIP. See also Enhanced IGRP and IGRP (Interior Gateway Routing Protocol) in the "Cisco Systems Terms and Acronyms" section.
OTDR	Used with optical fiber cable mainly to measure signal attenuation and the length of an installed cable base; sometimes, however, they can also detect illegal wire taps.
OTP	1.) A "one-time password" is a simple authentication technique in which each password is used only once as authentication information that verifies an identity. This technique counters the threat of a replay attack that uses passwords captured by wiretapping. 2.) "One-Time Password" is an Internet protocol that is based on S/KEY and uses a cryptographic hash function to generate one-time passwords for use as authentication information in system login and in other processes that need protection against replay attacks.
Overload	Used to translate all “internal” (local) private addresses to a single “outside” (global)—usually registered—IP address.
Overruns	Occur when the network interface card is overwhelmed and cannot buffer received information before more needs to be sent.

P

Packet Filter Firewall	A *packet filter firewall* is a first-generation firewall technology that analyzes network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining which data flows are allowed. These rules identify whether communication is allowed based upon information contained within the internet and transport layer headers and the direction that the packet is headed (internal to external network or vice-versa).
Packet Filtering	Limits information into a network based on static packet header information.
packet filters	Packet filters augment authentication and authorization mechanisms to help protect network resources from unauthorized use, theft, destruction, and denial-of-service (DoS) attacks.
Packet Internet Exchange Firewall	See PIX Firewall.
Packet Spoofing Protection	*Packet spoofing protection* is a firewall feature that prevents an attack scenario whereby an intruder modifies some portion of a network packet. Network packets may be modified at any layer in the Internet reference model.
PAM	Port-to-Application Mapping. Allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.
PAP	Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines.
PAT	Port Address Translation.
Path restrictions	Stop the packet flow in one direction between two interfaces. Packets can flow in the opposite direction without any effect from the path restriction. Path restrictions are usually used in pairs (symmetric path restrictions).
PBX	Private Branch Exchange. Digital or analog telephone switchboard located on the subscriber premises and used to connect private and public telephone networks.
PCM	pulse code modulation. Transmission of analog information in digital form through sampling and encoding the samples with a fixed number of bits.
PCMCIA	Personal Computer Memory Card International Association, a group of manufacturers, developers, and vendors, founded in 1989 to standardize plug-in peripheral memory cards for personal computers and now extended to deal with any technology that works in the PC card form factor. *(RFC 2828)*
PDA	Personal Digital Assistant. A handheld device that combines computing, telephone/fax, and networking features that functions as a cellular phone, fax sender, and personal organizer. *(http://www.thegrid.net/tech/smart/pda.htm)*
PDC	Primary Domain Controller. In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC.
PDP	
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.
PEM	An Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail. *(RFC 2828)*

PEP	Policy Enforcement Points. PIX Firewalls that have configurations generated by Cisco Secure Policy Manager, or Cisco routers that have the commands generated by Cisco Security Policy Manager inserted in their configurations.
Perfect Forward Secrecy	See PFS.
Perimeter network	A *perimeter network* is a network added between a protected, trusted network and an external, untrusted network in order to provide an additional layer of security (defense in depth).
Personal Digital Assistant	See PDA.
PFC	
PFS	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.
PFSS	PIX Firewall Syslog Server. A very basic application that lets you view PIX Firewall or Cisco Router event information from a Windows NT system and includes special features not found on other syslog servers.
PFTP	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.
Phreaking	The act of cracking the phone network to, for example, make free long-distance calls.
Physical Layer	Layer 1 of the OSI reference model. The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.
Ping	packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.
Ping of Death	Modifies the IP portion of header indicating there is more data in the packet than there actually is, or exceeds the maximum allowed packet size, causing the receiving system to crash.
Ping sweep	An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities. *(RFC 2828)*
PIX Firewall	A dedicated hardware/software security solution that delivers high-level security without impacting network performance. It is a hybrid system because it uses features from both the packet filtering and proxy server technologies.
PIX Firewall Syslog Server	See PFSS.
PKCS#10	Public Key Cryptography Standard # 10. A standard syntax from RSA Data Security, Inc. for certificate requests. The PIX Firewall automatically creates the certificate requests as part of the Simple Certificate Enrollment Protocol (SCEP) process.
PKCS#7	Public Key Cryptography Standard # 7. A standard from RSA Data Security, Inc. used to encrypt, sign and package certificate enrollment messages.
PKI	Public Key Infrastructure. Software, encryption and authentication technologies, and services that allows secure communications for enterprises over the Internet.
PMP	Collects the audit event streams from one or more PEPs and combines them into audit records that can be further refined into meaningful data. The PMP provides this data to the Policy Report Point (PRP) for administrative reports about network activity.
Point-to-Point Protocol	See PPP.
Policy Builder	Policy Builder is used to develop and modify security policies. After the policy has been created, CSPM provides drag-and-drop application of the policy to the network.

Policy Distribution Point	See PDP.
Policy Domains	Logical collections of network perimeters that can be referenced in the source or destination conditions of security policies or placed in the Security Policy Enforcement branch and have policy applied. Perimeters, previously only available in the source or destination conditions of a security policy, are now branch objects on the Policy Domains branch of the Tools and Services tree. Policy Domains can also be placed in the Security Policy Enforcement branch and have policy applied to them.
Policy Enforcement Point	See PEP.
Policy Feature Card	See PFC.
Policy Inheritance	*Policy inheritance* refers to Cisco Centri Firewall's ability to use recursive lists of security policies. If a policy on a lower node of a tree has the action Use Next Policy applied to a condition branch, then the next policy up and in the direct path of that node is applied. This ability is transferred all the way up to the Trusted Network, Logical Network, or Internet node if the policies below those nodes use the Use Next Policy action. Dominance is an attribute of the lowest node to which a security policy is applied. If the parameters of a session request match two security policies within a direct path, the one applied to the lowest node in that path is applied to that session.
Policy Monitor Point	See PMP.
Policy Report Point	See PRP.
POP3	The most commonly used protocol used for retrieving email messages on the Internet. *(http://perl.about.com/compute/perl/library/glossary/bldef-POP3.htm?rnk=r3&terms=POP3)*
Port Scan	An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service. *(RFC 2828)*
port security	Allows a network administrator to configure a set of MAC addresses to provide additional security. If port security is enabled, only the MAC addresses that are explicitly allowed can use the port.
Port-to-Application Mapping	See PAM.
PostOffice	Designed to guarantee the transmission of messages to the intended recipient; therefore, it expects acknowledgement for every message sent from the receiver. If no acknowledgement is received within a predetermined length of time, the message is resent until the acknowledgement is received.
PPD	
PPP	Point-to-Point Protocol. A successor to SLIP, PPP provides router-to-router and host-to-network connections over synchronous and asynchronous circuits.
PPTP	Point-to-Point Tunneling Protocol. A Microsoft proprietary tunneling protocol that was combined with L2F to create L2TP.
Presentation Layer	Layer 6 of the OSI reference model. This layer ensures that information sent by the application layer of one system will be readable by the application layer of another. The presentation layer is also concerned with the data structures used by programs and therefore negotiates data transfer syntax for the application layer.
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.
Primary Policy Database	See PPD.
Privacy Enhanced Rules	See PEM.

Private 1	Private I is a syslog management tool designed for automatic verification of corporate network security and network productivity policies. Private I features a robust syslog server, a relational database engine, and comprehensive reporting and alerting that together process massive amounts of abstract syslog data from multiple Cisco devices concurrently. By intelligently managing the syslog data, Private I provides management with comprehensive reports on all traffic coming in and out of the corporation while also providing network administrators real time alerts based upon individually defined security and productivity rules.
Privelege Escalation	Occurs when a user obtains privileges or rights to objects that were not assigned to the user by an administrator. These objects can be files, commands, or other components on a network device.
Privelege Ticket-Granting Ticket	See PTGT.
priveleged level	Allows users to issue all commands on the Cisco IOS, including configuration and debug commands.
Priveleged mode	This mode displays the **#** prompt and enables you to change the current settings. Any unprivileged command also works in privileged mode. Applicable to both Cisco routers and PIX Firewalls.
Proxy	An entity that has the authority to act for another. *See also* proxy client and proxy server.
Proxy client	A *proxy client* is part of a user application that talks to the real server on the external network on behalf of the real client. When a real client requests a service, the proxy server evaluates that request against the policy rules defined for that proxy and determines whether to approve it. If it approves the request, the proxy server forwards that request to the proxy client. The proxy client then contacts the real server on behalf of the client (thus the term "proxy") and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server. Likewise, the proxy server relays requests and responses between the proxy client and the real client.
Proxy server	A *proxy server* acts as the end server for all connection requests originated on a trusted network by a real client. That is, all communication between internal users and the Internet passes through the proxy server rather than allowing users to communicate directly with other users and servers on the Internet. An internal user, or client, sends a request to the proxy server for connecting to an external service, such as FTP or Telnet. The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service. Proxy servers understand the protocol of the service that they are evaluating, and therefore, they only allow those packets through that comply with the protocol definitions. They also enable additional benefits, such as detailed logging of session information and user authentication.
Proxy service	A proxy service is a software program that connects a user to a remote destination through an intermediary gateway. They are special-purpose programs that manage traffic through a firewall for a specific service, such as HTTP or FTP, that is able to enforce security as well as provide valuable services such as logging. Proxy services tend to be specific to the protocol they are designed to forward, and they can provide increased access control, careful checks for valid data, and generate audit event records about the traffic that they transfer (see Figure C-3). In addition, proxy services tend to offer certain common features such as authentication, data caching, and application layer protocol validation.
PRP	Analyzes detailed audit event data and generates an event summary report based on that analysis.
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).
PTGT	

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.

Q

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

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.
RADIUS	A distributed client/server system implemented through AAA that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.
RAM	Random Access Memory. Volatile memory that can be read and written by a microprocessor.
Random Access Memory	See RAM.
RAS	Remote Access Service. A service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a Windows NT computer can dial in to remotely access their networks for services, such as file and printer sharing, e-mail, scheduling, and SQL database access.
RC4	Rivest Cipher #4. A proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc. (now a wholly-owned subsidiary of Security Dynamics, Inc.). *(RFC 2828)*
rcp	remote copy protocol. Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data.
Rcpinfo	
RDN	Relative Distinguished Name. One or more attribute values from the entries in the DTT. See also DTT.
RDT	Real Data Transport Protocol.
Read Only Memory	See ROM.
Reconnaissance attacks	The unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also known as information gathering and, in most cases, precedes an actual access or denial of service attack.
Relative Distinguished Name	See RDN.
Remote Monitoring	See RMON.
Remote Procedure Call	See RPC.
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.
Reusable passwords	The simplest form of authentication. It requires the user to enter a text string that only he or she knows. Every time a user needs to authenticate himself, he enters the same password. However, reusable passwords are vulnerable to packet sniffers and common password attacks. Therefore, reusable passwords are not considered a reliable authentication mechanism. For this reason, we do not recommend that you use reusable passwords, and we strongly recommend that you do not use reusable passwords to gain access from untrusted networks or for the firewall administrator account.
RFC	Request for Comments. The naming convention for specifications produced by the IETF that are made publicly available for comments.
RIP	Routing Information Protocol. IGP supplied with UNIX BSD systems. The most common IGP in the Internet. RIP uses hop count as a routing metric.
rlogin	
RMON	remote monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.
ROM	read-only memory. Nonvolatile memory that can be read, but not written, by the microprocessor.
Root certificate	The root certificate is used to verify the identity certificates. The identity certificate installed in this Concentrator is received from another Concentrator during IKE negotiations. See also Identity certificate.
router	Network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information. Occasionally called a gateway (although this definition of gateway is becoming increasingly outdated).
router-based firewall	A firewall where the security is implemented using screening routers as the primary means of protecting the network.
Routing	The process of forwarding packets to other routers until the packet is eventually delivered to a router connected to the specified destination. See also network packet and router.
RPC	remote-procedure call. Technological foundation of client-server computing. 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.
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.
RSA Encrypted nonces	Provide a strong method of authenticating the IPSec peers and the Diffie-Hellman key exchange. RSA encrypted nonces provide repudiation-a quality that prevents a third party from being able to trace your activities over a network.
RSA Signature	Specifies how RSA is used with the MD5 hash function.
RTCP	Real Time Control Protocol. Duplex (bidirectional) UDP session used to provide synchronization information to the client and packet loss information to the server. The RTCP port is always the next consecutive port from the RTP data port.
RTP	Real-Time Transport Protocol. Simplex (unidirectional) UDP session used for media delivery using the RTP packet format from the sever to the client. The client’s port is always an even numbered port.

RTSP	Real Time Streaming Protocol. Enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such live audio and video, and stored content, such as pre-recorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.
runts	Packets with less information than expected.

S

S/Key	An authentication method that uses a one-time password system developed at Bellcore. Under this system, the user generates a set of passwords based on a "seed" word or phase. When the firewall server prompts the user for authentication information, it provides a challenge based on the result of an algorithm applied iteratively to the seed value. The user must enter the password appropriate for that challenge. While S/Key is able to validate the user's current response, it has no way of predicting the user's next response. Each time users attempt to log in, they are prompted for a different password.
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.
SATAN	Security Administrator's Tool for Analyzing Networks. The Security Analysis Tool for Auditing Networks which gathers as much information about remote hosts and networks as possible by examining such network services as finger, NFS, NIS, ftp and tftp, rexd, and other services.
Scalable Encryption Processing modules	See SEP modules.
Scalable Encryption Processor 2	See SEP2.
SCEP	Simple Certificate Enrollment Protocol. A PKI communication protocol which leverages existing technology by using PKCS #7 and PKCS #10.
SCP	A session layer protocol which lets a server and client have multiple conversations over a single TCP connection.
Screened subnet	A firewall architecture in which a "sand box" or "demilitarized zone" network is set up between the protected network and the Internet, with traffic between the protected network and the Internet blocked. Conceptually, a subnet is similar to a dual-homed gateway, except for the fact that an entire network, rather than a single host, is reachable from the outside.
Screening router	A router that is used to implement part of the security of a firewall by configuring it to selectively permit or deny traffic at a network level.
script kiddies	Hackers that are motivated by the intellectual challenge of breaking into a network system.
Secure Hyper Text Transport Protocol	See SHTTP.
Secure Shell	See SSH.
Secure Socket Layer	See SSL.
security	1.) Protection against malicious attack by outsiders. 2.) Controlling the effects of errors and equipment failures.

Security gateway	A security gateway is an intermediate system that acts as the communications interface between two networks. The set of hosts (and networks) on the external side of the security gateway is viewed as untrusted (or less trusted), while the networks and hosts and on the internal side are viewed as trusted (or more trusted). The internal subnets and hosts served by a security gateway are presumed to be trusted by virtue of sharing a common, local, security administration.
Security Knowledge Base	A proprietary knowledge-based system that persistently stores configuration information, as well as audit events generated by the security system. It combines knowledge representation technology from the artificial intelligence community with object-oriented technology from the programming community to enable agents within the Cisco Centri Firewall to communicate with each other and to store information using a flexible representation.
Security Parameter Database	Set up in dynamic random-access memory (DRAM), and contains parameter values for each SA.
Security policy	A security policy is a company's statement delineating what its assets are, how valuable they are to the company, what measures the company is willing to use to protect its assets, and what balance they wish to achieve between ease of use and securing its assets. The security policy also defines areas of responsibility, including who is to be notified when an incident occurs. CSPM supports notification using e-mail, pagers, and terminal display.
Security Policy Abstracts	The object that represents the security policy in the CSPM Navigator pane. The Security Policy Abstracts branch of the Tools and Services tree is where security policy abstracts are created, stored, and managed. The security policy that it contains consists of a graphical decision tree with source, service, and destination conditions and actions on each branch of the conditions.
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.
Security Policy Enforcement Branch	CSPM branch where you directly apply security policies to network objects.
security posture	The state of hardware, operating system software, utilities, and applications designed to control access to and use of services and information resident on the system.
Security Technology Assessment Team	See STAT.
Security Wheel	A continuous security policy that is effective because it promotes retesting and reapplying updated security measures on a continuous basis.
Sendmail	A program used to run e-mail on UNIX systems.
Sensor	High-speed network "appliances" which analyze the content and context of individual packets to determine if traffic is authorized.
SEP modules	Field-swappable and customer-upgradeable components of the Cisco VPN 3000 Concentrator series.
SEP2	A hardware-based encryption module that allows a network administrator to off-load processor intensive encryption tasks to hardware.
Server	A system that provides services to the network. These services can include Web servers, FTP servers, Gopher servers, proxy services, NFS file system and NIS database access.
Server Application	A networked application that provides network services directly to a client application.
service set identifiers	See SSID.

session	1.) A session is the act of two network objects communicating. It is a four step process that includes a session request, a session acceptance, communication of data, and a close request. 2.)A communication between two users using TCP or UDP to make and manage the connection. TCP sessions are started with a connection request, followed by connection acceptance, and are closed by a close request.
session control	A *session control* is a particular setting or characteristic about a session that you can use to provide stricter control over what is and what is not allowed during a session and to act upon a session. Session controls are specific to a network service.
Session Control Protocol	See SCP.
Session Layer	Layer 5 of the OSI reference model. This layer establishes, manages, and terminates sessions between applications and manages data exchange between presentation layer entities.
session request	A *session request* is the initial request by a network object to begin a session with another network object.
SHA	Secure Hash Algorith. 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.
SHTTP	Secure HyperText Transport Protocol. A secure message-oriented communications protocol designed to be used for securing messages using the HTTP protocol. The protocol preserves the characteristics of HTTP while allowing request and reply messages to be signed, authenticated, encrypted, or any combination of these (including no protection). SHTTP clients can communicate with non-HTTP supported servers (although in these cases, the security features of SHTTP would not be applied).
signature	A set of rules pertaining to typical intrusion activity, which is compared against the network traffic. When this set of rules is matched to network activity, a unique response is generated for the event.
Simple Network Managemet Protocol	See SNMP.
site	*Sites* represent a network that is trusted, untrusted, or unknown, and they are tied to a network adapter card. Because more than one network can be assigned to a network adapter card, sites represent the relationships among networks. When a network packet arrives at the firewall server, it arrives from a particular site. The site that it arrives from determines which network security policy is applied to that packet.
Skeme Key Exchange	A key exchange protocol which defines how to derive authenticated keying material, with rapid key refreshment.
SMB	Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.
SMTP	Simple Mail Transfer Protocol. Used to transfer electronic mail between computers.
SMURF attack	The SMURF attack starts with a perpetrator sending a large number of spoofed ICMP ECHO requests to broadcast addresses, hoping that these packets will be magnified and sent to the spoofed addresses. If the routing device delivering traffic to those broadcast addresses performs the Layer 3 broadcast to Layer 2 broadcast function, most hosts on that IP network will reply to the ICMP ECHO request with an ICMP ECHO reply each, multiplying the traffic by the number of hosts responding. On a multiaccess broadcast network, there could potentially be hundreds of machines replying to each ECHO packet.
Sneaker	Someone hired to test the security of a system by attempting to break into it.
sniffers	A program that can record all network packets that travel past a certain network interface, computer, or network. It can be used to troubleshoot network problems, or extract sensitive information.

SNK	SecurityNetKey. An authentication method that uses a random challenge password to authenticate users.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SNMPv1	SNMP version 1 uses cleartext passwords for authentication and access control. *(RFC 2828)*
SNMPv2	SNMP version 2 adds cryptographic mechanisms based on DES and MD5. *(RFC 2828)*
SNMPv3	SNMP version 3 provides enhanced, integrated support for security services, including data confidentiality, data integrity, data origin authentication, and message timeliness and limited replay protection. *(RFC 2828)*
Socket Security	See SOCKS.
SOCKS	An Internet protocol that provides a generalized proxy server that enables client-server applications--such as TELNET, FTP, and HTTP; running over either TCP or UDP--to use the services of a firewall. *(RFC 2828)*
Softtoken	
SPAM attack	A large contingency of e-mail attacks are based on e-mail bombing or spamming. E-mail *bombing* is characterized by abusers repeatedly sending an identical e-mail message to a particular address. E-mail *spamming* is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users (or to lists that expand to that many users).
SPAN	Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any of the other Catalyst switched ports.
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.
spoofing	1.) Scheme used by routers to cause a host to treat an interface as if it were up and supporting a session. The router spoofs replies to keepalive messages from the host in order to convince that host that the session still exists. Spoofing is useful in routing environments such as DDR, in which a circuit-switched link is taken down when there is no traffic to be sent across it in order to save toll charges. 2.) The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms such as filters and access lists.
SPX	Sequenced Packet Exchange. Reliable, connection-oriented protocol that supplements the datagram service provided by network layer (Layer 3) protocols. Novell derived this commonly used NetWare transport protocol from the SPP of the XNS protocol suite.
SQL	Structured Query Language. International standard language for defining and accessing relational databases.
SQL*Net	Oracle's client/server middleware product that offers transparent connection from client tools to the database or from one database to another. SQL*Net works across multiple network protocols and operating systems. *(consider revising, this is Oracle's definition)*
srvinfo	
SSH	A protocol for secure remote login and other secure network services over an insecure network. *(RFC 2828)*

SSID	A common network name for the devices in a wireless LAN subsystem; it serves to logically segment that subsystem. The use of the SSID as a handle to permit/deny access is dangerous because the SSID typically is not well secured.
SSL	An open protocol designed by Netscape; it specifies a mechanism for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP. It provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
SSL/TLS	
standard ACL	An access list that is placed near the destination. Standard access lists can block by either source or destination address but not both. *(consider revising)*
STAT	
Stateful failover	Provides a mechanism for the firewall to be redundant by allowing two identical units to serve the same functionality. The active unit performs normal security functions, while the standby unit monitors, ready to take control should the active unit fail.
stateful firewalling	
stateful inspection	Examines each IP header and maintains a state table of connections. Stateful inspection allows enterprises to take advantage of new protocols and security technologies.
Stateful Packet Filtering	A secure method of analyzing data packets that places extensive information about a data packet into a table. In order for a session to be established, information about the connection must match the information in the table.
static crypto map	A manually assigned crypto map. See crypto map.
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.
static route	Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols. *(RFC 2828)*
Static translation	A bi-directional one-to-one address-mapping rule-which gives external users access to one of the internal network devices. Static translation rules apply to all forms of IP traffic, which means they do not limit access to the device based on a specific network service.
strict adherence administrative model	Within this model, each node is assigned a discrete set of administrative actions and privileges, and only those users associated with that node are allowed to perform administrative actions at that level.
Structured Threats	Consists of hackers who are more highly motivated and technically competent than those of unstructured threats. See also Unstuctured threats.
subnet number	A part of the Internet address that designates a subnet. Ignored for the purpose of Internet routing, it is used for intranet routing.
Switch Port Analyzer	See SPAN.
Syn Floods	Randomly opens up many TCP ports, tying up the network equipment or computer with bogus requests, thereby denying sessions to others. Accomplished with protocol analyzers or programs
SYN packets	A TCP connection initiation packet sent from the host requesting authentication, used for verification. *(consider revision)*
SYN-ACK packets	A packet sent by the server after receipt of a SYN packet from a host requesting authentication. *(consider revision)*
synchronous transmission	Term describing digital signals that are transmitted with precise clocking. Such signals have the same frequency, with individual characters encapsulated in control bits (called start bits and stop bits) that designate the beginning and end of each character.

SYSLOG messages	Based on the User Datagram Protocol (UDP) and are received on UDP port 514. The message text is kept under 512 bytes to ensure that the UDP packet is smaller than 576 bytes---the smallest packet that must be accepted by a host without packet fragmentation. Syslog messages are categorized by eight priority levels.1 Syslog messages generated by various devices can be logged locally or redirected to a log file or syslog management server. A syslog management server can be used to collect all syslog information that is deemed critical as part of the corporate network for auditing purposes.
system access	The ability of an intruder to gain access to a machine, which the intruder is not allowed access to (for example, the intruder does not have an account or password). Entering or accessing systems which one does not have access to usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.
system administrator	*See* network administrator.
System attack	The ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or password. Entering or accessing systems to which one does not have access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

T

T1	Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using AMI or B8ZS coding.
TACACS	See TACACS+.
TACACS+	Terminal Access Controller Access Control System+. A security application implemented through AAA that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. See also TACACS.
Targa.c	Multi-platform DoS attack which integrates bonk, jolt, land, nestea, netear, syndrop, teardrop, and winnuke all into one exploit. See also DoS.
task	Tasks are the ordered collection of specific actions into a meaningful relationship. Tasks signify the ordered completion of actions that must be performed to conclude a higher goal.
TCP	Transmission Control Protocol. A sequenced, bi-directional network protocol commonly used for services on the Internet such as Telnet, FTP, SMTP, NNTP and HTTP. The TCP protocol is considered reliable because transmitted data is resubmitted until its receipt is acknowledged by the receiver.
TCP Syn Floods	These attacks are created by sending repeated TCP connection requests with no subsequent completion, causing the target system to allocate TCP control blocks until it runs out of resources.
TCP/IP	Transmission Control Protocol/Internet Protocol. The suite of applications and transport protocols that runs over IP. These protocols include FTP, Telnet, SMTP, and UDP (a transport layer protocol).
TDR	time domain reflectometer. Device capable of sending signals through a network medium to check cable continuity and other attributes. TDRs are used to find physical layer network problems.
teardrop.c	Fragmentation implementation of IP whereby reassembly problems can cause machines to crash.

TED	An enhancement to the IP Security Protocol (IPSec) feature. Defining a dynamic crypto map allows you to be able to dynamically determine an IPSec peer; however, only the receiving router has this ability. With Tunnel Endpoint Discovery, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.
Telemate.Net	With Telemate.Net, customers can report on activity, and security trends or both over various periods—by day, week, month, and over several months. The software can be configured to track Internet activity by user, IP address, organizational levels, or sources of data, and provide the information needed to manage network use, cost, security, and electronic commerce. It can also monitor alarm levels, number of alarms, source and destination IP addresses, and alarm signatures for more effective intrusion detection management, or to justify additional network sensors.
Telnet	The Internet standard protocol for remote terminal connection service.
TFN	An attack made up of client and daemon programs which implements a distributed network denial of service tool capable of initiating ICMP floods, SYN floods, UDP floods, and Smurf style attacks, as well as providing an "on demand" root shell bound to a TCP port. *(http://fatty.opf.slu.cz/bugtraq/msg00286.html)*
TFTP	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.
Threats	Unauthorized attempts at access "on or against" all networks.
Time bomb	A type of logic bomb set by a programmer to go off if he is not there to suppress it periodically. For instance if he is fired or laid off.
Time Domain Reflectometer	See TDR.
Time to Block	Specifies how long the Sensor blocks traffic from the specified source when you issue a Block command from the Event Viewer. The block duration value that can be specified for the Sensor in the Network Topology Tree (NTT) applies only to blocks that are generated automatically by that Sensor.
TLS	TLS Version 1.0 is an Internet protocol based-on and very similar to SSL Version 3.0. *(RFC 2828)*
Token Ring network	Token-passing LAN developed and supported by IBM. Token Ring runs at 4 or 16 Mbps over a ring topology. *(RFC 2828)*
traffic flow	Two paths that follow the same route but travel in opposite directions.
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 layer	Layer 4 of the OSI reference model. This layer is responsible for reliable network communication between end nodes. The transport layer provides mechanisms for the establishment, maintenance, and termination of virtual circuits, transport fault detection and recovery, and information flow control. Corresponds to the transmission control layer of the SNA model.
Transport Layer Security	See TLS.
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.

Tribe Flood Network	See TFN.
Triple Data Encryption Standard	An alternative to DES that preserves the existing investment in software but makes a brute-force attack more difficult. The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES, in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES.
Trojan Horse	A security-breaching program disguised as something harmless such as a game, directory lister, or archiver. See also worm, virus.
Trusted Networks	Trusted networks are the networks inside your network security perimeter. These networks are the ones you are trying to protect. Often, you or someone in your organization administers the computers that comprise these networks, and your organization controls their security measures.
TSCC	Enables CSPM to play small *.avi files that demonstrate how to use the common features of CSPM. It is not necessary for successful installation, but the *.avi files will not play without the codec.
TTL	Time-To-Live. Field in an IP header that indicates how long a packet is considered valid.
TTY	
tunnel	A secure communication path between two peers, such as a client and a router.
Tunnel Endpoint Discovery	See TED.
tunnel ID	A two-octet value that denotes a tunnel between an ISP and a home gateway.
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.

U

UDP	A non-sequenced and unreliable network protocol. UDP sends and receives datagrams. UDP is at the same layer as TCP, but it does not acknowledge transmissions, and therefore, it is unreliable.
UDP bomb	
UID	User ID.
Underruns	Occur when the PIX Firewall is overwhelmed and cannot get data fast enough to the network interface card.
Uniform Resource Locator	A method of specifying an address for a network server on the world-wide web (WWW).
UNIX	An operating system developed by Bell Laboratories that supports multi-user and multitasking operations.
unknown network	Unknown networks are those networks that are neither trusted nor untrusted. They are unknown quantities to the firewall because you cannot explicitly tell the firewall server that this network is a trusted or an untrusted network. Unknown networks exist outside of your security perimeter. By default, all unknown networks are assumed to be untrusted networks.
Unpriveleged mode	This mode is available when you first access the PIX Firewall. The > prompt is displayed. This mode lets you view restricted settings.
Unstructured threats	When inexperienced individuals using easily accessible hacking tools breach the security of a network.

untrusted network	Untrusted networks are the networks that are known to be outside your security perimeter. They are untrusted because they are outside of your control. You have no control over the administration or security policies for these sites. They are the private and shared networks from which you are trying to protect your network. However, you still need and want to communicate with these networks even though they are untrusted.
Upstream	Toward the core or inside of the network.
URL	Universal Resource Locator. Standardized addressing scheme for accessing hypertext documents and other services using a WWW browser.
user level	Allows users to perform certain commands but does not give them the ability to modify the configuration or perform a debug.
user mode	The non-privileged mode in which application code runs. A thread running in user mode can gain access to the system only by calling system services. Compare kernel mode.
UUID	Universal Unique ID.

V

V.120	An ISDN rate adaptation standard, V.120 allows one B channel to carry multiple subrate channels in a succession of statistically multiplexed (variable-length) frames which can support error detection and correction procedures. *(http://www.shiva.com/prod/docs/snmhelp.45/snm01325.htm)*
VDOLive	An MPEG video player that attempts to provide access through a firewall by either using a proxy server or enabling a specific port.
Verisign Onsite 4.5	Delivers a fully-integrated enterprise PKI to control, issue, and manage IPSec certificates for PIX Firewalls and Cisco routers.
Vigenere cipher	A simple poly-alphabetic cipher.
virtual circuit	A virtual communication channel between two computers. Multiple network sessions are multiplexed across a single virtual circuit.
Virtual Local Area Network	See VLAN.
Virtual Private Dial-up Network	See VPDN.
virus	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting--i.e. inserting a copy of itself into and becoming part of--another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. *(RFC 2828)*
VLAN	virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VPDN	virtual private dial-up network. See also VPN.
VPN	A trusted network that transmits data across an untrusted network infrastructure. Network packets that originate on a VPN are considered to originate from within your internal perimeter network. This origin is logical because of how VPNs are established. For communications that originate on a VPN, security mechanisms must exist by which the firewall server can authenticate the origin, data integrity, and other security principles contained within the network traffic according to the same security principles that are enforced on trusted networks.
VPN Concentrator	See Cisco VPN Concentrator series.

VRRP	A protocol which allows several routers on a multiaccess link to utilize the same virtual IP address where one router will be elected as a master with the other routers acting as backups in case of the failure of the master router. *(consider revision http://www.ietf.org/html.charters/vrrp-charter.html)*
VTY	virtual type terminal, but commonly used as virtual terminal lines.
vulnerability	Implies weakness, which can be caused by misconfigured hardware or software, poor design, or end user carelessness.
Vulnerability Patching	Apply fixes or measures to stop the exploitation of known vulnerabilities. This includes turning off services that are not needed on every system. The fewer services that are enabled, the harder it is for hackers to gain access.

W

W.W.W.	World Wide Web. The software, protocols ,conventions, and information that enable hypertext and multimedia publishing among disparate computers.
WAIS	Wide Area Information Server. Distributed database protocol developed to search for information over a network. WAIS supports full-text databases, which allow an entire document to be searched for a match (as opposed to other technologies that only allow an index of key words to be searched).
WAN	wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs. Compare with LAN and MAN.
Warez	Commercial software that has been pirated and made available to the public via a BBS or the Internet. See also BBS and Internet. *(http://webopedia.internet.com/TERM/w/warez.html)*
WebSENSE	Software that provides integrated, URL filtering for the PIX Firewall, giving network administrators the ability to effectively monitor and control network traffic. WebSENSE is used to block specific URLs because the PIX Firewall cannot. WebSENSE determines whether to block or permit specific URLs based on its configuration and the Master Database.
WECA	Wireless Ethernet Compatability Alliance. An alliance formed by 3Com, Aironet, Dell, Intersil, Lucent, Nokia, Nortel, and Symbol devoted to driving the adoption of a single IEEE 802.11 HR standard for wireless LANs. *(http://www.3com.com/nsc/glossary/wirelessethernetcompatibilityalliance.htm)*
WEP	Wired Equivalency Privacy. Offers a mechanism for securing wireless LAN data streams. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data.
Wetware	A term used by hackers to describe humans such as programmers, operators, or administrators involved with a certain computer system.
whois	
Wi-Fi certification	Wireless Fidelity Certification.
Windows	An operating system suite developed by Microsoft designed to work on personal computers as well as network terminals and portable computers. *(consider revising)*
Windows NT Server	A superset of the Windows NT Workstation operating system that is optimized to run server-based applications that are shared among multiple users and acts as the server in the Windows NT client-server model. It provides centralized, domain-based network management and security. It also offers advanced fault-tolerance features, such as disk mirroring, and additional connectivity.
Windows NT Workstation	The high-end operating system, introduced by Microsoft Corporation in 1993, that is optimized to run user applications. Along with Windows 95, Window NT Workstation acts as a client in the Windows NT client-server model. It is a portable 32-bit, preemptive multitasking operating system that features networking, symmetric multiprocessing, multithreading, and security.

winnuke	Sends out-of-band data to port 139 on Windows 95 or Windows NT machines.
WINS	A name resolution service that resolves Windows networking computer names to IP addresses in a routed environment. A WINS server handles name registrations, queries, and releases. See also IP address and routing.
wired equivalency privacy	See WEP.
Wizard	Someone who has detailed knowledge of a complex piece of software or hardware and can fix bugs quickly in an emergency. A superior form of hacker specific to only that piece of software or hardware.
worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. *(RFC 2828)*

X

X.25	ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. X.25 specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded X.25.
X.29	ITU-T recommendation that defines the form for control information in the terminal-to-PAD interface used in X.25 networks.
X.500	ITU-T recommendation specifying a standard for distributed maintenance of files and directories.
X.509	Constitutes a widely accepted basis for a PKI infrastructure, defining data formats and procedures related to the distribution of public keys using certificates digitally signed by CAs.
X.509v3 certificates	Certificate support that allows the IPSec-protected network to scale by providing the equivalent of a digital ID card to each device. When two devices wish to communicate, they exchange digital certificates to prove their identity (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a CA. X.509 is part of the X.500 standard.
Xauth	Deploys IPSec VPNs using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) as your user authentication method. This feature, which is designed for VPN clients, provides a user authentication by prompting the user for username and password and verifies them with the information stored in your TACACS+ or RADIUS database.
XML	eXtensible Markup Language. The universal format for structured documents and data on the Web. *(http://www.w3.org/XML/)*
Xwindow	Distributed, network-transparent, device-independent, multitasking windowing and graphics system originally developed by MIT for communication between X terminals and UNIX workstations.

Y

N/A

Z

ZIP	Maps zone names to network numbers on internet routers.
Zone Information Protocol	See ZIP.

#

3DES	See Triple Data Encryption Standard.