FNS Glossary

A

AAA	AAA is an acronym which stands for Authentication, Authorization, and Accounting. Allows all facets of user security to be defined on a central server. AAA provides identity based services to the network.
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	Access Control Server. ACS software offers centralized command and control for all user authentication, authorization, and accounting from a Web-based, graphical interface, and distributes those controls to hundreds or thousands of access gateways 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	Microsoft's Windows-specific non-Java technique for writing applets. ActiveX applets take considerably longer to download than the equivalent Java applets; however, they more fully exploit the features of Windows 95. ActiveX sometimes is said to be a superset of Java. See also applet and Java Formerly known as Object Linking and Embedding (OLE) or Object Linking and Embedding control (OCX). ActiveX controls create a potential security problem because they can provide a way for someone to attack servers.
AD	administrative domain.[1] A group of hosts, routers, and networks operated and managed by a single organization. [2] Microsoft Active Directory
ADSL	asymmetric digital subscriber line. One of four DSL technologies. ADSL is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. Downstream rates range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair. See also HDSL, SDSL, and VDSL.
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 control	See traffic policing.
AES	Advanced Encryption Standard. AES is a Federal Information Processing Standard (FIPS)-approved cryptographic algorithm which can be used to protect electronic data transmission (FIPS PUB 197). AES is based on the Rijndael algorithm, which specifies how to use keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits (all nine combinations of key length and block length are possible). Both block length and key length can be extended easily to multiples of 32 bits; although the FIPS PUB 197 version of the algorithm only specifies a block length of 128 bits.

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.
Agent (IDS)	The aspect of the Host Sensor system that is installed on each host in your network. An agent serves as a protective layer surrounding a computer's operating system kernel identifying and preventing suspected breaches of security and malicious attacks.
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.
algorithm	Well-defined rule or process for arriving at a solution to a problem. In networking, algorithms commonly are used to determine the best route for traffic from a particular source to a particular destination. Algorithms are also used in all encryption technologies.
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.
API	application program interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
Applet	A small program, often used in the context of a Java-based program, that is compiled and embedded in an HTML page. See also ActiveX and Java.
AppleTalk	A series of communications protocols designed by Apple Computer consisting of two phases. Phase 1, the earlier version, supports a single physical network that can have only one network number and be in one zone. Phase 2 supports multiple logical networks on a single physical network and allows networks to be in more than one zone
AppleTalk Remote Access	See ARA.
application	A program that performs a function directly for a user. FTP and Telnet clients are examples of network applications
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.
AS	A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the IANA. Sometimes abbreviated as *AS*
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.
attack	An assault on system security that derives from an intelligent threat, for example, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system
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).
authorization	The method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.
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. See trap door
Back Orifice (BO)	A program that can give unwanted access and control of a system by way of its Internet link. BO runs on Windows based operating 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.
bandwidth	The amount of information that a computer or transmission medium can hande in a unit of time.
bash	Bourne-again shell. Interactive UNIX shell based on the traditional Bourne shell, but with increased functionality. See also root account.
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.
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 hacking method used to find passwords or encryption keys by trying every possible combination of characters until the code is broken.
bug	An unwanted and unintended property of a program that often causes it to malfunction.
buffer	A storage area used for handling data in transit. Buffers are used in internetworking to compensate for differences in processing speed between network devices. Bursts of data can be stored in buffers until they can be handled by slower processing devices. Sometimes referred to as a *packet buffer*
Buffer overflow	The method of overfilling a software buffer in order to insert and execute some other code with elevated privileges, often a unix shell from which further commands can be issued. .

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 certificate	[Digital] certificate for one CA issued by another CA.
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. Prevents the problems associated with Electronic Codebook (ECB), where every block of "plain text" maps to exactly one block of "cipher text" by having each encrypted block XORed with the previous block of ciphertext. In this way

	identical patterns in different messages are encrypted differently, depending upon the difference in the previous data
CCO	Provides online access to glossaries of networking terminology and acronyms translated into 28 languages and regional dialects.
CCIE Security	Cisco Certified Internetworking Expert. The CCIE Security certification is the top level of Cisco security professionals. The exam covers IP and IP routing as well as specific security components. The two requirements to become a CCIE are a passing grade on the Security qualification exam and a passing grade on the Security lab exam.
CCSP	Cisco Certified Security Professional. The CCSP (Cisco Certified Security Professional) certification provides network professionals with professional level recognition in designing and implementing Cisco secure networks. The required exams are Securing Cisco IOS Networks (SECUR) (Formerly MCNS), Cisco Secure PIX Firewall Advanced (CSPFA),Cisco Secure Intrusion Detection System (CSIDS), Cisco Secure VPN (CSVPN) ,Cisco SAFE Implementation (CSI)
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	Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key
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	Cisco Encryption Technology. 40- and 56-bit Data Encryption Standard (DES) network layer encryption available since Cisco IOS Software Release 11.2
chargen	Character Generation. Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time the client sends a datagram
CGI	Common Gateway Interface. A set of rules that describe how a Web server communicates with another application running on the same computer and how the application (called a CGI program) communicates with the Web server. Any application can be a CGI program if it handles input and output according to the CGI standard.
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.

cipher	Cryptographic algorithm for encryption and decryption
Cipher key	Used to describe the encryption key value. For Data Encryption Standard (DES), a valid encryption key is a 16-byte hexadecimal value
ciphertext	Data that has been transformed by encryption so that its semantic information content (that is, its meaning) is no longer intelligible or directly available
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 Firewall Specialist	Cisco Firewall Specialists focus on securing network access using Cisco IOS Software and Cisco PIX Firewall Technologies. The required exams are Securing Cisco IOS Networks (SECUR) (Formerly MCNS) and Cisco Secure PIX Firewall Advanced (CSPFA)
Cisco VPN Specialist	Cisco VPN Specialists can configure VPNs across shared public networks using Cisco IOS Software and Cisco VPN 3000 Series Concentrator technologies. The required exams are Securing Cisco IOS Networks (SECUR) (Formerly MCNS) and Cisco Secure Virtual Networks (CSVPN)
Cisco IDS Specialist	Cisco IDS Specialists can operate and monitor Cisco IOS Software and IDS technologies to detect and respond to intrusion activities. The required exams are Securing Cisco IOS Networks (SECUR) (Formerly MCNS) and Cisco Secure Intrusion Detection System (CSIDS)
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 Security Appliance	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 Security Appliances and runs on the Windows operating system.
Cisco Systems TAC	Technical Assistance Center. TAC is for all Cisco customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides around-the-clock, award-winning technical support services, online and over the phone.
Cisco VPN Concentrator series	Offers powerful remote access and site-to-site VPN capability, easy-to-use management interface, and a free software 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.
community	In SNMP, a logical group of managed devices and NMSs in the same administrative domain.
Community string	Text string that acts as a password and is used to authenticate messages sent between a management station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the agent. Also called a community name.
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 Security Appliances.
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.
Cookie	piece of information sent by a Web server to a Web browser that the browser is expected to save and send back to the Web server whenever the browser makes additional requests of the Web server.
Coordinated Univeral Time	Coordinated Universal Time (UTC): Time scale, based on the second (SI), as defined and recommended by the CCIR, and maintained by the Bureau International des Poids et Mesures (BIPM). For most practical purposes associated with the Radio Regulations, UTC is equivalent to mean solar time at the prime meridian (0° longitude), formerly expressed in GMT.
Countermeasure	An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
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. See Crypto access list
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.
Cryptographic algorithm	Algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

Cryptographic key	Usually shortened to just "key." Input parameter that varies the transformation performed by a cryptographic algorithm. Typically, the longer the key length, the stronger the encryption.
Cryptoanalysis	Cryptoanalysis is the science of analyzing cryptography. The purpose is to find any errors or weaknesses in the strength of an encryption algorithm.
CSACS	Cisco Secure Access Control 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. Security across a distributed network (formerly called NetRanger).
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. A daemon performs a specific function, such as writing log files, analyzing IP traffic, or processing events.
DARPANET	The network used/created by the Department of Defense's Advanced Research Projects Agency. The agency is responsible for the development of military technology. Funded much of the development of the Internet, including Berkeley UNIX and TCP/IP
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.
DEA	Data Encryption Algorithm. Symmetric block cipher, defined as part of the U.S. Government's Data Encryption Standard. DEA uses a 64-bit key, of which 56 bits are independently chosen and 8 are parity bits, and maps a 64-bit block into another 64-bit block.
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.
Decryption	The process of converting encrypted data back into its original form.
DECnet	Group of communications products (including a protocol suite) developed and supported by Digital Equipment Corporation. DECnet/OSI (also called DECnet Phase V) is the most recent iteration and supports both OSI protocols and proprietary Digital protocols. Phase IV Prime supports inherent MAC addresses that allow DECnet nodes to coexist with systems running other protocols that have MAC address restrictions.
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 Security Appliance, 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].
DES	Data Encryption Standard. A standard that encrypts packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. Data Encryption Standard. Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.
DH	Diffie-Hellman. The Diffie-Hellman algorithm, introduced by Whitfield Diffie and Martin Hellman in 1976, was the first system to utilize "public-key" or "asymmetric" cryptographic keys. Today Diffie-Hellman is part of the IPSec standard. A protocol known as OAKLEY uses Diffie-Hellman, as described in RFC 2412. OAKLEY is used by the Internet Key Exchange (IKE) protocol (see RFC 2401), which is part of the overall framework called Internet Security Association and Key Management Protocol (ISAKMP; see RFC 2408).
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	Value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity
Digital Signature Standard	See DSS.
digital subscriber line	digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel. See also ADSL, HDSL, and VDSL.
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).
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.
DNSIX	Department of Defense Intelligence Information System Network Security for Information Exchange. Collection of security requirements for networking defined by the U.S. Defense Intelligence Agency
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.
DOCSIS	Data-over-Cable Service Interface Specifications. Defines technical specifications for equipment at both subscriber locations and cable operators' headends. Adoption of DOCSIS will accelerate the deployment of data-over-cable services and will ensure interoperability of equipment throughout system operators' infrastructures
DoD	Department of Defense. U.S. government organization that is responsible for national defense. The DoD frequently has funded communication protocol development
DoD Internet	Department of Defense (DoD) Internet. A wide area network to which the ARPANET belongs. See also Internet.
DoS	An attack method whereby a computer is overwhelmed with bogus requests, causing it to crash or keeping it from honoring legitimate requests.
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 Line
DSP	Digita Signal Processor.
DSS	The U.S. Government standard [FP186] that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.
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 Security Appliance 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 authentication 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.
ECDSA	Elliptic Curve Digital Signature Algorithm. Standard [A9062] that is the elliptic curve cryptography analog of the Digital Signature Algorithm
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.
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	Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network. See also tunneling.

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. The conversion of data from plaintext to ciphertext in order to keep the contents secure.
Encryption certificate	Public-key certificate that contains a public key that is intended to be used for encrypting data, rather than for verifying digital signatures or performing other cryptographic functions
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/PKII 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.
ephemeral key	A public key or a private key that is relatively short-lived. See Nonce
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	Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards. See also 10Base2 , 10Base5 , 10BaseF , 10BaseT , 10Broad36 , Fast Ethernet, and IEEE 802.3. .
event	Network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information. See also alarm and trap.
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.g. 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 Security Appliance fails. Specifically, when one PIX Security Appliance fails, another immediately takes its place.
False positive	A security event triggered by a benign process rather than an attack
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	Software tool for determining whether a person has an account at a particular Internet site. Many sites do not allow incoming finger requests . The 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 ser"er "process ta"les" and bring the Internet service prov'der'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. Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
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.
flooding	Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was receivedoriginally
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.
FQDN	fully qualified domain name. FQDN is the full name of a system, rather than just its host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN
fragment	Piece of a larger packet that has been broken down to smaller units

fragmentation	Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet. See also reassembly
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.
FWSM	Firewall Switch Module. A high-end firewall blade which can be used in a Catalyst 6500 Switch or 7600 Series Internet router.
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.
GMT	Greenwich Mean Time (GMT): Mean solar time at the meridian of Greenwich, England, formerly used as a basis for standard time throughout the world.
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.
GRE	Generic Router Encapsulation. A Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types, such as IPX and Appletalk, inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. GRE is defined in RFC 1701.
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.
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 ("he "hash re"ult") which is usually a fixed-size value. See also Hash Algorithm.
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.
HIDS	A security application, or program, that functions by virtue of being installed on and protecting each node (host) in a network. See Agent
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 "he "inherit"nce" 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.
Hijack attack	Form of active wire tapping in which the attacker seizes control of a previously established communication association
HMAC	Hash-based Message Authentication Code. HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, for example, MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.
HMAC MD5	Hashed Message Authentication Codes with MD5 (RFC 2104). A keyed version of MD5 that enables two parties to validate transmitted information using a shared secret
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 Based IDS	See HIDS
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.
Hub	1. Generally, a term used to describe a device that serves as the center of a star-topology network. 2. Hardware or software device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat, but merely split, signals sent through them).

I

IANA	Internet Assigned Numbers Authority. Organization operated under the auspices of the ISOC as a part of the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP stack, including autonomous system numbers. See also ICP cell , ISOC , and InterNIC .
IBNS	Cisco Identity Based Networking Services (IBNS) is an integrated solution combining several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. IBNS primarily controls access via switched or wireless network devices.
ICMP	Internet Control Message Protocol. A network protocol that handles network errors and error messages. The **ping** command uses ICMP.
ICMP Flood	Denial of service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle
IDEA	International Data Encryption Algorithm. Patented, symmetric block cipher that uses a 128-bit key and operates on 64-bit blocks.
Identity	Identity includes core technologies that enable network traffic security: Authentication, Authorization, and Accounting (AAA), Public Key Infrastructure (PKI), Secure Shell (SSH), and Secure Socket Layer (SSL).
Identity Based Network Service	See IBNS
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.
IEEE	Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.
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.
IGMP	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router. See also multicast router.
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 Multicast	Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination group address
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 is defined in RFC 2401.
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.
IPv4	IP version 4. Network layer for the TCP/IP protocol suite. Internet Protocol (version 4) is a connectionless, best-effort packet switching protocol. Defined in RFC 791
IPv6	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
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.
IRC	Internet Relay Chat. World-wide "party line" protocol that allows one to converse with others in real time. IRC is structured as a network of servers, each of which accepts connections from client programs, one per user.
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.
IV	initialization value. Input parameter that sets the starting state of a cryptographic algorithm or mode

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.
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 'ser'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	Process that delivers a cryptographic key from the location where it is generated to the locations where it is used in a cryptographic algorithm
Key Distribution Center	See KDC.
Key establishment	Process that combines the key generation and key distribution steps needed to set up or install a secure communication association.
Key pair	Set of mathematically related keys—a public key and a private key—that are used for asymmetric cryptography and are generated in a way that makes it computationally infeasible to derive the private key from knowledge of the public key
Key recovery	Process for learning the value of a cryptographic key that previously was used to perform some cryptographic operation. Techniques that provide an intentional, alternate (that is, secondary) means to access the key used for data confidentiality service in an encrypted association

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 cust'mer'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: Micro'oft's PPTP and C'sco's L2F. L2TP is the emerging IETF standard, currently being drafted by participants from Ascend, Cisco Systems, Copper Mountain Networks, IBM, Microsoft, and 3Com. L2TP is defined in RFC 2661.
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.
Layer 2 Tunneling Protocol	See L2TP
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	Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
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.
logging	The process of collecting a record of events. Logging of security information is performed on two levels: logging of events (such as IDS commands, errors, and alarms), and logging of individual IP session information

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. Lock-and-key is a traffic filtering security feature that dynamically filters IP protocol traffic
Logical bomb	Malicious logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources
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.
Managed object	In network management, a network device that can be managed by a network management protocol. See SNMP
Management Information Base	See MIB.
Manual Keys	This mode requires no negotiations; it is available for troubleshooting only.
Man-in-the-middle attack	Form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.
masquerade attack	Type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity. See Spoofing
MD4	Message Digest 4. A cryptographic hash that produces a 128-bit hash result and was designed by Ron Rivest.
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 (M"C)	"(The) Message Authentication "ode" 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.)
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 Security Appliance 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.
MPLS	Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information
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.
multicast	Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address Field. Compare with broadcast and unicast.
Multi-layer Switch Feature Card	See MSFC.
Multilevel Information Systems Security Initiative	See MISSi.
multiplex identifier	The number associated with a specific 'ser's L2TP/L2F session.
Multiprotocol Label Switching	See MPLS

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 Security Appliance and specifies its security level (except for the inside and outside PIX Security Appliance 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 enterp'ise's private network.
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as *Network Address Translator*
National Information Infrastructure	See NII.
National Institute of Standards and Technology	See NIST
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 Security Appliances 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 Address Translation	See NAT

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 Based IDS	See NIDS
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*.
NIDS	Network Based IDS. NIDS operates by first detecting an attack occurring at the network level and then either takes a corrective action itself or notifies a management system where an administrator can take action. Attacks are discovered by looking for their signatures in traffic flows in the network. Attack detection triggers NIDS to send an alarm and then take a pre-configured action. The two possible actions are shunning and TCP resets. NIDS consists on appliance based IDS sensors.
NIST	National Institute of Standards and Technology National Institute of Standards and Technology. U.S. government organization that supports and catalogs a variety of standards
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	Network Operations Center
nonce	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 See ephemeral key
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	A Cisco HTML-based encyclopedia of network security information, including vulnerabilities, their associated exploits, and possible countermeasures
NSA	US National Security Agency
Nslookup	A program that provides a host name to corresponding IP address record. It can also do reverse name lookup and find the host name for an IP address you specify.
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	Network Time Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods. 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.
Null Encryption Algorithm	Algorithm [RFC 2410] that does nothing to transform plaintext data; that is, a no-op. It originated because of IPsec ESP, which always specifies the use of an encryption algorithm to provide confidentiality. The NULL encryption algorithm is a convenient way to represent the option of not applying encryption in ESP (or in any other context where this is needed).

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.
OID	object identifier. Values are defined in specific MIB modules. The Event MIB allows a user or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, a user or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both
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.
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. RFC 2289
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 groper	See PING
Packet Internet Exchange Security Appliance	See PIX Security Appliance.
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	Translation method that allows the user to conserve addresses in the global address pool by allowing source ports in TCP connections or UDP conversations to be translated. Different local addresses then map to the same global address, with port translation providing the necessary uniqueness. When translation is required, the new port number is picked out of the same range as the original following the convention of Berkeley Standard Distribution (SD).
Password	Secret data value, usually a character string, that is used as authentication information
Password sniffing	Passive wiretapping or packet sniffing, usually on a local-area network, to gain knowledge of passwords.
PAT	Port Address Translation.
Path discovery	For a digital certificate, the process of finding a set of public-key certificates that comprise a certification path from a trusted key to that specific certificate
Path name	Full name of a DOS, Mac OS, or UNIX file or directory, including all directory and subdirectory names. Consecutive names in a path name typically are separated by a backslash (\) for DOS, a colon (:) for Mac OS, and a forward slash (/) for UNIX
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.
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.
Penetration	Successful, repeatable, unauthorized access to a protected system resource
PEP	Policy Enforcement Points. PIX Security Appliances 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.
PFS	perfect forward secrecy. 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 Security Appliance Syslog Server. A very basic application that lets you view PIX Security Appliance 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.
PGP	Pretty Good Privacy. A technique for encrypting messages that uses the public key method. The pubic key is distributed to those from whom you wish to receive encrypted messages; the private key is held by you to decrypt messages. Developed by Philip Zimmerman; freely available from the Massachusetts Institute of Technology.
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 attack	The method of overwhelming a network with ping commands.

Ping of Death	Attack that sends an improperly large ICMP [R0792] echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash
Ping sweep	Attack that sends ICMP [RFC 0792] echo requests, or pings, to a range of IP addresses with the goal of finding hosts that can be probed for vulnerabilities
PIX Security Appliance	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 Security Appliance Syslog Server	See PFSS.
PKCS	Public-Key Cryptography Standards. Series of specifications published by RSA Laboratories for data structures and algorithm usage for basic applications of asymmetric cryptography
PKCS#10	Public Key Cryptography Standard # 10. A standard syntax from RSA Data Security, Inc. for certificate requests. The PIX Security Appliance 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. System of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
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 address translation	See PAT
Port Scanning	A hacking technique used to check TCP/IP ports to reveal what services are available in order to plan an exploit involving those services, and to determine the operating system of a particular computer.
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. Shared secret key that is used during IKE authentication.
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.
Privilege	Authorization or set of authorizations to perform security-relevant functions, especially in the context of a computer operating system.
Privilege 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.
Privilege Ticket-Granting Ticket	See PTGT.
privileged level	Allows users to issue all commands on the Cisco IOS, including configuration and debug commands.

Privileged 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 Security Appliances.
Probe	Probe is an intrusive analysis technique that uses the information obtained during scanning to more fully interrogate each network device. The probe uses well known exploitation techniques to fully confirm each suspected vulnerability as well as to detect any vulnerabilities that cannot be found using nonintrusive techniques
Proxy	An entity that has the authority to act for another. *See also* proxy client and proxy server.
Proxy arp	proxy Address Resolution Protocol. Variation of the ARP protocol in which an intermediate device (for example, a router) sends an ARP response on behalf of an end node to the requesting host. Proxy ARP can lessen bandwidth use on slow-speed WAN links.
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).
Public key	Publicly shared component of a pair of cryptographic keys used for asymmetric cryptography
Public key certificate	Digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items; a digitally signed data structure that attests to the ownership of a public key.
public key cryptography	Each user has a key-pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. Public key cryptography is the same as public/private key system.
Public key cryptography standards	See PCKS

Q

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

R

RA	registration authority. Optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions
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.
RAT	Router Audit Tool. Provided by the Center for Internet Security (CIS), the Router Audit Tool or RAT was designed to help audit the configurations of Cisco routers quickly and efficiently. The Router Audit Tool performs a baseline test on the configuration of a Cisco Router. The baseline Level 1 is modeled on the Router Security Configuration Guide published by the National Security Agency (NSA) of the United States. The tool provides a list of the potential security vulnerabilities discovered in an easy to read format.
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.).
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.
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.
reassembly	The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node. See also fragmentation.
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.
registration	Administrative act or process whereby an entity's name and other attributes are established for the first time at a CA, prior to the CA issuing a digital certificate that has the entity's name as the subject

Registration authority	See RA
rekey	Change the value of a cryptographic key that is being used in an application of a cryptographic system
Relative Distinguished Name	See RDN.
Remote copy protocol	See rpc
Remote login	See rlogin
Remote Monitoring	See RMON.
Remote Procedure Call	See RPC.
Remote shell protocol	See rsh
Replay attack	Attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack
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.
repository	System for storing and distributing digital certificates and related information (including CRLs, CPSs, and certificate policies) to certificate users
Repudiation	Denial by a system entity that was involved in an association (especially an association that transfers information) of having participated in the relationship
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	remote login. Terminal emulation program, similar to Telnet, offered in most UNIX implementations
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 account	Privileged account on UNIX systems used exclusively by network or system administrators

Root CA	Ultimate CA, which signs the certificates of the subordinate CAs. The root CA has a self-signed certificate that contains its own public key
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.
Root key	Public key for which the matching private key is held by a root.
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.
rsh	remote shell protocol. Protocol that allows a user to execute commands on a remote system without having to log in to the system. For example, rsh can be used to remotely examine the status of a number of access servers without connecting to each communication server, executing the command, and then disconnecting from the communication server
RTCP	Real Time Control Protocol. Duplex (i-directional) 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.
Samba	A program that implements the SMB protocol for UNIX systems, allowing UNIX and NT systems to share files and directories
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.
SCA	subordinate certification authority. CA whose public-key certificate is issued by another (superior) CA
Scalable Encryption Processing modules	See SEP modules.
Scalable Encryption Processor 2	See SEP2.
scan	Scan is a nonintrusive analysis technique that identifies the open ports found on each live network device and collects the associated port banners found as each port is scanned. Each port banner is compared against a table of rules to identify the network device, its operating system, and all potential vulnerabilities.
SCEP	Simple Certificate Enrollment Protocol. Certificate Enrollment Protocol. Certificate management protocol jointly developed by Cisco Systems and VeriSign, Inc. CEP is an early implementation of Certificate Request Syntax (CRS), a standard proposed to the Internet Engineering Task Force (IETF). CEP specifies how a device communicates with a CA, including how to retrieve the public key of the CA, how to enroll a device with the CA, and how to retrieve a certificate revocation list (CRL). CEP uses Public Key Cryptography Standard (PKCS) 7 and PKCS 10 as key component technologies. The public key infrastructure working group (PKIX) of the IETF is working to standardize a protocol for these functions, either CRS or an equivalent.
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.
Secret key	See symmetrical key
Secure Copy	The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that it relies on SSH for security
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 association	See SA
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. SADB
Security Parameter Index	See SPI
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).
Shun	Shun or shunning refers to the Sensor's ability to use a network device to deny entry to a specific network host or an entire network.

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. A signature distills network information and compares it against a rule set that indicates typical intrusion activity.
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	A Denial of Service attack that floods its target with replies to ICMP echo (PING) requests. A smurf attack sends PING requests to internet broadcast addresses, which forward the PING requests to up to 255 hosts on a subnet. The return address of the PING request is spoofed to be the address of the attack target. All hosts receiving the PING requests reply to the attack target, flooding it with replies
Sneaker	Someone hired to test the security of a system by attempting to break into it.
sniffers	An application, program or device that monitors and analyzes network traffic. Sniffers are used by network managers to detect problems with network traffic. They are also used by hackers to steal information. Sniffers are difficult to detect and can be inserted almost anywhere in a network (a primary reason for their popularity among hackers).
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.
SNMPv2	SNMP version 2 adds cryptographic mechanisms based on DES and MD5.
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.
SNMP Trap	A method which specifies the level of notification when using SNMP.
snooping	Passively observing a network.
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.

Soft token	A type of one time passwords. See OTP
SOHO	small office, home office. Networking solutions and access technologies for offices that are not directly connected to large corporate networks.
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	Forging something, such as an IP Address to hide one's location and identity. Spoofing is designed to foil network security mechanisms such as filters and access lists. Also known as a "masquerade attack".
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)*
SSH	Secure Shell (SSH) is an application and a protocol that provides secure replacement for the suite of Berkeley r-tools such as rsh, rlogin and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.
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.
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 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.
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.
subordinate certification authority	See SCA
Switch Port Analyzer	See SPAN.
Symmetric key	Cryptographic key that is used in a symmetric cryptographic algorithm. Also known as a secret key.
Syn Floods	A hacking technique used to cause a denial of service. SYN packets are sent from a client with a spoofed IP address and are sent at a rate faster than the TCP stack on the host is set to time out. As the client address is spoofed, the client sends no SYN-ACK, but continues to flood the host with SYN packets, tying up the resources of the host.
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	Tribal Flood Network. Distributed Denial of Service attacks based on TCP/IP architecture that use a large number of computers to simultaneously attack a target. The attack originates from a single computer controlling several master computers, which in turn each control a number of daemons (other compromised computers). The masters maintain a list of responding daemons, signaling them to initiate the attack. Trinoo floods the target with UDP packets. TFN uses SYN flood, UDP flood, ICMP flood or smurf attack
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.
Token Ring network	Token-passing LAN developed and supported by IBM. Token Ring runs at 4 or 16 Mbps over a ring topology.
Top CA	The highest-level CA (that is, the most trusted CA) in a certification hierarchy
traffic flow	Two paths that follow the same route but travel in opposite directions.
traceroute	Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393
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.
trap	Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. See also alarm and event.
Trap door	Hidden computer flaw known to an intruder, or a hidden computer mechanism (usually software) installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms. See back door
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. In addition to corrupting data or giving away passwords, a rojan horse can open a back door to a system, providing further unwanted access. See also worm, virus.
Trusted certificate	Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path
Trusted key	Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path
Trust-file PKI	Non-hierarchical PKI in which each certificate user has a local file (which is used by application software) of public-key certificates that the user trusts as starting points (that is, roots) for certification paths. Also known as a trust list.
Trust level	Characterization of a standard of security protection to be met by a computer system.
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.
Trusted process	System process that has privileges that enable it to affect the state of system security and that can, therefore, through incorrect or malicious execution, violate the system's security policy
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.
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

uauth	user authentication.
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 Security Appliance 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 Security Appliance. 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.
Untrusted process	System process that cannot affect the state of system security through incorrect or malicious operation, usually because its operation is confined by a security kernel
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.
URL filtering	The process of blocking web sites based on a listing or keyword.
User authentication	See uauth
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.

UTC	Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.
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 Security Appliances 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.
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. Also known as virtual private dial network. A VPDN is a network that extends remote access to a private network using a shared infrastructure. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. VPDNs are a cost effective method of establishing a long distance, point-to-point connection between remote dial users and a private 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 Security Appliance, giving network administrators the ability to effectively monitor and control network traffic. WebSENSE is used to block specific URLs because the PIX Security Appliance 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.

wiretapping	An attack that intercepts and accesses data and other information contained in a flow in a communication system
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 and destroy data.

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.
802.1x	Also called 802.1X for 802.11. 802.1X is the new standard for wireless LAN and switch

	security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). For wireless, an access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network. For switching, see IBNS.

Decimal	Keyword	Description	
1/tcp	tcpmux	TCP Port Service Multiplexer	
1/udp	tcpmux	TCP Port Service Multiplexer	
2/tcp	compressnet	Management Utility	
2/udp	compressnet	Management Utility	
3/tcp	compressnet	Compression Process	
3/udp	compressnet	Compression Process	
5/tcp	rje	Remote Job Entry	
5/udp	rje	Remote Job Entry	
7/tcp	echo	Echo	
7/udp	echo	Echo	
9/tcp	discard	Discard	
9/udp	discard	Discard	
11/tcp	systat	Active Users	
11/udp	systat	Active Users	
13/tcp	daytime	Daytime (RFC 867)	
13/udp	daytime	Daytime (RFC 867)	
17/tcp	qotd	Quote of the Day	
17/udp	qotd	Quote of the Day	
18/tcp	msp	Message Send Protocol	
18/udp	msp	Message Send Protocol	
19/tcp	chargen	Character Generator	
19/udp	chargen	Character Generator	
20/tcp	ftp-data	File Transfer [Default Data]	
20/udp	ftp-data	File Transfer [Default Data]	
21/tcp	ftp	File Transfer [Control]	
21/udp	ftp	File Transfer [Control]	
22/tcp	ssh	SSH Remote Login Protocol	
22/udp	ssh	SSH Remote Login Protocol	
23/tcp	telnet	Telnet	
23/udp	telnet	Telnet	
24/tcp		any private mail system	
24/udp		any private mail system	
25/tcp	smtp	Simple Mail Transfer	
25/udp	smtp	Simple Mail Transfer	
27/tcp	nsw-fe	NSW User System FE	
27/udp	nsw-fe	NSW User System FE	
29/tcp	msg-icp	MSG ICP	
29/udp	msg-icp	MSG ICP	
31/tcp	msg-auth	MSG Authentication	
31/udp	msg-auth	MSG Authentication	
33/tcp	dsp	Display Support Protocol	
33/udp	dsp	Display Support Protocol	
35/tcp		any private printer server	
35/udp		any private printer server	
37/tcp	time	Time	
37/udp	time	Time	
38/tcp	rap	Route Access Protocol	
38/udp	rap	Route Access Protocol	
39/tcp	rlp	Resource Location Protocol	
39/udp	rlp	Resource Location Protocol	
41/tcp	graphics	Graphics	
41/udp	graphics	Graphics	
42/tcp	name	Host Name Server	
42/udp	name	Host Name Server	
42/tcp	nameserver	Host Name Server	
42/udp	nameserver	Host Name Server	
43/tcp	nicname	Who Is	

43/udp	nicname	Who Is	
44/tcp	mpm-flags	MPM FLAGS Protocol	
44/udp	mpm-flags	MPM FLAGS Protocol	
45/tcp	mpm	Message Processing Module [recv]	
45/udp	mpm	Message Processing Module [recv]	
46/tcp	mpm-snd	MPM [default send]	
46/udp	mpm-snd	MPM [default send]	
47/tcp	ni-ftp	NI FTP	
47/udp	ni-ftp	NI FTP	
48/tcp	auditd	Digital Audit Daemon	
48/udp	auditd	Digital Audit Daemon	
49/tcp	tacacs	Login Host Protocol (TACACS)	
49/udp	tacacs	Login Host Protocol (TACACS)	
50/tcp	re-mail-ck	Remote Mail Checking Protocol	
50/udp	re-mail-ck	Remote Mail Checking Protocol	
51/tcp	la-maint	IMP Logical Address Maintenance	
51/udp	la-maint	IMP Logical Address Maintenance	
52/tcp	xns-time	XNS Time Protocol	
52/udp	xns-time	XNS Time Protocol	
53/tcp	domain	Domain Name Server	
53/udp	domain	Domain Name Server	
54/tcp	xns-ch	XNS Clearinghouse	
54/udp	xns-ch	XNS Clearinghouse	
55/tcp	isi-gl	ISI Graphics Language	
55/udp	isi-gl	ISI Graphics Language	
56/tcp	xns-auth	XNS Authentication	
56/udp	xns-auth	XNS Authentication	
57/tcp		any private terminal access	
57/udp		any private terminal access	
58/tcp	xns-mail	XNS Mail	
58/udp	xns-mail	XNS Mail	
59/tcp		any private file service	
59/udp		any private file service	
61/tcp	ni-mail	NI MAIL	
61/udp	ni-mail	NI MAIL	
62/tcp	acas	ACA Services	
62/udp	acas	ACA Services	
63/tcp	whois++	whois++	
63/udp	whois++	whois++	
64/tcp	covia	Communications Integrator (CI)	
64/udp	covia	Communications Integrator (CI)	
65/tcp	tacacs-ds	TACACS-Database Service	
65/udp	tacacs-ds	TACACS-Database Service	
66/tcp	sql*net	Oracle SQL*NET	
66/udp	sql*net	Oracle SQL*NET	
67/tcp	bootps	Bootstrap Protocol Server	
67/udp	bootps	Bootstrap Protocol Server	
68/tcp	bootpc	Bootstrap Protocol Client	
68/udp	bootpc	Bootstrap Protocol Client	
69/tcp	tftp	Trivial File Transfer	
69/udp	tftp	Trivial File Transfer	
70/tcp	gopher	Gopher	
70/udp	gopher	Gopher	
71/tcp	netrjs-1	Remote Job Service	
71/udp	netrjs-1	Remote Job Service	
72/tcp	netrjs-2	Remote Job Service	
72/udp	netrjs-2	Remote Job Service	
73/tcp	netrjs-3	Remote Job Service	

Port Numbers

73/udp	netrjs-3	Remote Job Service	
74/tcp	netrjs-4	Remote Job Service	
74/udp	netrjs-4	Remote Job Service	
75/tcp		any private dial out service	
75/udp		any private dial out service	
76/tcp	deos	Distributed External Object Store	
76/udp	deos	Distributed External Object Store	
77/tcp		any private RJE service	
77/udp		any private RJE service	
78/tcp	vettcp	vettcp	
78/udp	vettcp	vettcp	
79/tcp	finger	Finger	
79/udp	finger	Finger	
80/tcp	http	World Wide Web HTTP	
80/udp	http	World Wide Web HTTP	
80/tcp	www	World Wide Web HTTP	
80/udp	www	World Wide Web HTTP	
80/tcp	www-http	World Wide Web HTTP	
80/udp	www-http	World Wide Web HTTP	
81/tcp	hosts2-ns	HOSTS2 Name Server	
81/udp	hosts2-ns	HOSTS2 Name Server	
82/tcp	xfer	XFER Utility	
82/udp	xfer	XFER Utility	
83/tcp	mit-ml-dev	MIT ML Device	
83/udp	mit-ml-dev	MIT ML Device	
84/tcp	ctf	Common Trace Facility	
84/udp	ctf	Common Trace Facility	
85/tcp	mit-ml-dev	MIT ML Device	
85/udp	mit-ml-dev	MIT ML Device	
86/tcp	mfcobol	Micro Focus Cobol	
86/udp	mfcobol	Micro Focus Cobol	
87/tcp		any private terminal link	
87/udp		any private terminal link	
88/tcp	kerberos	Kerberos	
88/udp	kerberos	Kerberos	
89/tcp	su-mit-tg	SU/MIT Telnet Gateway	
89/udp	su-mit-tg	SU/MIT Telnet Gateway	
90 also	########### PORT	being used unofficially by Pointcast #########	
90/tcp	dnsix	DNSIX Securit Attribute Token Map	
90/udp	dnsix	DNSIX Securit Attribute Token Map	
91/tcp	mit-dov	MIT Dover Spooler	
91/udp	mit-dov	MIT Dover Spooler	
92/tcp	npp	Network Printing Protocol	
92/udp	npp	Network Printing Protocol	
93/tcp	dcp	Device Control Protocol	
93/udp	dcp	Device Control Protocol	
94/tcp	objcall	Tivoli Object Dispatcher	
94/udp	objcall	Tivoli Object Dispatcher	
95/tcp	supdup	SUPDUP	
95/udp	supdup	SUPDUP	
96/tcp	dixie	DIXIE Protocol Specification	
96/udp	dixie	DIXIE Protocol Specification	
97/tcp	swift-rvf	Swift Remote Virtural File Protocol	
97/udp	swift-rvf	Swift Remote Virtural File Protocol	
98/tcp	tacnews	TAC News	
98/udp	tacnews	TAC News	
99/tcp	metagram	Metagram Relay	
99/udp	metagram	Metagram Relay	

100/tcp	newacct	[unauthorized use]	
101/tcp	hostname	NIC Host Name Server	
101/udp	hostname	NIC Host Name Server	
102/tcp	iso-tsap	ISO-TSAP Class 0	
102/udp	iso-tsap	ISO-TSAP Class 0	
103/tcp	gppitnp	Genesis Point-to-Point Trans Net	
103/udp	gppitnp	Genesis Point-to-Point Trans Net	
104/tcp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300	
104/udp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300	
105/tcp	cso	CCSO name server protocol	
105/udp	cso	CCSO name server protocol	
105/tcp	csnet-ns	Mailbox Name Nameserver	
105/udp	csnet-ns	Mailbox Name Nameserver	
106/tcp	3com-tsmux	3COM-TSMUX	
106/udp	3com-tsmux	3COM-TSMUX	
107/tcp	rtelnet	Remote Telnet Service	
107/udp	rtelnet	Remote Telnet Service	
108/tcp	snagas	SNA Gateway Access Server	
108/udp	snagas	SNA Gateway Access Server	
109/tcp	pop2	Post Office Protocol - Version 2	
109/udp	pop2	Post Office Protocol - Version 2	
110/tcp	pop3	Post Office Protocol - Version 3	
110/udp	pop3	Post Office Protocol - Version 3	
111/tcp	sunrpc	SUN Remote Procedure Call	
111/udp	sunrpc	SUN Remote Procedure Call	
112/tcp	mcidas	McIDAS Data Transmission Protocol	
112/udp	mcidas	McIDAS Data Transmission Protocol	
113/tcp	ident		
113/tcp	auth	Authentication Service	
113/udp	auth	Authentication Service	
114/tcp	audionews	Audio News Multicast	
114/udp	audionews	Audio News Multicast	
115/tcp	sftp	Simple File Transfer Protocol	
115/udp	sftp	Simple File Transfer Protocol	
116/tcp	ansanotify	ANSA REX Notify	
116/udp	ansanotify	ANSA REX Notify	
117/tcp	uucp-path	UUCP Path Service	
117/udp	uucp-path	UUCP Path Service	
118/tcp	sqlserv	SQL Services	
118/udp	sqlserv	SQL Services	
119/tcp	nntp	Network News Transfer Protocol	
119/udp	nntp	Network News Transfer Protocol	
120/tcp	cfdptkt	CFDPTKT	
120/udp	cfdptkt	CFDPTKT	
121/tcp	erpc	Encore Expedited Remote Pro.Call	
121/udp	erpc	Encore Expedited Remote Pro.Call	
122/tcp	smakynet	SMAKYNET	
122/udp	smakynet	SMAKYNET	
123/tcp	ntp	Network Time Protocol	
123/udp	ntp	Network Time Protocol	
124/tcp	ansatrader	ANSA REX Trader	
124/udp	ansatrader	ANSA REX Trader	
125/tcp	locus-map	Locus PC-Interface Net Map Ser	
125/udp	locus-map	Locus PC-Interface Net Map Ser	
126/tcp	#unitary	Unisys Unitary Login	
126/udp	#unitary	Unisys Unitary Login	
127/tcp	locus-con	Locus PC-Interface Conn Server	
127/udp	locus-con	Locus PC-Interface Conn Server	

Port Numbers

128/tcp	gss-xlicen	GSS X License Verification	
128/udp	gss-xlicen	GSS X License Verification	
129/tcp	pwdgen	Password Generator Protocol	
129/udp	pwdgen	Password Generator Protocol	
130/tcp	cisco-fna	cisco FNATIVE	
130/udp	cisco-fna	cisco FNATIVE	
131/tcp	cisco-tna	cisco TNATIVE	
131/udp	cisco-tna	cisco TNATIVE	
132/tcp	cisco-sys	cisco SYSMAINT	
132/udp	cisco-sys	cisco SYSMAINT	
133/tcp	statsrv	Statistics Service	
133/udp	statsrv	Statistics Service	
134/tcp	ingres-net	INGRES-NET Service	
134/udp	ingres-net	INGRES-NET Service	
135/tcp	epmap	DCE endpoint resolution	
135/udp	epmap	DCE endpoint resolution	
136/tcp	profile	PROFILE Naming System	
136/udp	profile	PROFILE Naming System	
137/tcp	netbios-ns	NETBIOS Name Service	
137/udp	netbios-ns	NETBIOS Name Service	
138/tcp	netbios-dgm	NETBIOS Datagram Service	
138/udp	netbios-dgm	NETBIOS Datagram Service	
139/tcp	netbios-ssn	NETBIOS Session Service	
139/udp	netbios-ssn	NETBIOS Session Service	
140/tcp	emfis-data	EMFIS Data Service	
140/udp	emfis-data	EMFIS Data Service	
141/tcp	emfis-cntl	EMFIS Control Service	
141/udp	emfis-cntl	EMFIS Control Service	
142/tcp	bl-idm	Britton-Lee IDM	
142/udp	bl-idm	Britton-Lee IDM	
143/tcp	imap	Internet Message Access Protocol	
143/udp	imap	Internet Message Access Protocol	
145/tcp	uaac	UAAC Protocol	
145/udp	uaac	UAAC Protocol	
146/tcp	iso-tp0	ISO-IP0	
146/udp	iso-tp0	ISO-IP0	
147/tcp	iso-ip	ISO-IP	
147/udp	iso-ip	ISO-IP	
148/tcp	jargon	Jargon	
148/udp	jargon	Jargon	
149/tcp	aed-512	AED 512 Emulation Service	
149/udp	aed-512	AED 512 Emulation Service	
150/tcp	sql-net	SQL-NET	
150/udp	sql-net	SQL-NET	
151/tcp	hems	HEMS	
151/udp	hems	HEMS	
152/tcp	bftp	Background File Transfer Program	
152/udp	bftp	Background File Transfer Program	
153/tcp	sgmp	SGMP	
153/udp	sgmp	SGMP	
154/tcp	netsc-prod	NETSC	
154/udp	netsc-prod	NETSC	
155/tcp	netsc-dev	NETSC	
155/udp	netsc-dev	NETSC	
156/tcp	sqlsrv	SQL Service	
156/udp	sqlsrv	SQL Service	
157/tcp	knet-cmp	KNET/VM Command/Message Protocol	
157/udp	knet-cmp	KNET/VM Command/Message Protocol	

158/tcp	pcmail-srv	PCMail Server	
158/udp	pcmail-srv	PCMail Server	
159/tcp	nss-routing	NSS-Routing	
159/udp	nss-routing	NSS-Routing	
160/tcp	sgmp-traps	SGMP-TRAPS	
160/udp	sgmp-traps	SGMP-TRAPS	
161/tcp	snmp	SNMP	
161/udp	snmp	SNMP	
162/tcp	snmptrap	SNMPTRAP	
162/udp	snmptrap	SNMPTRAP	
163/tcp	cmip-man	CMIP/TCP Manager	
163/udp	cmip-man	CMIP/TCP Manager	
164/tcp	cmip-agent	CMIP/TCP Agent	
164/udp	smip-agent	CMIP/TCP Agent	
165/tcp	xns-courier	Xerox	
165/udp	xns-courier	Xerox	
166/tcp	s-net	Sirius Systems	
166/udp	s-net	Sirius Systems	
167/tcp	namp	NAMP	
167/udp	namp	NAMP	
168/tcp	rsvd	RSVD	
168/udp	rsvd	RSVD	
169/tcp	send	SEND	
169/udp	send	SEND	
170/tcp	print-srv	Network PostScript	
170/udp	print-srv	Network PostScript	
171/tcp	multiplex	Network Innovations Multiplex	
171/udp	multiplex	Network Innovations Multiplex	
172/tcp	cl/1	Network Innovations CL/1	
172/udp	cl/1	Network Innovations CL/1	
173/tcp	xyplex-mux	Xyplex	
173/udp	xyplex-mux	Xyplex	
174/tcp	mailq	MAILQ	
174/udp	mailq	MAILQ	
175/tcp	vmnet	VMNET	
175/udp	vmnet	VMNET	
176/tcp	genrad-mux	GENRAD-MUX	
176/udp	genrad-mux	GENRAD-MUX	
177/tcp	xdmcp	X Display Manager Control Protocol	
177/udp	xdmcp	X Display Manager Control Protocol	
178/tcp	nextstep	NextStep Window Server	
178/udp	nextstep	NextStep Window Server	
179/tcp	bgp	Border Gateway Protocol	
179/udp	bgp	Border Gateway Protocol	
180/tcp	ris	Intergraph	
180/udp	ris	Intergraph	
181/tcp	unify	Unify	
181/udp	unify	Unify	
182/tcp	audit	Unisys Audit SITP	
182/udp	audit	Unisys Audit SITP	
183/tcp	ocbinder	OCBinder	
183/udp	ocbinder	OCBinder	
184/tcp	ocserver	OCServer	
184/udp	ocserver	OCServer	
185/tcp	remote-kis	Remote-KIS	
185/udp	remote-kis	Remote-KIS	
186/tcp	kis	KIS Protocol	
186/udp	kis	KIS Protocol	

Port Numbers

187/tcp	aci	Application Communication Interface	
187/udp	aci	Application Communication Interface	
188/tcp	mumps	Plus Five's MUMPS	
188/udp	mumps	Plus Five's MUMPS	
189/tcp	qft	Queued File Transport	
189/udp	qft	Queued File Transport	
190/tcp	gacp	Gateway Access Control Protocol	
190/udp	gacp	Gateway Access Control Protocol	
191/tcp	prospero	Prospero Directory Service	
191/udp	prospero	Prospero Directory Service	
192/tcp	osu-nms	OSU Network Monitoring System	
192/udp	osu-nms	OSU Network Monitoring System	
193/tcp	srmp	Spider Remote Monitoring Protocol	
193/udp	srmp	Spider Remote Monitoring Protocol	
194/tcp	irc	Internet Relay Chat Protocol	
194/udp	irc	Internet Relay Chat Protocol	
195/tcp	dn6-nlm-aud	DNSIX Network Level Module Audit	
195/udp	dn6-nlm-aud	DNSIX Network Level Module Audit	
196/tcp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir	
196/udp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir	
197/tcp	dls	Directory Location Service	
197/udp	dls	Directory Location Service	
198/tcp	dls-mon	Directory Location Service Monitor	
198/udp	dls-mon	Directory Location Service Monitor	
199/tcp	smux	SMUX	
199/udp	smux	SMUX	
200/tcp	src	IBM System Resource Controller	
200/udp	src	IBM System Resource Controller	
201/tcp	at-rtmp	AppleTalk Routing Maintenance	
201/udp	at-rtmp	AppleTalk Routing Maintenance	
202/tcp	at-nbp	AppleTalk Name Binding	
202/udp	at-nbp	AppleTalk Name Binding	
203/tcp	at-3	AppleTalk Unused	
203/udp	at-3	AppleTalk Unused	
204/tcp	at-echo	AppleTalk Echo	
204/udp	at-echo	AppleTalk Echo	
205/tcp	at-5	AppleTalk Unused	
205/udp	at-5	AppleTalk Unused	
206/tcp	at-zis	AppleTalk Zone Information	
206/udp	at-zis	AppleTalk Zone Information	
207/tcp	at-7	AppleTalk Unused	
207/udp	at-7	AppleTalk Unused	
208/tcp	at-8	AppleTalk Unused	
208/udp	at-8	AppleTalk Unused	
209/tcp	qmtp	The Quick Mail Transfer Protocol	
209/udp	qmtp	The Quick Mail Transfer Protocol	
210/tcp	z39.50	ANSI Z39.50	
210/udp	z39.50	ANSI Z39.50	
211/tcp	914c/g	Texas Instruments 914C/G Terminal	
211/udp	914c/g	Texas Instruments 914C/G Terminal	
212/tcp	anet	ATEXSSTR	
212/udp	anet	ATEXSSTR	
213/tcp	ipx	IPX	
213/udp	ipx	IPX	
214/tcp	vmpwscs	VM PWSCS	
214/udp	vmpwscs	VM PWSCS	
215/tcp	softpc	Insignia Solutions	
215/udp	softpc	Insignia Solutions	

Port Numbers

216/tcp	CAllic	Computer Associates Int'l License Server	
216/udp	CAllic	Computer Associates Int'l License Server	
217/tcp	dbase	dBASE Unix	
217/udp	dbase	dBASE Unix	
218/tcp	mpp	Netix Message Posting Protocol	
218/udp	mpp	Netix Message Posting Protocol	
219/tcp	uarps	Unisys ARPs	
219/udp	uarps	Unisys ARPs	
220/tcp	imap3	Interactive Mail Access Protocol v3	
220/udp	imap3	Interactive Mail Access Protocol v3	
221/tcp	fln-spx	Berkeley rlogind with SPX auth	
221/udp	fln-spx	Berkeley rlogind with SPX auth	
222/tcp	rsh-spx	Berkeley rshd with SPX auth	
222/udp	rsh-spx	Berkeley rshd with SPX auth	
223/tcp	cdc	Certificate Distribution Center	
223/udp	cdc	Certificate Distribution Center	
225-241	#	Reserved	
242/tcp	direct	Direct	
242/udp	direct	Direct	
243/tcp	sur-meas	Survey Measurement	
243/udp	sur-meas	Survey Measurement	
244/tcp	inbusiness	inbusiness	
244/udp	inbusiness	inbusiness	
245/tcp	link	LINK	
245/udp	link	LINK	
246/tcp	dsp3270	Display Systems Protocol	
246/udp	dsp3270	Display Systems Protocol	
247/tcp	subntbcst_tftp	SUBNTBCST_TFTP	
247/udp	subntbcst_tftp	SUBNTBCST_TFTP	
249-255	#	Reserved	
256/tcp	rap	RAP	
256/udp	rap	RAP	
257/tcp	set	Secure Electronic Transaction	
257/udp	set	Secure Electronic Transaction	
258/tcp	yak-chat	Yak Winsock Personal Chat	
258/udp	yak-chat	Yak Winsock Personal Chat	
259/tcp	esro-gen	Efficient Short Remote Operations	
259/udp	esro-gen	Efficient Short Remote Operations	
260/tcp	openport	Openport	
260/udp	openport	Openport	
286/tcp	fxp-1	FXP-1	
286/udp	fxp-1	FXP-1	
287/tcp	k-block	K-BLOCK	
287/udp	k-block	K-BLOCK	
288-307	#	Unassigned	
309/tcp	entrusttime	EntrustTime	
309/udp	entrusttime	EntrustTime	
344/tcp	pdap	Prospero Data Access Protocol	
344/udp	pdap	Prospero Data Access Protocol	
345/tcp	pawserv	Perf Analysis Workbench	
345/udp	pawserv	Perf Analysis Workbench	
346/tcp	zserv	Zebra server	
346/udp	zserv	Zebra server	
347/tcp	fatserv	Fatmen Server	
347/udp	fatserv	Fatmen Server	
348/tcp	csi-sgwp	Cabletron Management Protocol	
348/udp	csi-sgwp	Cabletron Management Protocol	
349/tcp	mftp	mftp	

Port Numbers

349/udp	mftp	mftp	
371/tcp	clearcase	Clearcase	
371/udp	clearcase	Clearcase	
372/tcp	ulistproc	ListProcessor	
372/udp	ulistproc	ListProcessor	
373/tcp	legent-1	Legent Corporation	
373/udp	legent-1	Legent Corporation	
374/tcp	legent-2	Legent Corporation	
374/udp	legent-2	Legent Corporation	
375/tcp	hassle	Hassle	
375/udp	hassle	Hassle	
376/tcp	nip	Amiga Envoy Network Inquiry Proto	
376/udp	nip	Amiga Envoy Network Inquiry Proto	
377/tcp	tnETOS	NEC Corporation	
377/udp	tnETOS	NEC Corporation	
378/tcp	dsETOS	NEC Corporation	
378/udp	dsETOS	NEC Corporation	
379/tcp	is99c	TIA/EIA/IS-99 modem client	
379/udp	is99c	TIA/EIA/IS-99 modem client	
380/tcp	is99s	TIA/EIA/IS-99 modem server	
380/udp	is99s	TIA/EIA/IS-99 modem server	
381/tcp	hp-collector	hp performance data collector	
381/udp	hp-collector	hp performance data collector	
382/tcp	hp-managed-node	hp performance data managed node	
382/udp	hp-managed-node	hp performance data managed node	
383/tcp	hp-alarm-mgr	hp performance data alarm manager	
383/udp	hp-alarm-mgr	hp performance data alarm manager	
384/tcp	arns	A Remote Network Server System	
384/udp	arns	A Remote Network Server System	
385/tcp	ibm-app	IBM Application	
385/udp	ibm-app	IBM Application	
386/tcp	asa	ASA Message Router Object Def.	
386/udp	asa	ASA Message Router Object Def.	
387/tcp	aurp	Appletalk Update-Based Routing Pro.	
387/udp	aurp	Appletalk Update-Based Routing Pro.	
388/tcp	unidata-ldm	Unidata LDM	
388/udp	unidata-ldm	Unidata LDM	
389/tcp	#	Lightweight Directory Access Protocol	
389/udp	ldap	Lightweight Directory Access Protocol	
390/tcp	uis	UIS	
390/udp	uis	UIS	
391/tcp	synotics-relay	SynOptics SNMP Relay Port	
391/udp	synotics-relay	SynOptics SNMP Relay Port	
392/tcp	synotics-broker	SynOptics Port Broker Port	
392/udp	synotics-broker	SynOptics Port Broker Port	
393/tcp	meta5	Meta5	
393/udp	meta5	Meta5	
394/tcp	embl-ndt	EMBL Nucleic Data Transfer	
394/udp	embl-ndt	EMBL Nucleic Data Transfer	
395/tcp	netcp	NETscout Control Protocol	
395/udp	netcp	NETscout Control Protocol	
396/tcp	netware-ip	Novell Netware over IP	
396/udp	netware-ip	Novell Netware over IP	
397/tcp	mptn	Multi Protocol Trans. Net.	
397/udp	mptn	Multi Protocol Trans. Net.	
398/tcp	kryptolan	Kryptolan	
398/udp	kryptolan	Kryptolan	
399/tcp	iso-tsap-c2	ISO Transport Class 2 Non-Control over TCP	

Port Numbers

399/udp	iso-tsap-c2	ISO Transport Class 2 Non-Control over TCP	
400/tcp	work-sol	Workstation Solutions	
400/udp	work-sol	Workstation Solutions	
401/tcp	ups	Uninterruptible Power Supply	
401/udp	ups	Uninterruptible Power Supply	
402/tcp	genie	Genie Protocol	
402/udp	genie	Genie Protocol	
403/tcp	decap	decap	
403/udp	decap	decap	
404/tcp	nced	nced	
404/udp	nced	nced	
405/tcp	ncld	ncld	
405/udp	ncld	ncld	
406/tcp	imsp	Interactive Mail Support Protocol	
406/udp	imsp	Interactive Mail Support Protocol	
407/tcp	timbuktu	Timbuktu	
407/udp	timbuktu	Timbuktu	
408/tcp	prm-sm	Prospero Resource Manager Sys. Man.	
408/udp	prm-sm	Prospero Resource Manager Sys. Man.	
409/tcp	prm-nm	Prospero Resource Manager Node Man.	
409/udp	prm-nm	Prospero Resource Manager Node Man.	
410/tcp	decladebug	DECLadebug Remote Debug Protocol	
410/udp	decladebug	DECLadebug Remote Debug Protocol	
411/tcp	rmt	Remote MT Protocol	
411/udp	rmt	Remote MT Protocol	
412/tcp	synoptics-trap	Trap Convention Port	
412/udp	synoptics-trap	Trap Convention Port	
413/tcp	smsp	Storage Management Services Protocol	
413/udp	smsp	Storage Management Services Protocol	
414/tcp	infoseek	InfoSeek	
414/udp	infoseek	InfoSeek	
415/tcp	bnet	BNet	
415/udp	bnet	BNet	
416/tcp	silverplatter	Silverplatter	
416/udp	silverplatter	Silverplatter	
417/tcp	onmux	Onmux	
417/udp	onmux	Onmux	
418/tcp	hyper-g	Hyper-G	
418/udp	hyper-g	Hyper-G	
419/tcp	ariel1	Ariel	
419/udp	ariel1	Ariel	
420/tcp	smpte	SMPTE	
420/udp	smpte	SMPTE	
421/tcp	ariel2	Ariel	
421/udp	ariel2	Ariel	
422/tcp	ariel3	Ariel	
422/udp	ariel3	Ariel	
423/tcp	opc-job-start	IBM Operations Planning and Control Start	
423/udp	opc-job-start	IBM Operations Planning and Control Start	
424/tcp	opc-job-track	IBM Operations Planning and Control Track	
424/udp	opc-job-track	IBM Operations Planning and Control Track	
425/tcp	icad-el	ICAD	
425/udp	icad-el	ICAD	
426/tcp	smartsdp	smartsdp	
426/udp	smartsdp	smartsdp	
427/tcp	svrloc	Server Location	
427/udp	svrloc	Server Location	
428/tcp	ocs_cmu	OCS_CMU	

Port Numbers

428/udp	ocs_cmu	OCS_CMU	
429/tcp	ocs_amu	OCS_AMU	
429/udp	ocs_amu	OCS_AMU	
430/tcp	utmpsd	UTMPSD	
430/udp	utmpsd	UTMPSD	
431/tcp	utmpcd	UTMPCD	
431/udp	utmpcd	UTMPCD	
432/tcp	iasd	IASD	
432/udp	iasd	IASD	
433/tcp	nnsp	NNSP	
433/udp	nnsp	NNSP	
434/tcp	mobileip-agent	MobileIP-Agent	
434/udp	mobileip-agent	MobileIP-Agent	
435/tcp	mobilip-mn	MobilIP-MN	
435/udp	mobilip-mn	MobilIP-MN	
436/tcp	dna-cml	DNA-CML	
436/udp	dna-cml	DNA-CML	
437/tcp	comscm	comscm	
437/udp	comscm	comscm	
438/tcp	dsfgw	dsfgw	
438/udp	dsfgw	dsfgw	
439/tcp	dasp	dasp Thomas Obermair	
439/udp	dasp	dasp tommy@inlab.m.eunet.de	
440/tcp	sgcp	sgcp	
440/udp	sgcp	sgcp	
441/tcp	decvms-sysmgt	decvms-sysmgt	
441/udp	decvms-sysmgt	decvms-sysmgt	
442/tcp	cvc_hostd	cvc_hostd	
442/udp	cvc_hostd	cvc_hostd	
443/tcp	https	http protocol over TLS/SSL	
443/udp	https	http protocol over TLS/SSL	
444/tcp	snpp	Simple Network Paging Protocol	
444/udp	snpp	Simple Network Paging Protocol	
445/tcp	microsoft-ds	Microsoft-DS	
445/udp	microsoft-ds	Microsoft-DS	
446/tcp	ddm-rdb	DDM-RDB	
446/udp	ddm-rdb	DDM-RDB	
447/tcp	ddm-dfm	DDM-RFM	
447/udp	ddm-dfm	DDM-RFM	
448/tcp	ddm-ssl	DDM-SSL	
448/udp	ddm-ssl	DDM-SSL	
449/tcp	as-servermap	AS Server Mapper	
449/udp	as-servermap	AS Server Mapper	
450/tcp	tserver	TServer	
450/udp	tserver	TServer	
451/tcp	sfs-smp-net	Cray Network Semaphore server	
451/udp	sfs-smp-net	Cray Network Semaphore server	
453/tcp	creativeserver	CreativeServer	
453/udp	creativeserver	CreativeServer	
454/tcp	contentserver	ContentServer	
454/udp	contentserver	ContentServer	
455/tcp	creativepartnr	CreativePartnr	
455/udp	creativepartnr	CreativePartnr	
456/tcp	macon-tcp	macon-tcp	
456/udp	macon-udp	macon-udp	
457/tcp	scohelp	scohelp	
457/udp	scohelp	scohelp	
458/tcp	appleqtc	apple quick time	

Port Numbers

458/udp	appleqtc	apple quick time	
459/tcp	ampr-rcmd	ampr-rcmd	
459/udp	ampr-rcmd	ampr-rcmd	
460/tcp	skronk	skronk	
460/udp	skronk	skronk	
461/tcp	datasurfsrv	DataRampSrv	
461/udp	datasurfsrv	DataRampSrv	
462/tcp	datasurfsrvsec	DataRampSrvSec	
462/udp	datasurfsrvsec	DataRampSrvSec	
463/tcp	alpes	alpes	
463/udp	alpes	alpes	
464/tcp	kpasswd	kpasswd	
464/udp	kpasswd	kpasswd	
466/tcp	digital-vrc	digital-vrc	
466/udp	digital-vrc	digital-vrc	
467/tcp	mylex-mapd	mylex-mapd	
467/udp	mylex-mapd	mylex-mapd	
468/tcp	photuris	proturis	
468/udp	photuris	proturis	
469/tcp	rcp	Radio Control Protocol	
469/udp	rcp	Radio Control Protocol	
470/tcp	scx-proxy	scx-proxy	
470/udp	scx-proxy	scx-proxy	
471/tcp	mondex	Mondex	
471/udp	mondex	Mondex	
472/tcp	ljk-login	ljk-login	
472/udp	ljk-login	ljk-login	
473/tcp	hybrid-pop	hybrid-pop	
473/udp	hybrid-pop	hybrid-pop	
474/tcp	tn-tl-w1	tn-tl-w1	
474/udp	tn-tl-w2	tn-tl-w2	
475/tcp	tcpnethaspsrv	tcpnethaspsrv	
475/udp	tcpnethaspsrv	tcpnethaspsrv	
476/tcp	tn-tl-fd1	tn-tl-fd1	
476/udp	tn-tl-fd1	tn-tl-fd1	
477/tcp	ss7ns	ss7ns	
477/udp	ss7ns	ss7ns	
478/tcp	spsc	spsc	
478/udp	spsc	spsc	
479/tcp	iafserver	iafserver	
479/udp	iafserver	iafserver	
480/tcp	iafdbase	iafdbase	
480/udp	iafdbase	iafdbase	
481/tcp	ph	Ph service	
481/udp	ph	Ph service	
482/tcp	bgs-nsi	bgs-nsi	
482/udp	bgs-nsi	bgs-nsi	
483/tcp	ulpnet	ulpnet	
483/udp	ulpnet	ulpnet	
484/tcp	integra-sme	Integra Software Management Environment	
484/udp	integra-sme	Integra Software Management Environment	
485/tcp	powerburst	Air Soft Power Burst	
485/udp	powerburst	Air Soft Power Burst	
486/tcp	avian	avian	
486/udp	avian	avian	
487/tcp	saft	saft Simple Asynchronous File Transfer	
487/udp	saft	saft Simple Asynchronous File Transfer	
488/tcp	gss-http	gss-http	

Port Numbers

488/udp	gss-http	gss-http	
489/tcp	nest-protocol	nest-protocol	
489/udp	nest-protocol	nest-protocol	
490/tcp	micom-pfs	micom-pfs	
490/udp	micom-pfs	micom-pfs	
491/tcp	go-login	go-login	
491/udp	go-login	go-login	
492/tcp	ticf-1	Transport Independent Convergence for FNA	
492/udp	ticf-1	Transport Independent Convergence for FNA	
493/tcp	ticf-2	Transport Independent Convergence for FNA	
493/udp	ticf-2	Transport Independent Convergence for FNA	
494/tcp	pov-ray	POV-Ray	
494/udp	pov-ray	POV-Ray	
495/tcp	intecourier	intecourier	
495/udp	intecourier	intecourier	
496/tcp	pim-rp-disc	PIM-RP-DISC	
496/udp	pim-rp-disc	PIM-RP-DISC	
497/tcp	dantz	dantz	
497/udp	dantz	dantz	
498/tcp	siam	siam	
498/udp	siam	siam	
499/tcp	iso-ill	ISO ILL Protocol	
499/udp	iso-ill	ISO ILL Protocol	
500/tcp	isakmp	isakmp	
500/udp	isakmp	isakmp	
501/tcp	stmf	STMF	
501/udp	stmf	STMF	
502/tcp	asa-appl-proto	asa-appl-proto	
502/udp	asa-appl-proto	asa-appl-proto	
503/tcp	intrinsa	Intrinsa	
503/udp	intrinsa	Intrinsa	
504/tcp	citadel	citadel	
504/udp	citadel	citadel	
505/tcp	mailbox-lm	mailbox-lm	
505/udp	mailbox-lm	mailbox-lm	
506/tcp	ohimsrv	ohimsrv	
506/udp	ohimsrv	ohimsrv	
507/tcp	crs	crs	
507/udp	crs	crs	
508/tcp	xvttp	xvttp	
508/udp	xvttp	xvttp	
509/tcp	snare	snare	
509/udp	snare	snare	
510/tcp	fcp	FirstClass Protocol	
510/udp	fcp	FirstClass Protocol	
511/tcp	passgo	PassGo	
511/udp	passgo	PassGo	
512/tcp	exec	remote process execution;	
512/udp	comsat		
512/udp	biff	used by mail system to notify users	
513/tcp	login	remote login a la telnet;	
513/udp	who	maintains data bases showing who's	
514/tcp	shell	cmd	
514/udp	syslog		
515/tcp	printer	spooler	
515/udp	printer	spooler	
516/tcp	videotex	videotex	
516/udp	videotex	videotex	

517/tcp	talk	like tenex link, but across	
517/udp	talk	like tenex link, but across	
518/tcp	ntalk		
518/udp	ntalk		
519/tcp	utime	unixtime	
519/udp	utime	unixtime	
520/tcp	efs	extended file name server	
520/udp	router	local routing process (on site);	
521/tcp	ripng	ripng	
521/udp	ripng	ripng	
522/tcp	ulp	ULP	
522/udp	ulp	ULP	
523/tcp	ibm-db2	IBM-DB2	
523/udp	ibm-db2	IBM-DB2	
524/tcp	ncp	NCP	
524/udp	ncp	NCP	
525/tcp	timed	timeserver	
525/udp	timed	timeserver	
527/tcp	stx	Stock IXChange	
527/udp	stx	Stock IXChange	
528/tcp	custix	Customer IXChange	
528/udp	custix	Customer IXChange	
529/tcp	irc-serv	IRC-SERV	
529/udp	irc-serv	IRC-SERV	
530/tcp	courier	rpc	
530/udp	courier	rpc	
531/tcp	conference	chat	
531/udp	conference	chat	
532/tcp	netnews	readnews	
532/udp	netnews	readnews	
533/tcp	netwall	for emergency broadcasts	
533/udp	netwall	for emergency broadcasts	
534/tcp	mm-admin	MegaMedia Admin	
534/udp	mm-admin	MegaMedia Admin	
535/tcp	iiop	iiop	
535/udp	iiop	iiop	
536/tcp	opalis-rdv	opalis-rdv	
536/udp	opalis-rdv	opalis-rdv	
537/tcp	nmsp	Networked Media Streaming Protocol	
537/udp	nmsp	Networked Media Streaming Protocol	
538/tcp	gdomap	gdomap	
538/udp	gdomap	gdomap	
539/tcp	apertus-ldp	Apertus Technologies Load Determination	
539/udp	apertus-ldp	Apertus Technologies Load Determination	
541/tcp	uucp-rlogin	uucp-rlogin	
541/udp	uucp-rlogin	uucp-rlogin	
542/tcp	commerce	commerce	
542/udp	commerce	commerce	
543/tcp	klogin		
543/udp	klogin		
544/tcp	kshell	krcmd	
544/udp	kshell	krcmd	
545/tcp	appleqtcsrvr	appleqtcsrvr	
545/udp	appleqtcsrvr	appleqtcsrvr	
546/tcp	dhcpv6-client	DHCPv6 Client	
546/udp	dhcpv6-client	DHCPv6 Client	
547/tcp	dhcpv6-server	DHCPv6 Server	
547/udp	dhcpv6-server	DHCPv6 Server	

Port Numbers

548/tcp	afpovertcp	AFP over TCP	
548/udp	afpovertcp	AFP over TCP	
549/tcp	idfp	IDFP	
549/udp	idfp	IDFP	
550/tcp	new-rwho	new-who	
550/udp	new-rwho	new-who	
551/tcp	cybercash	cybercash	
551/udp	cybercash	cybercash	
552/tcp	deviceshare	deviceshare	
552/udp	deviceshare	deviceshare	
553/tcp	pirp	pirp	
553/udp	pirp	pirp	
554/tcp	rtsp	Real Time Stream Control Protocol	
554/udp	rtsp	Real Time Stream Control Protocol	
555/tcp	dsf		
555/udp	dsf		
556/tcp	remotefs	rfs server	
556/udp	remotefs	rfs server	
557/tcp	openvms-sysipc	openvms-sysipc	
557/udp	openvms-sysipc	openvms-sysipc	
558/tcp	sdnskmp	SDNSKMP	
558/udp	sdnskmp	SDNSKMP	
559/tcp	teedtap	TEEDTAP	
559/udp	teedtap	TEEDTAP	
560/tcp	rmonitor	rmonitord	
560/udp	rmonitor	rmonitord	
561/tcp	monitor		
561/udp	monitor		
562/tcp	chshell	chcmd	
562/udp	chshell	chcmd	
563/tcp	nntps	nntp protocol over TLS/SSL (was snntp)	
563/udp	nntps	nntp protocol over TLS/SSL (was snntp)	
564/tcp	9pfs	plan 9 file service	
564/udp	9pfs	plan 9 file service	
565/tcp	whoami	whoami	
565/udp	whoami	whoami	
566/tcp	streettalk	streettalk	
566/udp	streettalk	streettalk	
567/tcp	banyan-rpc	banyan-rpc	
567/udp	banyan-rpc	banyan-rpc	
568/tcp	ms-shuttle	microsoft shuttle	
568/udp	ms-shuttle	microsoft shuttle	
569/tcp	ms-rome	microsoft rome	
569/udp	ms-rome	microsoft rome	
570/tcp	meter	demon	
570/udp	meter	demon	
572/tcp	sonar	sonar	
572/udp	sonar	sonar	
573/tcp	banyan-vip	banyan-vip	
573/udp	banyan-vip	banyan-vip	
574/tcp	ftp-agent	FTP Software Agent System	
574/udp	ftp-agent	FTP Software Agent System	
575/tcp	vemmi	VEMMI	
575/udp	vemmi	VEMMI	
576/tcp	ipcd	ipcd	
576/udp	ipcd	ipcd	
577/tcp	vnas	vnas	
577/udp	vnas	vnas	

Port Numbers

578/tcp	ipdd	ipdd	
578/udp	ipdd	ipdd	
580/tcp	sntp-heartbeat	SNTP HEARTBEAT	
580/udp	sntp-heartbeat	SNTP HEARTBEAT	
582/tcp	scc-security	SCC Security	
582/udp	scc-security	SCC Security	
593/tcp	http-rpc-epmap	HTTP RPC Ep Map	
593/udp	http-rpc-epmap	HTTP RPC Ep Map	
620/tcp	sco-websrvrmgr	SCO WebServer Manager	
620/udp	sco-websrvrmgr	SCO WebServer Manager	
634/tcp	ginad	ginad	
634/udp	ginad	ginad	
635/tcp	rlzdbase	RLZ DBase	
635/udp	rlzdbase	RLZ DBase	
636/tcp	ldaps	ldap protocol over TLS/SSL (was sldap)	
636/udp	ldaps	ldap protocol over TLS/SSL (was sldap)	
637/tcp	lanserver	lanserver	
637/udp	lanserver	lanserver	
647/tcp	dhcp-failover	DHCP Failover	
647/udp	dhcp-failover	DHCP Failover	
666/tcp	mdqs		
666/udp	mdqs		
666/tcp	doom	doom Id Software	
666/udp	doom	doom Id Software	
667/tcp	disclose	campaign contribution disclosures - SDR Technologies	
667/udp	disclose	campaign contribution disclosures - SDR Technologies	
668/tcp	mecomm	MeComm	
668/udp	mecomm	MeComm	
669/tcp	meregister	MeRegister	
669/udp	meregister	MeRegister	
670/tcp	vacdsm-sws	VACDSM-SWS	
670/udp	vacdsm-sws	VACDSM-SWS	
671/tcp	vacdsm-app	VACDSM-APP	
671/udp	vacdsm-app	VACDSM-APP	
672/tcp	vpps-qua	VPPS-QUA	
672/udp	vpps-qua	VPPS-QUA	
673/tcp	cimplex	CIMPLEX	
673/udp	cimplex	CIMPLEX	
695/tcp	ieee-mms-ssl	IEEE-MMS-SSL	
695/udp	ieee-mms-ssl	IEEE-MMS-SSL	
696/tcp	rushd	RUSHD	
696/udp	rushd	RUSHD	
697/tcp	uuidgen	UUIDGEN	
697/udp	uuidgen	UUIDGEN	
698/tcp	olsr	OLSR	
698/udp	olsr	OLSR	
699/tcp	accessnetwork	Access Network	
699/udp	accessnetwork	Access Network	
709/tcp	entrust-kmsh	Entrust Key Management Service Handler	
709/udp	entrust-kmsh	Entrust Key Management Service Handler	
710/tcp	entrust-ash	Entrust Administration Service Handler	
710/udp	entrust-ash	Entrust Administration Service Handler	
729/tcp	netviewdm1	IBM NetView DM/6000 Server/Client	
729/udp	netviewdm1	IBM NetView DM/6000 Server/Client	
730/tcp	netviewdm2	IBM NetView DM/6000 send/tcp	
730/udp	netviewdm2	IBM NetView DM/6000 send/tcp	
731/tcp	netviewdm3	IBM NetView DM/6000 receive/tcp	
731/udp	netviewdm3	IBM NetView DM/6000 receive/tcp	

732-740	#	Unassigned	
741/tcp	netgw	netGW	
741/udp	netgw	netGW	
742/tcp	netrcs	Network based Rev. Cont. Sys.	
742/udp	netrcs	Network based Rev. Cont. Sys.	
744/tcp	flexlm	Flexible License Manager	
744/udp	flexlm	Flexible License Manager	
747/tcp	fujitsu-dev	Fujitsu Device Control	
747/udp	fujitsu-dev	Fujitsu Device Control	
748/tcp	ris-cm	Russell Info Sci Calendar Manager	
748/udp	ris-cm	Russell Info Sci Calendar Manager	
749/tcp	kerberos-adm	kerberos administration	
749/udp	kerberos-adm	kerberos administration	
750/udp	loadav		
750/udp	kerberos-iv	kerberos version iv	
753/tcp	rrh		
763/tcp	cycleserv		
763/udp	cycleserv		
765/tcp	webster		
765/udp	webster		
767/tcp	phonebook	phone	
767/udp	phonebook	phone	
770/tcp	cadlock		
770/udp	cadlock		
772/tcp	cycleserv2		
772/udp	cycleserv2		
774/tcp	rpasswd		
774/udp	acmaint_dbd		
776/udp	wpages		
77/tcp	multiling-http 7	Multiling HTTP	
77/udp	multiling-http 7	Multiling HTTP	
781-785	#	Unassigned	
786/tcp	concert	Concert	
786/udp	concert	Concert	
829/udp	pkix-3-ca-ra	PKIX-3 CA/RA	
830-846	#	Unassigned	
847/tcp	dhcp-failover2	dhcp-failover 2	
847/udp	dhcp-failover2	dhcp-failover 2	
886/tcp	iclcnet-locate	ICL coNETion locate server	
886/udp	iclcnet-locate	ICL coNETion locate server	
887/tcp	iclcnet_svinfo	ICL coNETion server info	
887/udp	iclcnet_svinfo	ICL coNETion server info	
888/tcp	accessbuilder	AccessBuilder	
888/udp	accessbuilder	AccessBuilder	
888/tcp	cddbp	CD Database Protocol	
900/tcp	omginitialrefs	OMG Initial Refs	
900/udp	omginitialrefs	OMG Initial Refs	
901/tcp	smpnameres	SMPNAMERES	
901/udp	smpnameres	SMPNAMERES	
902/tcp	ideafarm-chat	IDEAFARM-CHAT	
902/udp	ideafarm-chat	IDEAFARM-CHAT	
903/tcp	ideafarm-catch	IDEAFARM-CATCH	
903/udp	ideafarm-catch	IDEAFARM-CATCH	
911/tcp	xact-backup	xact-backup	
911/udp	xact-backup	xact-backup	
995/tcp	pop3s	pop3 protocol over TLS/SSL (was spop3)	
995/udp	pop3s	pop3 protocol over TLS/SSL (was spop3)	
996/tcp	vsinet	vsinet	

Port Numbers

996/udp	vsinet	vsinet	
1521/tcp	sql-net		
1558/tcp	streamworks		
1720/tcp	h323		
1755/tcp	netshow		
2427/tcp	mgcp		
5060/tcp	sip		
7000/tcp	vdolive		
7070/tcp	realmedia		
7648/tcp	cuseeme		
8000/tcp			
1467/tcp			
7649/tcp			
7170/tcp			
6970/tcp			
1470/tcp			
The latest port list can be found at:			
http://www.iana.org/assignments/port-numbers			

RFC	Description
RFC 821	**Simple Mail Transfer Protocol** J. Postel, Aug-01-1982. IETF Standard #10 STANDARD Recommended
RFC 1321	**The MD5 Message-Digest Algorithm R. Rivest, April 1992. Informational**
RFC 1422	**Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management** S. Kent, February 1993. Proposed Elective
RFC 1510	**The Kerberos Network Authentication Service (V5)** J. Kohl & C. Neuman, September 1993. Proposed Elective
RFC 1700	**ASSIGNED IP Protocol NUMBERS** J. Reynolds,J. Postel, October 1994. IETF Standard #2 STANDARD Required
RFC 1760	**The S/KEY One-Time Password System** N. Haller, February 1995. Informational
RFC 1777	**Lightweight Directory Access Protocol** W. Yeong, T. Howes & S. Kille, March 1995. Draft Elective
RFC 1828	**IP Authentication using Keyed MD5** P. Metzger & W. Simpson, August 1995. Proposed IPv6: Required IPv4: Elective
RFC 1829	**The ESP DES-CBC Transform** P. Karn, P. Metzger & W. Simpson, August 1995. Proposed IPv6: Required IPv4: Elective
RFC 1858	**Security Considerations for IP Fragment Filtering** G. Ziemba, D. Reed & P. Traina, October 1995. Informational
RFC 1902	**ARPA Internet Protocol policy** J.K. Reynolds, J. Postel, Jul-01-1984
RFC 1905	**ISO Transport Protocol specification ISO DP 8073** A.M. McKenzie, Apr-01-1984.
RFC 1928	**Introduction to proposed DoD standard H-FP** M.A. Padlipsky, Dec-01-1984
RFC 2021	**Remote Network Monitoring Management Information Base Version 2 using SMIv2** S. Waldbusser, January 1997. Proposed Elective
RFC 2058	**Remote Authentication Dial In User Service (RADIUS)** C. Rigney, A. Rubens, W. Simpson, S. Willens, January 1997. Proposed
RFC 2059	**RADIUS Accounting** C. Rigney, January 1997. Informational
RFC 2101	**IPv4 Address Behaviour Today** B. Carpenter, J. Crowcroft, Y. Rekhter, February 1997. Informational
RFC 2104	**HMAC: Keyed-Hashing for Message Authentication** H. Krawczyk, M. Bellare, R. Canetti, February 1997. Informational
RFC 2196	**Site Security Handbook**
RFC 2326	**Real Time Streaming Protocol (RTSP)** H. Schulzrinne, A. Rao, R. Lanphier, April 1998. Proposed Elective
RFC 2401	**The IP Security Architecture, defines the overall architecture and specifies elements common to both the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP).**
RFC 2402	**The IP Authentication Header (AH), defines an algorithm-independent mechanism for providing exportable cryptographic authentication without encryption to IPv4 and IPv6 packets.**
RFC 2404	**The Use of HMAC-SHA-1-96 within ESP and AH** C. Madson, R. Glenn, November 1998. Proposed
RFC 2406	**The IP Encapsulating Security Payload (ESP), defines an algorithm-independent mechanism for providing encryption to IPv4 and IPv6 packets.**
RFC 2408	**The Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify, and delete Security Associations (SA).**
RFC 2459	**Internet X.509 Public Key Infrastructure Certificate and CRL Profile** R. Housley, W. Ford, W. Polk, D. Solo, January 1999. Proposed
RFC 2504	**Users' Security Handbook** E. Guttman, L. Leong, G. Malkin, February 1999. IETF FYI #34 Informational
RFC 2510	**Internet X.509 Public Key Infrastructure Certificate Management Protocols**

RFC 2511	**Internet X.509 Certificate Request Message Format**
RFC 2661	**Layer Two Tunneling Protocol "L2TP"**
For More RFC listing go to:	http://www.ietf.org/rfc.html
or	http://www.rfc-editor.org/rfc.html

Decimal	Keyword	Protocol
0	**HOPOPT**	IPv6 Hop-by-Hop Option
1	**ICMP**	Internet Control Message
2	**IGMP**	Internet Group Management
3	**GGP**	Gateway-to-Gateway
4	**IP**	IP in IP (encapsulation)
5	**ST**	Stream
6	**TCP**	Transmission Control
7	**CBT**	CBT
8	**EGP**	Exterior Gateway Protocol
9	**IGP**	any private interior gateway (Cisco)
10	**BBN-RCC-MON**	BBN RCC Monitoring
11	**NVP-II**	Network Voice Protocol
12	**PUP**	PUP
13	**ARGUS**	ARGUS
14	**EMCON**	
15	**XNET**	Cross Net Debugger
16	**CHAOS**	Chaos
17	**UDP**	User Datagram
18	**MUX**	Multiplexing
19	**DCN-MEAS**	DCN Measurement Subsystems
20	**HMP**	Host Monitoring
21	**PRM**	Packet Radio Measurement
22	**XNS-IDP**	XEROX NS IDP
23	**TRUNK-1**	Trunk-1
24	**TRUNK-2**	Trunk-2
25	**LEAF-1**	Leaf-1
26	**LEAF-2**	Leaf-2
27	**RDP**	Reliable Data Protocol
28	**IRTP**	Internet Reliable Transaction
29	**ISO-TP4**	ISO Transport Protocol Class4
30	**NETBLT**	Bulk Data Transfer Protocol
31	**MFE-NSP**	MFE Network Services Protocol
32	**MERIT-INP**	Internodal Protocol
33	**SEP**	Sequential Exchange Protocol
34	**3PC**	Third Party Connect Protocol

IP Protocols

35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	XTP
37	DDP	Datagram Delivery Protocol
38	IDPR-CMTP	Control Message Transport Protocol
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41	IPv6	Ipv6
42	SDRP	Source Demand Routing Protocol
43	IPv6-Route	Routing Header for IPv6
44	IPv6-Frag	Fragment Header for IPv6
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Reservation Protocol
47	GRE	General Routing Encapsulation
48	MHRP	Mobile Host Routing Protocol
49	BNA	BNA
50	ESP	Encap Security Payload for IPv6
51	AH	Authentication Header for IPv6
52	I-NLSP	Integrated Net Layer Security
53	SWIPE	IP with Encryption
54	NARP	NBMA Address Resolution Protocol
55	MOBILE	IP Mobility
56	TLSP	Transport Layer Security Protocol
57	SKIP	SKIP
58	IPv6-ICMP	ICMP for IPv6
59	IPv6-NoNxt	No Next Header for IPv6
60	IPv6-Opts	Destination Options for IPv6
61	AHIP	any host internal protocol
62	CFTP	CFTP
63	LN	any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
67	IPPC	Internet Pluribus Packet Core
68	DFS	any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol

IP Protocols

71	**IPCV**	Internet Packet Core Utility
72	**CPNX**	Computer Protocol Network Executive
73	**CPHB**	Computer Protocol Heart Beat
74	**WSN**	Wang Span Network
75	**PVP**	Packet Video Protocol
78	**BR-SAT-MON**	Backroom SATNET Monitoring
79	**WB-EXPAK**	WIDEBAND EXPAK
80	**ISO-IP**	ISO Internet Protocol
81	**VMTP**	VMTP
82	**SECURE-VMTP**	SECURE-VMTP
83	**VINES**	VINES
84	**TTP**	TTP
85	**NSFNET-IGP**	NSFNET-IGP
86	**DGP**	Dissimilar Gateway Protocol
87	**TCF**	TCF
88	**EIGRP**	EIGRP
89	**OSPFIGP**	OSPFIGP
90	**Sprite-RPC**	Sprite RPC Protocol
91	**LARP**	Locus Address Resolution Protocol
92	**MTP**	Multicast Transport Protocol
93	**AX.25**	AX.25 Frames
94	**IPIP**	IP-within-IP Encapsulation Protocol
95	**MICP**	Mobile Internetworking Control Protocol
96	**SCC-SP**	Semaphore Communications Sec. Pro.
97	**ETHERIP**	Ethernet-within-IP Encapsulation
98	**ENCAP**	Encapsulation Header
99	**PES**	any private encryption scheme
100	**GMTP**	GMTP
101	**IFMP**	Ipsilon Flow Management Protocol
102	**PNNI**	PNNI over IP
103	**PIM**	Protocol Independent Multicast
104	**ARIS**	ARIS
105	**SCPS**	SCPS
106	**QNX**	QNX
107	**A/N**	Active Networks
108	**IPComp**	IP Payload Compression Protocol

IP Protocols

109	SNP	Sitara Networks Protocol
110	Compaq-Peer	Compaq Peer Protocol
111	IPX-in-IP	IPX in IP
112	VRRP	Virtual Router Redundancy Protocol
113	PGM	PGM Reliable Transport Protocol
114	0-HP	any 0-hop protocol
115	L2TP	Layer Two Tunneling Protocol
116	DDX	D-II Data Exchange (DDX)
117	IATP	Interactive Agent Transfer Protocol
118	STP	Schedule Transfer Protocol
119	SRP	SpectraLink Radio Protocol
120	UTI	UTI
121	SMP	Simple Message Protocol
122	SM	SM
123	PTP	Performance Transparency Protocol
124	ISIS	über IPv4
125	FIRE	FIRE
126	CRTP	Combat Radio Transport Protocol
127	CRUDP	Combat Radio User Datagram
128	SSCOPMCE	SSCOPMCE
129	IPLT	IPLT
130	SPS	Secure Packet Shield
131	PIPE	Private IP Encapsulation within IP
132-254	Unassigned	Unassigned
255	Reserved	Reserved
		For the latest IP Protcol Values, go to:
		http://www.ietf.org/rfc/rfc1700.txt?number=1700