

Glossary

access control list (ACL) ACLs can provide basic traffic-filtering capabilities on Cisco routers. ACLs can be configured for all routed network protocols to filter packets as they pass through a router or security appliance. An ACL may be used for packet filtering (a type of firewall), as well as for selecting types of traffic to be analyzed, forwarded, or influenced in some manner.

accounting Tracking users' consumption of network resources. This information may be used for management purposes, planning, billing, or other purposes. Typical information that is gathered includes the user's name, the nature of the service delivered, when the service began, and when it concluded.

Advanced Encryption Standard (AES) The AES initiative was announced in 1997, when the public was invited to propose candidate encryption schemes to be evaluated as the encryption standard to replace DES. The Rijndael cipher was selected as the AES algorithm in October of 2000 by the U.S. National Institute of Standards and Technology (NIST). In 2002 the U.S. Secretary of Commerce approved the adoption of AES as an official U.S. government standard.

application layer firewall This third-generation firewall technology evaluates network packets for valid data at the application layer before allowing a connection. Data in all network packets is examined at the application layer and maintains complete connection state and sequencing information. Application layer firewalls also can validate other security items that appear only within the application layer data, such as user passwords and service requests.

asymmetric algorithm Employs a two-key technology: a public key and a private key. Often this is simply called public key encryption. In this key pair, the public key may be distributed freely, whereas the private key must be closely guarded. If it is compromised, the system as a whole will fail. The way that public key encryption works is that the public key is used to encrypt the data. After it is encrypted, only the private key can decrypt the data. The opposite is also true.

596 asymmetric encryption

asymmetric encryption Employs a two-key technology: a public key and a private key. Often this is simply called public key encryption. In this key pair, the public key may be distributed freely, whereas the private key must be closely guarded. If it is compromised, the system as a whole will fail. The way that public key encryption works is that the public key is used to encrypt the data. After it is encrypted, only the private key can decrypt the data. The opposite is also true.

auditing The process of recording the actions of an authenticated user. An example is tracking how long a user is authenticated on the network and the resources he or she works with while on the network, as well as the length of usage. Auditing can produce a history of network usage on the part of a given user or users.

authentication The confirmation that a user who is requesting a service is a valid user of the network services requested. Authentication is accomplished by presenting an identity and credentials. These might be such things as passwords, one-time tokens, or digital certificates.

authentication, authorization, and accounting (AAA) These three primary services give a network security as well as a record of user activity. AAA identifies who the user is, what the user can access, and what services and resources the user is using when he or she makes a connection with a server.

authentication server A RADIUS server (such as Cisco Secure ACS) that validates a client's credentials against its user database.

authenticator A device (such as a Cisco Catalyst switch) that provides access to a network. The authenticator typically does not authenticate the supplicant. Rather, the authenticator acts as a gateway, relaying authentication messages between the supplicant and an external authentication server.

authorization The granting of specific types of service to a user, based on his or her authentication, the services he or she is requesting, and the current system state.

AutoSecure An automated approach to applying security best practices to a router that is invoked from the CLI.

auxiliary VLAN The VLAN used by a Cisco IP Phone to carry voice traffic is often called an auxiliary VLAN.

availability The availability of data is a measure of its accessibility. For example, if a server were down only 5 minutes per year, it would have an availability of 99.999 percent (that is, "five nines" of availability).

awareness Awareness makes the end-user community conscious of security issues, without necessarily any in-depth procedural training. For example, distributing an e-mail or pamphlet describing the issue of viruses and the importance of virus protection creates awareness of the issue.

block cipher Derives its name from the fact that it transforms a fixed-length “block” of plain text into a “block” of ciphertext. These two blocks are the same length. When the reverse transformation is applied to the ciphertext block, by using the same secret key, it is decrypted. Block ciphers use a fixed length or block size. This generally is 128 bits, but they can range in size. For instance, DES has a block size of 64 bits.

bootset The collection of a router’s image and configuration files that can be protected using the Cisco IOS Resilient Configuration feature, which keeps a secure copy of the bootset.

brute-force attack Attempts to match password credentials by guessing a sequence of patterns (for example, the letter a through the letter z, followed by the letters aa through zz, followed by aaa through zzz, and so on). In such an attack, all possible combinations are used until the password is discovered. This may require a great deal of time, but it always eventually succeeds in discovering the password.

buffer overflow A programming error that may result in erratic program behavior, a memory access exception and program termination, or a possible breach of system security.

call agent Replaces many of the features previously provided by Private Branch Exchanges (PBX). For example, a call agent can be configured with rules that determine how calls are forwarded. Cisco Unified Communications Manager (UCM) is an example of a call agent.

catastrophe A disruption category in which all resources at a site are destroyed, and normal business operations must be moved to an alternative site.

certificate A document issued and signed by the certificate authority (CA) that binds the name of the entity and its public key.

certificate authority (CA) A trusted third party responsible for signing the public keys of entities in a PKI-based system.

Challenge Handshake Authentication Protocol (CHAP) An authentication scheme used by Point-to-Point Protocol (PPP) to validate the identity of remote clients. CHAP periodically verifies the client’s identity by using a three-way handshake. Verification is based on a shared secret. CHAP also is the mandatory protocol for iSCSI, as chosen by the Internet Engineering Task Force (IETF). CHAP is based on shared secrets. It periodically verifies the client’s identity by using a three-way handshake. This verification is based on a shared secret. With CHAP, the password never actually crosses the wire, just a hash of the challenge, hostname, and password.

598 checksum

checksum A mathematical computation used to verify that the contents of a message have not been altered.

ciphertext The representation of plain text in an unreadable form.

Cisco Discovery Protocol (CDP) A Layer 2 protocol that permits adjacent Cisco devices to learn information about one another (for example, protocol and platform information).

Cisco Security Agent (CSA) A host-based IPS (HIPS) solution. The CSA software can be installed on selected host systems and optionally report suspicious activity to a centralized management server.

Cisco Security Device Manager (SDM) Provides a graphical user interface (GUI) for configuring a wide variety of features on an IOS router.

Cisco Security Manager An application that can be used to configure security features on a wide variety of Cisco security products.

Cisco Security MARS The Cisco Security Monitoring, Analysis and Response System. The MARS product offers security monitoring for security devices and applications. In addition to Cisco devices and applications, Cisco Security MARS can monitor many third-party devices and applications.

Cisco Self-Defending Network The Cisco vision for using a network to recognize threats and then prevent and adapt to them.

class map A way of identifying a set of packets based on their contents using “match” conditions. Classes generally are defined so that you can apply an action to the identified traffic that reflects a policy. The class itself is designated via the class map. Class maps are created using the **class-map** command. After it is created, the class map is used to match packets to a specified class.

cold site A cold site offers an alternative site where business operations can be conducted, unlike a hot or warm site. However, a cold site typically does not contain redundant computing equipment such as servers and routers. As a result, the data network would need to be rebuilt from scratch, which might require weeks. Therefore, although a cold site is less expensive initially, as compared to hot or warm sites, a cold site could have more long-term consequences. In fact, the financial consequences could be far greater than the initial cost savings.

collision When two separate messages have the same message digest. A hash “collision” or hash “clash” happens when two distinct inputs entered into a hash function produce identical outputs. Each hash function has the potential for collisions. However, if you are working with a

well-designed hash function, collisions should occur less frequently. In terms of hash functions, collisions inhibit the distinguishing of data, making records more costly to find in hash tables and data processing.

community VLAN Ports belonging to a community VLAN can communicate with one another, but not with ports in other community VLANs.

confidentiality Data confidentiality is provided by encrypting data. If a third party intercepts the encrypted data, he or she cannot interpret it.

Context-Based Access Control (CBAC) Represents a significant advance over ACLs in that it provides stateful packet filtering capability. CBAC provides the capacity to monitor several attributes in TCP connections, UDP sessions, and Internet Control Message Protocol (ICMP). This monitoring is done in an effort to be sure that the only traffic allowed through a firewall ACL is the return traffic for a dialogue that was originated on the private side of the firewall.

cryptographic hash This function is a transformation that takes an input and returns a string, which is called the hash value. Cryptographic hash functions begin with the assumption that an adversary can deliberately try to find inputs with the same hash value. Creating a well-designed cryptographic hash involves a one-way operation in which there is no practical way to calculate a particular data input that will result in a desired hash value. This one-way nature makes the hash very difficult to forge.

cryptography The practice and study of encoding information to protect the original contents. In modern terms this is considered the breach between mathematics and computer science, combining to provide a means of securing information both in computer systems and on networks.

data diddling The process of changing data before it is stored in a computing system.

Data Encryption Standard (DES) Typically operates in block mode, where it encrypts data in 64-bit blocks. Like other symmetric algorithms, DES uses the same algorithm and key for both encryption and decryption. DES has weathered nearly 35 years of cryptographic scrutiny. To this point, no significant flaws have been found. Adding to its appeal, DES may be easily implemented and accelerated in hardware.

Defense in Depth A design philosophy that uses a layered security approach to eliminate a single point of failure and to provide overlapping protection.

demilitarized zone (DMZ) Sometimes called a screened subnet. A segment of the overall network that is cordoned off through the use of two firewalls. One of these firewalls sits between the DMZ and the Internet, and the other sits between the DMZ and the internal network. This configuration may also be referred to as creating a “perimeter” network.

600 denial of service (DoS)

denial of service (DoS) A class of attack in which the attacker seeks to make a given resource unavailable to legitimate users by overwhelming the resource with requests for service that appear legitimate. The resource, such as a server, seeks to handle all requests but ultimately fails. It either becomes unavailable for legitimate purposes or struggles to such an extent that it cannot respond to legitimate requests in a timely manner.

detective control Can detect when access to data or a system occurs.

deterrent control Attempts to prevent a security incident by influencing a potential attacker not to launch an attack.

DHCP snooping The Dynamic Host Configuration Protocol snooping feature on Cisco Catalyst switches can be used to combat a DHCP server spoofing attack. With this solution, Cisco Catalyst switch ports are configured in either a trusted or untrusted state. If a port is trusted, it is allowed to receive DHCP responses. If a port is untrusted, it is not allowed to receive DHCP responses. If a DHCP response attempts to enter an untrusted port, the port is disabled.

dictionary attack Attempts to match password credentials by guessing passwords from a “dictionary” of common words.

Diffie-Hellman (DH) algorithm A key exchange algorithm that was invented by Whitfield Diffie and Martin Hellman in 1976. The Diffie-Hellman algorithm derives its strength from the difficulty of calculating the discrete logarithms of very large numbers. The functional usage of this algorithm is to provide secure key exchange over insecure channels such as the Internet. DH is also often used to provide keying material for other symmetric algorithms, such as DES, 3DES, and AES.

Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) A variation of CHAP that may be used to authenticate devices connecting to a Fibre Channel switch so that only trusted devices may be added to a fabric. DHCHAP adds a DH exchange that both strengthens CHAP and provides an agreed-upon secret key.

digital signature Also called a digital signature scheme. A form of asymmetric cryptography that is used to simulate the security characteristics of a written signature in digital form. Digital signature schemes typically use two algorithms that employ a pair of public and private keys. One of these is used for signing, which involves the user’s secret or private key. The other is used to verify these signatures. This typically involves the use of the user’s public key.

Digital Signature Algorithm (DSA) The Digital Signature Standard (DSS) outlines the use of the DSA by a signer to generate a digital signature to be applied to data and by a recipient of the data to verify the signature’s authenticity. To create the digital signature, you need both a public key and a private key. The private key is used to generate the signature, and the public key is used

to verify it. For both signature generation and verification, the data, which is called a message, is reduced through the use of the Secure Hash Algorithm (SHA).

disaster A disruption category in which normal business operations are interrupted for one or more days. However, not all critical resources at a site are destroyed.

disaster recovery plan Sometimes called a business continuity plan. Addresses actions taken during and immediately following a disaster.

Dynamic ARP Inspection (DAI) Uses trusted and untrusted ports. ARP replies are allowed into the switch on trusted ports. However, if an ARP reply enters the switch on an untrusted port, the contents of the ARP reply are compared to the DHCP binding table to verify its accuracy. If the ARP reply is inconsistent with the DHCP binding table, the ARP reply is dropped, and the port is disabled.

dynamic firewall This fourth-generation firewall technology, sometimes called a stateful firewall, keeps track of the communication process through the use of a state table. This firewall operates at Layers 3, 4, and 5.

EAP Extensible Authentication Protocol. Dictates the specific authentication messages transported by 802.1x and RADIUS protocols used in an IEEE 802.1x solution.

education More comprehensive than training because it covers a larger body of knowledge. Obtaining a college degree focusing on IT security is an example of a comprehensive security education.

elevation of privileges The act of exploiting a bug in a software application to gain access to resources that normally would be protected from an application or user. The result is that the application performs actions with more privileges than intended by the application developer or system administrator.

Encapsulating Security Payload (ESP) An Internet standard that allows for the authentication and encryption of IP packets. ESP over Fibre Channel provides a means of protecting data in transit throughout the Fibre Channel network. However, it does not address the need to secure data while it is stored on the Fibre Channel network.

endpoint The final point of connection in a communication channel.

exploit A malicious program designed to take advantage of a vulnerability.

602 extended access control list (ACL)

extended access control list (ACL) Made up of a series of statements created in global mode. With extended ACLs, IP packets may be filtered based on a number of attributes. Extended ACLs can filter packets according to protocol type, source and IP address, destination IP address, source TCP or UDP ports, destination TCP or UDP ports, and optional protocol type information if finer granularity of control is required.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) Protects authentication messages within a secure Transport Layer Security (TLS) tunnel using shared secret keys. Security is provided by an SSL (Secure Socket Layer)/TLS certificate on the “server side”/ACS and by a username and password on the client side.

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) A standards-based EAP type that uses an MD5-Challenge message. This is much like the challenge message used in PPP CHAP (Point-to-Point Protocol Challenge Handshake Authentication Protocol), which also uses MD5 as its hashing algorithm.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) Developed by Microsoft Corporation to address weaknesses found in other EAP types (such as the one-way authentication used by EAP-MD5). EAP-TLS uses certificate-based (X.509 certificate-based) authentication. It requires both a supplicant and an authentication server to possess a digital certification to perform mutual authentication.

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) Uses a secured Transport Layer Security (TLS) tunnel to send other EAP authentication messages.

Fibre Channel In terms of SAN networking, this is the primary SAN transport used for host-to-SAN connectivity.

Fibre Channel Authentication Protocol (FCAP) Born from Switch Link Authentication Protocol (SLAP), the first authentication protocol proposed for Fibre Channel. This optional authentication mechanism may be employed between any two devices or entities on a Fibre Channel network. It uses certificates or optional keys to provide security.

Fibre Channel over IP (FCIP) Represents the implementation of Fibre Channel in an IP implementation that relies on TCP/IP as the network protocol.

Fibre Channel Password Authentication Protocol (FCPAP) An optional password-based authentication key-exchange protocol. It may be used in Fibre Channel networks to provide mutual authentication between Fibre Channel ports. As compared to FCAP, FCPAP does not require a PKI to operate.

Fibre Channel Security Protocol (FC-SP) Designed to overcome the security challenges for enterprise-wide fabrics by providing switch-to-switch and host-to-switch authentication. The focus of FC-SP is protecting data in transit throughout the Fibre Channel network.

Fibre Channel zoning The partitioning of a Fibre Channel fabric into smaller subsets for security purposes.

firewall Allows for the segmentation of networks into different physical subnetworks, thereby helping limit the potential damage that could spread from one subnet to another. This term comes from firewalls in buildings, which limit the spread of a fire. A firewall may be a piece of software or hardware that acts as a barrier between the internal (trusted) network and the external (untrusted) network, such as the Internet.

gatekeeper Can be thought of as the “traffic cop” of the WAN. For example, because bandwidth on a WAN typically is somewhat limited, a gatekeeper can monitor the available bandwidth. Then, when there is not enough bandwidth to support another voice call, the gatekeeper can deny future call attempts.

gateway Can forward calls between different types of networks. For example, you could place a call from an IP phone in your office, through a gateway to the PSTN, to call your home.

hashing Used to provide data integrity. Hashes are based on one-way mathematical functions that can be easy to compute but extremely challenging to reverse. The way that hashing works in practice is that data of an arbitrary length is input into the hash function and is processed through the function, resulting in a fixed-length hash. The resultant fixed-length hash is called either the digest or fingerprint.

heap overflow A type of buffer overflow that occurs in the heap data area. Memory on the heap is dynamically allocated by the application at runtime and typically contains program data. A heap overflow is not as likely to result in a condition permitting remote code execution as a buffer overflow.

HMAC Keyed Hash Message Authentication Code. An HMAC in cryptographic terms is a type of message authentication code calculated by using a cryptographic hash function along with a secret key. This may be used to simultaneously verify both the data’s integrity and the message’s authenticity. An iterative cryptographic hash function such as MD5 or SHA-1 may be used to calculate the HMAC. When these are used, the resulting MAC algorithm is called HMAC-MD5 or HMAC-SHA-1, for instance. The cryptographic strength of the underlying hash function, along with the key’s size and quality and the hash output length in bits, define the cryptographic strength of the HMAC.

604 host-based intrusion prevention system (HIPS)

host-based intrusion prevention system (HIPS) An IPS in which the intrusion-prevention application resides on that specific host, typically a single computer. The IPS monitors system activities for malicious or unwanted behaviors. It can react in real time to block or prevent those activities. The key benefit is that HIPS is behavior-based as opposed to signature-based.

Host Bus Adapter (HBA) Connects a host system to other network and storage devices. This term primarily refers to devices for connecting SCSI, Fibre Channel, and eSATA devices, but devices for connecting to IDE, Ethernet, FireWire, USB, and other systems may also be called host adapters.

hot site A completely redundant site that has equipment very similar to that at the original site. Data is routinely copied from a primary site to a hot site. As a result, a hot site can be up and functioning within a few minutes (or even seconds) after a catastrophe at the primary site.

IEEE 802.1x A standards-based approach for providing port-based network access. Specifically, 802.1x is a Layer 2 protocol that defines how Extensible Authentication Protocol (EAP) frames are encapsulated, typically between a user's network device (such as a PC) and a switch or wireless access point.

IKE proposal Internet Key Exchange proposal. A collection of security protocols and algorithms that can be used to establish an IKE Phase 1 (ISAKMP) tunnel.

in-band management An approach that allows management traffic to be transmitted across a production network.

inline mode Inline mode operation requires at least two monitoring interfaces on an IPS sensor, because the sensor resides inline with the traffic. (In other words, traffic enters the sensor on one monitoring interface and exits the sensor on another monitoring interface.) Therefore, a sensor running in inline mode supports IPS operation and can drop malicious traffic before it reaches its intended target.

Integrated Services Router (ISR) As its name suggests, this kind of Cisco router integrates various services (such as voice and security services) into a router's architecture.

integrity Data integrity ensures that data is not modified in transit. For example, routers at each end of a tunnel could calculate checksum values or hash values for the data. If both routers calculate the same values, the data most likely was not modified in transit.

intrusion detection system (IDS) Can recognize network attacks by analyzing a copy of network traffic. Can deliver a comprehensive, pervasive security solution for combating unauthorized intrusions, malicious Internet worms, and bandwidth and e-business application attacks.

intrusion prevention system (IPS) Provides end-to-end protection for the network via a network-based defense that can identify, classify, and stop known and unknown threats, including worms, network viruses, application threats, system intrusion attempts, and application misuse.

IP spoofing An attack in which an attacker falsifies packets' source IP address (for example, causing the source IP address to be a trusted IP address).

IP telephony Similar to VoIP, sends voice traffic over an IP network. However, the primary distinction from a VoIP network is that an IP telephony environment contains endpoints that natively communicate using IP.

isolated VLAN Ports belonging to an isolated VLAN lack Layer 2 connectivity between one another. However, they can communicate with a promiscuous port.

key pair In terms of a PKI, the key pair is composed of one public key and one private key. These two keys work together to provide a means to both encrypt and decrypt data. The public key may be widely distributed publicly, but the private key should be closely held by its owner. Data encrypted with the public key can be decrypted only by the matching private key.

keyspace The keyspace of an algorithm represents a defined set of all possible key values. For each key of n bits, a keyspace is produced that has 2^n possible key values. This means that if 1 bit were added to the key, this would effectively double the size of the keyspace.

Lightweight Extensible Authentication Protocol (LEAP) Uses a username/password combination to perform authentication. Typically is found in a Cisco wireless LAN (WLAN) implementation.

LUN masking A Logical Unit Number is an address used by the SCSI protocol to differentiate an individual disk drive that makes up a common SCSI target device. LUN masking represents a defense against attacks. In this authorization process, a LUN is made available to some hosts and unavailable to other hosts.

Management Information Base (MIB) Information about a managed device's resources and activity is defined by a series of objects. The structure of these management objects is defined by a managed device's MIB.

Media Gateway Control Protocol (MGCP) Originally developed by Cisco and considered to be a client/server protocol. The client (such as an analog port in a voice-enabled router) can communicate with a server (such as a Cisco Unified Communications Manager server) via a series of events and signals. For example, the server could tell the client that if an attached phone goes off-hook, play the signal of dial tone to that phone.

606 message

message In cryptographic terms, a collection of plain text. Messages may be anything from an e-mail, to a username-and-password combination, to a string of data.

Message Digest 5 (MD5) An iterative hash function that breaks a message into blocks of a fixed size and then iterates over them with a compression function. Defined in RFC 1321, MD5 with its 128-bit hash value has been employed in a wide variety of security applications. It is also commonly used to check the integrity of files. An MD5 hash typically is expressed as a 32-character hexadecimal number.

method list A sequential list that defines the authentication methods used to authenticate a user. Method lists enable the designation of one or more security protocols to be used for authentication, ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users. If that method does not respond, Cisco IOS software selects the next authentication method in the method list. This process continues until either successful communication with a listed authentication method occurs or the authentication method list is exhausted, in which case authentication fails.

microengine Handles a group of similar signatures. A sensor contains multiple microengines and decides which one(s) it will use to analyze traffic. It uses criteria such as the network protocol being used by the traffic, the signature's associated operating system, the port number being used by the session, and the type of attack the sensor is looking for.

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) Microsoft's version of CHAP. This protocol exists in two versions: MS-CHAPv1 (RFC 2433) and MS-CHAPv2 (RFC 2759).

Multipoint Control Unit (MCU) Useful for conference calling. During a conference call, several people might be speaking at the same time, and everyone on that conference call can hear them. It takes processing power to mix together these audio streams. MCUs provide that processing power. MCUs might contain digital signal processors (DSP), which are dedicated pieces of computer circuitry that can mix together these audio streams.

National Institute of Standards and Technology (NIST) The U.S. government body that is responsible for defining and publishing U.S. Federal Information Processing Standards (FIPS).

network access device (NAD) The system that provides network access in an enterprise network environment.

network access server (NAS) Provides enterprise access services and implements security mechanisms for those connecting with a corporate network. A NAS is the intermediate device between an end user and authentication server. It could be a router, VPN endpoint (perhaps ASA), WiFi access point, or Catalyst switch running 802.1x. Any device that handles user credentials via

Telnet, SSH, HTTP, IKE, EAP, PPP, and so on and then passes these credentials to a RADIUS/TACACS server on the back end would qualify as a NAS.

Network Address Translation (NAT) Employed by networks that use private IP addresses. In terms of security uses, it is used by the application inspection function of firewalls to help identify the location of embedded addressing information. NAT is used to translate embedded addresses and to update any checksum or other fields that are affected by the translation.

Network Admission Control (NAC) Refers to the Cisco NAC appliance, which provides network access features to enterprise environments to help ensure a secure and clean environment.

Network Time Protocol (NTP) Allows a router to act as a time source, helping to ensure that the time is consistent across multiple network devices. Synchronizing clocks in this manner makes event correlation much easier.

nondisaster A disruption category in which normal business operations are briefly interrupted.

nonrepudiation Blocks the false denial of a particular action.

out-of-band (OOB) management Keeps management traffic isolated from production data traffic.

parameter map Specifies parameters to be applied to classified traffic. Using the **parameter-map type** command you may specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map.

phreaker A hacker of a telephony system.

Point-to-Point Protocol (PPP) A data link protocol commonly used to establish a direct connection between two nodes over serial cable, phone line, trunk line, cellular telephone, specialized radio links, or fiber-optic links. Most Internet service providers use PPP for customers' dialup access to the Internet.

policy map Actions are associated with traffic classified by class maps using policy maps. An action is defined as a specific functionality and typically is associated with a traffic class. Some common actions are **inspect**, **drop**, and **pass**.

preventive control Attempts to prevent access to data or a system. This could be any number of things that attempt to block this access.

608 private key

private key One half of a public key/private key key pair. This key must remain privately held and should be guarded by its owner. As soon as data has been encrypted by the associated public key, only the private key may be used to decrypt the data. With regard to digital signatures, its function is to sign a message. The message signature may then be verified through the use of the associated public key.

privilege level An IOS EXEC mode that allows an administrator logged into that privilege level to access all commands available to that privilege level and all lower privilege levels. Cisco IOS routers support privilege levels in the range 0 to 15. By default, when you attach to a router, you are in unprivileged mode, which has a privilege level of 1. Privilege level 0 may be assigned to a user account. Those who have this level may then be assigned a subset of the commands available at level 1. After entering the **enable** command and providing appropriate credentials, you are moved to privileged mode, which has a privilege level of 15.

promiscuous mode Uses a single monitoring interface on an IDS/IPS sensor. When running in promiscuous mode, a sensor receives a copy of selected network traffic. If the sensor detects malicious traffic, it can take a variety of actions. For example, it can trigger an alarm or instruct a security appliance to drop traffic coming from a specific source. Because a sensor running in promiscuous mode is not inline with the traffic, IDS operation is supported, but not IPS operation.

Protected Extensible Authentication Protocol (PEAP) Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) An EAP type that increases protection of authentication messages by creating a protected Transport Layer Security (TLS) tunnel. Then, within the protection of the TLS tunnel, an authentication protocol such as MS-CHAPv2 can be used.

proxy server Acts as an intermediary between networks, often your internal network and the Internet at large. In such configurations there is no direct connection between an outside user and internal network resources. The proxy provides the only visible IP address on the Internet. Clients connect to the proxy server to submit their application layer request. These requests include the actual destination as well as the data request itself. Based on the proxy server settings, the proxy analyzes the request and may even filter or change the packet contents before proceeding. The proxy server also makes a copy of all the incoming packets and then changes the source address. It does this to hide the internal address from the outside world before it sends the packet to the destination address.

public key One half of a public key/private key key pair. This key may be made available publicly. It can be used to encrypt data that may then be decrypted only by the matching private key. With regard to digital signatures, its function is to verify a message signature. In this case, the message would be signed with the sender's private key, and then the recipient would verify the signature's authenticity using the sender's public key.

Public Key Infrastructure (PKI) Taken as a whole, a set of technical, organizational, and legal components that combine to establish a system that enables large-scale use of public key cryptography. Via a PKI, an organization can provide authenticity, confidentiality, integrity, and nonrepudiation services.

public switched telephone network (PSTN) The North American public telephone network.

rainbow table A precomputed table of all possible combinations of characters and the hashes they create. If an attacker were to discover the contents of a password file, such as the SAM file in Windows, he could load the hashes stored in the SAM into a rainbow table. The rainbow table then displays the input required to generate that hash. This is often referred to as a time-versus-space trade-off attack. An attacker does not have to spend time trying every possible combination until he finds a match. However, he must sacrifice more than 50 GB of hard drive space to store these tables, or have access to an online rainbow table.

Real-time Transport Protocol (RTP) Carries the voice payload in VoIP streams. Interestingly, although RTP is a Layer 4 protocol, it is encapsulated inside UDP (also a Layer 4 protocol). The UDP port numbers used can vary by vendor, but in Cisco environments, RTP typically uses even UDP ports in the range 16,384 to 32,767.

registration authority (RA) To make the operation of the CA more secure, many key management tasks may be effectively offloaded to RAs. These RAs are PKI servers that are responsible for performing management tasks on behalf of the CA. These include authenticating users when they enroll with the PKI, key generation for users who cannot generate their own keys, and distributing certificates after enrollment.

Remote Authentication Dial-In User Service (RADIUS) An authentication, authorization, and accounting (AAA) protocol for controlling access to network resources. RADIUS is commonly used by ISPs and corporations to manage access to the Internet or internal networks across an array of access technologies, including modems, DSL, wireless, and VPNs.

risk analysis Beyond basic identification of threats, a key design decision revolves around analyzing the probability that a threat will occur and the severity of the consequences if the threat does occur. This is called risk analysis.

Rivest Cipher (RC) algorithms A number of widely used RC algorithms or RC ciphers exist, and many were developed by Ronald Rivest. Four of the most widely used RC algorithms are RC2, RC4, RC5, and RC6. Of these, RC4 is the most popular. It is a variable key-size stream cipher that employs byte-oriented operations and is based on the use of a random permutation.

610 Rivest, Shamir, and Adleman (RSA)

Rivest, Shamir, and Adleman (RSA) Invented by Ron Rivest, Adi Shamir, and Len Adleman in 1977, RSA is one of the most common asymmetric algorithms in use today. This public-key algorithm was patented until September 2000, when the patent expired, making the algorithm part of the public domain. RSA has been widely embraced over the years, in part because of its ease of implementation and its flexibility.

role-based command-line interface (CLI) views Can be used to provide different sets of configuration information to different administrators. However, unlike making commands available via privilege levels, using role-based CLI views you can control exactly what commands an administrator has access to.

RTP Control Protocol (RTCP) Provides information about an RTP flow, such as information about the quality of the call. In a Cisco environment, RTCP typically uses odd-numbered UDP ports in the range 16,384 to 32,767.

salami attack A collection of small attacks that result in a larger attack when combined.

salt A series of random bits added to a password. When the password is hashed, and that hash is stored in a database, two identical passwords do not create the same hash. This also protects the passwords from attacks involving rainbow tables.

Secure RTP (SRTP) Secures the transmission of voice via Real-time Transport Protocol (RTP). Specifically, SRTP adds encryption, authentication, integrity, and antireplay mechanisms to voice traffic.

Secure Shell (SSH) A protocol that provides encryption and authentication functions for remote terminal sessions. This allows an administrator to securely attach to and exchange information with a router, for example. Cisco recommends that SSH be used instead of Telnet because Telnet sends data in plain text.

security level Defines the type of security algorithm performed on SNMP packets. Examples of security levels are noAuthNoPriv, authNoPriv, and authPriv.

security model Defines an approach for user and group authentication. Cisco IOS supports the SNMPv1, SNMPv2c, and SNMPv3 security models.

security policy A continually changing document that dictates a set of guidelines for network use. These guidelines complement organizational objectives by specifying rules for how the network is used.

security zone Consists of a group of interfaces to which a policy can be applied. Grouping interfaces into zones involves two steps. First, a zone must be created so that interfaces may be attached to it. Second, an interface must be configured to be a member of a given zone.

Session Initiation Protocol (SIP) Like H.323, SIP is considered a peer-to-peer protocol. SIP is a very popular protocol to use in mixed-vendor environments, perhaps because of its use of existing protocols, such as HTTP and SMTP.

SHA-1 Secure Hash Algorithm 1. One of five cryptographic hash functions known as SHA hash functions. They were designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard. SHA-1 computes a fixed-length digital representation (a message digest) from an input data sequence (the message) of any length.

signature definition file (SDF) A database of signatures used to identify malicious traffic. Modern routers typically ship with an SDF file installed in flash memory. However, the administrator usually needs to periodically update the router's SDF, because Cisco routinely updates these files to address emerging threats.

Simple Network Management Protocol (SNMP) A management protocol that allows an SNMP manager to collect information from an SNMP agent.

Skinny Client Control Protocol (SCCP) A Cisco-proprietary signaling protocol often called Skinny protocol. SCCP is often used for signaling between Cisco IP Phones and Cisco Unified Communications Manager servers. However, some Cisco gateways also support SCCP. SCCP is considered a client/server protocol, such as MGCP and H.248.

Small Computer Systems Interface (SCSI) In terms of SAN networking, the SCSI communications model serves as the basis for all the major SAN transport technologies. In fact, you could say that a SAN can best be described as the merging of SCSI and networking.

SNMP agent A piece of software that runs on a managed device (such as a server, router, or switch).

SNMP GET A message that is used to retrieve information from a managed device.

SNMP manager Runs a network management application. Sometimes called a Network Management Server (NMS).

SNMP SET A message that is used to set a variable in a managed device or to trigger an action on the managed device.

612 SNMP trap

SNMP trap An unsolicited message sent from the managed device to an SNMP manager. It can be used to notify the SNMP manager about a significant event that occurred on a managed device.

snooping Broadly defines a class of attacks focused on compromising the confidentiality of data. In terms of SAN deployments, these attacks seek to give an attacker access to data that would otherwise be confidential.

Software Encryption Algorithm (SEAL) This kind of encryption uses a 160-bit encryption key. It offers the benefit of having less of an impact on the CPU compared to other software-based algorithms. It is an alternative to software-based DES, 3DES, and AES.

spam over IP telephony (SPIT) VoIP spam. A SPIT attack on your Cisco IP Phone could, for example, make unsolicited messages periodically appear on the phone's LCD screen or make the phone ring periodically.

spoofing Imitating a given resource by alternative means. In network terms this might represent the spoofing of an IP address, where an attacker poses as the valid recipient at a given IP address to intercept traffic.

standard access control list (ACL) Standard ACLs allow traffic to be permitted or denied from only specific IP addresses. With these ACLs, the packet's destination and the ports involved are not taken into account.

static firewall This first-generation firewall technology analyzes network traffic at the transport protocol layer. IP packets are examined to see if they match one of a set of rules defining which data flows are allowed. These rules specify whether communication is allowed based on information contained in the network and transport layer headers as well as the direction of the packet flow.

storage-area network (SAN) In a SAN, storage devices are shared among all networked servers as peer resources. A SAN may be used to connect servers to storage, servers to each other, and storage to storage.

stream cipher Uses smaller units of plain text than what are used with block ciphers. Typically they work with bits. Transformation of these smaller plain-text units also varies, depending on when during the encryption process they are encountered. One of the great benefits of stream ciphers as compared to block ciphers is that they are much faster. Generally they do not increase the message size because they can encrypt an arbitrary number of bits.

supplicant A user device (such as a PC) that requests permission to access the network. This device must support the 802.1x standard. For example, a PC running the Microsoft Windows XP operating system supporting 802.1x could act as a supplicant.

Switch Port Analyzer (SPAN) port Can receive a copy of traffic crossing another port or VLAN.

symmetric algorithm Because of the simplicity of its mathematics and the speed at which it operates, a symmetric algorithm is the most commonly used form of cryptography. Symmetric encryption algorithms are also stronger. Therefore, they can use shorter key lengths compared to asymmetric algorithms. This further helps increase their speed of execution in software.

syslog A protocol used to collect log information. The logs are transmitted in clear text. A syslog logging solution consists of two primary components: syslog servers and syslog clients. A syslog server receives and stores log messages sent from syslog clients.

System Development Life Cycle (SDLC) Describes the life cycle of a component, which is broken into five phases: initiation, acquisition and development, implementation, operations and maintenance, and disposition.

Terminal Access Controller Access-Control System Plus (TACACS+) A protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

threat identification The process that network security designers use to identify what potential threats exist, regardless of the probability that the threat will be carried out.

training Creates competence on the part of the end user to perform a specific task or to serve in a specific role. Conducting a class for network administrators about the features of a Cisco Adaptive Security Appliance (ASA) is an example of training.

transform set A collection of security protocols and algorithms that can be used to establish an IKE Phase 2 (IPsec) tunnel.

Transmission Control Protocol (TCP) One of the core protocols of the Internet protocol suite. TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications such as file transfer and e-mail. It is so important in the Internet protocol suite that sometimes the entire suite is called “the TCP/IP protocol suite.” TCP is the transport protocol that manages individual conversations between web servers and web clients. TCP divides HTTP messages into smaller pieces, called segments, to be sent to the destination client. It is also responsible for controlling the size of messages and rate at which they are exchanged between the server and the client.

614 transparent firewall

transparent firewall A Layer 2 firewall that behaves like a “stealth firewall.” In other words, it is not seen as a router hop to connected devices. In this implementation, the security appliance connects the same network on its inside and outside ports. However, each interface resides on a separate VLAN.

transport mode Uses a packet’s original IP header, as opposed to adding a tunnel header for packets traveling over an IPsec-protected VPN. This approach works well in networks in which increasing a packet’s size could cause an issue.

Triple Data Encryption Standard (3DES) Applies the DES algorithm three times in a row to a plain-text block, but each application uses a different key. Applying DES three times with different keys makes brute-force attacks on 3DES unfeasible. This stems from the fact that the basic algorithm has stood the test of time, weathering 35 years in the field, proving quite trustworthy.

Trojan horse A piece of software that appears to perform a certain action but in fact performs another action, such as a computer virus. This action, generally encoded in a hidden payload, may or may not be malicious in nature.

tunnel mode Unlike transport mode, tunnel mode encapsulates an entire packet traveling over an IPsec-protected VPN. As a result, the encapsulated packet has a new IPsec header. This new header has source and destination IP address information that reflects the two VPN termination devices at two different sites. Therefore, tunnel mode is frequently used in an IPsec site-to-site VPN.

turbo access control list (ACL) Processes ACLs into lookup tables for greater efficiency. Turbo ACLs use the packet header to access these tables in a small, fixed number of lookups, independent of the existing number of ACL entries.

user datagram protocol (UDP) A communications protocol that has no error recovery features and is mostly used to send streamed material over the Internet.

VACL VLAN access control list. An ACL applied *within* a VLAN, as opposed to an ACL applied when traffic travels from one VLAN, or subnet, to another (as typically seen on a router).

virtual private network (VPN) A logical connection (sometimes called a tunnel) that can be established over an “untrusted” network (such as the Internet). An IPsec VPN can use a series of security protocols and algorithms to protect the traffic flowing over a VPN tunnel.

virtual SAN (VSAN) Created from a collection of ports that are part of a set of connected Fibre Channel switches. Together these ports form a virtual fabric. Ports within a single switch may be partitioned off to form multiple VSANs. Conversely, multiple switches may be used together, and any number of their ports may be joined to form a single VSAN.

virus A computer program that can copy itself and infect a computer without the user's permission or knowledge. A virus may spread from one computer to another only when its host is taken to the uninfected computer. For instance, a user sends the virus over a network or the Internet, or carries it on a removable medium such as a CD or USB drive. Compared to other malicious code, a virus generally requires end-user interaction. A worm, on the other hand, is based on a system vulnerability. A virus attaches itself to a file, whereas a worm lives in RAM.

vishing Maliciously collecting private information over the phone.

VLAN hopping An attack that allows traffic from one VLAN to pass into another VLAN without first being routed.

voice over IP (VoIP) Sends packetized voice over an IP network. VoIP networks use devices such as gateways to interconnect traditional telephony equipment (such as POTS phones, PBXs, and key systems) to an IP infrastructure.

vulnerability A weakness in an information system that an attacker might leverage to gain unauthorized access to a system or its data.

warm site Like a hot site, a facility that has very similar equipment to that on the original site. However, a warm site is unlikely to have current data because of a lack of frequent replication with the original site. Therefore, disaster recovery personnel typically need to go to the warm site and manually bring systems online. As a result, critical business operations might not be restored for days.

World Wide Name (WWN) Fibre Channel networks use this kind of 64-bit address to uniquely identify each element in a Fibre Channel network. These WWNs may be used in zoning to assign security permissions.

worm A self-replicating computer program that lives in RAM, rather than attaching itself to a file like a virus does. It uses a network to send copies of itself to other nodes in the network and may do so without user intervention.

X.509v3 An industry standard that has been incorporated to define basic PKI formats. Areas that are based on X.509v3 include the certificate and certificate revocation list (CRL) format.

zone-based firewall In this kind of firewall, zones establish the network's security borders. The zone itself defines a boundary where traffic is subjected to policy restrictions as it crosses into another region of the network. The default policy between zones is deny all. This means that if no policy is explicitly configured, all traffic moving between zones is blocked.

zone pair Used to specify a unidirectional firewall policy between two security zones. To define the zone pair, the **zone-pair security** command is used. The direction of the traffic flow is defined by specifying a source and destination zone. These must be security zones. The same zone cannot be defined as both the source and the destination.