



Network Security Glossary

A LIST OF FREQUENTLY USED TERMS

This glossary contains a list of terms, abbreviations, and acronyms frequently used when discussing networks security practices and products.

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

#

10BaseT; 100BaseT

An Ethernet specification that can handle up to 10 mega bits of data per second. 10BaseT Ethernet imposes differing limitations, depending on what type of physical wire is being used and how many stations are attached to the network. For example, the maximum distance a hub can be from a workstation in 10BaseT is 325 feet if using twisted pair cables, but 3,000 feet if using fiber optic cable. Most modern Ethernets are migrating to 100BaseT, which is ten times faster than 10BaseT.

A

ACL (Access Control List)

A method of keeping in check the Internet traffic that attempts to flow through a given hub, router, firewall, or similar device. Access control is often accomplished by creating a list specifying the IP addresses and/or ports from which permitted traffic can come. The device stops any traffic coming from IP addresses or ports not on the ACL.

active mode FTP (File Transfer Protocol)

One of two ways an FTP data connection is made. In active mode, the FTP server establishes the data connection. In passive mode, the client establishes the connection. In general, FTP user agents use active mode and Web user agents use passive mode.

activity light

An LED (light-emitting diode) that shines when a piece of hardware is working, communicating with the network, and transmitting data.

address learning

A method by which switches and routers determine the unique address number for each device on a network, enabling accurate transmission to and from each node.

address space probe

An intrusion technique in which a hacker sequentially scans IP addresses, generally as the information-gathering prelude to an attack. These probes are usually attempts to map IP address space as the hacker looks for security holes that might be exploited to compromise system security.

agent

A computer program that reports information to another computer or allows another computer access to the local system. Agents can be used for good or evil. Many security programs have agent components that report security information back to a central reporting

platform. However, agents can also be remotely controlled programs hackers use to access machines.

AH (authentication header)

An *IPSec* header used to verify that the contents of a packet have not been modified while the packet was in transit.

algorithm (encryption)

A set of mathematical rules (logic) for the process of encryption and decryption.

alias

A shortcut that enables a user to identify a group of hosts, networks, or users under one name. Aliases are used to speed user authentication and service configuration. For example, in configuring a Firebox a user can set up the alias "Marketing" to include the IP addresses of every network user in a company's marketing department.

API (Application Programming Interface)

Programming tools that specify standard ways software programs within a given operating environment should act, so that numerous applications can play well together. These specifications and tools enable a developer to create applications that will interact well with other applications that the developer has never seen, because all the developers are working from standardized specifications. For example, the robust APIs in Windows allow many dissimilar software products to interact upon one another (and even look similar) within the Windows environment.

Argument

See *parameter*.

armed

When a Firebox is armed, it is actively guarding against intrusion and attack.

ARP (Address Resolution Protocol)

Each device on a network has at least two addresses: a media access control (*MAC*) address, and an Internet Protocol (*IP*) address. The *MAC* address is the address of the physical network interface card inside the device, and never changes for the life of the device. The *IP* address can change if the machine moves to another part of the network or the network uses *DHCP*. *ARP*, one of the *IP* protocols, is used to match, or *resolve*, an *IP* address to its appropriate *MAC* address (and vice versa). *ARP* works by broadcasting a packet to all hosts attached to an Ethernet. The packet contains the *IP* address the sender is interested in communicating with. Most hosts ignore the packet. The target machine, recognizing that the *IP* address in the packet matches its own, returns an answer.

ARP table

A table of *IP* addresses stored on a local computer, used to match *IP* addresses to their corresponding *MAC* addresses. See also *ARP*.

ASN.1 (Abstract Syntax Notation One)

An international standard that aims at specifying data used in communication protocols. ISO/IEC standard for encoding rules used in ANSI X.509 certificates. Two common types exist: DER (Distinguished Encoding Rules) and BER (Basic Encoding Rules).

asymmetric keys

A pair of encryption keys, composed of one public key and one private key. Each key is *one way*, meaning that a key used to encrypt data cannot be used to decrypt the same data. However, information encrypted using the public key can be decrypted using the private key, and vice versa. This technology is commonly applied to e-mails, which are encrypted for confidentiality en route.

attack

An attempt to break into a system.

ATM (asynchronous transfer mode)

A networking technology that breaks data into fixed-length cells, enabling high transfer speeds. ATM is widely used for the *backbone*, or core, of the Internet.

authentication

1. The process of identifying an individual, usually based on a user name and password. Authentication usually requires something a person has (such as a key, badge, or token), something a person knows (such as a password, ID number, or mother's maiden name), or something a person is (represented by a photo, fingerprint or retina scan, etc). When authentication requires two of those three things, it is considered strong authentication.
2. A method of associating a user name with a workstation IP address, allowing the tracking of connections based on name rather than IP address. With authentication, you can track users regardless of which machine a person chooses to work from.

autopartitioning

A feature on some network devices that isolates a node within the workgroup when the node becomes disabled, so as not to affect the entire network or group.

authorization

To convey official access or legal power to a person or entity.

B**backbone**

A term often used to describe the main network connections composing the Internet.

backdoor

A design fault, planned or accidental, that allows the apparent strength of the design to be easily avoided by those who know the trick.

bandwidth

The rate at which a network segment can transfer data.

Bandwidth Meter

A monitoring tool that provides a real-time graphical display of network activities across a Firebox. This comes as a part of the application called Firebox Monitors.

bastion host

A computer placed outside a firewall to provide public services (such as World Wide Web access and *FTP*) to other Internet sites, *hardened* to withstand whatever attacks the Internet can throw at it. Hardening is accomplished by making the box as single-purpose as possible, removing all unneeded services and potential security vulnerabilities. Bastion host is sometimes inaccurately generalized to refer to any host critical to the defense of a local network.

bitmask

A pattern of bits for an IP address that determines how much of the IP address identifies the host and how much identifies the network. For example, if a bitmask of 24 were applied to the address 10.12.132.208, 10.12.132 identifies the network and the remainder of the address (1-254) can be used to specify individual machines on the 10.12.132 network.

black hat

A person of malicious intent who researches, develops, and uses techniques to defeat security measures and invade computer networks. See *white hat*.

block cipher

A procedure that translates plain text into coded text, operating on blocks of plain text of a fixed size (usually 64 bits). Every block is padded out to be the same size, making the encrypted message harder to guess.

blocked port

A security measure in which a specific port is disabled, stopping users outside the firewall from gaining access to the network through that port. The ports commonly blocked by network administrators are the ports most commonly used in attacks. See also *port*.

blocked site

An IP address outside the firewall, explicitly blocked so it cannot connect with hosts behind the firewall. Sites can be blocked manually and permanently, or automatically and temporarily.

Blue Screen of Death (BSOD)

When a Windows NT-based system encounters a serious error, the entire operating system halts and displays a screen with information regarding the error. The name comes from the blue color of the error screen.

boot up

To start a computer. Inspired by the phrase, "pull oneself up by one's boot straps."

botnet

Collection of computers that are infected with small bits of code (bots) that allow a remote computer to control some or all of the functions of the infected machines. The botmaster who controls the infected computers has the ability to manipulate them individually, or collectively as bot armies that act in concert. Botnets are typically used for disreputable purposes, such as Denial of Service attacks, click fraud, and spam.

BOVPN (Branch Office Virtual Private Network)

A type of *VPN* that creates a securely encrypted tunnel over an unsecured public network, either between two networks that are protected by the WatchGuard Firebox System, or between a WatchGuard Firebox and an IPSec-compliant device. BOVPN allows a user to connect two or more locations over the Internet while protecting the resources on the Trusted and Optional networks.

bridge

A piece of hardware used to connect two local area networks, or segments of a LAN, so that devices on the network can communicate without requiring a router. Bridges can only connect networks running the same protocol.

broadcast

A network transmission sent to all nodes on a network.

broadcast address

A special type of networking address that denotes all machines on a given network segment.

browser

See *Web browser*.

buffer overflow

The result of a programming flaw. Some computer programs expect input from the user (for example, a Web page form might accept phone numbers from prospective customers). The program allows some virtual memory for accepting the expected input. If the programmer did not write his program to discard extra input (e.g., if instead of a phone number, someone submitted one thousand characters), the input can overflow the amount of memory allocated for it, and break into the portion of memory where code is executed. A skillful hacker can exploit this flaw to make someone's computer execute the hacker's code. Used interchangeably with the term, "buffer overrun."

bus topology

A type of network design used by all Ethernet systems, in which all the devices are connected to a central cable.

C**cable segment**

A section of network cable separated by switches, routers, or bridges.

cascade

A command that arranges windows so that they are overlapped, with the active window in front.

Category 3 cabling

A cabling specification for 10BaseT networks, which are capable of handling up to 10 mega bits of data per second. See also *10BaseT / 100BaseT*.

Category 5 cabling

A cabling specification for 100BaseT networks, which are capable of handling up to 100 mega bits of data per second. See also *10BaseT / 100BaseT*.

CBC (Cipher Block Chaining)

A technique commonly used by encryption algorithms like Data Encryption Standard (*DES*) - CBC, where a plain text message is broken into sequential blocks. The first block is encrypted using a given cipher, creating cipher text. That cipher text is used to encrypt the second block of plain text. This pattern continues, with each subsequent block of plain text being encrypted using the cipher text encrypted just before it.

CD-ROM (Compact Disc Read-Only Memory)

A compact disk on which data is stored.

certificate

An electronic document attached to someone's public key by a trusted third party, which attests that the public key belongs to a legitimate owner and has not been compromised. Certificates are intended to help you verify that a file or message actually comes from the entity it claims to come from.

certificate authority (CA)

A trusted third party (TTP) who verifies the identity of a person or entity, then issues digital certificates vouching that various attributes (e. g., name, a given public key) have a valid association with that entity.

certificate revocation list

See *CRL*.

channel

1. A communications path between two computers or devices.
2. A category of topics for LiveSecurity broadcasts (e.g., Virus Alerts, Editorials, etc.). LiveSecurity Service subscribers can turn on and off which channels they receive by logging in at www.watchguard.com/archive login, and then clicking Broadcast Preferences.

CHAP (Challenge Handshake Authentication Protocol)

A type of authentication where the person logging in uses secret information and some special mathematical operations to come up with a number value. The server he or she is logging into knows the same secret value and performs the same mathematical operations. If the results match, the person is authorized to access the server. One of the numbers in the mathematical operation is changed after every log-in, to protect against an intruder secretly copying a valid authentication session and replaying it later to log in. Often contrasted with *PAP*.

CIDR (Classless Inter-Domain Routing)

Originally, Internet addresses were classified as A, B, or C. The early classification system did not envision the massive popularity of the Internet, and is in danger of running out of new unique addresses. CIDR is an addressing scheme that allows one IP address to designate many IP addresses. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number; for example, 192.168.0.0/16. CIDR is described in RFC 1519.

cipher block chaining

See *CBC*.

cipher text

The result of encrypting either characters or bits using some algorithm. Cipher text is unreadable until it is decrypted.

Class A, Class B, Class C See *Internet address class*.

clear-signed message

A message that is digitally signed but not encrypted.

See *digital signature*.

clear text

Characters in a human readable form prior to encryption or after decryption. Also called *plain text*.

click fraud

An online crime that involves automating the act of clicking on a web link to perpetrate a fraud. In a classic click fraud scenario, a legitimate web site decides to advertise on another site, which hosts the ad. The legitimate web site agrees to pay the ad hosting site a few cents each time a potential customer clicks on the ad, which links back to the legitimate site. Cheaters use automated tools to click the ad over and over, earning money from the legitimate site under false pretenses (since the clicks do not come from actual people interested in the advertised products). Some click fraud attacks are launched by companies that use them to deplete the advertising budget of a competitor. Other click fraud scenarios can bias the results of a poll or vote.

client

A computer process that requests a service from another computer and accepts the server's responses.

Client/Server

A network computing system in which individual computers (clients) use a central computer (server) for services such as file storage, printing, and communications. See *peer-to-peer*.

coax (coaxial) cable

A type of cable, used in Ethernet networking, with a solid central conductor surrounded by an insulator, in turn surrounded by a cylindrical shield woven from fine wires. The shield minimizes electrical and radio frequency interference.

cold boot

The process of starting a computer by turning on the power to the system unit.

collisions

Conflicts that occur when two packets are sent over the network simultaneously. When packets collide, both packets are rejected. Ethernet automatically resends them at altered timing.

compress

To compact a file or group of files so that they occupy less disk space. See also *decompress*.

compression function

A function that accepts input and returns a shorter output. One common program that performs this is WinZIP.

Control Panel

The set of Microsoft Windows programs used to change system hardware, software, and settings.

conventional encryption

See *symmetric algorithm*.

cookie

A text file passed from the Web server to the Web client (a user's browser) that is used to identify a user and could record personal information such as ID and password, mailing address, credit card number, and more. A cookie is what enables your favorite Web site to "recognize" you each time you revisit it.

coprocessor

A microprocessor designed to assist another microprocessor in specific functions, such as handling complex mathematics or graphics, and to temporarily reduce the workload of the other microprocessor.

CPU (Central Processing Unit)

The microprocessor chip that interprets and carries out most of the instructions you give your computer. Also, simply, a term for a computer.

cracker

Another term for someone who attempts to defeat network security measures, with hostile intent. Commonly used in popular media as a synonym for hacker.

CRL (Certificate Revocation List)

An up-to-date list of previously issued certificates that are no longer valid. See also *revocation*.

cross-certification

A status where two or more organizations or certificate authorities share some level of trust.

crossover cable

Ethernet cables have multiple wires inside them. Some are dedicated to sending; some are dedicated to receiving. A crossover cable is a special cable in which the receive and send wires cross so that the sending leads on one device can directly connect to the receiving leads on the other device. When WatchGuard encloses a crossover cable with its products, it is typically color-coded red for easy identification.

cross-site scripting

An attack performed through Web browsers, taking advantage of poorly-written Web applications. Cross-site scripting attacks can take many forms. One common form is for an attacker to trick a user into clicking on a specially-crafted, malicious hyperlink. The link appears to lead to an innocent site, but the site is actually the attacker's, and includes embedded scripts. What the script does is up to the attacker; commonly, it collects data the victim might enter, such as a credit card number or password. The malicious link itself might also collect the victim's *cookie* data.

cryptanalysis

The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

CRYPTOCard

One element in a proprietary authentication system, which uses an offline card containing a large secret key to answer security "challenges" from the network. The large number inside the card, called a key, is like a hard-to-guess password used in encrypting and decrypting. The key is never stored on a computer, which increases its safety against unauthorized discovery.

cryptography

The art and science of encoding and decoding messages using mathematical algorithms that utilize a secret key. The concept has broadened to include managing messages that have some combination of: privacy (by being unreadable to anyone but the sender and receiver); integrity (not modified while en route), and non-repudiation (digitally signed in such a way that the originator cannot plausibly claim he or she did not originate it).

CSLIP (Compressed Serial Line Internet Protocol)

A protocol for exchanging IP packets over a serial line, which *compresses* the *headers* of many *TCP/IP* packets.

custom filter rules

A filter rule is a configuration setting to either deny or allow specific content types through the Firebox. A custom filter rule is a rule a Firebox user created in WatchGuard Policy Manager, in contrast with the pre-made rules WatchGuard created for the Firebox.

CVE-compatible

Common Vulnerabilities and Exposures (CVE) is a list of standardized names for vulnerabilities and other information security exposures, whose aim is to standardize the names for all publicly known vulnerabilities and security exposures. "CVE-compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names.

D

data compression

See *compress*.

datagram

A packet of data that contains information, plus origin and destination addresses. Generally used in reference to UDP and ICMP packets when talking about IP protocols.

data transmission speed

The number of bits that can travel per second over a network cable, typically measured in bits per second (bps).

DCE-RPC (Distributed Computing Environment Remote Procedure Call)

A Microsoft implementation of a portmapping service. A portmapper is a service that runs on a specific *port*, redirecting clients that send a request to that port. These initial calls typically result in a response from the trusted machine that redirects the client to a new port for the actual service the client wants. See also *RPC*.

DDoS

See *denial of service attack (DoS)*.

decompress

To expand a compressed file or group of files back to their normal size so that the file or files can be opened. See also *compress*.

decrypt

To decode data that has been encrypted, turning it back into plain text. See also *encrypt*.

dedicated server

A single computer in a network, reserved for serving the needs of the network.

default

A predefined setting built into a program, used when an alternative setting is not specified.

default gateway

When individual machines on a network segment send data packets, they check the packet's destination to figure out whether the destination is local (meaning, on the same *network segment*) or not. If the packet's destination is not local, the machine forwards it to a node on the network serving as the entrance to all other networks. This node is called the default gateway, and could be any routing device, such as a router or a firewall appliance.

default packet handling

A set of rules that instruct the Firebox on how to process packets when no other rules have been specified. For example, by default the Firebox logs any packet sent to a broadcast address.

denial of service attack (DoS)

A type of attack aimed at making the targeted system or network unusable, often by monopolizing system resources. For example, in February 2000 a hacker directed thousands of requests to eBay's Web site. The network traffic flooded the available Internet connection so that no users could access eBay for a few hours. A *distributed denial of service* (DDoS) involves many computer systems, possibly hundreds, all sending traffic to a few choice targets. The term "Denial of Service" is also used imprecisely to refer to any outwardly-induced condition that renders a computer unusable, thus "denying service" to its rightful user.

DES (Data Encryption Standard)

A commonly-used encryption algorithm that encrypts data using a key of 56 bits, which is considered fairly weak given the speed and power of modern computers. Until recently it was the US government's encryption standard, but it has largely been replaced by Triple-DES and AES. See also *Triple-DES*.

device

A generic term for computer equipment such as a hub, switch, router, or printer.

DHCP (Dynamic Host Configuration Protocol)

A standard proposed in RFC 1541 for transferring network configuration information from a central server to devices as the devices boot up. This data typically includes a machine's IP address, which the server can change and allocate automatically (on the fly) under DHCP.

DHCP server

A device that automatically assigns IP addresses to networked computers from a defined pool of numbers, returning unused IP addresses to the pool. Using a DHCP server, an administrator normally does not have to get involved with the details of assigning IP addresses to individual clients.

dialog box

A box that appears when you choose a command from a menu. It offers additional options, and requires your acknowledgement before it goes away.

dial-up connection

A connection between a remote computer and a server, established using software, a modem, and a telephone line.

dictionary attack

An attempt to guess a password by systematically trying every word in a dictionary as the password. This attack is usually automated, using a dictionary of the hacker's choosing, which may include both ordinary words and jargon, names, and slang.

Diffie-Hellman

A mathematical algorithm that allows two users to exchange a secret key over an insecure medium without any prior secrets. This protocol, named after the inventors who first published it in 1976, is used in Virtual Private Networking (*VPN*).

digital signature

An electronic identification of a person or thing, intended to verify to a recipient the integrity of data sent to them, and the identity of the sender. Creating a digital signature involves elaborate mathematical techniques that the sender and recipient can both perform on the transmitted data. Performing identical formulas on identical data should produce identical results at both the sending and receiving end. If the recipient's results do not equal the sender's results, the message may have been tampered with en route. If the message was modified after being sent -- even if all someone did was change the punctuation on a sentence, or added an extra space between two of the words -- you could tell. A digital signature typically depends upon three elements: *public key encryption*, a *Certificate Authority*, and a digital *certificate*.

disarmed

The state of a Firewall when it is not actively protecting a network.

DLL (Dynamic Link Library)

In Microsoft Windows, a Dynamic Link Library is a collection of *functions* that perform very commonly used tasks. This library is intended to be a universal resource that any program can use, reducing the need to have similar snippets of code existing on a computer in multiple places. Windows comes with many DLLs that programs can use to get the recognized "Windows" feel.

DMZ (Demilitarized Zone)

A partially-protected zone on a network, not exposed to the full fury of the Internet, but not fully behind the firewall. This technique is typically used on parts of the network which must remain open to the public (such as a Web server) but must also access trusted resources (such as a database). The point is to allow the inside firewall component, guarding the trusted resources, to make certain assumptions about the impossibility of outsiders forging DMZ addresses. WatchGuard refers to the DMZ as the *Optional network interface*.

DNS (Domain Name System)

A network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. This is what allows your computer network to understand that you want to reach the server at 192.168.100.1 (for example) when you type into your browser a domain name such as www.watchguard.com.

DNS cache poisoning

A clever technique that tricks your DNS server into believing it has received authentic information when, in reality, it has been lied to. Why would an attacker corrupt your DNS server's cache? So that your DNS server will give out incorrect answers that provide *IP addresses* of the attacker's choice, instead of the real addresses. Imagine that someone decides to use the Microsoft Update Web site to get the latest Internet Explorer patch. But, the attacker has inserted phony addresses for update.microsoft.com in your DNS server, so instead of being taken to Microsoft's download site, the victim's browser arrives at the attacker's site and downloads the latest worm.

DNS lookup

The Domain Name Service act of matching a friendly, readable domain name (such as www.watchguard.com) to its associated *IP address*.

DNS spoofing

An attack technique where a hacker intercepts your system's requests to a DNS server in order to issue false responses as though they came from the real DNS server. Using this technique, an attacker can convince your system that an existing Web page does not exist, or respond to requests that should lead to a legitimate Web site, with the IP address of a malicious Web site. This differs from *DNS cache poisoning* because in DNS spoofing, the attacker does not hack a

DNS server; instead, he inserts himself between you and the server and impersonates the server.

domain name hijacking

An attack technique where the attacker takes over a domain by first blocking access to the victim domain's *DNS* server, then putting up a malicious server in its place. For example, if a hacker wanted to take over fnark.com, he would have to remove the fnark.com DNS server from operation using a *Denial of Service* attack to block access to fnark's DNS server. Then, he would put up his own DNS server, advertising it to everyone on the Internet as fnark.com. When an unsuspecting user went to access fnark.com, he would get the attacker's domain instead of the real one.

Domain Name System (DNS) See *DNS*.

DoS

See *denial of service attack*.

dotted notation

The notation used to write IP addresses as four decimal numbers separated by dots (periods), sometimes called dotted quad. Example:
123.212.12.4.

driver

A software program that manipulates a device (such as a printer, keyboard, mouse, or hard drive). The driver accepts generic commands from a program and then translates them into specialized commands for the device.

drop-in mode

A network configuration in which the Firebox is physically located between the router and the LAN without any of the computers on the Trusted interface being reconfigured. This is a quick and simplified way to get the Firebox into the network, but can only protect a single network that is not subdivided into smaller networks. See also *proxy ARP*. For a contrasting approach, see *routed mode*.

drop-in network

A network being used in drop-in mode. See *drop-in mode*.

DSA (Digital Signature Algorithm)

A public key digital signature algorithm proposed by the National Institute of Standards and Technology.

DSS (Digital Signature Standard)

A standard for digital signatures proposed by the National Institute of Standards and Technology.

DVCP (Dynamic VPN Configuration Protocol)

A WatchGuard proprietary protocol that simplifies configuration of *VPNs*. A DVCP server provides centralized storage of all configured devices under management and builds Virtual Private Networks quickly and interactively for those devices.

Dynamic Link Library

See *DLL*.

dynamic NAT

On outgoing requests from your network, the Firebox replaces all private IP source addresses with one public address (usually its own). See *Network Address Translation*, and *IP masquerading*.

dynamic packet filtering

See *stateful packet filtering*.

E

ECC (Elliptic Curve Cryptosystem)

A method for creating public key algorithms, which some experts claim provides the highest strength-per-bit of any cryptosystem known today. Its algorithms accept an encryption key but then add extra numbers representing the coordinates of points on an imaginary wiggly curve as it crosses an imaginary line. Its complicated algebraic approach allows shorter keys to produce security equivalent to longer keys in other cryptosystems (such as RSA). Shorter keys mean the encryption and decryption can be performed relatively quickly and with less computer hardware. Numerous experts believe ECC will eventually enjoy widespread use.

elevation of privilege

Almost every computer program has some notion of "privilege" built in, meaning, permission to do some set of actions on the system. This permission is granted to individuals based on their ability to present proper credentials (for example, a username and password). Privilege has levels -- for example, a guest account typically has fewer privileges than an administrator account. Many network attacks begin with an attacker obtaining limited privileges on a system, then attempting to leverage those privileges into greater privileges that might ultimately lead to controlling the system. Any attempt to gain greater permissions illicitly (typically, by impersonating a privileged user or otherwise bypassing normal *authentication*) is considered an elevation of privilege.

encryption

The process of disguising data to hide its content. As used in a network security context, encryption is usually accomplished by putting the data through any of several established mathematical algorithms developed specifically for this purpose.

entropy

In cryptography, a mathematical measurement of the amount of uncertainty or randomness.

ESMTP (Extended Simple Mail Transfer Protocol)

A protocol that provides extensions to *SMTP* for sending e-mail that supports graphics, audio, and video files, and text in various foreign languages. These extensions were first described in RFC 1869.

ESP (Encapsulating Security Payload)

An IPSec protocol used in WatchGuard's Branch Office VPN. ESP encrypts all or part of a packet of data in a way that assures confidentiality even though the data travels over the public Internet. It provides data integrity, and offers assurance of the identity of the data's sender (authentication).

Ethernet

One of the least expensive, most widely deployed networking standards, enabling the transmission of data at 10 million bits per second (Mbps), using a specified protocol. A more recent Ethernet standard, called 100BaseTx, enables data to be transmitted and received at 100 Mbps.

Ethernet address

A unique ID number obtained automatically when an Ethernet adapter is added to a computer. This address identifies the machine as a unique communication item and enables direct communications to and from that particular computer. See also *MAC address*.

event

Any network incident that prompts some kind of log entry or other notification.

Event processor

See *WatchGuard Security Event Processor*.

extension

See *file extension*.

External interface

On the Firebox, an Ethernet port intended for connecting to the portion of your network that presents the greatest security risk (typically the Internet and any other switches, routers, or servers connected to, but outside, your network).

External network

Any network that can connect to yours, with which you have neither a trusted or semi-trusted relationship. For example, a company's employees would typically be trusted on your network, a primary vendor's network might be semi-trusted, but the public Internet would be untrusted — hence, External.

F**failover**

A configuration that allows a secondary machine to take over in the event of a stoppage in the first machine, thus allowing normal use to return or continue. See also *high availability*.

failover logging

A process in which the Firebox immediately establishes contact with a secondary log host, in the event that the Firebox cannot communicate with the primary log host.

fail-shut mode

A condition in which a firewall blocks all incoming and outgoing network traffic in the event of a firewall failure. This is the opposite of fail-open mode, in which a firewall crash opens all traffic in both directions. Fail-shut is the default failure mode of the WatchGuard Firebox System.

fast Ethernet

An Ethernet networking system that transmits data at 100 million bits per second (Mbps), ten times the speed of an earlier Ethernet standard. Derived from the Ethernet 802.3 standard, it is also known as *100Base-T*.

file server

A dedicated network computer that stores data files so that other computers can share access to them. See also *client/server*.

filtering process

Deciding whether a packet should be allowed or denied, depending on what is contained in its header or its contents, based on user-defined policies.

fingerprint

A unique identifier for a key that is obtained by hashing specific portions of the key data. See *one-way hash function*.

file extension

Under Windows, a period and up to three characters at the end of a file name. The extension can help identify the type of file, and often helps a computer know what to do with the file. For example, if a file is named *glossary.exe*, the file extension is ".exe." The .exe tells a Windows computer that the glossary file is executable.

filters

Small, fast programs in a firewall that examine packets as they arrive at the firewall and route or reject the packets based on user-definable rules.

Firebox

The WatchGuard firewall appliance.

Firebox Monitors

A suite of WatchGuard Firebox System observation tools combined into a single user interface accessible from Firebox® System Manager. Firebox Monitors allows you to keep an eye on bandwidth usage, who has authenticated to the Firebox, what Web sites have been automatically blocked because they sent questionable traffic, and more.

Firebox® System Manager

WatchGuard's toolkit of applications enabling configuration, management, and monitoring of a network security policy.

firewall

Software or hardware components that restrict access between a protected network and the Internet, or between other sets of networks, to block unwanted use or abuse.

flash disk

An 8-megabyte, on-board flash ROM disk that acts like a hard disk in a Firebox. The word "flash" arises from the fact that it can be erased and reprogrammed rapidly, in blocks instead of one byte at a time.

forward DNS lookup

See *DNS lookup*

FQDN (Fully Qualified Domain Name)

A fully qualified domain name consists of a host and domain name, including a top-level domain such as .com, .net, .gov, .edu, etc. For example, www.watchguard.com is a fully qualified domain name. www is the local host, watchguard is the second-level domain, and .com is the top level domain.

FTP (File Transfer Protocol)

The most common protocol for copying files over the Internet. See also *active mode FTP*.

Fully Qualified Domain Name

See *FQDN*.

Function

In programming, a function is part of a program that performs a specific task. Computer programs usually consist of modules of code. Each module consists of a small part of the program written to perform one specific task. These small, special-purpose chunks of code are called *functions*. When a program runs, it calls different functions to perform certain tasks. For example, a programmer could write a function to alphabetize a list of names. When the program got to the place where it needed to alphabetize a list of names, the program would call the alphabetizing function, and the function would return the list of names in the correct order. If those names then had to be inserted into a database, the program might call a different function to accomplish that. See also parameter and Dynamic Link Libraries.

G**gateway**

A system that provides access between two or more networks. Gateways are typically used to connect networks that are dissimilar. The Firebox often serves as the gateway between the Internet and your network.

GUI (Graphical User Interface)

The visual representation on a computer screen that allows users to view, enter, or change information. It is characterized by icons and commonly utilizes a mouse, in contrast to a Command Line Interface (CLI), which uses strictly text.

H

handshake

See *TCP handshake*.

hash code

A unique, mathematical summary of a document that serves to identify the document and its contents. See *message digest*.

header

A series of bytes at the beginning of a communication packet that provides information about the packet such as its computer of origin, the intended recipient, packet size, and destination port number. The header of a packet is like the envelope of a traditionally-mailed letter, in that it conveys "return address" and "intended recipient" information but is not the real content of the message.

hexadecimal

A base-16 numbering system (from *hexadecem*, Latin for 16) particularly important in computer programming, since four bits (each consisting of a one or zero) are succinctly expressed using a single hexadecimal digit. Hexadecimal resembles decimal (base-10) numbering with the digits 0 through 9, but the decimal equivalents of 10 - 16 are represented in hexadecimal by the letters A through F. Example: the decimal number 252 is written in hexadecimal as FC.

hierarchical trust

A method of organizing "trust" within an organization by allowing one Certificate Authority to delegate a portion of its responsibility to a subordinate Certificate Authority. For example, a business might have a master Certificate Authority, which vouches for a Certificate Authority at the company's Los Angeles office, which vouches for a Certificate Authority at the company's Phoenix office. Commonly used in ANSI X.509 certificates.

High Availability

High Availability enables the installation of two Fireboxes so that if one fails for any reason, the other takes over immediately. This minimizes data loss while the failed box is replaced or repaired.

Historical Reports

A WatchGuard Firebox System application that creates HTML reports of Firebox log files, displaying session types, most active hosts, most used services, and other information useful in monitoring and troubleshooting a network.

HMAC (Hashed Message Authentication Code)

A mechanism for message *authentication*, using cryptographic *one-way hash* functions, based upon RFC 2104 and commonly used in *VPNs*. The end result is that when you receive a data packet, you can know that whoever sent the packet possesses the same secret key that you do. You can combine this with other technologies, such as *IKE*, to know who sent a given message.

home page

The first page of a multi-page Web site, used as an entrance into the site.

host

A network-connected computer.

host route

A network configuration where a router sits between the Firebox and an internal host. For the Firebox to be able to send data to the host, it must be informed of the existence of the additional router (and the host behind it). This entry in the Firebox's routing table is the *host route*.

HostWatch™

A WatchGuard Firebox® System Manager application that provides a real-time display of which hosts are connected from behind the Firebox to hosts on the Internet.

HTML (HyperText Markup Language)

A simple programming language used to format Web pages, including methods to specify text characteristics, graphic placement, and links. HTML files are written in plain text, then read or interpreted by a Web browser.

HTTP (HyperText Transfer Protocol)

A communications standard designed and used to transfer information and documents between servers or from a server to a client. This standard is what enables your Web browser to fetch pages from the World Wide Web.

HTTPS (Secure HTTP)

A variation of HTTP enabling the secure transmission of data. Generally used in conjunction with Secure Sockets Layer (*SSL*), which encrypts the HTTP.

hub

A device that serves as a common connection point for multiple devices on a network. There are several different types of hubs, but in general each receives and sends signals to all the devices connected to it.

hyperlink

An object on a Web page such as a graphic or underlined text that represents a link to another location, either on the same Web site or on a different Web site. When a user clicks on a hyperlink, a page or graphic from the linked location appears in the user's Web browser.

I**IANA** (Internet Assigned Number Authority)

The central authority charged with assigning parameter values (numbers) to Internet protocols. For example, IANA controls the assignment of well-known TCP/IP port numbers. Currently IANA manages port numbers 1 through 1023.

ICANN (Internet Corporation for Assigned Names and Numbers)

A non-profit, private-sector corporation formed by a broad coalition of the Internet's business, technical, academic, and user communities. ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.

ICMP (Internet Control Message Protocol)

A protocol used to pass control and error messages back and forth between nodes on the Internet. Perhaps the most used ICMP command is *ping*.

identity certificate

A signed statement that binds a public encryption key to the name of an individual and therefore delegates authority from that individual to the public key. Any message encrypted with that person's public key can then be regarded as being from that person.

IDS (Intrusion Detection System)

A class of networking products devoted to detecting attacks from hackers. Network-based intrusion detection systems examine the traffic on a network for signs of unauthorized access or attacks in progress, while host-based systems look at processes running on a local machine for activity an administrator has defined as "bad."

IEEE (Institute of Electrical and Electronics Engineers)

Pronounced "eye-triple-E." An organization of engineers, scientists, and students who issue

standards related to electrical, electronic, and computer engineering. For example, IEEE developed the standards for using Ethernet, token ring, and WiFi.

IETF (Internet Engineering Task Force)

A large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. *IANA* is chartered by one of the IETF's working groups.

IKE (Internet Key Exchange)

A standard proposed in RFC 2409 used with IPSec virtual private networks (VPNs) for automating the process of negotiating encryption keys, changing keys, and determining when to change keys. IKE first mutually *authenticates* the two endpoints that plan to set up IPSec *tunnels* between them; then the endpoints can establish mutually agreed-upon security parameters.

initialization vector

A block of arbitrary data that serves as the starting point for a block cipher like Triple-DES. See also *cipher block chaining*.

initialize

To prepare (a disk) for information storage.

installation wizard

A software tool specifically designed to guide a user through the process of installing a new application.

integrity; data integrity

The concept that you can discern whether data is in the condition its authors or owners intend it to be, and that it has not been modified by unauthorized persons during storage or transmittal.

interface

A boundary across which two independent systems meet and act on or communicate with each other. The term sometimes refers to the wires, plugs, and sockets that hardware devices use to communicate with each other. Other times, it refers to the style in which a software program receives and responds to user input; for example, command line interface or *graphical user interface*.

Internet address class

Historically, to efficiently administer the whole range of possible 32-bit IP addresses, the addresses were separated into three classes that describe networks of varying sizes: **Class A** - If the first octet of an IP address is less than 128, it is a Class A address. A network with a Class A address can have up to about 16 million hosts. *Example: 64.64.10.1*. **Class B** - If the first octet of an IP address is from 128 to 191, it is a Class B address. A network with a Class B address can have up to 64,000 hosts. *Example: 155.155.24.301*. **Class C** - If the first octet of an IP address is from 192 to 223, it is a Class C address. A network with a Class C address can have up to 254 hosts. *Example: 192.168.14.4*. Modern addressing techniques favor classless routing, rendering these class categorizations less and less relevant. See also *network address*.

Internet Engineering Task Force

See *IETF*.

intranet

A self-contained network with a limited number of participants who extend limited trust to one another in order to accomplish an agreed-upon goal. For example, a manufacturer and its key vendors might create an intranet to facilitate managing the process of turning raw materials into finished products.

Intrusion Detection System

See *IDS*.

IP (Internet Protocol)

A fundamental set of detailed specifications that controls how data packets are formatted and how they move from one networked computer to another.

IP address

An understanding of IP addresses is foundational for managing a network, so we go into some depth with this definition. In short, an IP address is a numeric identifier that represents a computer or device on a TCP/IP network. The devices on the network rely on the address in order to know where to route data. The format of an IP address is a 32-bit number divided into four 8-bit segments, separated by periods. The four segments, called octets, can be represented in binary notation (ones and zeros, the basic building blocks of all software) like this: 11010000.10001100.00100011.00000010. Because writing so many ones and zeros is inefficient and laborious for humans, IP addresses are usually converted to decimal notation when written out (but remember, the machines always understand them as ones and zeros). For example, the same binary address above, expressed in decimal, is 208.140.35.2. In decimal notation, no octet can have a value greater than 255. This is because binary requires 9 ones and zeros to express a number greater than 255, and the rules for IP addresses only allow 8. Some portion of any IP address designates a network, and the remaining portion of the address designates a specific device on that network.

IP fragment

A formatted portion of data that is part of a larger IP packet. IP fragments are typically used when an IP packet is too large for the physical media that the data must cross. For example, the IP standard for Ethernet limits IP packets to about 1,500 bytes, but the maximum IP packet size is 65,536 bytes. To send packets larger than 1,500 bytes over an Ethernet, IP fragments must be used.

IP masquerading

See *NAT*.

IP options

Extensions to the Internet Protocol used mainly for debugging and for special applications on local networks. In general, there are no legitimate uses of IP options over an Internet connection.

IP options attack

A method of gaining unauthorized network access by utilizing IP options.

IPSec (Internet Protocol Security)

An open-standard methodology of exchanging data over the public Internet while protecting the data from prying eyes as it travels from the originator to the recipient. IPSec provides encryption and authentication options to maximize the confidentiality of data transmissions, employing cryptographic protocols in conjunction with *IKE* and *ISAKMP*. The IETF chartered the IPSec work group to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality. IPSec standards are commonly employed when establishing a *VPN*.

IP spoofing

The act of inserting a false (but ordinary-seeming) sender IP address into the "From" field of an Internet transmission's header in order to hide the actual origin of the transmission. There are few, if any, legitimate reasons to perform IP spoofing; the technique is usually one aspect of an attack.

ISAKMP (Internet Security Association Key Management Protocol)

A set of specifications defined in RFC 2408 and used in close conjunction with *IPSec*. Defines the procedures for authenticating, creating and managing security associations, generating keys, and using digital certificates when establishing VPN connections.

ISO (International Organization for Standardization)

An international organization composed of national standards bodies from over 75 countries. For example, ANSI (American National Standards Institute) is a member of ISO. ISO has defined a number of important computer standards, the most significant of which is perhaps OSI (Open Systems Interconnection), a standardized architecture for designing networks.

ISP (Internet service provider)

A business that sells access to the Internet. A government bureau or an educational institution may be the ISP for some organizations.

ITU-T (International Telecommunication Union-Telecommunication)

Formerly the CCITT (Consultative Committee for International Telegraph and Telephone), a worldwide telecommunications technology standards organization. Just as IETF and ICANN propose and maintain standards for the Internet, ITUT proposes and establishes standards for international telephony.

See *initialization vector*.

J**Java applet**

A small program written in the Java programming language that can be included on an HTML page, much in the same way an image is included. When someone uses a Java-enabled browser to view a page that contains an applet, the applet's code is transferred to that user's system and executed by the browser's Java virtual machine (JVM). For example, if you access a Web page that shows a virtual stock ticker streaming by with live data, that might be enabled by a Java applet.

K**Kerberos**

A trusted third-party authentication protocol developed at Massachusetts Institute of Technology and used widely in the United States. Unlike other authentication schemes, Kerberos does not use public key technology. Instead, it uses symmetric ciphers and secrets shared between the Kerberos server and each individual user. Each user has a unique password, and the Kerberos server uses this password to encrypt messages sent to that user, so the message can't be read by anyone else.

key

A secret code, most often expressed as a numeric value, used to encrypt a message, to make the text unreadable to anyone but the intended recipient. If a message encrypted by a key must be decrypted by using the same key, the key is called a *symmetric key*. If a message encrypted by a key must be decrypted using a different key, the keys are called *asymmetric keys*, or a *key pair*. Key pairs (usually comprised of a public key and a private key) form the basis of public key cryptography.

key exchange

A scheme for two or more nodes to transfer a secret session key across an unsecured channel, such as the Internet.

key fingerprint

A uniquely identifying string of numbers and characters used to authenticate public keys.

key ID

A code that uniquely identifies a key pair. Two key pairs can have the same user ID, but they have different key IDs. See also *key* and *key fingerprint*.

key length

The number of bits representing the key size; the longer the key, the stronger it is.

key management

The process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic keys to authorized recipients in a secure manner.

key pair

Public key cryptography uses a pair of key codes related to each other in this way: if you *lock-up* data using one key code, you can only unlock it using the other key code. And vice versa. One of the keys is made known publicly, while the other is kept private. The two, together, form a key pair. See also *key* and *keyring*.

keyring

A set of digital codes, or keys, used to encrypt and decrypt messages in asymmetric cryptography. Each user has two types of keyrings: a private keyring and a public one. People who wish to receive encrypted messages typically publish their public keys in directories or make their keys otherwise available. To send them an encrypted message, all you have to do is get a copy of their public key, use the public key to encrypt your message, and send it to them. The only person who can decrypt the message is the person who possesses the matching private key.

key splitting

The process of dividing a private key into multiple pieces and sharing those pieces among several users. A designated number of users must bring their shares of the key together to use the key.

L**LAN (local area network)**

A computer network that spans a relatively small area, generally confined to a single building or group of buildings.

LDAP (Lightweight Directory Access Protocol)

A protocol that helps manage information about authorized users on a network such as names, phone numbers, addresses, and what a user is and is not allowed to access. LDAP is vendor- and platform-neutral, working across otherwise incompatible systems.

LED (light-emitting diode)

A small indicator light on a networking device that indicates status and other information about the device. For example, an LED on the WatchGuard SOHO blinks to indicate when the SOHO is receiving data.

link

See *hyperlink*.

Linux

An open source version of the UNIX operating system.

LiveSecurity® Service

See *WatchGuard LiveSecurity Service*.

log host, logging host

A designated device for receiving and storing a record of events from another device or program (such as a Firebox, SOHO, or ServerLock).

LogViewer

A WatchGuard Firebox® System Manager application for viewing Firebox log files.

loopback interface

A special type of interface that allows you to make network connections to yourself, using IP. This convention, which all Internet-aware applications expect and utilize, has a variety of purposes, including routing and application testing.

M

MAC (Machine Authentication Code)

A way to check the integrity of information transmitted over, or stored on, an unreliable medium, based on a secret key. Typically, MACs are used between two parties who share a secret key, in order to validate the information transmitted between the two parties. key-dependent, one-way hash function, requiring the use of the identical key to verify the hash. See also *HMAC*.

MAC address (Media Access Control)

One of the two addresses every networked computer has (the other being an IP address), a Media Access Control address is a unique 48-bit identifier usually written as 12 hexadecimal characters grouped in pairs (e. g., 00-00-0c-34-11-4e). This address is usually hard-coded into a Network Interface Card (NIC) by its manufacturer, and does not change. It is the physical address of a data device, and is used as an aid for routers trying to locate machines on large networks. See also *ARP* and *Ethernet address*.

mail server

Refers to both the application and the physical machine tasked with routing incoming and outgoing electronic mail.

Management Station

The computer on which the WatchGuard Firebox System Firebox® System Manager and Policy Manager run. In its simplest terms, this is the computer you use to configure and monitor a WatchGuard Firebox.

masquerading

In the WatchGuard Firebox System, masquerading sets up addressing so that a Firebox presents its IP address to the outside world in place of the private IP addresses of the hosts protected by the Firebox. See also *NAT*.

MD2 (Message Digest 2)

128-bit, one-way hash function that is dependent on a random permutation of bytes. MD2 is considered very secure, but takes a long time to compute, and therefore is rarely used. See also *message digest*.

MD4 (Message Digest 4)

A 128-bit, one-way hash function that uses a simple set of bit manipulations on 32-bit operands, developed as a weaker but faster alternative to MD2. See also *message digest*.

MD5 (Message Digest 5)

A more secure, more complex version of MD4, but still a 128-bit, one-way hash function. Although now widely used, MD5 contains a few flaws discovered in 1996 making it slightly weaker, so it is gradually falling out of favor in deference to another message digest function known as SHA-1. See also *message digest*.

message digest

A mathematical function used in encryption to distill the information contained in a file into a single large number, typically between 128 and 256 bits in length. Message digests are also known as *one-way hash* functions because they produce results where it is mathematically

infeasible to try to calculate the original message by computing backwards from the result. Message digest functions are designed so that a change to a single character in the message will cause the message to result in a very different message digest number. Many different message digest functions have been proposed and are now in use; most are considered highly resistant to attack.

MIME (Multipurpose Internet Mail Extensions)

A specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

MIME type

Though MIME was developed for email (SMTP), it proved so useful that other application protocols also adopted it. For example, HTTP uses MIME headers to indicate what sort of data is being transferred. RFC 2046 defines how MIME can handle various media types, such as image, audio, video, and application. MIME content types are expressed as a type and a subtype, separated by a slash. (Example: image/jpeg).

modem

A shortened version of "modulator/demodulator," this is the word for a communications device that sends computer transmissions over a standard telephone line.

motherboard

The main printed circuit board in a computer, which contains sockets that accept additional boards (daughterboards).

MSDUN

An abbreviation for Microsoft Dial-Up Networking, required for *remote user VPN*.

multiple network configuration

See *routed mode*.

N

name resolution

The successful look-up of an IP address to discover the name of the networked computer it indicates. See *DNS*.

NAT (Network Address Translation)

A technology where you advertise one IP address for the world to send stuff to (e-mails, HTTP, database traffic, whatever). Then the Firewall translates that request from the outside world and sends it to the appropriate IP address inside your network. In this way, the Firewall can hide from outsiders the IP addresses of machines on your internal network. Various techniques for applying NAT include *dynamic NAT*, and *static NAT*. Some people use the term NAT interchangeably with *masquerading*.

National Institute for Standards and Technology

See *NIST*.

NetBIOS (Network Basic Input/Output System)

An older proprietary Microsoft networking protocol that enables a computer to connect to and communicate with a Local Area Network (*LAN*).

NetBEUI (NetBIOS Extended User Interface)

A non-routable networking protocol used by smaller, non-*subnetted* networks for internal communications. Because NetBEUI is not publicly routable, network transmissions sent via NetBEUI cannot be transmitted over the Internet.

network address

The network portion of an Internet Protocol (*IP*) address. For a Class A network, the network address is the first byte of the IP address (e.g., in 74.10.10.10, the network address is 74). For a class B network, the network address is the first two bytes of the IP address (e.g., in 128.10.10.10, the network address is 128.10). For a class C network, the network address is the first three bytes of the IP address (e.g., in 192.168.10.10, the network address is 192.168.10). In each case, the remaining bits can be used to identify specific computers, often called *hosts*. In the Internet, assigned network addresses are globally unique; that is, a computer cannot have the same IP address as any other computer with which it can communicate. See also *CIDR block addressing*, *Internet address class*, and *subnet mask*.

network address translation

See *NAT*.

netmask

See *subnet mask*.

Network Configuration wizard

Automated software presenting a series of windows. The various windows and fields prompt you for essential information that helps create a basic Firebox configuration.

network adaptor, network interface card (NIC)

A device that sends and receives data between the computer and the network cabling. Every computer attached to a network must have a NIC.

network range

See *subnet mask*.

network segment

A subdivision of a computer network, bounded by a device such as a router, switch, or even a Firebox. Dividing an Ethernet into multiple segments is a common way of increasing available bandwidth on the individual segments.

NFS (Network File System)

A popular TCP/IP service for providing shared file systems over a network. NFS allows all network users to access shared files stored on computers of different types. A user can manipulate shared files as if the files were stored locally on the user's own hard disk. NFS is typically found on Unix computers.

NIST (National Institute for Standards and Technology)

A division of the U.S. Department of Commerce that publishes open interoperability standards called Federal Information Processing Standards (FIPSs). Part of NIST's charter is to distribute complete and accurate information about computer security issues to government and the general public.

node

A computer or CPU on a network.

non-seed router

A router that waits to receive information (the routing maintenance table) from other routers on the network before it begins routing packets.

NTP (Network Time Protocol)

An Internet service used to synchronize clocks among Internet hosts. Properly configured, NTP can usually keep the clocks of participating hosts within a few milliseconds of each other.

O**Oakley**

The Oakley Session Key Exchange provides a hybrid *Diffie-Hellman* session key exchange for

use within the *ISAKMP* framework. Oakley provides the important property of Perfect Forward Secrecy (*PFS*).

octet

A byte. Used instead of "byte" in most IP documents because historically many hosts did not use 8-bit bytes.

one-time pad

A stack of papers bound together, with each paper providing one large, non-repeating set of truly random letters and/or numbers used as an encryption key. Widely used in World War II, the method consisted of using the key on a page exactly once, then tearing off the page and using the key on the next page for the next message. Since the key changes with every message, the enemy does not have a feasible chance to decrypt any given message; thus, one-time pads are considered the only perfect encryption scheme -- as long as the bad guys don't intercept a copy of the pad.

one-way hash function

A mathematical process performed on data to produce a numeric result called a *message digest*, which cannot be reversed to produce the original message. See *hash* and *message digest*.

open source software

A term applied when the source code of a computer program is made available free of charge to the general public. The reason for doing so is that potentially, a larger group of programmers will produce a more useful and bug-free product than a smaller group of programmers, and that more people will use software that is free. The concept relies on peer review to find and eliminate bugs in the program code, which happens at a much quicker rate than with commercial software because the information is shared throughout the open source community instead of through a corporation's smaller, proprietary R & D department. One of the most famous examples of open source software is Linux.

Optional interface

The Ethernet port on the Firebox provided so you can connect a second secured network. This second network is often referred to as the "demilitarized zone" (*DMZ*), or the *Optional network*.

Optional network

A network architecture used by an organization that wants to host its own Internet services without allowing unauthorized access to its private network. Typically, the Optional network contains devices accessible to public Internet traffic, such as Web (*HTTP*) servers, *FTP* servers, *SMTP* (e-mail) servers and *DNS* servers. Access from the Optional network to the Trusted network can then be appropriately restricted by the firewall. For that reason, some refer to the Optional network as a "semi-public" network.

out-of-band (OOB)

A management feature that enables the Management Station to communicate with the Firebox via a telephone line and a modem. OOB is very useful for remotely configuring a Firebox when Ethernet access is unavailable.

P

packet

A unit of information formatted according to specific protocols that allow precise transmittal of data from one node in a network to another. Also called a datagram or a data packet, it contains two parts: a header and a payload. The header is like an envelope; the payload is the contents. In Internet Protocol, any message that is larger than 1,500 bytes gets fragmented into packets for transmission.

packet filtering

Controlling access to a network by analyzing the headers of incoming and outgoing packets, and letting them pass or halting them based on rules created by a network administrator. A packet filter allows or denies packets depending on where they are going, from whom they are sent, or what port they use. Packet filtering is one technique, among many, for implementing security firewalls.

PAP (Password Authentication Protocol)

An identity verification method used to send a user name and password over a network to a computer that compares the user name and password to a table listing authorized users. WatchGuard products do not support this authentication method because the user name and password travel as clear text that a hacker could read. See also *CHAP*.

parameter

In programming, some value passed to a *function*. The function either uses the parameter in its task, or performs an operation on the parameter. A parameter can be a value such as a number, a name, or even a file. For instance, a function that alphabetizes might not know what text file to alphabetize unless a file name is passed to the function as a parameter. The function might not know whether to print the alphabetized list, display it on a screen, or save it as a new file unless one of those options is also expressed as a parameter. A parameter can also be referred to as an *argument*.

passive mode FTP

See *active mode FTP*.

passphrase

An easy-to-remember phrase which offers better security than a single-word password, because it is longer and thus harder to guess or calculate.

password

A secret sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification. WatchGuard recommends the use of passphrases in place of passwords.

password caching

The temporary storage of a user's username and password by some application.

peer-to-peer

Sometimes abbreviated as P2P, this is a method of distributing files over a network where all computers are treated as equals (in contrast to a *client/server* architecture). Using P2P *client* software, a client can receive files from another client. Some P2P file distribution systems require a centralized database of available files (such as Napster), while other distribution systems like Gnutella are decentralized.

perfect forward secrecy (PFS)

A cryptosystem in which, if one encryption key is compromised, only the data encrypted by that specific key is compromised. Some cryptosystems allow keys to be derived from previous keys, so that if the first key is compromised, an attacker might have enough information to figure out other keys and/or decrypt data encrypted using those keys. RFC 2409 describes PFS in detail.

PGP (Pretty Good Privacy)

An application and protocol (RFC 1991) for secure e-mail and file encryption. PGP uses a variety of algorithms (like RSA, DSA, *MD5*, *SHA-1*) to provide encryption, *authentication*, message integrity, and key management.

PGP/MIME

An IETF standard (detailed in RFCs 2015 and 3156) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC 1847, currently deployed in *PGP* 5.0 and later versions.

Phase 1, Phase 2

Stages in establishing a site-to-site Virtual Private Network (*VPN*) *tunnel*. Designated computers negotiate security parameters to protect the managing of the tunnel itself using *IKE* (Internet Key Exchange); the result of this negotiation is called the Phase 1, or *ISAKMP*, security association (*SA*). The Phase 1 *SA* is then used to securely negotiate security parameters to protect *IP packets*; the result of that negotiation is called the Phase 2, or *IPSec*, *SA*. The Phase 2 *SA* is then used to securely tunnel *ESP* or *AH*-protected *IP packets* between these two computers.

ping

A utility to determine whether a specific *IP address* is accessible. It works by sending a packet to the specified address and waiting for a reply; hence, it was named after the sound echo sonar makes when trying to locate an object.

PKCS (Public Key Crypto Standards)

A set of standards published by RSA Security, developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, and Sun), that includes algorithm-specific and algorithm-independent implementation standards for reliable, secure *public key cryptography*.

PKI (Public Key Infrastructure)

A system of digital *certificates*, *Certificate Authorities*, and other registration authorities that verify the validity of each party involved in an Internet transaction. The intent is to establish a trusted relationship between the parties. PKI's various mechanisms can provide a foundation for message confidentiality, message integrity, non-repudiation (which means the author of a message cannot later claim he did not write it), and authentication. PKI is necessary and foundational for certificate-based Virtual Private Networks (*VPN*).

plain text

Characters in a human readable form prior to encryption or after decryption. Also called *clear text*.

plug and play

An ease-of-use ideal in the personal computer market that assures the user that a hardware device (for example, a mouse, a modem, or a scanner) can be installed without resorting to manual hardware configuration of either the device or the PC into which the device is being installed.

Policy Manager

The Windows-based interface used to modify and upload a Firebox configuration file. One component of the WatchGuard Firebox System.

port

1. A physical hole in a computing device where you plug something in (such as, "this PC communicates with the printer via the serial port").
2. When used in relation to *IP services*, a made-up, or *logical*, endpoint for a connection, conceived so that the computer can handle multiple applications over one network connection. Your system figures out how to treat data coming at it partially by looking at what port the data is destined for (for example, HTTP, or Web traffic, by convention uses port 80; SMTP, or e-mail traffic, uses port 25).

port address translation

See *NAT*.

port forwarding

See *NAT*.

port space probe

An intrusion technique whereby a hacker attempts to connect to sequential port numbers. These probes are usually attempts to find security holes which the attacker might exploit. When a listening computer responds to a message sent to a given port, the attacker then knows there really is a computer there, listening on that port.

PPP (Point-to-Point Protocol)

A method of connecting a computer to the Internet, often used with dialup modems.

PPPoE (Point-to-Point Protocol over Ethernet)

A method of transmitting PPP traffic over Ethernet to the Internet through a common broadband medium. Commonly used in Europe. The users have the appearance of "dialing" the Internet, but their computers are in fact always connected.

PPTP (Point-to-Point Tunneling Protocol)

A VPN tunneling protocol with encryption. It uses one TCP port (for negotiation and authentication of a VPN connection) and one IP protocol (for data transfer) to connect the two nodes in a VPN. Though favored by Microsoft, many experts feel PPTP offers weaker confidentiality of data than a competing standard, *IPSec*.

Pretty Good Privacy

See *PGP*.

primary key(IPSec)

An *IPSec* key responsible for creating a security association. Values can be set in time or data size.

principle of precedence

Logic followed by the Firebox when deciding which permissions and prohibitions in your security policy override others. As a general guideline, a more specific rule usually overrides a more general rule. For example, if you've established a general rule that says to let Any Internet traffic enter your network, and you also have a rule that says to block any traffic over port 31337, then port 31337 will be blocked: the specific rule takes precedence over the general.

private key

The "secret" component of an asymmetric key pair, often referred to as the decryption key. In a key pair (composed of a public key and a private key), it is essential that you keep the private key to yourself. See also *asymmetric key*, *key pair*, and *public key*.

private network address

A private network address is an IP address range that is used only within the confines of a single organization. Private addresses are used for traffic from one location to another within a clearly defined network and at no time are meant to extend beyond the perimeter, or firewall, of the organization. They are not routable on the Internet, and require some sort of address translation (see *NAT*) to reach the Internet. Private network address ranges are defined by the IANA and RFC 1918 as being 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

privilege elevation

See *elevation of privilege*.

probe

A type of hacking attempt characterized by repetitious, sequential access attempts. For example, a hacker might try to probe a series of ports in search of one that is open, or one

might probe a range of IP addresses in search of a responsive computer.

procedure

See *function*.

protocol

A set of formal rules describing how to transmit data, especially across a network. The protocol determines issues such as: the type of error checking to be used, data compression method, if any; how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, character sets, and sequencing of messages.

proxy ARP

Proxy Address Resolution Protocol allows a network to use one network address across two physical interfaces. In typical routing, separate network interfaces on a routing device must connect to different networks with distinct IP addresses (e.g., 192.168.10.n and 192.168.11.n). Thus, adding a firewall appliance that has multiple interfaces could potentially force a network to be subdivided into separate network addresses (because although a firewall appliance is not a router, it performs routing). Proxy ARP is the answer for administrators who do not want to renumber their network. It is a technique that the Firebox uses to handle traffic between hosts that don't expect to encounter a routing device -- those hosts would expect to transmit directly to hosts now placed behind a firewall. Using Proxy ARP, the Firebox responds to ARP requests for hosts on the "other side" of it that can't reply for themselves. The Firebox gives an ARP reply matching the remote IP address with the Firebox's own Ethernet address (in essence, a lie, so that the requesting half of the network can continue acting as if the other half of the network is local). The Firebox then receives packets on behalf of hosts behind it, and forwards them appropriately. Proxy ARP is what allows you to use the same network address across all three Ethernet interfaces of the Firebox, known as *drop-in mode*. See also *Address Resolution Protocol*.

proxy server

A server that sits between a client application (such as a browser) and a "real" server. The proxy server intercepts client requests and forwards them to the other server. Its purpose is two-fold: for outgoing traffic, it allows private, non-routable machines to reach a machine which can reach the Internet for them. Secondly, as it receives responses to the client machine requests (for example, Web pages) it can cache them locally so that further client requests can be answered locally and immediately. Use of the Firebox removes the need for a proxy server, unless the proxy server is used for caching files.

proxy service

A combination of stateful packet filtering with content inspection. Essentially, the Firebox intercepts traffic intended for another destination (for example, a Web server or an e-mail server) and imposes rigid access and routing rules with the defense of the internal networks and servers in mind. Dangerous traffic is discarded, while normal traffic is passed to the intended destination.

pseudo-random number

A number that results from applying randomizing algorithms to input derived from the computing environment, such as mouse coordinates or the time of day. See also *random number*.

Public Key Crypto Standards

See *PKCS*.

public key

The publicly available component of an asymmetric key pair, often referred to as the encryption key. In a key pair (composed of a public key and a private key), you can make your public key well-known, as messages encrypted with it can only be decrypted by your private key. See also *asymmetric key*, *key pair*, and *private key*.

public key cryptography

Cryptography in which a public and private key pair is used, encrypting the data at the sender's end and decrypting it at the receiver's end. Since the data is encrypted while it travels the public Internet, no additional security is needed -- it can safely use public networks without loss of confidentiality. See also *asymmetric key* and *key pair*.

Public Key Infrastructure

See *PKI*.

R**RADIUS** (Remote Authentication Dial-In User Service)

A method widely used on the Internet by ISPs and large organizations to validate usernames and passwords for dial-up users, and to provide proper accounting. RADIUS is distributed in source-code form, making it highly modifiable.

random number

A number generated from a large set of numbers, using an algorithm that gives every number an equal probability of occurring. Random numbers are used as an ingredient in encryption keys; thus, a random number generator is a necessary element in creating unique keys that are unpredictable to an adversary.

RC4 (Rivest Cipher 4)

One of many *symmetric* key algorithms. Once a proprietary algorithm of RSA Data Security, Inc., RC4 creates keys of variable size which are called *streaming ciphers*; that is, they are used to encrypt a stream of data byte-by-byte as it goes by.

RC5 (Rivest Cipher 5)

A cipher that encrypts a block (many bytes) of data at a time. The RC5 algorithm enables the user to specify block size, key length, and how many times the encrypted message should be re-encrypted (referred to as *encryption rounds*).

related hosts

A method for informing the Firebox of the physical location of a particular computer or device. This is most commonly used when the Firebox is utilizing proxy ARP in drop-in mode. Although the Firebox can use proxy ARP to automatically learn the location of hosts on its interfaces, an administrator can specify related hosts in the WatchGuard Firebox Software to make sure the Firebox knows the location of critical machines immediately.

related networks

A legacy term synonymous with secondary network.
See *secondary network*.

remote user

Someone you allow to access your office network, who is geographically removed from the office.

repeater

A network device that regenerates signals so that they can travel farther along a cable without losing or distorting data. A repeater is not as smart as a router, but it can relay messages between subnetworks that use different protocols or cable types.

reverse lookup; reverse DNS lookup

The opposite of a *DNS lookup*. *DNS* works like the phone book: in a *DNS lookup*, you have a name (such as *watchguard.com*) but you want the number (an *IP address*). In a reverse lookup, you have the number (e.g., *64.119.131.128*), but you want to find the domain name associated with it (e.g., *watchguard.com*).

revocation

This term is most often used in the context of digital certificates. A Certificate Authority assures that all parties in a digital transaction are who they claim to be and that all documents are genuine. The Certificate Authority (CA) vouches for your digital certificate, which is like ID the CA issued you. If the CA subsequently finds out one of the parties misrepresented themselves (as happened in March of 2001, when Verisign issued digital certificates to imposters claiming to represent Microsoft), the CA can *revoke* the digital certificate. Thus, revocation is the retraction of certification or authorization.

RFC (Request for Comments)

RFC documents describe standards used or proposed for the Internet. Each RFC is identified by a number, such as RFC 1700. The Internet Engineering Task Force maintains RFCs on the World Wide Web, at www.ietf.org/rfc.html.

ring topology

A basic networking configuration in which all nodes are connected in a circle with no terminated ends on the cable.

route

1. The sequence of computerized devices through which information travels to reach its target machine. Each device the information travels through delineates one stage of the route, referred to as a "hop."
2. An entry stored on a computer, telling it how to reach other devices or networks. These entries can be automatically generated when you set up your network and can also be entered manually. They are stored in your local host's *routing table*.

routed mode

A Firebox configuration where each of the Firebox's three Ethernet interfaces must use IP addresses in different subnets. This type of configuration is intended for situations in which the Firebox is put in place with separate logical networks on its interfaces. For a contrasting approach, see *drop-in mode*.

router

A device, connected to at least two networks, that receives and sends data packets between those networks. Routers refer to packet headers and a forwarding table to decide where to forward packets to.

routine

See *function*.

RPC (Remote Procedure Call)

A protocol that allows a computer to ask some other computer to perform a task or service and return the result. The computer making the request is often referred to as a *client*, and the computer doing the task is called the *server*. The client computer does not need to know how to perform the task itself, it just sends an RPC request to a server and gets some result.

RUVPN (Remote User Virtual Private Networking)

RUVPN establishes a secure connection over the Internet between a remote computer and your protected network.

S

salt

A tiny bit of near-random data inserted where too much predictability would be undesirable. In cryptography, *salt* is a random string that is added onto passwords (or random numbers) before an algorithm is performed on the password. The extra data effectively lengthens and obscures the password, making the cipher text less susceptible to dictionary attacks.

scalable architecture

Software and/or hardware constructed so that it can grow efficiently.

SCSI (Small Computer System Interface)

A processor-independent standard for system-level interfacing between a computer and intelligent devices including hard disks, floppy disks, CDROM, printers, and scanners.

Pronounced "scuzzy."

secondary network

A network on the same physical wire as a Firebox interface having a different IP network address. This technique allows you to add as many subnets as you want to a single Ethernet interface on a Firebox.

secret key

The encryption key used in *symmetric algorithms*.

secret sharing

See *key splitting*.

secure channel

A means of conveying information from one entity to another using a method that does not offer an intruder the ability to reorder, delete, insert, or read information.

SecurID token

A hardware-based authentication method owned by RSA. The user enters his PIN into the token, which resembles a small hand-held calculator. The token combines the user's PIN with numbers inside itself to create a number that RSA calls a "passcode." The user then logs in with his username on a PC, entering the passcode number. The PC sends it to an authentication server. If the passcode matches what the server expects, the user is authorized. This method is known as "response only" because the server did not issue a challenge.

security association (SA)

In Internet Protocol Security (*IPSec*), settings that establish policy and encryption keys used to protect communications between two end points in a Virtual Private Network (*VPN*). Security associations are negotiated between two computers during the first phase of establishing an Internet Key Exchange (*IKE*) connection. See also *Phase 1*, *Phase 2*.

segment

A section of a network. Typically, a segment is thought of as ending where it reaches a router or a routing device (such as the Firebox).

self-extracting file

A compressed file that automatically decompresses when double-clicked.

server

A computer that provides shared resources to network users. The network users are often referred to as *clients* of that server. See also *client/server*.

server-based network

A network in which all client computers use a dedicated central server computer for network functions such as storage, security, and other resources. See also *server*.

Server Message Block (SMB)

A message format used by DOS and Windows to share files, directories and devices (such as printers). NetBIOS is based on the SMB format, and many network products use SMB. SMB runs over most common network protocols, including *TCP/IP*.

Services Arena

WatchGuard's term for the area in WatchGuard Firebox System's Policy Manager that displays icons representing the services (such as proxies and packet filters) configured for a Firebox.

ServiceWatch

A graphical monitor providing a real-time display that graphs how many connections exist, by service. This comes as part of an application called Firebox Monitors.

session hijacking

An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker's goal is to gain access to a server while bypassing normal authentication measures.

session key

The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session. See also *asymmetric key* and *key pair*.

session stealing

See *session hijacking*.

setup keys (IKE)

Internet Key Exchange keys responsible for creating a *security association*.

SHA-1 (Secure Hash Algorithm)

A message digest function (also called a *one-way hash*) used in encryption. The 1994 revision to SHA, developed by *NIST*. SHA-1 is a mathematical process used to change the contents of a file into a 160-bit number, similar to *MD4*. See also *message digest*.

shared secret

In *IPSec* usage, a passphrase or password that exists on two devices to be connected by VPN. In order to begin the security negotiations that result in a VPN tunnel, both devices must know the pre-existing secret, which is used by each party to authenticate the other.

sign

To apply a *digital signature* which, in the USA, is as legally binding as a handwritten signature.

signature

A digital code created with a *private key*.

See *digital signature*.

single sign-on

A log-in routine in which one logon provides access to all resources on the network.

slash notation

A concise decimal format for expressing a binary *subnet mask*. For example: 192.168.44.0/24 indicates that in the 32-bit IP address, the first 24 bits (192.168.44) are the address of a network. The remaining 8 bits can be used to indicate the addresses of specific devices on that network.

SLIP (Serial Line Internet Protocol)

A protocol for exchanging IP packets over a serial line (for example, a modem connection).

S/MIME (Secure Multipurpose Mail Extension)

A proposed standard for encrypting and authenticating MIME data, which is used primarily for

Internet e-mail. See *MIME*.

SMS (Security Management System)

The former name of the *GUI* used to configure a Firebox. Now known as the WatchGuard Policy Manager.

SMTP (Simple Mail Transfer Protocol)

A protocol for sending electronic mail between servers.

social engineering attack

An attack that does not depend on technology as much as it depends upon tricking or persuading an individual to divulge privileged information to the attacker, usually unknowingly. For example, an attacker might phone a company's internal help desk, posing as an employee, and say, "This is Fred in Accounting. I was on vacation for five weeks and forgot my network password. Could you look it up for me?" If the gullible help desk technician reveals the password to the attacker, the attacker "socially engineered" it out of him.

SOCKS

A protocol for handling TCP traffic through a proxy server. It can be used with virtually any TCP application, including Web browsers and FTP clients. It provides a simple firewall because it checks incoming and outgoing packets and hides the IP addresses of client applications. SOCKS is an IETF standard, documented in RFCs 1928, 1929 and 1961. WatchGuard's SOHO uses a SOCKSv5 proxy.

SOHO

An abbreviation for businesses categorized as Small Office/Home Office. Also the name of the WatchGuard firewall devices designed for businesses of this size.

spam

Unsolicited commercial e-mail sent to many recipients, much like an electronic version of junk mail.

spoofing

Altering data packets to falsely identify the originating computer. Spoofing is generally used when a hacker wants to make it difficult to trace where the attacks are coming from.

SSID (Service Set Identifier)

Usually pronounced as a word, rather than initials. A unique string, up to 32 characters, that serves as the name of a wireless local area network (WLAN). Because a SSID differentiates one network from another, multiple wireless networks can function even when their ranges overlap. In an open network, the access point broadcasts the SSID. You can configure your wireless access point (WAP) not to broadcast the SSID, so that users trying to join the network must already know the network name.

SSL (Secure Sockets Layer)

A protocol for transmitting private documents over the Internet, often used by e-commerce sites (among others). SSL works by using a private key to encrypt data transferred over an SSL connection.

stance

The policy of a firewall regarding the default handling of IP packets. Stance dictates what the firewall will do with any given packet in the absence of explicit instructions. The WatchGuard default stance is to discard all packets that are not explicitly allowed, often stated as "That which is not explicitly allowed is denied."

star topology

A networking setup used with 10Base-T Ethernet cabling and a hub. Each node on the network is connected to the hub, like points of a star.

stateful packet filtering

"Packet filtering" means using a firewall to examine where each packet comes from (by IP source address), where it's going (IP destination), and what port it's using. This information helps the firewall determine whether to allow or deny the packet's passage through your network. In *stateful inspection*, the firewall also examines more of the packet's delivery information and its conditions, including what port the packet is using, and maintains a sense of context. For example, a packet might arrive looking like a valid Reply packet, but if you never issued a Request, through dynamic packet filtering the firewall can sense that this is a spurious packet, and deny it.

static NAT (Network Address Translation)

The ability to have the Firewall forward all traffic received on a given port and a given public IP, to a private IP behind the firewall. See also *NAT*.

stream cypher

A class of symmetric key encryption that encrypts each byte of data as it is received, instead of gathering the data into large blocks before encrypting. Useful for equipment that has little memory for buffering data.

subnet

A *subdivision* of a *network* that uses a sequential range of IP addresses (i.e. 10.45.32.1 to 10.45.32.128). Administrators divide large networks into subnets for many reasons. One reason: subnets are typically easier to troubleshoot than a large network because the administrator is dealing with fewer machines at a time.

subnet mask

This is a difficult concept to express succinctly. If it is new to you, please begin by reading the entry for *IP address*. A subnet mask is a numeric value that helps a networked host or router understand how to interpret the destination IP address on packets the machine receives. When a computer receives a data packet, it tries to figure out if the IP address the packet is destined for is local (meaning, on the same network segment as the machine), or non-local. This matters to the machine because if the destination is local, the machine can deliver the packet (using *ARP*). If the address is not local, the machine does not know how to deliver the packet. Figuratively, it says, "I give up!" and forwards the packet to the *default gateway* (another machine, often a router, which handles everything non-local). In trying to decide whether a destination IP address is local or not, the machine must discern how much of the IP address designates the destination network, and how much of the address designates the destination host. If the destination address is 192.168.14.10, what part of that address specifies the destination network? 192? Or 192.168? Or perhaps 192.168.14? The subnet mask, which is specified on each networked machine in a routing table, provides the answer. Like an IP address, a subnet mask is a 32-bit value. The machine combines it mathematically with the destination IP address, using an operation called a "Boolean AND." The nature of the subnet mask plus the Boolean AND guarantee a result that will tell the machine, in binary values, how much of the IP address is the network range and how much is the host address. The machine then understands how to properly forward the packet. See also *CIDR* and *slash notation*.

subroutine

See *function*.

substitution cipher

An encoding method in which plain text characters are replaced with other characters to form coded text. For example, the most elementary substitution cipher might say A=1, B=2, C=3, etc. to encrypt the word "DOG" as "4-15-7." Real substitution ciphers, of course, are much more complex.

switch

A device that filters and forwards packets between LAN segments. A typical switch has numerous physical ports, each acting as a connection point for a network segment. Larger networks utilize switches to break the network into smaller, more manageable chunks, which are easier to secure. With the traffic on the entire network broken into smaller units, packets encounter fewer collisions, enhancing network performance.

symmetric algorithm

An encryption method where the same key is used both to encrypt and decrypt messages. Also called conventional, secret key, and single key algorithm. See also *asymmetric keys*.

SYN flood attack

A method of denying service to legitimate users of a network resource (such as a Web server) by intentionally overloading a network with illegitimate TCP connection requests. SYN is short for "synchronize," the first packet sent when one computer tries to connect to another using TCP. In a normal TCP connection, or *handshake*:

1. Computer A sends a SYN packet;
2. Computer B acknowledges the connection attempt and sends back its own SYN packet (thus, a SYN/ACK packet), and
3. Computer A acknowledges Computer B's response. In a SYN flood attack, Computer A never acknowledges Computer B (in other words, Step 3 never happens). This forces Computer B to wait for A's acknowledgment until B times out and drops the connection. Flooding Computer B with a huge number of such incomplete requests keeps B tied up uselessly. This is one version of a *Denial of Service* attack.

syslog

An industry-standard protocol used for sending and receiving log information for devices on a network. Syslog support is included in Unix-based and Linux-based systems.

T**TCP (Transmission Control Protocol)**

A set of rules that enables a broad spectrum of different kinds of computers to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent, so it is considered "reliable." Most long-haul traffic on the Internet uses TCP.

TCP handshake

A three-step process computers go through when negotiating a connection with one another. Simplistically described, in a normal TCP handshake:

1. Computer A sends a SYN packet (for "synchronize");
2. Computer B acknowledges the connection attempt and sends back its own SYN packet (thus, a SYN/ACK packet), and
3. Computer A acknowledges Computer B's response. Once both computers are synchronized and acknowledged, they can begin passing data back and forth. To learn how attackers might exploit this, see *SYN flood attack*.

TCP/IP (Transmission Control Protocol/Internet Protocol)

A common networking standard with the ability to connect a diverse array of systems. This is one of the underlying protocols of the Internet. For others, see *ICMP, IP, TCP, and UDP*.

TCP session hijacking

See *session hijacking*.

Telnet

A remote control program typically found on Unix systems in TCP/IP networks. A telnet client runs on your PC and connects it to a remote server on a network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on that remote network.

timestamping

Recording the time when an event happens (typically in a log) or when a piece of information is created or modified.

TLS (Transport Layer Security)

A general-purpose protocol for encrypting Web, e-mail, and other stream-oriented information sent over the Internet. TLS is a relatively recent (first published in 1999) derivative of the Secure Sockets Layer (SSL) version 3.0 protocol, and is described in RFCs 2246, 2712, 2817, and 2818.

token

Also called a security token or an authentication token. Something a person has that evidences validity, or identity. It is usually a hardware device that resembles a hand-held calculator, since it often has some sort of display and perhaps a keypad for entering numbers. Tokens achieve the goal of "two-factor authentication," considered a strong standard of security when validating who a user is, because accessing a network that uses tokens requires two factors: something the person knows (a password) and something the person has (the token).

tooltip

A name or phrase that appears when the mouse pointer pauses over a button or icon.

topology

A wiring configuration used for a network. Also referred to as a network's architecture.

transposition cipher

A cipher in which the plain text remains the same but the order of the characters is scrambled. Thus, the word "DOG" might become "OGD." Transposition is sometimes used as one step in the midst of several mathematical operations that, together, make up a cryptographic algorithm.

Triple-DES (3DES)

A cryptographic algorithm using three keys (rather than one or two). Triple DES is simply another mode of DES operation, where the DES algorithm is applied three times on the data to be encrypted, using a different key each time. 3DES is currently one of two US federal government standards for encrypting non-classified data.

trust

Confidence in the honesty, integrity, or reliability of a person, company, or other entity. The concept also extends to believing that an unseen remote party is who he or she claims to be.

Trusted interface

The Ethernet port on the Firebox that connects it to your internal network. See *Trusted network* and *Optional interface*.

Trusted network

The private network which you intend your firewall to primarily protect. The Trusted network is usually where your most sensitive corporate resources reside or where home office employees do their work. This contrasts with the semi-public *Optional network*.

tunnel

In Virtual Private Networks (VPN), an encrypted connection between sites. Only the originator

and the receiver of the message see it in its clear state. Any hacker trying to intercept the message en route gets nothing but a scrambled mess. Because the path of a VPN message has "light" (clear text) at each end but "darkness" (obscurity) at all the between-points, it is called, metaphorically, a VPN tunnel. On a technical level, a tunnel is a means of exchanging *encapsulated* data packets between two parties. Though some tunneling protocols forward *cleartext* packets, WatchGuard utilizes tunneling protocols such as *PPTP* and *IPSec ESP* that forward encrypted packets.

twisted-pair cable

A cable used for both network and telephone communications. Also known as UTP (unshielded twisted pair) and *10Base-T/100Base-T* cable.

U

UDP (User Datagram Protocol)

A set of standards for transmitting data over networks. Some technicians have nicknamed it the "Unreliable Darn Protocol" because when sending data, UDP does not verify that it has established a connection at the receiving end; it simply blasts away until the message has been sent. Thus, UDP is termed a "connectionless" protocol. Because it doesn't perform the checks and verifications of *TCP*, UDP is simpler to implement and is used where a small amount of packet loss is acceptable. On the Internet, UDP is often used for streaming video and audio.

URL (Universal Resource Locator)

The user-friendly address that identifies the location of a Web site, such as <http://www.watchguard.com>.

V

validation

The act of examining information provided by a person (or a system) to ascertain what rights, privileges, or permissions they may (or may not) have to perform some action. For example, when you attempt to charge a purchase at a retail store to a credit card, the cashier validates your identity by examining your identification and comparing your signature on the receipt with the signature on the credit card.

verification

In cryptography, the act of testing the authenticity of a digital signature by performing special mathematical operations on data provided by a sender, to see if it matches an expected result. If the information provided by the sender yields the expected result, the signature is valid, because calculating the proper answer requires secret data known only by the sender. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else. See also *asymmetric key* and *digital signature*.

VPN (Virtual Private Network)

A means of having the security benefits of a private, dedicated, leased-line network, without the cost of actually owning one. VPN uses cryptography to scramble data so it's unreadable while traveling over the Internet, thus providing privacy over public lines. Companies with branch offices commonly use VPNs to connect multiple locations.

Vulnerability Assessment

Vulnerability Assessment is the process of identifying network and device vulnerabilities before hackers can exploit the security holes. QualysGuard is a Managed Vulnerability Assessment Web service solution to audit networks. QualysGuard is a continuous preventive process to:

- Detect network and system vulnerabilities.
- Deliver near-instantaneous email alerts summarizing discovered vulnerabilities and trends.
- Prioritize the severity of each vulnerability on an industry-standard scale, from "watch" to "urgent", so administrators can readily determine where to deploy their security specialists for fixes.
- Recommend and make direct links to verified remedies for each vulnerability.
- Produce trend analysis in graphical form, with granular detail appropriate for both security specialists and non-technical management to track vulnerabilities over time.

W

WAN (Wide Area Network)

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (*LANs*) connected by a high-speed line.

WatchGuard LiveSecurity® Service

Part of the WatchGuard Firebox Security System offering, separate from the software and the Firebox, which keeps network defenses current. The LiveSecurity Service includes software updates, technical support, timely broadcasts of security intelligence, and a resource-rich Web site containing FAQs, archived articles, online training, a moderated user forum, and the latest software.

WatchGuard Security Event Processor (WSEP)

WatchGuard's proprietary log server software. It provides critical timing services for the Firebox and includes its own *GUI*. See *server* and *client/server*.

WebBlocker

An optional WatchGuard software module that prevents users behind the Firebox from accessing undesirable Web sites. It works based on a regularly updated database of sites that could be objectionable, categorized by content type (e.g., pornography, gambling, or racist hatred sites).

Web browser

Software used to view the World Wide Web, a graphically rich presentation of information on the Internet. The most popular Web browser is Microsoft's Internet Explorer, but other browsers such as Netscape Navigator and Opera are available. To find specific sites on the Web, you enter a *URL* in your Web browser.

Web of Trust

A term describing a relationship-based extension of the concept of *trust*, popularized in PGP. For example, if you trust Bob and Bob says Rachel is a good auto mechanic, you'll trust Rachel to fix your car even if you have not previously met Rachel. A similar concept is used to validate encryption keys in PGP. If you know and trust Bob, and Bob gives you a text block and says it is Rachel's public key, you'll accept the text block as Rachel's key even if you don't know Rachel. If Rachel later sends a message encrypted with or signed by her private key, you'll be ready to decrypt it or verify the signature because you have her public key. You can then pass Rachel's public key to someone who trusts you, thus extending the Web of Trust by another node.

Web page

A single HTML-formatted file posted where it can be accessed via the World Wide Web.

Web site

A collection of affiliated Web pages.

WEP (Wired Equivalent Privacy)

The security aspects of 802.11b, a standard that enables wireless devices such as PDAs and

laptop computers to access a network via radio frequencies instead of physical wiring. WEP has three tasks: 1) to authenticate clients to access points; 2) to encrypt the data exchanged between the clients and access points; and 3) to include an integrity check with every packet exchanged. The initial implementation of WEP provides weak security. While it is not completely useless, it is best used as another layer of security in conjunction with stronger measures.

WFS (WatchGuard Firebox System)

Software used for managing WatchGuard's Firebox model firewalls. WFS consists of multiple components, some used on a PC you designate as a Management Station, and some loaded into the Firebox's memory. WFS enables such features as configuring the policies of the Firebox, setting up and customizing services, logging, monitoring, and reporting.

white hat

A person who investigates flaws in network security measures in order to strengthen them and to prevent computer networks from being invaded. When such a researcher discovers new security flaws, he or she reports them to the appropriate vendor to be fixed, rather than using the knowledge illicitly. See *black hat*.

WINS (Windows Internet Name Service)

WINS provides name resolution for computers running Windows NT, Windows 98, and earlier versions of Microsoft operating systems. With name resolution, users access servers by name rather than needing to use IP addresses.

WLAN (Wireless Local Area Network)

A computer network that spans a relatively small area, generally confined to a single building or group of buildings. In a wireless network, devices connect through high-frequency radio waves using IEEE standard 802.11.

World Wide Web Consortium (W3C)

An international industry consortium founded in 1994 to develop common protocols for the evolution of the World Wide Web. W3C has around 450 member organizations from around the world.

WPA (WiFi Protected Access)

A data encryption specification for 802.11 wireless networks. Wireless networks rely on radio waves, which broadcast in all directions. Any device within range of a wireless access point could eavesdrop upon its transmissions. WPA encrypts wireless data so that an eavesdropper intercepts gibberish, while authorized endpoints receive clear, decrypted data. WPA replaces *WEP*, a weaker wireless encryption standard that attackers can readily break.

worm

A self-replicating program that seeks access into other computers by exploiting security flaws. After a worm penetrates another computer, it continues seeking access to other areas. Worms often steal or vandalize computer data. Many viruses are more accurately termed worms, and use e-mail or database systems to propagate themselves to their victims.

X

XOR

Shorthand for "Exclusive-or," a mathematical operation used to represent the differences between two values.

XTM (extensible threat management)

Refers to a security appliance that delivers all the features of a UTM (unified threat management) solution – firewall, VPN, anti-virus, and intrusion blocking – but with extended security, networking, and management capabilities. The goal of XTM is to create an

ever-expandable network security platform. An appliance that is flexible enough to support new technologies can protect against threats even when they evolve into new forms. XTM extensibility also tries to ensure that appliances interoperate and support mixed network infrastructures, giving an administrator a wide array of configuration options.

X.509v3

An ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature.