INTRUSION.COM

Security solutions for a .com world™

Glossary

1-2-3

802.1P priority queuing An extension of the IEEE standard for interconnecting LANs through MAC bridges. The 802.1.P defines how MAC-layer bridges filter and expedite multicast traffic. Traffic prioritization is accomplished with the addition of a 3-bit, priority value in the frame header.

802.1Q switching The implementation of VLANS in Layer 2 LAN switches, with an emphasis on Ethernet. Similar to 802.1P, prioritization of packet traffic is accomplished using an additional 4 bytes in the frame header. Most data fields for this specification support VLAN operation. Also included is a field which provides the same 3-bit priority flag specified in 802.1P's, priority-mapping scheme. 802.1Q supports voice and video transmission through Ethernet switches.

10/100 Refers to running Ethernet using twisted-pair wiring, with a throughput of 10 or 100 Mbps.

10BaseT Ethernet LANs standard that has limting distance of 100 meters per segment and a peak transmission speed of 10 Mbps. See *Ethernet*.

A

abuse of privilege When a user performs an action that they should not have, according to organizational policy or law.

access control The prevention of unauthorized use of a resource, including the prevention of use of resources in an unauthorized manner. Under this concept authorized entity is granted only specified access rights to a resource.

access control lists Rules for packet filters (typically routers) that define which packets to pass and which to block.

access router A router that connects your network to the external Internet. Typically, this is your first line of defense against attackers from the outside Internet. By enabling access control lists on this router, you'll be able to provide a level of protection for all of the hosts "behind" that router, effectively making that network a DMZ instead of an unprotected external LAN.

active backplane A physical area at the rear of the SecureCom 8000 chassis that can accommodate up to 40 active wires (maximum of eight application module slots and five traces [wires] per slot). This permits SecureCom 8000 modules, for example, a Cisco Router in slot 2 and a firewall—application module (dual NIC) in slots 3 and 4 to communicate with each other. See *passive backplane*.

active connect card The SecureCom 8000 module that provides the active backplane its communication ability. Slot 0 of the SecureCom 8000 Chassis is reserved for a five-port active connection card. This card has a 802.3-compliant repeater chip (10 Mbps) for each of the five traces. This provides both internal repeating of all traces and external connection via an RJ-45 connector.

address spoofing A technique, in which one host impersonates the IP address of another.

agent The software in a network device that communicates at the Simple Network Management Protocol (SNMP) level.

agent system A device (host, gateway, router, hub, bridge, or terminal server) that has an SNMP agent responsible for performing the network management operations requested by the manager.

AH **A**uthentication **H**eader. A security protocol which provides data authentication and connectionless integrity for an entire IP datagram. AH is embedded in the data to be protected (a full IP datagram).

alarms A signal that signifies that an error has arisen or an abnormal situation exists.

analyzer The intrusion detection (**ID**) component or process that analyzes the data collected by the sensor for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. In many existing ID systems, the sensor and the analyzer are part of the same component.

anti-replay With anti-replay service, each IP packet passing within the secure association is tagged with a sequence number. On the receiving end, each packet's sequence number is checked to see if it falls within a specified range. If an IP packet tag number falls outside of the range, the packet is blocked.

API **A**pplication **P**rogramming **I**nterface. A set of programming conventions that provide access through protocol layers and defines how a service is invoked through a software package.

application module A hardware and software module that plugs into the passive and (optional) active backplanes of the SecureCom 8000 chassis.

application-level firewall A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

ARP **A**ddress **R**esolution **P**rotocol. The TCP/IP protocol used to dynamically associate a high-level, 32-bit IP address with a low-level (48-bit MAC) physical hardware address.

AST Automatic Spanning Tree. Function that supports the automatic resolution of spanning trees in SRB networks, providing a single path for spanning explorer frames to traverse from a given node in the network to another. AST is based on the IEEE 802.1 standard.

ATM Asynchronous Transfer Mode**.** Switching technology for broadband ISDN (B-ISDN) that allows traffic (voice, data, image, and video) to be combined into evenly-sized cells for high-speed transmission and switching over one access circuit.

AUI Attachment User Interface. Most commonly references the 15pin D type connector and cables used to connect single and multiple channel equipment to an Ethernet transceiver.

authentication The process of determining the identity of a user that is attempting to access a network. Authentication occurs through challenge/response, time-based code sequences, or other techniques.

authentication token A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

authorization The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

autonegotiation An algorithm that allows devices at each end of a link segment to negotiate common features and functions.

authority Ability of a switch to transfer packets to this port.

backplane The data bus connections used to interconnect different communication modules inside a SecureCom 8000 chassis.

bastion host A designated Internet firewall system specifically armored and protected against attacks Bastion hosts are often components of firewalls, or may be "outside" Web servers or public access systems. Generally, a bastion host is running some form of general purpose operating system (Linux, Unix, VMS, NT, etc.) rather than a ROM-based or firmware operating system.

blade Synonym for a SecureCom 8000 application module that is pre-configured for NT, Linux, HP/UX, or Solaris operating systems. See *application module*.

block cipher A digital encryption method that encrypts long messages by segmenting them into blocks (for DES, 64 bits) of fixed length. each block is individually encrypted.

BOOTP A TCP/IP network protocol that lets network nodes request configuration information from a BOOTP “server” node.

BPDU **B**ridge **D**ata **P**rotocol **U**nits, or Spanning-tree Protocol “hello”-management packet – used by bridges to communicate when performing a spanning tree computation. Each bridge interprets the information in the BPDUs it receives to discover a loop-free subset of the topology. As a result, there is only one connection between every pair of networks.

bridge A device operating at the data link layer to connect local and wide-area networks that use the same protocol. The bridge only forwards packets that do not have a local network address.

bridge forwarding Process that uses entries in a filtering database to determine whether packets with a given MAC destination address can be forwarded to a given port or ports. Described in the IEEE 802.1 standard.

broadcast A message from one station addressed to all stations on a network simultaneously.

brouter A bridge/router that can route one or more protocols, and bridges all other network traffic.

card General term for a network module. Literally refers to the board that contains the circuitry and chipsets.

Category 5 wiring Data-grade unshielded twisted-pair, capable of transmission rates up to 155 Mbps.

CGI exploit When a denial of service attack is aimed at the CGI (common gateway interface), it is referred to as a CGI exploit. The CGI is a standard way for a Web server to pass a Web user's request to an application program and to receive data back to forward to the user. It is part of the Web's HTTP protocol.

CHAP **C**hallenge-**H**andshake **A**uthentication **P**rotocol. An authentication technique where after a link is established, a server sends a challenge to the requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it its own calculation of the expected hash value. If the values match, the authentication is acknowledged otherwise the connection is usually terminated.

chassis A hardware device that houses user cards, controller cards and third party cards and also contains a central power supply (or power supplies) which is used by the cards.

chip number The number of the chip to which the spanning tree is assigned.

chroot A technique under UNIX whereby a process is permanently restricted to an isolated subset of the filesystem.

CIFS

Common **I**nternet **F**ile **S**ystem. Enhanced version of SMB that enables computers to open and share remote files on the Internet. See *SMB*.

CLI

Command **L**ine **I**nterface. A primitive asynchronous connection (usually through a serial port) that permits a user with a simple terminal to communicate with SecureCom module using simple, non-graphical commands.

CMDS

Computer **M**isuse **D**etection **S**ystem. An enterprise security solution that uses agent technology to collect data from hosts, desktops, routers, firewalls, intrusion detection systems, databases, enterprise resource planning, and applications. The collected event data is analyzed for attack and misuse signatures (behavioral profile, complex, or simple), then stored in an ODBC database.

cold start

Process of loading the bootROM software into the SecureCom 8000 Port Concentrator Module and subsequently loading the PCM application software.

collector

The designation of one or more PCM ports to receive traffic only. Typically this would be traffic from several network hubs that we want to monitor. This is similar to Cisco Networks “port mirroring” done on a Category 5500 switch. See *distributor.*

community string

Text string that acts as a password and is used to authenticate messages sent between a management station and a SecureCom module containing an SNMP agent. The community string is sent in every packet between the manager and the module. See *SNMP.*

Concert

A joint venture of AT&T and British telecommunications to provide services for multinational customers, international carriers, and service providers wordwide.

configuration area

One of two firmware memories that contain all the information necessary to configure the SecureCom 8000 Port Concentrator Modules. Volatile memory holds the current configuration. Non-volatile memory contains the configuration information copied to volatile memory during a PCM cold start. See *cold start*, *volatile memory,* and *non-volatile memory.*

content security

An application-level security product such as a virus-checker that determines what enters and leaves a secure network.

controller card

The network module in a chassis or agent system that controls the user cards in the chassis and monitors statistics about designated network segments.

cookie

A small data file written to a user’s computer by some Web servers that can contain passwords, lists of web pages the user has visted, or other information.

core bridge (switch) A broadband switching system located in the core of the network. Other branch switches (such as the SecureCom 8000 Port Concentrator Modules) exchange network configuration information with this device.

CPE **C**ustomer **P**remises **E**quipment. The American term for customer provided equipment. The European equivalent term is *Connected Telecommunications Equipment* (CTE).

cryptographic checksum A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting filesystem tampering on UNIX.

cryptography The science and methodology behind enciphering and deciphering messages in secret code so that the information is unreadable by anyone for whom it is not intended.

CSU/DSU **C**hannel **S**ervice **U**nit/**D**ata **S**ervice **U**nit. Hardware device that provides a digital interface to high-speed leased lines. The DSU portion of the device is the digital equivalent of a modem.

cycle The process ofstopping and restarting a software application.

data authentication Data authentication can refer either to data integrity alone or to both integrity and origin authentication (although data origin authentication is dependent upon data integrity.)

data driven attack A form of attack in which the attack is encoded in innocuous-seeming data which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

data flow A grouping of traffic, identified by a combination of source address/mask, destination address/mask, IP next protocol field, and source and destination ports, where the protocol and port fields can have the values of any. In effect, all traffic matching a specific combination of these values is logically grouped together into a data flow. A data flow can represent a single TCP connection between two hosts, or it can represent all of the traffic between two subnets. IPSec protection is applied to data flows.

data integrity Verify that data has not been altered. One of two data authentication components.

data origin authentication Verify that the data was actually sent by the claimed sender. One of two data authentication components.

default gateway The gateway used to receive management traffic requests (via an Internet Browser) form a SecureCom module.

defense in depth The security approach whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.

denial of service attack A user or program takes up all the system resources by launching a multitude of requests, leaving no resources and thereby "denying" service to other users.

DES The **D**ata **E**ncryption **S**tandard is a block cipher, symmetrical algorithm (extremely fast) that uses the same private 64-bit key for encryption and decrypting. This is a 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector to start encryption. The IV is explicitly given in the IPSec packet. *See block cipher* and *triple DES*.

DES-MAC An algorithm, based on DES, for calculating a digest of a message, based on the message and a key.

DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol. A method for letting a server provide static and dynamic IP addresses to network nodes (workstations) from a master list.

dial back The process whereby a modem script prompts the administrator for a telephone number, verifies the dialback number is valid, and after a fixed period, dials a call to a **S**ecure **N**etwork **O**perations **C**entre. See *SNOC*.

Diffie-Helman An algorithm which enables two parties to create a shared secret over an insecure channel.

digital signature A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the message has been altered since the transformation was made.

distributor The designation of one or more ports of SecureCom 8000 (PCM) to transmit packets only. Traffic never switches between collector and distributor ports of a SecureCom PCM.
See *collector*. Typically, a distributor port would send collected packets to a FireWall or Internet security application program running on a PC or UNIX module.

DLCI Data-link connection identifier. Number that specifies a Frame Relay virtual circuit.

DMZ **Dem**ilitarized **Z**one. Denotes the additional network between the Internet (external network) and the protected corporate Intranet. This network includes the Firewalls and ARP routers to provide an additional layer of security. *Sometimes called a perimeter network.*

DNS **D**omain **N**ame **S**ystem. The Internet's standard for naming a host, and a hierarchical system of domain name servers to resolve the host name into IP addresses for TCP/IP communications. (For example, `radguard.com` to 192.168.1.50).

DNS Spoofing Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

DS-1 **D**igital **S**ignal **L**evel **1**. Transmission at 1.544Mbps through the telephone switching network using copper, coaxial cable, optical fiber, or other media.

dual-homed gateway A dual homed gateway is a system that has two or more network interfaces, each of which is connected to a different network. In firewall configurations, a dual homed gateway usually acts to block or filter some or all of the traffic trying to pass between the networks.

duplex Simultaneous two-way transmission in both directions.

dynamic VLAN Refers to a virtual LAN that can constantly reconfigure itself based on new equipment or traffic patterns. It broadcasts new configuration information to other parts of the network that can "learn" how the virtual LAN configuration has changed.

E1 The European digital carrier facility used for transmitting data through the telephone hierarchy. The transmission rate for E1 is 2.048 Mbps.

encrypting router See *tunneling router* and *Virtual Network Perimeter.*

encryption The process of transforming plain text data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decrypting process (two-way encryption).

enterprise management [*Security Perspective*] The integration of a company's virtual private networks into its overall security policy, centralized management from local and remote consoles, and solution scalability.

ESP **E**ncapsulating **S**ecurity **P**ayload. A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

Ethernet A local-area network protocol that uses a bus or star topology. Based on the IEEE 802.3 standard, it supports data transfer rates of 100 Mbps over thin coax, thin coax, twisted pair, or fiber optic cable.

Ethernet transceiver A device used in an Ethernet LAN that couples data terminal equipment to other transmission media.

F

Fast Ethernet Fast Ethernet has an Ethernet hub with an internal bus that runs at 100 Mbps. Workstations and hubs are connected using datagrade UTP and category 5 wiring.

FDB **F**orwarding **D**ata**B**ase. A database used to send packets toward their ultimate destination by way of an internetwork device.

FDDI **F**iber **D**istributed **D**ata **I**nterface – A cable network interface capable of transmitting at 100 Mbps over either fiber or twisted copper wire.

firewall A combination of software/hardware that limits exposure of a network to outside intrusion. A network-level firewall (packet filter) examines traffic at the network level. An application level firewall examines traffic at an application level (for example, FTP, Email, or Telnet) and can readdress outgoing traffic so it appears to originate from the firewall, rather than an internal host.

FID **F**orwarding **I**dentifier.

flooding A packet-switched network routing method whereby identical packets are sent in all directions to ensure that they reach their intended destination.

fractional T1 Digital WAN transmission link with data rates between 56 kbps and 1.544 Mbps (T1 rate). The data rates on a fractional T1 are usually provided in increments of 64 kbps (64, 128, 256 kbps, and so on).

Frame Relay An access standard that uses packet switching analogous to a streamlined version of X.25 networks. A frame relay network can accommodate data packets of various sizes. Native data is encapsulated in a Frame relay Frame, with header and trailer information. The network assumes no responsibility for protocol conversion, transport errors, or detection of lost packets.

framing Dividing data into groups of bits for transmission and adding a header and a check sequence to form a frame.

FWZ-1 Check Point’s FireWall-1 proprietary encryption algorithm.

G

GARP **G**eneric **A**pplication **R**egistration **P**rotocol.

gateway A network point that acts as an entrance to another network. In a company network, a proxy server acts as a gateway between the internal network and the Internet. A gateway may also be any machine or service that passes packets from one network to another network in their trip across the Internet.

Gigabit Ethernet A 1000 Mbps access standard that attempts to address higher bandwidth problems inherent in 10/100 Mbps Ethernet networks, due to multimedia Internet and Intranet applications.

GVRP

GARP **V**LAN **R**egistration **P**rotocol. A GARP used for dynamic VLANs that changes VLAN configuration information (Add, Moves, and Drops) as port connections and interface equipment is changed.

H

harmonic block

A wiring card used to make three passive and (optional) five active connections between the SecureCom 8000 chassis backplanes and a single application module.

hash function

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that: (**1**) a message yields the same result every time the algorithm is executed using the same message as input, (**2**) it is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm, and (**3**) it is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Hello Message

See *BPDU*.

hot-swappable

The ability to add or remove application modules from the box without removing power from the SecureCom 8000 chassis.

hub

A device used as a central connection point for multiple nodes with a common architecture (Ethernet, FDDI, Token Ring, etc.) and that can relay signals. A hub is generally more simple than a concentrator (which supports multiple architectures.)

I

IB

In-**B**and. Signaling that occurs on the voice channels. See *out-of-band* signaling.

IE

Internet **E**xplorer. A popular GUI-based hypertext client application, such as Netscape Navigator, used to access hypertext documents and other services located on innumerable remote servers throughout the WWW and Internet.

IEEE

Institute of **E**lectrical and **E**lectronics **E**ngineers. Technical professional society for electrical, electronics, and computer engineers and computer scientists.

ingress

IEEE 802.3

The IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Physical variations of the original IEEE 802.3 specification include 10Base2, 10Base5, 10BaseF, 10BaseT, and 10Broad36. Physical variations for Fast Ethernet include 100BaseT, 100BaseT4, and 100BaseX.
An Intel-based application module for the SecureCom 8000 chassis.

ICMP

Internet **C**ontrol **M**essage **P**rotocol. ICMP provides diagnostic functions and sends error packets to hosts.

IDS

Intrusion **D**etection **S**ystem. A security product that detects unauthorized network access using some combination of one or more of the following components: (**1**) sensor, (**2**) analyzer, or (**3**) manager.

An IDS can be (**1**) host based─audit data from a single host is used to detect intrusions, (**2**) multihost based─audit data from multiple hosts is used to detect intrusions, or (**3**) network based─network traffic data, along with audit data from one or more hosts, is used to detect intrusions.

IDSs can use either an anomaly detection model (detects intrusions by looking for activity that is different from a user's or system's normal behavior) or a misuse detection model (detects intrusions by looking for activity that corresponds to known intrusion techniques or system vulnerabilities. *See sensor, analyzer, and manager.*

IKE

Internet **K**ey **E**xchange. A hybrid protocol which implements Oakley and SKEME key exchanges inside the ISAKMP framework. While IKE can be used with other protocols, its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. *See IPSec.*
The unwanted leakage of interfering packets into a network.

IP Address

The four-byte address convention that uniquely identifies each node under Simple Network Management Protocol (SNMP). The format of the IP address is X.X.X.X, where X is one byte with a decimal value of 0 to 255. Users must define their own conventions for determining the IP address for the network or internetwork they manage. See *SNMP*.

IP spoofing

An attack whereby a system attempts to illicitly impersonate another system by using its IP network address.

IP Splicing / Hijacking

An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

IPSec

IP security Protocol. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec.

IPSP

IP Security **P**rotocol, the former name of the IPsec protocol, now standardized by RFC1825 - RFC1829.

IP subnet
All devices which share the same network address. Routers are boundaries between subnets so each connection to a router has a different network address. See *subnet mask*.

ISAKMP/Oakley
The key exchange protocol used for exchanging cryptographic keys and for automatically establishing security associations.

IV
Initialization **V**ector. A string whose purpose is to ensure that two identical plain texts does not result in the same cypher text; when encrypted under the same key.

L

LAN
Local **A**rea **N**etwork, spanning a limited geographical area. A LAN enables sharing of disks, files, printers, and other resources. The LAN provides the computer user with the opportunity to communicate with other users. The LAN consists of a network cable linking the computers and nodes and the Network Operating System.

Least Privilege
Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

LED
Light **E**mitting **D**iode. Used to transmit fiber optic signals in multimode and to display status information on the front panel of a module.

LLC
Logical **L**ink **C**ontrol. A layer 2 protocol governing transmission, also known as the IEEE 802.2 standard.

LMS
Log **M**anagement **S**ystem. The customer-based management of the SecureCom 8001 Concert Linux Firewall logs, that is configured using the LMS scripts.

logging
The process of storing information about events that occurred on the firewall or network.

log retention
How long audit logs are retained and maintained.

log processing
How audit logs are processed, searched for key events, or summarized.

M

MAC
Media **A**ccess **C**ontrol. In the IEEE 802.x networking model, the MAC sublayer is below the LLC sublayer. Together, these two sublayers are equivalent to the data-link layer in the OSI Reference Model.

MAC address

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a *hardware address, a MAC-layer address, or a physical address.*

MAC address learning

Service that characterizes a learning bridge, in which the source MAC address of each received packet is stored so that future packets destined for that address can be forwarded only to the bridge interface on which that address is located. Packets destined for unrecognized addresses are forwarded out every bridge interface. This scheme helps minimize traffic on the attached LANs. MAC address learning is defined in the IEEE 802.1 standard. See also *learning bridge* and *MAC address*.

manager

The intrusion detection (**ID**) component or process from which the operator manages the various components of the ID system. Management functions typically include (but are not limited to) sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting. *See IDS - **I**ntrusion **D**etection **S**ystem.*

manager system

Executes network management operations that monitor and control agent systems. The implementation of these management operations is called the manager. The manager can retrieve information from an agent through query and reply or set (change) the management information on the agent.

MD5

Message **D**igest **5** is a hash (data authentication) algorithm. HMAC is a keyed hash variant used to authenticate data.

MIB

Management **I**nformation **B**ase. A database of network parameters used by SNMP and CMIP to monitor and change network device settings. It provides logical naming for all information resources (objects) that are pertinent to the network's management. An SNMP MIB is a set of parameters that an SNMP management station can query or use to set the SNMP agent of a network device.

MIME

Multipurpose **I**nternet **M**ail **E**xtensions. A protocol used for encoding documents with different formats (binary, proprietary, etc.) into ASCII characters for transfer across TCP/IP networks.

module

An ODS Networks card or a stand-alone port concentrator, hub, converter, etc.

module

A SecureCom 8000 series connect card, communication card, network interface card, or processor that occupies one or more slots in the chassis.

multicast

Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the destination address field. Compare with *broadcast* and *unicast*.

N

NAT **N**etwork **A**ddress **T**ranslation. Allows your Intranet to use addresses that are different from what the outside Internet thinks you are using. It permits many users to share a single external IP address at the same time. NAT provides "address hiding", which is security through obscurity at best.

netmask An addressing scheme used to specify what part of an IP address X.X.X.X (X is value 0 to 255) designates the network, and what part designates nodes or hosts residing on the network. Each octet in the netmask greater than zero indicates that the corresponding octet of the IP address specifies the network.

network-level firewall A firewall in which traffic is examined at the network protocol packet level.

NIC **N**etwork **I**nterface **C**ard. A network interface device in circuit card form that is installed into one or more slots of the SecureCom 8000 chassis.

node An individually addressable location in a data communications network. In RMON-MIB terminology, a Host and a Node are identical. A node may be any of a number of physical devices including personal computers, larger scale server computers, printers, etc. A physical device may have multiple connections to a network and therefore may constitute multiple nodes.

NTP **N**etwork **T**ime **P**rotocol. The protocol supplied by Red Hat 6.1 release CD that synchronizes the time to all IPVPDN devices. This protocol uses 56 or “triple” DES encryption system.

O

Omnibus probe Software used to improve intrusion detection for the SecureCom 8001 Concert Linux Firewall.

OOB **O**ut-**O**f-**B**and. Signaling that occurs on dedicated channels separate from voice channels. The dialback functionally for the VPDN firewall so it can dial back the SNOC for authentication of the administrator. See *in-band* signaling.

OPSEC The **O**pen **P**latform for **S**ecure **E**nterprise **C**onnectivity developed by Check Point Software Technologies and supported by the SecureCom 8000 product line.

P

packet A series of bits containing data and control information including source and destination node addresses, formatted for transmission from one node to another. The native data network protocol may call the packet a (**1**) packet, (**2**) block, (**3**) frame, or (**4**) cell.

packet filtering A feature that allows a router to make a permit/deny decision for each packet based on the packet header information that is made available to the IP forwarding process.

passive backplane Three backplane segments that permit you to directly connect SecureCom 8000 application modules to each other. Use a twisted-pair Ethernet cable with RJ-45 connectors to patch the signals from one module to another. The passive component of the SecureCom 8000 chassis that has no electronic components other than connectors and etched-in wires.

PBIC **P**acket **B**us **I**nterface **C**hip. An interface that provides the ability to receive and transmit packets on the packet bus.

PCI **P**eripheral **C**omponent **I**nterconnect. 132 Mbps bus technology that supports communication between devices. An example PCI card would be a single, dual, or quad 10/100 Mbps Ethernet ports.

PCM **P**ort **C**oncentrator **M**odule. A 12 or 24-Port Intrusion.com Spanning Tree Protocol (STP) switch that goes in a SecureCom 8000 chassis and is used to examine traffic packets and route them (with a flexible set of priorities) to other network devices.

PDU **P**rotocol **D**ata **U**nit. “Generic packet” A message of a given protocol comprising payload and protocol-specific control information, typically contained in the header. In the OSI Reference Model, a packet created at a particular layer and used to communicate with the same layer on another machine.

peer A peer refers to a router or other device that participates in IPSec.

perimeter-based security The technique of securing a network by controlling access to all entry and exit points of the network.

PFS **P**erfect **F**orward **S**ecrecy. A cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

PING **P**acket **I**nter**N**et **G**opher. A program used to test whether a specific network IP address is working; that is the destination address can be reached and responds to the set of packets sent to it.

PKI **P**ublic **K**ey **I**nfrastructure. The IEFT’s X.509 standard is the defacto means by which public keys can be managed on a secure basis.

plug-and-play The ability of a peripheral card’s software and hardware to identify itself and the resources required from the host operation system. A user need only plug the module into the PC or chassis slot. The software automatically sets up a suitable configuration for the card.

policy rules

Policy rules are the guidelines that make up a security policy. They define which hosts are allowed to send or receive data packets, what services are allowed, during what time periods data packets may be sent or received, and how this data will be secured.

POP3

Post **O**ffice **P**rotocol. Electonic mail server protocol used with TCP/IP that provides services for downloading email from the network to a PC. See *SMTP*.

port

(1) The physical or electrical interface where data may be accessed, such as one of 12/24 ports on the front of the SecureCom 8000 Port Concentrator Modules. **(2)** The identifier (16-bit unsigned integer) used by Internet Transport protocols to distinguish among multiple simultaneous connections to a single destination host.

port group

A collection of switch interfaces through which packets can be switched. Port groupings can be distinct for different types of destination addresses: multicast, broadcast, and unicast sprays.

port identifier

The identifier assigned by a logical node to represent the point of attachment of a link to that node.

Port Level VLAN

VLAN based on the source port ID. This is a multiple bridge configuration of a switch.

port-mirroring

A fault tolerance technique in which a second port maintains packet data identical to another port or set of ports.

private key

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key. Alternative names are *single-key* and *secret-key.*

protocol

A standardized set of rules that specify the format, timing, sequencing, and/or error checking for data transmissions.

proxy

An agent that acts on behalf of a user, typically accepting a connection from a user and completing a connection on behalf of the user with a remote host or service. Alternative names are *gateway* and *proxy server.*

proxy server

A proxy server is one that acts on behalf of one or more other servers, usually for screening, firewall, caching, or a combination of these purposes. Typically, a proxy server is used within a company or enterprise to gather all Internet requests, forward them out to Internet servers, receive the responses, and in turn, forwards them to the original requestor within the company. See *gateway* or *router.*

public key

Algorithms that encrypt and decrypt using asymmetrical (different), yet mathematically-linked keys. Each security module is assigned a pair of keys. The encryption key is “public” and does not require distribution by secure means. The decrypting or “private” key cannot be discovered through knowledge of the public key or its underlying algorithm. Can apply to key distribution, encryption, authentication, or digital signature.

public key encryption

A form of key encryption which uses two keys, a public key (for encrypting messages) and a private key (for decrypting messages) to enable users to verify each other’s messages without having to securely exchange secret keys.

PVID

Port **V**LAN **ID**. A priority value (uses 3 bits for 8 possible priorties) assigned to packets queued for transmission. The eight priorities are assigned to specific port numbers of the SecureCom 8000.

QoS

Quality **o**f **S**ervice. On the Internet and in other networks, QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

Q

RAID

Redundant **A**rray of **I**nexpensive **D**isks.

R

RAS

Remote **A**ccess **S**ervices. A feature built into Windows NT that enables users to log into an NT-based LAN using a modem, X.25 connection or WAN link.

RC-4

A private key (symmetric) cryptosystem.

repeater

A device that receives a signal from a network segment, cleans and amplifies the signal, and then sends it on another segment of the same network. The optional SecureCom 8000 active connector card, located in slot 0, contains five 10 Mbps repeaters, one for each of the active backplane segments.

RFC

Request **F**or **C**omment. Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards.

RPM

Red Hat **P**ackage **M**anager. A Linux-based software installation, upgrade, and source-code deployment system that requires a minimum of effort. This tool is used by the Concert program to deploy software upgrades and security patches.

RIP

Routing **I**nformation **P**rotocol. Routing protocol that measures the shortest path between two points on a network in terms of the number of “hops” between those points.

RJ-45

An 8-pin **R**egistered **J**ack connector used for data transmission over standard telephone wire. It comes in flat or twisted wire.

RMON

Remote Network **MON**itoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.

RMON agent

A hardware or software device that is physically attached to a network segment. The agent accumulates statistical information regarding all packets that are present on that segment and, when commanded, records and stores selected traffic data for further analysis. The agent provides complete statistics regarding nodes on that specific segment, but only partial or no information for nodes that reside on other network segments.

root bridge

The bridge that the transmitting bridge finds “best” based on root cost path and spanning tree calculations.

root cost path

The path with the lowest cost of all paths from the transmitting bridge to the root bridge.

root port

The port that provides the best path from the transmitting bridge to the root bridge.

router

A network device that determines the optimal path for packet traffic based on considerations such as destination address, priority level, least-cost route, minimum route delay, route congestion, privileges, and community of interest. A device that performs network interface functions—altering physical, data link, and network layer protocols—within a network or between dissimilar networks. Routers are protocol-sensitive, typically supporting multiple protocols.

RS-232-C

A popular standard employed in serial connections for computers. The standard defines how Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) are connected.

RSA

Rivest **S**hamir **A**dleman. A public key (asymmetric) cryptosystem used for encryption and transmitting digital signatures. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Netscape and Microsoft.

router

An internet protocol gateway that sends data using an IP or MAC destination address. A device that performs network interface functions—altering physical, data link, and network layer protocols—within a network or between dissimilar networks. Routers are protocol-sensitive, typically supporting multiple protocols.

SAR

Segmentation and **R**eassembly.

SATAN

Security **A**nalysis **T**ool for **A**uditing **N**etworks. A tool that allows a network analyt to mimic a malicious hacker (or cracker) to identify weaknesses in the system and network security.

S

screened host
A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

screened subnet
A subnet behind a screening router. The degree to which the subnet may be accessed depends on the screening rules in the router.

screening router
A router configured to permit or deny traffic based on a set of permission rules installed by the administrator.

SCSI
Small **C**omputer **S**ystem **I**nterface. A high-speed peripheral interface used to access hard disks and network devices.

security
A set of three technologies that include (**1**) access control to guarantee the network connections, (**2**) encryption to protect data privacy, and (**3**) authentication to verify the user’s identity and the integrity of the data. See access control, authentication, and encryption.

security audit
A log of security-related events.

security association
An IPSec security association (**SA**) is a description of how two or more entities will use security services in the context of a particular security protocol (**AH** or **ESP**) to communicate securely on behalf of a particular data flow. It includes such things as the transform and the shared secret keys to be used for protecting the traffic.

The IPSec security association is established either by IKE or by manual user configuration. Security associations are unidirectional and are unique per security protocol. So when security associations are established for IPSec, the security associations (for each protocol) for both directions are established at the same time.

When using IKE to establish the security associations for the data flow, the security associations are established when needed and expire after a period of time (or volume of traffic). If the security associations are manually established, they are established as soon as the necessary configuration is completed and do not expire.

segment (network)
A network or subnet in which all nodes are physically and logically connected so all nodes receive all data traffic seen by all other nodes on the segment. A segment may be one physical bus or loop or may be interconnected by repeaters, which pass all traffic, but not by bridges, routers, or gateways, which logically are separate networks.

segment (chassis)
One of five communication channels that make up the active backplane of the SecureCom 8000 chassis. Each segment has eight traces or signal wires. Connections to and from segments are made using a standard RJ-45 connect with Category 5 Twisted-Pair Ethernet (TPE) wiring. See *active backplane* and *passive backplane*.

sensor
The ID component that collects data from the data source. The frequency of data collection varies across IDS products.

signature
A rule used by the analyzer to identify interesting activity (possible misuse) to the security administrator. Signatures (misuse patterns) and anomalies are two methods by which ID systems detect intrusions.

SHA-1
Secure **H**ash **A**lgorithm is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

SHH
An internet protocol and suite of programs that implement secure, encrypted communication channels between hosts on a TCP/IP network using public key encryption. See *public key encryption*.

slot
(**1**) A narrow opening in a chassis where a module can be inserted using its bottom track and left/right ejection levers. SecureCom 8000 application modules fit into one of several slots in the chassis. (**2**) A circuit board can be inserted into PCI-compliant slots within the SecureCom 8000 application modules.

SMB
Server **M**essage **B**lock. File-system protocol to package and exchnage information with other systems.

SNMP
Simple **N**etwork **M**anagement **P**rotocol. A software standard which network management applications use to remotely monitor, maintain, and configure network devices such as TCP/IP-based internets. An SNMP message consists of three parts:

1.a protocol version

2.an SNMP community identifier (also for security)

3.a data area

The applications can also query a management agent using a supported Management Information Base (MIB).

SNOC
Secure **N**etwork **O**perations **C**entre. The Concert center fro mwhich administrators dial into the Concert customer networks and the SecureCom 8001 VPDN appliances dial back. Omnibus client syslog events are also passed back to the SNOC for analysis and intrusion detection.

SNMP communities
Authentication scheme that enables an intelligent network device to validate SNMP requests from sources such as the NMS. A SecureCom 12-24 Port Concentrator Modules, for example, responds only to SNMP requests that come from members of known communities and that have the access privileges required for that request.

SMTP
Simple **M**ail **T**ransfer **P**rotocol. TCP/IP protocol for transferring electronic mail from one machine to another. See *POP3*.

source routing

Normal IP packets have only source and destination addresses in their headers, leaving the actual route taken to the routers located between the source and the destination. Source-routed IP packets have additional routing information in the header (specified by the host source) that specifies the route the IP packet should take.

source routing attacks

An attack in which the source station specifie the route that a packet should take (with the hope of bypassing security measures) and causing the packet to follow an unexpected path to its final destination. Easily defeated by dicarding all packets that contain the source route option.

spanning tree

A bridging algorithm used to determine the best paths for multiple bridges in a network.

SPI

Security **P**arameter **I**ndex. This is a number which, together with an IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish the security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association.

spoofing

Establishing a connection with a forged sender address. This normally involves exploiting a trust relationship that exists between source and destination addresses/systems.

SSL

Secure **S**ockets **L**ayer. A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

static routes

Routes that are preset and automatically loaded into a routing table. The static routes take precedence over routes chosen by all dynamic routing protocols.

static VLAN

A VLAN that is configured and requires an individual to update the configuration when port connections or equipment changes.

STP

Spanning **T**ree **P**rotocol. Refer to a type of bridge, defined in the IEEE 802.1 standard (in contrast to SRP and SRT bridges), that is self-learning and can filter packets. Some STP bridges have built-in security mechanisms which can deny access to resources on the basis of user and terminal ID.

STP bridges can automatically reconfigure themselves for alternate paths should a network segment fail. Self-learning bridges “learn” the addresses of attached devices on each segment by initiating broadcast query packets and then remembering the originating addresses of the responding devices. The replacement of Network Interface cards (NICs) and dynamic movement of switches requires this learning process to repeat at regular intervals.

subnet mask A number that, in conjunction with an IP address, defines the set of IP addresses considered “local” for this portion of the network. For example, if your IP address is 192.168.25.77 and your subnet mask is 255.255.255.0, then addresses between 192.168.25.1 and 192.168.25.255 are considered local.

T1 A digital WAN carrier facility used to transmit a DS1 formatted digital signal at 1.544 Mbps through the PSTN and broken down into 24 channels, digitized at 64Kbps streams. (U.S. and Japan). See *E1*.

T3 The North American standard for DS-3 (Digital Signal Level 3) that operates at a signalling rate of 44.736 Mbps (equivalent to 28 T1s). Both Bill Gates and George Lucas have T3 lines coming to their houses.

Telnet **Tel**ecommunications **Net**work. An application that provides a VDT interface between hosts using the TCP/IP network protocols.

TFTP **T**rivial **F**ile **T**ransfer **P**rotocol. Simplified version of FTP that allows files to be transferred from a host computer to a SecureCom module over a network.

Token Ring A 4 or 16 Mbps network media developed by IBM that uses a ring topology and IP-based token-passing access method.

TPE **T**wisted-**P**air **E**thernet. An eight signal cable that supports 10/100 Mbps Ethernet communication and uses RJ-45 connectors.

traffic class Set of Class of Service attribute (profile) values assigned to a given port. The profile affects numerous parameters for data transmitted from the port including rate, transmit priority, and inactivity timer.

traffic management Technologies that guarantee the reliability of data delivery, quality of service or prioritization of traffic, and performance within a secure Internet network.

transform A transform lists a security protocol (AH or ESP) with its corresponding algorithms. For example, one transform is the AH protocol with the HMAC-MD5 authentication algorithm; another transform is the ESP protocol with the 56-bit DES encryption algorithm and the HMAC-SHA authentication algorithm.

trap Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that has been reached.

trojan horse A packet sniffer that hides its sniffing activity. These packet sniffers can collect account names and passwords for Internet services, allowing a hacker to gain unauthorized access to other machines.

triple DES A security enhancement to DES encryption that employs three-successive single-DES block operations. Using two or three unique DES keys, this increases resistance to known cryptographic attacks by increasing the effective key length.

tunneling A secure, temporary communication path between two Internet peers. It does not refer to using IPSec in tunnel mode.

tunneling router A router capable of routing traffic by encrypting it and encapsulating it for transmission across an unsecure network, for eventual de-encapsulation and decrypting.

u-Series module UNIX-based SUN UltraSPARC application module, based on the SPARCengine Ultra AX*i* board, for the SecureCom 8000 chassis.
Message sent to a single network destination.

URL filtering **U**niform **R**esource **L**ocator filtering. A security application feature that denies access to content based on the address in a standard format that locates files (resources) on the Internet and the Web.

user card A network module that has ports through which users can connect to the network.

UTP **U**nshielded **T**wisted **P**air. A cable that consists of two or more insulated conductors in which each pair of conductors are twisted around each other. There is no external protection. Noise resistance comes solely from the twists.

V.35 An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the U.S. and Europe, and is recommended for speeds up to 48Kbps.

vandal A vandal is an executable file, usually a Java applet or an ActiveX control, associated with a Web page that is designed to be harmful, malicious, or at the very least inconvenient to the user.

Virtual Network Perimeter A network that appears to be a single protected network behind firewalls, which actually encompasses encrypted virtual links over untrusted networks.

virus A replicating code segment that attaches itself to a program or data file. Viruses might or might not not contain attack programs or trapdoors.

VLAN **V**irtual **LAN**. Group of devices on a LAN that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN tagging

VPDN

Virtual **P**rivate **D**ata **N**etwork. A business solution that provides secure, private connections to network applications using a public or “unsecured” medium such as the internet. The shared network is augmented on a secure basis using encryption or tunneling.

VPN

Virtual **P**rivate **N**etwork. A business solution that provides secure, private connections to network applications using a public or “unsecured” medium such as the Internet. The shared network is augmented on a secure basis using encryption or tunneling techniques.

W

WAN

Wide **A**rea **N**etwork. Two or more LANs connected using telephone company services or another method of communication. Also, a comprehensive multimode network connecting a large number of terminals and computers spread over a wide geographical area.

wideband

A channel that uses a wider bandwidth than a voice-grade (56 Kbps) channel.

WINS

Windows **I**nternet **N**ame **S**ervice. A name resolution service that resolve Windows NT networking computer names to IP addresses in a routed environment. A WINS server handles name registrations, queries, and releases. See *IP address*.

worm

A standalone program that, when run, copies itself from one host to another, and then runs itself on each newly infected host.

X

X.21

An ITU-T standard for serial communication over synchronous digitial lines. This protocol is used primarily in Europe and Japan.

X.509

An ITU specification that describes the format for hierarchical maintenance and storage of public keys for public-key systems.