Juniper
NETWORKS

Security Products

ScreenOS Glossary of Terms

Release 6.2.0, Rev. 01

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Consult the dealer or an experienced radio/TV technician for help.

- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

ScreenOS Glossary of Terms

802.11a	Wireless local area network (WLAN) standard that provides up to 54 Mbps in the 5GHz radio band.
802.11b	WLAN standard that provides up to 11 Mbps in the 2.4 GHz radio band.
802.11g	WLAN standard that provides 20+ Mbps in the 2.4 GHz radio band.
802.11SuperG	WLAN standard that provides up to 108 Mbps in the 2.4 GHz radio band.
ABR	*See* Area Border Router (ABR).
Access-Challenge	Additional condition required for a successful Telnet login by an authentication user via a RADIUS server.
Access Control List (ACL)	Identifies clients by their media access control (MAC) addresses and specifies whether the wireless device allows or denies access for each address.
Access List	List of network prefixes that are compared to a given route. If the route matches a network prefix defined in the access list, the route is either permitted or denied.
Access Point (AP)	*See* Wireless Access Point (AP).
Access Point Name (APN)	Information element (IE) included in the header of a GTP packet that provides information about reaching a network. It is composed of a network ID and an operator ID.
ACL	*See* Access Control List (ACL).
Address Shifting	Mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in another range.
Adjacencies	When two routers can exchange routing information, they are considered to have constructed an adjacency. Point-to-point networks, which have only two routers, automatically form an adjacency. Point-to-multipoint networks are a series of several point-to-point networks. When routers pair in this more complex networking scheme, they are considered to be adjacent to one another.
ADSL	*See* Asymmetric Digital Subscriber Line (ADSL).
Aggregate State	A router is in an aggregate state when it is one of multiple virtual BGP routing instances bundled into one address. *See also* Border Gateway Protocol (BGP).
Aggregation	Process of combining several routes in such a way that only a single route advertises itself. This technique minimizes the size of the routing table for the router.

Aggregator	Object used to bundle multiple routes under one common route generalized according to the value of the network mask.
Aggressive Aging	Mechanism for accelerating the timeout process when the number of sessions in the session table surpasses a specified high-watermark threshold. When the number of sessions in the table dips below a specified low-watermark threshold, the timeout process returns to normal.
AH	*See* Encapsulating Security Protocol/Authentication Header (ESP/AH).
ALG	*See* Application Layer Gateway (ALG).
Antivirus (AV) Scanning	Mechanism for detecting and blocking viruses in File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP)—including HTTP webmail—and Post Office Protocol version 3 (POP3) traffic. ScreenOS offers an internal and an external AV-scanning solution.
Application Layer Gateway (ALG)	On a security device, a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP) or File Transfer Protocol (FTP). The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.
Area Border Router (ABR)	Router with at least one interface in Area 0 and at least one interface in another area.
AS	*See* Autonomous System (AS).
AS Boundary Router	Router that connects an autonomous system (AS) running one routing protocol to another AS running a different protocol. *See also* Autonomous System (AS).
AS Number	Identification number of the local autonomous system (AS) mapped to a BGP routing instance. The ID number can be any valid integer. *See also* Border Gateway Protocol (BGP).
AS Path	List of all the autonomous systems that a router update has traveled through in the current transmission.
AS Path Access List	Access list used by a BGP routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance. *See also* Border Gateway Protocol (BGP).
AS Path Attribute Class	Border Gateway Protocol (BGP) provides four classes of path attributes: well-known mandatory, well-known discretionary, optional transitive, and optional non-transitive. *See also* Border Gateway Protocol (BGP).
AS Path String	String that acts as an identifier for an autonomous system (AS) path. It is configured alongside an AS Path access list ID.
Asymmetric Digital Subscriber Line (ADSL)	DSL technology that allows existing telephone lines to carry both voice telephone service and high-speed digital transmission. A growing number of service providers offers ADSL service to home and business customers.
Atomic Aggregate	Object used by a Border Gateway Protocol (BGP) router to inform other BGP routers that the local system has selected a generalized route.

Attack Objects	Stateful signatures and protocol anomalies that a security device with deep inspection (DI) functionality uses to detect attacks aimed at compromising one or more hosts on a network.
Authentication	Ensures that digital data transmissions are delivered to the intended recipient. Authentication also validates the integrity of the message for the receiver, including its source (where or whom it came from). The simplest form of authentication requires a username and password for access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES or 3DES, or on public-key systems that use digital signatures.
Authentication Header (AH)	*See* Encapsulating Security Protocol/Authentication Header (ESP/AH).
Autonomous System (AS)	A group of networks under mutual administration that share the same routing methodology. An AS uses an Interior Gateway Protocol (IGP) or several IGPs and common metrics to route packets within the group. The group also uses an Exterior Gateway Protocol (EGP) to route packets to other autonomous systems. Each AS has a routing plan that indicates which destinations are reachable through it. This plan is called the *Network Layer Reachability Information (NLRI)* object. Border Gateway Protocol (BGP) routers periodically generate and receive NLRI updates..
Auxiliary (AUX) Port	This port is usually the same as COM 1 and is used to access external networks.
B8ZS	8 bits zero suppression.
Backward Explicit Congestion Notification (BECN)	In a Frame Relay network, Forward Explicit Congestion Notification (FECN) is a header bit transmitted by the source (sending) terminal requesting that the destination (receiving) terminal slow down its requests for data. BECN is a header bit transmitted by the destination terminal requesting that the source terminal send data more slowly. BECN and FECN are intended to minimize the possibility that packets will be discarded (and thus have to be resent) when more packets arrive than can be handled.
Basic Rate Interface (BRI)	ISDN service also called *2B+ D*, because it consists of two 64 Kbps B-channels and one 16 Kbps D-channel.
B-Channel	ISDN Basic Rate Interface (BRI) service provided by telephone service providers: two bearer channels (B-channels) and one data channel (D-channel). The B-channel operates at 64 Kbps and carries user data.
bgroup	*See* Bridge Group Interface.
Bit Error Rate (BER)	Ratio of error bits to the total number of bits received in a transmission, usually expressed as 10 to a negative power.
Border Gateway Protocol (BGP)	Inter-autonomous system routing protocol. BGP routers and autonomous systems exchange routing information for the Internet.
Bridge Group Interface	Also known as the *bgroup interface*. These interfaces allow several physical ports to be grouped together to act like a pseudo switch. You can group multiple wired interfaces or wireless and wired interfaces so they are located in the same subnet.
Broadcast Network	Network that supports many routers with the capability of communicating directly with one another. Ethernet is an example of a broadcast network.

Bundle   Aggregation of multiple physical links.

Certificate Revocation List (CRL)   List of invalid certificates.

Circuit-Level Proxy   Proxy servers are available for common Internet services; for example, an HTTP proxy is used for Web access, and an FTP proxy is used for file transfers. Such proxies are called *application-level proxies* or *application-level gateways*, because they are dedicated to a particular application and protocol and are aware of the content of the packets being sent. A generic proxy, called a *circuit-level* proxy, supports multiple applications. For example, SOCKS is a generic IP-based proxy server that supports TCP and UDP applications. *See also* Proxy Server.

Cisco High-Level Data Link Control (Cisco-HDLC)   Proprietary Cisco encapsulation for transmitting LAN protocols over a WAN. HDLC specifies a data encapsulation method on synchronous serial links by means of frame characters and checksums. Cisco HDLC enables the transmission of multiple protocols.

Classless Routing   Support for interdomain routing, regardless of the size or class of the network. Network addresses are divided into three classes, but these are transparent in BGP, giving the network greater flexibility. *See also* Border Gateway Protocol (BGP).

Community   Grouping of Border Gateway Protocol (BGP) destinations. By updating the community, you automatically update its member destinations with new attributes.

Confederation   Object inside a Border Gateway Protocol autonomous system (BGP AS) that is a subset of routing instances in the AS. By grouping devices into confederations inside a BGP AS, you reduce the complexity associated with the matrix of routing connections, known as a *mesh*, within the AS.

Connection States   When a packet sent from one router arrives at another router, a negotiation occurs between the source and destination routers. The negotiation goes through six states: Idle, Connect, Active, OpenSent, OpenConnect, and Establish.

CRL   *See* Certificate Revocation List (CRL).

Data Circuit-Terminating Equipment (DCE)   Equipment that provides switching services in the WAN and is typically owned and managed by the service provider.

Data Encryption Standard–Cipher Block Chaining (DES–CBC)   Message text and, if required, message signatures can be encrypted using the Data Encryption Standard (DES) algorithm in the Cipher Block Chaining (CBC) mode of operation. The character string "DES-CBC" within an encapsulated Privacy Enhanced Mail (PEM) header field indicates the use of DES–CBC.

Data Encryption Standard (DES)   A 40-bit and 56-bit encryption algorithm that was developed by the National Institute of Standards and Technology (NIST). DES is a block-encryption method originally developed by IBM. It has since been certified by the U.S. government for transmission of any data that is not classified as top secret. DES uses an algorithm for private-key encryption. The key consists of 64 bits of data, which are transformed and combined with the first 64 bits of the message to be sent. To apply the encryption, the message is broken up into 64-bit blocks so that each can be combined with the key using a complex 16-step process. Although DES is fairly weak, with only one iteration, repeating it using slightly different keys can provide excellent security.

Data-Link Connection Identifier (DLCI)	Separates customer traffic in Frame Relay configurations.
Data Terminal Equipment (DTE)	RS-232 interface used to exchange information with a serial device. This equipment is the terminating point for a specific network and is typically located on the customer premises.
Dead Interval	Period that elapses before a routing instance determines that another routing instance is not running.
Dead Peer Detection (DPD)	Allows an IPsec device to verify the current existence and availability of other IPsec peer devices. The device performs this verification by sending encrypted Internet Key Exchange (IKE) Phase 1 notification payloads (R-U-THERE) to the peers and waiting for DPD acknowledgements (R-U-THERE-ACK).
Deep Inspection (DI)	Mechanism for filtering the traffic permitted by the firewall. DI examines Layer 3 and Layer 4 packet headers and Layer 7 application content and protocol characteristics in an effort to detect and prevent any attacks or anomalous behavior that might be present.
Default Route	Catch-all routing table entry that defines the forwarding of traffic for destination networks that are not explicitly defined in the routing table. The destination network for the default route is represented by the network address 0.0.0.0/0.
Demilitarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.
DES	*See* Data Encryption Standard (DES).
DES–CBC	*See* Data Encryption Standard–Cipher Block Chaining (DES–CBC).
Destination Network Address Translation (NAT-dst)	Translation of the original destination IP address in a packet header to a different destination address. ScreenOS supports the translation of one or several original destination IP addresses to a single IP address (one-to-one or many-to-one relationships). The security device also supports the translation of one range of IP addresses to another range (a many-to-many relationship) using address shifting.

When the security device performs NAT-dst without address shifting it can also map the destination port number to a different predetermined port number. When the security device performs NAT-dst with address shifting, it cannot also perform port mapping. |
DI	*See* Deep Inspection (DI).
Digital Signal 0 (DS0)	Base for the Digital Signal *X* series. Provides a transmission rate of 64 Kbps.
Distance Vector	Routing strategy that relies on an algorithm that works by having routers sporadically broadcast entire copies of their own routing table to all directly connected neighbors. This update identifies the networks each router knows about, and the distance between each of those networks. The distance is measured in hop counts or the number of routing domains that a packet must traverse between its source device and the device it attempts to reach.
DMZ	*See* Demilitarized Zone (DMZ).

Domain Name System (DNS) Stores information about hostnames and domain names in a type of distributed database on networks such as the Internet. Of the many types of information that can be stored, DNS most importantly provides a physical location (IP address) for each domain name and lists the mail-exchange servers accepting email for each domain.

DNS allows technical information to be transmitted in a human-readable way. While computers and network hardware work with IP addresses (such as 207.17.137.68) to perform tasks such as addressing and routing, humans generally find it easier to work with host names and domain names (such as www.juniper.com) in URLs and email addresses. DNS therefore mediates between the needs and preferences of humans and of software by translating domain names to IP addresses, such as www.juniper.net = 207.17.137.68.

DPD *See* Dead Peer Detection (DPD).

DS1 Digital Signal 1, also known as a T1 interface. *See* Digital Signal 0 (DS0).

DS3 Digital Signal 3, also known as a T3 interface. *See* Digital Signal 0 (DS0).

Dynamic Filtering IP service that can be used within VPN tunnels. Filters are one method some security devices use to control traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, Transmission Control Protocol (TCP) ports, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or TCP responses. *See also* Tunneling; Virtual Private Network (VPN).

Dynamic Host Configuration Protocol (DHCP) Method for automatically assigning IP addresses to hosts on a network. Depending upon the specific device model, security devices can allocate dynamic IP addresses to hosts, receive dynamically assigned IP addresses, or receive DHCP information from a DHCP server and relay the information to hosts.

Dynamic Routing Routing method which adjusts to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages. These messages populate the network, directing routers to rerun their algorithms and change their routing tables accordingly. There are two common forms of dynamic routing, including Distance Vector Routing and Link State Routing.

E1 Interface European format for digital transmission. This format carries signals at 2Mbps (32 channels at 64 Kbps, with 2 channels reserved for signaling and controlling).

Encapsulating Security Protocol/ Authentication Header (ESP/AH) IP-level security protocols, AH and ESP, were originally proposed by the Network Working Group focused on IP security mechanisms, IPsec. The term IPsec is used loosely here to refer to packets, keys, and routes that are associated with these protocols. The IP AH protocol provides authentication. ESP provides both authentication and encryption.

Encapsulating Security Protocol (ESP) *See* Encapsulating Security Protocol/Authentication Header (ESP/AH).

Encryption Process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. Data Encryption Standard (DES) and Triple DES (3DES) are two of the most popular public-key encryption schemes.

Equal Cost Multipath (ECMP) Assists with load balancing among two to four routes to the same destination or increases the effective bandwidth usage among two or more destinations. When enabled, security devices use the statically defined routes or dynamically learn multiple routes to the same destination through a routing protocol. The security device assigns routes of equal cost in round-robin fashion.

Export Rules When you have two or more virtual routers on a security device, you can configure export rules that define which routes on one virtual router are allowed to learned by another virtual router. *See also* Import Rules.

External Neighbors Two peer BGP routers residing in two different autonomous systems. *See* Border Gateway Protocol (BGP).

Filter List List of IP addresses permitted to send packets to the current routing domain.

Firewall Device that protects and controls the connection of one network to another, for traffic both entering and leaving. Firewalls are used by companies that want to protect any network-connected server from damage (intentional or otherwise) by those who log into it. This could be a dedicated computer equipped with security measures, or it could be a software-based protection.

Forward Explicit Congestion Notification (FECN) In a Frame Relay network, FECN is a header bit transmitted by the source (sending) terminal requesting that the destination (receiving) terminal slow down its requests for data. Backward Explicit Congestion Notification (BECN) is a header bit transmitted by the destination terminal requesting that the source terminal send data more slowly. FECN and BECN are intended to minimize the possibility that packets will be discarded (and thus have to be resent) when more packets arrive than can be handled.

Frame Relay WAN protocol that operates over a variety of network interfaces, including serial, T1/E1, and T3/E3. Frame Relay allows private networks to reduce costs by sharing facilities between the end-point switches of a network managed by a Frame Relay service provider.

Gateway Also called a *router*; a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

Gateway GPRS Support Node (GGSN) Device that acts as an interface between the GPRS backbone network and the external packet data networks (radio and IP). Among other things, a GGSN converts GPRS packets coming from an SGSN into the appropriate Packet Data Protocol (PDP) format and sends them out on the corresponding PDN. A GGSN also performs authentication and charging functions. *See also* General Packet Radio Service (GPRS).

GBIC	*See* Gigabit Interface Connector (GBIC).
General Packet Radio Service (GPRS)	Packet-based technology that enables high-speed wireless Internet and other data communications. GPRS provides more than three to four times greater speed than conventional Global System for Mobile Communications (GSM) systems. Often referred to as the *2.5G mobile telecommunications system.*
Generic Routing Encapsulation (GRE)	Protocol that encapsulates any type of packet within IPv4 unicast packets. For additional information on GRE, refer to RFC 1701, *Generic Routing Encapsulation (GRE).*
GGSN	*See* Gateway GPRS Support Node (GGSN).
Gigabit Interface Connector (GBIC)	Type of interface module card used on some security devices for connecting to a fiber optic network.
Gi Interface	Interface between a GSN and an external network or the Internet. *See* GPRS Support Node (GSN).
Global System for Mobile Communication (GSM)	Globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that formulates specifications for a pan-European mobile cellular radio system operating at 900 MHz.
Gn Interface	Interface between two GSNs within the same Public Land Mobile Network (PLMN).
Gp Interface	Interface between two GSNs located in different PLMNs.
G-PDU	User data message consisting of a T-PDU plus a GPRS Tunneling Protocol (GTP) header. *See also* T-PDU.
GPRS	*See* General Packet Radio Service (GPRS).
GPRS Roaming Exchange (GRX)	Since the Gp interface is IP based, it must support appropriate routing and security protocols to enable a subscriber to access its home services from any of its home PLMN's roaming partners. Many GPRS operators/carriers have abstracted these functions through the GPRS Roaming Exchange (GRX). This function is typically provided by a third-party IP network that offers VPN services to connect the roaming partners. The GRX service provider ensures that all aspects of routing and security between the networks are optimized for efficient operation. *See also* General Packet Radio Service (GPRS).
GPRS Support Node (GSN)	Term used to include both Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN). *See also* General Packet Radio Service (GPRS).
GPRS Tunneling Protocol (GTP)	IP-based protocol used within Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. GTP is layered on top of User Datagram Protocol (UDP). There are actually three separate protocols: GTP', GTP-Control (GTP-C), and GTP User (GTP-U). *See also* General Packet Radio Service (GPRS); GTP-Control (GTP-C) Message; GTP-User (GTP-U) Message.
GRX	*See* GPRS Roaming Exchange (GRX).
GSM	*See* Global System for Mobile Communication (GSM).
GSN	*See* GPRS Support Node (GSN).

GTP	*See* GPRS Tunneling Protocol (GTP).
GTP-Control (GTP-C) Messages	Exchanged between GPRS Support Node (GSN) pairs in a path. The messages are used to transfer GSN capability information between GSN pairs; to create, update and delete GPRS Tunneling Protocol (GTP) tunnels; and for path management. *See also* GPRS Tunneling Protocol (GTP); GTP Tunnel.
GTP-Protocol Data Unit (GTP-PDU)	Either a GTP-C or a GTP-U message. *See also* GPRS Tunneling Protocol (GTP).
GTP Signaling Messages	Exchanged between GPRS Support Node (GSN) pairs in a path. The messages are used to transfer GSN capability information between GSN pairs and to create, update, and delete GTP tunnels. *See* G-PDU.
GTP Tunnel	For each Packet Data Protocol (PDP) Context in the GPRS Support Node (GSN), a GPRS Tunneling Protocol (GTP) tunnel in the GTP-U plane is defined. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and access point name (APN) for tunnel-management messages or for each mobile station (MS) for messages not related to tunnel management. A GTP tunnel is identified in each node with a Tunnel Endpoint Identifier (TEID), an IP address, and a User Datagram Protocol (UDP) port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.
GTP-User (GTP-U) Messages	Exchanged between GPRS Support Node (GSN) pairs or GSN/Radio Network Controller (RNC) pairs in a path. The GTP-U messages are used to carry user data packets and signaling messages for path management and error indication. The user data transported can be packets in any of IPv4, IPv6, or PPP formats.
HA	*See* High Availability (HA).
High Availability (HA)	Configuring pairs of security devices to ensure service continuity in the event of a network outage or device failure.
Import Rules	When you have two or more virtual routers on a security device, you can configure import rules on one virtual router that define which routes are allowed to be learned from another virtual router. If you do not configure any import rules for a virtual router, all routes that are exported to that virtual router are accepted. *See also* Export Rules.
Infranet	Public network that combines the ubiquitous connectivity of the Internet with the assured performance and security of a private network.
Integrated Services Digital Network (ISDN)	international communications standard for sending voice, video, and data over digital telephone lines.
International Mobile Station Identity (IMSI)	A GPRS Support Node (GSN) identifies a mobile station by its IMSI, which is composed of three elements: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or Public Land Mobile Network (PLMN). *See also* GPRS Support Node (GSN); Public Land Mobile Network (PLMN).
Internet Control Message Protocol (ICMP)	Occasionally a gateway or destination host uses ICMP to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher-level protocol; however, ICMP is actually an integral part of IP and must be implemented by every IP module. ICMP messages

are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. IP is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communications environment, not to make IP reliable.

Internet Group Management Protocol (IGMP)
Protocol that runs between hosts and routers to communicate multicast group-membership information.

Internet Key Exchange (IKE)
Method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

Internet Security Association and Key Management Protocol (ISAKMP)
Provides a framework for Internet-key management and specific protocol support for negotiating security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

Intranet
Computer network, based on Internet technology, designed to meet the internal needs for sharing information within a single organization or company.

IP Security (IPsec)
Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides authentication, integrity, and confidentiality for secure communications and supports key exchanges even in larger networks. *See also* Data Encryption Standard-Cipher Block Chaining (DES-CBC); Encapsulating Security Protocol/Authentication Header (ESP/AH).

IP Tracking
Mechanism for monitoring configured IP addresses to see if they respond to ping or ARP requests. You can configure IP tracking with NSRP to determine device or VSD group failover. You can also configure IP tracking on a device interface to determine if the interface is up or down.

Key Management
Selection, exchange, storage, certification, expiration, revocation, changing, and transmission of encryption keys. *See also* Internet Security Association and Key Management Protocol (ISAKMP).

Local Preference
Border Gateway Protocol (BGP) attribute superior to the Multi-Exit Discriminator (MED) attribute for selecting a packet's path. LOCAL_PREF is the attribute used most often to configure preferences for one set of paths over another. *See also* Multi-Exit Discriminator (MED).

Loopback Interface
Logical interface that emulates a physical interface on the security device, but is always in the up state as long as the device is up. You must assign an IP address to a loopback interface and bind it to a security zone.

Mapped IP (MIP)
Direct one-to-one mapping of traffic destined for one IP address to another IP address.

MCC
See Mobile Country Code (MCC).

MED
See Multi-Exit Discriminator (MED).

Media Access Control (MAC) Address
Address that uniquely identifies the network interface card (NIC) such as an Ethernet adapter. For Ethernet, the MAC address is a 6-octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, the MAC address is the same as the Ethernet address.) When you are connected to the Internet from your computer (or *host*, as the Internet Protocol (IP) interprets it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sub-layer of the Data-Link Control Layer of telecommunications protocols. Each physical device type has a different MAC sub-layer.

Message Digest 5 (MD5)
An algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used, like a fingerprint of the input, to verify authenticity.

MIME
See Multipurpose Internet Mail Extension (MIME).

MIP
See Mapped IP (MIP).

MNC
See Mobile Network Code (MNC).

Mobile Country Code (MCC)
One of the three elements of an International Mobile Station Identity (IMSI); the other two are the Mobile Network Code (MNC) and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or Public Land Mobile Network (PLMN). *See also* International Mobile Station Identity (IMSI); Public Land Mobile Network (PLMN).

Mobile Network Code (MNC)
One of the three elements of an International Mobile Station Identity (IMSI); the other two are the Mobile Country Code (MCC) and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or Public Land Mobile Network (PLMN). *See also* International Mobile Station Identity (IMSI); Public Land Mobile Network (PLMN).

Mobile Subscriber Identification Number (MSIN)
One of the three elements of an International Mobile Station Identity (IMSI); the other two are the Mobile Country Code (MCC) and the Mobile Network Code (MNC). *See also* International Mobile Station Identity (IMSI).

MSIN
See Mobile Subscriber Identification Number (MSIN).

Multicast Policies
Policies that allow multicast control traffic, such as Internet Group Management Protocol (IGMP) or Protocol-Independent Multicast (PIM) messages, to cross security devices.

Multicast Routing
Routing method used to send multimedia streams to a group of receivers. Multicast-enabled routers transmit multicast traffic only to hosts that want to receive the traffic. Hosts must signal their interest in receiving multicast data and they must join a multicast group in order to receive the data.

Multi-Exit Discriminator (MED)
Border Gateway Protocol (BGP) attribute that determines the relative preference of entry points into an autonomous system (AS). *See also* Local Preference.

Multi-Exit Discriminator (MED) Comparison	Border Gateway Protocol (BGP) attribute used to determine an ideal link to reach a particular prefix in or behind the current autonomous system (AS). The MED contains a metric expressing a degree of preference for entry into the AS. You can establish precedence for one link over others by configuring a MED value for one link that is lower than other links. The lower the MED value, the higher priority the link has. The way this occurs is that one AS sets the MED value and the other AS uses the value in deciding which path to choose.
Multipurpose Internet Mail Extension (MIME)	Extensions that allow users to download different types of electronic media, such as video, audio, and graphics.
NAT	*See* Network Address Translation (NAT).
NAT-dst	*See* Destination Network Address Translation (NAT-dst).
NAT-src	*See* Network Address Translation (NAT).
NAT-Traversal (NAT-T)	Method for allowing IPsec traffic to pass through Network Address Translation (NAT) devices along the data path of a virtual private network (VPN) by adding a layer of User Datagram Protocol (UDP) encapsulation. The method first provides a means for detecting NAT devices during Phase 1 IKE exchanges and then provides a means for traversing them after Phase 2 IKE negotiations are complete. *See* Internet Key Exchange (IKE); Network Address Translation (NAT).
NetScreen Gatekeeper Protocol (NSGP)	Proprietary protocol that uses Transmission Control Protocol (TCP) and monitors the connectivity between client and server by sending Hello messages at specified intervals.
NetScreen Redundancy Protocol (NSRP)	Proprietary protocol that provides configuration and Run-Time Object (RTO) redundancy and a device failover mechanism for security units in a high availability (HA) cluster.
NetScreen Reliable Transfer Protocol (NRTP)	Proprietary protocol for multicasting NetScreen Redundancy Protocol (NSRP) control messages to multiple receivers when security devices are in a redundancy cluster (interconnected through the High Availability, or HA, ports). NRTP ensures that the primary security device always forwards configuration and policy messages to the backup devices.
Network Address Translation (NAT)	Translation of the source IP address in a packet header to a different IP address. Translated source IP addresses can come from a dynamic IP (DIP) address pool or from the IP address of the egress interface. When the security device draws addresses from a DIP pool, it can do so dynamically or deterministically. When doing the former, it randomly draws an address from the DIP pool and translates the original source IP address to the randomly selected address. When doing the latter, it uses address shifting to translate the source IP address to a predetermined IP address in the range of addresses that constitute the pool. When the security device uses the IP address of the egress interface, it translates all original source IP addresses to the address of the egress interface.

When the translated address comes from a DIP pool using address shifting, it cannot perform source port address translation. When the translated address comes from a DIP pool without address shifting, port translation is optional. When the translated address comes from the egress interface, port translation is required. |

NAT is also referred to as *NAT-src* to distinguish it from Destination Network Address Translation (NAT-dst).

Network and Security Manager (NSM)

why no definition?

Network and Security Manager (NSM) is Juniper Networks' enterprise-level management software application that configures and monitors multiple Juniper Networks security devices over a local area network (LAN) or a wide area network (WAN) environment. The NSM user interface (UI) enables network administrators to deploy, configure, and manage multiple devices from central locations. NSM uses three components to enable remote communication with security devices: the NSM UI; NSM Agent; and the management system, consisting of the GUI and Device Servers.

Network Layer Reachability Information (NLRI)

Each autonomous system (AS) has a routing plan that indicates the destinations that are reachable through it. This routing plan is called the NLRI object. BGP routers periodically generate and receive NLRI updates. Each update contains information on the list of autonomous systems that reachability information capsules traverse. Common values described by an NLRI update include a network number, a list of autonomous systems that the information passed through, and other path attributes.

Network Service Access Point Identifier (NSAPI)

Index to the Packet Data Protocol (PDP) context that is using the services provided by the lower layer Subnetwork Dependent Convergence Protocol (SNDCP). One PDP may have several PDP contexts and NSAPIs. *See also* Packet Data Protocol (PDP).

Next Hop

In the routing table, an IP address to which traffic for the destination network is forwarded. The next hop can also be another virtual router in the same security device.

Nonce

In security engineering, a nonce is a *number used once*, often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. For example, nonces are used in HTTP digest access authentication to calculate an MD5 digest of the password. The nonces are different each time the 401 authentication challenge-response code is presented, thus making the replay attack virtually impossible.

NRTP

See NetScreen Reliable Transfer Protocol.

NSAPI

See Network Service Access Point Identifier (NSAPI).

NSGP

See NetScreen Gatekeeper Protocol (NSGP).

NSRP

See NetScreen Redundancy Protocol (NSRP).

Online Certificate Status Protocol (OCSP)

When a security device performs an operation that uses a certificate, it is usually important to verify the validity of that certificate. Certificates might have become invalid through expiration or revocation. The default way to check the status of certificates is to use certificate revocation lists (CRLs). The Online Certificate Status Protocol (OCSP) is an alternative way to check the status of certificates. OCSP can quickly provide additional information about certificates and provide status checks.

Open Shortest Path First (OSPF)

Dynamic routing protocol intended to operate within a single autonomous system (AS).

Packet Data Protocol (PDP)	Primary protocol(s) used for packet data communications on a public data network (PDN), for example, TCP/IP on the Internet.
Packet Data Protocol (PDP) Context	User session on a GPRS network.
Perfect Forward Secrecy (PFS)	Defines how the security device generates the encryption key. PFS is a method for generating each new encryption key independently from the previous key.
PDU	*See* Protocol Data Unit.
Peer	*See* Neighbor.
PFA	*See* Packet Flow Acceleration (PFA).
PFS	*See* Perfect Forward Secrecy (PFS).
PIM	*See* Protocol Independent Multicast (PIM).
PLMN	*See* Public Land Mobile Network (PLMN).
Point-to-Point Protocol over ATM (PPPoA)	Usually used for Point-to-Point (PPP) sessions that are to be terminated on a security device with an ADSL interface. PPPoA is primarily used for business class services because it does not require a desktop client (which is required for PPPoE termination). *See also* Point-to-Point Protocol over Ethernet (PPPoE).
Point-to-Point Protocol over Ethernet (PPPoE)	Allows multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. You can configure PPPoE client instances, including the username and password, on any or all interfaces on some security devices.
Policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine which traffic passes across it based on IP session details. You can use policies to protect the resources in a security zone from attacks from another zone (interzone policies) or from attacks from within a zone (intrazone policies). You can also use policies to monitor traffic attempting to cross your firewall.
Port Address Translation (PAT)	Translation of the original source port number in a packet to a different, randomly designated port number.
Port Mapping	Translation of the original destination port number in a packet to a different, predetermined port number.
PPPoA	*See* Point-to-Point Protocol over ATM (PPPoA).
PPPoE	*See* Point-to-Point Protocol over Ethernet (PPPoE).
Preference	Value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network. The preference value is determined by the protocol or origin of the route. The lower the preference value of a route, the more likely the route is to be selected as the active route.
Protocol Data Unit (PDU)	Information delivered as a unit among peer entities of a network and that may contain control information, address information, or data.

In layered systems, a PDU is a unit of data specified in a protocol for a given layer and consisting of protocol-control information (and possibly user data) for the layer.

Protocol Independent Multicast (PIM) Multicast routing protocol that runs between routers to forward multicast traffic to multicast group members throughout the network. PIM-Dense Mode (PIM-DM) floods multicast traffic throughout the network and then prunes routes to receivers that do not want to receive the multicast traffic. PIM-Sparse Mode (PIM-SM) forwards multicast traffic only to those receivers that request it.

Protocol Independent Multicast-Source-Specific Mode (PIM-SSM) is derived from PIM-SM, and, like PIM-SM, it forwards multicast traffic to interested receivers only. Unlike PIM-SM, it immediately forms a Shortest Path Tree (SPT) to the source.

Proxy Server Also called a *proxy*, a technique used to cache information on a webserver and act as an intermediary between a web client and that webserver. It stores the most commonly and recently used web content in order to provide quicker access and to increase server security. This is common for an ISP, especially if it has a slow link to the Internet. *See also* Circuit-Level Proxy.

Public Land Mobile Network (PLMN) Public network dedicated to the operation of mobile radio communications.

Received Signal Strength Indicator (RSSI) Measurement of the strength (not necessarily the quality) of the received signal strength in a wireless environment. Measured in decibels relative to 1 milliwatt (dBm). The lower the RSSI, the stronger the signal.

Redistribution Process of importing a route into the current routing domain from another part of the network that uses another routing protocol. When this occurs, the current domain has to translate all the information, particularly known routes, from the other protocol. For example, if you are on an OSPF network and it connects to a BGP network, the OSPF domain has to import all the routes from the BGP network to inform all of its devices about how to reach all the devices on the BGP network. The receipt of all the route information is known as *route redistribution*.

Redistribution List List of routes the current routing domain imported from another routing domain that uses a different protocol.

Rendezvous Point (RP) Router at the root of the multicast distribution tree. All sources in a group send their packets to the RP, and the RP sends data down the shared distribution tree to all receivers in a network.

Reverse Path Forwarding Method used by multicast routers to check the validity of multicast packets. A router performs a route lookup on the unicast route table to check if the interface on which it received the packet (ingress interface) is the same interface it must use to send packets back to the sender. If it is, the router creates the multicast route entry and forwards the packet to the next-hop router. If it is not, the router drops the packet.

RIP *See* Routing Information Protocol (RIP).

RJ-11 Four-wire or six-wire connector used primarily to connect telephone equipment in the United States. RJ-11 connectors are also used to connect some types of local area networks (LANs), although RJ-45 connectors are more common.

RJ-45 Resembling a standard telephone connector, an RJ-45 connector is twice as wide (with eight wires) and is used for hooking up computers to local area networks (LANs) or telephones with multiple lines.

Route Flap Damping   Border Gateway Protocol (BGP) provides a technique, called *flap damping*, for blocking the advertisement of a route somewhere near its source until the route becomes stable. Route flap damping allows routing instability to be contained at an autonomous system (AS) border router adjacent to the region where instability is occurring. Limiting such unnecessary propagation maintains reasonable route-change convergence time as a routing topology grows.

Route Map   Used with Border Gateway Protocol (BGP) to control and modify routing information and to define the conditions by which routes are redistributed between routing domains. A route map contains a list of route-map entries, each containing a sequence number along with a match and a set value. The route-map entries are evaluated in the order of an incrementing sequence number. Once an entry returns a matched condition, no further route maps are evaluated. Once a match has been found, the route map carries out a permit or deny operation for the entry. If the route-map entry is not a match, then the next entry is evaluated for matching criteria.

Route Redistribution   Exporting of route rules from one virtual router to another.

Route Reflector   Router whose Border Gateway Protocol (BGP) configuration enables readvertising of routes between Interior BGP (IBGP) neighbors or neighbors within the same BGP autonomous system (AS). A route reflector client is a device that uses a route reflector to readvertise its routes to the entire AS. It also relies on that route reflector to learn about routes from the rest of the network.

Routing Information Protocol (RIP)   Dynamic routing protocol used within a moderate-sized autonomous system (AS).

Routing Table   List in a virtual router's memory that contains a real-time view of all the connected and remote networks to which a router is currently routing packets.

RSSI   *See* Received Signal Strength Indicator (RSSI).

Run-Time Object (RTO)   Code object created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, certificates, DHCP leases, and IPsec Phase 2 security associations (SAs).

SBR   *See* Source-Based Routing (SBR).

Secure Copy (SCP)   Method of transferring files between a remote client and a security device using the SSH protocol. The security device acts as an SCP server, accepting connections from SCP clients on remote hosts.

Secure Hash Algorithm-1 (SHA-1)   Algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

Secure Shell (SSH)   Protocol that allows device administrators to remotely manage the device in a secure manner. You can run either an SSH version 1 or version 2 server on the security device.

Security Association (SA)   Unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. For bidirectional communications, there must be at least two SAs, one for each direction. The VPN participants negotiate and agree to Phase 1 and Phase 2 SAs during an AutoKey IKE negotiation. *See also* Security Parameters Index (SPI).

Security Parameters Index (SPI)	Hexadecimal value that uniquely identifies each tunnel. It also tells the security device which key to use to decrypt packets.
Security Zone	Security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic via policies.
Service Set Identifier (SSID)	Thirty-two-character unique identifier attached to the header of packets sent over a wireless local area network (WLAN), which acts as a password when a mobile device tries to connect to the basic service set (BSS). The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID.
Serving GPRS Support Node (SGSN)	Connects one or more base station controllers (BSCs) to the GPRS backbone network, providing IP connectivity to the Gateway GPRS Support Node *(*GGSN).
Session Description Protocol (SDP)	Session descriptions appear in many SIP messages and provide information that a system can use to join a multimedia session. SDP information includes IP addresses, port numbers, times, dates, and information about the media stream.
Session Initiation Protocol (SIP)	Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.
Shared Distribution Tree	Multicast distribution tree where the source transmits the multicast traffic to the rendezvous point (RP), which then forwards the traffic downstream to receivers on the distribution tree.
Shortest Path Tree (SPT)	Multicast distribution tree where the source is at the root of the tree and it forwards multicast data downstream to each receiver. This is also referred to as a *source-specific tree*.
Signal-to-Noise Ratio (SNR)	Ratio of the amplitude of a desired analog or digital data signal to the amplitude of noise in a transmission channel at a specific time. SNR is typically expressed logarithmically in decibels (dB).
SIP	*See* Session Initiation Protocol (SIP).
Source-Based Routing (SBR)	Configuration of a virtual router on a security device to forward traffic based on the source address of the data packet instead of just the destination address.
Source Interface-Based Routing (SIBR)	Allows a security device to forward traffic based on the source interface (the interface on which the data packet arrives on the device).
SSID	*See* Service Set Identifier (SSID).
Static Routing	User-defined routes that cause packets moving between a source and a destination to take a specified path. Static routing algorithms are table mappings established by the network administrator prior to the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

The software remembers static routes until you remove them. However, you can override static routes with dynamic routing information through judicious assignment of administrative distance values. To do this, you must ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

Subinterface Logical division of a physical interface that borrows the bandwidth it needs from the physical interface from which it stems. A subinterface is an abstraction that functions identically to an interface for a physically present port and is distinguished by 802.1Q VLAN tagging.

Symmetric High-Speed Digital Subscriber Line (SHDSL) Physical WAN symmetric DSL interface capable of sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 Kbps and 2.31 Mbps. G.SHDSL incorporates features of other DSl technologies such as asymmetric DSL and transports T1, E1, ISDN, Asynchronous Transfer Mode (ATM), and Internet Protocol (IP) signals.

Syslog Protocol that enables a device to send log messages to a host running the syslog daemon (syslog server). The syslog server then collects and stores these log messages locally.

T1 Interface Physical WAN interface for transmitting digital signals in the T-carrier system, used in North America and Japan. Usually a dedicated phone connection supporting data rates of 1.544 Mbps. This interface is also known as DS1.

T3 Interface Physical WAN interface for transmitting digital signals in the T-carrier system, used in North America and Japan. A dedicated phone connection supporting data rates of about 43 Mbps. This interface is also known as DS3.

TEID *See* Tunnel Endpoint Identifier (TEID).

TID *See* Tunnel Identifier (TID).

T-PDU Payload tunneled in the GPRS Tunneling Protocol (GTP) tunnel.

Transmission Control Protocol/Internet Protocol (TCP/IP) Set of communication protocols that supports peer-to-peer connectivity functions both for local area networks (LANs) and for wide area networks (WANs). TCP/IP controls how data is transferred between computers on the Internet. See *Communications Protocol.*

Trunk Port Allows a switch to bundle traffic from several virtual local area networks (VLANs) through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.

Trust Zone One of two security zones that enables packets to be secured from being seen by devices external to your current security domain.

Tunnel Endpoint Identifier (TEID) Uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end side of a GPRS Tunneling Protocol (GTP) tunnel locally assigns the TEID value that the transmitting side has to use. The TEID values are exchanged between tunnel endpoints using GTP-C messages. *See also* GPRS Tunneling Protocol (GTP); GTP-Control (GTP-C) Messages; GTP Tunnel; GTP-User (GTP-U) Messages.

Tunnel Identifier (TID)   Packets traveling along the GPRS backbone are wrapped inside an additional addressing layer to form GPRS Tunneling Protocol (GTP) packets. Each GTP packet then carries a TID. *See also G*lobal System for Mobile Communication (GSM).

Tunneling   Method of data encapsulation. With virtual private network (VPN) tunneling, a mobile professional dials into a Point of Presence (POP) of a local Internet Service Provider (ISP) instead of dialing directly into a corporate network. This means that no matter where mobile professionals are located, they can dial a local ISP that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call. When remote users dial into their corporate network using an ISP that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the ISP's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network and that they can access only the hosts that they are authorized to use.

Tunnel Interface   Opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface.

Tunnel Zone   Logical segment that hosts one or more tunnel interfaces. Associated with a security zone that acts as its carrier.

Universal Serial Bus (USB)   External bus standard that supports data transfer rates of up to 12 Mbps.

Untrust Zone   One of two security zones that enables packets to be seen by devices external to your current security domain.

User Datagram Protocol (UDP)   Protocol in the TCP/IP protocol suite that allows an application program to send datagrams to other application programs on a remote machine. UDP provides an unreliable and connectionless datagram service where delivery and duplicate detection are not guaranteed. It does not use acknowledgments or control the order of arrival.

Virtual Adapter   TCP/IP settings that a security device assigns to a remote XAuth user for use in a virtual private network (VPN) connection. These settings include Internet Protocol (IP) address, Domain Name System (DNS) server addresses, and Windows Internet Naming Service (WINS) server addresses.

Virtual IP (VIP) Address   A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.

Virtual Link   Logical path from a remote OSPF area to the backbone area.

Virtual Local Area Network (VLAN)   Logical rather than physical grouping of devices that constitutes a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.

Virtual Private Network (VPN) Network scheme in which portions of a network are connected via the Internet, but information sent across the Internet is encrypted. The result is a virtual network that is also part of a larger network entity. This enables corporations to provide telecommuters and mobile professionals with local dialup access to their corporate network or to another Internet Service Provider (ISP). VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPsec.

Virtual Router Component of ScreenOS that performs routing functions. By default, a security device supports two virtual routers: Untrust-VR and Trust-VR.

Virtual Security Device (VSD) Single logical device comprising a set of physical security devices.

Virtual Security Interface (VSI) Logical entity at Layer 3 that is linked to multiple Layer 2 physical interfaces in a Virtual Security Device (VSD) group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover, and it becomes the new master.

Virtual System (vsys) Subdivision of the main system that appears to the user to be a standalone entity. Virtual systems reside separately from each other in the same security device. Each one can be managed by its own virtual system administrator.

WEP *See* Wired Equivalent Privacy (WEP).

Wi-Fi Protected Access (WPA) Wi-Fi standard designed to improve upon the security features of Wired Equivalent Privacy (WEP).

Windows Internet Naming Service (WINS) Service for mapping Internet Protocol (IP) addresses to NetBIOS computer names on Windows NT server-based networks. A WINS server maps a NetBIOS name used in a Windows network environment to an IP address used on an IP-based network.

Wired Equivalent Privacy (WEP) Encrypts and decrypts data as it travels over the wireless link with the Rivest Cipher 4 (RC4) stream cipher algorithm.

Wireless Access Point (WAP) Hardware device that acts as a communication hub for wireless clients to connect to a wired LAN.

Wireless Local Area Network (WLAN) Type of LAN that uses high-frequency radio waves rather than wires to communicate between nodes.

WPA *See* Wi-Fi Protected Access (WPA).

XAuth Protocol comprising two components: remote VPN user authentication (username plus password) and TCP/IP address assignments (IP address, netmask, DNS server, and WINS server assignments).

Zone Segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or either a physical or a logical entity that performs a specific function (a function zone).