



ScreenOS Glossary of Terms

Release 6.3.0, Rev. 01

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

Copyright Notice

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright 2009 Juniper Networks, Inc. All rights reserved.
Printed in the USA.

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 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 the instruction manual, 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 and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Juniper Networks, Inc. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

ScreenOS Glossary of Terms

3DES	See Triple Data Encryption Standard (3DES).
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	See wireless access point.
access point name (APN)	Information element (IE) included in the header of a GPRS Tunneling Protocol (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 Resolution Protocol (ARP)	Protocol for mapping an IP address to a physical (MAC) address that is recognized in the local network. A table, called the <i>ARP cache</i> , is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.
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	<i>See asymmetric digital subscriber line (ADSL).</i>
aggregate state	A router is in an aggregate state when it is one of multiple virtual Border Gateway Protocol (BGP) routing instances bundled into one address.
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	<i>See Encapsulating Security Protocol/Authentication Header (ESP/AH).</i>
ALG	<i>See Application Layer Gateway (ALG).</i>
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.
ARP	<i>See Address Resolution Protocol (ARP).</i>
AS	<i>See autonomous system (AS).</i>
AS boundary router	Router that connects an autonomous system (AS) running one routing protocol to another AS running a different protocol.
AS number	Identification number of the local autonomous system (AS) mapped to a Border Gateway Protocol (BGP) routing instance. The ID number can be any valid integer.
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 Border Gateway Protocol (BGP) routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance.
AS path attribute class	Border Gateway Protocol (BGP) provides four classes of path attributes: well-known mandatory, well-known discretionary, optional transitive, and optional nontransitive.

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 Advanced Encryption Standard (AES), Data Encryption Standard (DES), or Triple DES (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 <i>network layer reachability information (NLRI)</i> 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 re-sent) when more packets arrive than can be handled.
Basic Rate Interface (BRI)	ISDN service also called <i>2B+D</i> , 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 a <i>bgroup interface</i> . 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	Piece of cryptographic data that guarantees that a particular public key is associated with the private key of a particular entity.
Certificate Authority (CA)	Entity responsible for issuing certificates and certificate revocation lists (CRLs).
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 <i>application-level proxies</i> or <i>application-level gateways</i> , 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 <i>circuit-level</i> proxy, supports multiple applications. For example, SOCKS is a generic IP-based proxy server that supports TCP and UDP applications.
Cisco High-Level Data Link Control (Cisco-HDLC)	Proprietary Cisco encapsulation for transmitting local area network (LAN) protocols over a wide area network (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 Border Gateway Protocol (BGP), giving the network greater flexibility.
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 (BGP) autonomous system (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 <i>mesh</i> , 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).

Differentiated Services code point (DSCP) A field in the header of IP packets used for packet-classification purposes. A DSCP is a 6-bit value that, when included in the DS field of an IP header, indicates how a packet must be forwarded. It uses the six most significant bits in the type of service (ToS) field defined for IPv4 or IPv6 packet headers.

Differentiated Services (DiffServ) Based on RFC 2474, DiffServ uses the type of service (ToS) byte to identify different packet flows on a packet-by-packet basis.

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 along with 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 hostnames and domain names (such as www.juniper.net) in URLs and email addresses. DNS therefore mediates between the needs and preferences of humans and software by translating domain names to IP addresses, such as www.juniper.net = 207.17.137.68.

DP See DSCP Precedence (DP).

DPD See dead peer detection (DPD).

DSCP See Differentiated Services code point (DSCP).

DSCP Precedence (DP) A type of quality of service (QoS) profile that contains entries for mapping Differentiated Services code point (DSCP) with QoS parameters.

DS0 See Digital Signal 0 (DS0).

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. <i>See also</i> 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 that 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: <i>distance vector</i> and <i>link state</i> .
E1 interface	European format for digital transmission. This format carries signals at 2 Mbps (32 channels at 64 Kbps, with 2 channels reserved for signaling and controlling).
ECDH	<i>See</i> Elliptical Curve Diffie-Hellman (ECDH).
Elliptical Curve Diffie-Hellman (ECDH)	A public key algorithm that allows two parties, each with an elliptic curve public-private key pair, to establish a shared secret key over an insecure channel.
Encapsulating Security Protocol/Authentication Header (ESP/AH)	IP-level security protocols, AH and ESP, were originally proposed by the Network Working Group, which focused on IP security mechanisms (IPsec). The term <i>IPsec</i> 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)	<i>See</i> 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 be learned by another virtual router. <i>See also</i> import rules.
external neighbors	Two peer Border Gateway Protocol (BGP) routers residing in two different autonomous systems.
filter list	List of IP addresses permitted to send packets to the current routing domain.
firewall	A firewall screens traffic crossing the boundary between a private LAN and the public network, such as the Internet. It can be a dedicated computer equipped with security measures, or it can be a software-based system.
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 re-sent) 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 <i>router</i> , 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. <i>See also</i> General Packet Radio Service (GPRS).
GBIC	<i>See</i> 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 <i>2.5G mobile telecommunications system</i> .
Generic Routing Encapsulation (GRE)	Protocol that encapsulates any type of packet within IPv4 unicast packets. For additional information on GRE, refer to RFC 1701, <i>Generic Routing Encapsulation (GRE)</i> .
GGSN	<i>See</i> 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. <i>See</i> 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 Public Land Mobile Networks (PLMNs).
G-PDU	User data message consisting of a T-PDU plus a GPRS Tunneling Protocol (GTP) header. <i>See also</i> T-PDU.
GPRS	<i>See</i> 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 Public Land Mobile Network's (PLMN) 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. <i>See also</i> 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). <i>See also</i> 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). <i>See also</i> General Packet Radio Service (GPRS).
GRX	<i>See</i> GPRS Roaming Exchange (GRX).
GSM	<i>See</i> Global System for Mobile Communication (GSM).
GSN	<i>See</i> GPRS Support Node (GSN).
GTP	<i>See</i> 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. <i>See also</i> GPRS Tunneling Protocol (GTP); GTP tunnel.
GTP-Protocol Data Unit (GTP-PDU)	Either a GTP-C or a GTP-U message. <i>See also</i> 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. <i>See</i> 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.
HMAC	See Key-Hashing Message Authentication Code (HMAC).
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. <i>See also</i> 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 comprises 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).
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. <i>See also</i> 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 NetScreen Redundancy Protocol (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-Hashing Message Authentication Code (HMAC)	In cryptography, an HMAC is a type of message-authentication code calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.
key management	Selection, exchange, storage, certification, expiration, revocation, changing, and transmission of encryption keys. <i>See also</i> 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. <i>See also</i> 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.
Management Information Base (MIB)	A MIB serves as a data dictionary, or code book, used to assemble and interpret Simple Network Management Protocol (SNMP) messages. Each SNMP element manages specific objects, with each object having specific characteristics such as a unique object identifier (OID) consisting of numbers separated by decimal points (for example, 1.3.6.1.4.1.2682.1). These OIDs naturally form a tree. The MIB associates each OID with a readable label and various other parameters related to the object.
Mapped IP (MIP)	Direct one-to-one mapping of traffic destined for one IP address to another IP address.
MCC	<i>See</i> Mobile Country Code (MCC).
MED	<i>See</i> 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 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.
MIB	<i>See</i> Management Information Base (MIB).
MIME	<i>See</i> Multipurpose Internet Mail Extension (MIME).
MIP	<i>See</i> Mapped IP (MIP).
MNC	<i>See</i> 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). <i>See also</i> 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). <i>See also</i> 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). <i>See also</i> International Mobile Station Identity (IMSI), Public Land Mobile Network (PLMN).
MSIN	<i>See</i> 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). <i>See also</i> 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 the priority of the link. One AS sets the MED value, and the other AS uses the value in deciding which path to choose.
Multipurpose Internet Mail Extension (MIME)	Extension that allows 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)	<p>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.</p> <p>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 <i>NAT-src</i> to distinguish it from Destination Network Address Translation (NAT-dst).</p>

Network and Security Manager (NSM)	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 <i>NLRI object</i> . 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 (SNDP). One PDP can have several PDP contexts and NSAPIs. <i>See also</i> 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 <i>number used once</i> , 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	<i>See</i> NetScreen Reliable Transfer Protocol.
NSAPI	<i>See</i> network service access point identifier (NSAPI).
NSGP	<i>See</i> NetScreen Gatekeeper Protocol (NSGP).
NSRP	<i>See</i> 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, since a certificate could be invalid because it has expired or been revoked. The default way to check the status of certificates is to use certificate revocation lists (CRLs). 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.

PDU	<i>See</i> protocol data unit.
Perfect Forward Secrecy (PFS)	Protocol that defines how the security device generates an encryption key. PFS is a method for generating each new encryption key independently from the previous key.
PFS	<i>See</i> Perfect Forward Secrecy (PFS).
PIM	<i>See</i> Protocol Independent Multicast (PIM).
PLMN	<i>See</i> 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 asymmetric digital subscriber line (ADSL) interface. PPPoA is primarily used for business class services because it does not require a desktop client (which is required for PPPoE termination). <i>See also</i> 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 security device, 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 traverse your network.
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.
PP	<i>See</i> Precedence Profile (PP).
PPPoA	<i>See</i> Point-to-Point Protocol over ATM (PPPoA).
PPPoE	<i>See</i> 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.
Precedence Profile (PP)	A type of quality of service (QoS) profile that contains entries for mapping IP precedence with QoS parameters.
protocol data unit (PDU)	Information delivered as a unit among peer entities of a network, which 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 consists of protocol-control information (and possibly user data) for the layer.

Protocol Independent Multicast (PIM)	<p>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.</p> <p>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.</p>
proxy server	Also called a <i>proxy</i> , 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. <i>See also</i> circuit-level proxy.
Public Land Mobile Network (PLMN)	Public network dedicated to the operation of mobile radio communications.
quality of service (QoS)	Measurement of performance, such as transmission rates and error rates, of a communications channel or system.
QoS	<i>See</i> quality of service (QoS).
QoS profile	A quality of service (QoS) profile maps IP precedence and Differentiated Services code point (DSCP) values of incoming packets with QoS parameters.
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 Open Shortest Path First (OSPF) network and it connects to a Border Gateway Protocol (BGP) network, the OSPF domain has to import all the routes from the BGP network to inform all its devices about how to reach all the devices on the BGP network. The receipt of all route information is known as <i>route redistribution</i> .
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	<i>See</i> 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 <i>flap damping</i> , 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).
SCTP	See Stream Control Transmission Protocol (SCTP).
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 Hash Algorithm-2 (SHA2-256)	An algorithm that produces a 256-bit hash from a message of arbitrary length and a 32-byte key. It is more secure than SHA-1 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 an SSH version 2 server on the security device.
security association (SA)	Unidirectional agreement between the virtual private network (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. <i>See also</i> 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	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 cache	A special structure that stores (caches) all reusable information in software and hardware sessions that are created by the first connection of an HTTP session bundle.
Session Description Protocol (SDP)	Session descriptions appear in many session Initiation Protocol (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.
SHA-1	<i>See</i> Secure Hash Algorithm-1 (SHA-1).
SHA2-256	<i>See</i> Secure Hash Algorithm-2 (SHA2-256).
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 <i>source-specific tree</i> .

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).
SIM	See Subscriber Identity Module (SIM).
Simple Network Management Protocol (SNMP)	The default standard network management protocol on TCP/IP-based networks.
SIP	See Session Initiation Protocol (SIP).
SNMP	See Simple Network Management Protocol (SNMP).
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	<p>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.</p> <p>ScreenOS retains 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.</p>
Stream Control Transmission Protocol (SCTP)	A Transport Layer protocol that ensures reliable, in-sequence transport of data with congestion control.
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.
Subscriber Identity Module (SIM)	Smart card used in cellular telephones.
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. Also known as <i>G.SHDSL</i> , it incorporates features of other DSL technologies such as asymmetric DSL (ADSL) and transports T1, E1, ISDN, ATM, and 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 <i>DS1</i> .
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 <i>DS3</i> .
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.
Triple Data Encryption Standard (3DES)	A more powerful version of DES in which the original DES algorithm is applied in three rounds using a 168-bit key. DES provides significant performance savings but is considered unacceptable for many classified or sensitive material transfers.
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. The other is the untrust zone
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. <i>See also</i> 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. <i>See also</i> Global 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) belonging to 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 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. The other is the trust zone.
User-based Security Model (USM)	One of the core modules within the Simple Network Management Protocol version 3 (SNMPv3) framework. The USM authenticates, encrypts, and decrypts SNMP packets. The USM in an SNMPv3 packet uses six values. The USM secures message transfer by verifying the message's sender and timeliness, a process called <i>authentication</i> . The authentication module uses the values to ensure data integrity and origin authentication. The USM encrypts the messages being sent, a process called <i>privacy</i> . The privacy module uses the values to protect against payload disclosure. The timeliness module uses the values to protect against message delay.
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 nor control the order of arrival.
USM	See User-based Security Model (USM).
VACM	See View-based Access Control Model (VACM).
View-based Access Control Model (VACM)	A core access-control module in Simple Network Management Protocol version 3 (SNMPv3) that is responsible for determining whether a specific type of access to a specified managed object is allowed.
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 Open Shortest Path First (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 instead 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 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 primary for 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 primary.
virtual system (vsys)	Subdivision of the main system, which appears to the user to be a standalone entity. Vsyes reside separately from each other in the same security device. Each one can be managed by its own vsys 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	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).