NetScreen Concepts & Examples

ScreenOS Reference Guide

Volume 1: Overview

ScreenOS 5.0.0

P/N 093-0924-000

Rev. B

Copyright Notice

Copyright © 2003 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089
www.netscreen.com

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 NetScreen's 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

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 THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Volume 1: Overview

Volume 2: Fundamentals

Volume 3: Administration

Volume 4: Attack Detection and Defense Mechanisms

Volume 5: VPNs

Volume 6: Dynamic Routing

Volume 7: Virtual Systems

Volume 8: High Availability

Preface

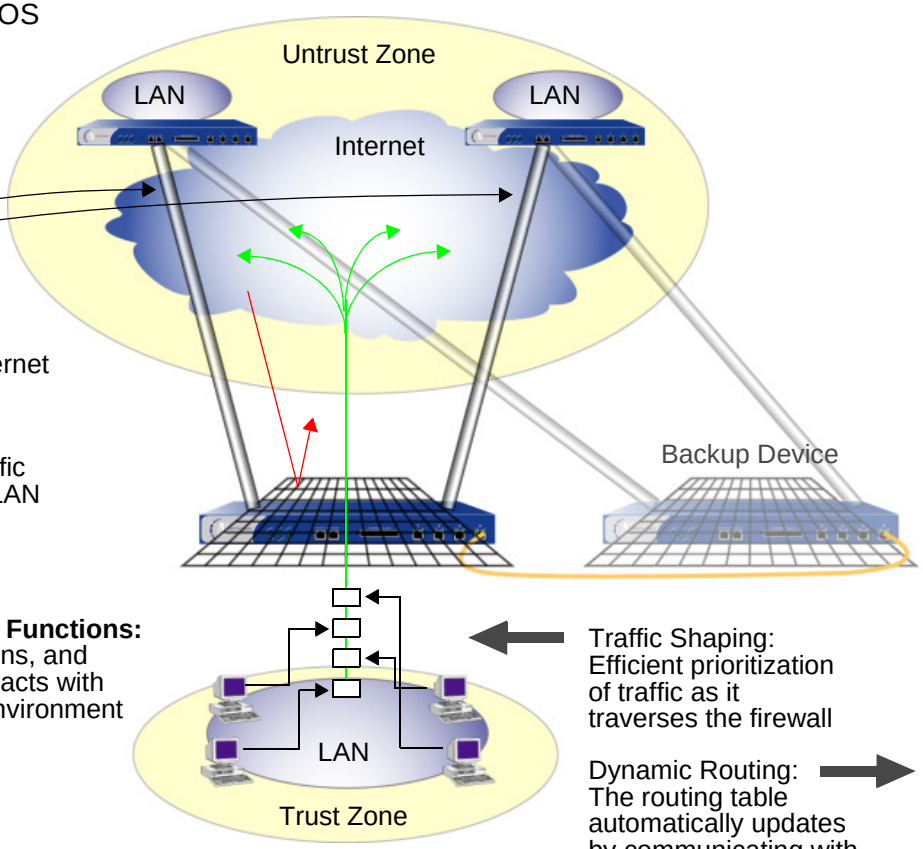
NetScreen devices are ASIC-based, ICSA-certified[1] Internet security appliances and security systems that integrate firewall, virtual private networking (VPN), and traffic-shaping features to provide flexible protection for security zones such as the internal local area network (LAN) or demilitarized zone (DMZ) when connecting to the Internet.

- **Firewall:** A firewall screens traffic crossing the boundary between a private LAN and the public network, such as the Internet.
- **VPN:** A VPN provides a secure communications channel between two or more remote network appliances.
- **Integrated Networking Functions:** Dynamic routing protocols learn reachability and advertise dynamically changing network topologies. In addition, traffic shaping functionality allows administrative monitoring and control of traffic passing across the NetScreen firewall to maintain a network's quality-of-service (QoS) level.
- **Redundancy:** High availability of interfaces, routing paths, NetScreen devices, and—on high-end NetScreen devices—power supplies and fans, to avoid a single point of failure in any of these areas.

Note: *For information on NetScreen compliance with Federal Information Processing Standards (FIPS) and for instructions on setting a FIPS-compliant NetScreen device in FIPS mode, see the platform-specific* NetScreen Cryptographic Module Security Policy *document on the NetScreen documentation CD-ROM*.

1. The Internet Computer Security Association (ICSA) is an organization focused on all types of network security for Internet-connected companies. Among its many functions, ICSA provides product certification for several kinds of security products such as virus protection, firewall, PKI, intrusion detection, IPSec, and cryptography. ICSA has certified all NetScreen products for firewall and IPSec.

Key Features in ScreenOS



VPNs: Secure communication tunnels between sites for traffic passing through the Internet

Firewall: Screening traffic between the protected LAN and the Internet

Integrated Networking Functions: Performs routing functions, and communicates and interacts with routing devices in the environment

Redundancy: The backup device maintains identical configuration and sessions as those on the primary device to assume the place of the primary device if necessary. (Note: Interfaces, routing paths, power supplies, and fans can also be redundant.)

Traffic Shaping: Efficient prioritization of traffic as it traverses the firewall

Dynamic Routing: The routing table automatically updates by communicating with dynamic routing peers.

Dst	Use
0.0.0.0/0	1.1.1.250
1.1.1.0/24	eth3
1.2.1.0/24	eth2
10.1.0.0/16	trust-vr
10.2.2.0/24	tunnel.1
10.3.3.0/24	tunnel.2

NetScreen ScreenOS is the operating system that provides all the features needed to set up and manage any NetScreen security appliance or system. The *NetScreen Concepts & Examples ScreenOS Reference Guide* provides a useful reference guide for configuring and managing a NetScreen appliance through the ScreenOS.

CONCEPTS & EXAMPLES ORGANIZATION

The *NetScreen Concepts & Examples ScreenOS Reference Guide* is a multiple-volume set of documents. The following information outlines and summarizes the material in each volume:

Volume 1, "Overview"

- "Contents" contains a master table of contents for all volumes in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.
- Appendix A, "Glossary" provides definitions for all the key terms used throughout all volumes in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.
- "Index" is a master index encompassing all volumes in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Volume 2, "Fundamentals"

- Chapter 1, "ScreenOS Architecture" presents the fundamental elements of USGA—the architecture in the NetScreen ScreenOS—and concludes with a four-part example illustrating an enterprise-based configuration incorporating most of those elements. In this and all subsequent chapters, each concept is accompanied by illustrative examples.
- Chapter 2, "Routing Tables and Static Routing" describes the ScreenOS routing table, the basic routing process on the NetScreen device, and how to configure static routes on NetScreen devices.
- Chapter 3, "Zones" explains security zones, tunnel zones, and function zones.
- Chapter 4, "Interfaces" describes the various physical, logical, and virtual interfaces on NetScreen devices, and includes information on various firewall attacks and the attack blocking options that NetScreen provides.
- Chapter 5, "Interface Modes" explains the concepts behind Transparent, Network Address Translation (NAT), and Route interface operational modes.
- Chapter 6, "Building Blocks for Policies" discusses the elements used for creating policies and virtual private networks (VPNs): addresses (including VIP addresses), users, and services. It also presents several example configurations support for the H.323 protocol.
- Chapter 7, "Policies" explores the components and functions of policies and offers guidance on their creation and application.

- Chapter 8, “Address Translation” explains the different methods for source address translation and destination address translation.
- Chapter 9, “User Authentication” details the various authentication methods and uses that NetScreen supports.
- Chapter 10, “Traffic Shaping” explains how you can manage bandwidth at the interface and Policy levels and prioritize services.
- Chapter 11, “System Parameters” presents the concepts behind Domain Name System (DNS) addressing; using Dynamic Host Configuration Protocol (DHCP) to assign or relay TCP/IP settings; downloading and uploading system configurations and software; and setting the system clock.

Volume 3, “Administration”

- Chapter 1, “Administration” explains the different means available for managing a NetScreen device both locally and remotely. This chapter also explains the privileges pertaining to each of the four levels of network administrators that can be defined. Finally, it explains how to secure local and remote administrative traffic.
- Chapter 2, “Monitoring NetScreen Devices” explains various monitoring methods and provides guidance in interpreting monitoring output.
- Appendix A, “SNMP MIB Files” lists and briefly describes the Management Information Base (MIB) files available for MIB compilers.

Volume 4, “Attack Detection and Defense Mechanisms”

- Chapter 1, “Protecting a Network” outlines the basic stages of an attack and the firewall options available to combat the attacker at each stage.
- Chapter 2, “Reconnaissance Deterrence” describes the options available for blocking IP address sweeps, port scans, and attempts to discover the type of operating system (OS) of a targeted system.
- Chapter 3, “Denial-of-Service Attack Defenses” explains firewall, network, and OS-specific DoS attacks and how NetScreen mitigates such attacks.
- Chapter 4, “Content Monitoring and Filtering” describes how to protect Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) users from malicious uniform resource locators (URLs) and how to configure the NetScreen device to work with third party products to provide antivirus scanning and URL filtering.

- Chapter 5, “Deep Inspection” describes how to configure the NetScreen device to obtain IDP attack object updates, how to create user-defined attack objects and attack object groups, and how to apply IDP at the policy level.
- Chapter 1, “Suspicious Packet Attributes” explains a number of SCREEN options that block potentially dangerous packets.

Volume 5, “VPNs”

- Chapter 1, “IPSec” provides background information about IPSec, presents a flow sequence for Phase 1 in IKE negotiations in Aggressive and Main modes, and concludes with information regarding NAT-Traversal.
- Chapter 2, “Public Key Cryptography” provides information on how to obtain and load digital certificates and certificate revocation lists (CRLs).
- Chapter 3, “VPN Guidelines” offers some useful information to help in the selection of the available VPN options. It also presents a packet flow chart to demystify VPN packet processing.
- Chapter 4, “Site-to-Site VPNs” provides extensive examples VPN configurations connecting two private networks.
- Chapter 5, “Dialup VPNs” provides extensive examples of client-to-LAN communication using AutoKey IKE. It also details group IKE ID and shared IKE ID configurations.
- Chapter 6, “L2TP” explains the Layer 2 Tunneling Protocol (L2TP), its use alone and in conjunction with IPSec (L2TP-over-IPSec).
- Chapter 7, “Advanced VPN Features” contains information and examples for the more advanced VPN configurations, such as VPN monitoring, binding multiple tunnels to a single tunnel interface, and hub-and-spoke and back-to-back tunnel designs

Volume 6, “Dynamic Routing”

- Chapter 1, “Virtual Routers” explains how to configure virtual routers on NetScreen devices and how to redistribute routing table entries between protocols or between virtual routers.
- Chapter 2, “Open Shortest Path First (OSPF)” describes how to configure the OSPF dynamic routing protocol on NetScreen devices.
- Chapter 3, “Routing Information Protocol (RIP)” describes how to configure the RIP dynamic routing protocol on NetScreen devices.
- Chapter 4, “Border Gateway Protocol (BGP)” describes how to configure the BGP dynamic routing protocol on NetScreen devices.

Volume 7, “Virtual Systems”

- Chapter 1, “Virtual Systems” presents the concepts of virtual systems, dedicated and shared interfaces, and VLAN-based and IP-based traffic classification. It also explains how to set up virtual systems and create virtual system administrators.

Volume 8, “High Availability”

- Chapter 1, “NSRP” explains how to cable, configure, and manage NetScreen devices in a redundant group to provide high availability using the NetScreen Redundancy Protocol (NSRP).
- Chapter 2, “NSRP-Lite” explains how to configure NetScreen devices that support NSRP-Lite.
- Chapter 3, “Interface Redundancy” describes the various ways in which NetScreen devices provide interface redundancy.
- Chapter 4, “Failover” describes the configuration for the failover of a device, virtual security device (VSD) group, and virtual system. It also explains how to monitor certain objects to determine the failover of a device or VSD group.

CONVENTIONS

This document contains several types of conventions, which are introduced in the following sections:

CLI Conventions

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 } manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".
- Variables appear in *italic.* For example:

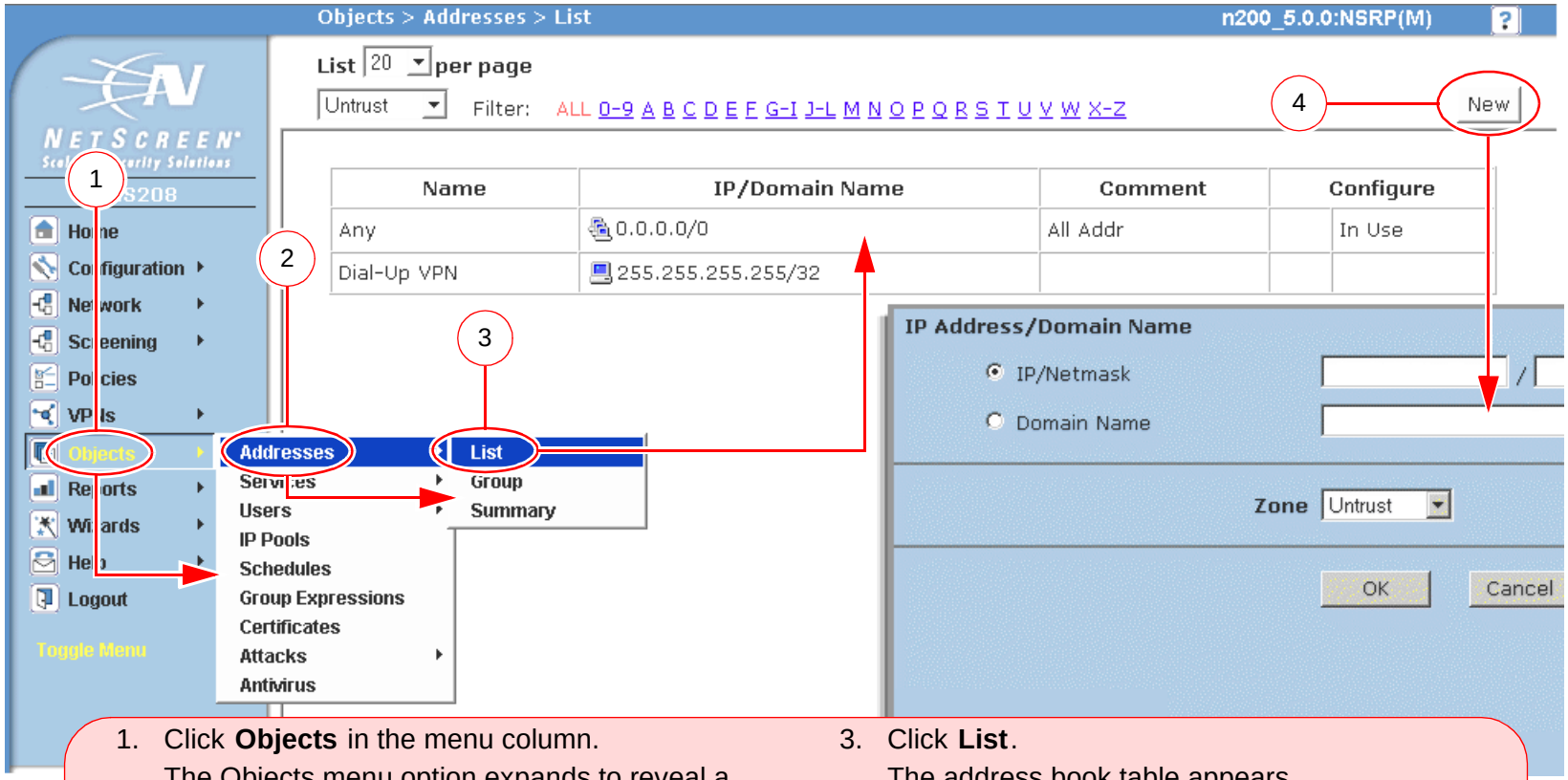
  ```
  set admin user name password
  ```

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: "Use the **get system** command to display the serial number of a NetScreen device."

Note: *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

WebUI Conventions

Throughout this book, a chevron (>) is used to indicate navigation through the WebUI by clicking menu options and links. For example, the path to the address configuration dialog box is presented as **Objects > Addresses > List > New**. This navigational sequence is shown below.



1. Click **Objects** in the menu column.
   The Objects menu option expands to reveal a subset of options for Objects.
2. (Applet menu) Hover the mouse over **Addresses**.
   (DHTML menu) Click **Addresses**.
   The Addresses option expands to reveal a subset of options for Addresses.
3. Click **List**.
   The address book table appears.
4. Click the **New** link.
   The new address configuration dialog box appears.

To perform a task with the WebUI, you must first navigate to the appropriate dialog box where you can then define objects and set parameters. The set of instructions for each task is divided into two parts: a navigational path and configuration details. For example, the following set of instructions includes the path to the address configuration dialog box and the settings for you to configure:

Objects > Addresses > List > New: Enter the following, and then click **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (select), 10.2.2.5/32

Zone: Untrust

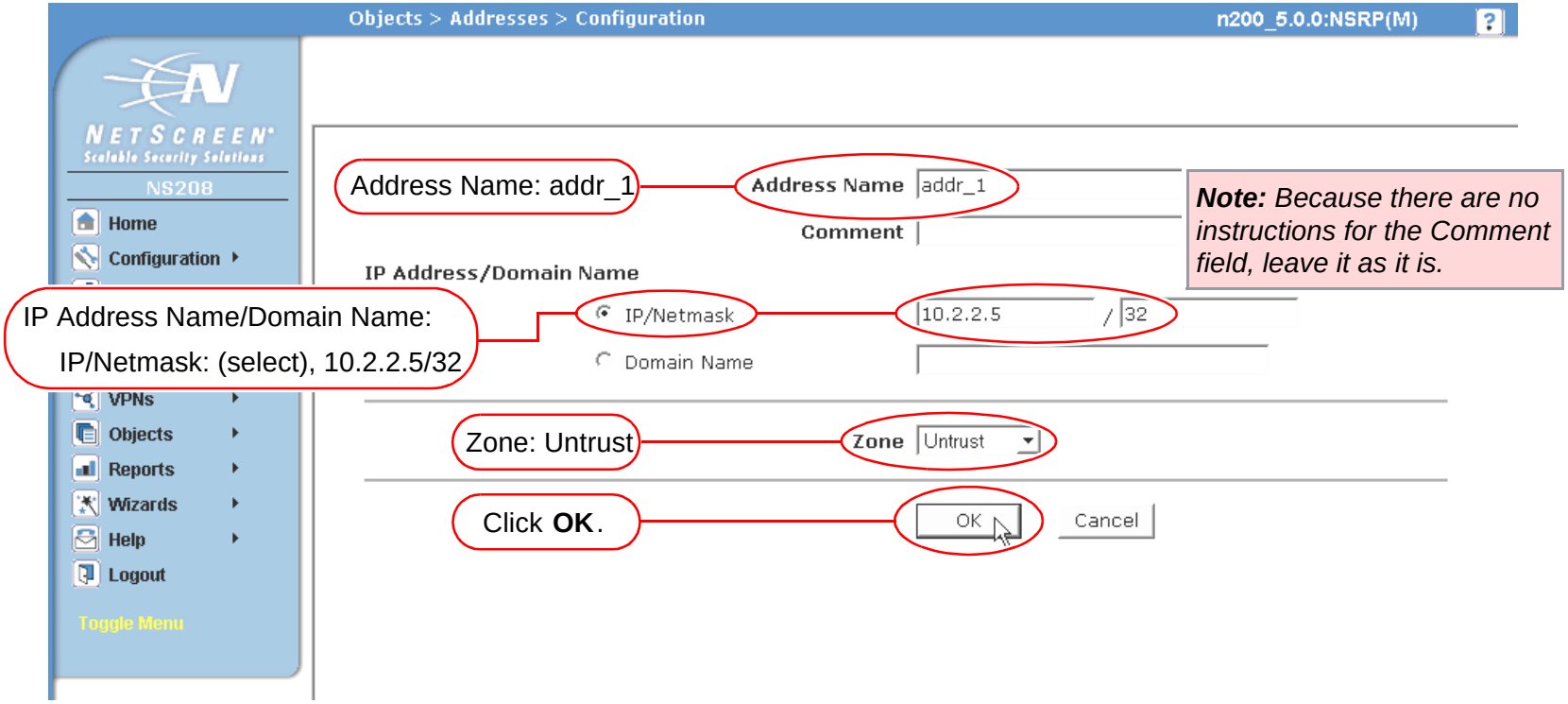


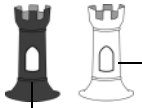
Illustration Conventions

The following graphics make up the basic set of images used in illustrations throughout this book:

Generic NetScreen Device

Virtual Routing Domain

Security Zone



Security Zone Interfaces

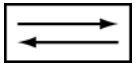
White = Protected Zone Interface (example: Trust Zone)

Black = Outside Zone Interface (example: Untrust Zone)

Tunnel Interface

VPN Tunnel

Router Icon

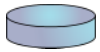


Switch Icon

Local Area Network (LAN) with a Single Subnet

(example: 10.1.1.0/24)

Internet



Dynamic IP (DIP) Pool

Desktop Computer

Laptop Computer

Generic Network Device

(examples: NAT server, Access Concentrator)

Server

Naming Conventions and Character Types

ScreenOS employs the following conventions regarding the names of objects—such as addresses, admin users, auth servers, IKE gateways, virtual systems, VPN tunnels, and zones—defined in ScreenOS configurations.

- If a name string includes one or more spaces, the entire string must be enclosed within double quotes ("); for example, **set address trust "local LAN" 10.1.1.0/24**.
- NetScreen trims any spaces leading or trailing text within a set of double quotes; for example, **" local LAN "** becomes **"local LAN"**.
- NetScreen treats multiple consecutive spaces as a single space.
- Name strings are case sensitive, although many CLI key words are case insensitive. For example, **"local LAN"** is different from **"local lan"**.

ScreenOS supports the following character types:

- Single-byte character sets (SBCS) and multiple-byte character sets (MBCS). Examples of SBCS are ASCII, European, and Hebrew. Examples of MBCS—also referred to as double-byte character sets (DBCS)—are Chinese, Korean, and Japanese.

  Note: *A console connection only supports SBCS. The WebUI supports both SBCS and MBCS, depending on the character sets that your Web browser supports.*

- ASCII characters from 32 (0x20 in hexidecimals) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

NETSCREEN DOCUMENTATION

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download NetScreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

A

Glossary

10BaseT: The most common form of ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024. See also *100BaseT* and *Unshielded Twisted Pair (UTP).*

100BaseT: Another term for fast ethernet, an upgraded standard for connecting computers into a local area network (LAN). 100BaseT ethernet works just like regular ethernet except that it can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than its slower 10BaseT sibling. See also *10BaseT.*

Access List: To restrict the routing information that the router learns or advertises, you can filter based on routing updates to or from a particular neighbor. The filter consists of an access list that is applied to updates to or from a neighbor. The filtering of routing information can be applied on a per-neighbor or per-peer-group basis.

Access-Challenge: An additional condition required for a successful Telnet login by an authentication user via a RADIUS server.

Adjacencies: When two routers can exchange routing information with one another, they are considered to have constructed an adjacency. Point-to-point networks have only two routers so those routers automatically form an adjacency. But 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.

Advertisement: A method a router uses to announce itself to other devices on the network, transmitting basic information including IP address, network mask, and other data.

Aggregate State: A router is in an aggregate state when it is one of multiple virtual BGP routing instances bundled into one address.

Aggregation: The process of combining several different 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: An object used to bundle multiple routes under one common route generalized according to the value of the network mask.

Aggressive Aging: A mechanism to accelerate 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.

Area: The most fundamental ordering method in the OSPF routing protocol. An OSPF area divides the internetwork into smaller, more manageable constituent pieces. This technique reduces the amount of information that each router must store and maintain about all the other routers. When a router in the area needs information about another device in or out of the area, it contacts a special router that stores this information. This router is called the Area Border Router (ABR) and contains all essential device information. In addition, the ABR area border router filters all information coming into the area to avoid bogging down other routers in the area with information they may not need.

Area Range: A sequence of IP addresses defined by a lower limit and upper limit that indicates a series of addresses of devices that exist within an area.

Area Border Router: A router with at least one interface in Area 0 and at least one interface in another area.

AS: See *Autonomous System*.

AS Number: The identification number of the local autonomous system mapped to a BGP routing instance. The ID number can be any valid integer.

AS Path Access List: An access list used by a BGP routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance.

AS Path Attribute Class: The BGP provides four classes of path attributes: Well-Known Discretionary, Optional Transitive, and Optional Non-Transitive.

AS Path String: A string that acts as an identifier for an AS path. It is configured alongside an AS Path access list ID.

Atomic Aggregate: An object used by a BGP router to inform other BGP routers that the local system selected a generalized route.

Attack Objects: Stateful signatures and protocol anomalies that a NetScreen device with Deep Inspection functionality uses to detect attacks aimed at compromising one or more hosts on a network.

Authentication Header (AH): See *ESP/AH*.

Authentication: Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain 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 using digital signatures.

Autonomous System (AS): An AS is a set of routers set off from the rest of the network and governed by a single technical administration. This router group 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 ASs. Each AS has a routing plan that indicates what destinations are reachable through it. This plan is called the Network Layer Reachability Information (NLRI) object. BGP routers generate and receive NLRI updates periodically.

Autonomous System Boundary Router: A router that connects an AS running one routing protocol to another AS running a different protocol.

Autonomous System Path: A list of all the autonomous systems that a router update has traveled through in the current transmission.

BGP: An inter-autonomous system routing protocol. BGP routers and autonomous systems exchange routing information for the Internet.

Bridge: A device that forwards traffic between network segments based on data link layer information. These segments share a common network layer address space.

Broadcast Network: A broadcast network is a network that supports many routers with the capability to communicate directly with one another. Ethernet is an example of a broadcast network.

Circuit-level Proxy: Proxy or Proxy Server is a technique used to cache information on a Web server and acts as an intermediary between a Web client and that Web server. It basically holds the most commonly and recently used content from the World Wide Web for users in order to provide quicker access and to increase server security. This is common for an ISP especially if they have a slow link to the Internet. On the Web, a proxy first attempts to find data locally, and if it is not there, fetches it from the remote server where the data resides permanently. Proxy servers are also constructs that allow direct Internet access from behind a firewall. They open a socket on the

server, and allow communication via that socket to the Internet. For example, if your computer is inside a protected network, and you want to browse the Web using Netscape, you can set up a proxy server on a firewall. You can configure the proxy server to allow HTTP requests to port 80 from your computer, and it then redirects all requests to the proper places.

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.

Cluster: A group of routers in a BGP AS where one is established as a route reflector and the others are clients to the reflector. The reflector is responsible for informing the clients of route and address information it learns from devices in another AS.

Note: *The term "cluster" has another meaning in regards to high availability. See "NetScreen Redundancy Protocol (NSRP)".*

Cluster List: A list of paths recorded as a packet travels through a BGP route reflector cluster.

Community: A community is a grouping of BGP destination. By updating the community, you automatically update its member destinations with new attributes.

Confederation: An object inside a 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.

Data Encryption Standard (DES): A 40- 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 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 Encryption Standard-Cipher Block Chaining (DES-CBC): Until recently, the most significant use of triple-DES (3DES) was for the encryption of single DES keys, and there was really no need to consider how one might implement various block cipher modes when the block cipher in question is actually one derived from multiple encryption. However, as DES nears the end of its useful lifetime, more thought is being given to an increasingly widespread use of triple-DES. In particular, there are two obvious ways to implement the CBC mode for triple-DES. With single-DES in CBC mode, the ciphertext is exclusive-ored with the plaintext before encryption. With triple-DES however, we might use feedback around all three DES operations from the ciphertext to the plaintext, something which is called outer-CBC. Alternatively, we might run the feedback around each individual encryption component, thereby making, in effect, triple-(DES-CBC). This is referred to as inner-CBC, since there are internal feedbacks that are never seen by the crypto-analyst. Performance-wise, there can be some advantages to use the inner-CBC option, but research has established that outer-CBC is in fact more secure. Outer-CBC is the recommended way for using triple-DES in the CBC mode.

De-Militarized 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.

Dead Interval: The amount of time that elapses before a routing instance determines another routing instance is not running.

Distance Vector: A 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.

Dynamic Routing: A 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 send s 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.

Encryption: Encryption is the 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. DES (Data Encryption Standard) and 3DES (Triple DES) are two of the most popular public-key encryption schemes.

ESP/AH: The 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 Authentication Header (AH) protocol provides authentication. The Encapsulating Security Protocol (ESP) provides both authentication and encryption.

Ethernet: A local area network technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network (LAN). The most common form of ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.

External Neighbors: Two BGP routers that are peers that reside in two different autonomous systems.

Extranet: The connecting of two or more intranets. An intranet is an internal Web site that allows users inside a company to communicate and exchange information. An extranet connects that virtual space with the intranet of another company, thus allowing these two (or more) companies to share resources and communicate over the Internet in their own virtual space. This technology greatly enhances business-to-business communications.

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

Filtering, Dynamic: An IP service that can be used within VPN tunnels. Filters are one way some NetScreen devices 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, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. See also *Tunneling* and *Virtual Private Network (VPN).*

Firewall: A 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 in to it. This could be a dedicated computer equipped with security measures or it could be a software-based protection.

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.

GBIC: A Gigabit Interface Connector (GBIC) is the kind of interface module card used on some NetScreen devices for connecting to a fiber optic network.

Hello Interval: The amount of time that elapses between instances of Hello Packets.

Hello Packet: A packet that advertises information, such as its presence and availability, to the network about the router that generated the packet.

Hold Time: In OSPF, the maximum amount of time between instances of initiating Shortest Path First (SPF) computations. In BGP, the maximum amount of time that elapses between message transmissions between a BGP speaker and its neighbor.

Hub: A hub is a hardware device used to link computers together (usually over an ethernet connection). It serves as a common wiring point so that information can flow through a central location to any other computer on the network. A hub repeats signals at the physical ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.

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. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

Internet: Also known as “the Net.” Originally designed by the U.S. Defense Department so that a communication signal could withstand a nuclear war and serve military institutions worldwide. The Internet was first known as the ARPAnet. A system of linked computer networks, international in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, and newsgroups. The Internet is a way of connecting existing computer networks that greatly extends the reach of each participating system.

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

Internet Protocol (IP): An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

IP Address: Each node on a TCP/IP network usually has an IP address. The IP address has a network number portion and a host number portion, as shown in the following table of IP address classes and formats:

Class	Number of Nodes	Address Format
A	> 32,768	nnn.hhh.hhh.hhh
B	256–32,768	nnn.nnn.hhh.hhh
C	< 256	nnn.nnn.nnn.hhh

This format is called decimal-dot format. The “n” represents a digit of a network number and “h” represents a digit of a host number; for example, 128.11.2.30. If you are sending data outside of your network, such as to the Internet, you need to obtain the network number from a central authority, currently the Network Information Center. See also *Netmask* and *Subnet Mask*.

IP 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.

IP Security (IPSec): Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. See also *DES-CBC,* and *ESP/AH.*

ISAKMP: The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of 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: A play on the word Internet, an intranet is a restricted-access network that works like the Web, but isn't on it. Usually owned and managed by a corporation, an intranet enables a company to share its resources with its employees without confidential information being made available to everyone with Internet access.

Keepalive: The amount of time in seconds that elapses between keepalive packets which ensures that the TCP connection between the local BGP router and a neighbor router is up. This value is equal to one-third of the hold time. The default is 60 seconds.

Key Management: The only reasonable way to protect the integrity and privacy of information is to rely upon the use of secret information in the form of private keys for signing and/or encryption. The management and handling of these pieces of secret information is generally referred to as "key management." This includes the activities of selection, exchange, storage, certification, expiration, revocation, changing, and transmission of keys. Most of the work in managing information security systems lies in the key management.

Link State: Link state routing protocols operate using an algorithm commonly called the Shortest Path First (SPF) algorithm. Instead of relying on rumored information from directly connected neighbors as in distance vector protocols, each router in a link state system maintains a complete topology of the network and computes SPF information based on the topology.

Link State Advertisement: The conveyance that enables OSPF routers to make device, network, and routing information available for the link state database. Each router retrieves information from the LSAs sent by other routers on the network to construct a picture of the entire internetwork from which an individual routing instance distills path information to use in its routing table.

Load balancing: Load balancing is the mapping (or re-mapping) of work to two or more processors, with the intent of improving the efficiency of a concurrent computation.

Local Area Network (LAN): Any network technology that interconnects resources within an office environment, usually at high speeds, such as ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 1,640 feet (500 meters) and provide low-cost, high-bandwidth networking capabilities within a small geographical area.

Local Preference: To provide better information than the Multi-Exit Discriminator (MED) value provides for a packet's path selection, BGP provides an attribute known as the LOCAL_PREF or local preference value. You can configure the LOCAL_PREF attribute so that it has a higher value for prefixes received from a router that provides a desired path to be higher than prefixes heard on the router that provides a less desirable path. The higher the value, the more preferred the route. The LOCAL_PREF attribute is the metric most often used in practice to express preferences for one set of paths over another.

Mapped IP Address: A MIP is a direct one-to-one mapping of traffic destined for one IP address to another IP address.

MD5: Message Digest (version) 5, 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.

MED Comparison: The Multi Exit Discriminator (MED) attribute is 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.

Media Access Control (MAC) Address: An address that uniquely identifies the network interface card, 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, it's the same as the ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of 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 sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.

Multi Exit Discriminator: A BGP attribute that determines the relative preference of entry points into an Autonomous System.

Member AS: The name of the autonomous system being included in a BGP confederation.

Neighbor: To begin configuring a BGP network, you need to establish a connection between the current device and a counterpart, adjacent device known as a *neighbor* or *peer*. While this counterpart device may seem like unneeded information at first, it is actually central to the way BGP works. Unlike RIP or OSPF, you now have to configure two devices, both the current router and its neighbor, for BGP to work. While this requires more effort, it enables networking to occur on a larger scale as BGP eludes deploying the limited advertising techniques inherent to interior networking standards.

There are two types of BGP neighbors: **internal neighbors** which are in the same autonomous system and **external neighbors** which are in different autonomous systems. A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or *states* before a true connection can be made. See *Connection States*.

Netmask: A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refers to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refers to a single host. See also *IP Address* and *Subnet Mask.*

NetScreen Redundancy Protocol (NSRP): A proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for NetScreen units in a high availability (HA) cluster.

Network Address Translation (NAT): A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network.

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

Peer: See *Neighbor*

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.

Prefix: An IP address that represents a route.

Redistribution: The 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: A list of routes the current routing domain imported from another routing domain using a different protocol.

RJ-45: Resembling a standard phone 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 phones with multiple lines.

Route Flap Damping: BGP provides a technique to block the advertisement of the route somewhere close to the source until the route becomes stable. This method is called *flap damping*. Route flap damping allows routing instability to be contained at an AS border router adjacent to the region where instability is occurring. The impact of limiting the unnecessary propagation is to maintain reasonable route change convergence time as a routing topology grows.

Route Map: Route maps are used with 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 and 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: The exporting of route rules from one virtual router to another.

Route Reflector: A router whose BGP configuration enables readvertising of routes between Interior BGP (IBGP) neighbors or neighbors within the same BGP 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.

Router: A hardware or virtual (in a NetScreen environment) device that distributes data to all other routers and receiving points in or outside of the local routing domain. Routers also act as filters, allowing only authorized devices to transmit data into the local network so that private information can remain secure. In addition to supporting these connections, routers also handle errors, keep network usage statistics, and handle security issues.

Routing Table: A 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.

Run Time Object (RTO): A 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).

Security Association: An SA is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. For bidirectional communication, 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.*

Security Parameters Index: (SPI) is a hexadecimal value which uniquely identifies each tunnel. It also tells the NetScreen device which key to use to decrypt packets.

Security Zone: A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic via policies.

SHA-1: Secure Hash Algorithm-1, an 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.)

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.

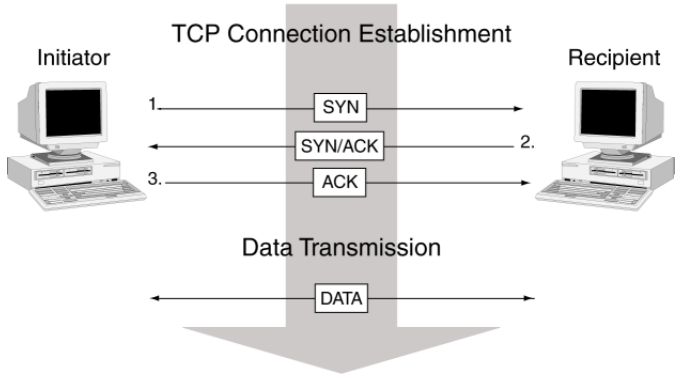
The software remembers static routes until you remove them. However, you can override static routes with dynamic routing information through judicious assignment of administrative distance values. To do this, you must ensure that the administrative distance of the static route is higher than that of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

Subinterface: A subinterface is a 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.

Subnet Mask: In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network ID, while the third portion is a subnet ID. The fourth portion is the host ID. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. See also *IP address* and *Netmask.*

Three-Way Handshake: A TCP connection is established with a triple exchange of packets known as a three-way handshake. The procedure transpires as follows:

1. The initiator sends a SYN (synchronize/start) packet.
2. The recipient replies with a SYN/ACK (synchronize/acknowledge) packet.
3. The initiator responds with an ACK (acknowledge) packet.
4. At this point, the two endpoints of the connection have been established and data transmission can commence.



Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP is a set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks. (A communication protocol is a set of rules that allow computers with different operating systems to communicate with each other.) TCP/IP controls how data is transferred between computers on the Internet.

Trunk Port: A trunk port allows a switch to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.

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

Tunneling: A method of data encapsulation.With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider 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 Internet Service Provider 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 Internet Service Provider'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 can access only the hosts that they are authorized to use.

Tunnel Interface: A tunnel interfaces is the 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: A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

User Datagram Protocol (UDP): A protocol in the TCP/IP protocol suite, the User Datagram Protocol or UDP allows an application program to send datagrams to other application programs on a remote machine. Basically UDP is a protocol that 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.

Uniform Resource Locator (URL): A standard way developed to specify the location of a resource available electronically. Also referred to as a location or address, URLs specify the location of files on servers. A general URL has the syntax protocol://address. For example, http://www.netscreen.com/support/manuals.html specifies that the protocol is HTTP and the address is www.netscreen.com/support/manuals.html.

Unshielded Twisted Pair (UTP): Also known as 10BaseT. This is the standard cabling used for telephone lines. It is also used for ethernet connections. See also *10BaseT.*

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

Virtual Adapter: The TCP/IP settings (IP address, DNS server addresses, and WINS server addresses) that a NetScreen device assigns to a remote XAuth user for use in a VPN connection.

Virtual IP 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 Local Area Network (VLAN): A logical rather than physical grouping of devices that constitute 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): A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPSec.

Virtual Router: A virtual router is the component of ScreenOS that performs routing functions. By default, a NetScreen device supports two virtual routers: Untrust-VR and Trust-VR.

Virtual Security Device (VSD): A single logical device composed by a set of physical NetScreen devices.

Virtual Security Interface (VSI): A logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a 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: A virtual system (vsys) is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same NetScreen device. Each one can be managed by its own virtual system administrator.

Windows Internet Naming Service (WINS): WINS is a service for mapping 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.

Zone: A zone can be a 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 logical entity that performs a specific function (a function zone).

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z