

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

Contents	i
Preface	xxi
Concepts & Examples Organization.....	xxiii
Conventions	xxvii
CLI Conventions.....	xxvii
WebUI Conventions.....	xxviii

Illustration Conventions	xxx
Naming Conventions and Character Types.....	xxxii
NetScreen Documentation	xxxii
Appendix A Glossary	A-I
Index.....	IX-I

Volume 2: Fundamentals

Contents	i
Preface	ix
Conventions	x
CLI Conventions.....	x
WebUI Conventions.....	xi
Illustration Conventions.....	xiii
Naming Conventions and Character Types	xiv
NetScreen Documentation	xv
Chapter 1 ScreenOS Architecture.....	1
Security Zones	2
Security Zone Interfaces	3
Physical Interfaces	3
Subinterfaces	4
Virtual Routers	5

Policies	6
VPNs.....	8
Virtual Systems	10
Packet Flow Sequence	11
Example (Part 1): Enterprise with Six Zones	14
Example (Part 2): Interfaces for Six Zones	16
Example (Part 3): Enterprise with Two Routing Domains.....	20
Example (Part 4): Policies for an Enterprise with Six Zones	22
Chapter 2 Routing Tables and Static Routing	29
Routing Essentials	30
Routing Methods	30
Static Routing	30
Dynamic Routing	30
Routing Tables.....	31

Routing with Static Routes	33	Chapter 4 Interfaces	65
Virtual Routers on NetScreen Devices.....	35	Interface Types	66
When to Configure Static Routes	36	Security Zone Interfaces	66
Configuring Static Routes	38	Physical	66
Example: Configuring Static Routes	39	Subinterface	66
Example: Static Route through		Aggregate Interfaces.....	67
a Tunnel Interface	43	Redundant Interfaces	67
Chapter 3 Zones	45	Virtual Security Interfaces.....	68
Security Zones	48	Function Zone Interfaces.....	68
Global Zone.....	48	Management Interface	68
SCREEN Options	48	HA Interface	69
Tunnel Zones.....	49	Tunnel Interfaces	69
Example: Binding a Tunnel Interface		Deleting Tunnel Interfaces	72
to a Tunnel Zone.....	50	Example: Deleting a Tunnel Interface.....	72
Configuring Security Zones and Tunnel Zones.....	51	Viewing Interfaces	74
Creating a Zone	51	Interface Table.....	74
Modifying a Zone	52	Configuring Security Zone Interfaces	76
Deleting a Zone	53	Binding an Interface to a Security Zone	76
Function Zones	54	Example: Binding an Interface	76
Null Zone.....	54	Defining an Address for a L3 Security	
MGT Zone	54	Zone Interface.....	77
HA Zone	54	Public IP Addresses	77
Self Zone	54	Private IP Addresses	78
VLAN Zone.....	54	Example: Addressing an Interface.....	79
Port Modes	55	Unbinding an Interface from a Security Zone	80
Setting the Port Mode on NetScreen Appliances.....	59	Example: Unbinding an Interface	80
Example: Setting Home-Work Port Mode	60	Modifying Interfaces	81
Home Zone/Work Zone	61	Example: Modifying Settings	
Example: Configuring Home		on an Interface.....	81
and Work Zones.....	63	Creating Subinterfaces	82
		Example: Creating a Subinterface	
		in the Root System.....	82

Deleting Subinterfaces.....	83	Route Mode.....	118
Example: Deleting a Security Zone Interface	83	Interface Settings	119
Secondary IP Addresses	84	Example: Route Mode	120
Secondary IP Address Properties.....	84	Chapter 6 Building Blocks for Policies	125
Example: Creating a Secondary IP Address.....	85	Addresses	126
Loopback Interfaces	86	Address Entries.....	127
Example: Creating a Loopback Interface.....	86	Example: Adding Addresses	127
Using Loopback Interfaces	87	Example: Modifying Addresses	128
Example: Using the Loopback Interface		Example: Deleting Addresses.....	129
to Manage a Device	87	Address Groups	129
Example: Enabling BGP		Example: Creating an Address Group	131
on a Loopback Interface	88	Example: Editing a Group Address Entry	132
Example: Configuring NSRP VSIs		Example: Removing an Address Group	
on a Loopback Interface	88	Member and a Group	133
Example: Specifying a Loopback		Services	134
Interface as a Source Interface.....	89	Predefined Services.....	134
Chapter 5 Interface Modes	91	Example: Setting a Predefined	
Transparent Mode	92	Service Timeout.....	136
Zone Settings	93	Custom Services	136
VLAN Zone	93	Example: Adding a Custom Service	136
Predefined Layer 2 Zones.....	93	Example: Modifying a Custom Service	138
Traffic Forwarding	94	Example: Removing a Custom Service	138
Unknown Unicast Options.....	95	ICMP Services	139
Flood Method.....	96	Example: Defining an ICMP Service.....	140
ARP/Trace-Route Method.....	98	RSH ALG	140
Example: VLAN1 Interface for Management	102	H.323 Protocol for Voice-over-IP.....	141
Example: Transparent Mode	105	Example: Gatekeeper in the Trust Zone	
NAT Mode	110	(Transparent or Route Mode)	141
Inbound and Outbound NAT Traffic	112	Example: Gatekeeper in the Trust Zone	
Interface Settings	113	(NAT Mode)	143
Example: NAT Mode	114	Example: Gatekeeper in the Untrust Zone	
		(Transparent or Route Mode)	148

Example: Gatekeeper in the Untrust Zone (NAT Mode)	151	Three Types of Policies	200
SIP – Session Initiation Protocol	156	Interzone Policies	200
SIP Request Methods	157	Intrazone Policies	201
Classes of SIP Responses	157	Global Policies	201
ALG – Application-Layer Gateway	159	Policy Set Lists	202
SDP	160	Policies Defined	203
Pinhole Creation	161	Policies and Rules	203
Session Inactivity Timeout	163	Anatomy of a Policy	205
Example: Creating a Policy to Permit SIP	164	ID	206
Example: Signaling and Media Inactivity Timeouts	166	Zones	206
Service Groups	167	Addresses	206
Example: Creating a Service Group	168	Services	206
Example: Modifying a Service Group	169	Action	207
Example: Removing a Service Group	170	Application	207
DIP Pools	171	Name	208
Port Address Translation	172	VPN Tunneling	208
Example: Creating a DIP Pool with PAT	172	L2TP Tunneling	209
Example: Modifying a DIP Pool	174	Deep Inspection	209
Sticky DIP Addresses	174	Placement at the Top of the Policy List	209
Extended Interface and DIP	175	Source Address Translation	210
Example: Using DIP in a Different Subnet	175	Destination Address Translation	210
Loopback Interface and DIP	183	User Authentication	210
Example: DIP on a Loopback Interface	184	HA Session Backup	212
DIP Groups	189	URL Filtering	213
Example: DIP Group	191	Logging	213
Schedules	193	Counting	213
Example: Recurring Schedule	193	Traffic Alarm Threshold	213
Chapter 7 Policies	197	Schedules	214
Basic Elements	199	Antivirus Scanning	214
		Traffic Shaping	215
		Policies Applied	216
		Viewing Policies	216

Policy Icons	216	Routing for Destination Translation	282
Creating Policies	217	Addresses Connected to	
Policy Location	218	the Same Interface	283
Example: Interzone Policies for E-Mail		Addresses Connected to the Same	
Service	218	Interface but Separated by a Router	284
Example: Interzone Policy Set	223	Addresses Separated by an Interface	285
Example: Intrazone Policies	231	NAT-Dst: One-to-One Mapping	286
Example: Global Policy	234	Example: One-to-One Destination	
Entering a Policy Context	235	Translation	287
Multiple Items per Policy Component	236	Translating from One Address	
Address Negation	237	to Multiple Addresses	291
Example: Destination Address Negation	237	Example: One-to-Many Destination	
Modifying and Disabling Policies	241	Translation	291
Policy Verification	242	NAT-Dst: Many-to-One Mapping	295
Reordering Policies	243	Example: Many-to-One Destination	
Removing a Policy	244	Translation	295
Chapter 8 Address Translation	245	NAT-Dst: Many-to-Many Mapping	300
Introduction to Address Translation	246	Example: Many-to-Many Destination	
Policy-Based Translation Options	253	Translation	301
Directional Nature of NAT-Src and NAT-Dst	257	NAT-Dst with Port Mapping	305
Source Network Address Translation	259	Example: NAT-Dst with Port Mapping	305
NAT-Src from a DIP Pool with PAT Enabled	260	NAT-Src and NAT-Dst in the Same Policy	310
Example: NAT-Src with PAT Enabled	261	Example: NAT-Src and NAT-Dst Combined	310
NAT-Src from a DIP Pool with PAT Disabled	264	Mapped IP Addresses	331
Example: NAT-Src with PAT Disabled	264	MIP and the Global Zone	332
NAT-Src from a DIP Pool with Address Shifting	267	Example: Adding a MIP to	
Example: NAT-Src with Address Shifting	268	an Untrust Zone Interface	333
NAT-Src from the Egress Interface IP Address	273	Example: Reaching a MIP	
Example: NAT-Src without DIP	273	from Different Zones	336
Destination Network Address Translation	276	Example: Adding a MIP	
Packet Flow for Destination Translation	278	to a Tunnel Interface	341
		MIP-Same-as-Untrust	342
		Example: MIP on the Untrust Interface	343
		MIP and the Loopback Interface	346

Example: MIP for Two Tunnel Interfaces	347
Virtual IP Addresses	356
VIP and the Global Zone.....	359
Example: Configuring Virtual IP Servers	359
Example: Editing a VIP Configuration	362
Example: Removing a VIP Configuration.....	362
Example: VIP with Custom and Multiple-Port Services	363
Chapter 9 User Authentication.....	371
Authentication Servers	372
Local Database.....	374
Supported User Types and Features	374
Example: Setting the Local Database Timeout	375
External Auth Servers.....	376
Auth Server Object Properties	377
Auth Server Types	379
RADIUS	379
RADIUS Auth Server Object Properties	380
Supported User Types and Features	380
NetScreen Dictionary File	381
RADIUS Access-Challenge	382
SecurID	384
SecurID Auth Server Object Properties	385
Supported User Types and Features	385
LDAP	386
LDAP Auth Server Object Properties	387
Supported User Types and Features	387
Defining Auth Server Objects	388
Example: Defining an Auth Server Object for RADIUS	388
Example: Defining an Auth Server Object for SecurID	391
Example: Defining an Auth Server Object for LDAP	393
Defining Default Auth Servers	395
Example: Changing the Default Auth Servers.....	395
Authentication Types and Applications	397
Auth Users and User Groups.....	398
Referencing Auth Users in Policies	398
Referencing Auth User Groups in Policies.....	402
Example: Run-Time Authentication (Local User).....	403
Example: Run-Time Authentication (Local User Group)	406
Example: Run-Time Authentication (External User).....	409
Example: Run-Time Authentication (External User Group).....	412
Example: Local Auth User in Multiple Groups.....	416
Example: WebAuth (Local User Group)	420
Example: WebAuth (External User Group).....	423
Example: WebAuth + SSL (External User Group).....	427
IKE Users and User Groups	431
Example: Defining IKE Users	432
Example: Creating an IKE User Group.....	434
Referencing IKE Users in Gateways	435
XAuth Users and User Groups.....	436
XAuth Users in IKE Negotiations.....	437
Example: XAuth Authentication (Local User).....	440

Example: XAuth Authentication (Local User Group)	442	DNS Lookup	496
Example: XAuth Authentication (External User)	444	DNS Status Table	497
Example: XAuth Authentication (External User Group)	447	Example: Defining DNS Server Addresses and Scheduling Lookups	498
Example: XAuth Authentication and Address Assignments (Local User Group)	452	Example: Setting a DNS Refresh Interval	499
XAuth Client	458	DHCP	500
Example: NetScreen Device as an XAuth Client	459	DHCP Server	502
L2TP Users and User Groups	460	Example: NetScreen Device as DHCP Server	502
Example: Local and External L2TP Auth Servers	461	DHCP Server in an NSRP Cluster	508
Admin Users	465	DHCP Server Detection	508
Multiple-Type Users	467	Example: Turning on DHCP Server Detection	509
Group Expressions	468	Example: Turning off DHCP Server Detection	509
Example: Group Expressions (AND)	470	DHCP Relay Agent	510
Example: Group Expressions (OR)	472	Example: NetScreen Device as DHCP Relay Agent	511
Example: Group Expressions (NOT)	474	DHCP Client	516
Banner Customization	476	Example: NetScreen Device as DHCP Client	516
Example: Customizing the WebAuth Success Message	476	TCP/IP Settings Propagation	518
Chapter 10 Traffic Shaping	477	Example: Forwarding TCP/IP Settings	519
Applying Traffic Shaping	478	PPPoE	521
Managing Bandwidth at the Policy Level	478	Example: Setting Up PPPoE	521
Example: Traffic Shaping	479	Example: Configuring PPPoE on Primary and Backup Untrust Interfaces	526
Setting Service Priorities	485	Downloading/Uploading Settings and Software	528
Example: Priority Queuing	486	Saving and Importing Settings	528
Chapter 11 System Parameters	493	Uploading and Downloading Software	530
Domain Name System Support	495	Configuration Rollback	531
		Last-Known-Good Configuration	531

Automatic and Manual Configuration	
Rollback	531
Loading a New Configuration File	533
Locking the Configuration File	534
Adding Comments to a Configuration File	535
License Keys	536
Example: Expanding User Capacity	537
Registration and Activation	
of Signature Services	538
Temporary Service	538
AV and DI Bundled with a New Device	538
AV Upgrade with DI	539

DI Upgrade Only	540
System Clock	541
Date and Time	541
Time Zone	541
NTP	542
Multiple NTP Servers	542
Maximum Time Adjustment	542
NTP and NSRP	543
Example: Configuring NTP Servers	
and a Maximum Time Adjustment Value	544
Secure NTP Servers	545
Index	IX-I

Volume 3: Administration

Contents	i
Preface	v
Conventions	vi
CLI Conventions	vi
WebUI Conventions	vii
Illustration Conventions	ix
Naming Conventions and Character Types	x
NetScreen Documentation	xi
Chapter 1 Administration	1
Management via the Web User Interface	3
WebUI Help	4
Copying the Help Files to a Local Drive	4
Pointing the WebUI to the New Help Location	4
HTTP	5
Session ID	5

Secure Sockets Layer	7
Management via the Command Line Interface	9
Telnet	9
Securing Telnet Connections	10
Secure Shell	11
Client Requirements	13
Basic SSH Configuration on	
the NetScreen Device	13
Authentication	15
SSH and Vsys	17
Host Key	18
Example: SSHv1 with PKA	
for Automated Logins	19
Secure Copy (SCP)	20
Serial Console	21
Modem Port	22
Management via NetScreen-Security Manager	23

Initiating Connectivity Between Agent and Management System	24
Enabling and Disabling the Agent.....	25
Example: Enabling the Security Manager Agent	25
Changing Management System Server Address	26
Example: Setting the Primary Server IP Address	26
Setting Report Parameters	26
Example: Enabling Alarm and Statistics Reporting	27
Controlling Administrative Traffic	29
MGT and VLAN1 Interfaces	30
Example: Administration through the MGT Interface.....	30
Example: Administration through the VLAN1 Interface	31
Administrative Interface	32
Example: Setting Administrative Interface Options.....	32
Manage IP	34
Example: Setting Manage IPs for Multiple Interfaces.....	34
Levels of Administration	37
Root Administrator	37
Read/Write Administrator	38
Read-Only Administrator.....	38
Virtual System Administrator	38
Virtual System Read-Only Administrator	39
Defining Admin Users	39
Example: Adding a Read-Only Admin	39
Example: Modifying an Admin	40
Example: Deleting an Admin.....	40
Example: Clearing an Admin's Sessions	41
Securing Administrative Traffic	42
Changing the Port Number	43
Example: Changing the Port Number	43
Changing the Admin Login Name and Password	44
Example: Changing an Admin User's Login Name and Password	45
Example: Changing One's Own Password	46
Setting the Minimum Length of the Root Admin Password.....	47
Resetting the Device to the Factory Default Settings	48
Restricting Administrative Access	49
Example: Restricting Administration to a Single Workstation.....	49
Example: Restricting Administration to a Subnet	50
Restricting the Root Admin to Console Access.....	50
VPN Tunnels for Administrative Traffic	51
Example: Administration through a Route-Based Manual Key VPN Tunnel	52
Example: Administration through a Policy-Based Manual Key VPN Tunnel	58
Chapter 2 Monitoring NetScreen Devices	65
Storing Log Information.....	66
Event Log	67
Viewing the Event Log	68
Example: Viewing the Event Log by Severity Level and Keyword	69
Sorting and Filtering the Event Log	70
Example: Sorting Event Log Entries by IP Address.....	70
Downloading the Event Log	71

Example: Downloading the Event Log.....	71
Example: Downloading the Event Log for Critical Events	71
Traffic Log	72
Viewing the Traffic Log	74
Example: Viewing Traffic Log Entries	74
Sorting and Filtering the Traffic Log	75
Example: Sorting the Traffic Log by Time	75
Downloading the Traffic Log	76
Example: Downloading a Traffic Log.....	76
Self Log	77
Viewing the Self Log	77
Sorting and Filtering the Self Log	78
Example: Filtering the Self Log by Time	79
Downloading the Self Log.....	80
Example: Downloading the Self Log.....	80
Asset Recovery Log	81
Example: Downloading the Asset Recovery Log	81
Traffic Alarms	82
Example: Policy-Based Intrusion Detection.....	83

Example: Compromised System Notification	84
Example: Sending E-mail Alerts	86
Syslog	87
Example: Enabling Multiple Syslog Servers	88
WebTrends	89
Example: Enabling Syslog and WebTrends for Notification Events	89
SNMP	91
Implementation Overview	94
Example: Defining a Read/Write SNMP Community.....	95
VPN Tunnels for Self-Initiated Traffic	97
Example: Self-Generated Traffic through a Route-Based Tunnel	99
Example: Self-Generated Traffic through a Policy-Based Tunnel	109
Counters	120
Example: Viewing Screen Counters	126
Appendix A SNMP MIB Files	A-I
Index.....	IX-I

Volume 4: Attack Detection and Defense Mechanisms

Contents	i
Preface	v
Conventions	vi
CLI Conventions.....	vi
WebUI Conventions.....	vii
Illustration Conventions.....	ix

Naming Conventions and Character Types.....	x
NetScreen Documentation	xi
Chapter 1 Protecting a Network	1
Stages of an Attack	2
Detection and Defense Mechanisms	3
Exploit Monitoring	5

Example: Monitoring Attacks from the Untrust Zone	6	ICMP Flood	59
Chapter 2 Reconnaissance Deterrence	7	UDP Flood	61
IP Address Sweep	8	Land Attack	63
Port Scanning	10	OS-Specific DoS Attacks	65
Network Reconnaissance Using IP Options	12	Ping of Death	65
Operating System Probes	16	Teardrop Attack	67
SYN and FIN Flags Set	16	WinNuke	69
FIN Flag without ACK Flag	18	Chapter 4 Content Monitoring and Filtering	71
TCP Header without Flags Set	20	Fragment Reassembly	72
Evasion Techniques	22	Malicious URL Protection	72
FIN Scan	22	Application Layer Gateway	73
IP Spoofing	22	Example: Blocking Malicious URLs in Packet Fragments	74
Example: L3 IP Spoof Protection	25	Antivirus Scanning	76
Example: L2 IP Spoof Protection	29	Internal AV Scanning	77
IP Source Route Options	31	Enabling Internal AV Scanning	81
Chapter 3 Denial-of-Service Attack Defenses	35	Updating the Pattern File Automatically or Semi-Automatically	82
Firewall DoS Attacks	36	Example: Automatic Pattern Update	83
Session Table Flood	36	Example: Semi-Automatic Pattern Update	83
Source- and Destination-Based Session Limits	36	Configuring Content Processing	84
Example: Source-Based Session Limiting	39	Example: Internal AV Scanning for SMTP	84
Example: Destination-Based Session Limiting	40	Example: Internal AV Scanning for SMTP and HTTP	85
Aggressive Aging	40	Configuring Decompression and Maximum Content Size	85
Example: Aggressively Aging Out Sessions	42	Example: Dropping Large Files	86
SYN-ACK-ACK Proxy Flood	43	Applying Internal AV Scanning	87
Network DoS Attacks	45	Example: Internal AV Scanning (POP3)	87
SYN Flood	45	External AV Scanning	90
Example: SYN Flood Protection	52	Defining AV Objects	93
		Example: Defining Three AV Objects	99

Applying External AV Scanning	102
Example: Antivirus with One AV Object	103
Example: Antivirus with Two AV Objects	106
URL Filtering	113
Example: URL Filtering Configuration	119
Chapter 5 Deep Inspection	123
Deep Inspection Overview	124
Attack Object Database Server	128
Example: Immediate Update	129
Example: Automatic Updates	130
Example: Automatic Notification and Immediate Update	132
Example: Manual Update	134
Attack Objects and Groups	136
Stateful Signatures	138
TCP Stream Signatures	139
Protocol Anomalies	139
Attack Object Groups	140
Changing Severity Levels	140
Attack Actions	142
Example: Attack Actions – Close Server, Close, Close Client	143
Mapping Custom Services to Applications	152
Example: Mapping an Application to a Custom Service	153

Customized Attack Objects and Groups	156
User-Defined Stateful Signature Attack Objects	156
Contexts	156
Signatures	157
Example: User-Defined Stateful Signature Attack Objects	160
TCP Stream Signature Attack Objects	164
Example: User-Defined Stream Signature Attack Object	164
Granular Blocking of HTTP Components	167
ActiveX Controls	167
Java Applets	168
EXE Files	168
ZIP Files	168
Example: Blocking Java Applets and .exe Files	169
Chapter 1 Suspicious Packet Attributes	1
ICMP Fragments	2
Large ICMP Packets	4
Bad IP Options	6
Unknown Protocols	8
IP Packet Fragments	10
SYN Fragments	12
Index	IX--I

Volume 5: VPNs

Contents	i
Preface	v

Conventions	vi
CLI Conventions	vi
WebUI Conventions	vii

Illustration Conventions	ix
Naming Conventions and Character Types	x
NetScreen Documentation	xi
Chapter 1 IPsec	1
Introduction to VPNs	2
IPsec Concepts	3
Modes.....	4
Transport Mode	4
Tunnel Mode	5
Protocols	7
AH	7
ESP	8
Key Management.....	9
Manual Key	9
AutoKey IKE.....	9
Security Association	10
Tunnel Negotiation	11
Phase 1	11
Main Mode and Aggressive Mode	12
The Diffie-Hellman Exchange	13
Phase 2	13
Perfect Forward Secrecy	14
Replay Protection	14
Chapter 2 Public Key Cryptography.....	15
Introduction to Public Key Cryptography	16
PKI.....	18
Certificates and CRLs	21
Obtaining a Certificate Manually	22
Example: Requesting a Certificate Manually	23
Example: Loading Certificates and CRLs	26
Example: Configuring CRL Settings for a CA Certificate	28
Obtaining a Local Certificate Automatically.....	30
Example: Requesting a Local Certificate Automatically	31
Automatic Certificate Renewal	34
Key Pair Generation	35
Checking for Revocation Using OCSP	36
Configuring for OCSP	37
Specifying either CRL or OCSP for Revocation Checking	37
Displaying Certificate Revocation Status Attributes	37
Specifying the URL of an OCSP Responder for a Certificate	38
Removing Certificate Revocation Check Attributes.....	38
Chapter 3 VPN Guidelines	39
Cryptographic Options.....	40
Site-to-Site Cryptographic Options	41
Dialup VPN Options	50
Route- and Policy-Based Tunnels.....	58
Packet Flow: Site-to-Site VPN	60
Tunnel Configuration Tips	67
Chapter 4 Site-to-Site VPNs	69
Site-to-Site VPN Configurations	70
Site-to-Site Tunnel Configuration Steps	71
Example: Route-Based Site-to-Site VPN, AutoKey IKE	77
Example: Policy-Based Site-to-Site VPN, AutoKey IKE	91

Example: Route-Based Site-to-Site VPN, Dynamic Peer	102	Group IKE ID with Preshared Keys	250
Example: Policy-Based Site-to-Site VPN, Dynamic Peer	117	Example: Group IKE ID (Preshared Keys)	252
Example: Route-Based Site-to-Site VPN, Manual Key	131	Shared IKE IDs	259
Example: Policy-Based Site-to-Site VPN, Manual Key	142	Example: Shared IKE ID (Preshared Keys)	260
FQDN for Dynamic IKE Gateways	151	Chapter 6 L2TP	269
Aliases	152	Introduction to L2TP	270
Example: AutoKey IKE Peer with FQDN	153	Packet Encapsulation and Decapsulation	274
VPN Sites with Overlapping Addresses	168	Encapsulation	274
Example: Tunnel Interface with NAT-Src and NAT-Dst	171	Decapsulation	275
Transparent Mode VPN	186	L2TP Parameters	276
Example: Transparent Mode, Policy-Based AutoKey IKE VPN	187	Example: Configuring an IP Pool and L2TP Default Settings	277
Chapter 5 Dialup VPNs	199	L2TP and L2TP-over-IPSec	279
Dialup VPNs	200	Example: Configuring L2TP	280
Example: Policy-Based Dialup VPN, AutoKey IKE	201	Example: Configuring L2TP-over-IPSec	286
Example: Route-Based Dialup VPN, Dynamic Peer	209	Chapter 7 Advanced VPN Features	299
Example: Policy-Based Dialup VPN, Dynamic Peer	220	IPSec NAT Traversal	301
Bidirectional Policies for Dialup VPN Users	229	Traversing a NAT Device	302
Example: Bidirectional Dialup VPN Policies	230	UDP Checksum	303
Group IKE ID	237	The Keepalive Frequency Value	303
Group IKE ID with Certificates	238	IPSec NAT-Traversal and Initiator/Responder Symmetry	304
Wildcard and Container ASN1-DN IKE ID Types	240	Example: Enabling NAT-Traversal	305
Example: Group IKE ID (Certificates)	243	VPN Monitoring	307
		Rekey and Optimization Options	307
		Source Interface and Destination Address	308
		Policy Considerations	310
		Configuring the VPN Monitoring Feature	310
		Example: Specifying Source and Destination Addresses for VPN Monitoring	312

Security Consideration for a Route-Based VPN Design	323
SNMP VPN Monitoring Objects and Traps.....	325
Multiple Tunnels per Tunnel Interface	326
Route-to-Tunnel Mapping	327
Remote Peers' Addresses	328
Manual and Automatic Table Entries	330
Manual Table Entries	330
Automatic Table Entries	331
Example: Multiple VPNs on One Tunnel Interface to Overlapping Subnets	333
Example: Automatic Route and NHTB Table Entries	364

Redundant VPN Gateways	382
VPN Groups	383
Monitoring Mechanisms	384
IKE Heartbeats.....	384
IKE Recovery Procedure.....	385
TCP SYN-Flag Checking.....	388
Example: Redundant VPN Gateways	389
Back-to-Back VPNs.....	401
Example: Back-to-Back VPNs	402
Hub-and-Spoke VPNs.....	412
Example: Hub-and-Spoke VPNs	413
Index.....	IX-I

Volume 6: Dynamic Routing

Contents	i
Preface	v
Conventions	vi
CLI Conventions.....	vi
WebUI Conventions.....	vii
Illustration Conventions.....	ix
Naming Conventions and Character Types	x
NetScreen Documentation	xi
Chapter 1 Virtual Routers	1
Virtual Routers on NetScreen Devices.....	3
Using Two VRs.....	3
Forwarding Traffic between VRs.....	4
Configuring Two Virtual Routers.....	4
Example: Binding a Zone to the untrust-vr	5

Custom Virtual Routers.....	7
Example: Creating a Custom Virtual Router.....	7
Example: Removing a Custom Virtual Router.....	8
Virtual Routers and Virtual Systems	9
Example: Creating a Custom Virtual Router in a vsys.....	10
Example: Defining a Route with a Shared Virtual Router as the Next-Hop.....	11
Modifying Virtual Routers	12
Virtual Router ID.....	12
Example: Assigning a Virtual Router ID.....	13
Maximum Number of Routing Table Entries.....	14
Example: Limiting the Maximum Number of Routing Table Entries.....	14
Route Selection	15
Route Preference	15

Example: Setting a Route Preference	16	Assigning Interfaces to an OSPF Area	42
Route Metric	17	Example: Assigning Interfaces to OSPF Areas.....	42
Source-Based Routing	17	Example: Configuring an Area Range.....	43
Example: Source-Based Routing	19	Enabling OSPF on Interfaces	44
Route Redistribution	21	Example: Enabling OSPF on Interfaces	44
Configuring a Route Map	22	Example: Disabling OSPF on an Interface.....	45
Route Filtering	24	Verifying the Configuration	46
Access Lists	24	Redistributing Routes	49
Example: Configuring an Access List.....	25	Example: Redistributing a BGP Route	
Example: Redistributing BGP Routes		into OSPF	49
into OSPF	26	Summarizing Redistributed Routes.....	50
Exporting and Importing Routes between VRs.....	28	Example: Summarizing Redistributed Routes.....	50
Example: Configuring a Route Export Rule.....	29	Global OSPF Parameters	51
Chapter 2 Open Shortest Path First (OSPF)	33	Example: Advertising the Default Route	52
Overview of OSPF	34	Virtual Links	53
Areas.....	34	Example: Creating a Virtual Link	54
Router Classification	35	Example: Creating an Automatic Virtual Link.....	56
Hello Protocol.....	35	OSPF Interface Parameters	57
Network Types	36	Example: Setting OSPF Interface Parameters	59
Broadcast Networks	36	Security Configuration	60
Point-to-Point Networks	36	Authenticating Neighbors.....	60
Link State Advertisements.....	37	Example: Configuring the Clear-Text	
Basic OSPF Configuration	38	Password Authentication Method.....	60
Creating an OSPF Routing Instance		Example: Configuring the MD5	
in a Virtual Router.....	39	Password Authentication Method.....	61
Example: Creating an OSPF Routing		Filtering OSPF Neighbors.....	62
Instance	39	Example: Configuring a Neighbor List.....	62
Example: Removing an OSPF Routing		Rejecting Default Routes	63
Instance	40	Example: Removing the Default Route	
Defining an OSPF Area.....	41	from the Route Table.....	63
Example: Creating an OSPF Area.....	41	Protecting against Flooding	64
		Example: Configuring the Hello Threshold	64

Example: Configuring the LSA Threshold	65	Chapter 4 Border Gateway Protocol (BGP)	87
Chapter 3 Routing Information Protocol (RIP)	67	Overview of BGP	88
Overview of RIP	68	Types of BGP Messages	89
Basic RIP Configuration	69	Path Attributes	89
Creating a RIP Routing Instance		External and Internal BGP	90
in a Virtual Router	70	Basic BGP Configuration	91
Example: Creating a RIP Routing		Creating and Enabling a BGP Routing	
Instance	70	Instance in a Virtual Router	92
Example: Removing a RIP Routing		Example: Creating a BGP Routing Instance	92
Instance	71	Example: Removing a BGP Routing	
Enabling RIP on Interfaces	72	Instance	93
Example: Enabling RIP on Interfaces	72	Enabling BGP on Interfaces	94
Example: Disabling RIP on an Interface	73	Example: Enabling BGP on Interfaces	94
Redistributing Routes	73	Example: Disabling BGP on Interfaces	94
Example: Redistributing Routes into RIP	74	Configuring a BGP Peer	95
Global RIP Parameters	76	Example: Configuring a BGP Peer	97
Example: Advertising the Default Route		Example: Configuring an IBGP Peer-Group	98
to RIP Neighbors	77	Verifying the BGP Configuration	100
RIP Interface Parameters	78	Security Configuration	102
Example: Setting RIP Interface Parameters	79	Authenticating Neighbors	102
Security Configuration	80	Example: Configuring MD5	
Authenticating Neighbors	80	Authentication for BGP Peers	102
Example: Configuring the MD5		Rejecting Default Routes	103
Password Authentication Method	81	Example: Rejecting Default Routes	103
Filtering RIP Neighbors	82	Optional BGP Configurations	104
Example: Configuring Trusted Neighbors	82	Redistributing Routes	105
Rejecting Default Routes	83	Example: Redistributing an OSPF	
Example: Rejecting Default Routes	83	Route into BGP	105
Protecting Against Flooding	84	AS-Path Access List	106
Example: Configuring an Update Threshold	84	Example: Configuring an AS-Path	
Example: RIP on Tunnel Interfaces	85	Access List	106
		Route Reflection	107

Example: Configuring the Virtual Router as a Route Reflector	108
Confederations	110
Example: Configuring a Confederation	111

Volume 7: Virtual Systems

Contents	i
Preface	iii
Conventions	iv
CLI Conventions	iv
WebUI Conventions	v
Illustration Conventions	vii
Naming Conventions and Character Types	viii
NetScreen Documentation	ix
Chapter 1 Virtual Systems	1
Creating a Vsys Object	3
Example: Vsys Objects and Admins	3
Virtual Routers	6
Zones	7
Interfaces	8
Traffic Sorting	10
Traffic Destined for the NetScreen Device	10
Through Traffic	11
Dedicated and Shared Interfaces	15
Dedicated Interfaces	15

Volume 8: High Availability

Contents	i
----------------	---

BGP Communities	113
Index	IX-I

Shared Interfaces	15
Importing and Exporting Physical Interfaces	18
Example: Importing a Physical Interface to a Virtual System	18
Example: Exporting a Physical Interface from a Virtual System	19
VLAN-Based Traffic Classification	21
VLANs	22
Defining Subinterfaces and VLAN Tags	23
Example: Defining Three Subinterfaces and VLAN Tags	25
Communicating between Virtual Systems	28
Example: InterVsys Communication	28
IP-Based Traffic Classification	33
Example: Configuring IP-Based Traffic Classification	35
Logging On as a Vsys Admin	38
Example: Logging On and Changing Your Password	38
Index	IX-I

Preface	v
---------------	---

Conventions	vi	Example: Adding a Device to an Active NSRP Cluster	36
CLI Conventions	vi	Synchronizing System Clocks	37
WebUI Conventions	vii	Dual HA Interfaces	38
Illustration Conventions	ix	Control Messages	39
Naming Conventions and Character Types	x	Data Messages (Packet Forwarding)	40
NetScreen Documentation	xi	Dynamic Routing Advisory	41
Chapter 1 NSRP	1	Dual HA Link Probes	42
NSRP Overview	3	Example: Sending Link Probes Manually	43
NSRP and NetScreen Operational Modes	8	Example: Sending Link Probes Automatically	44
Basic Active/Passive NSRP Configuration	8	Setup Procedure	45
Default Settings	9	Cabling for a Full-Mesh Configuration	45
Example: NSRP for an Active/Passive Configuration	10	Active/Active NSRP Configuration	49
NSRP Clusters	15	Example: NSRP for an Active/Active Configuration	49
Cluster Name	17	Chapter 2 NSRP-Lite	57
Example: Creating an NSRP Cluster	18	Introduction to NSRP-Lite	59
Run-Time Objects	21	Clusters and VSD Groups	60
RTO Mirror States	22	Default Settings	61
VSD Groups	23	Cluster	62
Preempt Option	23	Cluster Name	63
VSD Group Member States	24	Authentication and Encryption	64
Heartbeat Messages	25	VSD Group	65
Example: Creating Two VSD Groups	26	VSD Group Member States	65
VSIs and Static Routes	28	Heartbeat Messages	66
Example: Trust and Untrust Zone VSIs	29	Preempt Option	67
Synchronization	33	Cabling and Configuring NSRP-Lite	68
Synchronizing Configurations	33	Example: Configuring NSRP-Lite	69
Synchronizing Files	34	Configuration and File Synchronization	76
Synchronizing RTOs	34	Synchronizing Configurations	76
Example: Manually Resynchronizing RTOs	35		

Synchronizing Files	77	Serial Interface	118
Example: Adding a Device to an Active NSRP Cluster	77	Modem Settings	119
Disabling Configuration and File Synchronization	78	Example: Configuring Modem Settings.....	120
Path Monitoring	79	ISP Configuration	121
Setting Thresholds	80	Example: Configuring ISP Information	122
Weighting Tracked IP Addresses	80	Serial Interface Failover.....	123
IP Tracking for VPN Tunnel Failover.....	81	Example: Configuring Dial Backup in the Trust-Untrust Mode	124
Example: IP Tracking through a VPN Tunnel.....	82	Example: Deleting a Default Route for the Serial Interface.....	127
Chapter 3 Interface Redundancy	93	Example: Adding a Default Route for the Serial Interface.....	127
Redundant Interfaces.....	94	Example: Specifying a Policy as Inactive for Serial Interface Failover	128
Example: Creating Redundant Interfaces for VSIs	96	Chapter 4 Failover	129
Aggregate Interfaces	101	Device Failover (NSRP).....	130
Example: Configuring an Aggregate Interface.....	102	VSD Group Failover (NSRP)	131
Dual Untrust Interfaces.....	103	Configuring Object Monitoring for Device or VSD Group Failover.....	132
Interface Failover.....	104	Configuring Monitored Objects.....	134
Example: Manually Forcing Traffic from the Primary to the Backup Interface.....	104	Physical Interface Objects	134
Example: Manually Forcing Traffic from the Backup to the Primary Interface.....	104	Example: Monitoring an Interface	134
Example: Automatically Switching Traffic between the Primary and Backup Interface	105	Zone Objects	135
Determining Interface Failover	105	Example: Monitoring an Interface	135
Interface Failover with IP Tracking	106	Tracked IP Objects	136
Example: Configuring Automatic Failover with IP Tracking	107	Example: Track IP for Device Failover	139
Interface Failover with VPN Tunnel Monitoring	111	Virtual System Failover	144
Example: Configuring Automatic Failover with VPN Tunnel Monitoring.....	112	Example: VSIs for Inter-Virtual System Load Sharing.....	144
		Index.....	IX-I

Preface

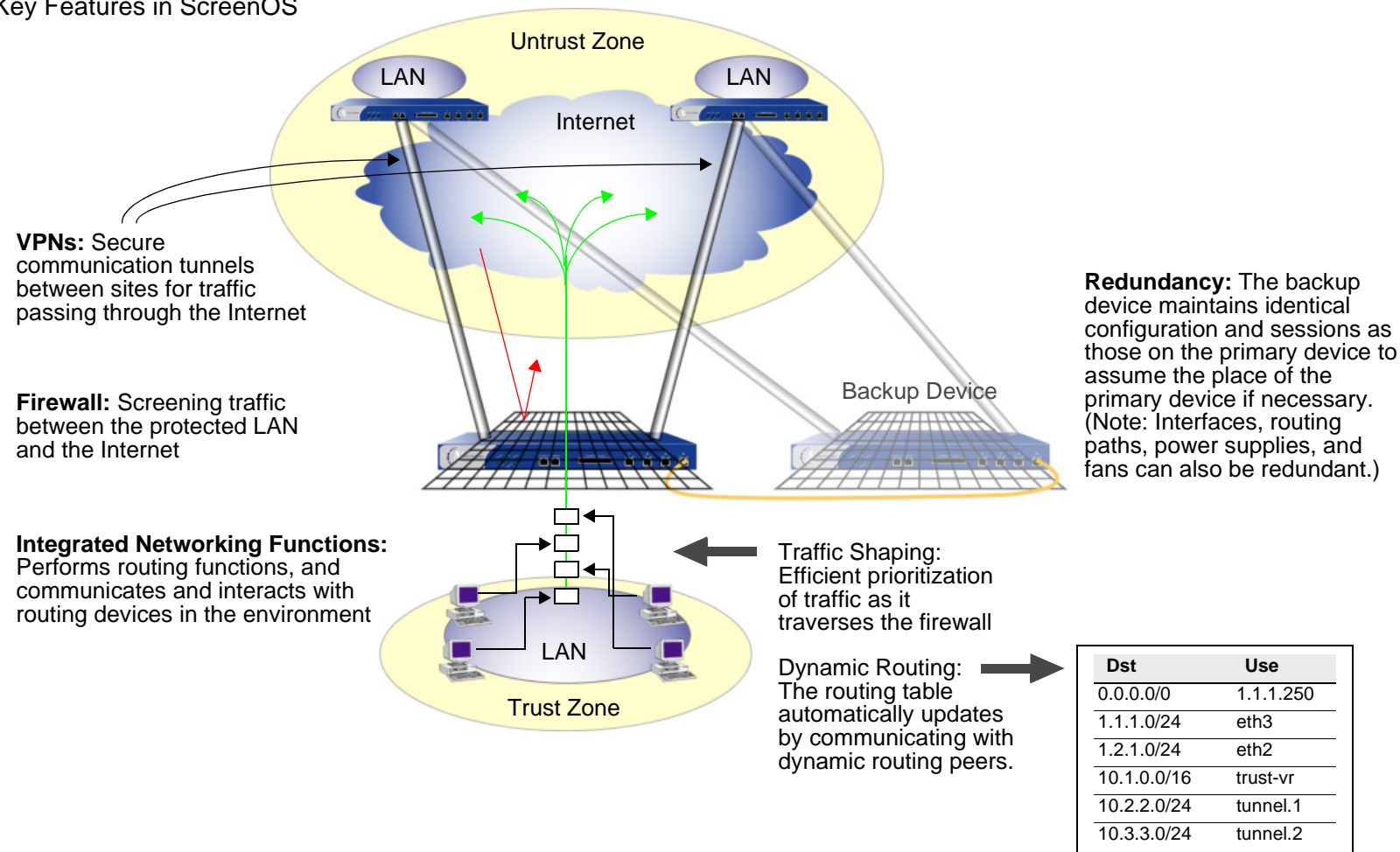
NetScreen devices are ASIC-based, ICSA-certified¹ Internet security appliances and security systems that integrate firewall, virtual private networking (VPN), and traffic-shaping features to provide flexible protection for security zones such as the internal local area network (LAN) or demilitarized 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



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”](#)
- [“WebUI Conventions” on page xxviii](#)
- [“Illustration Conventions” on page xxx](#)
- [“Naming Conventions and Character Types” on page xxxi](#)

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.

The screenshot shows the NetScreen WebUI interface. The breadcrumb path at the top is "Objects > Addresses > List". The left sidebar contains a menu with "Objects" highlighted. The "Addresses" sub-menu is expanded, showing "List" as the selected option. The "List" view displays a table of addresses. A "New" link is visible in the top right corner. Red circles and arrows indicate the navigation sequence: 1. Click "Objects" in the menu column. 2. (Applet menu) Hover the mouse over "Addresses". (DHTML menu) Click "Addresses". 3. Click "List". 4. Click the "New" link.

Name	IP/Domain Name	Comment	Configure
Any	0.0.0.0/0	All Addr	In Use
Dial-Up VPN	255.255.255.255/32		

IP Address/Domain Name

☐ IP/Netmask /

☐ Domain Name

Zone: Untrust

OK Cancel

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

Objects > Addresses > Configuration n200_5.0.0:NSRP(M)

Address Name: addr_1 Address Name addr_1

Comment

IP Address/Domain Name

IP/Netmask 10.2.2.5 / 32

Domain Name







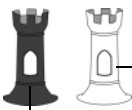







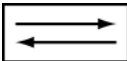
Zone: Untrust Zone Untrust

Click **OK**. OK Cancel

Note: Because there are no instructions for the Comment field, leave it as it is.

Illustration Conventions

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

	Generic NetScreen Device		Local Area Network (LAN) with a Single Subnet (example: 10.1.1.0/24)
	Virtual Routing Domain		Internet
	Security Zone		Dynamic IP (DIP) Pool
	Security Zone Interfaces White = Protected Zone Interface (example: Trust Zone) Black = Outside Zone Interface (example: Untrust Zone)		Desktop Computer
			Laptop Computer
	Tunnel Interface		Generic Network Device (examples: NAT server, Access Concentrator)
	VPN Tunnel		Server
	Router Icon		
	Switch Icon		

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 hexadecimal) 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

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 ethernet 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 Thinnets), 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.

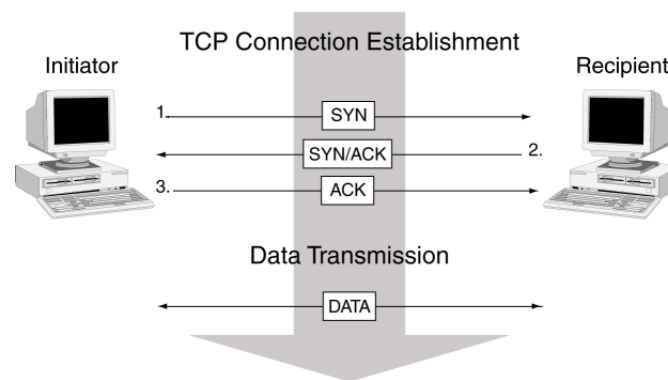
The software remembers static routes until you remove them. However, you can override static routes with dynamic routing information through judicious assignment of administrative distance values. To do this, you must ensure that the administrative distance of the static route is higher than that of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

100BaseT, defined 1-A-I
 10BaseT, defined 1-A-I
 3DES 5-8

A

access list 1-A-I
 access list for routes 6-24
 access policies
 See policies
 access-challenge 1-A-I
 ActiveX controls, blocking 4-167
 address book
 adding addresses 2-127
 editing group entries 2-132
 entries 2-127
 groups 2-129
 modifying addresses 2-128
 removing addresses 2-133
 See also addresses
 address groups 2-129, 2-206
 creating 2-131
 editing 2-132
 options 2-130
 removing entries 2-133
 address negation 2-237
 address sweep 4-8
 address translation
 See NAT, NAT-dst, and NAT-src
 addresses
 address book entries 2-127
 defined 2-206
 in policies 2-206
 private 2-78
 public 2-77
 adjacencies 1-A-I
 admin users 2-465–2-466
 auth process 2-466
 privileges from RADIUS 2-465

server support 2-372
 timeout 2-378
 administration
 CLI (Command Line Interface) 3-9
 restricting 3-49, 3-50
 vsys admin 7-38
 WebUI 3-3
 administrative traffic 3-30
 advertisement 1-A-I
 AES (Advanced Encryption Standard) 5-8
 aggregate interfaces 2-67, 8-101
 aggregate state 1-A-I
 aggregation 1-A-I
 aggregator 1-A-I
 aggressive aging 4-40–4-42
 defined 1-A-II
 Aggressive Mode 5-12
 AH 5-3, 5-7
 alarms
 E-mail alert 3-82
 reporting to NSM 3-26
 thresholds 2-213, 3-82
 traffic 3-82–3-86
 ALG 2-159, 4-73
 for custom services 2-207
 anti-replay checking 5-46, 5-54
 antivirus objects
 See AV objects
 antivirus scanning
 policies 2-214
 See AV scanning
 application layer gateway
 See ALG
 application, in policies 2-207
 area 1-A-II
 area border router 1-A-II
 area range 1-A-II
 ARP 2-95, 8-56, 8-136
 broadcasts 8-18
 ingress IP address 2-98
 path monitoring 8-79
 AS number 1-A-II

AS path access list 1-A-II
 AS path attribute class 1-A-II
 AS path string 1-A-II
 asset recovery log 3-81
 atomic aggregate 1-A-II
 attack actions 4-142–4-151
 close 4-142
 close client 4-142
 close server 4-142
 drop 4-142
 drop packet 4-142
 ignore 4-143
 none 4-143
 attack object database 4-128–4-135
 auto notification and manual update 4-128, 4-132
 automatic update 4-128, 4-130
 changing the default URL 4-134
 immediate update 4-128, 4-129
 manual update 4-129, 4-134
 attack object groups 4-140
 changing severity 4-140
 severity levels 4-140
 attack objects 4-125
 defined 1-A-II
 protocol anomalies 4-139
 stateful signatures 4-138
 TCP stream signatures 4-164
 attack protection
 policy level 4-5
 security zone level 4-5
 attacks
 common objectives 4-1
 detection and defense options 4-3–4-5
 ICMP flood 4-59
 ICMP fragments 4-2
 IP packet fragments 4-10
 Land attack 4-63
 large ICMP packets 4-4
 Ping of Death 4-65
 Replay 5-14
 stages of 4-2

- SYN flood 4-45– 4-51
- SYN fragments 4-12– 4-13
- Teardrop 4-67
- UDP flood 4-61
- unknown MAC addresses 4-51
- unknown protocols 4-8
- WinNuke 4-69
- auth servers 2-372
 - address 2-377
 - authentication process 2-376
 - backup servers 2-377
 - default 2-395
 - defining 2-388– 2-396
 - external 2-376
 - feature support 2-372
 - ID number 2-377
 - in IKE gateways 2-396
 - in policies 2-396
 - LDAP 2-386– 2-387
 - LDAP, defining 2-393
 - maximum number 2-373
 - multiple user types 2-373
 - object name 2-377
 - object properties 2-377
 - RADIUS 2-379– 2-381
 - RADIUS, defining 2-388
 - RADIUS, user type support 2-380
 - SecurID 2-384– 2-385
 - SecurID, defining 2-391
 - timeout 2-377
 - types 2-377
 - user type support 2-372
 - XAuth queries 2-437
- auth users 2-398– 2-430
 - groups 2-398, 2-402
 - in policies 2-398
 - point of authentication 2-397
 - pre-policy auth 2-212, 2-400
 - run-time (external user group) 2-412
 - run-time (external user) 2-409
 - run-time (local user group) 2-406
 - run-time (local user) 2-403
 - run-time auth process 2-211, 2-399
 - run-time authentication 2-211, 2-399
 - server support 2-372
 - timeout 2-377

- WebAuth 2-212, 2-400
- WebAuth (external user group) 2-423
- WebAuth (local user group) 2-420
- WebAuth + SSL (external user group) 2-427
- authentication
 - algorithms 5-7, 5-44, 5-49, 5-53, 5-57
 - Allow Any 2-212
 - IPSec 1-A-III
 - NSRP 8-7, 8-18
 - NSRP-Lite 8-64
 - policies 2-210
 - users 2-210, 2-371– 2-476
 - WebAuth 2-400
- Authentication Header
 - See AH
- authentication, users 2-371– 2-476
 - accounts 2-371
 - admin 2-465
 - auth servers 2-372
 - auth users 2-398
 - IKE users 2-372, 2-431
 - L2TP users 2-460
 - local database 2-374– 2-375
 - Manual Key users 2-372
 - multiple-type 2-467
 - point of authentication 2-397
 - profiles 2-371
 - types and applications 2-397– 2-467
 - user types 2-372
 - WebAuth 2-372
 - with different logins 2-467
 - XAuth users 2-436
- AutoKey IKE VPN 3-51, 3-98, 5-9
 - management 5-9
- autonomous system boundary router 1-A-III
- autonomous system path 1-A-III
- autonomous systems
 - defined 1-A-III
- AV objects 4-93– 4-101
 - port number 4-94
 - states 4-93
 - timeout 4-94
- AV scanning 4-76– 4-112
 - application 4-102
 - AV objects 4-93– 4-101
 - decompression 4-85

- external AV scanner 4-90– 4-112
- external, CSP resources 4-95
- external, HTTP 4-92
- external, SMTP 4-91
- fail-mode 4-95
- fail-mode threshold 4-96
- HTTP keep-alive 4-96
- HTTP trickling 4-97
- HTTP webmail 4-80
- internal AV scanner 4-77– 4-89
- internal, HTTP 4-79
- internal, POP3 4-78
- internal, SMTP 4-77
- internal, subscription 4-81
- InterScan VirusWall 4-90
- max TCP connections 4-94
- multiple AV objects 4-106

B

- back store 3-122
- bandwidth 2-215
 - default priority 2-485
 - guaranteed 2-215, 2-478, 2-486
 - managing 2-478
 - maximum 2-215, 2-486
 - maximum specification 2-478
 - priority levels 2-485
 - priority queues 2-485
 - unlimited maximum 2-478
- banners, customizing 2-476
- BGP 1-A-III
 - AS-path access list 6-106
 - authenticating neighbors 6-102
 - communities 6-113
 - confederations 6-110
 - configuration steps 6-91
 - configuring peer group 6-95
 - configuring peers 6-95
 - creating instance in VR 6-92
 - enabling in VR 6-92
 - enabling on interface 6-94
 - external BGP 6-90
 - internal BGP 6-90
 - message types 6-89
 - parameters 6-104

- path attributes 6-89
- protocol overview 6-88
- redistributing routes 6-105
- regular expressions 6-106
- rejecting default routes 6-103
- route reflection 6-107
- security configuration 6-102
- verifying configuration 6-100

bit stream 3-121

bridges 1-A-III

broadcast networks 1-A-III

browser requirements 3-3

C

CA certificates 5-18, 5-22

cables, serial 3-21

certificates 5-10

- CA 5-18, 5-22
- loading 5-26
- local 5-22
- requesting 5-23
- revocation 5-21, 5-36
- via e-mail 5-22

Challenge Handshake Authentication Protocol

- See CHAP

CHAP 2-453, 5-273, 5-276

character types, ScreenOS supported 1-xxxi, 2-xiv, 3-x, 4-x, 5-x, 6-x, 7-viii, 8-x

classless routing 1-A-IV

CLI 3-9, 3-30, 3-31

- conventions 1-xxvii, 2-x, 3-vi, 4-vi, 5-vi, 6-vi, 7-iv, 8-vi
- set arp always-on-dest 8-56
- set vip multi -port 2-358

clock, system 2-541–2-545

- See also system clock

cluster list 1-A-IV

cluster name, NSRP 8-17, 8-63

clusters 8-16–8-20, 8-49, 8-60–8-63

- defined 1-A-IV

command line interface

- See CLI

common name 2-387

community 1-A-IV

CompactFlash 3-66

confederation 1-A-IV

configuration

- adding comments 2-535
- LKG 2-531
- loading 2-533
- locking 2-534
- rollback 2-531–2-532, 2-533

configuration settings

- browser requirements 3-3
- downloading 2-528
- uploading 2-528

connection states 1-A-IV

connectors

- GBIC, definition 1-A-VII
- RJ-45, definition 1-A-XII

console 3-66

container 5-242

content filtering 4-71–4-121

Content Scanning Protocol

- See CSP

control messages 8-38

- HA messages 8-40
- HA physical link heartbeats 8-39
- RTO heartbeats 8-40
- VSD heartbeats 8-40

conventions

- CLI 1-xxvii, 2-x, 3-vi, 4-vi, 5-vi, 6-vi, 7-iv, 8-vi
- illustration 1-xxx, 2-xiii, 3-ix, 4-ix, 5-ix, 6-ix, 7-vii, 8-ix
- names 1-xxxi, 2-xiv, 3-x, 4-x, 5-x, 6-x, 7-viii, 8-x
- WebUI 1-xxviii, 2-xi, 3-vii, 4-vii, 5-vii, 6-vii, 7-v, 8-vii

counting 2-213

creating

- address groups 2-131
- keys 3-7
- MIP addresses 2-333
- service groups 2-168
- zones 2-51

CRL (Certificate Revocation List) 5-20, 5-36

- loading 5-20

cryptographic options 5-40–5-57

- anti-replay checking 5-46, 5-54
- authentication algorithms 5-44, 5-49, 5-53, 5-57
- authentication types 5-42, 5-51
- certificate bit lengths 5-43, 5-51
- dialup 5-50–5-57
- dialup VPN recommendations 5-57
- Diffie-Hellman groups 5-43, 5-46, 5-52, 5-55
- encryption algorithms 5-44, 5-48, 5-52, 5-57
- ESP 5-48, 5-56
- IKE ID 5-44–5-46, 5-53–5-54
- IPSec protocols 5-47, 5-56
- key methods 5-42
- PFS 5-46, 5-55
- Phase 1 modes 5-42, 5-51
- site-to-site 5-41–5-49
- site-to-site VPN recommendations 5-49
- Transport mode 5-56
- Tunnel mode 5-56

CSP 4-90

D

Data Encryption Standard

- See DES

data messages 8-40

DDoS 4-35

dead interval 1-A-V

decompression, AV scanning 4-85

Deep Inspection 4-140–4-163

- attack actions 4-142–4-151
- attack object database 4-128–4-135
- attack object groups 4-140
- attack objects 4-125
- attack objects, defined 1-A-II
- changing severity 4-140
- context 4-156
- custom attack objects 4-156
- custom services 4-152–4-155
- custom signatures 4-157–4-163
- protocol anomalies 4-139
- regular expressions 4-157–4-159
- stateful signatures 4-138

- defining
 - subinterfaces 7-25
 - zones 2-51
- Denial-of-Service
 - See DoS
- DES 5-8
 - defined 1-A-IV
- DES-CBC, defined 1-A-V
- device failover 8-130
- DHCP 2-115, 2-121, 2-521
 - client 2-500
 - HA 2-508
 - relay agent 2-500
 - server 2-500
- dictionary file 2-465
- Diffie-Hellman exchange 5-13
- Diffie-Hellman groups 5-13, 5-43, 5-46, 5-52, 5-55
- DiffServ 2-215
 - See DS Codepoint Marking
- digital signature 5-16
- DIP 2-119, 2-171–2-174, 3-124
 - fix-port 2-173
 - groups 2-189–2-192
 - modifying a DIP pool 2-174
 - PAT 2-172
 - pools 2-210
- DIP pools
 - address considerations 2-259
 - extended interfaces 5-168
 - NAT for VPNs 5-168
 - NAT-src 2-246
 - size 2-259
- distance vector 1-A-V
- distinguished name 2-387
- DMZ, definition 1-A-V
- DN (distinguished name) 5-237
- DNS 2-495
 - L2TP settings 5-276
 - lookup 2-496
 - server 2-523
 - status table 2-497
- Domain name system
 - See DNS

- DoS 4-35–4-70
 - firewall 4-36–4-44
 - network 4-45–4-63
 - OS-specific 4-65–4-70
 - session table flood 4-36
- drop-no-rpf-route 4-23
- DS Codepoint Marking 2-478, 2-487, 2-488
- DSL 2-517, 2-522
- dual Untrust interfaces 8-103
- Dynamic IP
 - See DIP
- Dynamic IP pools
 - See DIP pools
- dynamic packet filtering 4-3
- dynamic routing 1-A-V, 2-30

E

- editing
 - address groups 2-132
 - policies 2-241
 - zones 2-52
- e-mail alert notification 3-86, 3-89, 3-90
- Encapsulating Security Payload
 - See ESP
- encryption
 - algorithms 5-8, 5-44, 5-48, 5-52, 5-57
 - definition 1-A-VI
 - NSRP 8-7, 8-18
 - NSRP-Lite 8-64
- ESP 5-3, 5-7, 5-8
 - authenticate only 5-48
 - encrypt and authenticate 5-48, 5-56
 - encrypt only 5-48
- Ethernet, definition 1-A-VI
- evasion 4-22–4-33
- event log 3-67
- exe files, blocking 4-168
- exploits
 - See attacks
- exporting routes 6-28
- external neighbors 1-A-VI
- extranet, definition 1-A-VI

F

- fail/pass mode, URL filtering 4-116
- fail-mode 4-95
 - threshold 4-96
- failover
 - device 8-130
 - dual Untrust interfaces 8-104, 8-105
 - object monitor 8-132
 - serial interface 8-123
 - virtual system 8-144
 - VSD group 8-131
- filter list 1-A-VI
- filter source route 3-125
- filtering, packets 1-A-VI
- FIN scan 4-22
- FIN without ACK flag 4-18
- FIPS 1-xxi
- firewall, definition 1-xxi, 1-A-VII
- fragment reassembly 4-72–4-75
- full-mesh configuration 8-144
- Function Zone Interfaces 2-68
 - HA Interface 2-69
 - Management Interface 2-68

G

- gatekeeper devices 2-141
- gateway
 - routing 1-A-VIII
- gateway (router) 1-A-VII
- global zone 2-359
- graphs, historical 2-213
- group
 - addresses 2-129
 - services 2-167
- group expressions 2-468–2-475
 - operators 2-468
 - other group expressions 2-469
 - server support 2-372
 - user groups 2-468
 - users 2-468
- group IKE ID
 - certificates 5-238–5-249
 - preshared key 5-250–5-258

group IKE ID user 5-237– 5-258
 certificates 5-238
 preshared key 5-250

H

H.323 protocol 2-141

HA

 active/active failover 8-6
 active/passive failover 8-4
 aggregate interfaces 8-101
 cabling 8-45– 8-48
 cabling for dedicated HA interfaces 8-45
 cabling network interfaces as HA links 8-47
 control link 8-38
 data link 8-41
 DHCP 2-508
 dual Untrust interfaces 8-103
 HA LED 8-25
 IP tracking 8-79, 8-136
 link probes 8-42
 messages 8-40
 path monitoring 8-79
 redundant interfaces 8-94
 secondary path 8-25
 serial interface 8-118
 Virtual HA Interface 2-69
 See also NSRP
hash-based message authentication code
 See HMAC
hello interval 1-A-VII
hello packet 1-A-VII
High Availability
 See HA
high-watermark threshold 4-41
historical graphs 2-213
HMAC 5-7
hold time 1-A-VII
Home zone 2-61
HTTP 3-5
 blocking components 4-167– 4-169
 keep-alive 4-96
 session ID 3-5
 session timeout 4-41
 trickling 4-97
hubs, definition 1-A-VII

Hypertext Transfer Protocol
 See HTTP

I

ICMP

 definition 1-A-VII
 fragments 4-2
 large packets 4-4
ICMP flood 4-59
ICMP services 2-139
 message code 2-139
 message type 2-139
icons
 defined 2-216
 policy 2-216
Ident-Reset 3-29
idle session timeout 2-377
IEEE 802.1Q VLAN standard 7-21
IKE 5-9, 5-77, 5-91, 5-201
 group IKE ID user 5-237– 5-258
 group IKE ID, container 5-242
 group IKE ID, wildcard 5-241
 heartbeats 5-384
 hello messages 5-384
 IKE ID 2-431, 2-452, 5-44– 5-46, 5-53– 5-54
 IKE ID recommendations 5-68
 IKE ID, Windows 200 5-288
 ISAKMP 1-A-IX
 key management 1-A-IX
 local ID, ASN1-DN 5-240
 Phase 1 proposals, predefined 5-11
 Phase 2 proposals, predefined 5-14
 proxy IDs 5-14
 redundant gateways 5-382– 5-400
 remote ID, ASN1-DN 5-240
 shared IKE ID user 5-259– 5-267
 user groups, defining 2-434
 users 2-431– 2-435
 users, defining 2-432
 users, groups 2-431
IKE users
 IKE ID 2-397, 2-431
 server support 2-372
 with other use types 2-467

illustration

 conventions 1-xxx, 2-xiii, 3-ix, 4-ix, 5-ix, 6-ix, 7-vii, 8-ix
importing routes 6-28
inactive SA 3-125
in-short error 3-122
interfaces
 addressing 2-77
 aggregate 2-67, 8-101
 binding to zone 2-76
 dedicated 7-15, 7-33
 default 2-79
 DIP 2-171
 dual Untrust 8-103
 exporting from vsys 7-19
 extended 5-168
 HA 2-69
 HA, dual 8-38– 8-41
 importing to vsys 7-18
 L3 security zones 2-77
 loopback 2-86
 manageable 3-34
 management options 3-29
 MGT 2-68
 MIP 2-331
 modifying 2-81
 monitoring 8-18
 physical 2-3
 redundant 2-67, 8-94
 secondary IP address 2-84
 serial 8-118
 shared 7-15, 7-33
 tunnel 2-49, 2-69, 2-70– 2-73
 tunnel, definition 1-A-XVI
 unbinding from zone 2-80
 viewing interface table 2-74
 VIP 2-356
 Virtual HA 2-69, 8-47
 VSI 2-68
 VSIs 8-28
internal flash storage 3-66
Internet Key Exchange
 See IKE
Internet, definition 1-A-VIII
InterScan VirusWall 4-90
intranet, definition 1-A-IX

- IP
 - definition 1-A-VIII
 - packet fragments 4-10
- IP addresses
 - defining for each port 2-127
 - definition 1-A-VIII
 - extended 5-168
 - host ID 2-78
 - L3 security zones 2-77– 2-78
 - manage IP 3-34
 - network ID 2-78
 - NSM servers 3-26
 - private 2-77
 - private address ranges 2-78
 - public 2-77
 - secondary 2-84
 - virtual 2-356
- IP options 4-12– 4-14
 - attributes 4-12– 4-14
 - incorrectly formatted 4-6
 - loose source route 4-13, 4-31– 4-33
 - record route 4-13, 4-14
 - security 4-13, 4-14
 - source route 4-31
 - stream ID 4-13, 4-14
 - strict source route 4-14, 4-31– 4-33
 - timestamp 4-14
- IP pools
 - See DIP pools
- IP Security
 - See IPSec
- IP spoofing 4-22– 4-30
 - drop-no-rpf-route 4-23
 - Layer 2 4-24, 4-29
 - Layer 3 4-23, 4-25
- IP tracking 8-79, 8-136
 - device failover threshold 8-80
 - ping and ARP 8-79, 8-136
 - tracked IP failure threshold 8-80, 8-133
 - tunnel failover 8-81
 - weights 8-80
- IP-based traffic classification 7-33
- IPSec 5-3
 - AH 5-2, 5-47, 5-56
 - AH, defined 1-A-VI
 - authentication 1-A-III
 - definition 1-A-VIII
 - digital signature 5-16
 - encryption 1-A-VI
 - ESP 5-2, 5-47, 5-56
 - ESP, defined 1-A-VI
 - SAs 1-A-XIII, 5-2, 5-10, 5-11, 5-13
 - SPI 5-2
 - SPI, definition 1-A-XIII
 - transport mode 5-4, 5-273, 5-279, 5-286
 - tunnel 5-2
 - tunnel mode 5-5
 - tunnel negotiation 5-11
- ISAKMP 1-A-IX
- ISP configuration for serial interface 8-121
- J**
- Java applets, blocking 4-168
- K**
- keep alive, BGP 1-A-IX
- keepalive
 - frequency, NAT-T 5-303
 - L2TP 5-283
- keys
 - creating 3-7
 - management 1-A-IX
- L**
- L2TP 5-269– 5-298
 - access concentrator, See LAC
 - address assignment 2-460
 - compulsory configuration 5-270
 - decapsulation 5-275
 - default parameters 5-276
 - encapsulation 5-274
 - external auth server 2-461
 - hello signal 5-284
 - Keep Alive 5-283, 5-284
 - L2TP-only on Windows 2000 5-273
 - local database 2-461
 - network server, See LNS
 - operational mode 5-273
 - policies 2-209
 - RADIUS server 5-276
 - ScreenOS support 5-273
 - SecurID server 5-276
 - tunnel 5-279
 - user authentication 2-460
 - voluntary configuration 5-270
 - Windows 2000 5-291
 - Windows 2000 tunnel authentication 5-283
- L2TP users 2-460– 2-464
 - point of authentication 2-397
 - server support 2-372
 - with XAuth 2-467
- L2TP-over-IPSec 5-4, 5-279, 5-286
 - tunnel 5-279
- LAC 5-270
 - NetScreen-Remote 5.0 5-270
 - Windows 2000 5-270
- LAN, definition 1-A-X
- Land attack 4-63
- Last-Known-Good configuration
 - See LKG configuration
- Layer 2 Tunneling Protocol
 - See L2TP
- LDAP 2-386– 2-387
 - auth server object 2-393
 - common name identifier 2-387
 - distinguished name 2-387
 - server port 2-387
 - structure 2-386
 - user types supported 2-387
- LED indicators, HA 8-25
- license keys 2-536– 2-537
- Lightweight Directory Access Protocol
 - See LDAP
- link state 1-A-IX
- link state advertisement 1-A-IX
- LKG (last-known-good) 2-531
- LKG configuration 2-531
- LNS 5-270
- load balancing
 - definition 1-A-IX
- load sharing 8-144
- local certificate 5-22

- local database 2-374– 2-375
 - IKE users 2-431
 - timeout 2-375
 - user types supported 2-374
- local preference 1-A-X
- logging 2-213, 3-66– 3-81
 - asset recovery log 3-81
 - CompactFlash (PCMCIA) 3-66
 - console 3-66
 - e-mail 3-66
 - event log 3-67
 - internal 3-66
 - NSM reporting 3-26
 - self log 3-77
 - SNMP 3-66, 3-91
 - syslog 3-66, 3-87
 - WebTrends 3-66, 3-89
- logging in
 - root admin 3-50
 - Telnet 3-10
 - vsys 7-33, 7-38
- loopback interfaces 2-86
- loose source route IP option 4-13, 4-31– 4-33
- low-watermark threshold 4-41

M

- MAC address
 - definition 1-A-X
- Main Mode 5-12
- malicious URL protection 4-72– 4-75
- manage IP 3-34
 - VSD group 0 8-8
- management client IP addresses 3-49
- Management information base II
 - See MIB II
- Management interface
 - See MGT interface
- management methods
 - CLI 3-9
 - console 3-21
 - SSL 3-7
 - Telnet 3-9
 - WebUI 3-3
- management options 3-29
 - manageable 3-34
 - NSM 3-29
 - ping 3-29
 - SCS 3-29
 - SNMP 3-29
 - SSL 3-29
 - Telnet 3-29
 - Transparent mode 3-30
 - WebUI 3-29
- Manual Key 5-131, 5-142
 - management 5-9
 - VPNs 3-51, 3-98
- mapped IP
 - See MIP
- MD5 5-7
 - definition 1-A-X
- MED comparison 1-A-X
- Message Digest version 5
 - See MD5
- messages
 - alert 3-67
 - critical 3-67
 - debug 3-67
 - emergency 3-67
 - error 3-67
 - info 3-67
 - notice 3-67
 - warning 3-67
 - WebTrends 3-90
- MGT interface 2-68
 - management options 3-30
- MIB files 3-A-I
- MIB files, importing 5-325
- MIB folders
 - primary 3-A-II
- MIB II 3-29, 3-91
- MIP 2-12, 2-331
 - address range 2-335
 - bidirectional translation 2-252
 - creating addresses 2-333
 - creating on tunnel interface 2-341
 - creating on zone interface 2-333
 - default netmask 2-335
 - default virtual router 2-335
 - definition 1-A-X, 2-252

- global zone 2-332
 - reachable from other zones 2-336
- same-as-untrust interface 2-342– 2-345
- to zone with interface-based NAT 2-112
- virtual systems 7-10
- VPNs 5-168
- modem configuration for serial interface 8-119
- modem port 3-22
- modulus 5-13
- multi exit discriminator 1-A-X
- multimedia sessions, SIP 2-156
- multiple-type users 2-467

N

- names
 - conventions 1-xxxi, 2-xiv, 3-x, 4-x, 5-x, 6-x, 7-viii, 8-x
- NAT
 - definition 1-A-XI, 2-246
 - IPSec and NAT 5-301
 - NAT servers 5-301
 - NAT-src with NAT-dst 2-310– 2-330
- NAT mode 2-110– 2-117
 - interface settings 2-113
 - traffic to Untrust zone 2-91, 2-112
- NAT vector error 3-125
- NAT-dst 2-276– 2-330
 - address range 2-250
 - address range to address range 2-256, 2-300
 - address range to single IP 2-256, 2-295
 - address shifting 2-251, 2-277, 2-300
 - one-to-many translation 2-291
 - one-to-one translation 2-286
 - packet flow 2-278– 2-281
 - port mapping 2-249, 2-276, 2-305
 - route considerations 2-277, 2-282– 2-285
 - single IP with port mapping 2-255
 - single IP, no port mapping 2-255
 - unidirectional translation 2-252, 2-257
 - VPNs 5-168
 - with MIPs or VIPs 2-248
- NAT-src 2-246, 2-259– 2-275
 - address shifting 2-267– 2-272
 - address shifting, range considerations 2-267

- DIP pool with address shifting 2-254
- DIP pool with PAT 2-253, 2-260–2-263
- DIP pool, fixed port 2-253
- DIP pools 2-246
- egress interface 2-254, 2-273–2-275
- fixed port 2-259, 2-264–2-266
- interface based 2-247
- port address translation 2-247
- Route mode Route mode
 - NAT-src 2-118
- unidirectional translation 2-252, 2-257
- VPNs 5-171
- NAT-T 5-301
 - enabling 5-305
 - keepalive frequency 5-303
- NAT-Traversal
 - See NAT-T
- negation, address 2-237
- neighbor 1-A-XI
- NetInfo 2-501
- netmasks 2-206
 - definition 1-A-XI, 1-A-XIV
 - uses of 2-78
- NetScreen dictionary file 2-381
- NetScreen Redundancy Protocol
 - See NSRP
- NetScreen Reliable Transport Protocol
 - See NRTP
- NetScreen Security Manager
 - See NSM
- NetScreen-Remote
 - AutoKey IKE VPN 5-201
 - dynamic peer 5-209, 5-220
 - NAT-T option 5-301
- Network Address Translation (NAT) 3-124
- network layer reachability information 1-A-XI
- network, bandwidth 2-478
- NHTB table 5-326–5-331
 - addressing scheme 5-328
 - automatic entries 5-331
 - manual entries 5-330
 - mapping routes to tunnels 5-327
- NRTP 8-33, 8-76
- NSM
 - Agent 3-23, 3-26
 - definition 3-23
 - enabling the Agent 3-25
 - initial connectivity setup 3-24
 - management options 3-29
 - Management System 3-23, 3-26
 - reporting events 3-26, 3-27
 - UI 3-23
- NSRP
 - ARP 8-56
 - ARP broadcasts 8-18
 - backup 8-4
 - cabling 8-45–8-48
 - clear cluster command 8-16, 8-63
 - cluster name 8-17, 8-63
 - clusters 8-16–8-20, 8-49
 - config sync 8-33
 - configuration rollback 2-533
 - control link 8-38
 - control messages 8-38, 8-39
 - data link 8-41
 - data messages 8-40
 - debug cluster command 8-16, 8-63
 - default settings 8-9, 8-61
 - DHCP 2-508
 - DIP groups 2-189–2-192
 - files, sync 8-34
 - full-mesh configuration 8-45, 8-144
 - HA cabling, dedicated interfaces 8-45
 - HA cabling, network interfaces 8-47
 - HA interfaces 8-39
 - HA LED 8-25
 - HA ports, redundant interfaces 8-94
 - HA session backup 2-212, 8-21
 - hold-down time 8-51, 8-55
 - interface monitoring 8-18
 - load sharing 8-144
 - manage IP 8-80, 8-136
 - master 8-4
 - NAT and Route modes 8-8
 - NSRP, defined 1-A-XI
 - NTP synchronization 2-543, 8-37
 - overview 8-3
 - packet forwarding and dynamic routing 8-41
 - port failover 8-94
 - port monitoring 8-134
 - preempt mode 8-23
 - priority numbers 8-23
 - redundant interfaces 2-67
 - redundant ports 8-38
 - RTO states 8-22
 - RTOs 1-A-XIII, 8-21–8-22, 8-49
 - RTOs, sync 8-34
 - secondary path 8-18, 8-25
 - secure communications 8-7, 8-18
 - synchronization, PKI 8-34
 - Transparent mode 8-8
 - virtual systems 8-144–8-150
 - VSD groups 8-5, 8-23–8-27, 8-49, 8-79
 - VSD, defined 1-A-XVII
 - VSI 1-A-XVII
 - VSIs 2-68, 8-5
 - VSIs, static routes 8-28, 8-99, 8-100
- NSRP-Lite 8-57–8-78
 - cabling 8-68
 - clusters 8-60–8-63
 - config synchronization 8-76
 - disabling synchronization 8-78
 - file synchronization 8-77
 - port monitoring 8-79
 - preempt mode 8-67
 - secure communications 8-64
 - VSD groups 8-65–8-67
- NTP 2-542–2-545
 - authentication types 2-545
 - max time adjustment 2-542
 - maximum time adjustment 2-542
 - multiple servers 2-542
 - NSRP synchronization 2-543, 8-37
 - secure servers 2-545
 - server configuration 2-544
 - servers 2-542
-
- object monitoring 8-132
- OCSP (Online Certificate Status Protocol) 5-36
 - client 5-36
 - responder 5-36
- operating system 3-9
- OSPF
 - areas 6-34
 - assigning interface to area 6-42
 - authenticating neighbors 6-60

- backup designated router 6-36
- broadcast network 6-36
- configuration steps 6-38
- creating instance in VR 6-39
- defining area 6-41
- designated router 6-36
- enabling on interface 6-44
- filtering neighbors 6-62
- global parameters 6-51
- hello protocol 6-35
- interface parameters 6-57
- link-state advertisements 6-34, 6-37
- not so stubby area 6-35
- point-to-point network 6-36
- protecting against flooding 6-64
- redistributing routes 6-49
- rejecting default routes 6-63
- router adjacency 6-35
- router types 6-35
- security configuration 6-60
- stub area 6-35
- summarizing redistributed routes 6-50
- virtual links 6-53

P

- packet filtering 1-A-VI
- packet flow 2-11– 2-13
 - inbound VPN 5-63– 5-64
 - NAT-dst 2-278– 2-281
 - outbound VPN 5-61– 5-62
 - policy-based VPN 5-65– 5-66
 - route-based VPN 5-60– 5-64
- packets 3-125
 - address spoofing attack 3-123
 - collision 3-122
 - denied 3-125
 - dropped 3-124, 3-125
 - fragmented 3-125
 - incoming 3-122
 - Internet Control Message Protocol (ICMP) 3-120, 3-123
 - IPSec 3-123
 - land attack 3-124
 - Network Address Translation (NAT) 3-124

- Point to Point Tunneling Protocol (PPTP) 3-123
 - received 3-121, 3-122, 3-123, 3-125
 - transmitted underrun 3-122
 - unreceivable 3-122
 - unroutable 3-124
- PAP 5-273, 5-276
- parent connection 3-124
- password
 - forgetting 3-44
 - root admin 3-47
 - vsys admin 7-38
- Password Authentication Protocol
 - See PAP
- PAT 2-172, 2-259
- path monitoring 8-79
 - tunnel failover 8-81
- PC card 2-528, 2-530
- PCMCIA 3-66
- peer 1-A-XI
- Perfect Forward Secrecy
 - See PFS
- PFS 5-14, 5-46, 5-55
- Phase 1 5-11
 - proposals 5-11
 - proposals, predefined 5-11
- Phase 2 5-13
 - proposals 5-13
 - proposals, predefined 5-14
- ping
 - management options 3-29
- Ping of Death 4-65
- pinholes 2-161
- PKI 5-18
 - encryption 1-A-VI
 - key 3-7
- Point-to-Point Protocol
 - See PPP
- Point-to-Point Tunneling Protocol (PPTP) 3-123
- policies 2-3
 - actions 2-207
 - address groups 2-206
 - address negation 2-237
 - addresses 2-206
 - addresses in 2-206
 - alarms 2-213

- antivirus scanning 2-214
- application 2-207
- authentication 2-210
- bidirectional VPNs 2-208, 2-216, 5-143
- changing 2-241
- context 4-127
- core section 4-126
- counting 2-213
- Deep Inspection 2-209
- definition 1-A-XII
- deny 2-207
- DIP groups 2-190
- disabling 2-241
- enabling 2-241
- functions of 2-197
- global 2-201, 2-217, 2-234
- HA session backup 2-212
- icons 2-216
- ID 2-206
- internal rules 2-203
- interzone 2-200, 2-217, 2-218, 2-223
- intrazone 2-201, 2-217, 2-231
- L2TP 2-209
- L2TP tunnels 2-209
- location 2-218
- lookup sequence 2-202
- management 2-216
- managing bandwidth 2-478
- maximum limit 2-130
- multiple items per component 2-236
- name 2-208
- NAT-dst 2-210
- NAT-src 2-210
- order 2-243
- permit 2-207
- policy context 2-235
- policy set lists 2-202
- policy verification 2-242
- position at top 2-209, 2-243
- removing 2-244
- reordering 2-243
- required elements 2-199
- root system 2-203
- schedules 2-214
- security zones 2-206
- service book 2-134

- service groups 2-167
- services 2-206
- services in 2-134, 2-206
- shadowing 2-242
- traffic logging 2-213
- traffic shaping 2-215
- tunnel 2-207
- types 2-200–2-201
- URL filtering 2-213, 4-118
- virtual systems 2-203
- VPN dialup user groups 2-206
- VPNs 2-208
- policy-based NAT
 - See NAT-dst and NAT-src
- tunnel interfaces 2-69
- policy-based VPNs 5-58
- Port Address Translation
 - See PAT
- port mapping 2-249, 2-276
- port modes 2-55
- port scan 4-10
- ports
 - modem 3-22
 - monitoring 8-79, 8-134
 - port failover 8-94
 - port numbers 2-366
 - primary trusted and untrusted 8-94
 - redundant 8-38
 - secondary trusted and untrusted 8-94
 - trunk 7-23
 - trunk ports 1-A-XV
- PPP 5-271
- preempt mode 8-23, 8-67
- prefixes
 - defined 1-A-XII
- preshared key 5-9, 5-201
- priority queuing 2-485
- private addresses 2-78
- probes
 - network 4-8
 - open ports 4-10
 - operating systems 4-16–4-20
- proposals
 - Phase 1 5-11, 5-67
 - Phase 2 5-13, 5-67
- protocol anomalies 4-139

- protocol distribution
 - reporting to NSM 3-26
- protocols
 - CHAP 5-273
 - NRTP 8-33, 8-76
 - NSRP 8-1, 8-57
 - PAP 5-273
 - PPP 5-271
 - VRRP 8-79, 8-136
- proxy IDs 5-14
 - matching 5-67
 - VPNs and NAT 5-168–5-169
- proxy servers 1-A-III
- public addresses 2-77
- Public key infrastructure
 - See PKI
- Public/private key pair 5-19

Q

- QoS 1-xxi, 2-478
- Quality-of-service
 - See QoS

R

- RADIUS 2-379–2-381, 3-44
 - access-challenge 1-A-I
 - auth server object 2-388
 - L2TP 5-276
 - NetScreen dictionary file 2-465
 - object properties 2-380
 - port 2-380
 - retry timeout 2-380
 - shared secret 2-380
- reconnaissance 4-7–4-33
 - address sweep 4-8
 - FIN scan 4-22
 - IP options 4-12
 - port scan 4-10
 - SYN and FIN flags set 4-16
 - TCP packet without flags 4-20
- record route IP option 4-13, 4-14
- redistribution 1-A-XII
- redistribution list 1-A-XII

- redundant gateways 5-382–5-400
 - recovery procedure 5-385
 - TCP SYN flag checking 5-388
- regular expressions 4-157–4-159
- rekey option, VPN monitoring 5-308
- Remote authentication dial in user service
 - See RADIUS
- replay protection 5-14
- reset to factory defaults 3-48
- RFCs
 - 1349, "Type of Service in the Internet Protocol Suite" 2-215
 - 1777, "Lightweight Directory Access Protocol" 2-386
 - 1918, "Address Allocation for Private Internets" 2-78
 - 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" 2-215
- RIP
 - authenticating neighbors 6-80
 - configuration steps 6-69
 - creating instance in VR 6-70
 - enabling on interface 6-72
 - filtering neighbors 6-82
 - global parameters 6-76
 - interface parameters 6-78
 - protecting against flooding 6-84
 - protocol overview 6-68
 - redistributing routes 6-73
 - rejecting default routes 6-83
 - security configuration 6-80
- rollback, configuration 2-531–2-532
- route filtering 6-24
- route flap dampening 1-A-XII
- route map 1-A-XII, 6-22
- route metric 6-17
- Route mode 2-118–2-123
 - interface settings 2-119
- route redistribution 1-A-XII, 6-21
- route reflector 1-A-XIII
- route-based VPNs 5-58
- routers, definition 1-A-XIII
- routing 2-30
 - between secondary IP addresses 2-84
 - route preference 6-15

- route selection 6-15
- routing table 1-A-XIII, 2-31
 - route selection 6-15
- RSH ALG 2-140
- RTOs 8-21–8-22
 - operational states 8-22
 - RTO peer 8-24
- rules, derived from policies 2-203
- run-time authentication 2-211, 2-399
- run-time objects
 - See RTOs

S

- SA policy 3-125
- SAs 5-10, 5-11, 5-13
 - check in packet flow 5-62
 - definition 1-A-XIII
- SCEP (Simple Certificate Enrollment Protocol) 5-30
- schedules 2-193, 2-214
- SCREEN
 - address sweep 4-8
 - bad IP options, drop 4-6
 - drop unknown MAC addresses 4-51
 - FIN with no ACK 4-22
 - FIN without ACK flag, drop 4-18
 - ICMP flood 4-59
 - ICMP fragments, block 4-2
 - IP options 4-12
 - IP packet fragments, block 4-10
 - IP spoofing 4-22–4-30
 - Land attack 4-63
 - large ICMP packets, block 4-4
 - loose source route IP option, detect 4-33
 - MGT zone 2-48
 - Ping of Death 4-65
 - port scan 4-10
 - source route IP option, deny 4-33
 - strict source route IP option, detect 4-33
 - SYN and FIN flags set 4-16
 - SYN flood 4-45–4-51
 - SYN fragments, detect 4-12–4-13
 - SYN-ACK-ACK proxy flood 4-43
 - TCP packet without flags, detect 4-20
 - Teardrop 4-67
- UDP flood 4-61
- unknown protocols, drop 4-8
- VLAN and MGT zones 4-3
- WinNuke attack 4-69
- ScreenOS 1-xxii
 - function zones 2-54
 - global zone 2-48
 - Home-Work zone 2-61
 - interfaces physical 2-3
 - overview 2-1–2-27
 - packet flow 2-11–2-13
 - policies 2-3
 - port modes 2-55
 - security zone interfaces 2-3
 - security zones 2-2, 2-48
 - security zones, global 2-2
 - security zones, predefined 2-2
 - subinterfaces 2-4
 - tunnel zones 2-49
 - updating 2-530
 - virtual systems 2-10
 - virtual systems, VRs 7-6
 - virtual systems, zones 7-7
 - zones 2-45–2-54
- SCS 3-29
- SDP 2-159–2-160
- secondary IP addresses 2-84
- secondary path 8-18, 8-25
- Secure Hash Algorithm-1
 - See SHA-1
- Secure Sockets Layer
 - See SSL
- SecurID 2-384–2-385
 - ACE server 2-384
 - auth server object 2-391
 - authentication port 2-385
 - authenticator 2-384
 - client retries 2-385
 - client timeout 2-385
 - duress 2-385
 - encryption type 2-385
 - L2TP 5-276
 - token code 2-384
 - user type support 2-385
- security association
 - See SAs
- Security Associations (SA) 3-124
- security IP option 4-13, 4-14
- security zones 1-A-XIII, 2-2
 - destination zone determination 2-13
 - global 2-2
 - interfaces 2-3, 2-66
 - physical interfaces 2-66
 - predefined 2-2
 - See zones
 - source zone determination 2-12
 - subinterfaces 2-66
- self log 3-77
- serial cables 3-21
- serial interface 8-118
 - failover 8-123
 - ISP configuration 8-121
 - modem configuration 8-119
- service book
 - adding service 2-136
 - custom service 2-134
 - custom service (CLI) 2-136
 - modifying entries (CLI) 2-138
 - modifying entries (Web UI) 2-169
 - pre-configured services 2-134
 - removing entries (CLI) 2-138
 - service groups (Web UI) 2-167
- service groups 2-167–2-170
 - creating 2-168
 - deleting 2-170
 - modifying 2-169
- services 2-134
 - custom 4-152
 - custom ALGs 2-207
 - defined 2-206
 - drop-down list 2-134
 - ICMP 2-139
 - in policies 2-206
 - modifying timeout 2-136
 - timeout threshold 2-135
- session ID 3-5
- Session Initiation Protocol
 - See SIP
- session limits 4-36–4-40
 - destination based 4-37, 4-40
 - source based 4-36, 4-39
- session table flood 4-36

- session timeout
 - HTTP 4-41
 - idle timeout 2-377
 - TCP 4-41
 - UDP 4-41
- settings
 - downloading 2-528
 - importing 2-528
 - saving 2-528
 - uploading 2-528
- SHA-1 5-7
 - definition 1-A-XIII
- shadowed policies 2-242
- SIP 2-156–2-166
 - ALG 2-159, 2-163
 - connection information 2-160
 - defined 2-156
 - inactivity timeouts 2-163
 - media announcements 2-160
 - media inactivity timeout 2-163, 2-166
 - messages 2-156
 - multimedia sessions 2-156
 - pinholes 2-159
 - request method types 2-157
 - Request Methods 2-157
 - response codes 2-158
 - response types 2-157
 - responses 2-157
 - RTCP 2-160
 - RTP 2-160
 - SDP 2-159–2-160
 - session inactivity timeout 2-163
 - signaling 2-159
 - signaling inactivity timeout 2-163, 2-166
- SMTP server IP 3-86
- SNMP 3-29, 3-91
 - cold start trap 3-91
 - community, private 3-95
 - community, public 3-95
 - configuration 3-95
 - encryption 3-94, 3-97
 - implementation 3-94
 - management options 3-29
 - MIB files 3-A-I
 - MIB files, importing 5-325
 - MIB folders, primary 3-A-II
 - system alarm traps 3-91
 - traffic alarm traps 3-91
 - trap types 3-92
 - traps 3-91
 - VPN monitoring 5-325
- SNMP traps
 - 100, hardware problems 3-92
 - 200, firewall problems 3-92
 - 300, software problems 3-92
 - 400, traffic problems 3-92
 - 500, VPN problems 3-92
 - allow or deny 3-94
- software
 - key, vsys 7-15
 - updating 2-530
 - uploading and downloading 2-530
- source route 3-125
- source-based routing 6-17
- SPI
 - definition 1-A-XIII
- SSH 3-11–3-17
 - authentication method priority 3-17
 - automated logins 3-19
 - connection procedure 3-12
 - forcing PKA authentication only 3-17
 - host key 3-12
 - loading public keys, CLI 3-16
 - loading public keys, TFTP 3-16, 3-19
 - loading public keys, WebUI 3-16
 - password authentication 3-15
 - PKA 3-15
 - PKA authentication 3-15
 - PKA key 3-12
 - server key 3-12
 - session key 3-12
- SSL 3-7
 - management options 3-29
 - with WebAuth 2-427
- SSL Handshake Protocol
 - See SSLHP
- SSLHP 3-7
- stateful inspection 4-3
- stateful signatures 4-138
 - definition 4-138
- static routing 1-A-XIV, 2-30, 2-33–2-44
 - configuring 2-38
 - using 2-36
- statistics
 - reporting to NSM 3-27
- stream ID IP option 4-13, 4-14
- strict source route IP option 4-14, 4-31–4-33
- subinterfaces 2-4, 7-23
 - configuring (vsys) 7-23
 - creating (root system) 2-82
 - creating (vsys) 7-23
 - defined 1-A-XIV
 - defining 7-25
 - deleting 2-83
 - multiple subinterfaces per vsys 7-23
- subnet masks
 - definition 1-A-XIV
- subscriptions
 - registration and activation 2-538–2-540
 - temporary service 2-538
- support certificate 2-539, 2-540
- SYN and FIN flags set 4-16
- SYN flood 4-45–4-51
 - alarm threshold 4-49
 - attack 4-45
 - attack threshold 4-49
 - destination threshold 4-50
 - drop unknown MAC addresses 4-51
 - queue size 4-51
 - source threshold 4-50
 - threshold 4-46
 - timeout 4-51
- SYN fragments 4-12–4-13
- SYN-ACK-ACK proxy flood 4-43
- synchronization
 - configuration 8-33
 - files 8-34
 - PKI objects 8-34
 - RTOs 8-34
- syslog 3-66
 - encryption 3-97
 - facility 3-88, 3-90, 3-101, 3-112
 - host 3-87
 - host name 3-88, 3-89, 3-90, 3-101, 3-112

- messages 3-87
- port 3-88, 3-101, 3-112
- security facility 3-88, 3-90, 3-101, 3-112
- system clock 2-541–2-545
 - date & time 2-541
 - sync with client 2-541
 - time zone 2-541
- system, parameters 2-493–2-544

T

- TCP
 - max simultaneous connections 4-94
 - packet without flags 4-20
 - proxy 3-125
 - session timeout 4-41
 - stream signatures 4-164
 - SYN flag checking 5-388
 - three-way handshake 1-A-XV
- TCP/IP, definition 1-A-XV
- Teardrop attack 4-67
- Telnet 3-9, 3-29
- TFTP server 2-528, 2-530
- three-way handshake 1-A-XV, 4-45
- time zone 2-541
- timeout
 - admin user 2-378
 - auth user 2-377
- timestamp IP option 4-14
- token code 2-384
- trace-route 2-98, 2-101
- traffic
 - alarms 3-82–3-86
 - classification, IP-based 7-33
 - classification, VLAN-based 7-21
 - counting 2-213
 - logging 2-213
 - priority 2-215
 - shaping 2-478
 - through traffic, vsys sorting 7-11–7-14
- traffic shaping 1-xxi, 2-477–2-491
 - automatic 2-478
 - interface requirement 2-478
 - service priorities 2-485

- Transparent mode 2-92–2-109
 - ARP/trace-route 2-96
 - blocking non-ARP traffic 2-94
 - blocking non-IP traffic 2-94
 - broadcast traffic 2-94
 - drop unknown MAC addresses 4-51
 - flood 2-96
 - management options 3-30
 - routes 2-94
 - unicast options 2-96
- transport mode 5-4, 5-273, 5-279, 5-286
- Triple DES
 - See 3DES
- trunk ports 7-23
 - defined 7-22
 - definition 1-A-XV
 - manually setting 7-22
- trust 1-A-XV
- tunnel interfaces 2-69
 - definition 1-A-XVI, 2-69
 - policy-based NAT 2-69
- tunnel mode 5-5
- tunnel zones
 - definition 1-A-XVI

U

- UDP
 - checksum 5-303
 - definition 1-A-XVI
 - NAT-T encapsulation 5-301
 - session timeout 4-41
- UDP flood 4-61
- unknown protocols 4-8
- unknown unicast options 2-95–2-101
 - ARP 2-98–2-101
 - flood 2-96–2-97
 - trace-route 2-98, 2-101
- untrust 1-A-XVI
- URL filtering 2-213, 4-113–4-121
 - blocked URL message type 4-117
 - communication timeout 4-116
 - device-level activation 4-117
 - fail/pass mode 4-116
 - NetScreen blocked URL message 4-117
 - policy-level application 4-118

- routing 4-119
- server status 4-118
- servers per vsys 4-115
- Websense server name 4-116
- Websense server port 4-116
- URL, definition 1-A-XVI
- user authentication
 - See authentication, users
- users
 - group IKE ID 5-237–5-258
 - groups, server support 2-372
 - IKE 2-431–2-435
 - IKE, groups 2-434
 - multiple administrative users 3-37
 - shared IKE ID 5-259–5-267
- users, admin 2-465–2-466
 - auth process 2-466
 - timeout 2-378
- users, IKE
 - defining 2-432
 - groups 2-431
 - IKE ID 2-431
- users, L2TP 2-460–2-464
- users, XAuth 2-436–2-458

V

- Valicert 5-36
- vendor-specific attributes
 - See VSAs
- Verisign 5-36
- VIP 2-12
 - bidirectional translation 2-252
 - configuring 2-359
 - custom and multi-port services 2-363–2-369
 - custom services, low port numbers 2-357
 - definition 1-A-XVI, 2-252
 - editing 2-362
 - global zone 2-359
 - reachable from other zones 2-359
 - removing 2-362
 - required information 2-357
 - to zone with interface-based NAT 2-112
 - virtual systems 7-10
- virtual adapter 2-436
 - definition 1-A-XVI

- Virtual HA interface 2-69, 8-47
- Virtual IP
 - See VIP
- virtual private network
 - See VPNs
- virtual routers
 - See VRs
- virtual security device groups
 - See VSD groups
- virtual security interface
 - See VSI
- virtual system 2-10, 7-1–7-39
 - admin types 7-3
 - administrators 3-38
 - admins 7-iii, 7-1
 - basic functional requirements 7-3
 - changing admin's password 7-3, 7-38
 - creating a vsys object 7-3
 - definition 1-A-XVII
 - exporting a physical interface 7-19
 - failover 8-144
 - importing a physical interface 7-18
 - interfaces 7-8
 - IP-based traffic classification 7-33–7-37
 - load sharing 8-144
 - manageability and security 7-34
 - MIP 7-10
 - NSRP 8-144
 - overlapping address ranges 7-25, 7-34
 - overlapping subnets 7-25
 - read-only admins 3-38
 - shared VR 7-15
 - shared zone 7-15
 - software key 7-15
 - traffic sorting 7-10–7-17
 - Transparent mode 7-22
 - VIP 7-10
 - VLAN-based traffic classification 7-21–7-32
 - VRs 7-6
 - zones 7-7
- VLAN zone 2-93
- VLAN1
 - Interface 2-93, 2-102
 - management options 3-30
 - Zones 2-93
- VLANs
 - communicating with another VLAN 7-28–7-32
 - creating 7-25–7-27
 - definition 1-A-XVII
 - subinterfaces 7-23
 - tag 7-23, 7-24
 - tags 1-XIV, 2-4
 - Transparent mode 7-22, 7-23
 - trunking 7-22
 - VLAN-based traffic classification 7-21
- voice-over IP communication 2-141
- VPN monitoring 5-307–5-322
 - destination address 5-308–5-311
 - destination address, XAuth 5-309
 - ICMP echo requests 5-325
 - outgoing interface 5-308–5-311
 - policies 5-310
 - rekey option 5-308, 5-331
 - routing design 5-323
 - SNMP 5-325
 - status changes 5-307, 5-310
- VPNs 1-xxi
 - Aggressive mode 5-12
 - AutoKey IKE 3-51, 3-98, 5-9
 - configuration tips 5-67–5-68
 - cryptographic options 5-40–5-57
 - definition 1-A-XVII
 - Diffie-Hellman exchange 5-13
 - Diffie-Hellman groups 5-13
 - for administrative traffic 3-97
 - FQDN aliases 5-152
 - FQDN for gateway 5-151–5-167
 - idletime 2-439
 - Main mode 5-12
 - Manual Key 3-51, 3-98
 - MIP 5-168
 - multiple tunnels per tunnel interface 5-326–5-381
 - NAT for overlapping addresses 5-168–5-185
 - NAT-dst 5-168
 - NAT-src 5-171
 - packet flow 5-60–5-66
 - Phase 1 5-11
 - Phase 2 5-13
 - policies 2-208
 - proxy IDs, matching 5-67
 - redundant gateways 5-382–5-400
 - redundant groups, recovery procedure 5-385
 - replay protection 5-14
 - route- vs policy-based 5-58
 - SAs 5-10
 - to zone with interface-based NAT 2-112
 - tunnel always up 5-308
 - tunnel zones 2-49
 - tunneling, definition 1-A-XV
 - VPN groups 5-382
 - VPN monitoring and rekey 5-308
- VRRP 8-79, 8-136
- VRs 2-35, 6-3–6-28
 - access lists 6-24
 - BGP 6-91–6-101
 - creating a shared VR 7-16
 - custom 6-7
 - definition 1-A-XVII
 - exporting routes 6-28
 - forwarding traffic between 2-5, 6-4
 - importing routes 6-28
 - introduction 2-5
 - maximum routing table entries 6-14
 - modifying 6-12
 - on vsys 6-9
 - OSPF 6-38–6-65
 - predefined 6-3
 - RIP 6-69–6-86
 - route filtering 6-24
 - route map 6-22
 - route metric 6-17
 - route preference 6-15
 - route redistribution 6-21
 - route selection 6-15
 - router ID 6-12
 - shared 7-15
 - source-based routing 6-17
 - using two VRs 6-3, 6-4
- VSA 2-381
 - attribute name 2-381
 - attribute number 2-381
 - attribute type 2-381
 - vendor ID 2-381

VSD groups 8-5, 8-23–8-27, 8-65–8-67
 failover 8-131
 heartbeats 8-18, 8-25, 8-66
 hold-down time 8-51, 8-55
 member states 8-24, 8-65–8-66, 8-79
 priority numbers 8-23
 VSD, defined 1-A-XVII
VSIs 8-5, 8-23, 8-65
 defined 1-A-XVII
 multiple VSIs per VSD group 8-144
 static routes 8-28

W

Web browser requirements 3-3
Web user interface
 See WebUI
WebAuth 2-372
 external user group 2-423
 local user group 2-420
 pre-policy auth process 2-212, 2-400
 with SSL (external user group) 2-427
Websense 4-113
WebTrends 3-66, 3-89
 encryption 3-89, 3-97
 messages 3-90

WebUI 3-3, 3-30, 3-31
 conventions 1-xxviii, 2-xi, 3-vii, 5-vii, 6-vii,
 7-v, 8-vii
wildcard 5-241
WinNuke attack 4-69
WINS
 definition 1-A-XVII
 L2TP settings 5-276
Work zone 2-61

X

XAuth
 address assignments 2-436, 2-438
 address timeout 2-438
 auth and address 2-452
 client authentication 2-458
 defined 2-436
 external auth server queries 2-437
 external user auth 2-444
 external user group auth 2-447
 IP address lifetime 2-438–2-439
 lifetime 2-439
 local user auth 2-440
 local user group auth 2-442
 query remote settings 2-437

ScreenOS as client 2-458
TCP/IP assignments 2-437
user authentication 2-436
virtual adapter 2-436
VPN idletime 2-439
VPN monitoring 5-309
XAuth users 2-436–2-458
 point of authentication 2-397
 server support 2-372
 with L2TP 2-467

Z

zip files, blocking 4-168
zombie agent 4-35, 4-37
zones 2-45–2-54
 definition 1-A-XVII
 function 2-54
 global 2-48, 2-359
 Layer 2 2-93
 security 1-A-XIII, 2-48
 shared 7-15
 tunnel 1-A-XVI, 2-49
 VLAN 2-54, 2-93
 vsys 7-7

