Concepts & Examples ScreenOS Reference Guide

Volume 1: Overview

Release 5.4.0, Rev. A

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

Part Number: 530-015768-01, Revision A

Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

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

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

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

Disclaimer

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 JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Writers: ScreenOS Team

Editor: Lisa Eldridge

Table of Contents

Volume 1: Overview

About the Concepts & Examples ScreenOS Reference Guide xlix

Volume Organization li
Document Conventions........ lvii
CLI Conventions lviii
Illustration Conventions........ lix
Naming Conventions and Character Types lx
WebUI Conventions........ lx
Juniper Networks Documentation lxi

Appendix A Glossary A-I

Master Index........IX-I

Volume 2: Fundamentals

About This Volume xi

Document Conventions........ xii
CLI Conventions xii
Illustration Conventions........ xiii
Naming Conventions and Character Types xiv
WebUI Conventions........ xiv
Juniper Networks Documentation xv

Chapter 1 ScreenOS Architecture 1

Security Zones 2
Security Zone Interfaces........ 3
Physical Interfaces........ 3
Subinterfaces........ 3
Virtual Routers 4
Policies........ 5
Virtual Private Networks 7
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) Two Routing Domains........ 18
Example: (Part 4) Policies........ 20

Chapter 2 **Zones** 25

Viewing Preconfigured Zones....26
Security Zones....28
Global Zone....28
SCREEN Options....28
Binding a Tunnel Interface to a Tunnel Zone....28
Configuring Security Zones and Tunnel Zones....30
Creating a Zone....30
Modifying a Zone....31
Deleting a Zone....32
Function Zones....32
Null Zone....32
MGT Zone....32
HA Zone....32
Self Zone....33
VLAN Zone....33
Port Modes....33
Trust-Untrust Mode....34
Home-Work Mode....35
Dual Untrust Mode....36
Combined Mode....37
Trust/Untrust/DMZ (Extended) Mode....38
DMZ/Dual Untrust Mode....38
Dual DMZ Mode....39
Setting Port Modes....40
Example: Home-Work Port Mode....40
Zones in Home-Work and Combined Port Modes....41
Example: Home-Work Zones....42

Chapter 3 **Interfaces** 45

Interface Types....45
Logical Interfaces....45
Physical Interfaces....46
Wireless Interfaces....46
Bridge Group Interfaces....46
Subinterfaces....46
Aggregate Interfaces....46
Redundant Interfaces....47
Virtual Security Interfaces....47
Function Zone Interfaces....47
Management Interfaces....47
High Availability Interfaces....48
Tunnel Interfaces....48
Deleting Tunnel Interfaces....51
Viewing Interfaces....52
Configuring Security Zone Interfaces....53
Binding an Interface to a Security Zone....53
Unbinding an Interface from a Security Zone....54
Addressing an L3 Security Zone Interface....55
Public IP Addresses....56
Private IP Addresses....56
Addressing an Interface....57
Modifying Interface Settings....57

Creating a Subinterface in the Root System 58
Deleting a Subinterface 59
Creating a Secondary IP Address 59
Backup System Interfaces 60
Configuring a Backup Interface 61
Configuring an IP Tracking Backup Interface 61
Configuring a Tunnel-if Backup Interface 62
Configuring a Route Monitoring Backup Interface 65
Loopback Interfaces 66
Creating a Loopback Interface 67
Setting the Loopback Interface for Management 68
Setting BGP on a Loopback Interface 68
Setting VSIs on a Loopback Interface 68
Setting the Loopback Interface as a Source Interface 69
Interface State Changes 69
Physical Connection Monitoring 71
Tracking IP Addresses 72
Interface Monitoring 77
Monitoring Two Interfaces 78
Monitoring an Interface Loop 79
Security Zone Monitoring 82
Down Interfaces and Traffic Flow 82
Failure on the Egress Interface 83
Failure on the Ingress Interface 85

Chapter 4 Interface Modes 89

Transparent Mode 90
Zone Settings 91
VLAN Zone 91
Predefined Layer 2 Zones 91
Traffic Forwarding 91
Unknown Unicast Options 92
Flood Method 93
ARP/Trace-Route Method 94
Configuring VLAN1 Interface for Management 97
Configuring Transparent Mode 99
NAT Mode 102
Inbound and Outbound NAT Traffic 104
Interface Settings 105
Configuring NAT Mode 105
Route Mode 108
Interface Settings 109
Configuring Route Mode 109

Chapter 5 Building Blocks for Policies 113

Addresses 114
Address Entries 114
Adding an Address 115
Modifying an Address 115
Deleting an Address 116
Address Groups 116
Creating an Address Group 118
Editing an Address Group Entry 118
Removing a Member and a Group 118
Services 119
Predefined Services 119
Internet Control Messaging Protocol 120
Handling ICMP Unreachable Errors 123
Internet-Related Predefined Services 124
Microsoft Remote Procedure Call Services 125
Dynamic Routing Protocols 127
Streaming Video 128
Sun Remote Procedure Call Services 128
Security and Tunnel Services 129
IP-Related Services 129
Instant Messaging Services 131
Management Services 131
Mail Services 132
UNIX Services 133
Miscellaneous Services 133
Custom Services 134
Adding a Custom Service 134
Modifying a Custom Service 135
Removing a Custom Service 135
Setting a Service Timeout 136
Service Timeout Configuration and Lookup 136
Contingencies 137
Example 138
Defining a Custom Internet Control Message Protocol Service 138
Remote Shell Application-Layer Gateway 139
Sun Remote Procedure Call Application Layer Gateway 139
Typical RPC Call Scenario 140
Customizing Sun RPC Services 140
Customizing Microsoft Remote Procedure Call Application Layer Gateway.. 141
Real-Time Streaming Protocol Application Layer Gateway 142
RTSP Request Methods 143
RTSP Status Codes 145
Configuring a Media Server in a Private Domain 147
Configuring a Media Server in a Public Domain 148
Service Groups 150
Creating a Service Group 151
Modifying a Service Group 151
Removing a Service Group 152

Dynamic IP Pools 152
- Port Address Translation 153
- Creating a DIP Pool with PAT 154
- Modifying a DIP Pool 155
- Sticky DIP Addresses 155
- Using DIP in a Different Subnet 156
- Using a DIP on a Loopback Interface 161
- Creating a DIP Group 165

Setting a Recurring Schedule 168

Chapter 6 Policies 171

Basic Elements 172

Three Types of Policies 173
- Interzone Policies 173
- Intrazone Policies 173
- Global Policies 174

Policy Set Lists 175

Policies Defined 176
- Policies and Rules 176
- Anatomy of a Policy 177
  - ID 178
  - Zones 178
  - Addresses 178
  - Services 178
  - Action 179
  - Application 180
  - Name 180
  - VPN Tunneling 180
  - L2TP Tunneling 181
  - Deep Inspection 181
  - Placement at the Top of the Policy List 181
  - Source Address Translation 181
  - Destination Address Translation 182
  - User Authentication 182
  - HA Session Backup 184
  - Web Filtering 184
  - Logging 184
  - Counting 184
  - Traffic Alarm Threshold 184
  - Schedules 185
  - Antivirus Scanning 185
  - Traffic Shaping 185

Policies Applied ... 186
Viewing Policies ... 186
Creating Policies ... 186
Creating Interzone Policies Mail Service ... 187
Creating an Interzone Policy Set ... 190
Creating Intrazone Policies ... 194
Creating a Global Policy ... 196
Entering a Policy Context ... 197
Multiple Items per Policy Component ... 197
Setting Address Negation ... 198
Modifying and Disabling Policies ... 201
Policy Verification ... 201
Reordering Policies ... 202
Removing a Policy ... 203

Chapter 7 Traffic Shaping 205

Managing Bandwidth at the Policy Level ... 205
Setting Traffic Shaping ... 206
Setting Service Priorities ... 210
Setting Priority Queuing ... 211
Ingress Policing ... 214
Shaping Traffic on Virtual Interfaces ... 215
Interface-Level Traffic Shaping ... 215
Policy-Level Traffic Shaping ... 217
Packet Flow ... 217
Example: Route-Based VPN with Ingress Policing ... 218
Example: Policy-Based VPN with Ingress Policing ... 221
Traffic Shaping Using a Loopback Interface ... 225
DSCP Marking and Shaping ... 225

Chapter 8 System Parameters 229

Domain Name System Support ... 229
DNS Lookup ... 230
DNS Status Table ... 231
Setting the DNS Server and Refresh Schedule ... 231
Setting a DNS Refresh Interval ... 232
Dynamic Domain Name System ... 232
Setting Up DDNS for a DynDNS Server ... 233
Setting up DDNS for DDO Server ... 234
Proxy DNS Address Splitting ... 234
Dynamic Host Configuration Protocol ... 237
Configuring a DHCP Server ... 238
Customizing DHCP Server Options ... 242
Placing the DHCP Server in an NSRP Cluster ... 243
DHCP Server Detection ... 243
Enabling DHCP Server Detection ... 244
Disabling DHCP Server Detection ... 244
Assigning a Security Device as a DHCP Relay Agent ... 245
Forwarding all DHCP Packets ... 249
Configuring Next-Server-IP ... 249
Using a Security Device as a DHCP Client ... 250
Propagating TCP/IP Settings ... 251
Configuring DHCP in Virtual Systems ... 254

Setting DHCP Message Relay in Virtual Systems 254
Point-to-Point Protocol over Ethernet...255
Setting Up PPPoE 256
Configuring PPPoE on Primary and Backup Untrust Interfaces.............259
Configuring Multiple PPPoE Sessions over a Single Interface 260
PPPoE and High Availability 262
License Keys 263
Registration and Activation of Subscription Services 264
Trial Service...264
Updating Subscription Keys 265
Adding Antivirus, Web Filtering, Anti-Spam, and Deep Inspection to an Existing or a New Device 265
System Clock 266
Date and Time..266
Time Zone 266
Network Time Protocol..267
Configuring Multiple NTP Servers...267
Configuring a Backup Network Time Protocol Server 267
Maximum Time Adjustment...268
NTP and NSRP 269
Setting a Maximum Time Adjustment Value to an NTP Server........269
Securing NTP Servers 269

Index...**IX-I**

Volume 3: Administration

About This Volume **vii**

Document Conventions.. vii
CLI Conventions viii
Illustration Conventions.. ix
Naming Conventions and Character Types x
WebUI Conventions..x
Juniper Networks Documentation xi

Chapter 1 **Administration** **1**

Management via the Web User Interface 2
WebUI Help 2
Copying the Help Files to a Local Drive 3
Pointing the WebUI to the New Help Location 3
HyperText Transfer Protocol...4
Session ID..4
Secure Sockets Layer 5
SSL Configuration...7
Redirecting HTTP to SSL 8

Management via the Command Line Interface 9
- Telnet 10
- Securing Telnet Connections 10
- Secure Shell 11
  - Client Requirements 12
  - Basic SSH Configuration on the Device 13
  - Authentication 14
  - SSH and Vsys 16
  - Host Key 16
  - Example: SSHv1 with PKA for Automated Logins 17
- Secure Copy 18
- Serial Console 19
- Modem Port 19

Management via NetScreen-Security Manager 20
- Initiating Connectivity Between NSM Agent and the MGT System 21
- Enabling, Disabling, and Unsetting NSM Agent 22
- Setting the Primary Server IP Address of the Management System 23
- Setting Alarm and Statistics Reporting 23
- Configuration Synchronization 24
  - Example: Viewing the Configuration State 25
  - Example: Retrieving the Configuration Hash 25
- Retrieving the Configuration Timestamp 25

Controlling Administrative Traffic 26
- MGT and VLAN1 Interfaces 27
  - Example: Administration Through the MGT Interface 27
  - Example: Administration Through the VLAN1 Interface 27
- Setting Administrative Interface Options 28
- Setting Manage IPs for Multiple Interfaces 29

Levels of Administration 31
- Root Administrator 31
- Read/Write Administrator 32
- Read-Only Administrator 32
- Virtual System Administrator 32
- Virtual System Read-Only Administrator 33

Defining Admin Users 33
- Example: Adding a Read-Only Admin 33
- Example: Modifying an Admin 33
- Example: Deleting an Admin 34
- Example: Configuring Admin Accounts for Dialup Connections 34
- Example: Clearing an Admin’s Sessions 35

Securing Administrative Traffic 35
- Changing the Port Number 36
- Changing the Admin Login Name and Password 37
  - Example: Changing an Admin User’s Login Name and Password 38
  - Example: Changing Your Own Password 38
  - Setting the Minimum Length of the Root Admin Password 39
- Resetting the Device to the Factory Default Settings 39
- Restricting Administrative Access 40
  - Example: Restricting Administration to a Single Workstation 40
  - Example: Restricting Administration to a Subnet 40
  - Restricting the Root Admin to Console Access 40
- VPN Tunnels for Administrative Traffic 41
  - Administration Through a Route-Based Manual Key VPN Tunnel 42
  - Administration Through a Policy-Based Manual Key VPN Tunnel 45

Password Policy 49
Setting a Password Policy 49
Removing a Password Policy 50
Viewing a Password Policy 50
Recovering from a Rejected Default Admin Password 50

Chapter 2 Monitoring Security Devices 53

Storing Log Information 53
Event Log 54
Viewing the Event Log by Severity Level and Keyword 55
Sorting and Filtering the Event Log 56
Downloading the Event Log 57
Example: Downloading the Entire Event Log 57
Example: Downloading the Event Log for Critical Events 57
Traffic Log 58
Viewing the Traffic Log 59
Example: Viewing Traffic Log Entries 59
Sorting and Filtering the Traffic Log 60
Example: Sorting the Traffic Log by Time 60
Downloading the Traffic Log 60
Removing the Reason for Close Field 61
Self Log 63
Viewing the Self Log 63
Sorting and Filtering the Self Log 63
Example: Filtering the Self Log by Time 64
Downloading the Self Log 64
Downloading the Asset Recovery Log 65
Traffic Alarms 65
Example: Policy-Based Intrusion Detection 66
Example: Compromised System Notification 67
Example: Sending E-mail Alerts 67
Syslog 68
Example: Enabling Multiple Syslog Servers 69
Enabling WebTrends for Notification Events 69
Simple Network Management Protocol 70
Implementation Overview 73
Defining a Read/Write SNMP Community 74
VPN Tunnels for Self-Initiated Traffic 75
Example: Self-Generated Traffic Through a Route-Based Tunnel 76
Example: Self-Generated Traffic Through a Policy-Based Tunnel 83
Viewing Screen Counters 89

Index .... IX-I

Volume 4: Attack Detection and Defense Mechanisms

About This Volume ix

Document Conventions x
CLI Conventions xi
Illustration Conventions xii
Naming Conventions and Character Types xiii
WebUI Conventions xiv
Juniper Networks Documentation xiv

Chapter 1 Protecting a Network 1

Stages of an Attack 2
Detection and Defense Mechanisms 2
Exploit Monitoring 5
Example: Monitoring Attacks from the Untrust Zone 5

Chapter 2 Reconnaissance Deterrence 7

IP Address Sweep 8
Port Scanning 9
Network Reconnaissance Using IP Options 10
Operating System Probes 12
SYN and FIN Flags Set 12
FIN Flag Without ACK Flag 13
TCP Header Without Flags Set 14
Evasion Techniques 15
FIN Scan 15
Non-SYN Flags 15
IP Spoofing 18
Example: L3 IP Spoof Protection 20
Example: L2 IP Spoof Protection 22
IP Source Route Options 23

Chapter 3 Denial-of-Service (DoS) Attack Defenses 27

Firewall DoS Attacks 28
Session Table Flood 28
Source-Based and Destination-Based Session Limits 28
Example: Source-Based Session Limiting 29
Example: Destination-Based Session Limiting 30
Aggressive Aging 30
Example: Aggressively Aging Out Sessions 32
SYN-ACK-ACK Proxy Flood 32
Network DoS Attacks 34
SYN Flood 34
Example: SYN Flood Protection 40
SYN Cookie 44
ICMP Flood 46
UDP Flood 47
Land Attack 48

OS-Specific DoS Attacks 49
Ping of Death 49
Teardrop Attack 50
WinNuke 51

Chapter 4 Content Monitoring and Filtering 53

Fragment Reassembly 54
Malicious URL Protection 54
Application Layer Gateway 55
Example: Blocking Malicious URLs in Packet Fragments 56
Antivirus Scanning 58
External AV Scanning 58
Scanning Modes 60
Load-Balancing ICAP Scan Servers 60
Internal AV Scanning 61
AV Scanning Results 62
Policy-Based AV Scanning 63
Scanning Application Protocols 64
Scanning FTP Traffic 65
Scanning HTTP Traffic 66
Scanning IMAP and POP3 Traffic 69
Scanning SMTP Traffic 71
Redirecting Traffic to ICAP AV Scan Servers 73
Updating the AV Pattern Files for the Embedded Scanner 74
Subscribing to the AV Signature Service 74
Updating AV Patterns 75
AV Scanner Global Settings 77
AV Resource Allotment 77
Fail-Mode Behavior 77
Maximum Content Size and Maximum Messages (Internal AV Only) 78
HTTP Keep-Alive 79
HTTP Trickling (Internal AV Only) 79
AV Scanner Profile Settings 81
Initiating an AV Profile for Internal AV 81
Example: (Internal AV) Scanning for All Traffic Types 82
Example: AV Scanning for SMTP and HTTP Traffic Only 82
AV Profile Settings 84
Anti-Spam Filtering 87
Black Lists and White Lists 88
Basic Configuration 88
Filtering Spam Traffic 88
Dropping Spam Messages 89
Defining a Black List 89
Defining a White List 89
Defining a Default Action 90
Enabling a Spam-Blocking List Server 90

Web Filtering 91
Using the CLI to Initiate Web-Filtering Modes 91
Integrated Web Filtering...92
SurfControl Servers 93
Web-Filtering Cache...93
Configuring Integrated Web Filtering 94
Example: Integrated Web Filtering...99
Redirect Web Filtering..101
Virtual System Support...102
Configuring Redirect Web Filtering 103
Example: Redirect Web Filtering..106

Chapter 5 Deep Inspection 109

Overview 110
Attack Object Database Server 114
Predefined Signature Packs 114
Updating Signature Packs 115
Before You Start Updating Attack Objects 116
Immediate Update 116
Automatic Update 117
Automatic Notification and Immediate Update 118
Manual Update..119
Attack Objects and Groups...121
Supported Protocols 123
Stateful Signatures..126
TCP Stream Signatures 127
Protocol Anomalies...128
Attack Object Groups..128
Changing Severity Levels..128
Example: Deep Inspection for P2P 130
Disabling Attack Objects...131
Attack Actions..132
Example: Attack Actions—Close Server, Close, Close Client...........134
Brute Force Attack Actions 140
Brute Force Attack Objects...140
Brute Force Attack Target...141
Brute Force Attack Timeout..141
Example 1 142
Example 2..142
Example 3..142
Attack Logging 143
Example: Disabling Logging per Attack Group................................143
Mapping Custom Services to Applications 145
Example: Mapping an Application to a Custom Service..................146
Example: Application-to-Service Mapping for HTTP Attacks...........148
Customized Attack Objects and Groups..149
User-Defined Stateful Signature Attack Objects.....................................149
Regular Expressions...150
Example: User-Defined Stateful Signature Attack Objects 151
TCP Stream Signature Attack Objects 153
Example: User-Defined Stream Signature Attack Object.................154
Configurable Protocol Anomaly Parameters 155
Example: Modifying Parameters 155

Negation 156
Example: Attack Object Negation 156
Granular Blocking of HTTP Components 160
ActiveX Controls 161
Java Applets 161
EXE Files 161
ZIP Files 161
Example: Blocking Java Applets and .exe Files 162

Chapter 6 Intrusion Detection and Prevention 163

IDP-Capable Security Devices 164
Configuring Basic Intrusion Detection and Prevention 165
Preconfiguration Tasks 165
Example 1: Basic IDP Configuration 166
Example 2: Configuring IDP for Active–Passive Failover 168
Example 3: Configuring IDP for Active–Active Failover 170
Configuring Security Policies 173
About Security Policies 173
Managing Security Policies 173
Installing Security Policies 174
Using IDP Rulebases 174
Role-Based Administration of IDP Rulebases 175
Configuring Objects for IDP Rules 175
Using Security Policy Templates 176
Enabling IDP in Firewall Rules 177
Enabling IDP 178
Specifying Inline or Inline Tap Mode 178
Configuring IDP Rules 178
Adding the IDP Rulebase 179
Matching Traffic 180
Source and Destination Zones 181
Source and Destination Address Objects 181
Example: Setting Source and Destination 181
Example: Setting Multiple Sources and Destinations 182
Services 182
Example: Setting Default Services 183
Example: Setting Specific Services 183
Example: Setting Nonstandard Services 183
Terminal Rules 185
Example: Setting Terminal Rules 185
Defining Actions 187
Setting Attack Objects 187
Adding Attack Objects Individually 188
Adding Attack Objects by Category 188
Example: Adding Attack Objects by Service 188
Adding Attack Objects by Operating System 188
Adding Attack Objects by Severity 188
Setting IP Action 189
Choosing an IP Action 189
Choosing a Blocking Option 190
Setting Logging Options 190
Setting Timeout Options 190
Setting Notification 190
Setting Logging 190

- Setting an Alert 191
- Logging Packets 191
- Setting Severity........ 191
- Setting Targets........ 191
- Entering Comments........ 192
- Configuring Exempt Rules........ 192
- Adding the Exempt Rulebase........ 193
- Defining a Match 194
- Source and Destination Zones........ 194
- Source and Destination Address Objects........ 194
- Example: Exempting a Source/Destination Pair 195
- Setting Attack Objects........ 195
- Example: Exempting Specific Attack Objects 195
- Setting Targets........ 195
- Entering Comments........ 196
- Creating an Exempt Rule from the Log Viewer 196
- Configuring Backdoor Rules 197
- Adding the Backdoor Rulebase 197
- Defining a Match 198
- Source and Destination Zones........ 198
- Source and Destination Address Objects........ 199
- Services........ 199
- Setting the Operation 199
- Setting Actions........ 199
- Setting Notification 200
- Setting Logging 200
- Setting an Alert 200
- Logging Packets 200
- Setting Severity........ 201
- Setting Targets........ 201
- Entering Comments........ 201
- Configuring IDP Attack Objects 201
- About IDP Attack Object Types........ 201
- Signature Attack Objects 202
- Protocol Anomaly Attack Objects 202
- Compound Attack Objects........ 202
- Viewing Predefined IDP Attack Objects and Groups 202
- Viewing Predefined Attacks........ 203
- Viewing Predefined Groups 203
- Creating Custom IDP Attack Objects........ 204
- Creating a Signature Attack Object 205
- Creating a Protocol Anomaly Attack........ 211
- Creating a Compound Attack 212
- Editing a Custom Attack Object........ 214
- Deleting a Custom Attack Object........ 214
- Creating Custom IDP Attack Groups 215
- Configuring Static Groups........ 215
- Configuring Dynamic Groups 216
- Example: Creating a Dynamic Group 217
- Updating Dynamic Groups 218
- Editing a Custom Attack Group 219
- Deleting a Custom Attack Group 219

Configuring the Device as a Standalone IDP Device 219
Enabling IDP..219
Example: Configuring a Firewall Rule for Standalone IDP 220
Configuring Role-Based Administration 220
Example: Configuring an IDP-Only Administrator 221
Managing IDP 222
About Attack Database Updates..222
Downloading Attack Database Updates 222
Using Updated Attack Objects 223
Updating the IDP Engine 223
Viewing IDP Logs..225

Chapter 7 Suspicious Packet Attributes 227

ICMP Fragments 228
Large ICMP Packets...229
Bad IP Options 230
Unknown Protocols..231
IP Packet Fragments 232
SYN Fragments 233

Appendix A Contexts for User-Defined Signatures A-I

Index...IX-I

Volume 5: Virtual Private Networks

About This Volume vii

Document Conventions.. viii
CLI Conventions viii
Illustration Conventions..ix
Naming Conventions and Character Types x
WebUI Conventions..x
Juniper Networks Documentation xi

Chapter 1 Internet Protocol Security 1

Introduction to Virtual Private Networks 2
IPSec Concepts 3
Modes...4
Transport Mode 4
Tunnel Mode...4
Protocols 5
Authentication Header 6
Encapsulating Security Payload...6
Key Management 7
Manual Key...7
AutoKey IKE...7
Security Associations 8

Tunnel Negotiation 8
  Phase 1 9
    Main and Aggressive Modes 9
    Diffie-Hellman Exchange 10
  Phase 2 11
    Perfect Forward Secrecy 11
    Replay Protection 12
IKE and IPSec Packets 12
  IKE Packets 12
  IPSec Packets 15

Chapter 2 Public Key Cryptography 19

Introduction to Public Key Cryptography 20
  Signing a Certificate 20
  Verifying a Digital Signature 20
Public Key Infrastructure 22
Certificates and CRLs 24
  Requesting a Certificate Manually 26
  Loading Certificates and Certificate Revocation Lists 28
  Configuring CRL Settings 29
  Obtaining a Local Certificate Automatically 30
  Automatic Certificate Renewal 33
  Key-Pair Generation 34
Online Certificate Status Protocol 34
  Specifying a Certificate Revocation Check Method 35
  Viewing Status Check Attributes 36
  Specifying an Online Certificate Status Protocol Responder URL 36
  Removing Status Check Attributes 36
Self-Signed Certificates 37
  Certificate Validation 38
  Manually Creating Self-Signed Certificates 39
  Setting an Admin-Defined Self-Signed Certificate 40
  Certificate Auto-Generation 44
  Deleting Self-Signed Certificates 45

Chapter 3 Virtual Private Network Guidelines 47

Cryptographic Options 48
  Site-to-Site Cryptographic Options 48
  Dialup VPN Options 55
Route-Based and Policy-Based Tunnels 62
Packet Flow: Site-to-Site VPN 63
Tunnel Configuration Guidelines 69
Route-Based Virtual Private Network Security Considerations 71
  Null Route 72
  Dialup or Leased Line 73
  VPN Failover to Leased Line or Null Route 74
  Decoy Tunnel Interface 76
  Virtual Router for Tunnel Interfaces 77
  Reroute to Another Tunnel 77

Chapter 4 Site-to-Site Virtual Private Networks 79

Site-to-Site VPN Configurations 80
Route-Based Site-to-Site VPN, AutoKey IKE 86
Policy-Based Site-to-Site VPN, AutoKey IKE 95
Route-Based Site-to-Site VPN, Dynamic Peer 101
Policy-Based Site-to-Site VPN, Dynamic Peer 109
Route-Based Site-to-Site VPN, Manual Key 117
Policy-Based Site-to-Site VPN, Manual Key 124
Dynamic IKE Gateways Using FQDN 129
Aliases 130
Setting AutoKey IKE Peer with FQDN 130
VPN Sites with Overlapping Addresses 139
Transparent Mode VPN 149

Chapter 5 Dialup Virtual Private Networks 157

Dialup 158
Policy-Based Dialup VPN, AutoKey IKE 158
Route-Based Dialup VPN, Dynamic Peer 164
Policy-Based Dialup VPN, Dynamic Peer 171
Bidirectional Policies for Dialup VPN Users 176
Group IKE ID 181
Group IKE ID with Certificates 181
Wildcard and Container ASN1-DN IKE ID Types 183
Creating a Group IKE ID (Certificates) 185
Setting a Group IKE ID with Preshared Keys 190
Shared IKE ID 196

Chapter 6 Layer 2 Tunneling Protocol 203

Introduction to L2TP 203
Packet Encapsulation and Decapsulation 206
Encapsulation 206
Decapsulation 207
Setting L2TP Parameters 209
L2TP and L2TP-over-IPSec 211
Configuring L2TP 211
Configuring L2TP-over-IPSec 216
Bidirectional L2TP-over-IPSec 223

Chapter 7 Advanced Virtual Private Network Features 229

NAT-Traversal 230
Probing for NAT 231
Traversing a NAT Device 233
UDP Checksum 235
Keepalive Packets 235
Initiator/Responder Symmetry 235
Enabling NAT-Traversal 237
VPN Monitoring 238
Rekey and Optimization Options 239
Source Interface and Destination Address 240
Policy Considerations 241
Configuring the VPN Monitoring Feature 241
SNMP VPN Monitoring Objects and Traps 249

Multiple Tunnels per Tunnel Interface 251
Route-to-Tunnel Mapping 252
Remote Peers' Addresses 253
Manual and Automatic Table Entries 254
Manual Table Entries 254
Automatic Table Entries 254
Setting VPNs on a Tunnel Interface to Overlapping Subnets 256
Binding Automatic Route and NHTB Table Entries 274
Using OSPF for Automatic Route Table Entries 286
Redundant VPN Gateways 287
VPN Groups 288
Monitoring Mechanisms 289
IKE Heartbeats 290
Dead Peer Detection 290
IKE Recovery Procedure 292
TCP SYN-Flag Checking 293
Creating Redundant VPN Gateways 294
Creating Back-to-Back VPNs 300
Creating Hub-and-Spoke VPNs 307

Index .... IX-I

Volume 6: Voice-over-Internet Protocol

About This Volume v

Document Conventions vi
CLI Conventions vi
Illustration Conventions vii
Naming Conventions and Character Types viii
WebUI Conventions viii
Juniper Networks Documentation ix

Chapter 1 H.323 Application Layer Gateway 1

Overview 1
Examples 2
Example: Gatekeeper in the Trust Zone 2
Example: Gatekeeper in the Untrust Zone 3
Example: Outgoing Calls with NAT 4
Example: Incoming Calls with NAT 7
Example: Gatekeeper in the Untrust Zone with NAT 10

Chapter 2 Session Initiation Protocol Application Layer Gateway 13

Overview 13
- SIP Request Methods 14
- Classes of SIP Responses 16
- ALG—Application-Layer Gateway 17
- SDP 18
- Pinhole Creation 19
- Session Inactivity Timeout 20
- SIP Attack Protection 21
  - Example: SIP Protect Deny 21
  - Example: Signaling-Inactivity and Media-Inactivity Timeouts 22
  - Example: UDP Flooding Protection 22
  - Example: SIP Connection Maximum 23

SIP with Network Address Translation 23
- Outgoing Calls 24
- Incoming Calls 24
- Forwarded Calls 25
- Call Termination 25
- Call Re-INVITE Messages 25
- Call Session Timers 25
- Call Cancellation 26
- Forking 26
- SIP Messages 26
- SIP Headers 26
- SIP Body 28
- SIP NAT Scenario 28

Examples 30
- Incoming SIP Call Support Using the SIP Registrar 31
  - Example: Incoming Call (Interface DIP) 32
  - Example: Incoming Call (DIP Pool) 35
  - Example: Incoming Call with MIP 37
  - Example: Proxy in the Private Zone 39
  - Example: Proxy in the Public Zone 41
  - Example: Three-Zone, Proxy in the DMZ 44
  - Example: Untrust Intrazone 47
  - Example: Trust Intrazone 51
  - Example: Full-Mesh VPN for SIP 53
- Bandwidth Management for VoIP Services 62

Chapter 3 Media Gateway Control Protocol Application Layer Gateway 65

Overview 65

MGCP Security 66

About MGCP 66
- Entities in MGCP 66
  - Endpoint 67
  - Connection 67
  - Call 67
  - Call Agent 67
- Commands 68
- Response Codes 70

Examples 71
- Media Gateway in Subscribers' Homes—Call Agent at the ISP 71
- ISP-Hosted Service 74

Chapter 4 **Skinny Client Control Protocol Application Layer Gateway** 79

Overview ... 79
SCCP Security ... 80
About SCCP ... 81
SCCP Components ... 81
SCCP Client ... 81
Call Manager ... 81
Cluster ... 81
SCCP Transactions ... 82
Client Initialization ... 82
Client Registration ... 82
Call Setup ... 83
Media Setup ... 83
SCCP Control Messages and RTP Flow ... 84
SCCP Messages ... 85
Examples ... 85
Example: Call Manager/TFTP Server in the Trust Zone ... 86
Example: Call Manager/TFTP Server in the Untrust Zone ... 88
Example: Three-Zone, Call Manager/TFTP Server in the DMZ ... 90
Example: Intrazone, Call Manager/TFTP Server in Trust Zone ... 93
Example: Intrazone, Call Manager/TFTP Server in Untrust Zone ... 97
Example: Full-Mesh VPN for SCCP ... 99

Index ... IX-I

Volume 7: Routing

About This Volume ix

Document Conventions ... x
CLI Conventions ... x
Illustration Conventions ... xi
Naming Conventions and Character Types ... xii
WebUI Conventions ... xii
Juniper Networks Documentation ... xiii

Chapter 1 **Static Routing** 1

Overview ... 2
How Static Routing Works ... 2
When to Configure Static Routes ... 3
Configuring Static Routes ... 5
Setting Static Routes ... 5
Setting a Static Route for a Tunnel Interface ... 9
Enabling Gateway Tracking ... 10
Forwarding Traffic to the Null Interface ... 11
Preventing Route Lookup in Other Routing Tables ... 11
Preventing Tunnel Traffic from Being Sent on Non-Tunnel Interfaces ... 11
Preventing Loops Created by Summarized Routes ... 11
Permanently Active Routes ... 12
Changing Routing Preference with Equal Cost Multipath ... 12

Chapter 2 Routing 13

Overview 14
Virtual Router Routing Tables 15
Destination-Based Routing Table 16
Source-Based Routing Table 17
Source Interface-Based Routing Table 19
Creating and Modifying Virtual Routers 21
Modifying Virtual Routers 21
Assigning a Virtual Router ID 22
Forwarding Traffic Between Virtual Routers 23
Configuring Two Virtual Routers 23
Creating and Deleting Virtual Routers 25
Creating a Custom Virtual Router 26
Deleting a Custom Virtual Router 26
Virtual Routers and Virtual Systems 26
Creating a Virtual Router in a Vsys 27
Sharing Routes Between Virtual Routers 28
Limiting the Number of Routing Table Entries 29
Routing Features and Examples 30
Route Selection 30
Setting a Route Preference 30
Route Metrics 31
Changing the Default Route Lookup Sequence 32
Route Lookup in Multiple Virtual Routers 34
Configuring Equal Cost Multipath Routing 35
Route Redistribution 37
Configuring a Route Map 38
Route Filtering 39
Configuring an Access List 40
Redistributing Routes into OSPF 40
Exporting and Importing Routes Between Virtual Routers 42
Configuring an Export Rule 42
Configuring Automatic Export 43

Chapter 3 Open Shortest Path First 45

Overview 46
Areas 46
Router Classification 47
Hello Protocol 47
Network Types 48
Broadcast Networks 48
Point-to-Point Networks 48
Point-to-Multipoint Networks 48
Link-State Advertisements 49

Basic OSPF Configuration 49
Creating and Removing an OSPF Routing Instance 50
Creating an OSPF Instance 50
Removing an OSPF Instance 51
Creating and Deleting an OSPF Area 51
Creating an OSPF Area 52
Deleting an OSPF Area 52
Assigning Interfaces to an OSPF Area 53
Assigning Interfaces to Areas 53
Configuring an Area Range 53
Enabling OSPF on Interfaces 54
Enabling OSPF on Interfaces 54
Disabling OSPF on an Interface 54
Verifying the Configuration 55
Redistributing Routes into Routing Protocols 56
Summarizing Redistributed Routes 57
Summarizing Redistributed Routes 58
Global OSPF Parameters 58
Advertising the Default Route 59
Virtual Links 59
Creating a Virtual Link 60
Creating an Automatic Virtual Link 61
Setting OSPF Interface Parameters 62
Security Configuration 64
Authenticating Neighbors 64
Configuring a Clear-Text Password 64
Configuring an MD5 Password 64
Configuring an OSPF Neighbor List 65
Rejecting Default Routes 66
Protecting Against Flooding 66
Configuring the Hello Threshold 66
Configuring the LSA Threshold 67
Enabling Reduced Flooding 67
Creating an OSPF Demand Circuit on a Tunnel Interface 67
Point-to-Multipoint Tunnel Interface 68
Setting the OSPF Link-Type 68
Disabling the Route-Deny Restriction 69
Creating a Point-to-Multipoint Network 69

Chapter 4 Routing Information Protocol 73

Overview 74
Basic RIP Configuration 75
Creating and Deleting a RIP Instance 76
Creating a RIP Instance 76
Deleting a RIP Instance 76
Enabling and Disabling RIP on Interfaces 77
Enabling RIP on an Interface 77
Disabling RIP on an Interface 77
Redistributing Routes 77
Viewing RIP Information 79
Viewing the RIP Database 79
Viewing RIP Details 80
Viewing RIP Neighbor Information 81
Viewing RIP Details for a Specific Interface 82

Global RIP Parameters 83
Advertising the Default Route 84
Configuring RIP Interface Parameters 85
Security Configuration 86
Authenticating Neighbors by Setting a Password 86
Configuring Trusted Neighbors 87
Rejecting Default Routes 88
Protecting Against Flooding 88
Configuring an Update Threshold 89
Enabling RIP on Tunnel Interfaces 89
Optional RIP Configurations 90
Setting the RIP Version 90
Enabling and Disabling a Prefix Summary 92
Enabling a Prefix Summary 92
Disabling a Prefix Summary 93
Setting Alternate Routes 93
Demand Circuits on Tunnel Interfaces 94
Configuring a Static Neighbor 96
Configuring a Point-to-Multipoint Tunnel Interface 97

Chapter 5 Border Gateway Protocol 103

Overview 104
Types of BGP Messages 104
Path Attributes 105
External and Internal BGP 105
Basic BGP Configuration 106
Creating and Enabling a BGP Instance 107
Creating a BGP Routing Instance 107
Removing a BGP Instance 108
Enabling and Disabling BGP on Interfaces 108
Enabling BGP on Interfaces 108
Disabling BGP on Interfaces 108
Configuring BGP Peers and Peer Groups 109
Configuring a BGP Peer 110
Configuring an IBGP Peer Group 110
Verifying the BGP Configuration 112
Security Configuration 113
Authenticating BGP Neighbors 113
Rejecting Default Routes 114

Optional BGP Configurations..115
Redistributing Routes into BGP 116
Configuring an AS-Path Access List...116
Adding Routes to BGP...117
Conditional Route Advertisement...118
Setting the Route Weight..118
Setting Route Attributes 119
Route-Refresh Capability 119
Requesting an Inbound Routing Table Update 120
Requesting an Outbound Routing Table Update.............................120
Configuring Route Reflection 120
Configuring a Confederation...122
BGP Communities 124
Route Aggregation 125
Aggregating Routes with Different AS-Paths...................................125
Suppressing More-Specific Routes in Updates 126
Selecting Routes for Path Attribute...127
Changing Attributes of an Aggregated Route 128

Chapter 6 Policy-Based Routing 129

Policy-Based Routing Overview..130
Extended Access-Lists...130
Match Groups 130
Action Groups...131
Route Lookup with Policy-Based Routing 132
Configuring Policy-Based Routing 132
Configuring an Extended Access List 133
Configuring a Match Group...134
Configuring an Action Group 135
Configuring a PBR Policy 136
Binding a Policy-Based Routing Policy 136
Binding a Policy-Based Routing Policy to an Interface....................136
Binding a Policy-Based Routing Policy to a Zone............................136
Binding a Policy-Based Routing Policy to a Virtual Router 137
Viewing Policy-Based Routing Output 137
Viewing an Extended Access List..137
Viewing a Match Group...138
Viewing an Action Group 138
Viewing a Policy-Based Routing Policy Configuration 139
Viewing a Complete Policy-Based Routing Configuration.......................139
Advanced PBR Example...140
Routing...141
PBR Elements..142
Extended Access Lists 143
Match Groups...143
Action Group..143
PBR Policies 144
Interface Binding...144
Advanced PBR with High Availability and Scalability...................................145
Resilient PBR Solution 145
Scalable PBR Solution 145

Chapter 7 **Multicast Routing** 147

Overview 147
Multicast Addresses 148
Reverse Path Forwarding 148
Multicast Routing on Security Devices 149
Multicast Routing Table 149
Configuring a Static Multicast Route 150
Access Lists 151
Configuring Generic Routing Encapsulation on Tunnel Interfaces 151
Multicast Policies 153

Chapter 8 **Internet Group Management Protocol** 155

Overview 156
Hosts 156
Multicast Routers 157
IGMP on Security Devices 157
Enabling and Disabling IGMP on Interfaces 157
Enabling IGMP on an Interface 158
Disabling IGMP on an Interface 158
Configuring an Access List for Accepted Groups 158
Configuring IGMP 159
Verifying an IGMP Configuration 161
IGMP Operational Parameters 162
IGMP Proxy 163
Membership Reports Upstream to the Source 164
Multicast Data Downstream to Receivers 165
Configuring IGMP Proxy 166
Configuring IGMP Proxy on an Interface 166
Multicast Policies for IGMP and IGMP Proxy Configurations 168
Creating a Multicast Group Policy for IGMP 168
Creating an IGMP Proxy Configuration 168
Setting Up an IGMP Sender Proxy 175

Chapter 9 **Protocol Independent Multicast** 181

Overview 182
PIM-SM 183
Multicast Distribution Trees 183
Designated Router 184
Mapping Rendezvous Points to Groups 184
Forwarding Traffic on the Distribution Tree 185
PIM-SSM 187
Configuring PIM-SM on Security Devices 187
Enabling and Deleting a PIM-SM Instance for a VR 188
Enabling PIM-SM Instance 188
Deleting a PIM-SM Instance 188
Enabling and Disabling PIM-SM on Interfaces 189
Enabling PIM-SM on an Interface 189
Disabling PIM-SM on an Interface 189
Multicast Group Policies 189
Static-RP-BSR Messages 190
Join-Prune Messages 190
Defining a Multicast Group Policy for PIM-SM 190
Setting a Basic PIM-SM Configuration 191

Verifying the Configuration 195
Configuring Rendezvous Points 197
Configuring a Static Rendezvous Point 197
Configuring a Candidate Rendezvous Point 198
Security Considerations 199
Restricting Multicast Groups 199
Restricting Multicast Sources 200
Restricting Rendezvous Points 201
PIM-SM Interface Parameters 202
Defining a Neighbor Policy 202
Defining a Bootstrap Border 203
Configuring a Proxy Rendezvous Point 204
PIM-SM and IGMPv3 213

Chapter 10 ICMP Router Discovery Protocol 215

Overview 215
Configuring ICMP Router Discovery Protocol 215
Enabling ICMP Router Discovery Protocol 216
Configuring ICMP Router Discovery Protocol from the WebUI 216
Configuring ICMP Router Discovery Protocol from the CLI 217
Advertising an Interface 217
Broadcasting the Address 217
Setting a Maximum Advertisement Interval 217
Setting a Minimum Advertisement Interval 217
Setting an Advertisement Lifetime Value 218
Setting a Response Delay 218
Setting an Initial Advertisement Interval 218
Setting a Number of Initial Advertisement Packets 218
Disabling IRDP 219
Viewing IRDP Settings 219

Index .... IX-I

Volume 8: Address Translation

About This Volume v

Document Conventions vi
CLI Conventions vi
Illustration Conventions vii
Naming Conventions and Character Types viii
WebUI Conventions viii
Juniper Networks Documentation ix

Chapter 1 Address Translation 1

Introduction to Address Translation 1
Source Network Address Translation 1
Destination Network Address Translation 3
Policy-Based NAT-Dst 4
Mapped IP 6
Virtual IP 6
Policy-Based Translation Options 7
Example: NAT-Src from a DIP Pool with PAT 7
Example: NAT-Src From a DIP Pool Without PAT 7
Example: NAT-Src from a DIP Pool with Address Shifting 8
Example: NAT-Src from the Egress Interface IP Address 8
Example: NAT-Dst to a Single IP Address with Port Mapping 8
Example: NAT-Dst to a Single IP Address Without Port Mapping 9
Example: NAT-Dst from an IP Address Range to a Single IP Address 9
Example: NAT-Dst Between IP Address Ranges 10
Directional Nature of NAT-Src and NAT-Dst 10

Chapter 2 Source Network Address Translation 13

Introduction to NAT-Src 13
NAT-Src from a DIP Pool with PAT Enabled 15
Example: NAT-Src with PAT Enabled 15
NAT-Src from a DIP Pool with PAT Disabled 18
Example: NAT-Src with PAT Disabled 18
NAT-Src from a DIP Pool with Address Shifting 20
Example: NAT-Src with Address Shifting 21
NAT-Src from the Egress Interface IP Address 24
Example: NAT-Src Without DIP 24

Chapter 3 Destination Network Address Translation 27

Introduction to NAT-Dst 28
Packet Flow for NAT-Dst 29
Routing for NAT-Dst 32
Example: Addresses Connected to One Interface 33
Example: Addresses Connected to One Interface But Separated by a Router 34
Example: Addresses Separated by an Interface 34
NAT-Dst—One-to-One Mapping 35
Example: One-to-One Destination Translation 36
Translating from One Address to Multiple Addresses 38
Example: One-to-Many Destination Translation 38
NAT-Dst—Many-to-One Mapping 41
Example: Many-to-One Destination Translation 41
NAT-Dst—Many-to-Many Mapping 44
Example: Many-to-Many Destination Translation 45
NAT-Dst with Port Mapping 47
Example: NAT-Dst with Port Mapping 47
NAT-Src and NAT-Dst in the Same Policy 50
Example: NAT-Src and NAT-Dst Combined 50

Chapter 4 Mapped and Virtual Addresses 63

Mapped IP Addresses....................63
MIP and the Global Zone....................64
Example: MIP on an Untrust Zone Interface....................65
Example: Reaching a MIP from Different Zones....................67
Example: Adding a MIP to a Tunnel Interface....................70
MIP-Same-as-Untrust....................70
Example: MIP on the Untrust Interface....................71
MIP and the Loopback Interface....................73
Example: MIP for Two Tunnel Interfaces....................74
MIP Grouping....................79
Example: MIP Grouping with Multi-Cell Policy....................79
Virtual IP Addresses....................80
VIP and the Global Zone....................82
Example: Configuring Virtual IP Servers....................82
Example: Editing a VIP Configuration....................84
Example: Removing a VIP Configuration....................84
Example: VIP with Custom and Multiple-Port Services....................85

Index....................IX-I

Volume 9: User Authentication

About This Volume vii

Document Conventions....................viii
CLI Conventions....................viii
Illustration Conventions....................ix
Naming Conventions and Character Types....................x
WebUI Conventions....................x
Juniper Networks Documentation....................xi

Chapter 1 Authentication 1

User Authentication Types....................1
Admin Users....................2
Multiple-Type Users....................4
Group Expressions....................5
Example: Group Expressions (AND)....................6
Example: Group Expressions (OR)....................7
Example: Group Expressions (NOT)....................9
Banner Customization....................10
Example: Customizing a WebAuth Banner....................10

Chapter 2 **Authentication Servers** 11

Authentication Server Types ... 11
Local Database ... 13
Example: Local Database Timeout ... 14
External Authentication Servers ... 15
Auth Server Object Properties ... 16
Auth Server Types ... 17
Remote Authentication Dial-In User Service ... 17
RADIUS Auth Server Object Properties ... 18
Supported User Types and Features ... 18
RADIUS Dictionary File ... 18
RADIUS Access Challenge ... 20
RADIUS Accounting ... 21
SecurID ... 23
SecurID Auth Server Object Properties ... 23
Supported User Types and Features ... 24
Lightweight Directory Access Protocol ... 24
LDAP Auth Server Object Properties ... 25
Supported User Types and Features ... 25
Defining Auth Server Objects ... 26
Example: RADIUS Auth Server ... 26
Example: SecurID Auth Server ... 28
Example: LDAP Auth Server ... 29
Defining Default Auth Servers ... 31
Example: Changing Default Auth Servers ... 31

Chapter 3 **Infranet Authentication** 33

Unified Access Control Solution ... 34
How the Firewall Works with the Infranet Controller ... 35
Configuring for Infranet Authentication ... 36

Chapter 4 **Authentication Users** 37

Referencing Auth Users in Policies ... 38
Run-Time Authentication ... 38
Pre-Policy Check Authentication (WebAuth) ... 39
Referencing Auth User Groups in Policies ... 40
Example: Run-Time Authentication (Local User) ... 41
Example: Run-Time Authentication (Local User Group) ... 42
Example: Run-Time Authentication (External User) ... 43
Example: Run-Time Authentication (External User Group) ... 45
Example: Local Auth User in Multiple Groups ... 47
Example: WebAuth (Local User Group) ... 50
Example: WebAuth (External User Group) ... 51
Example: WebAuth + SSL Only (External User Group) ... 53

Chapter 5 **IKE, XAuth, and L2TP Users** **57**

IKE Users and User Groups 57
Example: Defining IKE Users 58
Example: Creating an IKE User Group 59
Referencing IKE Users in Gateways 60
XAuth Users and User Groups 60
Event Logging for IKE Mode 61
XAuth Users in IKE Negotiations 62
Example: XAuth Authentication (Local User) 63
Example: XAuth Authentication (Local User Group) 65
Example: XAuth Authentication (External User) 66
Example: XAuth Authentication (External User Group) 68
Example: XAuth Authentication and Address Assignments (Local User Group) 71
XAuth Client 75
Example: Security Device as an XAuth Client 75
L2TP Users and User Groups 76
Example: Local and External L2TP Auth Servers 76

Chapter 6 **Extensible Authentication for Wireless and Ethernet Interfaces** **81**

Overview 82
Supported EAP Types 82
Enabling and Disabling 802.1X Authentication 83
Ethernet Interfaces 83
Wireless Interfaces 83
Configuring 802.1X Settings 84
Configuring 802.1X Port Control 84
Configuring 802.1X Control Mode 85
Setting the Maximum Number of Simultaneous Users 85
Configuring the Reauthentication Period 86
Enabling EAP Retransmissions 86
Configuring EAP Retransmission Count 87
Configuring EAP Retransmission Period 87
Configuring the Silent (Quiet) Period 87
Configuring Authentication Server Options 88
Specifying an Authentication Server 88
Ethernet Interfaces 88
Wireless Interfaces 89
Setting the Account Type 89
Enabling Zone Verification 90
Viewing 802.1X Information 90
Viewing 802.1X Global Configuration Information 90
Viewing 802.1X Information for an Interface 91
Viewing 802.1X Statistics 91
Viewing 802.1X Session Statistics 92
Viewing 802.1X Session Details 92

Configuration Examples 93
Configuring the Security Device with a Directly Connected Client and RADIUS Server 93
Configuring a Security Device with a Hub Between a Client and the Security Device 94
Configuring the Authentication Server with a Wireless Interface 96

Index........ IX-I

Volume 10: Virtual Systems

About This Volume v

Document Conventions........ vi
CLI Conventions vi
Illustration Conventions........ vii
Naming Conventions and Character Types viii
WebUI Conventions........ ix
Juniper Networks Documentation ix

Chapter 1 Virtual Systems 1

Overview 2
Vsys Objects 4
Creating a Vsys Object and Admin 4
Setting a Default Virtual Router for a Vsys 6
Binding Zones to a Shared Virtual Router 6
Logging In as a Vsys Admin 7
Virtual System Profiles 8
Vsys Session Counters 9
Vsys Session Information 9
Behavior in High-Availability Pairs 10
Creating a Vsys Profile 10
Setting Resource Limits 10
Adding Session Limits Through Vsys Profile Assignment 12
Setting a Session Override 13
Overriding a Session Limit Reached Alarm 13
Deleting a Vsys Profile 13
Viewing Vsys Settings 14
Viewing Overrides 14
Viewing a Profile 15
Viewing Session Statistics 16
Sharing and Partitioning CPU Resources 16
Configuring CPU Weight 17
Fair Mode Packet Flow 18
Returning from Fair Mode to Shared Mode 19
Enabling the CPU Limit Feature 19
Measuring CPU Use 20
Setting the Shared to Fair Mode CPU Utilization Threshold 22
Configuring a Method to Return to Shared Mode 25
Setting a Fixed Root Vsys CPU Weight 26
Vsys and Virtual Private Networks 26
Viewing Security Associations 27
Viewing IKE Cookies 27

Policy Scheduler..28
- Creating a Policy Scheduler..28
- Binding a Policy Schedule to a Policy..29
- Viewing Policy Schedules..29
- Deleting a Policy Schedule..30

Chapter 2 Traffic Sorting 31

Overview..31
- Sorting Traffic..31
- Sorting Through Traffic..32
- Dedicated and Shared Interfaces..37
  - Dedicated Interfaces..37
  - Shared Interfaces..37

Importing and Exporting Physical Interfaces..39
- Importing a Physical Interface to a Virtual System..39
- Exporting a Physical Interface from a Virtual System..40

Chapter 3 VLAN-Based Traffic Classification 41

Overview..41
- VLANs..42
- VLANS with Vsys..42

Configuring Layer 2 Virtual Systems..43
  - Example 1: Configuring a Single Port..45
  - Example 2: Configuring Two 4-Port Aggregates with Separate Untrust Zones..49
  - Example 3: Configuring Two 4-Port Aggregates that Share One Untrusted Zone..55

Defining Subinterfaces and VLAN Tags..61

Communicating Between Virtual Systems..64

Chapter 4 IP-Based Traffic Classification 69

Overview..69

Designating an IP Range to the Root System..70

Configuring IP-Based Traffic Classification..71

Index..IX-I

Volume 11: High Availability

About This Volume vii

Document Conventions viii
CLI Conventions viii
Illustration Conventions ix
Naming Conventions and Character Types x
WebUI Conventions x
Juniper Networks Documentation xi

Chapter 1 NetScreen Redundancy Protocol 1

Overview 2
NetScreen Redundancy Protocol 5
Default Settings 6
NSRP Clusters 7
Creating an NSRP Cluster 8
Run-Time Objects 10
Configuring an Active/Passive NSRP Cluster 11
Setting an RTO Mirror State 15
Virtual Security Device Groups 16
Preempt Option 16
VSD Group Member States 17
Heartbeat Messages 18
Creating Two VSD Groups 19
Virtual Security Interfaces and Static Routes 20
Synchronization 23
Synchronizing Configurations 23
Synchronizing Files 24
Synchronizing Run-Time Objects 24
Resynchronizing RTOs Manually 24
Adding a Device to an Active NSRP Cluster 25
Synchronizing System Clocks 26
Dual High Availability Interfaces 26
Control Messages 28
Data Messages (Packet Forwarding) 29
Dynamic Routing Advisory 29
Dual HA Link Probes 30
Sending Link Probes Manually 31
Sending Link Probes Automatically 31
Setup Procedure 32
Cabling for a Full-Mesh Configuration 32
Configuring an Active/Active NSRP Cluster 35

Chapter 2 Interface Redundancy 41

Redundant Interfaces and Zones 42
Creating a Redundant Interface 42
Setting a Holddown Time Before Failover 42
Creating Redundant Interfaces for VSIs 43
Configuring Aggregate Interfaces 47
Dual Untrust Interfaces 48
Interface Failover 49
Forcing Traffic to the Backup Interface 49
Reverting Traffic to the Primary Interface 49
Automatically Failing Over Traffic 49
Determining Interface Failover 50
Interface Failover with IP Tracking 51
Interface Failover 51
Active-to-Backup Tunnel Failover 55
Interface Failover with VPN Tunnel Monitoring 60
Dual Active Tunnels 60
Applying Weights to Tunnel Failover 64
Serial Interface 71
Modem Overview 72
Modem Configuration 73
Configuring ISP Information 74
Serial Interface Failover 75
Configuring Dial Backup in Trust-Untrust Mode 75
Deleting a Default Route for the Serial Interface 78
Adding a Default Route for the Serial Interface 78
Deactivating a Policy for Serial Interface Failover 78

Chapter 3 Failover 79

Device Failover 79
VSD Group Failover (NSRP) 80
Object Monitoring for Device or VSD Group Failover 81
Monitoring a Physical Interface Object to Trigger Failover 82
Monitoring a Zone Object to Trigger Failover 83
Monitoring a Tracked IP Object to Trigger Failover 83
Setting Track IP for Device Failover 85
Virtual System Failover 88

Chapter 4 NSRP-Lite 95

Introduction to NSRP-Lite 96
- Clusters and VSD Groups 98
- Default Settings 99

Clusters 99
- Cluster Names 101
- Authentication and Encryption 101

VSD Groups 102
- VSD Group Member States 102
- Heartbeat Messages 103
- Preempt Option 103

Cabling and Configuring NSRP-Lite 104

Configuration and File Synchronization 109
- Synchronizing Configurations 109
- Synchronizing Files 110
- Adding a Device to an Active NSRP Cluster 110
- Automatic Configuration Synchronization 111

Path Monitoring 111
- Setting Thresholds 113
- Weighting Tracked IP Addresses 113
- IP Tracking for VPN Tunnel Failover 113

Index........ IX-I

Volume 12: WAN, ADSL, Dial, and Wireless

About This Volume ix

Document Conventions x
- CLI Conventions x
- Illustration Conventions xi
- Naming Conventions and Character Types xii
- WebUI Conventions xii

Juniper Networks Documentation xiii

Chapter 1 Wide Area Networks 1

WAN Overview 1
- Serial 2
- T1 3
- E1 3
- T3 4
- ISDN 5

WAN Interface Options 7
- Hold time 8
- Frame Checksum 9
- Idle-cycle Flag 9
- Start/End Flag 9
- Line Encoding 10
  - Alternate Mark Inversion (AMI) Encoding 10
  - B8ZS and HDB3 Line Encoding 11
  - Byte Encoding 11
  - Line Buildout 11

- Framing Mode 12
    - Extended Superframe (ESF) Framing for T1 12
    - C-Bit Parity Framing for T3 13
- Clocking 13
    - Clocking Mode 13
    - Clocking Source 15
    - Internal Clock Rate 15
    - Transmit Clock Inversion 16
- Signal Handling 17
- Loopback Signal 18
    - Remote and Local Loopback 18
    - Loopback Mode 18
    - CSU Compatibility Mode 20
    - Remote Loopback Response 21
    - FEAC Response 21
- Time Slots 22
    - Fractional T1 22
    - Fractional E1 22
- Bit-Error Rate Testing 23
- ISDN Options 25
    - Switch Type 25
    - SPID 25
    - TEI Negotiation 25
    - Calling Number 26
    - T310 Value 26
    - Send Complete 26
- BRI Mode 27
    - Leased-Line Mode 27
    - Dialer Enable 27
- Dialer Options 27
- Disabling a WAN Interface 29

WAN Interface Encapsulation 30
- Point-to-Point Protocol (PPP) 30
- Frame Relay 31
- Cisco-High-Level Data Link Control (Cisco-HDLC) 32
- Basic Encapsulation Options 32
    - Unnumbered Interfaces 32
    - Protocol Maximum Transmission Unit Configuration 33
    - Static IP Address Configuration 33
    - Keepalives 33
- PPP Encapsulation Options 34
    - PPP Access Profile 35
    - PPP Authentication Method 35
    - Password 36
- PPP Authentication Protocols 37
    - Challenge Handshake Authentication Protocol (CHAP) 37
    - Password Authentication Protocol (PAP) 37
    - Local Database User 38
- Frame Relay Encapsulation Options 38
    - Keep Alive Messages 38
    - Frame Relay LMI Type 39
    - Creating and Configuring PVCs 40
    - Inverse Address Resolution Protocol 41

Multi-Link Encapsulation 42
Multi-Link Encapsulation Overview..42
Basic Multi-Link Bundle Configuration 42
Bundle Identifier 43
Drop Timeout..43
Fragment Threshold..44
Minimum Links 45
Multi-Link PPP Configuration Options..45
Basic Configuration Steps...45
Maximum Received Reconstructed Unit...46
Sequence-Header Format...46
Multi-Link Frame Relay Configuration Options 46
Basic Configuration Steps...46
Link Assignment for MLFR 47
Acknowledge Retries...48
Acknowledge Timer 48
Hello Timer 48
WAN Interface Configuration Examples..49
Configuring a Serial Interface 49
Configuring a T1 Interface 50
Configuring an E1 Interface...51
Configuring a T3 Interface 52
Configuring your Device for ISDN Connectivity 53
Dialing Out to a Single Destination Only 54
Dialing Out Using the Dialer Interface 54
Using the Leased Line Mode...58
Routing Traffic through the ISDN BRI...58
Routing Traffic through the Dialer Interface 59
Encapsulation Configuration Examples...60
Configuring PPP Encapsulation..60
Configuring MLPPP Encapsulation...62
Configuring Frame Relay Encapsulation 63
Configuring ML Frame Relay 65
Configuring Cisco HDLC Encapsulation...66

Chapter 2 **Asymmetric Digital Subscriber Line** 69

ADSL Overview ... 69
The ADSL Interface on a Security Device ... 70
Point-to-Point Protocol over Adaptation Layer 5 ... 72
Multi-Link PPP ... 73
Asynchronous Transfer Mode Quality of Service ... 73
Configuration Examples ... 74
Example 1: (Small Business/Home) PPPoA on ADSL Interface ... 75
Example 2: (Small Business/Home) 1483 Bridging on ADSL Interface ... 77
Example 3: (Small Business) 1483 Routing on ADSL Interface ... 79
Example 4: (Small Business/Home) Dialup Backup ... 81
Example 5: (Small Business/Home) Ethernet Backup ... 84
Example 6: (Small Business/Home) ADSL Backup ... 88
Example 7: (Small Business) MLPPP ADSL ... 91
Example 8: (Small Business) Allow Access to Local Servers ... 93
Example 9: (Branch Office) VPN Tunnel Through ADSL ... 96
Example 10: (Branch Office) Secondary VPN Tunnel ... 100

Chapter 3 **ISP Failover and Dial Recovery** 107

Setting ISP Priority for Failover ... 107
Defining Conditions for ISP Failover ... 108
Configuring a Dialup Recovery Solution ... 109

Chapter 4 **Wireless Local Area Network** 113

Overview ... 114
Security Zones and Port Modes ... 115
Wireless Product Interface Naming Differences ... 115
Basic Wireless Network Feature Configuration ... 116
Creating a Service Set Identifier ... 116
Suppressing SSID Broadcast ... 117
Isolating a Client ... 117
Setting the Operation Mode for a 2.4 GHz Radio Transceiver ... 117
Setting the Operation Mode for a 5 GHz Radio Transceiver ... 118
Configuring Minimum Data Transmit Rate ... 119
Configuring Transmit Power ... 119
Reactivating a WLAN Configuration ... 120
Configuring Authentication and Encryption for SSIDs ... 120
Configuring Wired Equivalent Privacy ... 121
Multiple WEP Keys ... 121
Configuring Open Authentication ... 123
Configuring WEP Shared-Key Authentication ... 125
Configuring Wi-Fi Protected Access ... 126
Configuring 802.1X Authentication for WPA and WPA2 ... 127
Configuring Pre-Shared Key Authentication for WPA and WPA2 ... 128
Specifying Antenna Use ... 129
Setting the Country Code, Channel, and Frequency ... 129
Using Extended Channels ... 130
Performing a Site Survey ... 130
Locating Available Channels ... 131
Setting an Access Control List Entry ... 131
Configuring Super G ... 132
Configuring Atheros XR (Extended Range) ... 133

Configuring Wi-Fi Multimedia Quality of Service 134
Enabling WMM 134
Configuring WMM Quality of Service 134
Access Categories 134
WMM Default Settings 135
Example 137
Configuring Advanced Wireless Parameters 138
Configuring Aging Interval 138
Configuring Beacon Interval 139
Configuring Delivery Traffic Indication Message Period 140
Configuring Burst Threshold 140
Configuring Fragment Threshold 140
Configuring Request To Send Threshold 141
Configuring Clear To Send Mode 141
Configuring Clear To Send Rate 142
Configuring Clear To Send Type 142
Configuring Slot Time 142
Configuring Preamble Length 143
Working with Wireless Interface 143
Binding an SSID to a Wireless Interface 143
Binding a Wireless Interface to a Radio 144
Creating Wireless Bridge Groups 145
Disabling a Wireless Interface 145
Viewing Wireless Configuration Information 145
Configuration Examples 146
Example 1: Open Authentication and WEP Encryption 146
Example 2: WPA-PSK Authentication with Passphrase and Automatic Encryption 147
Example 3: WLAN in Transparent Mode 147
Example 4: Multiple and Differentiated Profiles 151

Appendix A Wireless Information A-I

Country Codes .... A-I
802.11a Channel Numbers .... A-IV
802.11b and 802.11g Channels .... A-VI
Turbo-Mode Channel Numbers .... A-VI

Index .... IX-I

Volume 13: General Packet Radio Service

About This Volume v

Document Conventions vi
- CLI Conventions vi
- Illustration Conventions vii
- Naming Conventions and Character Types viii
- WebUI Conventions viii

Juniper Networks Documentation ix

Chapter 1 GPRS 1

The Security Device as a GPRS Tunneling Protocol Firewall 2
- Gp and Gn Interfaces 3
- Gi Interface 3
- Operational Modes 4
- Virtual System Support 5

Policy-Based GPRS Tunneling Protocol 5
- Example: Configuring Policies to Enable GTP Inspection 6

GPRS Tunneling Protocol Inspection Object 7
- Example: Creating a GTP Inspection Object 8

GTP Message Filtering 8
- Packet Sanity Check 8
- Message-Length Filtering 9
  - Example: Setting GTP Message Lengths 9
- Message-Type Filtering 10
  - Example: Permitting and Denying Message Types 10
  - Supported Message Types 10
- Message-Rate Limiting 12
  - Example: Setting a Rate Limit 12
- Sequence Number Validation 13
  - Example: Enabling Sequence Number Validation 13
- IP Fragmentation 13
- GTP-in-GTP Packet Filtering 13
  - Example: Enabling GTP-in-GTP Packet Filtering 13
- Deep Inspection 14
  - Example: Enabling GTP-in-GTP Packet Filtering 14

GTP Information Elements 14
Access Point Name Filtering 15
Example: Setting an APN and a Selection Mode 16
IMSI Prefix Filtering 16
Example: Setting a Combined IMSI Prefix and APN Filter 17
Radio Access Technology 17
Example: Setting an RAT and APN Filter 17
Routing Area Identity and User Location Information 18
Example: Setting an RAI and APN Filter 18
Example: Setting a ULI and APN Filter 18
APN Restriction 18
IMEI-SV 19
Example: Setting an IMEI-SV and APN Filter 19
Protocol and Signaling Requirements 19
Combined Support 20
Supported R6 Information Elements 20
3GPP R6 IE Removal 22
Example: R6 Removal 22
GTP Tunnels 23
GTP Tunnel Limiting 23
Example: Setting GTP Tunnel Limits 23
Stateful Inspection 23
GTP Tunnel Establishment and Teardown 24
Inter SGSN Routing Area Update 24
Tunnel Failover for High Availability 24
Hanging GTP Tunnel Cleanup 25
Example: Setting the Timeout for GTP Tunnels 25
SGSN and GGSN Redirection 26
Overbilling-Attack Prevention 26
Overbilling-Attack Description 26
Overbilling-Attack Solution 28
Example: Configuring the Overbilling Attack Prevention Feature 29
GTP Traffic Monitoring 31
Traffic Logging 31
Example: Enabling GTP Packet Logging 32
Traffic Counting 33
Example: Enabling GTP Traffic Counting 33
Lawful Interception 34
Example: Enabling Lawful Interception 34

Index .... IX-I

Volume 14: Dual-Stack Architecture with IPv6

About This Volume vii

Document Audience viii
Document Conventions viii
CLI Conventions viii
Illustration Conventions ix
Naming Conventions and Character Types x
WebUI Conventions xi
Juniper Networks Documentation xi

Chapter 1 Internet Protocol Version 6 Introduction 1

Overview 2
IPv6 Addressing 2
Notation 2
Prefixes 3
Address Types 3
Unicast Addresses 3
Anycast Addresses 4
Multicast Addresses 4
IPv6 Headers 4
Basic Header 4
Extension Headers 5
IPv6 Packet Handling 6
IPv6 Router and Host Modes 7
IPv6 Tunneling Guidelines 8

Chapter 2 IPv6 Configuration 9

Overview 11
Address Autoconfiguration 11
Extended Unique Identifier 11
Router Advertisement Messages 12
Router Solicitation Messages 12
Prefix Lists 12
Neighbor Discovery 13
Neighbor Cache Table 13
Neighbor Unreachability Detection 13
Neighbor Entry Categories 14
Neighbor Reachability States 14
How Reachability State Transitions Occur 15
Enabling an IPv6 Environment 18
Enabling IPv6 at the Device Level 18
Disabling IPv6 at the Device Level 19
Configuring an IPv6 Host 19
Binding the IPv6 Interface to a Zone 20
Enabling IPv6 Host Mode 20
Setting an Interface Identifier 20
Configuring Address Autoconfiguration 21
Configuring Neighbor Discovery 21

Configuring an IPv6 Router 22
Binding the IPv6 Interface to a Zone 22
Enabling IPv6 Router Mode 22
Setting an Interface Identifier 23
Setting Address Autoconfiguration 23
Outgoing Router Advertisements Flag 23
Managed Configuration Flag 24
Other Parameters Configuration Flag 24
Disabling Address Autoconfiguration 24
Setting Advertising Time Intervals 25
Advertised Reachable Time Interval 25
Advertised Retransmit Time Interval 26
Maximum Advertisement Interval 26
Minimum Advertisement Interval 26
Advertised Default Router Lifetime 27
Advertising Packet Characteristics 27
Link MTU Value 27
Current Hop Limit 28
Advertising Router Characteristics 28
Link Layer Address Setting 28
Advertised Router Preference 28
Configuring Neighbor Discovery Parameters 29
Neighbor Unreachability Detection 29
MAC Session-Caching 29
Static Neighbor Cache Entries 30
Base Reachable Time 30
Probe Time 31
Retransmission Time 31
Duplicate Address Detection Retry Count 31
Viewing IPv6 Interface Parameters 32
Viewing Neighbor Discovery Configurations 32
Viewing the Current RA Configuration 32
Configuration Examples 33
IPv6 Router 33
IPv6 Host 33

Chapter 3 Connection and Network Services 35

Overview 36
Dynamic Host Configuration Protocol Version 6 36
Device-Unique Identification 36
Identity Association Prefix Delegation-Identification 37
Prefix Features 37
Server Preference 38
Configuring a DHCPv6 Server 38
Configuring a DHCPv6 Client 40
Viewing DHCPv6 Settings 41
Configuring Domain Name System Servers 42
Requesting DNS and DNS Search List Information 43
Setting Proxy DNS Address Splitting 44
Configuring PPPoE 46
Setting Fragmentation 47

Chapter 4 Static and Dynamic Routing 49

Overview 50
Dual Routing Tables 50
Static and Dynamic Routing 51
Upstream and Downstream Prefix Delegation 51
Static Routing 52
RIPng Configuration 53
Creating and Deleting a RIPng Instance 54
Creating a RIPng Instance 54
Deleting a RIPng Instance 54
Enabling and Disabling RIPng on Interfaces 55
Enabling RIPng on an Interface 55
Disabling RIPng on an Interface 55
Global RIPng Parameters 56
Advertising the Default Route 56
Rejecting Default Routes 57
Configuring Trusted Neighbors 57
Redistributing Routes 58
Protecting Against Flooding by Setting an Update Threshold 59
RIPng Interface Parameters 60
Route, Interface, and Offset Metrics 60
Access Lists and Route Maps 61
Static Route Redistribution 61
Configuring Split Horizon with Poison Reverse 64
Viewing Routing and RIPng Information 64
Viewing the Routing Table 65
Viewing the RIPng Database 65
Viewing RIPng Details by Virtual Router 66
Viewing RIPng Details by Interface 67
Viewing RIPng Neighbor Information 68
Configuration Examples 69
Enabling RIPng on Tunnel Interfaces 69
Avoiding Traffic Loops to an ISP Router 71
Configuring the Customer Premises Equipment 71
Configuring the Gateway 75
Configuring the ISP Router 78
Setting a Null Interface Redistribution to OSPF 79
Redistributing Discovered Routes to OSPF 80
Setting Up OSPF-Summary Import 80

Chapter 5 **Address Translation** 81

Overview 82
Translating Source IP Addresses 83
DIP from IPv6 to IPv4 83
DIP from IPv4 to IPv6 83
Translating Destination IP Addresses 84
MIP from IPv6 to IPv4 84
MIP from IPv4 to IPv6 85
Configuration Examples 86
IPv6 Hosts to Multiple IPv4 Hosts 86
IPv6 Hosts to a Single IPv4 Host 88
IPv4 Hosts to Multiple IPv6 Hosts 90
IPv4 Hosts to a Single IPv6 Host 91
Translating Addresses for Domain Name System Servers 93

Chapter 6 **IPv6 in an IPv4 Environment** 97

Overview 98
Configuring Manual Tunneling 99
Configuring 6to4 Tunneling 102
6to4 Routers 102
6to4 Relay Routers 103
Tunnels to Remote Native Hosts 104
Tunnels to Remote 6to4 Hosts 107

Chapter 7 **IPSec Tunneling** 111

Overview 112
IPSec 6in6 Tunneling 112
IPSec 4in6 Tunneling 115
IPSec 6in4 Tunneling 120
Manual Tunneling with Fragmentation Enabled 124
IPv6 to IPv6 Route-Based VPN Tunnel 125
IPv4 to IPv6 Route-Based VPN Tunnel 127

Chapter 8 IPv6 XAuth User Authentication 131

Overview 132
- RADIUSv6........ 132
  - Single Client, Single Server........ 132
  - Multiple Clients, Single Server 132
  - Single Client, Multiple Servers 133
  - Multiple Hosts, Single Server........ 133
- IPSec Access Session Management........ 134
  - IPSec Access Session........ 134
  - Enabling and Disabling IAS Functionality........ 136
  - Releasing an IAS Session........ 136
  - Limiting IAS Settings 136
- Dead Peer Detection........ 137

Configuration Examples........ 138
- XAuth with RADIUS........ 138
- RADIUS with XAuth Route-Based VPN........ 139
- RADIUS with XAuth and Domain Name Stripping 143
- IP Pool Range Assignment........ 147
- RADIUS Retries........ 153
- Calling-Station-Id 153
- IPSec Access Session 154
- Dead Peer Detection........ 163

Appendix A Switching A-I

Index........ IX-I

About the *Concepts & Examples ScreenOS Reference Guide*

Juniper Networks security devices are Application-Specific Integrated Circuit (ASIC)-based, Internet Computer Security Association (ICSA)-certified Internet security appliances and security systems that integrate firewall, virtual private network (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.

- **Layered Security:** The layered security solution is deployed at different locations to repel attacks. If the first one fails, the second layer catches the attacks. Some functions help protect remote locations with site-to-site VPN. Devices deployed at the perimeter help repel network-based attacks. Another layer is the integrated intrusion prevention in the form of both IDP and Deep Inspection. Intrusion prevention automatically detects and prevents attacks from inflicting damages. Moving further into the network, the last security layer is network segmentation also described as virtualization. This is the ability to divide the network up into secure domains and protecting critical resources from unauthorized roaming users and network attacks.

- **Content Security:** Protects users from malicious URLs and provides embedded antivirus scanning and web filtering. In addition, works with third-party products to provide external antivirus scanning, anti-spam, and web filtering.

- **VPN:** A VPN provides a secure communications channel between two or more remote network appliances.

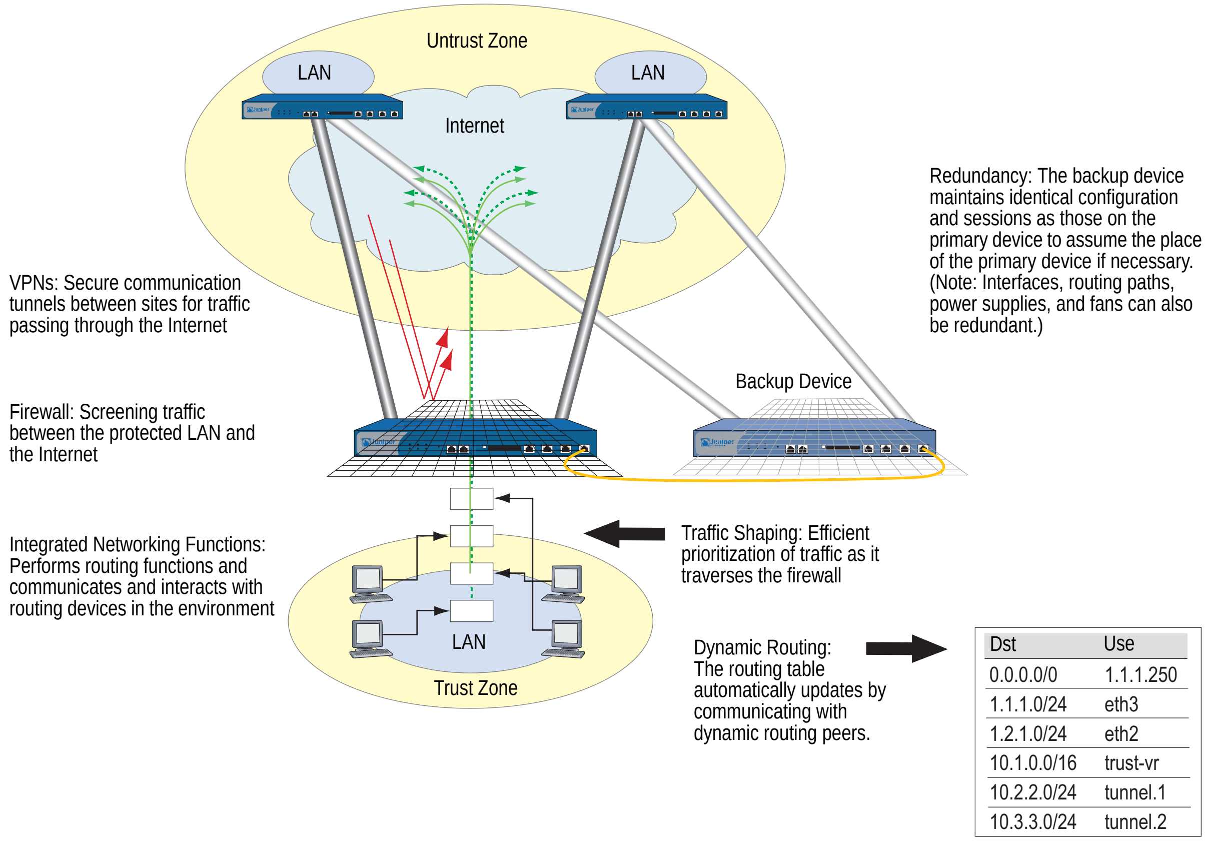
- **Integrated Networking Functions:** Dynamic routing protocols learn reachability and advertise dynamically changing network topologies. In addition, traffic shaping functionality allows administrative monitoring and control of traffic passing across the Juniper Networks firewall to maintain a network's quality-of-service (QoS) level.

- **Centralized Management:** The Netscreen-Security Manager tool simplifies configuration, deployment, and management of security devices.

- **Redundancy:** High availability of interfaces, routing paths, security devices, and—on high-end Juniper Networks devices—power supplies and fans, to avoid a single point of failure in any of these areas.

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

Figure 1: Key Features in ScreenOS



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

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

Firewall: Screening traffic between the protected LAN and the Internet

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

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

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

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

The ScreenOS system provides all the features needed to set up and manage any security appliance or system. This document is a reference guide for configuring and managing a Juniper Networks security device through ScreenOS.

Volume Organization

The *Concepts & Examples ScreenOS Reference Guide* is a multi-volume manual. The following information outlines and summarizes the material in each volume:

Volume 1: Overview

- "Table of Contents" contains a master table of contents for all volumes in the manual.
- Appendix A, "Glossary," provides definitions for all the key terms used throughout all volumes in the manual.
- "Master Index" is a master index for all volumes in the manual.

Volume 2: Fundamentals

- Chapter 1, "ScreenOS Architecture," presents the fundamental elements of the architecture in 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, "Zones," explains security zones, tunnel zones, and function zones.
- Chapter 3, "Interfaces," describes the various physical, logical, and virtual interfaces on security devices.
- Chapter 4, "Interface Modes," explains the concepts behind Transparent, Network Address Translation (NAT), and Route interface operational modes.
- Chapter 5, "Building Blocks for Policies," discusses the elements used for creating policies and virtual private networks (VPNs): addresses (including VIP addresses), services, and DIP pools. It also presents several example configurations support for the H.323 protocol.
- Chapter 6, "Policies," explores the components and functions of policies and offers guidance on their creation and application.
- Chapter 7, "Traffic Shaping," explains how you can manage bandwidth at the interface and policy levels and prioritize services.
- Chapter 8, "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 security 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.
- Chapter 2, "Monitoring Security Devices," explains various monitoring methods and provides guidance in interpreting monitoring output.

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 (DoS) Attack Defenses," explains firewall, network, and OS-specific DoS attacks and how ScreenOS mitigates such attacks.
- Chapter 4, "Content Monitoring and Filtering," describes how to protect HyperText Transfer Protocol (HTTP) users from malicious uniform resource locators (URLs) and how to configure the security device to work with third party products to provide antivirus scanning and web filtering.
- Chapter 5, "Deep Inspection," describes how to configure the security device to obtain Deep Inspection (DI) attack object updates, how to create user-defined attack objects and attack object groups, and how to apply IDP at the policy level.
- Chapter 6, "Intrusion Detection and Prevention," describes Juniper Networks Intrusion Detection and Prevention (IDP) technology which can both detect and then stop attacks when deployed inline to your network. The chapter describes how to apply IDP at the policy level to drop malicious packets or connections before the attacks can enter your network.
- Chapter 7, "Suspicious Packet Attributes," explains a number of SCREEN options that block potentially dangerous packets.
- Appendix A, "Contexts for User-Defined Signatures," provides a list and descriptions of contexts that you can specify when defining a stateful signature attack object.

Volume 5: Virtual Private Networks

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

Volume 6: Voice-over-Internet Protocol

- Chapter 1, “H.323 Application Layer Gateway,” describes the H.323 protocol and provides examples of typical scenarios.
- Chapter 2, “Session Initiation Protocol Application Layer Gateway,” describes the Session Initiation Protocol (SIP) and shows how the SIP ALG processes calls in Route and Network Address Translation (NAT) modes. Examples of typical scenarios follow a summary of the SIP architecture.
- Chapter 3, “Media Gateway Control Protocol Application Layer Gateway,” presents an overview of the Media Gateway Control Protocol (MGCP) ALG and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the MGCP architecture.
- Chapter 4, “Skinny Client Control Protocol Application Layer Gateway,” presents an overview of the Skinny Client Control Protocol (SCCP) ALG and lists the firewall security features of the implementation. Examples of typical scenarios follow a summary of the SCCP architecture.

Volume 7: Routing

- Chapter 1, “Static Routing,” describes the ScreenOS routing table, the basic routing process on the security device, and how to configure static routes on security devices.
- Chapter 2, “Routing,” explains how to configure virtual routers on security devices and how to redistribute routing table entries between protocols or between virtual routers.
- Chapter 3, “Open Shortest Path First,” describes how to configure the OSPF dynamic routing protocol on security devices.
- Chapter 4, “Routing Information Protocol,” describes how to configure the RIP dynamic routing protocol on security devices.
- Chapter 5, “Border Gateway Protocol,” describes how to configure the BGP dynamic routing protocol on security devices.
- Chapter 6, “Policy-Based Routing,” explains how to force interesting traffic along a specific path in the network.
- Chapter 7, “Multicast Routing,” introduces basic multicast routing concepts.
- Chapter 8, “Internet Group Management Protocol,” describes how to configure the Internet Group Management Protocol (IGMP) on security devices.
- Chapter 9, “Protocol Independent Multicast,” describes how to configure the Protocol Independent Multicast (PIM) routing protocol on security devices.
- Chapter 10, “ICMP Router Discovery Protocol,” explains how to set up an Internet Control Messages Protocol (ICMP) message exchange between a host and a router.

Volume 8: Address Translation

- Chapter 1, “Address Translation,” gives an overview of the various translation options, which are covered in detail in subsequent chapters.
- Chapter 2, “Source Network Address Translation,” describes NAT-src, the translation of the source IP address in a packet header, with and without Port Address Translation (PAT).
- Chapter 3, “Destination Network Address Translation,” describes NAT-dst, the translation of the destination IP address in a packet header, with and without destination port address mapping. This section also includes information about the packet flow when doing NAT-src, routing considerations, and address shifting.
- Chapter 4, “Mapped and Virtual Addresses,” describes the mapping of one destination IP address to another based on IP address alone (mapped IP) or based on destination IP address and destination port number (virtual IP).

Volume 9: User Authentication

- Chapter 1, “Authentication,” details the various authentication methods and uses that ScreenOS supports.

- Chapter 2, “Authentication Servers,” presents the options of using one of three possible types of external authentication server—RADIUS, SecurID, or LDAP—or the internal database and shows how to configure the security device to work with each type.

- Chapter 3, “Infranet Authentication,” details how the security device is deployed in a unified access control (UAC) solution. Juniper Networks unified access control solution (UAC) secures and assures the delivery of applications and services across an enterprise infranet.

- Chapter 4, “Authentication Users,” explains how to define profiles for authentication users and how to add them to user groups stored either locally or on an external RADIUS authentication server.

- Chapter 5, “IKE, XAuth, and L2TP Users,” explains how to define IKE, XAuth, and L2TP users. Although the XAuth section focusses primarily on using the security device as an XAuth server, it also includes a subsection on configuring select security devices to act as an XAuth client.

- Chapter 6, “Extensible Authentication for Wireless and Ethernet Interfaces,” explains the options available for and examples of how to use Extensible Authentication Protocol to provide authentication for Ethernet and wireless interfaces.

Volume 10: Virtual Systems

- Chapter 1, “Virtual Systems,” discusses virtual systems, objects, and administrative tasks.

- Chapter 2, “Traffic Sorting,” explains how ScreenOS sorts traffic.

- Chapter 3, “VLAN-Based Traffic Classification,” explains VLAN-based traffic classification for virtual systems.

- Chapter 4, “IP-Based Traffic Classification,” explains IP-based traffic classification for virtual systems.

Volume 11: High Availability

- Chapter 1, “NetScreen Redundancy Protocol,” explains how to cable, configure, and manage Juniper Networks security devices in a redundant group to provide high availability (HA) using the NetScreen Redundancy Protocol (NSRP).

- Chapter 2, “Interface Redundancy,” describes the various ways in which Juniper Networks security devices provide interface redundancy.

- Chapter 3, “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.

- Chapter 4, “NSRP-Lite,” explains how to configure Juniper Networks security devices that support NSRP-Lite.

Volume 12: WAN, ADSL, Dial, and Wireless

- Chapter 1, “Wide Area Networks,” describes how to configure a wide area network (WAN).

- Chapter 2, “Asymmetric Digital Subscriber Line,” describes the Asymmetric Digital Subscriber Line (ADSL) interface on the security device. ADSL is a Digital Subscriber Line (DSL) technology that allows existing telephone lines to carry both voice telephone service and high-speed digital transmission.

- Chapter 3, “ISP Failover and Dial Recovery,” describes how to set priority and define conditions for ISP failover and how to configure a dialup recovery solution.

- Chapter 4, “Wireless Local Area Network,” describes the wireless interfaces on Juniper Networks wireless devices and provides example configurations.

- Appendix A, “Wireless Information,” lists available channels, frequencies, and regulatory domains and lists the channels that are available on wireless devices for each country.

Volume 13: General Packet Radio Service

- Chapter 1, “GPRS,” describes the GPRS Tunneling Protocol (GTP) features in ScreenOS and demonstrates how to configure GTP functionality on a Juniper Networks security device.

Volume 14: Dual-Stack Architecture with IPv6

- Chapter 1, “Internet Protocol Version 6 Introduction,” explains IPv6 headers, concepts, and tunneling guidelines.
- Chapter 2, “IPv6 Configuration,” explains how to configure an interface for operation as an IPv6 router or host.
- Chapter 3, “Connection and Network Services,” explains how to configure Dynamic Host Configuration protocol version 6 (DHCPv6), Domain Name Services (DNS), Point-to-Point Protocol over Ethernet (PPPoE), and fragmentation.
- Chapter 4, “Static and Dynamic Routing,” explains how to set up static and dynamic routing. This chapter explains ScreenOS support for Routing Information Protocol-Next Generation (RIPng).
- Chapter 5, “Address Translation,” explains how to use Network Address Translation (NAT) with dynamic IP (DIP) and mapped-IP (MIP) addresses to traverse IPv4/IPv6 boundaries.
- Chapter 6, “IPv6 in an IPv4 Environment,” explains manual and dynamic tunneling .
- Chapter 7, “IPSec Tunneling,” explains how to configure IPSec tunneling to connect dissimilar hosts.
- Chapter 8, “IPv6 XAuth User Authentication,” explains how to configure Remote Authentication Dial In User Service (RADIUS) and IPSec Access Session (IAS) management.
- Appendix A, “Switching,” lists options for using the security device as a switch to pass IPv6 traffic.

Document Conventions

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

- “CLI Conventions” on page lviii
- “Illustration Conventions” on page lix
- “Naming Conventions and Character Types” on page lx
- “WebUI Conventions” on page lx

CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- 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, the ethernet2, *or* the ethernet3 interface."

- Variables are in *italic* type:

  set admin user *name1* password *xyz*

In text:

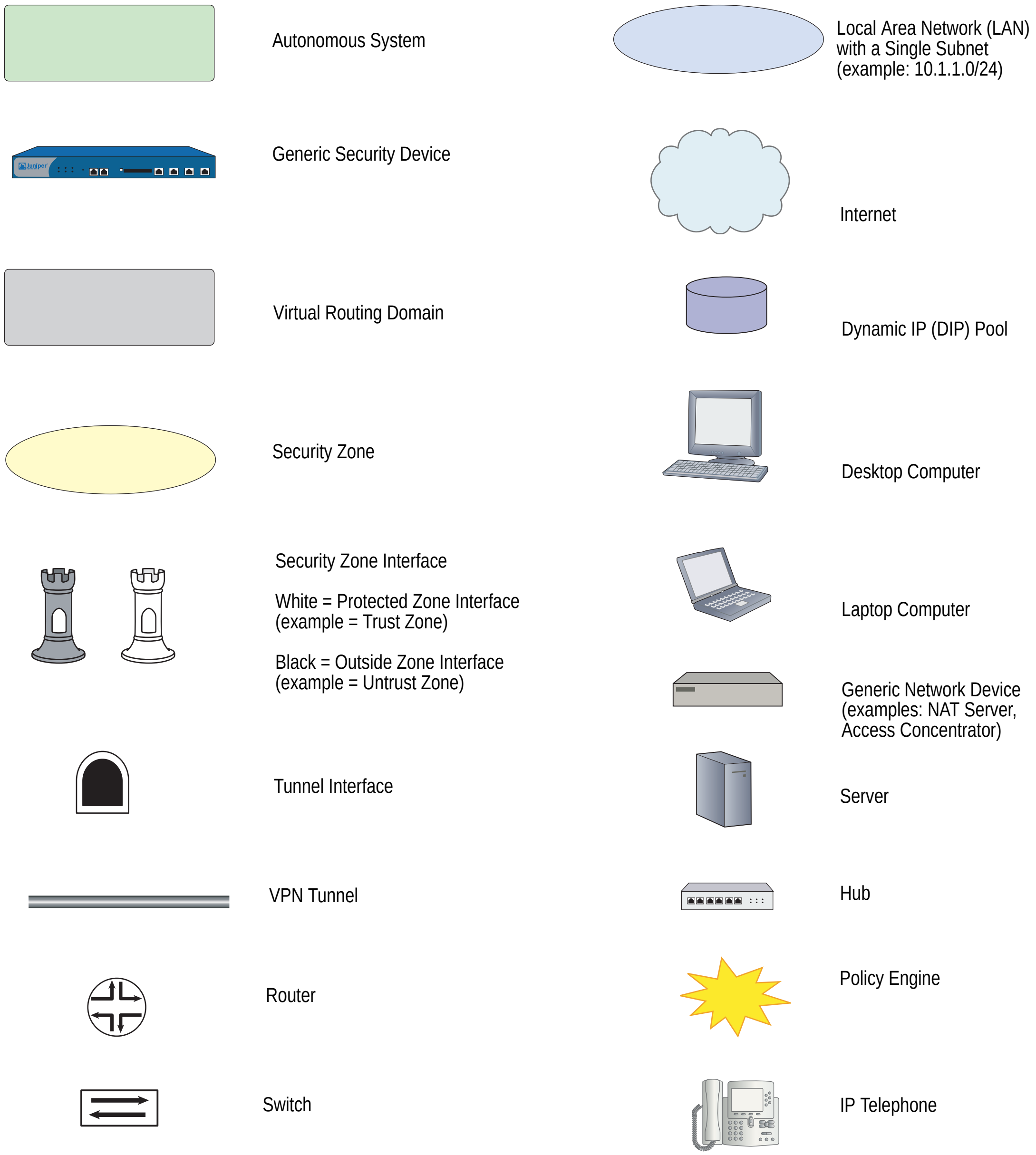
- Commands are in **boldface** type.
- Variables are in *italic* type.

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

Illustration Conventions

The following figure shows the basic set of images used in illustrations throughout this manual.

Figure 2: Images in Manual Illustrations



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

- Any leading spaces or trailing text within a set of double quotes are trimmed; for example, **" local LAN "** becomes **"local LAN"**.

- Multiple consecutive spaces are treated as a single space.

- Name strings are case-sensitive, although many CLI keywords 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.

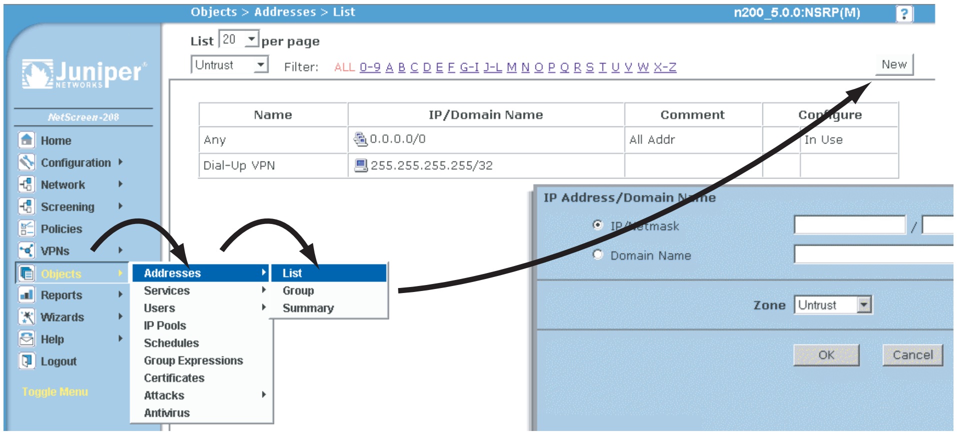
- ASCII characters from 32 (0x20 in hexadecimals) to 255 (0xff), except double quotes ("), which have special significance as an indicator of the beginning or end of a name string that includes spaces.

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

WebUI Conventions

A chevron (>) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

Figure 3: WebUI Navigation



Objects > Addresses > List

n200_5.0.0:NSRP(M)

List 20 per page

Untrust

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

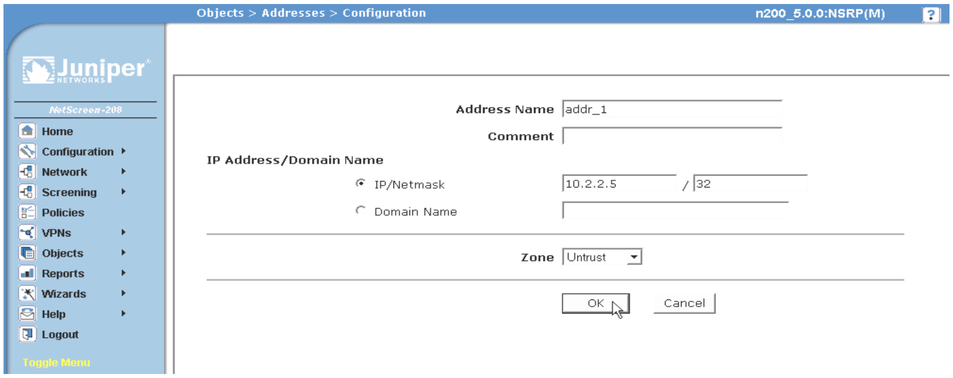
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

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

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

Figure 4: Navigational Path and Configuration Settings



Objects > Addresses > Configuration

n200_5.0.0:NSRP(M)

Address Name: addr_1
Comment:
IP Address/Domain Name
● IP/Netmask: 10.2.2.5 / 32
○ Domain Name:
Zone: Untrust

Juniper Networks Documentation

To obtain technical documentation for any Juniper Networks product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

techpubs-comments@juniper.net

Appendix A

Glossary

10BaseT Also known as *Unshielded Twisted Pair (UTP)*, 10BaseT is the standard cabling used for telephone lines and the most common form of Ethernet connection. 10BaseT denotes a peak transmission speed of 10 Megabits per second (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.

100BaseT Another term for *Fast Ethernet*, an upgraded standard for connecting computers in a LAN. 100BaseT ethernet works like regular ethernet but is able to 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.

802.11a A WLAN standard that provides up to 54 Mbps in the 5GHz radio band.

802.11b A WLAN standard that provides up to 11 Mbps in the 2.4 GHz radio band.

802.11g A WLAN standard that provides 20+ Mbps in the 2.4 GHz radio band.

802.11SuperG A WLAN standard that provides up to 108 Mbps in the 2.4 GHz radio band.

ABR *See* Area Border Router (ABR).

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

Access Control List (ACL) Identifies clients by their MAC addresses and specifies whether the wireless device allows or denies access for each address.

Access List A list of network prefixes that are compared to a given route. If the route matches a network prefix defined in the access list, the route is either permitted or denied.

Access Point (AP) *See* Wireless access point.

Access Point Name (APN) An information element (IE) included in the header of a GTP packet that provides information on how to reach a network. It is composed of a network ID and an operator ID.

ACL *See* Access Control List (ACL).

Address Shifting A mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in another range.

Adjacencies When two routers can exchange routing information, they are considered to have constructed an adjacency. Point-to-point networks, which have only two routers, automatically form an adjacency. Point-to-multipoint networks are a series of several point-to-point networks. When routers pair in this more complex networking scheme, they are considered to be adjacent to one another.

ADM *See* Add-Drop Multiplexer (ADM).

ADSL *See* Asymmetric Digital Subscriber Line (ADSL).

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. *See also* Border Gateway Protocol (BGP).

Aggregation The process of combining several routes in such a way that only a single route advertises itself. This technique minimizes the size of the routing table for the router.

Aggregator 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.

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

ALG *See* Application Layer Gateway (ALG).

Antivirus (AV) Scanning A mechanism for detecting and blocking viruses in File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP)—including HTTP webmail—and Post Office Protocol version 3 (POP3) traffic. ScreenOS offers an internal AV scanning solution.

Application Layer Gateway (ALG) On a security device, a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP) or File Transfer Protocol (FTP). The ALG intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.

Area The most fundamental ordering method in the Open Shortest Path First (OSPF) routing protocol. An OSPF area divides the internetwork into smaller, more manageable constituent pieces. This technique reduces the amount of information about all the other routers that each router must store and maintain. When a router in an area needs information about another device inside or outside its area, it contacts a special router, called the Area Border Router (ABR), that contains all essential device information. In addition, the ABR filters all information coming into the area to avoid burdening other routers in the area with unnecessary information.

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

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

AS *See* Autonomous System (AS).

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

AS Number The identification number of the local Autonomous System (AS) mapped to a BGP routing instance. The ID number can be any valid integer. *See also* Border Gateway Protocol (BGP).

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

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. *See also* Border Gateway Protocol (BGP).

AS Path Attribute Class BGP provides four classes of path attributes: well-known mandatory, well-known discretionary, optional transitive, and optional non-transitive. *See also* Border Gateway Protocol (BGP).

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

Asymmetric Digital Subscriber Line (ADSL) A Digital Subscriber Line (DSL) technology that allows existing telephone lines to carry both voice telephone service and high-speed digital transmission. A growing number of service providers offer ADSL service to home and business customers.

Atomic Aggregate An object used by a Border Gateway Protocol (BGP) router to inform other BGP routers that the local system has selected a generalized route.

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

Authentication Authentication ensures that digital data transmissions are delivered to the intended recipient. Authentication also validates the integrity of the message for the receiver, including its source (where or whom it came from). The simplest form of authentication requires a username and password for access to a particular account. Authentication protocols can also be based on secret-key encryption, such as DES or 3DES, or on public-key systems that use digital signatures.

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

Autonomous System (AS) A 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 autonomous systems. Each AS has a routing plan that indicates which destinations are reachable through it. This plan is called the *Network Layer Reachability Information (NLRI)* object. Border Gateway Protocol (BGP) routers periodically generate and receive NLRI updates.

Auxiliary port (AUX) This port is usually the same as COM 1 and is used to access external networks.

B8ZS 8 bits zero suppression.

B-Channel The ISDN BRI service provided by your telephone service provider two bearer channels (B channels) and one data channel (D channel). The B channel operates at 64 kbps and carries user data.

Bit error rate (BER) The ratio of error bits to the total number of bits received in a transmission, usually expressed as 10 to a negative power.

Border Gateway Protocol (BGP) An inter-autonomous system routing protocol. BGP routers and autonomous systems exchange routing information for the Internet.

Basic Rate Interface (BRI) An ISDN service also called 2B + D, because it consists of two 64 Kbps B-channels and one 16 Kbps D-channel.

Bridge A device that forwards traffic between network segments based on Data-Link Layer information. These segments share a common Network Layer address space.

Bridge Group interface This interface is also known as the bgroup interface. These interfaces allow several physical ports to be grouped together acting like a pseudo switch. You can group multiple wired interfaces or wireless and wired interfaces so they are located in the same subnet.

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

bundle An aggregation of multiple physical links.

Certificate Revocation List (CRL) A list of invalid certificates.

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

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

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

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. The term *cluster* has another meaning in regards to high availability. *See* High Availability; NetScreen Redundancy Protocol (NSRP). *See also* Border Gateway Protocol (BGP).

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

Communication Protocol A set of rules that allow computers with different operating systems to communicate with each other.

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

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

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

CRL *See* Certificate Revocation List (CRL).

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

Data Encryption Standard (DES) A 40-bit and 56-bit encryption algorithm that was developed by the National Institute of Standards and Technology (NIST). DES is a block-encryption method originally developed by IBM. It has since been certified by the U.S. government for transmission of any data that is not classified 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) Message text and, if required, message signatures can be encrypted using the Data Encryption Standard (DES) algorithm in the Cipher Block Chaining (CBC) mode of operation. The character string “DES-CBC” within an encapsulated Privacy Enhanced Mail (PEM) header field indicates the use of DES–CBC.

Data-Link Connection Identifier (DLCI) Separates customer traffic in Frame Relay configuration.

Data terminal equipment (DTE) A RS-232 interface that is used to exchange information with a serial device. This equipment is the terminating point for a specific network and is typically located on the customer premises.

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

Dead Peer Detection (DPD) DPD allows an IPSec device to verify the current existence and availability of other IPSec peer devices. The device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE) to the peers and waiting for DPD acknowledgements (R-U-THERE-ACK).

Deep Inspection (DI) A mechanism for filtering the traffic permitted by the firewall. Deep Inspection examines Layer 3 and Layer 4 packet headers and Layer 7 application content and protocol characteristics in an effort to detect and prevent any attacks or anomalous behavior that might be present.

Default Route A catch-all routing table entry that defines the forwarding of traffic for destination networks that are not explicitly defined in the routing table. The destination network for the default route is represented by the network address 0.0.0.0/0.

Demilitarized Zone (DMZ) From the military term for an area between two opponents where fighting is prevented. DMZ ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ ethernets link regional networks with routers.

DES *See* Data Encryption Standard (DES).

DES–CBC *See* Data Encryption Standard–Cipher Block Chaining (DES–CBC).

Destination Network Address Translation (NAT-dst) The translation of the original destination IP address in a packet header to a different destination address. ScreenOS supports the translation of one or several original destination IP addresses to a single IP address (one-to-one or many-to-one relationships). The security device also supports the translation of one range of IP addresses to another range (a many-to-many relationship) using address shifting.

When the security device performs NAT-dst without address shifting it can also map the destination port number to a different predetermined port number. When the security device performs NAT-dst with address shifting, it cannot also perform port mapping.

DI *See* Deep Inspection (DI).

Digital signal 0 (DS0) The base for the digital signal X series. Provides a transmission rate of 64 Kbps.

DS1 Digital signal 1, also known as a T1 interface.

DS3 Digital signal 3, also known as a T3 interface.

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.

DMZ *See* Demilitarized Zone (DMZ).

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

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

DPD *See* Dead Peer Detection (DPD).

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

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

Dynamic Routing 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 sends out new routing update messages. These messages populate the network, directing routers to rerun their algorithms and change their routing tables accordingly. There are two common forms of dynamic routing, including Distance Vector Routing and Link State Routing.

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

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

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

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

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

Ethernet A best-effort Local Area Network (LAN) delivery system that uses Carrier Sense Multiple Access with Collision Detection (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 LAN. The most common form of ethernet is 10BaseT, also called *Unshielded Twisted Pair (UTP)*, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. *See also* 100BaseT.

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

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

Extranet The connecting of two or more intranets. An intranet is an internal website 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.

Fast Ethernet *See* 100BaseT.

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

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.

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

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

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

Generic Routing Encapsulation (GRE) A protocol that encapsulates any type of packet within IPv4 unicast packets. For additional information on GRE, refer to RFC 1701, *Generic Routing Encapsulation (GRE)*.

General Packet Radio Service (GPRS) A mobile data service available to users of Global System for Mobile Communication (GSM) mobile phones. It is often described as 2.5G, that is, a technology between the second generation (2G) and third generation (3G) of mobile telephony. GPRS provides moderate speed data transfer by using unused Time Division Multiple Access (TDMA) channels in the GSM network.

GGSN *See* Gateway GPRS Support Node (GGSN).

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

General Packet Radio Service (GPRS) A packet-based technology that enables high-speed wireless Internet and other data communications. GPRS provides more than three to four times greater speed than conventional Global System for Mobile Communications (GSM) systems.

G-PDU A user data message consisting of a T-PDU plus a GPRS Tunneling Protocol (GTP) header. *See also* T-PDU.

Gi interface The interface between a GSN and an external network or the Internet. *See* GPRS Support Node (GSN).

Global System for Mobile Communication (GSM) A globally accepted standard for digital cellular communication. GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard that formulates specifications for a pan-European mobile cellular radio system operating at 900 MHz.

Gn interface The interface between two GSNs within the same Public Land Mobile Network (PLMN).

Gp interface The interface between two GSNs located in different Public Land Mobile Networks (PLMNs).

GPRS *See* General Packet Radio Service (GPRS).

GPRS Roaming Exchange (GRX) Since the Gp interface is IP based, it must support appropriate routing and security protocols to enable a subscriber to access its home services from any of its home PLMN’s roaming partners. Many GPRS operators/carriers have abstracted these functions through the GPRS Roaming Exchange (GRX). This function is typically provided by a third-party IP network that offers VPN services to connect the roaming partners. The GRX service provider ensures that all aspects of routing and security between the networks are optimized for efficient operation. *See also* General Packet Radio Service (GPRS).

GPRS Support Node (GSN) A term used to include both Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN). *See also* General Packet Radio Service (GPRS).

GPRS Tunneling Protocol (GTP) An IP-based protocol used within Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) networks. GTP is layered on top of User Datagram Protocol (UDP). There are actually three separate protocols: GTP’, GTP-Control (GTP-C), and GTP User (GTP-U). *See also* General Packet Radio Service (GPRS); GTP-Control (GTP-C) Message; GTP-User (GTP-U) Message.

GRX *See* GPRS Roaming Exchange (GRX).

GSM *See* Global System for Mobile Communication (GSM).

GSN *See* GPRS Support Node (GSN).

GTP *See* GPRS Tunneling Protocol (GTP).

GTP-Control (GTP-C) Message GTP-C messages are exchanged between GPRS Support Node (GSN) pairs in a path. The messages are used to transfer GSN capability information between GSN pairs; to create, update and delete GPRS Tunneling Protocol (GTP) tunnels; and for path management. *See also* GPRS Tunneling Protocol (GTP); GTP Tunnel.

GTP Protocol Data Unit (GTP-PDU) Either a GTP-C or a GTP-U message. *See also* GPRS Tunneling Protocol (GTP).

GTP Tunnel A GPRS Tunneling Protocol (GTP) tunnel in the GTP-U plane is defined for each Packet Data Protocol (PDP) Context in the GSNs. A GTP tunnel in the GTP-C plane is defined for all PDP Contexts with the same PDP address and access point name (APN) for tunnel-management messages or for each mobile station (MS) for messages not related to tunnel management. A GTP tunnel is identified in each node with a Tunnel Endpoint Identifier (TEID), an IP address, and a User Datagram Protocol (UDP) port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.

GTP-User (GTP-U) Message GTP-U messages are exchanged between GPRS Support Node (GSN) pairs or GSN/Radio Network Controller (RNC) pairs in a path. The GTP-U messages are used to carry user data packets and signaling messages for path management and error indication. The user data transported can be packets in any of IPv4, IPv6, or PPP formats.

HA *See* High Availability (HA).

Hello Interval The amount of time that elapses between instances of Hello packets. *See* Hello Packet.

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

High Availability (HA) Configuring pairs of security devices with NetScreen Redundancy Protocol (NSRP) to ensure service continuity in the event of a network outage or device failure.

HLR *See* Home Location Register (HLR).

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

Home Location Register (HLR) A database within a cellular network that stores current details about a subscriber, including the equipment in use, the service(s) required, the user’s identification encryption code and home cell, and the network the subscriber was last known to have used.

Hub A hardware device used to link computers (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 Layer (most commonly ethernet). A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.

Import Rules When you have two or more virtual routers on a security device, you can configure import rules on one virtual router that define which routes are allowed to be learned from another virtual router. If you do not configure any import rules for a virtual router, all routes that are exported to that virtual router are accepted. *See also* Export Rules.

International Mobile Station Identity (IMSI) A GPRS Support Node (GSN) identifies a mobile station by its IMSI, which is composed of three elements: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). The MCC and MNC combined constitute the IMSI prefix and identify the mobile subscriber's home network, or Public Land Mobile Network (PLMN). *See also* GPRS Support Node (GSN); Public Land Mobile Network (PLMN).

Internet A system of linked computer networks, international in scope, that facilitates data communications 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. Also known as the Net. Originally designed by the U.S. Defense Department so that a communications signal could withstand a nuclear war and serve military institutions worldwide. The Internet was first known as the ARPAnet. *See also* Intranet.

Internet Control Message Protocol (ICMP) Occasionally a gateway or destination host uses ICMP to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher-level protocol; however, ICMP is actually an integral part of IP and must be implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. IP is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communications environment, not to make IP reliable.

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

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*, which is used in a connectionless, best-effort delivery system. IP defines how information gets passed between systems across the Internet.

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

Infranet A public network that combines the ubiquitous connectivity of the Internet with the assured performance and security of a private network.

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.

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 authentication, integrity, and confidentiality for secure communications and supports key exchanges even in larger networks. *See also* Data Encryption Standard-Cipher Block Chaining (DES-CBC); Encapsulating Security Protocol/Authentication Header (ESP/AH).

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

Integrated Services Digital Network (ISDN) ISDN is an international communications standard for sending voice, video, and data over digital telephone lines.

Keepalive Interval The time, in seconds, that elapses between keepalive packets, which ensure that the TCP connection is up between a local BGP router and its neighbor.

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. *See also* Internet Security Association and Key Management Protocol (ISAKMP).

Link State Link-state routing protocols operate using an algorithm commonly called *Shortest Path First (SPF)*. 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 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 LAN 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 A Border Gateway Protocol (BGP) attribute superior to the Multi-Exit Discriminator (MED) attribute for selecting a packet's path. LOCAL_PREF is the attribute used most often to configure preferences for one set of paths over another. *See also* Multi-Exit Discriminator (MED).

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

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

MCC *See* Mobile Country Code (MCC).

MED *See* Multi Exit Discriminator (MED).

Media Access Control (MAC) Address 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, the MAC address is the same as the ethernet address.) When you are connected to the Internet from your computer (or *host*, as the Internet protocol views it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sub-layer of the Data-Link Control (DLC) Layer of telecommunications protocols. There is a different MAC sub-layer for each physical device type.

Member AS The name of the Autonomous System (AS) being included in a Border Gateway Protocol (BGP) confederation.

Message Digest 5 (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.

Metric A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network with the same preference value. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value when defining a static route.

MIME *See* Multipurpose Internet Mail Extension (MIME).

MIP *See* Mapped IP Address (MIP).

MNC *See* Mobile Network Code (MNC).

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

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

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

MSIN *See* Mobile Subscriber Identification Number (MSIN).

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

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

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

Multi Exit Discriminator (MED) Comparison A Border Gateway Protocol (BGP) attribute used to determine an ideal link to reach a particular prefix in or behind the current Autonomous System (AS). The MED contains a metric expressing a degree of preference for entry into the AS. You can establish precedence for one link over others by configuring a MED value for one link that is lower than other links. The lower the MED value, the higher priority the link has. The way this occurs is that one AS sets the MED value and the other AS uses the value in deciding which path to choose.

Multipurpose Internet Mail Extension (MIME) Extensions that allow users to download different types of electronic media, such as video, audio, and graphics.

NAT *See* Network Address Translation (NAT).

NAT-dst *See* Destination Network Address Translation (NAT-dst).

NAT-src *See* Network Address Translation (NAT).

NAT-Traversal (NAT-T) A method for allowing IPSec traffic to pass through NAT devices along the data path of a Virtual Private Network (VPN) by adding a layer of User Datagram Protocol (UDP) encapsulation. The method first provides a means for detecting NAT devices during Phase 1 IKE exchanges and then provides a means for traversing them after Phase 2 IKE negotiations are complete.

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 (AS), 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 also* 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; Subnet Mask.

NetScreen Gatekeeper Protocol (NSGP) A proprietary protocol that uses Transmission Control Protocol (TCP) and monitors the connectivity between client and server by sending Hello messages at specified intervals.

NetScreen Redundancy Protocol (NSRP) A proprietary protocol that provides configuration and Run-Time Object (RTO) redundancy and a device failover mechanism for security units in a high availability (HA) cluster.

NetScreen Reliable Transfer Protocol (NRTP) A proprietary protocol for multicasting NetScreen Redundancy Protocol (NSRP) control messages to multiple receivers when security devices are in a redundancy cluster (interconnected through the High Availability, or HA, ports). NRTP ensures that the primary security device always forwards configuration and policy messages to the backup devices.

Network Address Translation (NAT) The translation of the source IP address in a packet header to a different IP address. Translated source IP addresses can come from a dynamic IP (DIP) address pool or from the IP address of the egress interface. When the security device draws addresses from a DIP pool, it can do so dynamically or deterministically. When doing the former, it randomly draws an address from the DIP pool and translates the original source IP address to the randomly selected address. When doing the latter, it uses address shifting to translate the source IP address to a predetermined IP address in the range of addresses that constitute the pool. When the security device uses the IP address of the egress interface, it translates all original source IP addresses to the address of the egress interface.

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

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

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

Network Service Access Point Identifier (NSAPI) An index to the Packet Data Protocol (PDP) context that is using the services provided by the lower layer Subnetwork Dependent Convergence Protocol (SNDCP). One PDP may have several PDP contexts and NSAPIs. *See also* Packet Data Protocol (PDP).

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

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

NSAPI *See* Network Service Access Point Identifier (NSAPI).

NSGP *See* NetScreen Gatekeeper Protocol (NSGP).

NSRP *See* NetScreen Redundancy Protocol (NSRP).

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

Open Shortest Path First (OSPF) A dynamic routing protocol intended to operate within a single Autonomous System (AS).

Packet Data Protocol (PDP) The primary protocol(s) used for packet data communications on a PDN, for example, TCP/IP on the Internet.

Packet Data Protocol (PDP) Context A user session on a GPRS network.

PDU *See* Protocol Data Unit.

Peer *See* Neighbor.

PIM *See* Protocol Independent Multicast (PIM).

PLMN *See* Public Land Mobile Network (PLMN).

Point-to-Point Protocol over Ethernet (PPPoE) Allows multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. You can configure PPPoE client instances, including the username and password, on any or all interfaces on some security devices.

Policies Policies provide the initial protection mechanism for the firewall, allowing you to determine which traffic passes across it based on IP session details. You can use policies to protect the resources in a security zone from attacks from another zone (interzone policies) or from attacks from within a zone (intrazone policies). You can also use policies to monitor traffic attempting to cross your firewall.

Port Address Translation (PAT) The translation of the original source port number in a packet to a different, randomly designated port number.

Port Mapping The translation of the original destination port number in a packet to a different, predetermined port number.

Port Mode A feature supported on some Juniper Networks security appliances, port mode allows you to select one of several different sets of port, interface, and zone bindings on the device. Changing the port mode removes any existing configurations on the device and requires a system reset.

Preference A value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network. The preference value is determined by the protocol or origin of the route. The lower the preference value of a route, the more likely the route is to be selected as the active route.

Prefix An IP address that represents a route.

Protocol Data Unit (PDU) Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data.

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

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

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

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

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

Querier A router that sends Internet Group Management Protocol (IGMP) messages to all hosts in the network to solicit group membership information. There is usually one querier for each network.

Real-Time Transport Control Protocol (RTCP) RTCP provides information about the members of a session and the quality of the communication. It synchronizes media streams by associating timestamps and a real-time clock.

Real-Time Transport Protocol (RTP) RTP is used to ensure the reception of packets in a chronological sequence by assigning timestamps and sequence numbers to the packet header. Every RTP session has a corresponding RTCP session. *See* Real-Time Transport Control Protocol (RTCP).

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

Redistribution 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 that uses a different protocol.

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

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

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

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

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

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

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

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

Router A hardware or (in a security environment) virtual device that distributes data to all other routers and receiving points inside or outside 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 Information Protocol (RIP) A dynamic routing protocol used within moderate-sized autonomous systems.

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.

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

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).

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

Secure Hash Algorithm-1 (SHA-1) 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.)

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

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

Security Parameters Index (SPI) A hexadecimal value that uniquely identifies each tunnel. It also tells the security 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.

Session Description Protocol (SDP) SDP session descriptions appear in many SIP messages and provide information that a system can use to join a multimedia session. SDP might include information such as IP addresses, port numbers, times, dates, and information about the media stream.

Session Initiation Protocol (SIP) SIP is an Internet Engineering Task Force (IETF)-standard protocol for initiating, modifying, and terminating multimedia sessions over the Internet. Such sessions might include conferencing, telephony, or multimedia, with features such as instant messaging and application-level mobility in network environments.

Service Set Identifier (SSID) A 32-character unique identifier attached to the header of packets sent over a wireless local area network (WLAN), which acts as a password when a mobile device tries to connect to the basic service set (BSS). The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. *See also* Basic Service Set (BSS).

Serving GPRS Support Node (SGSN) Connects one or more base station controllers (BSCs) to the GPRS backbone network, providing IP connectivity to the Gateway GPRS Support Node (GGSN).

Shared Distribution Tree A multicast distribution tree where the source transmits the multicast traffic to the rendezvous point (RP), which then forwards the traffic downstream to receivers on the distribution tree.

Shortest Path Tree (SPT) A multicast distribution tree where the source is at the root of the tree and it forwards multicast data downstream to each receiver. This is also referred to as a *source-specific tree.*

Signaling Message GPRS Tunneling Protocol (GTP) signaling messages are exchanged between GPRS Support Node (GSN) pairs in a path. The messages are used to transfer GSN capability information between GSN pairs and to create, update, and delete GTP tunnels. *See* G-PDU.

Signal-to-Noise Ratio (SNR) The ratio of the amplitude of a desired analog or digital data signal to the amplitude of noise in a transmission channel at a specific time SNR is typically expressed logarithmically in decibels (dB).

Source-Based Routing (SBR) You can configure a virtual router on a security device to forward traffic based on the source address of the data packet instead of just the destination address.

Source Interface-Based Routing (SIBR) SIBR allows the security device to forward traffic based on the source interface (the interface on which the data packet arrives on the security device).

SSID *See* Service Set Identifier (SSID).

Static Routing User-defined routes that cause packets moving between a source and a destination to take a specified path. Static routing algorithms are table mappings established by the network administrator prior to the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

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

Subinterface 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; Netmask.

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

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

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

TEID *See* Tunnel Endpoint Identifier (TEID).

TID *See* Tunnel Identifier (TID).

Three-Way Handshake A Transmission Control Protocol (TCP) connection is established with a triple exchange of packets known as a three-way handshake: A sends a synchronize (SYN) packet to B, B responds with a synchronize/acknowledge (SYN/ACK) packet, and A responds with an acknowledge (ACK) packet.

T-PDU The payload that is tunneled in the GPRS Tunneling Protocol (GTP) tunnel.

Transmission Control Protocol/Internet Protocol (TCP/IP) A set of communication protocols that supports peer-to-peer connectivity functions both for Local Area Networks (LANs) and for Wide Area Networks (WANs). TCP/IP controls how data is transferred between computers on the Internet. See *Communication Protocols*.

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

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

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

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

Tunnel Interface 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.

Uniform Resource Locator (URL) A standard method developed for specifying the location of a resource available electronically. Also referred to as a *location* or an *address*, a URL specifies the location of files on servers. A general URL has the syntax *protocol://address*. For example, http://www.juniper.net/support/manuals.html specifies that the protocol is HTTP and that the address is www.juniper.net/support/manuals.html.

Unshielded Twisted Pair (UTP) *See* 10BaseT. *See also* 100BaseT.

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 12 Mbps.

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

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

V.92 modem A dial-up modem specification from the International Telecommunications Union (ITU) that introduces new features providing convenience and performance for the modem user.

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

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

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

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

Virtual Private Network (VPN) A simple, cost-effective, and secure way for corporations to provide telecommuters and mobile professionals with 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 The component of ScreenOS that performs routing functions. By default, a security device supports two virtual routers: Untrust-VR and Trust-VR.

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

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

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

WebTrends A product offered by NetIQ that supports the creation of customized reports based on the logs generated by a security device. WebTrends enables information to be displayed graphically.

WEP *See* Wired Equivalent Privacy (WEP).

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

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

Wireless access point (AP) A hardware device that acts as a communication hub for wireless clients to connect to a wired LAN.

Wireless local area network (WLAN) A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

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

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

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

Zone 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 a logical entity that performs a specific function (a function zone).

Master Index

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

Numerics

3DES 5-6
3DES encryption 14-121
4in6 tunneling
  basic setup 14-115
  definition 14-115
6in4 tunneling 14-111
  basic setup 14-120
  over IPv4 WAN 14-120
6over4 tunneling
  addresses, handling 14-99
  definition 14-98
  manual tunneling 14-99
  types 14-98
  when to use 14-98
6to4
  addresses 14-8, 14-102, 14-108
  hosts 14-107
  relay routers 14-102, 14-103
  routers 14-102
  tunneling 14-98, 14-102
  tunneling, description 14-102

A

AAL5 encapsulations 12-70
Access Concentrator (AC) 14-46
Access Control List
  See ACL
access lists
  for routes 7-40
  IGMP 7-158
  multicast routing 7-151
  PIM-SM 7-199
Access Point Name
  See APN
access policies
  See policies
ACL 12-131
ActiveX controls, blocking 4-161
address books
  addresses, adding 2-115
  addresses, modifying 2-115
  addresses, removing 2-118
  entries 2-114
  group entries, editing 2-118
  groups 2-116
  See also addresses
address groups 2-116, 2-178
  creating 2-118
  editing 2-118
  entries, removing 2-118
  options 2-116
address negation 2-198
address sweep 4-8
address translation
  See NAT, NAT-dst, *and* NAT-src
addresses
  address book entries .... 2-114 to 2-118
  autoconfiguration 14-11
  defined 2-178
  in policies 2-178
  IP lifetime for XAuth users 9-62
  IP, host and network IDs 2-56
  L2TP assignments 9-76
  link-local 14-12
  private 2-56
  public 2-56
  splitting 14-44
addresses, handling
  4in6 tunneling 14-116
  6to4 tunneling 14-104
  destination address translation 14-84
  DIP from IPv4 to IPv6 14-84
  DIP from IPv6 to IPv4 14-83
  IPv4 hosts to a single IPv6 host 14-113
  IPv6 hosts to multiple IPv4 hosts 14-87
  manual tunneling 14-99
addresses, overlapping ranges 10-62, 10-70
addresses, XAuth
  assignments 9-60
  authentication, and 9-71
  timeout 9-62
admin users 9-2
  privileges from RADIUS 9-2
  server support 9-12
  timeout 9-16

administration
- Command Line Interface (CLI) 3-9
- restricting 3-40
- WebUI 3-2

administration, vsys 10-7
administrative traffic 3-27
admins 10-2
- changing passwords 10-4, 10-7
- types 10-4

ADSL
- connecting the cable... 12-70
- overview... 12-69
- VPN tunnel... 12-96

Advanced Encryption Standard (AES)....................... 5-6
AES.. 5-6
AES128 encryption 14-121
agents, zombie...4-27, 4-29
aggregate interfaces 2-46, 11-47
aggressive aging ....4-30 to 4-32
Aggressive mode 5-10
AH 5-3, 5-5
AIM... 4-124
alarms
- email alert 3-65
- reporting to NetScreen-Security Manager........ 3-23
- thresholds 3-66
- traffic ....3-65 to 3-68

alarms, thresholds 2-184
ALG...4-55, 6-17
- SIP... 6-13
- SIP NAT 6-23

ALGs
- for custom services... 2-180
- MS RPC.. 2-141
- RTSP 2-142
- Sun RPC 2-139

America Online Instant Messaging
- *See* AIM

anti-replay checking...5-52, 5-59
APN
- filtering... 13-15
- selection mode 13-15

Application Layer Gateway
- *See* ALG

application option, in policies................................ 2-180
ARP 2-92, 11-83
- broadcasts.. 11-9
- lookup.. 11-39
- path monitoring 11-112

ARP, ingress IP address... 2-94
asset recovery log.. 3-65
Asynchronous Transfer Mode
- *See* ATM

ATM 12-70
attack actions ....4-132 to 4-140
- close 4-132
- close client 4-133
- close server 4-132
- drop 4-133
- drop packet 4-133
- ignore... 4-133
- none... 4-133

attack database updates
- downloading 4-222
- overview.. 4-222

attack object database ....4-114 to 4-121
- auto notification and manual update............. 4-118
- automatic update 4-117
- changing the default URL................................ 4-120
- immediate update 4-116
- manual update.......................................4-119, 4-120

attack object groups 4-128
- applied in policies 4-122
- changing severity 4-128
- Help URLs 4-125
- logging 4-143
- severity levels 4-128

attack objects ....4-111, 4-121 to 4-128
- brute force... 4-140
- custom 4-204
- disabling 4-131
- IDP 4-175
- negation 4-156
- overview.. 4-201
- protocol anomalies 4-128, 4-155
- protocol anomaly 4-202
- re-enabling 4-132
- signature.. 4-202
- stateful signatures 4-126
- stream signatures... 4-127
- TCP stream signatures..................................... 4-153

attack protection
- policy level 4-4
- security zone level 4-4

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

attacks
- common objectives 4-1
- detection and defense options .... 4-2 to 4-4
- DOS .... 4-27 to 4-51
- ICMP
  - floods 4-46
  - fragments 4-228
- IP packet fragments 4-232
- Land 4-48
- large ICMP packets 4-229
- Ping of Death 4-49
- Replay 5-12
- session table floods 4-17, 4-28
- stages of 4-2
- SYN floods .... 4-34 to 4-39
- SYN fragments 4-233
- Teardrop 4-50
- UDP floodsUDP floods 4-47
- unknown MAC addresses 4-39
- unknown protocols 4-231
- WinNuke 4-51

attacks, Overbilling .... 13-26 to 13-28

auth servers .... 9-11 to 9-32
- addresses 9-16
- authentication process 9-15
- backup 9-16
- default 9-31
- defining .... 9-26 to 9-32
- external 9-15
- ID number 9-16
- idle timeout 9-16
- LDAP .... 9-24 to 9-26
- maximum number 9-12
- SecurID 9-23
- SecurID, defining 9-28
- types 9-16
- XAuth queries 9-61

auth servers, objects
- names 9-16
- properties 9-16

auth servers, RADIUS .... 9-17 to 9-19
- defining 9-26
- user-type support 9-18

auth table entry 9-35

auth users .... 9-37 to 9-56
- admin 9-2
- groups 9-37, 9-40
- IKE 9-12, 9-57
- in policies 9-38
- L2TP 9-76
- local database .... 9-13 to 9-14
- logins, with different 9-5
- manual key 9-12
- multiple-type 9-4
- pre-policy auth 2-183
- run-time auth process 2-182
- run-time authentication 2-182
- server support 9-12
- timeout 9-16
- types and applications .... 9-1 to 9-5
- user types 9-11
- WebAuth 2-183, 9-12
- XAuth 9-60

auth users, authentication
- auth servers, with 9-12
- point of 9-1
- pre-policy 9-39

auth users, run-time
- auth process 9-38
- authentication 9-38
- user groups, external 9-45
- user groups, local 9-42
- users, external 9-43
- users, local 9-41

auth users, WebAuth 9-39
- user groups, external 9-51
- user groups, local 9-50
- with SSL (user groups, external) 9-53

authentication 14-112, 14-115, 14-138
- algorithms 5-6, 5-51, 5-54, 5-57, 5-61
- Allow Any 2-183
- NSRP 11-9
- NSRP-Lite 11-101
- policies 2-182
- users 2-182

Authentication and Encryption
- Multiple WEP Keys 12-121
- Wi-Fi Protected Access
  - *See* WPA
- Wireless Equivalent Privacy
  - *See* WEP

authentication and encryption, using RADIUS server 12-122

Authentication Header (AH) 5-5

authentication servers
- *See* auth servers

authentication users
- *See* auth users

autoconfiguration
    address autoconfiguration 14-11
    router advertisement messages 14-12
    stateless... 14-11
AutoKey IKE VPN..................................... 3-41, 3-76, 5-7
    management 5-7
Autonomous System (AS) numbers...................... 7-107
AV objects
    timeout.. 4-82
AV scanning..4-58 to 4-80
    AV resources per client 4-77
    decompression 4-84
    fail-mode 4-77
    file extensions 4-84
    FTP.. 4-65
    HTTP 4-66
    HTTP keep-alive 4-79
    HTTP trickling.. 4-79
    HTTP webmail 4-68
    IMAP 4-69
    MIME 4-67
    POP3.. 4-69
    SMTP 4-71
    subscription 4-74

B

back store 3-91
backdoor rulebase
    adding to Security Policy................................. 4-197
    overview... 4-197
backdoor rules ....4-197 to 4-201
    configuring actions 4-199
    configuring Match columns 4-198
    configuring operation 4-199
    configuring services... 4-199
    configuring severity 4-201
    configuring source and destination 4-199
    configuring targets... 4-201
    configuring zones... 4-198
bandwidth 2-185
    guaranteed 2-185, 2-205, 2-211
    managing 2-205
    maximum 2-185, 2-205, 2-211
    maximum, unlimited....................................... 2-206
bandwidth priority
    default 2-210
    levels... 2-210
    queues 2-210
banners... 9-10
BGP
    AS-path access list.. 7-116
    communities... 7-124
    confederations.. 7-122
    configurations, security 7-113
    configurations, verifying 7-112
    external 7-105
    internal 7-105
    load-balancing 7-36
    message types 7-104
    neighbors, authenticating 7-113
    parameters.. 7-115
    path attributes 7-105
    protocol overview 7-104
    regular expressions.. 7-116
    virtual router, creating an instance in 7-107
BGP routes
    adding... 7-117
    aggregation 7-125
    attributes, setting 7-119
    conditional advertisement 7-118
    default, rejecting.. 7-114
    redistributing 7-116
    reflection 7-120
    suppressing.. 7-126
    weight, setting 7-118
BGP routes, aggregate
    aggregation 7-125
    AS-Path in... 7-127
    AS-Set in 7-125
    attributes of.. 7-128
BGP, configuring
    peer groups 7-109
    peers 7-109
    steps.. 7-106
BGP, enabling
    in VR 7-107
    on interface.. 7-108
bit stream 3-91
bridge group
    logical interface 2-46
bridge groups
    unbinding... 2-55
browser requirements.. 3-2
brute force
    attack actions.. 4-140
brute force attack objects 4-140
bypass-auth 9-61

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

C

- CA certificates 5-22, 5-25
- cables, serial 3-19
- C-bit parity mode 12-13
- Certificate Revocation List 5-23, 5-34
  - loading 5-23
- certificates 5-7
  - CA 5-22, 5-25
  - loading 5-28
  - loading CRL 5-23
  - local 5-25
  - requesting 5-26
  - revocation 5-25, 5-34
  - via email 5-25
- Challenge Handshake Authentication Protocol
  - *See* CHAP
- channels, finding available 12-131
- CHAP 5-206, 5-209, 9-71
- Chargen 4-123
- CLI 3-9
- CLI, set arp always-on-dest 2-83, 2-86
- CLI, set vip multi -port 8-82
- clock, system
  - *See* system clock
- cluster names, NSRP 11-8, 11-101
- clusters ....11-8 to 11-10, 11-35, 11-98 to 11-101
- Command Line Interface
  - *See* CLI
- Command Line Interface (CLI) 14-30, 14-32
- commands
  - clear cluster 11-100
  - debug cluster 11-100
- common names 9-25
- CompactFlash 3-54
- compatibility-mode option
  - T3 interfaces 12-20
- configuration examples
  - 6to4 host, tunneling to a 14-108
  - access lists and route maps 14-61
  - delegating prefixes 14-38, 14-40
  - DNS server information, requesting 14-43
  - IPv4 tunneling over IPv6 (autokey IKE) 14-117
  - IPv6 requests to multiple IPv4 hosts 14-87
  - IPv6 to an IPv4 network over IPv4 14-113
  - IPv6 tunneling over IPv4 (autokey IKE) 14-121
  - manual tunneling 14-100
  - native host, tunneling to a 14-104
  - PPPoE instance, configuring a 14-46
  - static route redistribution 14-61
- configuration settings, browser requirements 3-2
- configurations
  - full-mesh 11-89
  - ISP for serial interfaces 11-74
  - modem for serial interfaces 11-72
- connection policy for Infranet Enforcer, configuring 9-34
- console 3-54
- containers 5-184
- content filtering ....4-53 to 4-108
- control messages 11-26
  - HA 11-28
  - HA physical link heartbeats 11-28
  - RTO heartbeats 11-28
  - VSD heartbeats 11-28
- cookies, SYN 4-44
- country codes and channels 12-129
- country codes and channels, regulatory domain for 12-129
- CRL
  - *See* Certificate Revocation List
- cryptographic options ....5-48 to 5-61
  - anti-replay checking 5-52, 5-59
  - authentication algorithms 5-51, 5-54, 5-57, 5-61
  - authentication types 5-50, 5-56
  - certificate bit lengths 5-50, 5-56
  - dialup ....5-55 to 5-61
  - dialup VPN recommendations 5-61
  - encryption algorithms ....5-51 to 5-57, 5-61
  - ESP 5-54, 5-60
  - IKE ID ....5-51 to 5-52, 5-57 to 5-58
  - IPSec protocols 5-53, 5-60
  - key methods 5-49
  - PFS 5-53, 5-59
  - Phase 1 modes 5-49, 5-56
  - site-to-site ....5-48 to 5-55
  - site-to-site VPN recommendations 5-55
  - Transport mode 5-60
  - Tunnel mode 5-60
- CSU compatibility, T3 interfaces 12-20
- custom services 2-134
- custom services, in root and vsys 2-134
- Customer Premises Equipment (CPE) 14-39, 14-134

D

- Data Encryption Standard (DES) 5-6
- data messages 11-29
- databases, local 9-13 to 9-14
- DDoS 4-27
- decompression, AV scanning 4-84
- Deep Inspection (DI) 4-129 to 4-153
  - attack actions 4-132 to 4-140
  - attack object database 4-114 to 4-121
  - attack object groups 4-128
  - attack object negation 4-156
  - attack objects 4-111
  - changing severity 4-128
  - context 4-I
  - custom attack objects 4-149
  - custom services 4-145 to 4-149
  - custom signatures 4-150 to 4-153
  - disabling attack objects 4-131
  - license keys 4-112
  - logging attack object groups 4-143
  - overview 4-110
  - protocol anomalies 4-128
  - re-enabling attack objects 4-132
  - regular expressions 4-150 to 4-151
  - signature packs 4-114
  - stateful signatures 4-126
  - stream signatures 4-127
- demand circuits, RIP 7-94
- Denial-of-Service
  - *See* DoS
- DES 5-6
- destination gateway 14-99
- device failover 11-79
- devices, resetting to factory defaults 3-39
- Device-Unique Identification (DUID) 14-36
- DHCP 2-106, 2-110, 2-256, 4-123
  - client 2-237
  - HA 2-243
  - PXE scenario 2-249
  - relay agent 2-237
  - server 2-237
- dialup recovery 12-107
- dictionary file, RADIUS 9-2
- Diffie-Hellman 5-10
- Diffie-Hellman Group 14-121
- DiffServ 2-186, 2-212
  - *See also* DS Codepoint Marking
- digital signature 5-20
- DIP 2-109, 2-152 to 2-155, 3-92
  - fix-port 2-154
  - groups 2-165 to 2-167
  - PAT 2-153, 2-154
  - pools 2-181
  - pools, modifying 2-155
- DIP pools
  - address considerations 8-14
  - extended interfaces 5-139
  - NAT for VPNs 5-139
  - NAT-src 8-1
  - size 8-14
- Discard 4-123
- Discrete multitone
  - *See* DMT
- dissimilar IP stacks 14-84, 14-86
- distinguished name (DN) 5-181
- distinguished names 9-25
- DMT 12-71
- DN 5-181
- DNS 2-229, 4-123
  - addresses, splitting 2-235
  - lookups 2-230
  - lookups, domain 2-235
  - servers 2-257
  - servers, tunneling to 2-235
  - status table 2-231
- DNS, L2TP settings 5-209
- Domain Name System
  - address splitting 14-44
  - address translation 14-93
  - addresses, splitting 14-45
  - DHCP client host 14-43
  - DHCPv6 search list 14-36
  - DNS refresh 14-42
  - DNS search list 14-43
  - DNS server 14-132
  - domain lookups 14-44
  - IPv4 or IPv6 addresses 14-42
  - partial domain names 14-36
  - proxy DNS 14-44
  - *See* DNS
  - servers, tunneling to 14-44
- DoS
  - firewall 4-28 to 4-33
  - network 4-34 to 4-48
  - OS-specific 4-49 to 4-51
  - session table floods 4-17, 4-28
- DoS attacks 4-27 to 4-51
- drop-no-rpf-route 4-19
- DS Codepoint Marking 2-206, 2-212
- DSL 2-251, 2-256
- dual Untrust interfaces 11-48
- dual-stack architecture 14-50
  - dissimilar networks 14-50
  - dissimilar WAN backbones 14-50
  - routing tables 14-50
- Duplicate Address Detection (DAD)
  - DAD Retry Count 14-31
  - function 14-31

Dynamic Host Configuration Protocol version 6 (DHCPv6)
client and server ... 14-36
delegated prefixes ... 14-38
purposes ... 14-35
TLA and SLA ... 14-37
Dynamic IP ... 14-82
from IPv6 to IPv4 ... 14-83
See DIP
Dynamic IP (DIP) pools ... 2-155, 2-181
dynamic packet filtering ... 4-3

E

Echo ... 4-123
ECMP ... 7-36, 7-59
email alert notification ... 3-68, 3-70
Encapsulating Security Payload
See ESP
encapsulation ... 14-103, 14-111, 14-117
encryption ... 14-112, 14-115
3DES ... 14-121
AES128 ... 14-121
algorithms ... 5-6, 5-51, 5-54 to 5-61
NSRP ... 11-9
NSRP-Lite ... 11-101
encryption, SecurID ... 9-23
endpoint host state mode
Base Reachable Time ... 14-30
Duplicate Address Detection (DAD) ... 14-31
Probe Forever state ... 14-31
Probe Time ... 14-31
Reachable Time ... 14-30
Retransmission Time ... 14-31
Stale mode ... 14-30
ESP ... 5-3, 5-5, 5-6
authenticate only ... 5-54
encrypt and authenticate ... 5-54, 5-60
encrypt only ... 5-54
evasion ... 4-15 to 4-25
event log ... 3-54
exe files, blocking ... 4-161
exempt rulebase
adding to Security Policy ... 4-193
overview ... 4-192
exempt rules ... 4-192 to 4-196
configuring ... 4-193
configuring attacks ... 4-195
configuring from the Log Viewer ... 4-196
configuring Match columns ... 4-194
configuring source and destination ... 4-194
configuring targets ... 4-195
configuring zones ... 4-194
exploits
See attacks
extended channels, setting for WLAN ... 12-130

F

factory defaults, resetting devices to ... 3-39
fail-mode ... 4-77
failover
devices ... 11-79
dual Untrust interfaces ... 11-49, 11-50
object monitoring ... 11-81
serial interfaces ... 11-75
virtual systems ... 11-88
VSD groups ... 11-80
file extensions, AV scanning ... 4-84
filter source route ... 3-93
FIN scans ... 4-15
FIN without ACK flag ... 4-13
Finger ... 4-123
floods
ICMP ... 4-46
session table ... 4-28
SYN ... 4-34 to 4-39, 4-44
UDP ... 4-47
fragment reassembly ... 4-54 to 4-57
full-mesh configuration ... 11-89
function zone interfaces ... 2-47
HA ... 2-48
management ... 2-47

G

gatekeeper devices ... 6-1
Generic Routing Encapsulation (GRE) ... 7-151
Gi interface ... 13-2
global unicast addresses ... 14-102, 14-120
global zones ... 8-82
Gn interface ... 13-2
Gopher ... 4-123
Gp interface ... 13-2
GPRS Tunneling Protocol (GTP)
See GTP
graphs, historical ... 2-184
group expressions ... 9-5 to 9-9
operators ... 9-5
server support ... 9-12
users ... 9-6
group IKE ID
certificates ... 5-181 to 5-190
preshared keys ... 5-190 to 5-196
groups
addresses ... 2-116
services ... 2-150

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

GTP
  Access Point Name (APN) filtering................. 13-15
  GTP-in-GTP packet filtering............................. 13-13
  IMSI prefix filtering.. 13-16
  inspection objects ....13-5 to 13-7
  IP fragmentation 13-13
  packet sanity check 13-8
  policy-based.. 13-5
  protocol 13-2
  standards 13-9
  stateful inspection.. 13-23
  tunnel timeout.. 13-25
GTP messages 13-10
  length, filtering by... 13-9
  rate, limiting by.. 13-12
  type, filtering by... 13-10
  types 13-10
  versions 0 and 1... 13-10
GTP traffic
  counting 13-33
  logging... 13-31
GTP tunnels
  failover 13-24
  limiting 13-23
  timeout.. 13-25

H

HA
  DHCP... 2-243
  interfaces 2-48
  interfaces, virtual HA.. 2-48
  See high availability
  See also NSRP
hanging GTP tunnel.. 13-25
hash-based message authentication code................ 5-6
hashing, Secure Hashing Algorithm (SHA) 14-121
heartbeats
  HA physical link 11-28
  RTO.. 11-28
  VSD 11-28
Help files... 3-2
high availability
  cabling ....11-32 to 11-34
  data link... 11-29
  IP tracking 11-83, 11-112
  LED 11-18
  link probes 11-30
  messages 11-28
  path monitoring 11-111
  See HA
  virtual interfaces... 11-34
high availability (HA) 13-4, 13-24
high availability failover
  active/active 11-4
  active/passive.. 11-3
high availability interfaces
  aggregate 11-47
  cabling network as HA links 11-33
  dual Untrust 11-48
  redundant.. 11-42
  serial 11-71
high-watermark threshold 4-30
historical graphs.. 2-184
HMAC 5-6
Host mode...14-46, 14-116
HTTP
  blocking components ....4-160 to 4-162
  keep-alive 4-79
  session timeout 4-31
  trickling 4-79
HTTP, session ID 3-4
HyperText Transfer Protocol (HTTP), session ID...... 3-4

I

IAS - IPSec Access Session................................... 14-134
ICMP... 4-123
  fragments 4-228
  large packets.. 4-229
ICMP floods 4-46
ICMP services.. 2-138
  message codes 2-139
  message types 2-139
IDENT... 4-123
Identity Association Prefix Delegation Identification (IAPD-ID)...14-37, 14-39
Ident-Reset 3-26
idle session timeout 9-16
IDP
  basic configuration... 4-165
  configuring device for standalone IDP 4-219
  configuring inline or inline tap mode 4-178
  enabling in firewall rule................................... 4-177
IDP attack objects.. 4-175
IDP engine, updating.. 4-223
IDP modes 4-178

IDP rulebase
- adding to Security Policy 4-179
- overview 4-178

IDP rulebases
- role-based administration 4-175
- types 4-174

IDP rules 4-178 to ??
- configuring 4-180
- configuring actions 4-187
- configuring address objects 4-175
- configuring attack severity 4-191
- configuring attacks 4-187
- configuring IDP attack objects 4-175
- configuring IP actions 4-189
- configuring Match columns 4-181
- configuring notification 4-191
- configuring service objects 4-175
- configuring services 4-182
- configuring source and destination 4-181
- configuring targets 4-191
- configuring terminal rules 4-185
- entering comments 4-192, 4-196, 4-201

IDP-capable system 4-164

IEEE 802.1Q VLAN standard 10-41

IGMP
- access lists, using 7-158
- configuration, basic 7-159
- configuration, verifying 7-161
- host messages 7-156
- interfaces, enabling on 7-157
- parameters 7-161, 7-162
- policies, multicast 7-168
- querier 7-157

IGMP proxies 7-163
- on interfaces 7-166
- sender 7-175

IKE 5-7, 5-86, 5-95, 5-158
- group IKE ID user 5-181 to 5-196
- group IKE ID, container 5-184
- group IKE ID, wildcards 5-184
- heartbeats 5-290
- hello messages 5-290
- IKE ID 5-51 to 5-52, 5-57 to 5-58
- IKE ID recommendations 5-71
- IKE ID, Windows 200 5-217, 5-225
- local ID, ASN1-DN 5-183
- Phase 1 proposals, predefined 5-9
- Phase 2 proposals, predefined 5-11
- proxy IDs 5-11
- redundant gateways 5-287 to 5-300
- remote ID, ASN1-DN 5-183
- shared IKE ID user 5-196 to 5-201

IKE users 9-12, 9-57 to 9-60
- defining 9-58
- groups 9-58
- groups, and 9-57
- groups, defining 9-59
- IKE ID 9-57, 9-71
- server support 9-12
- with other user types 9-4

IMSI prefix filtering 13-16

inactive SA 3-93

Infranet Controller
- overview 9-34

Infranet Enforcer
- connection policy, configuring 9-34
- overview 9-34

inline mode 4-178

inline tap mode 4-178

in-short error 3-91

inspections 4-3

Instant Messaging 4-124
- AIM 4-124
- IRC 4-124
- MSN Messenger 4-124
- Yahoo! Messenger 4-124

interfaces
- addressing 2-55
- aggregate 2-46, 11-47
- binding to zone 2-53
- connections, monitoring 2-71
- dedicated 10-37, 10-69
- default 2-57
- DHCPv6 14-35
- DIP 2-152
- down, logically 2-69
- down, physically 2-69
- dual routing tables 14-50
- dual Untrust 11-48
- extended 5-139
- function zone 2-47
- Gi 13-2
- Gn 13-2
- Gp 13-2
- HA 2-48
- HA function zone 2-48
- HA, dual 11-26 to 11-29
- interface tables, viewing 2-52
- IP tracking (*See* IP tracking)
- L3 security zones 2-55
- loopback 2-66
- manageable 3-29
- management options 3-26
- MGT 2-47
- MIP 8-64
- modifying 2-57

monitoring 11-9
Neighbor Discovery (ND) 14-29
Neighbor Discovery Parameter (NDP)........... 14-30
Neighbor Unreachability Detection (NUD)..... 14-29
null 5-85
physical 2-3
physical in security zones 2-46
physical, exporting from vsys 10-40
physical, importing to vsys.............................. 10-39
policy-based NAT tunnel 2-48
PPPoE 14-46
redundant 2-47, 11-42
secondary IP addresses..................................... 2-59
serial 11-71
shared..10-37, 10-69
state changes 2-69
tunnel ....2-48, 2-48 to 2-51
up, logically.. 2-69
up, physically... 2-69
viewing interface table 2-52
VIP 8-80
virtual HA 2-48, 11-34
VLAN1 2-91
VSI.. 2-47
VSIs 11-20
zones, unbinding from 2-54
interfaces, enabling IGMP on 7-157
interfaces, monitoring..................................2-77 to 2-82
loops 2-77
security zones... 2-82
Interior Gateway Protocol (IGP) 14-51
internal flash storage.. 3-54
Internet Group Management Protocol
See IGMP
Internet Key Exchange
See IKE
Internet Protocol (IP) addresses
See IP addresses
Internet Service Provider (ISP)....... 2-235, 14-36, 14-37, 14-44, 14-98
intrusion detection and prevention, defined........ 4-163
IP
packet fragments 4-232

IP addresses
extended 5-139
host IDs 2-56
interfaces, tracking on 2-72
L3 security zones ....2-55 to 2-56
Manage 2-105
manage IP 3-29
NetScreen-Security Manager servers 3-23
network IDs 2-56
ports, defining for each 2-114
private 2-55
private address ranges 2-56
public 2-55
secondary... 2-59
secondary, routing between 2-60
IP addresses, virtual 8-80
IP options ....4-10 to 4-11
attributes ....4-10 to 4-11
incorrectly formatted....................................... 4-230
loose source route ....4-10, 4-23 to 4-25
record route 4-11
security 4-10, 4-11
source route 4-23
stream ID 4-11
strict source route ....4-11, 4-23 to 4-25
timestamp 4-11
IP pools
See DIP pools
IP Security
See IPSec
IP spoofing ....4-18 to 4-23
drop-no-rpf-route... 4-19
Layer 2 ....4-19, 4-22
Layer 3 ....4-18, 4-20
IP tracking 11-83, 11-112, 12-109
device failover threshold 11-113
dynamic option 2-73
interfaces, shared 2-72
interfaces, supported 2-72
object failure threshold...................................... 2-73
ping and ARP 11-83, 11-112
rerouting traffic ....2-72 to 2-87
tracked IP failure threshold 11-113
tunnel failover... 11-113
vsys 2-72
weight 2-73
weights 11-113
IP tracking, failure
egress interface, on................................2-83 to 2-84
ingress interface, on ....2-85 to 2-87
tracked IP threshold 2-73
IP-based traffic classification................................. 10-69

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

IPSec
- AH 5-2, 5-53, 5-60
- digital signature 5-20
- ESP 5-2, 5-53, 5-60
- L2TP-over-IPSec 5-4
- SAs 5-2, 5-8, 5-11
- SPI 5-2
- Transport mode 5-4, 5-206, 5-211, 5-216
- tunnel 5-2
- Tunnel mode 5-4
- tunnel negotiation 5-8

IPv4 WAN 14-112
IPv4/IPv6 boundaries .... 14-81 to 14-86
IPv4/IPv6 boundary 14-90
IPv4-mapped addresses 14-82, 14-87
IPv4-to-IPv6 host mapping 14-91
IPv4-to-IPv6 network mapping 14-90
IPv6 addresses
- SLA - Site-Local Aggregator 14-37
- TLA - Top-Level Aggregator 14-37

IPv6 backbone 14-85, 14-115
IPv6/IPv4 boundary 14-82, 14-83, 14-86, 14-88
IPv6-to-IPv4 host mapping 14-88
IRC 4-124
island IPv6 networks 14-112
ISP 2-235, 14-46
- failover holddown timer 12-108
- priority 12-107

ISP configuration for serial interfaces 11-74

J

Java applets, blocking 4-161

K

keepalive
- frequency, NAT-T 5-235
- L2TP 5-214

keys
- manual 5-117, 5-124
- preshared 5-158

keys, license 2-263
keys, vsys 10-37

L

L2TP .... 5-203 to 5-228, 13-3
- access concentrator: *See* LAC
- address assignments 9-76
- bidirectional 5-206
- compulsory configuration 5-203
- decapsulation 5-207
- default parameters 5-209
- encapsulation 5-206
- external auth server 9-76
- hello signal 5-214, 5-219
- Keep Alive 5-214, 5-219
- L2TP-only on Windows 2000 5-205
- local database 9-76
- network server: *See* LNS
- operational mode 5-206
- RADIUS server 5-209
- ScreenOS support 5-205
- SecurID server 5-209
- tunnel 5-211
- user authentication 9-76
- voluntary configuration 5-204
- Windows 2000 tunnel authentication 5-214, 5-219

L2TP policies 2-181
L2TP users 9-76
- server support 9-12
- with XAuth 9-4

L2TP-over-IPSec 5-4, 5-211, 5-216
- bidirectional 5-206
- tunnel 5-211

LAC 5-203
- NetScreen-Remote 5.0 5-204
- Windows 2000 5-204

Land attacks 4-48
lawful interception 13-34
Layer 2 Tunneling Protocol
- *See* L2TP

LDAP .... 4-123, 9-24 to 9-26
- common name identifiers 9-25
- distinguished names 9-25
- server ports 9-25
- structure 9-24
- user types supported 9-25

LED indicators, HA 11-18
license keys 2-263
- advanced mode 4-112
- attack pattern update 4-112

Lightweight Directory Access Protocol
- *See* LDAP

link-local addresses 14-12, 14-14
Link-State Advertisement (LSA) suppression 7-67
LNS 5-203
load sharing 11-89
load-balancing by path cost 7-36, 7-59

local certificate 5-25
local database
  IKE users 9-58
  timeout 9-14
  user types supported 9-14
log entries
  enabling in IDP rules 4-225
Log Viewer
  creating an exempt rule 4-196
logging 2-184, 3-53 to 3-65
  asset recovery log 3-65
  attack object groups 4-143
  CompactFlash (PCMCIA) 3-54
  console 3-54
  email 3-54
  event log 3-54
  internal 3-54
  NetScreen-Security Manager 3-23
  self log 3-63
  SNMP 3-54, 3-70
  syslog 3-54, 3-69
  WebTrends 3-54, 3-69
logging, traffic 13-5
loopback interfaces 2-66
loose source route IP option 4-10, 4-23 to 4-25
low-watermark threshold 4-31
LPR spooler 4-123

M

MAC address 14-13
MAC addresses 14-21, 14-29
Main mode 5-9
malicious URL protection 4-54 to 4-57
Manage IP 2-105
manage IP 3-29
manage IP, VSD group 0 11-5
management client IP addresses 3-40
Management information base II
  See MIB II
management methods
  Command Line Interface 3-9
  console 3-19
  SSL 3-5
  Telnet 3-10
  WebUI 3-2
management options
  interfaces 3-26
  manageable 3-29
  MGT interface 3-27
  NetScreen-Security Manager 3-26
  ping 3-26
  SNMP 3-26
  SSH 3-26
  SSL 3-26
  Telnet 3-26
  Transparent mode 3-27
  VLAN1 3-27
  WebUI 3-26
manual 6over4 tunneling 14-98
Manual Key
  management 5-7
manual keys 5-117, 5-124, 9-12
manual keys, VPNs 3-41, 3-76
manual tunneling 14-99
mapped IP
  See MIP
Mapped IP - MIP 14-84
Mapped IP (MIP) 14-82
Maximum Transmission Unit (MTU) 14-12
MD5 5-6
Message Digest version 5 (MD5) 5-6
messages
  alert 3-54
  control 11-26
  critical 3-54
  data 11-29
  debug 3-55
  emergency 3-54
  error 3-54
  HA 11-28
  info 3-55
  notification 3-55
  warning 3-54
  WebTrends 3-70
MGT interface 2-47
MGT interface, management options 3-27
MIB files, importing 5-249
MIB II 3-26, 3-71
Microsoft Network Instant Messenger
  See MSN Instant Messenger
Microsoft-Remote Procedure Call
  See MS-RPC
MIME, AV scanning 4-67
MIP 2-12, 8-63
  address ranges 8-66
  bidirectional translation 8-6
  definition 8-6
  global zone 8-64
  grouping, multi-cell policies 8-79
  reachable from other zones 8-67
  same-as-untrust interface 8-70 to 8-73
MIP - Mapped IP 14-82
  IPv4 hosts to a single IPv6 host 14-91
  IPv4 hosts to multiple IPv6 hosts 14-90
  IPv6 hosts to a single IPv4 host 14-88
  IPv6 Hosts to Multiple IPv4 Hosts 14-86
  IPv6-to-IPv4 network mapping 14-86
  MIP from IPv6 to IPv4 14-84

MIP, creating
  addresses 8-65
  on tunnel interface 8-70
  on zone interface 8-65
MIP, default
  netmasks 8-66
  virtual routers 8-66
MIP, to zone with interface-based NAT 2-104
MIP, virtual systems 10-31
MIP, VPNs 5-139
Mobile Station (MS) mode 13-15
mode config 9-61
mode, Transparent 10-42
modem configuration for serial interfaces 11-72
modem port 12-107
modem ports 3-19
modes
  Aggressive 5-10
  Combined 2-37
  Dual DMZ 2-39
  Dual Untrust 2-36
  Home-Work 2-35
  L2TP operational 5-206
  Main 5-9
  NAT and Route 11-5
  NAT, traffic to Untrust zone 2-89
  Phase 1 cryptographic 5-49, 5-56
  port 2-33
  port-mode availability 2-34
  preempt 11-16
  Transparent 2-90
  Transport 5-4, 5-60, 5-206, 5-211, 5-216
  Trust-Untrust 2-34
  Tunnel 5-4, 5-60
modes, operational
  NAT 13-4
  Route 13-4
  Transparent 13-4
modes, selection
  APN 13-15
  Mobile Station (MS) 13-15
  Network 13-15
  Verified 13-15
modulus 5-10
MS RPC ALG, defined 2-141
MSN Messenger 4-124
MS-RPC 4-125
multicast
  addresses 7-148
  distribution trees 7-183
  policies 7-153
  policies for IGMP 7-168
  reverse path forwarding 7-148
  routing tables 7-149
  static routes 7-150
multicast routing
  IGMP 7-155
  PIM 7-181
multimedia sessions, SIP 6-13

N

NA - Neighbor Advertisement 14-30
NAT
  definition 8-1
  IPSec and NAT 5-230
  NAT servers 5-230
  NAT-src with NAT-dst .... 8-50 to 8-61
NAT mode .... 2-102 to 2-108, 11-5, 13-4
  interface settings 2-105
  traffic to Untrust zone 2-89, 2-104
NAT vector error 3-93
NAT-dst .... 8-28 to 8-61
  address shifting 8-5
  packet flow .... 8-29 to 8-31
  port mapping 8-4, 8-28, 8-47
  route considerations .... 8-29, 8-32 to 8-34
  unidirectional translation 8-6, 8-10
  VPNs 5-139
  with MIPs or VIPs 8-3
NAT-dst, addresses
  range to range 8-10, 8-44
  range to single IP 8-9, 8-41
  ranges 8-4
  shifting 8-28, 8-44
NAT-dst, single IP
  with port mapping 8-8
  without port mapping 8-9
NAT-dst, translation
  one-to-many 8-38
  one-to-one 8-35
native hosts 14-102, 14-104
NAT-PT
  See Network Address Translation-Port Translation
NAT-PT - Network Address Translation-Port Translation
  IPSec, when to use 14-112
NAT-src .... 8-1, 8-13 to 8-25
  egress interface .... 8-8, 8-24 to 8-25
  fixed port .... 8-14, 8-18 to 8-19
  interface-based 8-2
  VPNs 5-141
NAT-src, addresses
  shifting .... 8-20 to 8-24
  shifting, range considerations 8-20

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

NAT-src, DIP pools 8-1
  fixed port 8-7
  with address shifting 8-8
  with PAT........ 8-7, 8-15 to 8-17
NAT-src, Route mode 2-108
NAT-src, translation
  port addresses 8-2
  unidirectional........ 8-6, 8-10
NAT-T........ 5-230 to 5-237
  enabling........ 5-237
  IKE packet........ 5-233
  initiator and responder 5-235
  IPSec packet 5-234
  keepalive frequency........ 5-235
  obstacles for VPNs 5-233
  probing for NAT .... 5-231 to 5-232
NAT-Traversal
  See NAT-T
ND - Neighbor Discovery........ 14-29
  Accept Incoming RAs 14-21
  age of the neighbor entry 14-13
  bypassing MAC session-caching........ 14-29
  definition........ 14-13
  enabling........ 14-29
  Neighbor Cache table 14-13, 14-29
  neighbor reachability state 14-13
  neighbor reachability status 14-30
  packets currently queued for transmission ... 14-13
  reachability status 14-29
NDP - Neighbor Discovery Parameter........ 14-21, 14-30
negation, address 2-198
negation, Deep Inspection (DI)........ 4-156
Neighbor Cache table........ 14-13, 14-15, 14-30
  neighbor entry categories 14-14
neighbor cache table........ 14-13, 14-25
Neighbor Discovery (ND)
  displaying........ 14-32
Neighbor Discovery Parameter (NDP)........ 14-30
NetBIOS 4-125
NetInfo........ 2-238
netmasks 2-56, 2-178
netmasks, MIP default 8-66
NetScreen Redundancy Protocol
  See NSRP
NetScreen Reliable Transport Protocol
  See NRTP
NetScreen-Remote
  AutoKey IKE VPN........ 5-158
  dynamic peer 5-164, 5-171
  NAT-T option 5-230
NetScreen-Security Manager
  definition........ 3-20
  enabling NSM Agent 3-22
  initial connectivity setup 3-21
  logging........ 3-23
  management options........ 3-26
  management system 3-20, 3-21, 3-23
  NSM Agent 3-20, 3-23
  reporting events 3-23, 3-24
  UI........ 3-20
Network Address Translation (NAT)........ 3-92
Network Address Translation-Port Translation
  DIP addresses, translating........ 14-84
  DIP from IPv6 to IPv4 14-83
  Dynamic IP (DIP) 14-82
  IPv4 hosts to a single IPv6 host........ 14-91
  IPv4 hosts to multiple IPv6 hosts........ 14-90
  IPv6 hosts to a single IPv4 host........ 14-88
  IPv6 hosts to multiple IPv4 hosts........ 14-86
  MIP........ 14-82
  MIP from IPv4 to IPv6 14-85
  outgoing service requests........ 14-82, 14-86
  source address translation 14-83
  when to use 14-82
Network mode 13-15
network, bandwidth........ 2-205
next-hop gateway 14-31
NFS........ 4-123
NHTB table .... 5-251 to 5-255
  addressing scheme 5-253
  automatic entries 5-254
  manual entries........ 5-254
  mapping routes to tunnels 5-252
NNTP........ 4-123
NRTP 11-23, 11-110
NS - Neighbor Solicitation........ 14-14, 14-31
  setting........ 14-30
NSM Agent........ 3-20, 3-21
  enabling........ 3-22
  reporting events 3-23

NSRP 11-3
ARP broadcasts 11-9
ARP lookup 11-39
backup 11-3
cabling .... 11-32 to 11-34
clear cluster command 11-100
config sync 11-23
control messages 11-26, 11-28
debug cluster command 11-100
default settings 11-99
DHCP 2-243
DIP groups .... 2-165 to 2-167
files, sync 11-24
full-mesh configuration 11-32, 11-89
HA session backup 2-184
hold-down time 11-36, 11-38
interface monitoring 11-9
load sharing 11-89
manage IP 11-83, 11-112
master 11-3
NAT and Route modes 11-5
NTP synchronization 2-269, 11-26
packet forwarding and dynamic routing 11-29
preempt mode 11-16
priority numbers 11-16
redundant interfaces 2-47
redundant ports 11-26
RTOs 11-35
secondary path 11-9
secure communications 11-9
virtual systems .... 11-88 to 11-94
VSD groups ..... 4-172, 11-16 to 11-20, 11-35, 11-112
VSIs 2-47, 11-4
VSIs, static routes 11-20, 11-46
NSRP clusters .... 11-8 to 11-10, 11-35
clear cluster command 11-7
debug cluster command 11-7
names 11-8, 11-101
NSRP data
link 11-29
messages 11-29
NSRP HA
cabling, network interfaces 11-33
interfaces 11-27
LED 11-18
ports, redundant interfaces 11-42
session backup 11-10
NSRP ports
failover 11-42
monitoring 11-82
NSRP RTOs .... 11-10 to 11-15
states 11-15
sync 11-24
NSRP synchronization
NTP, NSRP 11-26
PKI 11-24
RTOs 11-24
NSRP-Lite .... 11-95 to 11-111
cabling 11-104
clusters .... 11-98 to 11-101
preempt mode 11-103
secure communications 11-101
VSD groups .... 11-102 to 11-104
NSRP-Lite synchronization
config 11-109
disabling 11-111
file 11-110
NTP .... 2-267 to 2-270, 4-124
authentication types 2-270
maximum time adjustment 2-268
multiple servers 2-267
NSRP synchronization 2-269
secure servers 2-269
servers 2-267
NTP, NSRP synchronization 11-26
NUD - Neighbor Unreachability Detection 14-13
Neighbor Cache Table 14-13, 14-25
Null interface, defining routes with 7-11
null route 5-85

O

objects
attack objects 4-201
attack objects, creating custom 4-204
attack objects, protocol anomaly 4-202
attack objects, signature 4-202
objects, monitoring 11-81
OCSP (Online Certificate Status Protocol) 5-34
client 5-34
responder 5-34
Open Shortest Path First
See OSPF
operating systems, probing hosts for .... 4-12 to 4-14
operational modes
NAT 13-4
Route 13-4
Transparent 13-4

OSPF
- broadcast networks 7-48
- configuration steps 7-49
- ECMP support 7-59
- flooding, protecting against 7-66
- flooding, reduced LSA 7-67
- global parameters 7-58
- hello protocol 7-47
- interface parameters 7-62
- interfaces, assigning to areas 7-53
- interfaces, tunnel 7-68
- link-state advertisements 7-46
- link-type, setting 7-68
- load-balancing 7-36
- LSA suppression 7-67
- neighbors, authenticating 7-64
- neighbors, filtering 7-65
- not so stubby area 7-47
- point-to-multipoint 7-68
- point-to-point network 7-48
- security configuration 7-64
- stub area 7-47
- virtual links 7-59

OSPF areas 7-46
- defining 7-51
- interfaces, assigning to 7-53

OSPF routers
- adjacency 7-47
- backup designated 7-47
- creating OSPF instance in VR 7-50
- designated 7-47
- types 7-47

OSPF routes
- default, rejecting 7-66
- redistributed, summarizing 7-57
- redistributing 7-56
- route-deny restriction, disabling 7-69

outgoing request packets
- from IPv6 to IPv4 14-84

outgoing service requests 14-86, 14-88

Overbilling attacks
- description 13-26
- prevention .... 13-26 to 13-31
- prevention, configuring 13-29
- solutions 13-28

P

P2P 4-125
- BitTorrent 4-125
- DC 4-125
- eDonkey 4-125
- FastTrack 4-125
- Gnutella 4-125
- KaZaa 4-125
- MLdonkey 4-125
- Skype 4-125
- SMB 4-125
- WinMX 4-125

packet flow .... 2-11 to 2-13
- inbound VPN .... 5-66 to 5-68
- outbound VPN 5-66
- policy-based VPN .... 5-68 to 5-69
- route-based VPN .... 5-63 to 5-68

packet flow, NAT-dst .... 8-29 to 8-31

packets 3-93
- address spoofing attack 3-92
- collision 3-91
- denied 3-93
- dropped 3-92, 3-93
- fragmented 3-93
- incoming 3-91
- Internet Control Message Protocol (ICMP) 3-90, 3-92
- IPSec 3-92
- land attack 3-92
- Network Address Translation (NAT) 3-92
- Point to Point Tunneling Protocol (PPTP) 3-92
- received 3-91, 3-92, 3-93
- transmitted underrun 3-91
- unreceivable 3-91
- unroutable 3-93

PAP 5-206, 5-209

parent connection 3-92

Password Authentication Protocol
- *See* PAP

passwords
- forgetting 3-37
- root admin 3-39

passwords, changing admin’s 10-4, 10-7

PAT 2-153, 8-14

paths
- monitoring 11-111
- tunnel failover 11-113

PCMCIA 3-54

Peer-to-Peer
- *See* P2P

Perfect Forward Secrecy
- *See* PFS

PFS 5-11, 5-53, 5-59

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

Phase 1 5-9
proposals 5-9
proposals, predefined 5-9
Phase 2 5-11
proposals 5-11
proposals, predefined 5-11
physical interface
logical interface 2-46
physical interfaces
C-bit parity mode 12-13
CSU compatibility 12-20
exporting from vsys 10-40
importing to vsys 10-39
PIM-SM 7-183
configuration steps 7-187
configuring rendezvous points 7-197
designated router 7-184
IGMPv3 7-213
instances, creating 7-188
interface parameters 7-202
proxy RP 7-204
rendezvous points 7-184
security configurations 7-199
traffic, forwarding 7-185
PIM-SSM 7-187
ping management options 3-26
Ping of Death 4-49
pinholes 6-19
PKI 5-22
PKI keys 3-6
point-to-multipoint configuration
OSPF 7-68
Point-to-Point Protocol
See PPP
Point-to-Point Tunneling Protocol (PPTP) 3-92
policies 2-3, 13-5
actions 2-179
address groups 2-178
address negation 2-198
addresses 2-178
addresses in 2-178
alarms 2-184
application, linking service to explicitly 2-180
authentication 2-182
bidirectional VPNs 2-180, 5-125
changing 2-201
context 4-114
core section 4-17, 4-112
counting 2-184
Deep Inspection (DI) 2-181
deny 2-179
DIP groups 2-165
disabling 2-201
editing 2-201
enabling 2-201
functions of 2-171
global 2-174, 2-186, 2-196
HA session backup 2-184
ID 2-178
internal rules 2-176
interzone 2-173, 2-186, 2-187, 2-190
intrazone 2-173, 2-186, 2-194
L2TP 2-181
L2TP tunnels 2-181
lookup sequence 2-175
management 2-186
managing bandwidth 2-205
maximum limit 2-117
multicast 7-153
multiple items per component 2-197
name 2-180
NAT-dst 2-182
NAT-src 2-181
order 2-202
permit 2-179
policy context 2-197
policy set lists 2-175
position at top 2-181, 2-202
reject 2-179
removing 2-203
reordering 2-202
required elements 2-172
root system 2-176
schedules 2-185
security zones 2-178
service book 2-119
service groups 2-150
services 2-178
services in 2-119, 2-178
shadowing 2-201, 2-202
traffic logging 2-184
traffic shaping 2-185
tunnel 2-179
types .... 2-173 to 2-174
verifying 2-201
virtual systems 2-176
VPN dialup user groups 2-178
VPNs 2-180
policies, configuring 13-6
policy-based NAT
See NAT-dst *and* NAT-src
policy-based NAT, tunnel interfaces 2-48
policy-based VPNs 5-62

Port Address Translation
See PAT
port modes 2-33
availability 2-34
Combined 2-37
default 2-34
DMZ/Dual Untrust 2-38
Dual DMZ 2-39
Dual Untrust 2-36
Home-Work 2-35
setting 2-40
Trust/Untrust/DMZ (Extended) 2-38
Trust-Untrust 2-34
port scan 4-9
Portmapper 4-124
ports
failover 11-42
mapping 8-4, 8-28
monitoring 11-82
numbers 8-87
primary trusted and untrusted 11-42
redundant 11-26
secondary trusted and untrusted 11-42
ports, modem 3-19
ports, trunk 10-42
PPP 5-204, 12-71
PPP - Point-to-Point Protocol 14-46
PPPoA 12-71, 12-72
PPPoE 12-71
PPPoE - Point-to-Point Protocol over Ethernet 14-46
preempt mode 11-16, 11-103
prefix list 14-12
prefixes
prefix list 14-12
preshared key 5-7
preshared keys 5-158
priority queuing 2-210
private addresses 2-56
probe 14-31
Probe Time 14-31
probes
network 4-8
open ports 4-9
operating systems 4-12, 4-14
proposals
Phase 1 .... 5-9, 5-69
Phase 2 .... 5-11, 5-69
protocol anomalies 4-128
ALGs 4-125
basic network protocols 4-123
configuring parameters 4-155
Instant Messaging applications 4-124
P2P applications 4-125
supported protocols .... 4-123 to 4-126
protocol distribution, reporting to NetScreen-Security Manager 3-23
Protocol Independent Multicast
See PIM
protocols
CHAP 5-206
Interior Gateway Protocol (IGP) 14-51
NRTP 11-23, 11-110
NSRP 11-1
PAP 5-206
PPP 5-204
VRRP 11-83, 11-112
protocols, CHAP 9-71
proxy IDs 5-11
matching 5-63, 5-70
VPNs and NAT .... 5-139 to 5-140
public addresses 2-56
Public key infrastructure
See PKI
Public/private key pair 5-23
PXE 2-249
PXE server 2-249

Q

QoS 2-205

R

RA - Router Advertisement 14-12
RADIUS .... 3-37, 4-124, 9-17 to 9-19
auth server objects 9-26
dictionary file 9-2
dictionary files 9-18
L2TP 5-209
object properties 9-18
ports 9-18
retry timeout 9-18
shared secret 9-18
rate limiting, GTP-C messages 13-12
reachability states 14-14
transitions 14-15
reconnaissance .... 4-7 to 4-25
address sweep 4-8
FIN scans 4-15
IP options 4-10
port scan 4-9
SYN and FIN flags set 4-12
TCP packet without flags 4-14
record route IP option 4-11
redundant gateways .... 5-287 to 5-300
recovery procedure 5-292
TCP SYN flag checking 5-293
regular expressions .... 4-150 to 4-151
rekey option, VPN monitoring 5-239

Remote Authentication Dial-in User Service
  See RADIUS
remote termination point....................14-104, 14-107
replay protection...5-12
requirements, basic functional.............................10-4
Retransmission Time 14-31
rexec..4-124
RFC 1777, *Lightweight Directory Access Protoco*... 9-25
RFCs
  0792, *Internet Control Message Protocol* 2-138
  1038, *Revised IP Security Option* 4-10
  1349, *Type of Service in the Internet Protocol Suite* 2-186
  1918, *Address Allocation for Private Internets* 2-56
  2132, *DHCP Options and BOOTP Vendor Extensions* 2-242
  2326, *Real Time Streaming Protocol (RTSP)*..2-142, 2-146
  2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* 2-186
  791, *Internet Protocol*.................................... 4-10
  793, *Transmission Control Protocol* 4-13
RIP
  authenticating neighbors.................................. 7-86
  database 7-93
  demand circuit configuration 7-94
  filtering neighbors 7-87, 14-57
  flooding, protecting against 7-88, 14-59
  global parameters 7-83, 14-56
  instances, creating in VR........................7-76, 14-54
  interface parameters...............................7-85, 14-60
  interfaces, enabling on 7-77, 14-55
  load-balancing 7-36
  point-to-multipoint 7-97
  prefix summary.. 7-92
  versions 7-90
  versions, protocol... 7-90
RIP routes
  alternate 7-93
  redistributing 7-77, 14-58
  rejecting default.......................................7-88, 14-57
  summary, configuring 7-92
RIP, configuring
  demand circuits.. 7-95
  security 7-86
  steps...7-75, 14-53
RIP, viewing
  database 7-80, 14-66
  interface details 7-82
  neighbor information 7-81, 14-68
  protocol details 7-80, 14-66
RIPng - Routing Information Protocol
 next-generation 14-49, 14-51
  interface cost 14-60
  interface cost metric 14-62
  metric calculation 14-62
  offset metric... 14-60, 14-62
  route metric 14-60, 14-62
  route redistribution 14-51
rlogin 4-124
role-based administration
  configuring IDP-only administrator................4-220
  IDP rulebases 4-175
root admin, logging in...3-40
route lookup
  multiple VRs..7-34
  sequence 7-32
Route mode .... 2-108 to 2-111, 11-5, 13-4
  interface settings 2-109
  NAT-src 2-108
route tracking 12-109
route-based VPNs... 5-62 to 5-63
routes
  exporting 7-42
  filtering 7-39
  importing...7-42
  maps 7-38
  metrics...7-31
  null 5-85
  preference 7-30
  redistributing...7-37
  selection 7-30
Routing Information Protocol
  See RIP
routing tables...7-15
  lookup 7-32
  lookup in multiple VRs 7-34
  multicast 7-149
  route selection 7-30
  types 7-15
routing, multicast..7-147
RS - Router Solicitation 14-12
RSA authentication 14-121
rsh..4-124
RSH ALG..2-139
RTOs .... 11-10 to 11-15
  operational states 11-15
  peers 11-17
  synchronization 11-24
RTSP 4-124

RTSP ALG
- defined 2-142
- request methods 2-143
- server in private domain 2-147
- server in public domain 2-148
- status codes 2-145

rules, derived from policies 2-176
run-time authentication 2-182, 9-38
Run-Time Objects
- *See* RTOs

S

SA policy 3-93
SAs 5-8, 5-11
- check in packet flow 5-65

SCEP (Simple Certificate Enrollment Protocol) 5-30
schedules 2-168, 2-185
SCP
- enabling 3-18
- example client command 3-18

SCREEN
- address sweep 4-8
- bad IP options, drop 4-230
- drop unknown MAC addresses 4-39
- FIN with no ACK 4-15
- FIN without ACK flag, drop 4-13
- ICMP
  - fragments, block 4-228
- ICMP floods 4-46
- IP options 4-10
- IP packet fragments, block 4-232
- IP spoofing .... 4-18 to 4-23
- Land attacks 4-48
- large ICMP packets, block 4-229
- loose source route IP option, detect 4-25
- Ping of Death 4-49
- port scan 4-9
- source route IP option, deny 4-25
- strict source route IP option, detect 4-25
- SYN and FIN flags set 4-12
- SYN floods .... 4-34 to 4-39
- SYN fragments, detect 4-233
- SYN-ACK-ACK proxy floods 4-32
- TCP packet without flags, detect 4-14
- Teardrop 4-50
- UDP floods 4-47
- unknown protocols, drop 4-231
- VLAN and MGT zones 4-2
- WinNuke attacks 4-51

SCREEN, MGT zone 2-28
ScreenOS
- function zones 2-32
- global zone 2-28
- overview 2-1
- packet flow .... 2-11 to 2-13
- policies 2-3
- RADIUS vendor IDs 9-19
- security zones 2-2, 2-28
- security zones, global 2-2
- security zones, predefined 2-2
- tunnel zones 2-28
- virtual systems 2-10
- VRs 10-6
- zones .... 2-25 to 2-33, 10-6

ScreenOS interfaces
- physical 2-3
- security zones 2-3
- subinterfaces 2-3

SDP .... 6-17 to 6-18
secondary IP addresses 2-59
secondary path 11-9
Secure Copy
- *See* SCP

Secure Hash Algorithm-1
- *See* SHA-1

Secure Shell
- *See* SSH

Secure Sockets Layer
- *See* SSL

SecurID 9-23
- ACE servers 9-23
- auth server object 9-28
- authentication port 9-23
- authenticator 9-23
- encryption types 9-23
- L2TP 5-209
- token codes 9-23
- Use Duress option 9-24
- user type support 9-24

SecurID clients
- retries 9-23
- timeout 9-23

security associations
- *See* SAs

Security Associations (SA) 3-93
security IP option 4-10, 4-11

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

security policies 4-173
- rulebase execution 4-177
- rulebases 4-173
- rules 4-173
- templates 4-177

security zones 2-2
- determination, destination zone 2-12
- determination, source zone 2-11
- global 2-2
- predefined 2-2
- *See* zones

security zones, interfaces 2-3
- physical 2-46

selection modes
- APN 13-15
- Mobile Station (MS) 13-15
- Network 13-15
- Verified 13-15

self log 3-63
sequence-number validation 13-13
serial cables 3-19
serial interfaces 11-71
- failover 11-75
- ISP configuration 11-74
- modem configuration 11-72

Server Message Block
- *See* SMB

servers, auth
- *See* auth servers

servers, SecurID ACE 9-23
service book
- entries, modifying (CLI) 2-135
- entries, removing (CLI) 2-135

service book, service groups (WebUI) 6-63
service book, services
- adding 2-134
- custom 2-119
- custom (CLI) 2-134
- preconfigured 2-119

service groups .... 2-150 to 2-152
- creating 2-151
- deleting 2-152
- modifying 2-151

service groups (WebUI) 2-150
service provider, information from 12-70
services 2-119
- custom 4-145
- defined 2-178
- drop-down list 2-119
- ICMP 2-138
- in policies 2-178
- timeout threshold 2-136

services, custom 2-134
- ALGs 2-180
- in vsys 2-134

session ID 3-4
session idle timeout 9-16
session limits .... 4-28 to 4-30
- destination-based 4-29, 4-30
- source-based 4-28, 4-29

session table floods 4-17, 4-28
session timeout
- HTTP 4-31

session timeouts
- TCP 4-31
- UDP 4-31

SHA-1 5-6
shared VRs 10-37
shared zones 10-37
signature packs, DI 4-114
signatures
- stateful 4-126

SIP
- ALG 6-17, 6-20
- connection information 6-18
- defined 6-13
- media announcements 6-18
- messages 6-14
- multimedia sessions 6-13
- pinholes 6-17
- request methods 6-14
- response codes 6-16
- RTCP 6-18
- RTP 6-18
- SDP .... 6-17 to 6-18
- signaling 6-17

SIP NAT
- call setup 6-23, 6-28
- defined 6-23
- DIP pool, using a 6-35
- DIP, using incoming 6-31
- DIP, using interface 6-32
- incoming, with MIP 6-35, 6-37
- proxy in DMZ 6-44
- proxy in private zone 6-39, 6-86
- proxy in public zone 6-41
- trust intrazone 6-51
- untrust intrazone 6-47, 6-93
- VPN, using full-mesh 6-53, 6-99

- SIP timeouts
  - inactivity 6-20
  - media inactivity 6-21, 6-22
  - session inactivity 6-20
  - signaling inactivity 6-21, 6-22
- site survey 12-130
- SLA - Site-Local Aggregator 14-37, 14-39
- SMB
  - NetBIOS 4-125
- SMTP server IP 3-68
- SNMP 3-26, 3-70
  - cold start trap 3-71
  - configuration 3-74
  - encryption 3-73, 3-75
  - management options 3-26
  - MIB files, importing 5-249
  - VPN monitoring 5-249
- SNMP community
  - private 3-74
  - public 3-74
- SNMP traps
  - 100, hardware problems 3-71
  - 200, firewall problems 3-71
  - 300, software problems 3-71
  - 400, traffic problems 3-71
  - 500, VPN problems 3-71
  - allow or deny 3-73
  - system alarm 3-71
  - traffic alarm 3-71
  - types 3-71
- SNMPTRAP 4-124
- software keys 10-37
- source address translation 14-83
- source interface-based routing (SIBR) 7-19
- source route 3-93
- source-based routing (SBR) 7-17
- SSH 3-11 to 3-16, 4-124
  - authentication method priority 3-15
  - automated logins 3-17
  - connection procedure 3-12
  - forcing PKA authentication only 3-15
  - loading public keys, CLI 3-15
  - loading public keys, TFTP 3-15, 3-17
  - loading public keys, WebUI 3-15
  - management options 3-26
  - password authentication 3-14
  - PKA 3-15
  - PKA authentication 3-14
- SSID
  - binding to wireless interface 12-143
- SSL 3-5, 4-124
- SSL Handshake Protocol
  - *See* SSLHP
- SSL management options 3-26
- SSL, with WebAuth 9-54
- SSLHP 3-5
- state transitions
  - endpoint host 14-15
  - next-hop gateway router 14-16
  - static entry 14-18
  - tunnel gateway 14-17
- stateful 4-3
  - inspection 4-3
  - signatures 4-126
- stateless address autoconfiguration 14-11
- static routing 7-2, 7-2 to 7-10
  - configuring 7-5
  - multicast 7-150
  - Null interface, forwarding on 7-11
  - using 7-3
- statistics, reporting to NSM 3-24
- stream ID IP option 4-11
- stream signatures 4-127
- strict source route IP option 4-11, 4-23 to 4-25
- subinterfaces 2-3, 10-61
  - configuring (vsys) 10-61
  - creating (root system) 2-58
  - creating (vsys) 10-61
  - deleting 2-59
  - multiple per vsys 10-61
- subnets, overlapping 10-62
- subrate option 12-20
- subscriptions
  - registration and activation 2-264 to 2-266
  - temporary service 2-264
- Sun RPC ALG
  - call scenarios 2-140
  - defined 2-139
- Super G 12-132
- SurfControl 4-92, 4-101
- SYN and FIN flags set 4-12
- SYN checking 4-15, 4-15 to 4-18
  - asymmetric routing 4-16
  - reconnaissance hole 4-17
  - session interruption 4-17
  - session table floods 4-17
- SYN cookies 4-44
- SYN floods 4-34 to 4-39
  - alarm threshold 4-38
  - attack threshold 4-37
  - attacks 4-34
  - destination threshold 4-38
  - drop unknown MAC addresses 4-39
  - queue size 4-39
  - source threshold 4-38
  - SYN cookies 4-44
  - threshold 4-35
  - timeout 4-39

SYN fragments 4-233
SYN-ACK-ACK proxy floods 4-32
synchronization
  configuration 11-23
  files 11-24
  PKI objects 11-24
  RTOs 11-24
syslog 3-54, 4-124
  encryption 3-75
  facility 3-69, 3-78, 3-85
  host 3-69
  host name 3-69, 3-70, 3-78, 3-85
  messages 3-68
  port 3-69, 3-78, 3-85
  security facility 3-69, 3-78, 3-85
system clock .... 2-266 to 2-270
  date & time 2-266
  sync with client 2-266
  time zone 2-266
system parameters 2-269

T

T3 interfaces
  C-bit parity mode 12-13
  CSU compatibility 12-20
tags, VLANs 2-3
TCP
  packet without flags 4-14
  session timeouts 4-31
  stream signatures 4-153
  SYN flag checking 5-293
TCP proxy 3-93
Teardrop attacks 4-50
Telnet 3-10, 4-124
Telnet management options 3-26
Telnet, logging in via 3-10
templates
  security policy 4-177
TFTP 4-124
three-way handshakes 4-34
threshold
  low-watermark 4-31
thresholds
  high-watermark 4-30
time zone 2-266
timeout 13-25
  admin users 9-16
  auth users 9-16
timestamp IP option 4-11
TLA - Top-Level Aggregator 14-37
token codes 9-23
trace-route 2-95
traffic
  counting 2-184, 13-5
  IP-based 10-69
  logging 2-184, 13-5
  priority 2-185
  shaping 2-205
  sorting .... 10-31 to 10-39
  through traffic, vsys sorting .... 10-32 to 10-35
  VLAN-based .... 10-40, 10-41 to 10-67
traffic alarms .... 3-65 to 3-68
traffic shaping 2-205
  automatic 2-206
  service priorities 2-210
Transparent mode ......2-90 to 2-102, 10-42, 10-43, 13-4
  ARP/trace-route 2-93
  blocking non-ARP traffic 2-91
  blocking non-IP traffic 2-91
  broadcast traffic 2-91
  drop unknown MAC addresses 4-39
  flood 2-93
  routes 2-92
  unicast options 2-93
Transparent mode, management options 3-27
Transport mode 5-4, 5-206, 5-211, 5-216
Triple DES
  See 3DES
trunk ports 10-42
trunk ports, Transparent mode 10-42
trustee administrator 12-107
tunnel interfaces 2-48
  definition 2-48
  policy-based NAT 2-48
Tunnel mode 5-4
tunnel termination points 14-102
tunnel tracking 12-109

U

UDP
  checksum 5-235
  NAT-T encapsulation 5-230
  session timeouts 4-31
unified access control solution
  overview of 1-xlix, 9-vii, 9-33
unknown protocols 4-231
unknown unicast options .... 2-92 to 2-97
  ARP .... 2-94 to 2-97
  flood .... 2-93 to 2-94
  trace-route 2-95
updating IDP engine 4-223
upstream router 14-38
URL filtering
  See web filtering

Note: The entries in this index use the numbering format volume-page. For example, 5-6 refers to volume 5, page 6.

users
- admin 9-2
- admin, timeout.......... 9-16
- group IKE ID..........5-181 to 5-196
- groups, server support 9-12
- IKE
  - *See* IKE users
- L2TP..........9-76 to 9-79
- multiple-type.......... 9-4
- shared IKE ID ....5-196 to 5-201
- WebAuth 9-12
- XAuth..........9-60 to 9-74

users, auth
- *See* auth users

users, IKE
- *See* IKE users

users, multiple administrative.......... 3-31

V

VC.......... 12-70

VCI.......... 12-70

vendor IDs, VSA.......... 9-19

vendor-specific attributes.......... 9-18

Verified mode.......... 13-15

Verisign.......... 5-34

VIP.......... 2-12
- configuring.......... 8-82
- definition.......... 8-6
- editing 8-84
- global zones.......... 8-82
- reachable from other zones.......... 8-82
- removing.......... 8-84
- required information 8-81

VIP services
- custom and multi-port..........8-85 to 8-88
- custom, low port numbers.......... 8-82

VIP, to zone with interface-based NAT 2-104

virtual adapters.......... 9-60

virtual channel identifier
- *See* VCI

virtual circuit
- *See* VC

virtual HA interfaces 2-48, 11-34

virtual IP
- *See* VIP

virtual path identifier
- *See* VPI

virtual private networks
- *See* VPNs

virtual router 14-50, 14-102

virtual routers
- *See* VRs

virtual routers, MIP default.......... 8-66

virtual security device groups
- *See* VSD groups

virtual security interface
- *See* VSI

virtual system support 13-5

virtual systems.......... 2-10
- admins.......... 3-32
- failover.......... 11-88
- load sharing 11-89
- manageability and security of 10-71
- NSRP.......... 11-88
- read-only admins 3-32
- VIP.......... 10-31

VLAN zone.......... 2-91

VLAN1
- interface 2-91, 2-97
- zones 2-91

VLAN1, management options.......... 3-27

VLAN-based traffic classification . 10-40, 10-41 to 10-67

VLANs
- communicating with another VLAN 10-39, 10-64 to 10-67
- creating..........10-43 to 10-64
- subinterfaces.......... 10-61
- tag 10-43, 10-61
- Transparent mode 10-42, 10-43
- trunking.......... 10-42
- VLAN-based traffic classification ......10-40, 10-41 to 10-67

VLANs, tags 2-3

VNC 4-124

voice-over IP
- bandwidth management.......... 6-62

VPI.......... 12-70

VPN idletime 9-63

VPN monitoring ....5-238 to 5-249, 12-110
- destination address..........5-240 to 5-242
- destination address, XAuth.......... 5-240
- ICMP echo requests 5-249
- outgoing interface ....5-240 to 5-242
- policies.......... 5-241
- rekey option..........5-239, 5-255
- routing design.......... 5-71
- SNMP 5-249
- status changes 5-238, 5-241

VPNs
- Aggressive mode 5-10
- AutoKey IKE 3-41, 3-76, 5-7
- configuration tips .... 5-69 to 5-71
- cryptographic options .... 5-48 to 5-61
- Diffie-Hellman exchange 5-10
- Diffie-Hellman groups 5-10
- for administrative traffic 3-75
- FQDN aliases 5-130
- FQDN for gateways .... 5-129 to 5-139
- Main mode 5-9
- manual key 3-76
- manual keys 3-41
- MIP 5-139
- multiple tunnels per tunnel interface 5-251 to 5-285
- NAT for overlapping addresses .... 5-139 to 5-149
- NAT-dst 5-139
- NAT-src 5-141
- packet flow .... 5-63 to 5-69
- Phase 1 5-9
- Phase 2 5-11
- policies 2-180
- policies for bidirectional 5-125
- proxy IDs, matching 5-70
- redundant gateways .... 5-287 to 5-300
- redundant groups, recovery procedure 5-292
- replay protection 5-12
- route- vs policy-based 5-62
- SAs 5-8
- to zone with interface-based NAT 2-104
- Transport mode 5-4
- tunnel always up 5-239
- tunnel zones 2-28
- VPN groups 5-288
- VPN monitoring and rekey 5-239

VRRP 11-83, 11-112

VRs .... 7-37 to 7-42, 10-6
- access lists 7-40
- BGP .... 7-106 to 7-113
- ECMP 7-36
- forwarding traffic between 2-5
- introduction 2-4
- modifying 7-22
- on vsys 7-26
- OSPF .... 7-49 to 7-67
- RIP .... 7-75 to 7-90, 14-53 to 14-70
- route metrics 7-31
- router IDs 7-22
- SBR 7-17
- shared 10-37
- shared, creating a 10-38
- SIBR 7-19
- using two 7-23

VRs, routes
- exporting 7-42
- filtering 7-39
- importing 7-42
- maps 7-38
- preference 7-30
- redistribution 7-37
- selection 7-30

VRs, routing tables
- lookup 7-32
- lookup in multiple VRs 7-34
- maximum entries 7-29

VSA attribute types 9-19

VSAs 9-18

VSD groups .... 4-172, 11-16 to 11-20, 11-102 to 11-104
- failover 11-80
- heartbeats 11-9, 11-18, 11-103
- hold-down time 11-36, 11-38
- member states .... 11-17, 11-102 to 11-103, 11-112
- priority numbers 11-16

VSIs 11-4, 11-16, 11-102
- multiple VSIs per VSD group 11-88
- static routes 11-20

vsys
- admin 10-7
- keys 10-37
- objects, creating 10-4

W

web browser requirements 3-2

web filtering .... 2-184, 4-101 to 4-108
- applying profiles to policies 4-98
- blocked URL message 4-105
- blocked URL message type 4-105
- cache 4-93
- communication timeout 4-104
- integrated 4-92
- profiles 4-96
- redirect 4-101
- routing 4-106
- server status 4-106
- servers per vsys 4-102
- SurfControl CPA servers 4-92
- SurfControl SCFP 4-103
- SurfControl server name 4-104
- SurfControl server port 4-104
- SurfControl servers 4-93
- URL categories 4-95
- Websense server name 4-104
- Websense server port 4-104

Web User Interface (WebUI) 14-32

Web User Interface (WebUI), on sample client, downstream router 14-40

WebAuth ... 9-12, 9-39
  external user groups ... 9-51
  pre-policy auth process ... 9-39
  user groups, local ... 9-50
  with SSL (user groups, external) ... 9-53
WebAuth, pre-policy auth process ... 2-183
WebTrends ... 3-54, 3-69
  encryption ... 3-70, 3-75
  messages ... 3-70
WebUI ... 3-2
  Help files ... 3-2
  management options ... 3-26
WEP ... 12-121
Whois ... 4-124
wildcards ... 5-184, 13-15
WinNuke attacks ... 4-51
WINS
  L2TP settings ... 5-209
WINS server ... 14-132
Wired Equivalent Privacy
  See WEP
wireless bridge groups ... 12-145
wireless interface
  logical interface ... 2-46
wireless interfaces
  binding SSID to ... 12-143
  binding to radio ... 12-144
  configuring ... 12-143
  disabling ... 12-145
Wireless Local Area Network
  See WLAN
WLAN
  access control list ... 12-131
  advanced parameters ... 12-138
  aging interval ... 12-138
  authentication and encryption ... 12-120
  beacon interval ... 12-139
  bridge groups ... 12-145
  burst threshold ... 12-140
  Clear To Send mode ... 12-141
  Clear To Send rate ... 12-142
  Clear To Send type ... 12-142
  configurations, reactivating ... 12-132
  configuring Super G ... 12-132
  country codes and channels ... 12-129
  DTIM ... 12-140
  extended channels ... 12-130
  finding available channels ... 12-131
  fragment threshold ... 12-140
  preamble length ... 12-143
  Request to Send threshold ... 12-141
  site survey ... 12-130
  slot time ... 12-142
  viewing wireless configuration information 12-145
  WMM ... 12-134
  XR ... 12-133
WLAN WAP operation modes
  802.11b clients, configuring ... 12-117, 12-118
  802.11g clients, configuring ... 12-118
WLAN, wireless interfaces
  binding ... 12-143
WMM
  access categories ... 12-134
  configuring quality of service ... 12-134
  default settings ... 12-135
  enabling ... 12-134

X

XAuth
  authentication ... 14-138
  bypass-auth ... 9-61
  client authentication ... 9-75
  defined ... 9-60
  query remote settings ... 9-61
  ScreenOS as client ... 9-75
  TCP/IP assignments ... 9-62
  virtual adapters ... 9-60
  VPN idletime ... 9-63
  VPN monitoring ... 5-240
  when to use ... 14-132
XAuth addresses
  assignments ... 9-60
  authentication, and ... 9-71
  IP address lifetime ... 9-62 to 9-63
  timeout ... 9-62
XAuth users ... 9-60 to 9-74
  authentication ... 9-60
  local authentication ... 9-63
  local group authentication ... 9-65
  server support ... 9-12
  with L2TP ... 9-4
XAuth, external
  auth server queries ... 9-61
  user authentication ... 9-66
  user group authentication ... 9-68
XR, configuring ... 12-133

Y

Yahoo! Messenger 4-124

Z

zip files, blocking 4-161
zombie agents...4-27, 4-29
zones..2-25 to 2-33, 10-6
    defining 2-30
    editing.. 2-31
    function 2-32
    function, MGT interface..................................... 2-47
    global 2-28
    global security.. 2-2
    Layer 2... 2-91
    shared 10-37
    tunnel... 2-28
    VLAN..2-33, 2-91
    vsys 10-6
zones, global.. 8-82
zones, ScreenOS ....2-25 to 2-33
    predefined.. 2-2
    security interfaces 2-3
zones, security 2-2, 2-28
    determination, destination zone 2-12
    determination, source zone 2-11
    global 2-2
    interfaces, monitoring 2-82
    interfaces, physical 2-46