NetScreen 概念与范例

ScreenOS 参考指南

第 1 卷：概述

ScreenOS 5.1.0

编号 093-1366-000-SC

修订本 B

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

第 1 卷：概述

目录 i
前言 xxix
概念与范例组织 xxxi
约定 xxxv
CLI 约定 xxxv
WebUI 约定 xxxvi
插图约定 xxxviii
命名约定和字符类型 xxxix
NetScreen 文档 xl
附录 A 词汇表 ..... A-I
索引 ..... IX-I

第 2 卷：基本原理

目录 i
前言 vii
约定 viii
CLI 约定 viii
WebUI 约定 ix
插图约定 xi
命名约定和字符类型 xii
Juniper Networks NetScreen 文档 xiii
第 1 章 ScreenOS 体系结构 1
安全区段 2
安全区段接口 3
物理接口 3
子接口 4
虚拟路由器 5
策略 6
VPN 9
虚拟系统 11
数据包流序列 12
范例 (第 1 部分): 具有六个区段的企业 15
范例 (第 2 部分): 六个区段的接口 17
范例 (第 3 部分): 两个路由选择域 21
范例 (第 4 部分): 策略 23
第 2 章 区段 29
安全区段 32
Global 区段 32
SCREEN 选项 32
通道区段 33
范例：将 Tunnel 接口绑定到 Tunnel 区段 34

配置安全区段和 Tunnel 区段 35
创建区段 35
修改区段 36
删除区段 37
功能区段 38
Null 区段 38
MGT 区段 38
HA 区段 38
Self 区段 38
VLAN 区段 38
端口模式 39
设置端口模式 45
范例：Home-Work 端口模式 46
Home-Work 和 Combined 端口模式下的区段 47
范例：Home-Work 区段 49
第 3 章 接口 51
接口类型 53
安全区段接口 53
物理接口 53
子接口 53
聚合接口 54
冗余接口 54
虚拟安全接口 54
功能区段接口 55
管理接口 55
HA 接口 55
通道接口 56
删除通道接口 59
范例：删除通道接口 59
查看接口 61
接口表 61
配置安全区段接口 63
将接口绑定到安全区段 63
范例：绑定接口 63
为 L3 安全区段接口编址 64
公共 IP 地址 64
私有 IP 地址 65
范例：编址接口 66
从安全区段解除接口绑定 67
范例：解除接口绑定 67
修改接口 68
范例：修改接口设置 69
创建子接口 70
范例：根系统中的子接口 70
删除子接口 71
范例：删除安全区段接口 71
二级 IP 地址 72
二级 IP 地址属性 72
范例：创建二级 IP 地址 73
回传接口 74
范例：创建回传接口 74
使用回传接口 75
范例：用于管理的回传接口 75
范例：回传接口上的 BGP 76
范例：回传接口上的 VSI 76
范例：回传接口作为源接口 77
接口状态更改 78
物理连接监控 80
跟踪 IP 地址 80
配置 IP 跟踪 81
范例：配置接口 IP 跟踪 83

接口监控 87
范例：两个被监控接口 89
范例：接口监控环 90
安全区段监控 94
非活动接口和信息流 95
出口接口上的故障 96
入口接口上的故障 99

第 4 章 接口模式 103

透明模式 104
区段设置 105
VLAN 区段 105
预定义的第 2 层区段 105
信息流转发 106
未知单播选项 107
泛滥方法 108
ARP/Trace-Route 方法 110
范例：用于管理的 VLAN1 接口 114
范例：透明模式 117

NAT 模式 122
入站和出站 NAT 信息流 124
接口设置 125
范例：NAT 模式 126

路由模式 130
接口设置 131
范例：路由模式 132

第 5 章 策略的构建块 137

地址 139
地址条目 140
范例：添加地址 140
范例：修改地址 141
范例：删除地址 142
地址组 142
范例：创建地址组 144
范例：编辑地址组条目 145
范例：移除成员和组 146

服务 147
预定义的服务 147
定制服务 149
范例：添加定制服务 149
范例：修改定制服务 151
范例：移除定制服务 151
服务超时 152
范例：设置服务超时 153
ICMP 服务 154
范例：定义 ICMP 服务 155
RSH ALG 156
Sun 远程过程调用应用程序层网关 156
典型 RPC 调用场景 156
Sun RPC 服务 157
范例：Sun RPC 服务 158
Microsoft 远程过程调用应用程序层网关 159
MS RPC 服务 159
MS RPC 服务组 162
范例：MS RPC 服务 162
实时流协议应用程序层网关 164
RTSP 请求方法 166
RTSP 状态代码 168
范例：专用域中的媒体服务器 170
范例：公共域中的媒体服务器 173

IP 语音通信的 H.323 协议 176
范例：Trust 区段中的关守设备（透明或路由模式）..... 176
范例：Untrust 区段中的关守设备（透明或路由模式）..... 178
范例：使用 NAT 的外向呼叫 181
范例：使用 NAT 的内向呼叫 186
范例：Untrust 区段中的关守设备（采用 NAT）..... 190
会话启动协议 (SIP) 195
SIP 请求方法 196
SIP 响应的类别 198
ALG – 应用程序层网关 199
SDP 200
针孔创建 201
会话静止超时 203
SIP 攻击保护 204
范例：SIP 保护拒绝 204
范例：信号发送与媒体静止超时 205
范例：UDP 泛滥保护 205
范例：SIP 最大连接数 206
使用网络地址转换的 SIP 207
外向呼叫 207
内向呼叫 208
已转移呼叫 208
呼叫终止 208
呼叫 Re-INVITE 消息 208
呼叫会话计时器 209
呼叫取消 209
分支 209
SIP 消息 209
SIP 包头 210
SIP 正文 213
SIP NAT 场景 213
使用 SIP Registrar 的内向 SIP 呼叫支持 216
范例：内向呼叫（接口 DIP）..... 218
范例：内向呼叫（DIP 池）..... 222
范例：使用 MIP 的内向呼叫 226
范例：私有区段中的代理 229
范例：公用区段中的代理 233
范例：三区段， DMZ 中的代理 237
范例：Untrust 区段内部 243
范例：Trust 内部区段 249
范例：SIP 的全网状 VPN 253
VoIP 服务的带宽管理 261
服务组 263
范例：创建服务组 264
范例：修改服务组 265
范例：移除服务组 266
DIP 池 267
端口地址转换 268
范例：创建使用 PAT 的 DIP 池 268
范例：修改 DIP 池 270
附着 DIP 地址 270
扩展接口和 DIP 271
范例：在不同子网中使用 DIP 271
回传接口和 DIP 279
范例：回传接口上的 DIP 280
DIP 组 285
范例：DIP 组 287
时间表 289
范例：循环时间表 289

第 6 章 策略 293
基本元素 295
三种类型的策略 296
区段间策略 296
区段内部策略 297
全局策略 297
策略组列表 298
定义的策略 299
策略和规则 299
策略的结构 300
ID 301
区段 301
地址 301
服务 301
动作 302
应用 303
名称 303
VPN 通道 303
L2TP 通道 304
深入检查 304
放置在策略列表的顶部 304
源地址转换 305
目标地址转换 305
用户认证 306
HA 会话备份 308
URL 过滤 308
记录 309
计数 309
信息流报警临界值 309
时间表 309
防病毒扫描 310
信息流整形 310
策略应用 312
查看策略 312
策略图标 312
创建策略 314
策略位置 314
范例：区段间策略邮件服务 315
范例：区段间策略设置 320
范例：区段内部策略 327
范例：全局策略 330
输入策略环境 331
每个策略组件含多个条目 332
地址排除 333
范例：目标地址排除 333
修改和禁用策略 337
策略验证 338
重新排序策略 339
移除策略 340
第 7 章 信息流整形 341
应用信息流整形 342
在策略级管理带宽 342
范例：信息流整形 343
设置服务优先级 349
范例：优先级排列 350
第 8 章 系统参数 357
域名系统支持 359
DNS 查找 360
DNS 状态表 361
范例：DNS 服务器和刷新时间安排 362
范例：设置 DNS 刷新时间间隔 363

动态 DNS 364
范例：dyndns 服务器的 DDNS 设置 365
范例：ddo 服务器的 DDNS 设置 366
代理 DNS 地址分隔 367
范例：分隔 DNS 请求 368
DHCP 370
DHCP 服务器 372
范例：充当 DHCP 服务器的 NetScreen 设备 372
DHCP 服务器选项 378
范例：定制 DHCP 服务器选项 379
NSRP 集群中的 DHCP 服务器 379
DHCP 服务器检测 380
范例：打开 DHCP 服务器检测 381
范例：关闭 DHCP 服务器检测 381
DHCP 中继代理 382
范例：NetScreen 设备作为 DHCP 中继代理 383
DHCP 客户端 388
范例：NetScreen 设备作为 DHCP 客户端 388
TCP/IP 设置传播 390
范例：转发 TCP/IP 设置 391
PPPoE 393
范例：设置 PPPoE 393
范例：在主 Untrust 接口和备份 Untrust 接口上配置 PPPoE 398
单个接口上的多个 PPPoE 会话 399
未标记的接口 400
范例：多个 PPPoE 实例 401
PPPoE 和高可用性 404
升级和降级固件 405
升级和降级设备固件的要求 406
NetScreen-Security Manager 服务器连接 407
下载新固件 407
上传新固件 410
使用启动 / OS 加载程序 412
升级 NSRP 配置中的 NetScreen 设备 414
升级 NSRP 主动 / 被动配置中的设备 414
升级 NSRP 主动 / 主动配置中的设备 419
认证固件和 DI 文件 425
获得认证证书 425
加载认证证书 426
认证 ScreenOS 固件 427
认证 DI 攻击对象数据库文件 428
下载和上传配置 429
保存和导入配置 429
配置回滚 431
上次已知正确的配置 431
自动与手动配置回滚 432
加载新的配置文件 433
锁定配置文件 434
向配置文件添加注释 435
设置 NetScreen-Security Manager Bulk-CLI 436
许可密钥 437
范例：扩大用户容量 438
预定服务的注册与激活 439
临时服务 439
新设备上捆绑的 AV、 URL 过滤和 DI 服务 440
在现有服务上升级 AV、 URL 过滤和 DI 服务 441
只升级 DI 服务 442
系统时钟 443
日期和时间 443
时区 443

NTP 444
多个 NTP 服务器 444
最大时间调整 445
NTP 与 NSRP 445
范例：配置 NTP 服务器和最大时间差值 446
保护 NTP 服务器 447
索引 ..... IX-I

第 3 卷：管理

目录 i
前言 v
约定 vi
CLI 约定 vi
WebUI 约定 vii
插图约定 ix
命名约定和字符类型 x
Juniper Networks NetScreen 文档 xi
第 1 章 管理 1
通过 Web 用户界面进行管理 3
WebUI 帮助 4
将帮助文件复制到本地驱动器 4
将 WebUI 指向新的帮助位置 4
HTTP 5
会话 ID 5
安全套接字层 7
SSL 配置 9
将 HTTP 重定向到 SSL 11
通过命令行界面进行管理 13
Telnet 13
保障 Telnet 连接安全 14
安全外壳 15
客户端要求 17
NetScreen 设备上的基本 SSH 配置 17
认证 19
SSH 和 Vsys 21
主机密钥 22
范例：SSHv1 使用 PKA 进行自动登录 23
安全复制 (SCP) 24
串行控制台 25
调制解调器端口 26
通过 NetScreen-Security Manager 进行管理 27
在代理与管理系统之间建立初始连接 28
启用、禁用和取消设置代理 29
更改管理系统服务器地址 30
范例：设置主服务器 IP 地址 30
设置报告参数 31
范例：启用警报和统计信息报告 32
配置同步 33
范例：查看配置状态 33
范例：检索配置散列信息 34
配置时戳 35
范例：检索配置时戳 35
控制管理信息流 36
MGT 和 VLAN1 接口 37
范例：通过 MGT 接口进行管理 37
范例：通过 VLAN1 接口进行管理 38

管理接口 39
范例：设置管理接口选项 39
管理 IP 41
范例：设置多个接口的管理 IP 42
管理级别 44
根管理员 44
可读 / 写管理员 45
只读管理员 45
虚拟系统管理员 45
虚拟系统只读管理员 46
定义 Admin 用户 46
范例：添加只读 Admin 46
范例：修改 Admin 47
范例：删除 Admin 47
范例：清除 Admin 的会话 48
保障管理信息流安全 49
更改端口号 50
范例：更改端口号 50
更改 Admin 登录名和密码 51
范例：更改 Admin 用户的登录名和密码 52
范例：更改自己的密码 53
设置根 Admin 密码的最小长度 54
重置设备到出厂缺省设置 55
限制管理访问 56
范例：限制对单个工作站的管理 56
范例：限制对子网的管理 57
限制根 Admin 通过控制台访问 57
用于管理信息流的 VPN 通道 58
范例：通过基于路由的手动密钥 VPN 通道进行管理 59
范例：通过基于策略的手动密钥 VPN 通道进行管理 65
第 2 章 监控 NetScreen 设备 73
存储日志信息 74
事件日志 75
查看事件日志 76
范例：按照严重性级别和关键字查看事件日志 77
排序和过滤事件日志 78
范例：按照 IP 地址排序事件日志条目 79
下载事件日志 80
范例：下载事件日志 80
范例：下载关键事件的事件日志 81
流量日志 82
查看流量日志 84
范例：查看流量日志条目 84
排序和过滤流量日志 85
范例：按照时间排序流量日志 85
下载流量日志 86
范例：下载流量日志 86
Self 日志 87
查看 Self 日志 87
排序和过滤 Self 日志 88
范例：按照时间过滤 Self 日志 89
下载 Self 日志 90
范例：下载 Self 日志 90
资源恢复日志 91
范例：下载资源恢复日志 91
流量报警 92
范例：基于策略的入侵检测 93
范例：受破坏系统通知 94
范例：发送电子邮件警示 96

系统日志 97
范例：启用多个系统日志服务器 98
WebTrends 99
范例：启用通知事件的 WebTrends 99
SNMP 101
执行概述 104
范例：定义读 / 写 SNMP 公共组 105
自行生成的信息流的 VPN 通道 107
范例：通过基于路由的通道的自行生成的信息流 .. 109
范例：通过基于策略的通道的自行生成的信息流 .. 119
计数器 130
范例：查看屏幕计数器 135
附录 A SNMP MIB 文件 ..... A-I
索引 ..... IX-I

第 4 卷：攻击检测和防御机制

目录 i
前言 v
约定 vi
CLI 约定 vi
WebUI 约定 vii
插图约定 ix
命名约定和字符类型 x
Juniper Networks NetScreen 文档 xi
第 1 章 保护网络 1
攻击阶段 2
检测和防御机制 3
攻击监视 5
范例：监视来自 Untrust 区段的攻击 6
第 2 章 侦查威慑 7
IP 地址扫描 8
端口扫描 10
使用 IP 选项的网络侦查 12
操作系统探查 16
设置 SYN 和 FIN 标志 16
有 FIN 标志但无 ACK 标志 18
未设置标志的 TCP 包头 20
逃避技术 22
FIN 扫描 22
非 SYN 标记 23
IP 欺骗 26
范例：L3 IP 欺骗防护 29
范例：L2 IP 欺骗防护 33
IP 源路由选项 35
第 3 章 拒绝服务攻击防御 39
防火墙 DoS 攻击 40
会话表泛滥 40
基于源和目标的会话限制 40
范例：基于源的会话限制 43
范例：基于目标的会话限制 44

主动调整会话时间 44
范例：主动加速超时会话 46
SYN-ACK-ACK 代理泛滥 47
网络 DoS 攻击 49
SYN 泛滥 49
范例：SYN 泛滥防护 56
ICMP 泛滥 63
UDP 泛滥 65
Land 攻击 67
与操作系统相关的 DoS 攻击 69
Ping of Death 69
Teardrop 攻击 71
WinNuke 73
第 4 章 内容监控和过滤 75
碎片重组 77
恶意 URL 保护 77
应用程序层网关 78
范例：封锁数据包碎片中的恶意 URL 79
防病毒扫描 81
扫描 FTP 信息流 82
扫描 HTTP 信息流 84
HTTP MIME 扩展 85
HTTP Web 邮件 86
扫描 IMAP 和 POP3 信息流 87
扫描 SMTP 信息流 89
更新防病毒模式文件 91
范例：自动更新 93
范例：手动更新 94
应用防病毒扫描 95
范例：内部防病毒扫描 (POP3) 95
防病毒扫描器设置 98
有选择性的内容扫描 98
范例：扫描所有信息流类型 99
范例：SMTP 和 HTTP 的防病毒扫描 100
解压缩和最大信息量大小 101
范例：丢弃大文件 101
防病毒资源分配 102
失败模式行为 103
HTTP Keep-Alive 103
HTTP Trickling 104
URL 过滤 106
集成 URL 过滤 107
域名服务器 (DNS) 108
URL 过滤环境 108
范例：启用 URL 过滤 109
URL 类别 110
范例：URL 类别 111
URL 过滤配置文件 112
范例：URL 过滤配置文件 114
URL 配置文件和策略 115
范例：集成 URL 过滤 116
SurfControl 服务器 119
URL 过滤高速缓存 120
范例：高速缓存参数 120
重新定向 URL 过滤 121
范例：URL 过滤配置 127
第 5 章 深入检查 131
深入检查概述 133
攻击对象数据库服务器 137
范例：立即更新 138
范例：自动更新 140

范例：自动通知和立即更新 141
范例：手动更新 143
攻击对象和组 145
支持的协议 147
状态式签名 151
TCP 流式签名 152
协议异常 152
攻击对象组 153
更改严重性级别 153
范例：针对 P2P 的深入检查 155
禁用攻击对象 157
攻击操作 158
范例：攻击操作 – Close Server、 Close、 Close Client 159
攻击记录 170
范例：按攻击组禁用记录 170
将定制服务映射到应用程序 173
范例：将应用程序映射到定制服务上 174
范例：HTTP 攻击的应用程序至服务映射 178
定制攻击对象和组 181
用户定义的状态式签名攻击对象 181
规则表达式 182
范例：用户定义的状态式签名攻击对象 185
TCP 流式签名攻击对象 189
范例：用户定义的流式签名攻击对象 190
可配置的协议异常参数 192
范例：修改参数 192
排除 194
范例：攻击对象排除 194
精确封锁 HTTP 组件 201
ActiveX 控件 201
Java Applet 202
EXE 文件 202
ZIP 文件 202
范例：封锁 Java Applet 和 .exe 文件 203
第 6 章 可疑数据包属性 205
ICMP 碎片 206
大型 ICMP 数据包 208
有害 IP 选项 210
未知协议 212
IP 数据包碎片 214
SYN 碎片 216
第 7 章 GPRS 超额计费攻击防护 219
超额计费攻击说明 220
超额计费攻击解决方案 222
NSGP 模块 222
NetScreen 网守协议 222
范例：配置超额计费攻击防护功能 224
附录 A 用户定义签名的环境 ..... A-I
索引 ..... IX-I

第 5 卷 : VPN

目录 i
前言 v
约定 vi
CLI 约定 vi
WebUI 约定 vii
插图约定 ix
命名约定和字符类型 x
Juniper Networks NetScreen 文档 xi
第 1 章 IPSec 1
VPN 简介 2
IPSec 概念 3
模式 4
传送模式 4
通道模式 5
协议 7
AH 7
ESP 8
密钥管理 9
手动密钥 9
自动密钥 IKE 9
安全联盟 10
通道协商 11
第 1 阶段 11
Main Mode / Aggressive Mode (主模式和主动模式) 12
Diffie-Hellman 交换 13
第 2 阶段 13
完全正向保密 14
回放攻击保护 14
IKE 和 IPSec 数据包 15
IKE 数据包 15
IPSec 数据包 19
第 2 章 公开密钥密码术 23
公开密钥密码术简介 24
PKI 26
证书和 CRL 29
手动获取证书 30
范例 : 手动证书申请 31
范例 : 加载证书和 CRL 34
范例 : 配置 CRL 设置 36
自动获取本地证书 38
范例 : 自动证书申请 39
自动证书更新 43
密钥对生成 43
使用 OCSP 的状态检查 44
配置 OCSP 45
指定 CRL 或 OCSP 45
查看状态检查属性 45
指定 OCSP 响应方 URL 46
删除状态检查属性 46
自签证书 47
用 SSL 保护管理信息流 48
证书验证 49
手动创建自签证书 51

范例 : 管理员定义的自签证书 52
证书自动生成 57
删除自签证书 59

第 3 章 VPN 准则 61

加密选项 62
站点到站点加密选项 63
拨号 VPN 选项 72
基于路由和基于策略的通道 80
数据包流 : 站点到站点 VPN.....82
通道配置技巧 88
基于路由的 VPN 安全注意事项 90
Null 路由.....91
拨号或租用线路 93
范例 : 租用线路或 Null 路由 VPN 故障切换 94
引诱通道接口 97
通道接口的虚拟路由器 98
重新路由到另一个通道 98

第 4 章 站点到站点 VPN.....99

站点到站点 VPN 配置 100
站点到站点通道的配置步骤 101
范例 : 基于路由的站点到站点 VPN，
自动密钥 IKE.....107
范例 : 基于策略的站点到站点 VPN，
自动密钥 IKE.....122
范例 : 基于路由的站点到站点 VPN，
动态对等方.....133
范例 : 基于策略的站点到站点 VPN，
动态对等方 148
范例 : 基于路由的站点到站点 VPN，
手动密钥..... 162
范例 : 基于策略的站点到站点 VPN，
手动密钥..... 173
使用 FQDN 的动态 IKE 网关 182
别名 183
范例 : 具有 FQDN 的自动密钥 IKE 对等方 184
具有重叠地址的 VPN 站点 199
范例 : 具有 NAT-Src 和 NAT-Dst 的通道接口 202
透明模式 VPN 217
范例 : 透明模式，基于策略的自动密钥 IKE VPN ... 218

第 5 章 拨号 VPN 229

拨号 VPN 230
范例 : 基于策略的拨号 VPN，自动密钥 IKE 231
范例 : 基于路由的拨号 VPN，动态对等方 240
范例 : 基于策略的拨号 VPN，动态对等方 252
用于拨号 VPN 用户的双向策略 262
范例 : 双向拨号 VPN 策略..... 263
组 IKE ID 270
具有证书的组 IKE ID 271
通配符和容器 ASN1-DN IKE ID 类型 273
范例 : 组 IKE ID (证书) 276
具有预共享密钥的组 IKE ID..... 283
范例 : 组 IKE ID (预共享密钥) 285
共享 IKE ID.....292
范例 : 共享 IKE ID (预共享密钥) 293

第 6 章 L2TP 301
L2TP 简介 302
数据包的封装和解封 306
封装 306
解封 307
L2TP 参数 308
范例 : 配置 IP 池和 L2TP 缺省设置 309
L2TP 和 IPSec 上的 L2TP 311
范例 : 配置 L2TP 312
范例 : 配置 IPSec 上的 L2TP 320
范例 : 双向的 IPSec 上的 L2TP 333
第 7 章 高级 VPN 功能 343
NAT 穿透 345
探查 NAT 346
穿透 NAT 设备 348
UDP 校验和 351
激活数据包 351
发起方 / 响应方对称 352
范例 : 启用 NAT 穿透 353
VPN 监控 355
重定密钥和优化选项 356
源接口和目标地址 357
策略注意事项 359
配置 VPN 监控功能 359
范例 : 为 VPN 监控指定源和目标地址 361
SNMP VPN 监控对象和陷阱 373
每个通道接口多个通道 374
路由到通道的映射 375
远程对等方的地址 376
手动和自动表条目 378
手动表条目 378
自动表条目 379
范例 : 重叠子网的一个通道接口上的多个 VPN 381
范例 : 自动路由表和 NHTB 表条目 413
范例附录 : 自动路由表条目的 OSPF 431
冗余 VPN 网关 434
VPN 组 435
监控机制 436
IKE 心跳信号 436
IKE 恢复过程 437
TCP SYN 标记检查 440
范例 : 冗余 VPN 网关 441
背对背的 VPN 453
范例 : 背对背的 VPN 454
集中星型 VPN 464
范例 : 集中星型 VPN 465
索引 ..... IX-I

第 6 卷：路由

目录 i
前言 vii
约定 viii
CLI 约定 viii
WebUI 约定 ix
插图约定 xi
命名约定和字符类型 xii
Juniper Networks NetScreen 文档 xiii
第 1 章 路由表和静态路由 1
路由选择基本原理 2
路由选择方法 2
静态路由选择 2
动态路由选择 3
组播路由选择 3
路由表 4
使用静态路由进行路由选择 6
NetScreen 设备上的虚拟路由器 8
配置静态路由的时机 9
配置静态路由 10
范例：静态路由 11
范例：用于通道接口的路由 15
将信息流转发到 Null 接口 17
永久活动路由 18
第 2 章 虚拟路由器 19
NetScreen 设备上的虚拟路由器 21
使用两个虚拟路由器 21
在虚拟路由器间转发信息流 22
配置两个虚拟路由器 22
范例：将区段绑定到 untrust-vr 23
定制虚拟路由器 25
范例：创建定制虚拟路由器 25
范例：删除定制虚拟路由器 26
虚拟路由器和虚拟系统 27
范例：在 Vsys 中创建虚拟路由器 28
范例：在虚拟路由器间共享路由 30
修改虚拟路由器 31
虚拟路由器 ID 32
范例：分配虚拟路由器 ID 33
最大路由表条目数 34
范例：限制路由表条目数 34
路由选择 35
路由优先级 35
范例：设置路由优先级 36
路由度量 37
路由表 38
基于源的路由选择 38
范例：基于源的路由选择 40
基于源接口的路由选择 42
范例：基于源接口的路由选择 43
路由查找顺序 44
范例：更改路由查找顺序 47
在多个虚拟路由器中的路由查找 48
等值路由 50
启用等值路由 52
范例：配置 ECMP 路由的最大数 52

路由重新分配 53
配置路由映射 54
路由过滤 56
访问列表 56
范例：配置访问列表 57
范例：将路由重新分配到 OSPF 58
在虚拟路由器之间导出和导入路由 60
范例：配置导出规则 61
范例：配置自动导出 63
第 3 章 开放式最短路径优先 (OSPF) 65
OSPF 概述 67
区域 67
路由器分类 68
Hello 协议 69
网络类型 69
广播网络 69
点对点网络 69
点对多点网络 70
链接状态通告 70
基本 OSPF 配置 71
创建 OSPF 路由选择实例 72
范例：创建 OSPF 实例 72
范例：移除 OSPF 实例 73
定义 OSPF 区域 74
范例：创建 OSPF 区域 75
为 OSPF 区域分配接口 76
范例：为区域分配接口 76
范例：配置区域范围 77
在接口上启用 OSPF 78
范例：在接口上启用 OSPF 78
范例：在接口上禁用 OSPF 79
检验配置 80
重新分配路由 83
范例：将路由重新分配给 OSPF 83
汇总重新分配的路由 84
范例：汇总重新分配的路由 84
范例：避免由汇总路由所创建的回路 85
全局 OSPF 参数 86
范例：通告缺省路由 87
虚拟链接 88
范例：创建虚拟链接 89
范例：创建自动虚拟链接 91
OSPF 接口参数 92
范例：设置 OSPF 接口参数 94
安全配置 95
邻居认证 95
范例：配置明文密码 95
范例：配置 MD5 密码 96
过滤 OSPF 邻居 97
范例：配置邻居列表 97
拒绝缺省路由 98
范例：删除缺省路由 98
防止泛滥 99
范例：配置 Hello 临界值 99
范例：配置 LSA 临界值 100
通道接口上的按需电路 101
范例：创建 OSPF 按需电路 101
范例：启用减少的泛滥 102

点对多点通道接口 103
设置链接类型 103
范例：设置 OSPF 链接类型 103
范例：禁用路由拒绝限制 104
范例：点对多点网络 104
第 4 章 路由选择信息协议 (RIP) 111
RIP 概述 113
基本 RIP 配置 114
创建 RIP 实例 115
范例：创建 RIP 实例 115
范例：删除 RIP 实例 116
在接口上启用 RIP 117
范例：在接口上启用 RIP 117
范例：在接口上禁用 RIP 118
重新分配路由 118
范例：将路由重新分配给 RIP 119
查看 RIP 信息 120
查看 RIP 数据库 120
范例：查看 RIP 数据库的详细信息 120
查看 RIP 协议详细信息 122
范例：查看 RIP 协议详细信息 122
查看 RIP 邻居信息 123
范例：查看有关 RIP 邻居的详细信息 123
查看接口的 RIP 协议详细信息 124
范例：查看特定接口的 RIP 124
全局 RIP 参数 125
通告缺省路由 127
范例：通告缺省路由 127
RIP 接口参数 128
范例：设置 RIP 接口参数 129
安全配置 130
邻居认证 130
范例：配置 MD5 密码 131
过滤 RIP 邻居 132
范例：配置可信任邻居 132
拒绝缺省路由 133
范例：拒绝缺省路由 133
防止泛滥 134
范例：配置更新临界值 134
范例：在通道接口上启用 RIP 135
可选 RIP 配置 137
RIP 协议版本 137
范例：设置 RIP 协议版本 137
前缀汇总 139
范例：启用前缀汇总 139
范例：禁用前缀汇总 140
备用路由 141
范例：设置备用路由 142
通道接口的按需电路 143
范例：配置按需电路 144
配置静态邻居 145
范例：配置静态邻居 145
点对多点通道接口 146
范例：具有按需电路的点对多点 146
第 5 章 边界网关协议 (BGP) 155
BGP 概述 156
BGP 消息的类型 157
路径属性 157
外部 BGP 和内部 BGP 158
基本 BGP 配置 159
创建并启用 BGP 实例 160

范例：创建 BGP 路由选择实例 160
范例：删除 BGP 实例 161
在接口上启用 BGP 162
范例：在接口上启用 BGP 162
范例：在接口上禁用 BGP 162
配置 BGP 对等方 163
范例：配置 BGP 对等方 165
范例：配置 IBGP 对等方组 166
验证 BGP 配置 168
安全配置 170
邻居认证 170
范例：配置 MD5 认证 170
拒绝缺省路由 171
范例：拒绝缺省路由 171
可选 BGP 配置 172
重新分配路由 173
范例：将路由重新分配给 BGP 174
AS 路径访问列表 174
范例：配置访问列表 175
将路由添加到 BGP 176
范例：带条件的路由通告 177
范例：设置路由权重 178
范例：设置路由属性 179
路由反射 180
范例：配置路由反射 181
联合 183
范例：配置联合 184
BGP 公共组 186
路由聚合 187
范例：聚合具有不同 AS 路径的路由 187
范例：在更新中过滤更具体的路由 188
范例：选择路径属性的路由 190
范例：更改聚合路由的属性 192
第 6 章 组播路由 193
组播路由概述 194
组播地址 194
反向路径转发 195
NetScreen 设备上的组播路由 196
组播路由表 196
静态组播路由 198
范例：配置静态组播路由 198
访问列表 199
通用路由封装 199
范例：配置 GRE 通道接口 201
组播策略 202
第 7 章 IGMP 205
IGMP 概述 206
主机 208
组播路由器 209
NetScreen 设备上的 IGMP 210
接口上的 IGMP 210
范例：在接口上启用 IGMP 210
范例：在接口上禁用 IGMP 211
安全注意事项 211
范例：为接受组配置访问列表 212
基本 IGMP 配置 213
范例：基本 IGMP 配置 213
检验您的 IGMP 配置 216
IGMP 操作参数 218

IGMP 代理 219
将成员关系报告向上游发送给源 219
将组播数据向下游发送到接收方 220
配置 IGMP 代理 222
接口上的 IGMP 代理 222
范例：接口上的 IGMP 代理 223
创建组播策略 225
范例：IGMP 的组播组策略 225
范例：基本 IGMP 代理配置 226
IGMP 发送方代理 238
范例：IGMP 发送方代理 239
第 8 章 PIM 247
PIM 概述 249
PIM-SM 250
组播分布树 251
指定路由器 252
将汇聚点映射到组 252
静态 RP 映射 252
动态 RP 映射 252
在分布树上转发信息流 253
源将数据发送到组 253
主机加入组 254
NetScreen 设备上的 PIM-SM 256
创建 PIM-SM 实例 257
范例：在虚拟路由器中启用 PIM-SM 实例 257
范例：移除 PIM-SM 实例 258
接口上的 PIM-SM 259
范例：接口上的 PIM-SM 259
范例：在接口上禁用 PIM-SM 260
组播组策略 261
Static-RP-BSR 消息 261
Join-Prune 消息 261
范例：PIM-SM 的组播组策略 262
基本 PIM-SM 配置 263
范例：基本 PIM-SM 配置 264
检验配置 270
配置 RP 273
静态 RP 273
范例：创建静态 RP 274
候选 RP 275
范例：创建候选 RP 275
安全注意事项 277
限制组播组 277
范例：限制组播组 277
限制组播源 279
范例：限制组播源 279
限制 RP 280
范例：限制 RP 280
PIM-SM 接口参数 281
邻居策略 281
范例：定义邻居策略 282
自举边界 283
范例：定义自举边界 283
代理 RP 284
配置代理 RP 287
范例：代理 RP 配置 288
PIM-SM 和 IGMPv3 301
PIM-SSM 302
NetScreen 设备上的 PIM-SSM 302
索引 ..... IX-I

第 7 卷：地址转换

目录 i
前言 iii
约定 iv
CLI 约定 iv
WebUI 约定 v
插图约定 vii
命名约定和字符类型 viii
Juniper Networks NetScreen 文档 ix
第 1 章 地址转换 1
地址转换简介 2
源网络地址转换 2
目标网络地址转换 4
基于策略的转换选项 9
NAT-Src 和 NAT-Dst 的方向特性 13
第 2 章 源网络地址转换 15
NAT-Src 简介 16
来自 DIP 池 (启用 PAT) 的 NAT-Src 17
范例：已启用 PAT 的 NAT-Src 18
来自 DIP 池 (禁用 PAT) 的 NAT-Src 21
范例：禁用 PAT 的 NAT-Src 21
来自 DIP 池 (带有地址变换) 的 NAT-Src 24
范例：带有地址变换的 NAT-Src 25
来自出口接口 IP 地址的 NAT-Src 30
范例：无 DIP 的 NAT-Src 30
第 3 章 目标网络地址转换 33
NAT-Dst 简介 34
NAT-Dst 的数据包流 36
NAT-Dst 的路由选择 40
连接到一个接口的地址 41
连接到一个接口但被路由器分隔的地址 42
由接口分隔的地址 43
NAT-Dst: 一对一映射 44
范例：一对一目标地址转换 45
从一个地址到多个地址的转换 49
范例：一对多目标地址转换 49
NAT-Dst: 多对一映射 53
范例：多对一目标地址转换 53
NAT-Dst: 多对多映射 58
范例：多对多目标地址转换 59
带有端口映射的 NAT-Dst 63
范例：带有端口映射的 NAT-Dst 63
同一策略中的 NAT-Src 和 NAT-Dst 68
范例：结合 NAT-Src 和 NAT-Dst 68
第 4 章 映射和虚拟 IP 地址 89
映射 IP 地址 90
MIP 和 Global 区段 91
范例：Untrust 区段接口上的 MIP 92
范例：从不同区段到达 MIP 95
范例：将 MIP 添加到通道接口 100
MIP-Same-as-Untrust 101
范例：Untrust 接口上的 MIP 102

MIP 和回传接口 105
范例：两个通道接口的 MIP 106
虚拟 IP 地址 115
VIP 和 Global 区段 117
范例：配置虚拟 IP 服务器 117
范例：编辑 VIP 配置 120
范例：移除 VIP 配置 120
范例：具有定制和多端口服务的 VIP 121
索引 ..... IX-I

第 8 卷：用户认证

目录 i
前言 iii
约定 iv
CLI 约定 iv
WebUI 约定 v
插图约定 vii
命名约定和字符类型 viii
Juniper Networks NetScreen 文档 ix
第 1 章 认证 1
用户认证类型 2
Admin 用户 3
多类型用户 5
组表达式 6
范例：组表达式 (AND) 8
范例：组表达式 (OR) 10
范例：组表达式 (NOT) 12
标题自定义 14
范例：自定义 WebAuth 标题 14
第 2 章 认证服务器 15
认证服务器类型 16
本地数据库 18
支持的用户类型和功能 18
范例：本地数据库超时 19
外部 Auth 服务器 20
Auth 服务器对象属性 21
Auth 服务器类型 23
RADIUS 23
RADIUS Auth 服务器对象属性 24
支持的用户类型和功能 24
NetScreen 词典文件 25
RADIUS 访问质询 26
SecurID 28
SecurID Auth 服务器对象属性 29
支持的用户类型和功能 29
LDAP 30
LDAP Auth 服务器对象属性 31
支持的用户类型和功能 31
定义 Auth 服务器对象 32
范例：RADIUS Auth 服务器 32
范例：SecurID Auth 服务器 35
范例：LDAP Auth 服务器 37

定义缺省 Auth 服务器 39
范例：更改缺省 Auth 服务器 39
第 3 章 认证用户 41
在策略中引用 Auth 用户 42
在策略中引用 Auth 用户组 45
范例：运行时认证 (本地用户) 46
范例：运行时认证 (本地用户组) 49
范例：运行时认证 (外部用户) 52
范例：运行时认证 (外部用户组) 55
范例：多个组中的本地 Auth 用户 59
范例：WebAuth (本地用户组) 63
范例：WebAuth (外部用户组) 66
范例：仅 WebAuth + SSL (外部用户组) 70
第 4 章 IKE、XAuth 和 L2TP 用户 75
IKE 用户和用户组 76
范例：定义 IKE 用户 77
范例：创建 IKE 用户组 79
在网关中引用 IKE 用户 80
XAuth 用户和用户组 81
IKE 协商中的 XAuth 用户 82
范例：XAuth 认证 (本地用户) 85
范例：XAuth 认证 (本地用户组) 87
范例：XAuth 认证 (外部用户) 89
范例：XAuth 认证 (外部用户组) 92
范例：XAuth 认证和地址分配 (本地用户组) 97
XAuth 客户端 103
范例：NetScreen 设备作为 XAuth 客户端 104
L2TP 用户和用户组 105
范例：本地和外部 L2TP Auth 服务器 106
索引 ..... IX-I

第 9 卷：虚拟系统

目录 i
前言 iii
约定 iv
CLI 约定 iv
WebUI 约定 v
插图约定 vii
命名约定和字符类型 viii
Juniper Networks NetScreen 文档 ix
第 1 章 虚拟系统 1
创建 Vsys 对象 3
范例：Vsys 对象和 Admin 3
虚拟路由器 6
区段 7
接口 8
信息流分类 10
发往 NetScreen 设备的信息流 10
直通信息流 11

专用和共享接口 15
专用接口 15
共享接口 15
导入和导出物理接口 18
范例：将物理接口导入到虚拟系统 18
范例：从虚拟系统导出物理接口 19
基于 VLAN 的信息流分类 21
VLAN 22
定义子接口和 VLAN 标记 23
范例：定义三个子接口和 VLAN 标记 25
在虚拟系统之间通信 28
范例：InterVsys 的通信 28
基于 IP 的信息流分类 33
范例：配置基于 IP 的信息流分类 35
以 Vsys Admin 身份登录 38
范例：登录并更改密码 38
索引 ..... IX-I

第 10 卷：高可用性

目录 i
前言 iii
约定 iv
CLI 约定 iv
WebUI 约定 v
插图约定 vii
命名约定和字符类型 viii
Juniper Networks NetScreen 文档 ix
第 1 章 NSRP 1
NSRP 概述 3
NSRP 和 NetScreen 的操作模式 8
基本主动 / 被动 NSRP 配置 8
缺省设置 9
范例：主动 / 被动配置的 NSRP 10
NSRP 集群 16
集群名称 18
范例：创建 NSRP 集群 19
执行对象 22
RTO 镜像状态 23
VSD 组 24
抢先选项 24
VSD 组成员状态 25
心跳信号消息 26
范例：创建两个 VSD 组 27
VSI 和静态路由 29
范例：Trust 和 Untrust 区段 VSI 30
同步 34
同步配置 34
同步文件 35

同步 RTO 35
范例：手动重新同步 RTO 36
范例：将设备添加到活动的 NSRP 集群 37
同步系统时钟 38
双 HA 接口 39
控制消息 40
数据消息 (数据包转发) 41
动态路由选择警告信息 42
双 HA 链接探查 43
范例：手动发送链接探查 44
范例：自动发送链接探查 45
设置过程 46
全网状配置的电缆连接 46
双主动 NSRP 配置 50
范例：双主动配置的 NSRP 50
第 2 章 接口冗余 59
冗余接口 60
范例：为 VSI 创建冗余接口 62
聚合接口 67
范例：配置聚合接口 68
Dual Untrust 接口 69
接口故障切换 70
范例：将信息流强制转发到备份接口 70
范例：将信息流从备份接口切换回主接口 70
范例：自动改发信息流 71
确定接口故障切换 72
使用 IP 跟踪的接口故障切换 73
范例：接口故障切换 73
范例：由活动通道到备份通道的故障切换 78
使用 VPN 通道监控的接口故障切换 85
范例：双活动通道 86
范例：对通道故障切换应用权重 93
串行接口 103
调制解调器的设置 104
范例：配置调制解调器的设置 105
ISP 配置 106
范例：配置 ISP 信息 107
串行接口故障切换 108
范例：配置 Trust-Untrust 模式下的拨号备份 109
范例：删除串行接口的缺省路由 112
范例：为串行接口添加缺省路由 112
范例：指定策略在串行接口故障切换后处于非活动状态 113
第 3 章 故障切换 115
设备故障切换 (NSRP) 116
VSD 组故障切换 (NSRP) 117
为设备或 VSD 组故障切换配置对象监控 118
配置被监控对象 120
物理接口对象 120
范例：监控接口 120
区段对象 121
范例：监控接口 121
被跟踪 IP 对象 122
范例：跟踪 IP 地址确定设备故障切换 125
虚拟系统故障切换 130
范例：虚拟系统间负载共享的 VSI 130

第 4 章 NSRP-Lite 137
NSRP-Lite 简介 139
集群和 VSD 组 140
缺省设置 141
集群 142
集群名称 143
认证和加密 144
VSD 组 145
VSD 组成员状态 145
心跳信号消息 146
抢先选项 147
用电缆连接和配置 NSRP-Lite 148
范例：配置 NSRP-Lite 149
配置和文件同步 156
同步配置 156
同步文件 157
范例：将设备添加到活动的 NSRP 集群 157
自动配置同步 158
路径监控 159
设置临界值 160
对被跟踪的 IP 地址加权 160
VPN 通道故障切换的 IP 跟踪 161
范例：通过 VPN 通道的 IP 跟踪 162
索引 ..... IX-I

前言

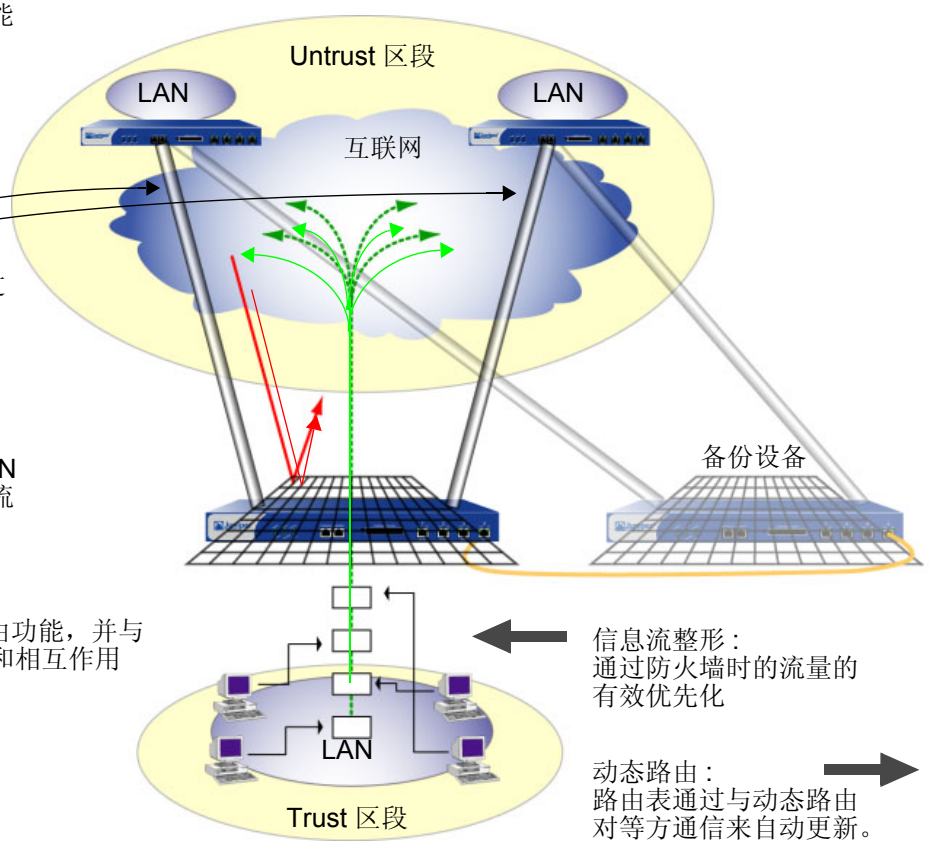
Juniper Networks NetScreen 设备是基于 ASIC 的、经 ICSA 认证[1] 的互联网安全装置和安全系统，它结合防火墙、虚拟专用网 (VPN) 和信息流整形功能，当连接到互联网时，对安全区段 [如内部局域网 (LAN) 或非军事区段 (DMZ)] 提供灵活的保护。

- **防火墙：**防火墙在专用的 LAN 和公用网 (如互联网) 之间的交叉边界处筛选流量。
- **VPN:** VPN 提供一个在两个或多个远程网络装置之间的安全信道。
- **集成网络功能：**动态路由协议获悉可达性并动态通告更改网络拓朴。此外，信息流整形功能允许管理监控，以及对通过 NetScreen 防火墙的信息流的控制，来维持网络的服务质量 (QoS) 级别。
- **冗余：**接口、路由路径、 NetScreen 设备以及 (在高端 NetScreen 设备上) 电源和风扇的高可用性，目的是避免这些区域存在单一故障点。

注意：*有关 NetScreen 符合 “联邦信息处理标准” (FIPS)，以及有关在 FIPS 模式下安装一个符合 FIPS 的 NetScreen 设备的说明，请参阅 NetScreen 资料 CD-ROM* 上的*特定平台* NetScreen Cryptographic Module Security Policy *文档。*

1. “互联网计算机安全联盟” (ICSA) 是一个组织，它集中所有类型的连接到互联网上的公司的网络安全。作为 ICSA 的功能之一，它向以下几种安全产品提供产品证书，如病毒防护、防火墙、 PKI、入侵检测、 IPSec 和密码系统。 ICSA 已经认证了 NetScreen 有关防火墙和 IPSec 的所有产品。

ScreenOS 中的关键功能



VPN: 在站点之间，通过互联网的信息流的安全信道

防火墙：在被保护的 LAN 和互联网之间筛选信息流

集成网络功能：执行路由功能，并与环境中的路由设备通信和相互作用

冗余：必要时，备份设备保持与主设备上相同的配置和会话，假扮主设备。（注意：接口、路由路径、电源和风扇也可能是冗余的。）

信息流整形：
通过防火墙时的流量的有效优先化

动态路由：
路由表通过与动态路由对等方通信来自动更新。

目标	使用
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

Juniper Networks NetScreen ScreenOS 这一操作系统可提供设置和管理任何 NetScreen 安全设备或系统所需的全部功能。*“NetScreen 概念与范例及 ScreenOS 参考指南”*提供关于通过 ScreenOS 配置和管理 NetScreen 设备的实用参考指南。

概念与范例组织

*“NetScreen 概念与范例及 ScreenOS 参考指南”*是一套多卷资料。以下信息概括和总结了每卷的资料：

第 1 卷，“概述”

- 在 *“NetScreen 概念与范例及 ScreenOS 参考指南”*中 “目录”包含了所有卷的主目录。
- 附录 A，“词汇表”提供所有关键术语的定义，这些术语贯穿于 *“NetScreen 概念与范例及 ScreenOS 参考指南”*的所有卷中。
- “索引”是一个主索引，它包括 *“NetScreen 概念与范例及 ScreenOS 参考指南”*的所有卷。

第 2 卷，“基本原理”

- 第 1 章，“ScreenOS 体系结构”介绍 NetScreen ScreenOS 中的体系结构的基本元素，并在最后给出一个包含这些元素中的多数元素、由四部分组成的、基于企业的示例。在本章及以后所有各章中，每个概念都附有说明性的例子。
- 第 2 章，“区段”解释安全区段、通道区段和功能区段。
- 第 3 章，“接口”介绍 NetScreen 设备上的各种物理、逻辑和虚拟接口。
- 第 4 章，“接口模式”解释 “透明的”、“网络地址转换” (NAT) 和 “路由器”接口操作模式的概念。
- 第 5 章，“策略的构建块”介绍用于创建策略和虚拟专用网 (VPN) 的元素：地址 (包括 VIP 地址)、服务及 DIP 池。它还介绍了几个支持 H.323 协议的配置的例子。
- 第 6 章，“策略”探究策略的组成及功能，而且给他们的创造和应用提供指导。
- 第 7 章，“信息流整形”说明如何在接口和 “策略”级别管理带宽和优先化服务。
- 第 8 章，“系统参数”介绍 “域名系统 (DNS)”寻址的概念；使用 “动态主机配置协议 (DHCP)”去分配或中继 TCP/IP 设置；下载及上载系统配置和软件；设置系统时钟。

第 3 卷，“管理”

- 第 1 章，“管理”说明可用于本地和远程管理 NetScreen 设备的不同方法。本章还解释了，属于可被定义的四个网络管理员级别中的每一个级别的特权。最后，它说明了如何确保本地和远程管理流量的安全。
- 第 2 章，“监控 NetScreen 设备”说明各种监控方法，并对解释监控输出提供指导。
- 附录 A，“SNMP MIB 文件”列出和简要描述了 MIB 编辑器可用的 “管理信息库 (MIB)”文件。

第 4 卷，“攻击检测和防御机制”

- 第 1 章，“保护网络”概述攻击的基本阶段，以及在每个阶段可用于对抗攻击的防火墙选项。
- 第 2 章，“侦查威慑”介绍可用于封锁 IP 地址扫描、端口扫描以及发现目标系统的操作系统 (OS) 类型的尝试的选项。
- 第 3 章，“拒绝服务攻击防御”解释防火墙、网络和与操作系统相关的 DoS 攻击，并说明 NetScreen 如何减轻这类攻击。
- 第 4 章，“内容监控和过滤”介绍如何保护 “超文本传输协议” (HTTP) 用户不受恶意 “统一资源定位器” (URL) 的影响，并说明如何配置 NetScreen 设备以便与第三方产品配合提供防病毒扫描和 URL 过滤。
- 第 5 章，“深入检查”说明如何配置 NetScreen 设备以获得 “深入检查” (DI) 攻击对象更新、如何创建用户定义的攻击对象和攻击对象组、以及如何在策略级应用 IDP。
- 第 6 章，“可疑数据包属性”介绍封锁潜在危险数据包的众多 SCREEN 选项。
- 第 7 章，“GPRS 超额计费攻击防护”介绍 “GPRS Overbilling”攻击并讲述解决方案。
- 附录 A，“用户定义签名的环境”提供定义状态式签名攻击对象时可指定的上下文列表和说明。

第 5 卷，“VPN”

- 第 1 章，“IPSec”提供有关 IPSec 的背景信息，介绍 “主动”和 “主”模式下 IKE 协商 “阶段 1”的流程顺序，并在最后提供有关 IKE 和 IPSec 数据包封装的信息。
- 第 2 章，“公开密钥密码术”提供有关如何获得和加载数字证书和证书撤消列表 (CRL) 的信息。
- 第 3 章，“VPN 准则”提供一些有用信息来帮助选择可用的 VPN 选项。它还提供数据包流图表来具体化 VPN 数据包处理。
- 第 4 章，“站点到站点 VPN”提供关于连接两个专用网络的 VPN 配置的多方面例子。
- 第 5 章，“拨号 VPN”提供使用 AutoKey IKE 的客户端到 LAN 通信的多方面例子。还详述组 IKE ID 和共享的 IKE ID 配置。
- 第 6 章，“L2TP”解释 “第 2 层通道协议 (L2TP)”，它单独使用以及与 IPSec (IPSec 上的 L2TP) 配合使用。
- 第 7 章，“高级 VPN 功能”包含高级 VPN 配置的信息和示例，例如 NAT 穿透、 VPN 监控、将多个通道绑定到单个通道接口以及集中星型背对背通道设计。

第 6 卷，“路由”

- 第 1 章，“路由表和静态路由”介绍 ScreenOS 路由表、 NetScreen 设备上的基本路由过程以及如何在 NetScreen 设备上配置静态路由。
- 第 2 章，“虚拟路由器”介绍如何在 NetScreen 设备上配置虚拟路由器以及如何在协议或虚拟路由器之间重新分配路由表条目。
- 第 3 章，“开放式最短路径优先 (OSPF)”介绍如何在 NetScreen 设备上配置 OSPF 动态路由协议。
- 第 4 章，“路由选择信息协议 (RIP)”介绍如何在 NetScreen 设备上配置 RIP 动态路由协议。
- 第 5 章，“边界网关协议 (BGP)”介绍如何在 NetScreen 设备上配置 BGP 动态路由协议。
- 第 6 章，“组播路由”介绍基本的组播路由概念。
- 第 7 章，“IGMP”介绍如何在 NetScreen 设备上配置 “互联网组管理协议” (IGMP)。
- 第 8 章，“PIM”介绍如何在 NetScreen 设备上配置 “协议无关组播”(PIM) 路由协议。

第 7 卷，“地址转换”

- 第 1 章，“地址转换”解释源地址转换和目的地址转换的不同方法。
- 第 2 章，“源网络地址转换”介绍源地址转换的不同方法。
- 第 3 章，“目标网络地址转换”介绍目标地址转换的不同方法。
- 第 4 章，“映射和虚拟 IP 地址”介绍如何使用映射 IP (MIP) 和虚拟 IP (VIP) 地址执行目标地址转换。

第 8 卷，“用户认证”

- 第 1 章，“认证”详述 NetScreen 支持的各种认证方法和用途。
- 第 2 章，“认证服务器”介绍使用三种可能类型的外部认证服务器 (RADIUS、 SecurID 或 LDAP) 或内部数据库的选项，并讲解如何配置 NetScreen 设备与每种类型协同工作。
- 第 3 章，“认证用户”说明如何定义认证用户的配置文件，及如何将其添加到存储在本地或外部 RADIUS 认证服务器上的用户组。
- 第 4 章，“IKE、XAuth 和 L2TP 用户”说明如何定义 IKE、XAuth 和 L2TP 用户。XAuth 部分主要介绍有关将 NetScreen 设备用作 XAuth 服务器的内容，但也包括有关配置所选 NetScreen 设备作为 XAuth 客户端的内容。

第 9 卷，“虚拟系统”

- 第 1 章，“虚拟系统”介绍虚拟系统的概念、专用的和共享的接口，以及基于 VLAN 和基于 IP 的流量分类。它还介绍如何建立虚拟系统，以及创建虚拟系统管理员。

第 10 卷，“高可用性”

- 第 1 章，“NSRP”说明如何架设 NetScreen 设备的电缆，如何配置和管理一个冗余组中的 NetScreen 设备，并以此提供使用 “NetScreen 冗余协议 (NSRP)”的高可用性。
- 第 2 章，“接口冗余”介绍 NetScreen 设备提供接口冗余用到的几种方法。
- 第 3 章，“故障切换”介绍设备、虚拟安全设备 (VSD) 组和虚拟系统的故障切换配置。还介绍如何监控特定对象以确定设备或 VSD 组的故障切换。
- 第 4 章，“NSRP-Lite”介绍如何配置支持 NSRP-Lite 的 NetScreen 设备。

约定

本文档包含几种类型的约定，以下部分将加以介绍：

- “CLI 约定”
- 第 xxxvi 页上的 “WebUI 约定”
- 第 xxxviii 页上的 “插图约定”
- 第 xxxix 页上的 “命名约定和字符类型”

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

- 在中括号 [ ] 中的任何内容都是可选的。
- 在大括号 { } 中的任何内容都是必需的。
- 如果选项不止一个，则使用管道 (|) 分隔每个选项。例如，

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

  意味着 “设置 ethernet1、 ethernet2 或 ethernet3 接口的管理选项”。
- 变量以*斜体*方式出现。例如：

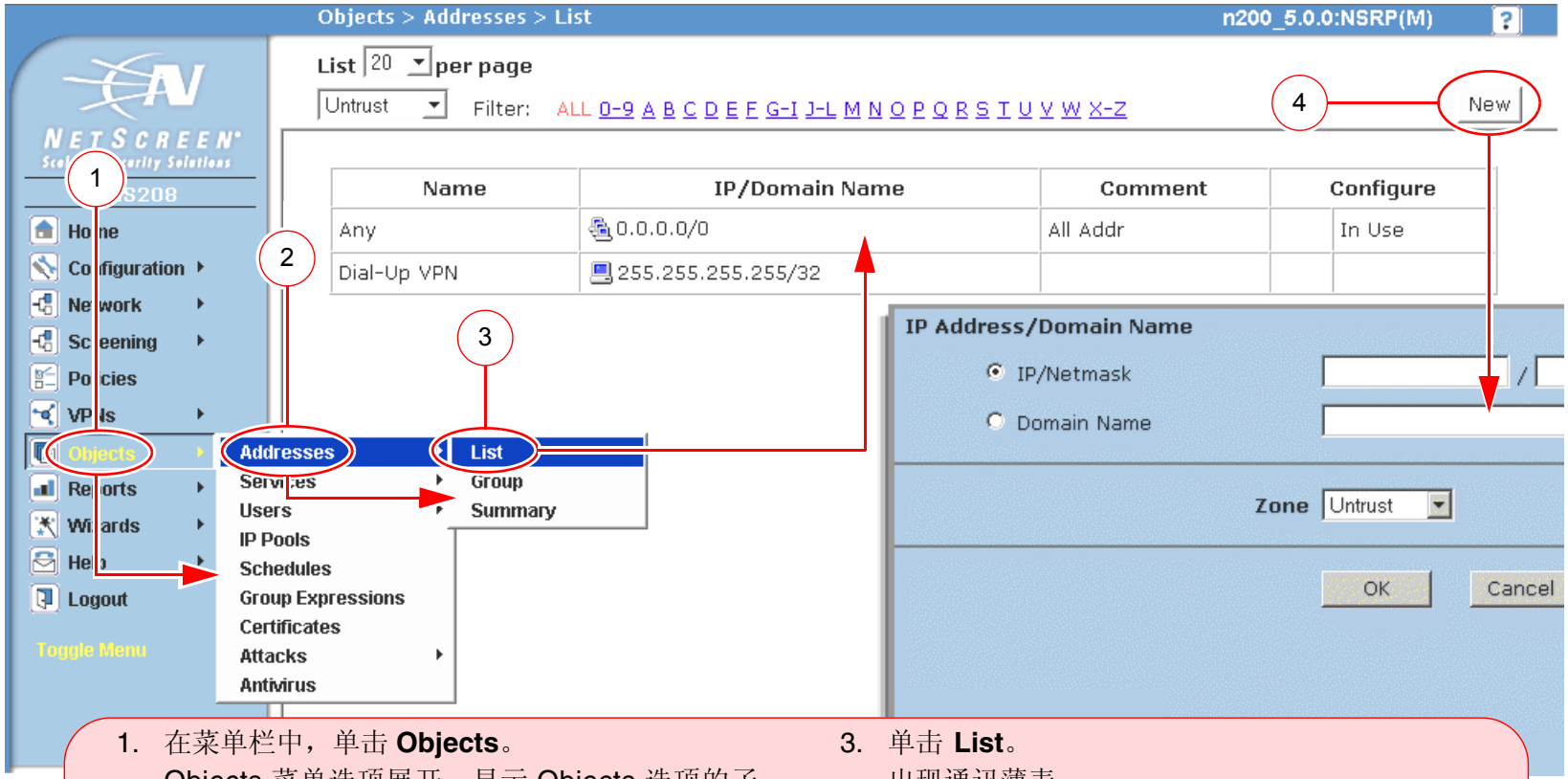
  ```
  set admin user name password
  ```

当 CLI 命令在句子的上下文中出现时，应为**粗体** (除了始终为*斜体*的变量之外)。例如：“使用 **get system** 命令显示 NetScreen 设备的序列号”。

> ***注意：****当键入关键字时，只需键入足够的字母就可以唯一地标识单词。例如，要输入命令* ***set admin user joe j12fmt54****，键入* ***set adm u joe j12fmt54*** *就足够了。尽管输入命令时可以使用此捷径，但本文所述的所有命令都以完整的方式提供。*

WebUI 约定

贯穿本书的全部篇章，用一个 V 形符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。例如，指向地址配置对话框的路径显示为 **Objects > Addresses > List > New**。此导航序列如下所示。



1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示 Objects 选项的子菜单。
2. (Applet 菜单) 将鼠标光标悬停在 **Addresses** 上。
   (DHTML 菜单) 单击 **Addresses**。
   Addresses 选项展开，显示 Addresses 选项的子菜单。
3. 单击 **List**。
   出现通讯薄表。
4. 单击 **New** 链接。
   出现新地址配置对话框。

如要用 WebUI 执行任务，必须首先导航到相应的对话框，然后可在该对话框中定义对象和设置参数。每个任务的指令集划分为两部分：导航路径和配置详细信息。例如，下列指令集包含指向地址配置对话框的路径和要配置的设置：

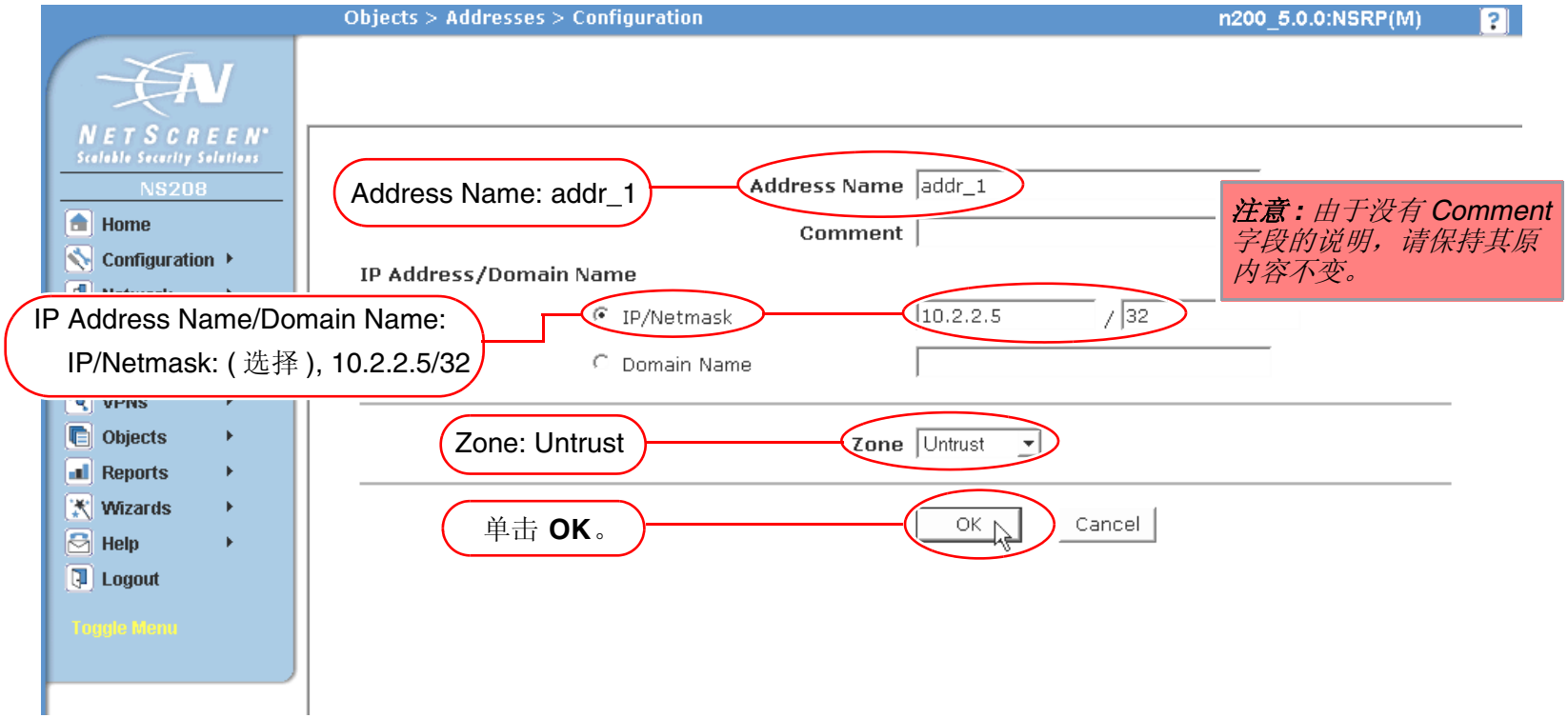
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

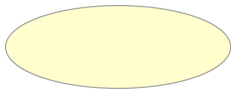


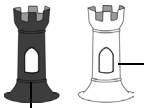
插图约定

下列图形构成了贯穿本书的插图所用的基本图像集：


通用 NetScreen 设备


虚拟路由选择域

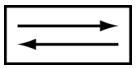

安全区段


安全区段接口
白色 = 受保护区段接口
(例如 : Trust 区段)
黑色 = 区段外接口
(例如 : Untrust 区段)


通道接口

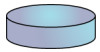

VPN 通道


路由器图标


交换机图标


包含单个子网的局域网 (LAN)
(例如 : 10.1.1.0/24)


互联网


动态 IP (DIP) 池


台式计算机


便携式计算机


通用网络设备
(例如： NAT 服务器，
接入集中器)


服务器

命名约定和字符类型

关于 ScreenOS 配置中定义的对象 (如地址、 admin 用户、 auth 服务器、 IKE 网关、虚拟系统、 VPN 通道和区段) 的名称， ScreenOS 采用下列约定。

- 如果名称字符串包含一个或多个空格，则必须将该整个名称字符串用双引号 (") 括起来；例如，**set address trust "local LAN" 10.1.1.0/24**。
- NetScreen 会删除一组双引号内文本的前导或结尾空格，例如，**" local LAN "** 将变为 **"local LAN"**。
- NetScreen 将多个连续的空格视为单个空格。
- 尽管许多 CLI 关键字不区分大小写，但名称字符串是区分大小写的。例如，**"local LAN"** 不同于 **"local lan"**。

ScreenOS 支持以下字符类型 :

- 单字节字符集 (SBCS) 和多字节字符集 (MBCS)。SBCS 的例子是 ASCII、欧洲语和希伯莱语。MBCS (也称为双字节字符集， DBCS) 的例子是中文、韩文和日文。

  注意 : *控制台连接只支持 SBCS。WebUI 对 SBCS 和 MBCS 都支持，取决于 Web 浏览器所支持的字符集。*

- 从 32 (十六进制 0x20) 到 255 (0xff) 的 ASCII 字符，双引号 (") 除外，该字符有特殊的意义，它用作包含空格的名称字符串的开始或结尾指示符。

NETSCREEN 文档

要获取任何 Juniper Networks NetScreen 产品的技术文档，请访问 www.juniper.net/techpubs/。

要获取技术支持，请使用 http://www.juniper.net/support/ 下的 Case Manager 链接打开支持个例，还可拨打电话 1-888-314-JTAC (美国国内) 或 1-408-745-9500 (美国以外的地区)。

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

A

词汇表

10BaseT: 最常用的以太网形式称为 10BaseT，它表示使用铜双绞线电缆时的最高传输速度为 10 Mbps。以太网是将计算机连接到局域网 (LAN) 的一种标准。电缆距离最长为 100 米 (325 英尺)，每段的设备数最多为 1，每个网络的设备数最多为 1024。另请参阅 *100BaseT* 和 *非屏蔽双绞线 (UTP)*。

100BaseT: 快速以太网的另一种说法，是将计算机连接到局域网 (LAN) 的一种已改进的标准。 100BaseT 以太网除了可以用最高速度 100 Mbps 传输数据外，其工作方式几乎与常规以太网一样。与较慢的同类标准 10BaseT 相比，它更昂贵、更不常用。另请参阅 *10BaseT*。

AS: 请参阅 *自治系统*。

AS 号 : 映射到 BGP 路由实例的本地自治系统的标识号。 ID 号可以是任何有效整数。

AS 路径访问列表 : 一种访问列表， BGP 路由实例用来允许或拒绝相邻路由实例发送到当前虚拟路由实例的数据包。

AS 路径属性类 : BGP 提供了四类路径属性 : Well-Known Discretionary、 Optional Transitive 和 Optional Non-Transitive。

AS 路径字符串 : 作为 AS 路径标识符的字符串。与 AS 路径访问列表 ID 一起配置。

Atomic 聚合 : BGP 路由器用来将本地系统选择了一个广义路由的信息通知到其它 BGP 路由器的对象。

安全参数索引 : (SPI) 是一个十六进制值，可对每个通道进行唯一标识。它还会告知 NetScreen 设备使用哪个密钥解密数据包。

安全副本 (SCP): 一种在远程客户端和 NetScreen 设备之间使用 SSH 协议传输文件的方法。 NetScreen 设备作为一个 SCP 服务器，接受来自远程主机上 SCP 客户端的连接。

安全联盟 : SA 是 VPN 参与者之间用于确保信道安全的有关方法和参数的单向协议。对于双向通信，必须至少有两个 SA，每个方向使用一个。在 “自动密钥 IKE” 协商期间， VPN 参与者会协商并同意 “阶段 1” 和 “阶段 2” 的 SA。另请参阅 *安全参数索引*。

安全区段 : 一个安全区段是一个或多个网络段的集合，这些网络段需要遵守按策略入站和出站信息流的规定。

安全外壳 (SSH): 一种允许设备管理员以安全方式远程管理设备的协议。您可以在 NetScreen 设备上运行 SSH 版本 1 或版本 2。

本地优先：为了使提供的信息比“多出口区分符”(MED) 值为数据包路径选择提供的信息更好， BGP 提供了一种称为 LOCAL_PREF 或本地优先值的属性。可配置 LOCAL_PREF 属性使其有更高的值，以便使接收自可以提供期望路径的路由器比接收自提供较低期望值的路径的路由器所提供的前缀更高。此值越高，则路由的优先程度越高。LOCAL_PREF 属性为度量值，实际中最常用于表达一组路径相对其它路径的优先级。

边界网关协议 (BGP): 一种自治系统间的路由协议。 BGP 路由器和自治系统交换互联网的路由信息。

不工作间隔：某一路由实例确定另一路由实例未运行之前所花费的时间。

策略：策略为防火墙提供初始保护机制，允许用户根据 IP 会话详细信息来确定通过它的信息流内容。可使用策略在安全区段对资源进行保护，使其免受来自其它区段 (区段间策略) 或来自区段内部 (区段内策略) 的攻击。还可使用策略来监控试图通过防火墙的信息流。

查询器：将 “互联网组管理协议” (IGMP) 消息发送到网络中的所有主机以请求组成员信息的路由器。通常每个网络中都会有一个查询器。

成员 AS: 包含在 BGP 联合体中的自治系统的名称。

重新分配：从使用其它路由协议的网络的另一部分将路由导入当前路由域的过程。发生此过程时，当前域必须转换来自其它协议的所有信息 (尤其是已知路由)。例如，如果当前位于 OSPF 网络，并且该网络连接到 BGP 网络，OSPF 域必须导入 BGP 网络的所有路由，以通知其所有设备有关如何到达 BGP 网络中的所有设备的信息。所有路由信息的接收过程称为路由重新分配。

重新分配列表：从使用其它协议的另一个路由域导入的当前路由域的路由列表。

传输控制协议 / 网际协议 (TCP/IP): TCP/IP 是一组通信协议，它支持局域网和广域网的对等连接功能。 (通信协议是一组规则，它允许使用不同操作系统的计算机彼此之间互相通信。) TCP/IP 可控制 “互联网” 上计算机之间的数据传输方式。

导出规则：当 NetScreen 设备上有两个或两个以上的虚拟路由器时，即可配置导出规则，在一个虚拟路由器上定义另一个虚拟路由器所接受的路由。另请参阅*导入规则*。

导入规则：当 NetScreen 设备上有两个或两个以上的虚拟路由器时，即可在一个虚拟路由器上配置导入规则，以定义允许从另一个虚拟路由器接收的路由。如果没有为虚拟路由器配置任何导入规则，将会接受导出到该虚拟路由器的所有路由。另请参阅*导出规则*。

等待时间：在 OSPF 中，开始进行 “最短路径优先” (SPF) 计算的实例之间的最大时间长度。在 BGP 中， BGP 发送方与其邻居之间消息传输的时间长度。

等值多通道：等值多通道可帮助实现到同一目标的二到四个路由间的负载均衡或者提高两个或更多目标间的有效带宽使用。启用时，NetScreen 设备将使用静态定义的路由或通过路由协议动态获知到同一目标的多个路由。NetScreen 设备以轮询方式分配等值路由。默认值 : disabled。

地址变换：一种在一个地址范围中的初始地址和不同范围中的特定已转换地址之间创建一对一映射的机制。

电路级代理：代理或代理服务器是一项技术，用于在 Web 服务器上高速缓存信息并作为某一 Web 客户端与该 Web 服务器之间的中介。它主要为用户存储最常用和最近已用过的万维网内容，目的是使访问更快速并且增强了服务器的安全性。这对于 ISP 而言比较常见，尤其是当它们链接到互联网的速度较慢时。在 Web 上，代理将首先尝试查找本地数据，如果未找到数据，则从数据长期驻留的远程服务器上获取数据。代理服务器还是允许通过防火墙直接访问互联网的机构。它们打开服务器上的套接字，允许通过该套接字与互联网进行通信。例如，如果计算机在受保护的网络内且要使用 Netscape 浏览 Web，则可在防火墙上设置代理服务器。可在计算机中将代理服务器配置为允许 HTTP 请求访问端口 80，然后将所有请求重新定向到适当位置。

动态路由：一种路由方法，适用于通过分析进入路由更新消息以调整到已更改的网络环境。如果该消息指示出网络已更改，路由软件会重新计算路由并发送新的路由更新消息。这些消息留置在网络中，以引导路由器重新运行其算法，并相应地更改其路由表。动态路由有两种常用形式，包括 “距离向量路由” 和 “链接状态路由”。

动态主机配置协议 (DHCP): 一种为网络主机自动分配 IP 地址的方法。根据特定的设备型号， NetScreen 设备可以分配动态 IP 地址给主机、动态获取分配的 IP 地址，也可以从 DHCP 服务器接收 DHCP 信息和将信息转递给主机。

端口地址转换 (PAT): 数据包中初始源端口号到随机指定的不同端口号的转换。

端口模式：某些 NetScreen 设备支持的功能。端口模式使您可以从设备上多组不同的端口、接口和地区绑定中选择一组。更改端口模式会删除设备上任何现有的配置，并要求系统重置。

端口映射：数据包中初始目的端口号到预定的不同端口号的转换。

对等方：请参阅 *邻接设备* 。

多出口区分符：BGP 属性，用于确定 “自治系统” 进入点的相对优先级。

ESP/AH: IP 级安全协议 (AH 和 ESP)，最初是由 Network Working Group 提出的，旨在建立 IP 安全机制和 IPSec。在此处概括地使用术语 IPSec 来指数据包、密钥和与这些协议相关的路由。“IP 认证报头 (AH)” 协议提供认证。“封装安全性协议 (ESP)” 既提供认证，又提供加密。

反向路径转发：组播路由器用于检查组播数据包有效性的方法。路由器在单播路由表中执行路由查询以检查在其上接收数据包的接口 (入口接口) 是否是必须用来将数据包发回发送方的同一接口。如果是，路由器将创建组播路由条目，并将数据包转发到下一跳跃路由器。如果不是，路由器将丢弃该数据包。

防病毒 (AV) 扫描：一种检测和封锁 “文件传输协议” (FTP)、“互联网消息访问协议” (IMAP)、“简单邮件传输协议” (SMTP)、“超文本传输协议” (HTTP) (包括 HTTP Web 邮件) 和 “邮局协议版本 3 (POP3)” 等信息流中的病毒的机制。 NetScreen 提供了内部防病毒扫描解决方案。

防火墙：是为信息流输入及输出保护并控制一个网络与另一个网络连接的设备。许多公司使用防火墙保护任何由网络连接的服务器，使其免受登录者的 (有意或无意的) 破坏。这种保护可以是一台装备安全措施的专用计算机，也可以是基于软件的保护。

访问列表：与指定路由进行比较的网络前缀的列表。如果路由和访问列表中定义的网络前缀匹配，则允许或拒绝该路由。

访问质询：认证用户通过 RADIUS 服务器成功 Telnet 登录所必需的一个附加条件。

非军事区段 (DMZ): 源自军事术语，是两个敌对方之间的禁战区。 DMZ 以太网将不同团体控制的网络和计算机连接在一起。它们可以是外部的，也可以是内部的。外部 DMZ 以太网通过路由器链接区域网络。

非屏蔽双绞线 (UTP): 也称为 10BaseT。是用于电话线的标准电缆。也可用于连接以太网。另请参阅 *10BaseT*。

负载均衡：负载均衡是到两个或多个处理器的映射 (或重新映射)，目的是提高并发计算的效率。

GBIC: “千兆位接口连接器” (GBIC) 是一种用于将某些 NetScreen 设备连接到光纤网络的接口模块卡。

公共组：公共组是 BGP 目标的组合。通过更新公共组，将用新属性自动更新其成员目标。

攻击对象：一些状态式签名和协议异常，它们被具有 “深入检查” 功能的 NetScreen 设备用以检测旨在损害网络上的主机的攻击。

共享分布树：一个组播分布树，其中源会将组播信息流传输到汇聚点 (RP)，然后汇聚点再将信息流向下游转发到分布树中的接收器。

广播网络：广播网络是一种支持许多路由器的网络，能够彼此直接通信。以太网即为广播网络的一个范例。

过滤，动态：一种可在 VPN 通道内使用的 IP 服务。过滤器是某些 NetScreen 设备控制从一个网络到另一个网络的信息流的一种方法。当 TCP/IP 将数据包发送到防火墙后，防火墙中的过滤功能会查看数据包中的报头信息，然后相应地进行发送。过滤器对诸如 IP 源地址或目标地址范围、 TCP 端口、 UDP、“互联网控制消息协议 (ICMP)”或 TCP 响应等标准起作用。另请参阅*通道*和*虚拟专用网 (VPN)*。

过滤列表：获准将数据包发送到当前路由域的一个 IP 地址列表。

Hello 间隔：“Hello 数据包”实例之间的时间长度。

Hello 数据包：是通告信息 (例如，它的存在与可用性) 的数据包，它将信息通告给生成数据包的路由器周围的网络。

互联网：也称为 “网络”。最初是由 “美国国防部”设计，其目的在于使用通信信号抵御核战争并且服务于美国在全球的军事机构。“互联网”最初被称作 ARPAnet。该系统由链接在一起的计算机网络构成，便于在全球范围内提供数据通信服务，例如，远程登录、文件传输、电子邮件及新闻组。“互联网”是连接现有计算机网络的一种方式，它极大扩展了每套参与系统的触及范围。

互联网控制信息协议 (ICMP): 有时，网关或目的主机使用 ICMP 与源主机通信，例如，报告一个数据报处理中出现的错误。 ICMP 作为更高级别的协议使用 IP 的基本支持，但是，它实际上也是 IP 的组成部分，因此必须由每个 IP 模块执行。 ICMP 消息在出现以下几种情况时被发送 : 例如，数据报无法到达其目的地，网关没有转发数据报的缓冲容量，以及网关可引导主机在较短的路由上发送信息流。“网际协议”的设计并非完全可靠。这些控制消息的目的是在通信环境中提供关于问题的反馈，而并非使 IP 更可靠。

互联网密钥交换 (IKE): 一种在不安全的媒体 (例如，互联网) 上进行加密和认证的密钥交换方法。

互联网组管理协议 (IGMP): 在主机和路由器间运行以传送组播组成员信息的协议。

回传接口：一种模拟 NetScreen 设备上物理接口的逻辑接口，但与物理接口不同的是，只要其所在的设备处于连接状态，该接口始终处于连接状态。您必须给回传接口分配 IP 地址，并将其绑定到安全区段。

汇聚点 (RP): 组播分布树的根部的路由器。组中的所有源将其数据包发送到 RP，然后 RP 将数据沿共享分布树向下发送到网络中的所有接收器。

会话启动协议 (SIP): SIP 是一种 IETF (互联网工程工作小组) 标准协议，用于在互联网上启动、修改和终止多媒体会话。这种会话可能包括会议、电话或多媒体，在网络环境中具有诸如即时消息和应用程序级灵活性等功能。

会话说明协议 (SDP): SDP 会话说明出现在多条 SIP 消息中，提供系统可用来加入多媒体会话的信息。 SDP 可能包括如 IP 地址、端口号、时间和日期等信息以及有关媒体流的信息。

IP 安全性 (IPSec): 由 “互联网工程工作小组” (IETF) 制定的安全标准。它是一个协议套件，提供您对安全通信所需要的一切 — 认证、完整性及机密性 — 甚至可以在更大型的网络中进行实际密钥交换。另请参阅 *DES-CBC* 和 *ESP/AH*。

IP 地址 : 通常， TCP/IP 网络上的每个节点有一个 IP 地址。如下表中的 IP 地址类及格式所示， IP 地址由网络编号部分和主机编号部分组成 :

类	节点数量	地址格式
A	> 32,768	nnn.hhh.hhh.hhh
B	256–32,768	nnn.nnn.hhh.hhh
C	< 256	nnn.nnn.nnn.hhh

此格式称为十进制点格式。“n” 表示网络编号的一位，“h” 表示主机编号的一位，例如， 128.11.2.30。如果您将数据发送到网络以外，例如，发送到 “互联网”，则需要从中央授权机构 (目前是 “网络信息中心”) 获得网络编号。另请参阅 *网络掩码* 和 *子网掩码*。

IP 跟踪 : 一种监视配置的 IP 地址以查看其是否响应 ping 或 ARP 请求的机制。您可以用 NSRP 配置 IP 跟踪，以确定设备或 VSD 组故障切换。也可以在设备接口上配置 IP 跟踪，以确定该接口是否处于工作中状态。

IP 网关 : 也称为路由器，网关是一个程序或一种专用设备，该设备将 IP 数据报从一个网络传输到另一个网络，直到抵达最终目标。

ISAKMP: “互联网安全协会和密钥管理协议” (ISAKMP) 为 “互联网” 密钥管理提供了一个框架，并且为安全属性的协商提供了具体的协议支持。此协议自身不建立会话密钥，但是，它可以配合多种会话协议建立协议使用，提供一个完整的 “互联网” 密钥管理解决方案。

基于源的路由 : 您可以在 NetScreen 设备上配置虚拟路由器，以根据数据包的源地址而非目的地址来转发信息流。

基于源接口的路由 (SIBR): SIBR 允许 NetScreen 设备基于源接口 (数据包从其到达 NetScreen 设备的接口) 转发信息流。

激活 : 两激活数据包之间的时间长度 (以秒为单位)，它可确保本地 BGP (边界网关协议) 路由器和邻接路由器间 TCP 连接成功。此值等于等待时间的三分之一。缺省值为 60 秒。

集群：BGP AS 中的一组路由器，其中一个路由器被设置为路由反射器，其它则为该反射器的客户端。该反射器负责将它从另一 AS 中的设备处获悉的路由和地址信息通知到客户端。

注意：*术语 “集群” 的另一含义与高可用性有关。请参阅 “NetScreen 冗余协议” (NSRP)。*

集群列表：数据包在通过 BGP 路由反射器集群时所记录的一个路径列表。

集线器：集线器是用于将计算机链接到一起的硬件设备 (通常在以太网连接上使用)。它用做公用布线点，以便信息能通过一个中央位置流动到网络上其它任何一台计算机。集线器在物理以太网层重复信号。它保持标准总线类型网络的行为 (例如，细电缆网)，但是位于星状中心的集线器会生成星状拓扑。此配置可实现集中的管理。

加密：加密是将数据变成只有预定接收方可读取的形式的过程。要解密消息，加密数据的接收方必须具有适当的解密密钥。在传统加密方案中，发送方和接收方使用相同的密钥加密和解密数据。公开密钥加密方案使用两种密钥 : 任何人都可以使用的公开密钥和只有创建者拥有的相应私有密钥。通过这种方法，任何人都可以发送用所有者的公开密钥加密的消息，但只有所有者才拥有解密必需的私有密钥。 DES (数据加密标准) 和 3DES (三重 DES) 是最流行的公开密钥加密方案中的两种方案。

静态路由：用户定义的路由，使得数据包以指定路径在源节点和目标节点之间移动。静态路由算法是网络管理员在开始路由之前建立的表映射。这些映射不会更改，除非网络管理员要这样做。使用静态路由的算法设计简单，并在网络信息流相对可预知以及网络设计相对简单的环境中运行良好。

只要不改变路由，软件就会记住静态路由。但是，通过对管理距离值进行合理指定，也可用动态路由信息覆盖静态路由。要做到这一点，必须确保静态路由的管理距离超过动态协议的管理距离。

局域网 (LAN): 任何将办公环境内的资源互联的网络技术，通常速度很快 (如以太网)。局域网是一种短距离网络，用于将一座建筑物内的一组计算机链接到一起。 10BaseT 以太网是最常用的局域网形式。一种称为集线器的硬件设备用做公用布线点，可通过网络将数据从一台机器发送到另一台。局域网的距离通常限制在 1,640 英尺 (500 米) 以内，可在较小的地理区域内提供低成本、高带宽的联网功能。

距离向量：依靠某一算法的路由策略，该算法通过使路由器偶而向所有直接连接的相邻路由器广播其路由表的整个副本而起作用。此更新信息将识别每个路由器知道的网络和这些网络彼此间的距离。该距离以跳越计数的方式测定，或以数据包在其源设备和试图到达的设备之间必须穿越的路由域数量测定。

聚合：将几个不同的路由组合在一起的过程，其中只有某一个路由通告自身身份。此项技术可使路由器的路由表最小化。

聚合器：根据网络掩码的值，将多个路由绑定到一个通用广义路由下的对象。

聚合状态：当某个路由器是绑定到一个地址的多个虚拟 BGP 路由实例之一时，则其即处于聚合状态。

开放式最短路径优先 (OSPF): 专用于在单一自治系统中运作的动态路由协议。

连接状态：当发自某一路由器的数据包到达另一路由器时，在源路由器和目的路由器之间会进行协商。协商将经过六种状态：空闲、连接、活动、开放发送、开放连接和确立。

联合：BGP AS 中的一个对象，是 AS 中路由实例的一个子集。通过将 BGP AS 中的设备组合成联合体，可减少 AS 中路由连接矩阵 (称为网格) 的复杂性。

链接状态：链接状态路由协议使用通常称为 “最短路径优先” (SPF) 的算法运作。与距离向量协议中依赖从直接连接的邻接路由器获得传播的信息不同，链接状态系统中的每台路由器都有网络的完整拓扑，并根据此拓扑计算 SPF 信息。

链接状态通告：启用 OSPF 路由器使设备、网络和路由信息可用于链接状态数据库的传送。每台路由器会检索来自网络中其它路由器发送的 LSA 中的信息，以构建整个互联网图，单个路由实例可从中提取路径信息以便在其路由表中使用。

邻接设备：要开始配置 BGP 网络，首先需要在当前设备与对等设备之间建立连接，相邻设备称为 *邻接设备*或 *对等方*。虽然最初此对等设备可能看似不需要的信息，但实际上它对于 BGP 的工作方式非常重要。与 RIP 或 OSPF 不同的是，要使 BGP 工作，必须配置当前路由器及其邻接路由器这两台设备。虽然这需要更多工作，却能使联网的规模更大，因为 BGP 不使用对于内部建网标准所固有的受限通告技术。

有两种类型的 BGP 邻接设备，**内部邻接设备**位于同一个自治系统中，而**外部邻接设备**位于不同的自治系统中。两邻接设备之间需建立可靠连接，这可通过在两者之间建立 TCP 连接实现。在真正建立连接之前，在两预期邻接设备之间会发生握手过程，这包括多个阶段或 *状态*。请参阅 *连接状态*。

邻居：当两个路由器可以相互交换路由信息时，它们即被视为已构建了邻居。点对点网络仅有两个路由器，因此这些路由器会自动形成邻居。但点对多点网络是一系列的多个点对点网络。当这种更复杂的网络方案中的路由器组成对时，它们即被视为彼此相邻。

路由表：虚拟路由器内存中的一个列表，包含某路由器当前正在向其传送数据包的所有已连接的网络和远程网络的实时视图。

路由重新分配：从一个虚拟路由器到另一个虚拟路由器的路由规则导出操作。

路由反射器：一个路由器，它的 BGP 配置允许在 “内部 BGP” (IBGP) 邻接路由器或同一 BGP AS 内部的邻接路由器之间进行路由的重新通告。路由反射器客户机是使用路由反射器将其路由重新通告到整个 AS 的设备。它还依赖该路由反射器了解网络其余部分的路由信息。

路由器：一种硬件或虚拟 (在 NetScreen 环境中) 设备，可将数据分配到本地路由域内部或外部的其它所有路由器和接收点。路由器还用作过滤器，只允许经过授权的设备将数据传送到本地网络中，从而保证私有信息的安全。除了支持这些连接外，路由器还可处理错误、保存网络使用情况统计数据并且处理安全问题。

路由映射：路由映射和 BGP 配合使用，可控制并修改路由信息，还可定义在路由域间重新分配路由的条件。路由映射包含一个路由映射条目的列表，每个条目包含一个序列号、一个匹配项和一个设置值。路由映射条目按递增序列号的顺序计算。某条目返回匹配条件后，不会再进一步计算路由映射。找到匹配项后，路由映射会执行对该条目的许可或拒绝操作。如果路由映射条目不是一个匹配项，则会为匹配标准进行下一条目的计算。

路由文件布置和分配程序衰减：BGP 提供一项技术，可以阻塞靠近源路由的某处的通告，直到路由变得稳定为止。此方法称为*分配程序衰减*。路由文件布置和分配程序衰减允许在临近发生不稳定区域的 AS 边界路由器处存在路由不稳定。在路由拓扑增长时，对不必要的传播进行限制的效果是维持合理的路由更改收敛时间。

路由信息协议 (RIP): 用在中等大小自治系统中的动态路由协议。

MD5: “信息整理” (版本) 5 是可以通过任意长度的消息生成 128 位消息摘要 (或散列) 的算法。生成的散列 (如同输入的 “指印”) 用于验证确认性。

MED 比较： “多出口区分符” (MED) 属性用于确定到达位于当前 “自治系统” (AS) 内部或之后的特定前缀的理想链接。 MED 包含一个度量值，该值表示进入该 AS 的优先程度。配置某链路的 MED 值，使其低于其它链路的 MED 值，即可建立该链路对其它链路的优先级。 MED 值越低，该链接的优先级就越高。工作方式为：由一个 AS 设置 MED 值，其它 AS 使用该值确定要选择的路径。

Metric: 当存在多个路由指向同一目的网络且优先级值相同时，虚拟路由器会使用一个路由来选择活动路由，度量就是与该路由相关的值。已连接路由的度量值始终为 0。静态路由的缺省度量值为 1，但可以在定义静态路由时指定其它值。

媒体访问控制 (MAC) 地址：用于唯一标识网络接口卡的地址，如以太网适配器。对于以太网， MAC 地址是由 IEEE 分配的 6 个八位长字节地址。在局域网或其它网络中， MAC 地址是计算机的唯一硬件编号 (在以太网的局域网中，它与以太网地址相同。)。从计算机连接到 “互联网” (或 “互联网” 协议认为是互联网的主机) 时，通信表会将您的 IP 地址与计算机在局域网上的物理 (MAC) 地址相关联。 MAC 地址由远程通信协议的 “数据链路控制 (DLC)” 层中的 “媒体访问控制” 子层使用。用于每种类型的物理设备都有不同的 MAC 子层。

密钥管理：依靠签署和 / 或加密的私有密钥的形式使用秘密信息，是保护信息完整性和私密性的唯一合理途径。对这些秘密信息的管理和处理通常称为 “密钥管理”。包括的活动有密钥的选择、交换、存储、证书、到期、撤消、更改和传输。管理信息安全系统的大部分操作在密钥管理中执行。

目标网络地址转换 (NAT-Dst): 数据包包头中初始目的 IP 地址到不同目的地址的转换。NetScreen 支持一个或多个初始目的 IP 地址转换成一个 IP 地址 (“一对一” 或 “多对一” 关系)。 NetScreen 设备还支持使用地址变换将一个范围的 IP 地址转换到另一个范围 (“多对多” 关系)。

当 NetScreen 设备不使用地址变换而执行 NAT-dst 时，还支持将目的端口号映射到不同的预定端口号。当 NetScreen 设备使用地址变换执行 NAT-dst 时，则无法执行端口映射。

NAT 穿透 (NAT-T): 一种通过添加一层 UDP 封装允许 IPSec 信息流沿着 VPN 的数据路径通过 NAT 设备的方法。该方法先在 “阶段 1” IKE 交换期间提供检测 NAT 设备的方式，然后在 “阶段 2” IKE 协商完成后提供穿越它们的方式。

NAT-Dst: 请参阅 *目标网络地址转换 (NAT-Dst)*。

NAT-Src: 请参阅 *网络地址转换 (NAT)*。

NetScreen 冗余协议 (NSRP): 一种专有协议，可提供配置和执行对象 (RTO) 冗余和高可用性 (HA) 集群中的 NetScreen 设备的设备故障切换机制。

内部网：该名称从 “互联网” 这个词衍生而来，它是一个类似于 Web 的访问受限制的网络，但它不在 Web 上。通常，内部网由一个公司所有并且进行管理，可以使公司与它的雇员分享资源，而不会让访问 “互联网” 的每个人获得机密信息。

前缀：代表路由的一个 IP 地址。

桥接器：一种根据数据链层信息在网络段间转发信息流的设备。这些网络段共享通用网络层的地址空间。

区段：区段可以是网络空间中应用了安全措施的部分 (安全区段)、绑定了 VPN 通道接口的逻辑部分 (通道区段)，或者是执行特定功能的物理或逻辑实体 (功能区段)。

区域：OSPF 路由协议中最基本的排序方法。 OSPF 区域将互联网络划分成更小、更易于管理的组件。此项技术可减少每个路由器必须存储和保持的有关所有其它路由器的信息量。当该区域中的某个路由器需要区域内部或外部另一个设备的信息时，它会与存储该信息的特定路由器联系。该路由器即被称为 “区域边界路由器” (ABR)，它包含所有设备的基本信息。此外， ABR 区域边界路由器过滤所有进入区域的信息，以避免引起区域中其它路由器因收到他们不需要的信息而停顿。

区域边界路由器：一种在 “区域 0”中至少有一个接口并在另一个区域中至少有一个接口的路由器。

区域范围：由下限和上限定义的 IP 地址序列，指示出某个区域内设备的一系列地址。

缺省路由：“应用最广”的路由表条目，定义没有在路由表中明确定义的目标网络信息流的转发。缺省路由的目标网络用网络地址 0.0.0.0/0 表示。

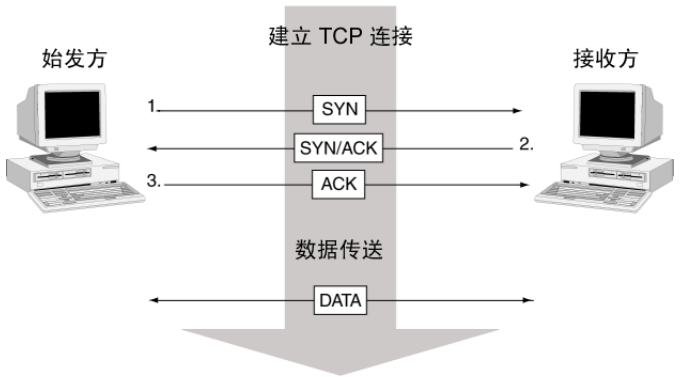
RJ-45: RJ-45 连接器与标准电话连接器类似，但宽度是其两倍 (使用八芯线)，并且使用多条线；路将计算机连接到局域网 (LAN) 或电话机。

认证报头 (AH): 请参阅 *ESP/AH*。

SHA-1: “安全散列算法 1”，一种用于从任意长度的消息生成 160 位散列的算法。(通常认为它比 MD5 更安全，因为它生成的散列更大。)

三方握手：一个建立的具有三方数据包交换的 TCP 连接，即通常所说的三方握手。程序如下所述：

1. 发起方发送 SYN (同步 / 开始) 数据包。
2. 接收方使用 SYN/ACK (同步 / 确认) 数据包回复。
3. 发起方使用 ACK (确认) 数据包响应。
4. 此时，已经建立该连接的两个端点，可以开始数据传输。



深入检查：一种用于过滤 NetScreen 防火墙所允许的信息流的机制。深入检查第 3、4 层数据包包头和第 7 层内容和协议特性，以努力检测和防止可能出现的任何攻击或异常行为。

实时传输控制协议 (RTCP): RTCP 提供有关会话成员和通信质量的信息。它通过将时戳和实时时钟相关联来同步媒体流。

实时传输协议 (RTP): RTP 用于通过分配时戳和序列号给数据包包头来按时间顺序接收数据包。每个 RTP 会话都有对应的 RTCP 会话 (请参阅 **RTCP**)。

数据加密标准 (DES): 由美国标准技术研究所 (NIST) 开发的一种 40 位和 56 位加密算法。DES 最初是由 IBM 开发的一种数据块加密方法。后来，经过美国政府认证用于传输任何非绝密类的数据。 DES 使用的是私有密钥加密算法。密钥由 64 位数据组成，这些数据经转换后与要发送消息的前 64 位组合。要采用加密，可通过使用由 16 个步骤组成的复杂过程将消息分解为 64 位的数据块，以便每个数据块可与密钥组合。虽然 DES 的保密性比较低，并仅有一次迭代，但是，如果使用稍稍不同的密钥对其进行重复，就可获得极佳的安全性能。

数据加密标准 - 密码字组链接 (DES-CBC): 直到最近，三重 DES (3DES) 最重要的用途才变为单一 DES 密钥加密，当所考虑的数据块密码实际上源自多重加密的结果时，确实没有必要考虑有人会如何执行各种数据块密码模式。但是，当 DES 接近其有效寿命期时，会更多地考虑使用日益广泛的三重 DES。特别是执行三重 DES 的 CBC 模式时，有两种显著的方法。在 CBC 模式中使用单一 DES 时，加密前，密文与明文不进行单独的 “或” 操作。然而在使用三重 DES 时，我们可能在从密文到明文的所有三项 DES 操作中使用反馈，这称为外部 CBC。或者，我们可能在各单个加密组件中运行反馈，进而达到三重 (DES-CBC) 的效果。因为存在解密者根本看不到的内部反馈，所以这称为内部 CBC。在性能方面，使用内部 CBC 选项可能有几项优点，但经过调查，使用外部 CBC 实际上更安全。外部 CBC 是在 CBC 模式中使用三重 DES 的推荐方法。

Trust 区段 : 两个 NetScreen 区段中的一个，可以确保数据包不被当前 NetScreen 域外部的设备看到。

通道 : 一种数据封装方法。使用 VPN 通道，专业移动设备用户会拨入当地的 “互联网服务提供商” 的 “出现点” (POP) 而不会直接拨入其企业网络。这意味着无论专业移动设备用户位于何处，只需花费本地通话费用，就能拨入支持 VPN 通道技术的本地 “互联网服务提供商”，并获得对其企业网络的访问权。当远程用户使用支持 VPN 通道的 “互联网服务提供商” 拨入其企业网络时，远程用户以及其组织都知道它是安全连接。所有的远程拨入用户均需经过 “互联网服务提供商” 站点的验证服务器进行验证，然后经过其企业网络的另一验证服务器再次验证。这意味着只有经过授权的远程用户才能访问其企业网络，并且只能访问授权其访问的主机。

通道接口 : 通道接口是开口或入口，发送到或接收自 VPN 通道的信息流均要经过它。可对通道接口进行编号 (即指定一个 IP 地址)，也可以不进行编号。编号后的通道接口可位于通道区段或安全区段。无编号的通道接口只能位于至少包含一个安全区段接口的安全区段。无编号的通道接口借用安全区段接口的 IP 地址。

通道区段 : 通道区是安装有一个或多个通道接口的逻辑段。通道区段与安全区段相关联，后者充当前者的承载方。

通告：路由器用来向网络中的其它设备通告自身身份，并传输基本信息 (包括 IP 地址、网络掩码和其它数据) 的一种方法。

通用路由封装 (GRE): 在 IPv4 单点数据包中封装任何类型数据包的协议。有关 GRE 的其它信息，请参阅 *RFC 1701, Generic Routing Encapsulation (GRE*)。

统一资源定位器 (URL): 实现用电子方式指定可用资源位置的标准方法。也指位置或地址， URL 指定文件在服务器上的位置。常规 URL 语法为 protocol://address。例如， http://www.netscreen.com/support/manuals.html 指定协议是 HTTP，地址是 www.netscreen.com/support/manuals.html。

Untrust 区段：使当前 NetScreen 域之外的设备能看见数据包的两个 NetScreen 区段之一。

WebTrends: NetIQ 提供的产品，可用于根据 NetScreen 设备创建的日志创建自定义报告。当使用 WebTrends 时，可用图形格式显示所需的信息。

Windows 互联网命名服务 (WINS): WINS 是一项将 IP 地址映射到基于 Windows NT 服务器网络的 NetBIOS 计算机名上的服务。 WINS 服务器将 Windows 网络环境下使用的 NetBIOS 名称映射到基于 IP 的网络中使用的 IP 地址上。

外部网：两个或几个内部网的连接。内部网是一种内部 Web 网络，允许某公司内部的用户进行通信和交换信息。外部网将虚拟空间和另一公司的内部网连接起来，从而允许这两个 (或几个) 公司在其自己的虚拟空间共享资源并通过互联网进行通信。此项技术极大地增强了公司间的相互沟通。

外部相邻路由器：两个不同的自治系统中的两个对等 BGP 路由器。

网关：也称为路由器，网关是一个程序或一种专用设备，该设备将 IP 数据报从一个网络传输到另一个网络，直到抵达最终目标。

网际协议 (IP): 一种 “互联网”标准协议，该协议定义了称为数据报的数据基本单位。数据报用在无连接、最费力的传输系统中。“网际协议”定义信息如何在 “互联网”上的系统之间传送。

网络层可达到性信息：每个 AS 都有一个路由方案，该方案会指出通过它可到达的目的地。此路由方案称为 “网络层可达到性信息”(NLRI) 对象。BGP 路由器定期生成并接收 NLRI 更新信息。各 NLRI 更新信息均包含可达到性信息包可通过的 AS 列表信息。NLRI 更新所说明的通用值包括: 网络编号、该信息所通过的 AS 列表以及其它路径属性列表。

网络地址转换 (NAT): 数据包包头中源 IP 地址到不同 IP 地址的转换。转换的源 IP 地址可能来自动态 IP (DIP) 地址池，或者来自出口接口的 IP 地址。当 NetScreen 设备从 DIP 池提取地址时，可以动态提取地址或提取明确的地址。如果是前者，它会从 DIP 池中随机提取地址，并将初始源 IP 地址转换为随机选择的地址。如果是后者，它将使用地址变换将源 IP 地址转换为地址池中的预定 IP 地址。当 NetScreen 设备使用出口接口的 IP 地址时，会将所有初始源 IP 地址转换为出口接口的地址。

当转换的地址来自使用地址变换的 DIP 池时，将无法执行源端口地址转换。当转换的地址来自不使用地址变换的 DIP 池时，端口转换是可选的。当转换的地址来自出口接口时，端口转换是必需的。

注意：为了与目标网络地址转换 (NAT-dst) 区分， NAT 也称为 NAT-src。

网络掩码：一个网络掩码可指出 IP 地址中指示网络标识的部分以及指示主机标识的部分。例如， IP 地址和网络掩码 10.20.30.1 255.255.255.0 (或 10.20.30.1/24) 是指 10.20.30.0 子网中的所有主机。 IP 地址和网络掩码 10.20.30.1 255.255.255.255 (或 10.20.30.1/32) 是指一台单独主机。另请参阅 *IP 地址*和 *子网掩码*。

无级路由：无论网络大小或类别如何，均支持域间路由。网络地址分为三类 (但在 BGP 中，这些是透明的)，使网络具有更大的灵活性。

XAuth: 一种协议，包括两个部分：远程 VPN 用户认证 (用户名加密码) 以及 TCP/IP 地址分配 (IP 地址、网络掩码、DNS 服务器与 WINS 服务器分配)。

系统日志：一种允许设备发送日志消息给运行系统日志 daemon (系统日志服务器) 的主机的协议。系统日志服务器然后会收集并在本机上存储这些日志消息。

下一跳跃：路由表中接收转发的目标网络信息流的 IP 地址。下一跳跃也可以是同一台 NetScreen 设备中的另一个虚拟路由器。

协议无关组播 (PIM): 在路由器间运行的组播路由协议，用于将组播信息流转发到整个网络中的组播组成员。“PIM 密集模式” (PIM-DM) 在整个网络中大量发送组播信息流，然后对不希望接收组播信息流的接收器的路由进行裁剪。“PIM 稀疏模式” (PIM-SM) 仅将组播信息流转发到请求该信息流的接收器。

虚拟 IP 地址：一个 VIP 地址将在一个 IP 地址上收到的信息流映射到基于数据包包头中的目标端口号的另一地址。

虚拟安全接口 (VSI): 第 3 层中的逻辑实体，与 VSD 组中多个第 2 层物理接口相链接。 VSI 绑定到一个设备的物理接口上，该设备充当 VSD 组的主设备。如果存在故障切换，并且成为新的主设备，则 VSI 转移到 VSD 组中另一设备的物理接口上。

虚拟安全设备 (VSD): 是由一组物理 NetScreen 设备组成的单独逻辑设备。

虚拟局域网 (VLAN): 组成单独广播域的设备的逻辑 (而非物理) 分组。通过在传输数据的帧报头中使用标记 (而不是通过在物理子网中的位置) 来识别 VLAN 成员。在 IEEE 802.1Q 标准中介绍了 VLAN。

虚拟链接 : 从远程 OSPF 区域到中枢区域的逻辑路径。

虚拟路由器 : 虚拟路由器是执行路由功能的 ScreenOS 组件。在缺省情况下， NetScreen 设备支持两个虚拟路由器 : 不可信虚拟路由器和可信虚拟路由器。

虚拟适配器 : 由 NetScreen 设备分配给远程 XAuth 用户，以便在 VPN 连接中使用的 TCP/IP 设置 (IP 地址、DNS 服务器地址和 WINS 服务器地址)。

虚拟系统 : 虚拟系统 (vsys) 是主系统的一部分，作为一个单独实体显示给用户。虚拟系统彼此独立地驻留在同一 NetScreen 设备中。每个虚拟系统都可由其自身的管理员进行管理。

虚拟专用网 (VPN): VPN 是一种简单、具有成本效益和安全的方法，用于企业为通信设备和专业移动设备提供对其企业网或另一 “互联网服务提供商” (ISP) 的本地拨号访问。通过 “互联网” 的安全秘密连接比专线连接更具有成本效益。由于通道、筛选、加密及 IPSec (互联网协议安全性) 等技术和标准的存在，令实现 VPN 成为可能。

验证 : 验证可确保将数字数据传输到预定的接收方。验证还可向接收方确保信息及其来源 (来自何处) 的完整性。最简单的验证形式要求有获准访问特定帐户的用户名和密码。验证协议可以根据秘密的密钥加密，例如 DES 或 3DES，也可以根据使用数字签名的公开密钥系统进行加密。

以太网 : 一种局域网技术，由施乐公司的 Palo Alto Research Center 发明。以太网是一种使用 CSMA/CD 技术的最佳传输系统。以太网可通过多种电缆方案互连，包括粗同轴电缆、细同轴电缆、双绞线和光纤电缆。以太网是将计算机连接到局域网 (LAN) 的一种标准。最常用的以太网形式称为 10BaseT，它表示使用铜双绞线电缆时的最高传输速度为 10 Mbps。

以太网点对点协议 (PPPoE): 允许一个站点中的多个用户共享相同的数字用户线、电缆调制解调器或互联网无线连接。您可以在某些 NetScreen 设备的任一或所有接口上配置 PPPoE 客户端实例，包括用户名和密码。

应用程序层网关 (ALG): 在 NetScreen 设备上，ALG 是一个设计为管理特定协议 (如 SIP 或 FTP) 的软件组件。ALG 截取和分析指定的信息流、分配资源和定义动态策略，以允许该信息流安全通过 NetScreen 设备。

映射 IP 地址 : MIP 是从一个 IP 地址到另一个 IP 地址发出的信息流的直接一对一映射。

用户数据报协议 (UDP): TCP/IP 协议套件中的一个协议，“用户数据报协议”或 UDP 允许应用程序将数据报发送到远程机器上的其它应用程序中。 UDP 协议主要在不保证传输和副本检测的位置提供不可靠和无连接数据报服务。它不使用应答，也不控制到达顺序。

优先级：当存在多个路由指向同一目的网络时，虚拟路由器会使用一个路由来选择活动路由，优等级就是与该路由相关的值。优先级值由协议或路由的来源决定。路由的优先级值越低，越有可能被选择为活动路由。

执行对象 (RTO): 正常操作时在内存中动态创建的代码对象。 RTO 的示例有会话表条目、 ARP 高速缓存条目、证书、 DHCP 租用和 “IPSec 阶段 2”安全联盟 (SAs) 等。

中继端口：中继端口允许交换机通过单个物理端口捆绑来自多个 VLAN 的信息流，并按数据包的帧报头中的 VLAN 标识符 (VID) 对数据包进行排序。

主动调整时间：一种在会话表中的会话数超过指定的高位临界值时加速超时过程的机制。当表中的会话数下降到指定的低位临界值之下时，超时过程恢复正常。

子接口：一个子接口是一个物理接口的逻辑分支，它从自己来源的物理接口借用所需的带宽。子接口是对物理上现有端口的某接口同一功能的抽象，并且通过 802.1Q VLAN 标记方法进行识别。

子网掩码：在较大规模的网络中，可使用子网掩码定义子网。例如，对于 B 类网络，如果子网掩码为 255.255.255.0，则指定小数点格式的前两部分为网络 ID，而第三部分为子网 ID。第四部分为主机 ID。如果不想在 B 类网络中使用子网，则应使用子网掩码 255.255.0.0。一个网络可划分为一个和多个物理网络，以构成主网络的一个子网。子网掩码是 IP 地址中用于代表网络内的子网的部分。使用子网掩码可允许使用通常不可用的网络地址空间，并可确保网络信息流不发送到整个网络中 (除非希望这样做)。另请参阅 *IP 地址* 和 *网络掩码*。

自治系统 (AS): AS 是一组与其余网络段分开并由单一技术管理的路由器。此路由器组使用一种内部网关协议 (IGP) 或几种 IGP 以及通用度量法在组内发送数据包。该组还使用外部网关协议 (EGP) 向其它 AS 发送数据包。每个 AS 均有一项路由计划，指示出通过它可到达的目标。此项计划即称为 “网络层可达性信息 (NLRI)”对象。 BGP 路由器定期生成并接收 NLRI 更新信息。

自治系统边界路由器：一种路由器，将某个运行一种路由协议的 AS 连接到运行不同协议的另一个 AS。

自治系统路径：当前传输过程中，路由器更新信息已到达的所有自治系统的一个列表。

组播策略：组播策略允许组播控制信息流 [如 “互联网组管理协议” (IGMP) 或 “协议无关组播” (PIM) 消息] 通过 NetScreen 设备。

组播路由：用于将多媒体流传送到一组接收器的路由方法。启用了组播的路由器仅将组播信息流传输到希望接收该信息流的主机。主机必须指明要接收组播数据，而且必须加入组播组才能接收该类数据。

最短路径树 (SPT): 一个组播分布树，其中源位于树的根部并且会将组播数据向下游转发到每个接收器。也称为源特定树。

索引

符号

“消息整理”版本 5
    请参阅 MD5

数字

10BaseT, 已定义 **1**-A-I
100BaseT, 已定义 **1**-A-I
3DES **5**-8

A

ActiveX 控件，封锁 **4**-201
admin 用户 **8**-3– **8**-4
    auth 过程 **8**-4
    超时 **8**-22
    服务器支持 **8**-16
    来自 RADIUS 的权限 **8**-3
AES (高级加密标准) **5**-8
Aggressive 模式 **5**-12
AH **5**-3, **5**-7
AIM **4**-148
ALG **2**-199, **4**-78
    定义 **1**-A-XVI
    对于定制服务 **2**-303
    MS RPC **2**-159
    RTSP **2**-164
    SIP **2**-195
    SIP NAT **2**-207
    Sun RPC **2**-156
America Online Instant Messaging
    请参阅 AIM
ARP **2**-107, **10**-57, **10**-122
    广播 **10**-19
    路径监控 **10**-159
    入口 IP 地址 **2**-110
AS 号 **1**-A-I
AS 路径访问列表 **1**-A-I
AS 路径属性类 **1**-A-I
AS 路径字符串 **1**-A-I
atomic 聚合 **1**-A-I
AV 服务 **2**-440, **2**-441
auth 服务器 **8**-16
    备份服务器 **8**-21
    超时 **8**-21
    地址 **8**-21
    定义 **8**-32– **8**-40
    对象名 **8**-21
    对象属性 **8**-21
    多种用户类型 **8**-17
    功能支持 **8**-16
    ID 号 **8**-21
    LDAP **8**-30– **8**-31
    LDAP，定义 **8**-37
    类型 **8**-21
    缺省 **8**-39
    RADIUS **8**-23– **8**-25
    RADIUS，定义 **8**-32
    RADIUS，用户类型支持 **8**-24
    认证过程 **8**-20
    SecurID **8**-28– **8**-29
    SecurID，定义 **8**-35
    外部 **8**-20
    XAuth 查询 **8**-82
    用户类型支持 **8**-16
    最大数量 **8**-17
auth 用户 **8**-41– **8**-74
    策略前认证 **2**-307, **8**-43
    策略中 **8**-42
    超时 **8**-21
    服务器支持 **8**-16
    认证点 **8**-2
    WebAuth **2**-307, **8**-43
    WebAuth (本地用户组) **8**-63
    WebAuth (外部用户组) **8**-66
    WebAuth + SSL (外部用户组) **8**-70
    运行时 (本地用户) **8**-46
    运行时 (本地用户组) **8**-49
    运行时 (外部用户) **8**-52
    运行时 (外部用户组) **8**-55
    运行时认证 **2**-306, **8**-42
    运行时认证过程 **2**-306, **8**-42
    组 **8**-41, **8**-45
安全 IP 选项 **4**-13
安全复制
    请参阅 SCP
安全联盟
    请参阅 SA
安全联盟 (SA) **3**-134
安全区段 **1**-A-I, **2**-2
    global **2**-2
    接口 **2**-3, **2**-53
    目标区段确定 **2**-13
    *请参阅*区段
    物理接口 **2**-53
    预定义的 **2**-2
    源区段确定 **2**-13
    子接口 **2**-53
安全散列算法 1
    请参阅 SHA-1
安全套接字层
    请参阅 SSL
安全外壳
    请参阅 SSH
按路径开销的负载均衡 **6**-50, **6**-86
按需电路
    OSPF **6**-101
    RIP **6**-143

B

bandwidth **2**-310
    guaranteed **2**-310
    maximum **2**-310
BGP
    AS 路径访问列表 **6**-174
    安全配置 **6**-170
    参数 **6**-172
    重新分配路由 **6**-173
    带条件的路由通告 **6**-177
    定义 **1**-A-II
    负载均衡 **6**-50
    公共组 **6**-186
    规则表达式 **6**-174
    过滤路由 **6**-188

聚合路由的属性 **6**-192
聚合路由中的 AS 路径 **6**-190
聚合路由中的 AS-Set **6**-187
拒绝缺省路由 **6**-171
联合 **6**-183
邻居认证 **6**-170
路径属性 **6**-157
路由反射 **6**-180
路由聚合 **6**-187
内部 BGP **6**-158
配置步骤 **6**-159
配置对等方 **6**-163
配置对等方组 **6**-163
设置路由权重 **6**-178
设置路由属性 **6**-179
添加路由 **6**-176
外部 BGP **6**-158
消息类型 **6**-157
协议概述 **6**-156
验证配置 **6**-168
在 VR 中创建实例 **6**-160
在 VR 中启用 **6**-160
在接口上启用 **6**-162
bulk-CLI **2**-436
bypass-auth **8**-82
帮助文件 **3**-4
报警
电子邮件警示 **3**-92
临界值 **2**-309, **3**-92
流量 **3**-92– **3**-96
被遮盖的策略 **2**-338
本地数据库 **8**-18– **8**-19
超时 **8**-19
IKE 用户 **8**-76
支持的用户类型 **8**-18
本地优先 **1**-A-II
本地证书 **5**-30
比特流 **3**-131
编辑
策略 **2**-337
地址组 **2**-145
区段 **2**-36
标题
定制 **8**-14
二级 **8**-14
不工作间隔 **1**-A-II

C

CA 证书 **5**-26, **5**-30
CHAP **5**-305, **5**-308, **8**-97
CLI **3**-13, **3**-37, **3**-38
delete crypto auth-key **2**-428
set arp always-on-dest **2**-95, **2**-101, **10**-57
set vip multi-port **7**-116
约定 **1**-xxxv, **2**-viii, **3**-vi, **4**-vi, **5**-vi, **6**-viii, **7**-iv, **8**-iv, **9**-iv, **10**-iv
common name **8**-31
CompactFlash **3**-74
CRL (证书撤消列表) **5**-28, **5**-44
加载 **5**-28
操作系统 **3**-13
策略 **2**-3
安全区段 **2**-301
报警 **2**-309
必要元素 **2**-295
策略环境 **2**-331
策略验证 **2**-338
策略组列表 **2**-298
查询顺序 **2**-298
重新排序 **2**-339
DIP 组 **2**-286
地址 **2**-301
地址排除 **2**-333
地址组 **2**-301
定位在顶部 **2**-304, **2**-339
定义 **1**-A-II
丢弃 **2**-302
动作 **2**-302
服务 **2**-301
服务簿 **2**-147
服务于 **2**-147
服务组 **2**-263
根系统 **2**-299
更改 **2**-337
功能 **2**-293
管理 **2**-312
管理带宽 **2**-342
HA 会话备份 **2**-308
核心部分 **4**-24, **4**-135
环境 **4**-136
ID **2**-301
计数 **2**-309
禁用 **2**-337
拒绝 **2**-302
L2TP **2**-304
L2TP 通道 **2**-304
类型 **2**-296– **2**-297
每个组件含多个条目 **2**-332
名称 **2**-303
NAT-dst **2**-305
NAT-src **2**-305
内部规则 **2**-299
启用 **2**-337
区段间 **2**-296, **2**-314, **2**-315, **2**-320
区段内部 **2**-297, **2**-314, **2**-327
全局 **2**-297, **2**-314, **2**-330
认证 **2**-306
深入检查 **2**-304
时间表 **2**-309
双向 VPN **2**-303, **2**-313, **5**-174
顺序 **2**-339
通道 **2**-302
图标 **2**-312
URL 过滤 **4**-126
VPN **2**-303
VPN 拔号用户组 **2**-301
位置 **2**-314
信息流记录 **2**-309
信息流整形 **2**-310
虚拟系统 **2**-299
移除 **2**-340
应用 **2**-303
允许 **2**-302
遮盖 **2**-338
组播 **6**-202
最大限制 **2**-143
插图
约定 **1**-xxxviii, **2**-xi, **3**-ix, **4**-ix, **5**-ix, **6**-xi, **7**-vii, **8**-vii, **9**-vii, **10**-vii
差异服务 **2**-310
超额计费攻击
解决方案 **4**-222
说明 **4**-220
超额计费攻击防护
配置 **4**-224
超时
admin 用户 **8**-22
auth 用户 **8**-21

超文本传输协议
请参阅 HTTP
重定密钥选项，VPN 监控 **5**-356
重启 **2**-436
重启超时值 **2**-436
重新分配 **1**-A-II
重新分配列表 **1**-A-II
重置为出厂缺省值 **3**-55
传送模式 **5**-4，**5**-305，**5**-311，**5**-320
串行电缆 **3**-25
串行接口 **10**-103
故障切换 **10**-108
ISP 配置 **10**-106
调制解调器配置 **10**-104
串行接口的 ISP 配置 **10**-106
串行接口的调制解调器配置 **10**-104
创建
地址组 **2**-144
服务组 **2**-264
MIP 地址 **7**-92
区段 **2**-35
词典文件 **8**-3
存取策略
请参阅 策略

D

DDoS **4**-39
DES **5**-8
已定义 **1**-A-XII
DES-CBC，已定义 **1**-A-XIII
DHCP **2**-127，**2**-133，**2**-393
定义 **1**-A-III
服务器 **2**-370
HA **2**-379
客户端 **2**-370
中继代理 **2**-370
DI 服务 **2**-440，**2**-441，**2**-442
Diffie-Hellman 交换 **5**-13
Diffie-Hellman 组 **5**-13，**5**-65，**5**-68，**5**-74，**5**-77
DiffServ
请参阅 DS 码点标记
DIP **2**-131，**2**-267– **2**-270，**3**-134
池 **2**-305
固定端口 **2**-269
PAT **2**-268
修改 DIP 池 **2**-270
组 **2**-285– **2**-288
DIP 池
大小 **7**-16
地址注意事项 **7**-16
扩展的接口 **5**-199
NAT-src **7**-2
VPN 的 NAT **5**-199
distinguished name **8**-31
DMZ，定义 **1**-A-IV
DN (识别名称) **5**-270
DNS **2**-359
查找 **2**-360
代理 DNS 地址分隔 **2**-367
到服务器的通道 **2**-367
地址分隔 **2**-368
动态 DNS **2**-364
服务器 **2**-395
L2TP 设置 **5**-308
域查找 **2**-367
状态表 **2**-361
DoS **4**-39– **4**-74
防火墙 **4**-40– **4**-48
会话表泛滥 **4**-25，**4**-40
网络 **4**-49– **4**-67
与操作系统相关的 **4**-69– **4**-74
drop-no-rpf-route **4**-27
DS 码点标记 **2**-342，**2**-351，**2**-352
DSL **2**-389，**2**-394
dyndns.org 和 ddo.jp **2**-364
带宽
保证的 **2**-342，**2**-350
管理 **2**-342
缺省优先级 **2**-349
未限定最大值 **2**-342
优先级 **2**-349
优先级排列 **2**-349
最大 **2**-350
最大规格 **2**-342
代理 ID **5**-14
匹配 **5**-81，**5**-88
VPN 和 NAT **5**-199– **5**-200
代理服务器 **1**-A-III
导出规则，定义 **1**-A-II
导出路由 **6**-60
导入规则，定义 **1**-A-II
导入路由 **6**-60
等待时间 **1**-A-III
等开销多路径 (ECMP) **6**-50，**6**-142
登录
根 admin **3**-57
Telnet **3**-14
vsys **9**-33，**9**-38
第 1 阶段 **5**-11
提议 **5**-11
提议，预定义 **5**-11
第 2 层通道协议
请参阅 L2TP
第 2 阶段 **5**-13
提议 **5**-13
提议，预定义 **5**-14
低位临界值 **4**-45
地址
策略中 **2**-301
定义的 **2**-301
公共 **2**-64
私有 **2**-65
通讯簿条目 **2**-140
地址变换
定义 **1**-A-III
另请参阅 NAT-dst 和 NAT-src
地址排除 **2**-333
地址扫描 **4**-8
地址转换
请参阅 NAT、NAT-dst *和* NAT-src
地址组 **2**-142，**2**-301
编辑 **2**-145
创建 **2**-144
选项 **2**-143
移除条目 **2**-146
点对点通道协议 (PPTP) **3**-133
点对点协议
请参阅 PPP
点对多点配置
OSPF **6**-103
电缆，串行 **3**-25
电子邮件警示通知 **3**-96，**3**-99
订购
服务激活 **2**-441，**2**-442
捆绑的服务 **2**-440
临时服务 **2**-439

密钥恢复 **2**-441
注册与激活 **2**-439– **2**-442
定义
区段 **2**-35
子接口 **9**-25
定制服务 **2**-149– **2**-151
在根和 vsys 中 **2**-149
动态 IP
请参阅 DIP
动态 IP 池
请参阅 DIP 池
动态路由 **1**-A-III
动态数据包过滤 **4**-3
度量，定义 **1**-A-X
端口
端口故障切换 **10**-60
端口号 **7**-124
二级可信和不可信 **10**-60
监控 **10**-120, **10**-159
调制解调器 **3**-26
冗余 **10**-39
中继 **9**-23
中继端口 **1**-A-XVI
主可信和不可信 **10**-60
端口地址转换
请参阅 PAT
端口模式 **2**-39– **2**-50
定义 **1**-A-III
端口扫描 **4**-10
端口映射 **7**-5, **7**-34
定义 **1**-A-III
另请参阅 NAT-dst
短缺错误 **3**-132
对等方 **1**-A-III
对等连接
请参阅 P2P
对象监控 **10**-118
多出口区分符 **1**-A-III
多类型用户 **8**-5
多媒体会话， SIP **2**-195

E

equal cost multipath (ECMP) **6**-86
ESP **5**-3, **5**-7, **5**-8
加密和认证 **5**-70, **5**-78
仅加密 **5**-70
仅认证 **5**-70
exe 文件，封锁 **4**-202
恶意 URL 保护 **4**-77– **4**-80
二级 IP 地址 **2**-72
二级路径 **10**-19, **10**-26

F

FIN 扫描 **4**-22
FIPS **1**-xxix
反回放检查 **5**-68, **5**-76
防病毒对象
超时 **4**-98
防病毒扫描 **4**-81– **4**-105
定义 **1**-A-IV
FTP **4**-82
HTTP **4**-84
HTTP keep-alive **4**-103
HTTP trickling **4**-104
HTTP Web 邮件 **4**-86
IMAP **4**-87
解压缩 **4**-101
MIME **4**-85
每个客户端的防病毒资源 **4**-102
POP3 **4**-87
*请参阅*防病毒扫描
SMTP **4**-89
失败模式 **4**-103
预订 **4**-91
防火墙，定义 **1**-xxix, **1**-A-IV
访问列表
定义 **1**-A-IV
IGMP **6**-211
PIM-SM **6**-277
用于路由 **6**-56
组播路由 **6**-199
访问质询 **1**-A-IV
非活动 SA **3**-134
封装安全性负荷
请参阅 ESP
父级连接 **3**-134
服务 **2**-147
策略中 **2**-301
超时临界值 **2**-152
定义的 **2**-301
定制 **2**-149– **2**-151, **4**-173
定制 ALG **2**-303
ICMP **2**-154
下拉式列表 **2**-147
修改超时 **2**-153
在 vsys 中定制 **2**-149
服务簿
定制服务 **2**-147
定制服务 (CLI) **2**-149
服务组 (WebUI) **2**-263
添加服务 **2**-149
修改条目 (CLI) **2**-151
修改条目 (WebUI) **2**-265
移除条目 (CLI) **2**-151
预配置服务 **2**-147
服务器消息块
请参阅 SMB
服务质量
请参阅 QoS
服务组 **2**-263– **2**-266
创建 **2**-264
删除 **2**-266
修改 **2**-265
负载共享 **10**-130
负载均衡
定义 **1**-A-IV

G

global 区段 **7**-117
GPRS 超额计费攻击防护 **4**-219– **4**-225
GRE **6**-199
高可用性
请参阅 HA
高位临界值 **4**-45
公共地址 **2**-64
公共组 **1**-A-IV
攻击
常见目的 **4**-1
大型 ICMP 数据包 **4**-208
回放 **5**-14
会话表泛滥 **4**-25, **4**-40
ICMP 泛滥 **4**-63
ICMP 碎片 **4**-206
IP 数据包碎片 **4**-214
检测和防御选项 **4**-3– **4**-5

阶段 **4**-2
Land 攻击 **4**-67
Ping of Death **4**-69
*请参阅*攻击
SYN 泛滥 **4**-49– **4**-55
SYN 碎片 **4**-216– **4**-217
Teardrop **4**-71
UDP 泛滥 **4**-65
WinNuke **4**-73
未知 MAC 地址 **4**-55
未知协议 **4**-212
攻击保护
安全区段级 **4**-5
策略级 **4**-5
攻击操作 **4**-158– **4**-169
丢弃 **4**-158
丢弃数据包 **4**-158
关闭 **4**-158
关闭服务器 **4**-158
关闭客户端 **4**-158
忽略 **4**-159
无 **4**-159
攻击对象 **4**-134, **4**-145– **4**-152
重新启用 **4**-157
禁用 **4**-157
流式签名 **4**-152
排除 **4**-194
TCP 流式签名 **4**-189
协议异常 **4**-152, **4**-192
已定义 **1**-A-IV
状态式签名 **4**-151
攻击对象数据库 **4**-137– **4**-144
更改缺省 URL **4**-143
立即更新 **4**-137, **4**-138
手动更新 **4**-138, **4**-143
自动更新 **4**-137, **4**-140
自动通知和手动更新 **4**-141
自动通知和自动更新 **4**-137
攻击对象组 **4**-153
帮助 URL **4**-150
更改严重性 **4**-153
记录 **4**-170
严重性级别 **4**-153
在策略中应用 **4**-146
公开 / 私有密钥对 **5**-27
公开密钥基础
请参阅 PKI
功能区段接口 **2**-55
管理接口 **2**-55
HA 接口 **2**-55
供应商专用属性
请参阅 VSA
固件
认证 **2**-425– **2**-427
故障切换
串行接口 **10**-108
对象监控器 **10**-118
设备 **10**-116
双 Untrust 接口 **10**-70, **10**-72
VSD 组 **10**-117
虚拟系统 **10**-130
管理
CLI (命令行界面) **3**-13
vsys admin **9**-38
WebUI **3**-3
限制 **3**-56, **3**-57
管理 IP **3**-41
VSD 组 0 **10**-8
管理方法
CLI **3**-13
控制台 **3**-25
SSL **3**-7
Telnet **3**-13
WebUI **3**-3
管理接口
请参阅 MGT 接口
管理客户端 IP 地址 **3**-56
管理信息库 II
请参阅 MIB II
管理信息流 **3**-37
管理选项 **3**-36
可管理 **3**-41
NSM **3**-36
ping **3**-36
SNMP **3**-36
SSH **3**-36
SSL **3**-36
Telnet **3**-36
透明模式 **3**-37
WebUI **3**-36
关守设备 **2**-176
广播网络 **1**-A-V
规则，源自策略 **2**-299
规则表达式 **4**-182– **4**-184
过滤，数据包 **1**-A-V
过滤器列表 **1**-A-V
过滤源路由 **3**-135

H

HA
串行接口 **10**-103
DHCP **2**-379
电缆连接 **10**-46– **10**-49
二级路径 **10**-26
HA LED **10**-26
IP 跟踪 **10**-122, **10**-159
将网络接口作为 HA 链接连接 **10**-48
聚合接口 **10**-67
控制链接 **10**-39
链接探查 **10**-43
路径监控 **10**-159
冗余接口 **10**-60
数据链接 **10**-41
双 Untrust 接口 **10**-69
双主动故障切换 **10**-6
消息 **10**-41
虚拟 HA 接口 **2**-55
另请参阅 NSRP
主动 / 被动故障切换 **10**-4
专用 HA 接口的电缆连接 **10**-46
hello 间隔 **1**-A-V
hello 数据包 **1**-A-V
HMAC **5**-7
Home 区段 **2**-47
HTTP **3**-5
封锁组件 **4**-201– **4**-203
会话 ID **3**-5
会话超时 **4**-45
keep-alive **4**-103
trickling **4**-104
后备存储器 **3**-132
互联网，定义 **1**-A-V
互联网密钥交换
请参阅 IKE
回放攻击保护 **5**-14
回滚 **2**-436

回滚，配置 **2**-431– **2**-432
会话 ID **3**-5
会话表泛滥 **4**-25, **4**-40
会话超时
HTTP **4**-45
空闲超时 **8**-21
TCP **4**-45
UDP **4**-45
会话限制 **4**-40– **4**-44
基于目标的 **4**-41, **4**-44
基于源的 **4**-40, **4**-43
回传接口 **2**-74
定义 **1**-A-V

I

ICMP
大型数据包 **4**-208
定义 **1**-A-V
碎片 **4**-206
ICMP 泛滥 **4**-63
ICMP 服务 **2**-154
消息代码 **2**-154
消息类型 **2**-154
Ident-Reset **3**-36
IEEE 802.1Q VLAN 标准 **9**-21
IGMP
参数 **6**-216, **6**-218
查询器 **6**-209
代理 **6**-219
发送方代理 **6**-238
基本配置 **6**-213
检验您的配置 **6**-216
接口上的代理 **6**-222
使用访问列表 **6**-211
在接口上启用 **6**-210
主机消息 **6**-208
组播策略 **6**-225
IKE **5**-9, **5**-107, **5**-122, **5**-231
本地 ID， ASN1-DN **5**-273
代理 ID **5**-14
第 1 阶段提议，预定义 **5**-11
第 2 阶段提议，预定义 **5**-14
共享 IKE ID 用户 **5**-292– **5**-300
hello 消息 **5**-436
IKE ID **5**-66– **5**-68, **5**-75– **5**-76, **8**-76, **8**-97
IKE ID 推荐项 **5**-89
IKE ID， Windows 2000 **5**-322, **5**-335
ISAKMP **1**-A-VI
密钥管理 **1**-A-X
冗余网关 **5**-434– **5**-452
心跳信号 **5**-436
用户 **8**-76– **8**-80
用户，定义 **8**-77
用户，组 **8**-76
用户组，定义 **8**-79
远程 ID， ASN1-DN **5**-273
组 IKE ID 用户 **5**-270– **5**-291
组 IKE ID，容器 **5**-275
组 IKE ID，通配符 **5**-274
IKE 用户
服务器支持 **8**-16
IKE ID **8**-2, **8**-76
与其它用户类型 **8**-5
IP
定义 **1**-A-XIV
数据包碎片 **4**-214
IP 安全性
请参阅 IPSec
IP 池
请参阅 DIP 池
IP 地址
第 3 层安全区段 **2**-64– **2**-65
定义 **1**-A-VI
定义每一个端口 **2**-140
二级 **2**-72
跟踪接口 **2**-80
公共 **2**-64
管理 IP **3**-41
扩展的 **5**-199
NSM 服务器 **3**-30
私有 **2**-64
私有地址范围 **2**-65
网络 ID **2**-65
虚拟 **7**-115
主机 ID **2**-65
IP 跟踪 **10**-122, **10**-159
重新路由信息流 **2**-80– **2**-102
出口接口上的故障 **2**-96– **2**-98
device failover threshold **10**-160
定义 **1**-A-VI
动态选项 **2**-82
对象故障临界值 **2**-82
跟踪的 IP 故障临界值 **2**-82, **10**-119
共享接口 **2**-81
ping 和 ARP **10**-122, **10**-159
权重 **2**-82, **10**-160
入口接口上的故障 **2**-99– **2**-102
tracked IP failure threshold **10**-160
通道故障切换 **10**-161
vsys **2**-81
支持的接口 **2**-81
IP 欺骗 **4**-26– **4**-34
drop-no-rpf-route **4**-27
第 2 层 **4**-27, **4**-33
第 3 层 **4**-26, **4**-29
IP 选项 **4**-12– **4**-14
安全 **4**-13
格式设置不正确 **4**-210
记录路由 **4**-13
流 ID **4**-13
record route **4**-14
security **4**-14
stream ID **4**-14
时戳 **4**-14
属性 **4**-12– **4**-14
松散源路由 **4**-13, **4**-35– **4**-37
timestamp **4**-14
严格源路由 **4**-14, **4**-35– **4**-37
源路由 **4**-35
IP 语音
带宽管理 **2**-261
已定义 **2**-176
IPSec **5**-3
AH **5**-2, **5**-69, **5**-78
AH，已定义 **1**-A-IV
传送模式 **5**-4, **5**-305, **5**-311, **5**-320
定义 **1**-A-VI
ESP **5**-2, **5**-69, **5**-78
ESP，已定义 **1**-A-IV
加密 **1**-A-VII
SA **1**-A-I, **5**-2, **5**-10, **5**-11, **5**-13
SPI **5**-2
SPI，定义 **1**-A-I
数字签名 **5**-24
通道 **5**-2
通道模式 **5**-5

通道协商 **5**-11
验证 **1**-A-XVI
IPSec 上的 L2TP **5**-4, **5**-311, **5**-320
双向 **5**-305
通道 **5**-311
ISAKMP **1**-A-VI
ISP - 互联网服务提供商 **2**-367

J

Java applet，封锁 **4**-202
基于 IP 的信息流分类 **9**-33
基于策略的 NAT
请参阅 NAT-dst 和 NAT-src
通道接口 **2**-56
基于策略的 VPN **5**-80
基于路由的 VPN **5**-80– **5**-81
基于散列的信息认证代码
请参阅 HMAC
基于源的路由，定义 **1**-A-VI
基于源的路由选择 **6**-38
基于源接口的路由选择 **6**-42
激活
L2TP **5**-316
频率， NAT-T **5**-351
集群 **10**-17– **10**-21, **10**-50, **10**-140– **10**-143
已定义 **1**-A-VII
集群列表 **1**-A-VII
集群名称， NSRP **10**-18, **10**-143
集线器，定义 **1**-A-VII
即时消息 **4**-148
AIM **4**-148
MSN Messenger **4**-148
Yahoo! Messenger **4**-148
计数 **2**-309
记录 **2**-309, **3**-74– **3**-91
CompactFlash (PCMCIA) **3**-74
电子邮件 **3**-74
攻击对象组 **4**-170
控制台 **3**-74
NSM 报告 **3**-31
内部 **3**-74
self 日志 **3**-87
SNMP **3**-74, **3**-101
事件日志 **3**-75
WebTrends **3**-74, **3**-99
系统日志 **3**-74, **3**-97
资源恢复日志 **3**-91
记录路由 IP 选项 **4**-13
加密
定义 **1**-A-VII
NSRP **10**-7, **10**-19
NSRP-Lite **10**-144
算法 **5**-8, **5**-66, **5**-70, **5**-74, **5**-79
加密选项 **5**-62– **5**-79
“阶段 1”模式 **5**-64, **5**-73
拨号 **5**-72– **5**-79
拨号 VPN 推荐项 **5**-79
传送模式 **5**-78
Diffie-Hellman 组 **5**-65, **5**-68, **5**-74, **5**-77
ESP **5**-70, **5**-78
反回放检查 **5**-68, **5**-76
IKE ID **5**-66– **5**-68, **5**-75– **5**-76
IPSec 协议 **5**-69, **5**-78
加密算法 **5**-66, **5**-70, **5**-74, **5**-79
密钥方法 **5**-64
PFS **5**-68, **5**-77
认证类型 **5**-64, **5**-73
认证算法 **5**-66, **5**-71, **5**-75, **5**-79
通道模式 **5**-78
站点到站点 **5**-63– **5**-71
站点到站点 VPN 推荐项 **5**-71
证书位长 **5**-65, **5**-73
接口
绑定到区段 **2**-63
编址 **2**-64
查看接口表 **2**-61
串行 **10**-103
从 vsys 导出 **9**-19
从区段解除绑定 **2**-67
DIP **2**-267
导入到 vsys **9**-18
第 3 层安全区段 **2**-64
二级 IP 地址 **2**-72
非活动，逻辑 **2**-78
非活动，物理 **2**-78
共享 **9**-15, **9**-33
管理选项 **3**-36
HA **2**-55
HA 双端口 **10**-39– **10**-42
回传 **2**-74
活动，逻辑 **2**-78
活动，物理 **2**-78
IP 跟踪 (*请参阅* IP 跟踪)
监控 **10**-19
监控连接 **2**-80
聚合 **2**-54, **10**-67
可管理 **3**-41
扩展的 **5**-199
MGT **2**-55
MIP **7**-90
Null **5**-105
启用 IGMP **6**-210
缺省 **2**-66
冗余 **2**-54, **10**-60
双 Untrust **10**-69
通道 **2**-33, **2**-56, **2**-56– **2**-60
通道，定义 **1**-A-XIII
VIP **7**-115
VSI **2**-54, **10**-29
物理 **2**-3
修改 **2**-68
虚拟 HA **2**-55, **10**-48
专用的 **9**-15, **9**-33
状态更改 **2**-78– **2**-102
接口监控
安全区段 **2**-94
环 **2**-88
接口 **2**-87– **2**-94
解压缩，防病毒扫描 **4**-101
警报
向 NSM 报告 **3**-31
静态路由 **1**-A-VII
组播 **6**-198
静态路由选择 **6**-2, **6**-6– **6**-16
配置 **6**-10
使用 **6**-9
在 Null 接口上转发 **6**-17
聚合 **1**-A-VIII
聚合接口 **2**-54, **10**-67
聚合器 **1**-A-VIII
聚合状态 **1**-A-VIII
拒绝服务
请参阅 DoS
距离向量 **1**-A-VIII
局域网，定义 **1**-A-VII

K

keep alive，BGP **1**-A-VII
空闲会话超时 **8**-21
控制台 **3**-74
控制消息 **10**-39
HA 物理链接心跳信号 **10**-40
HA 消息 **10**-41
RTO 心跳信号 **10**-41
VSD 心跳信号 **10**-40

L

L2TP **5**-301– **5**-342
本地数据库 **8**-106
操作模式 **5**-305
策略 **2**-304
地址分配 **8**-105
封装 **5**-306
hello 信号 **5**-316
激活 **5**-316
解封 **5**-307
接入集中器
请参阅 LAC
强制的配置 **5**-302
缺省参数 **5**-308
RADIUS 服务器 **5**-308
ScreenOS 支持 **5**-305
SecurID 服务器 **5**-308
双向 **5**-305
通道 **5**-311
Windows 2000 **5**-325
Windows 2000 通道认证 **5**-316
外部 auth 服务器 **8**-106
网络服务器
请参阅 LNS
用户认证 **8**-105
在 Windows 2000 中仅使用 L2TP **5**-305
自愿的配置 **5**-302
L2TP 用户 **8**-105– **8**-109
服务器支持 **8**-16
认证点 **8**-2
与 XAuth **8**-5
LAC **5**-302
NetScreen-Remote 5.0 **5**-302
Windows 2000 **5**-302
Land 攻击 **4**-67
LDAP **8**-30– **8**-31
auth 服务器对象 **8**-37
common name identifier **8**-31
distinguished name **8**-31
结构 **8**-30
server port **8**-31
支持的用户类型 **8**-31
LED 指示器，HA **10**-26
Lightweight Directory Access Protocol
请参阅 LDAP
LKG (上次已知正确) **2**-431
LKG 配置 **2**-431
LNS **5**-302
LSA 抑制 **6**-102
历史记录图表 **2**-309
联合 **1**-A-VIII
连接器
GBIC，定义 **1**-A-IV
RJ-45，定义 **1**-A-XI
连接状态 **1**-A-VIII
链接状态 **1**-A-VIII
链接状态通告 **1**-A-VIII
邻居 **1**-A-VIII, **1**-A-IX
令牌代码 **8**-28
浏览器要求 **3**-3
流 ID IP 选项 **4**-13
流量
报警 **3**-92– **3**-96
流式签名 **4**-152
路径监控 **10**-159
通道故障切换 **10**-161
路由
二级 IP 地址之间 **2**-72
基于源 **1**-A-VI
缺省路由 **1**-A-XI
下一跳跃 **1**-A-X, **1**-A-XV
优先级 **1**-A-XVI
组播 **6**-193
路由表 **1**-A-IX, **6**-4
查找 **6**-44
类型 **6**-38
路由选择 **6**-35
在多个 VR 中的查找 **6**-48
组播 **6**-196
路由查找
多个 VR **6**-48
顺序 **6**-44
路由重新分配 **1**-A-IX, **6**-53
路由度量 **6**-37
路由反射器 **1**-A-IX
路由过滤 **6**-56
路由模式 **2**-130– **2**-135
接口设置 **2**-131
路由器，定义 **1**-A-IX
路由文件布置和分配程序衰减 **1**-A-IX
路由选择 **6**-2
路由选择 **6**-35
路由优先级 **6**-35
路由映射 **1**-A-IX, **6**-54

M

MAC 地址
定义 **1**-A-X
Main 模式 **5**-12
MD5 **5**-7
定义 **1**-A-IX
MED 比较 **1**-A-X
MGT 接口 **2**-55
管理选项 **3**-37
MIB II **3**-36, **3**-101
MIB 文件 **3**-A-I
MIB 文件，导入 **5**-373
MIB 文件夹
一级 **3**-A-II
Microsoft Network Instant Messenger
请参阅 MSN Instant Messenger
Microsoft 远程过程调用
请参阅 MS-RPC
MIME，防病毒扫描 **4**-85
MIP **2**-13, **7**-90
创建地址 **7**-92
从其它区段可到达 **7**-95
地址范围 **7**-94
定义 **1**-A-XVI, **7**-8
global 区段 **7**-91
流向带有基于接口的 NAT 的区段 **2**-124
缺省网络掩码 **7**-94
缺省虚拟路由器 **7**-94
same-as-untrust 接口 **7**-101– **7**-104
双向转换 **7**-8
VPN **5**-199
虚拟系统 **9**-10

在区段接口上创建 **7**-92
在通道接口上创建 **7**-100
MS RPC ALG
服务 **2**-159
服务组 **2**-162
已定义 **2**-159
MSN Messenger **4**-148
MS-RPC **4**-149
密码
根 admin **3**-54
vsys admin **9**-38
遗忘 **3**-51
密码认证协议
请参阅 PAP
密钥
管理 **1**-A-X
名称
约定 **1**-xxxix, **2**-xii, **3**-x, **4**-x, **5**-x, **6**-xii, **7**-viii, **8**-viii, **9**-viii, **10**-viii
命令行界面
请参阅 CLI
模式配置 **8**-82
模数 **5**-13

N

NAT
定义 **1**-A-XIV, **7**-2
IPSec 和 NAT **5**-345
NAT 服务器 **5**-345
NAT-src 与 NAT-dst **7**-68– **7**-88
NAT 穿透
请参阅 NAT-T
NAT 模式 **2**-122– **2**-129
接口设置 **2**-125
流向 Untrust 区段的信息流 **2**-103, **2**-124
NAT 向量错误 **3**-134
NAT-dst **7**-34– **7**-88
带有端口映射的单个 IP 地址 **7**-11
单个 IP，无端口映射 **7**-11
单向转换 **7**-8, **7**-13
地址变换 **7**-7, **7**-35, **7**-58
地址范围 **7**-6
地址范围到单个 IP 地址 **7**-12, **7**-53
地址范围到地址范围 **7**-12, **7**-58
定义 **1**-A-X
端口映射 **7**-5, **7**-34, **7**-63
路由注意事项 **7**-35, **7**-40– **7**-43
数据包流 **7**-36– **7**-39
VPN **5**-199
一对多转换 **7**-49
一对一转换 **7**-44
与 MIP 或 VIP 一起 **7**-4
NAT-src **7**-2, **7**-16– **7**-32
出口接口 **7**-10, **7**-30– **7**-32
DIP 池 **7**-2
DIP 池，固定端口 **7**-9
带有 PAT 的 DIP 池 **7**-9, **7**-17– **7**-20
带有地址变换的 DIP 池 **7**-10
单向转换 **7**-8, **7**-13
地址变换 **7**-24– **7**-29
地址变换，范围注意事项 **7**-24
定义 **1**-A-XIV
端口地址转换 **7**-3
固定端口 **7**-16, **7**-21– **7**-23
基于接口 **7**-3
路由模式路由模式
NAT-src **2**-130
VPN **5**-202
NAT-T **5**-345– **5**-354
发起方和响应方 **5**-352
激活频率 **5**-351
IKE 数据包 **5**-348
IPSec 数据包 **5**-350
启用 **5**-353
探查 NAT **5**-346– **5**-347
VPN 的障碍 **5**-348
NetBIOS **4**-149
NetInfo **2**-371
NetScreen 词典文件 **8**-25
NetScreen 可靠传输协议
请参阅 NRTP
NetScreen 冗余协议
请参阅 NSRP
NetScreen-Remote
动态对等方 **5**-240, **5**-252
NAT-T 选项 **5**-345
自动密钥 IKE VPN **5**-231
NetScreen-Security Manager
请参阅 NSM
NHTB 表 **5**-374– **5**-379
路由到通道的映射 **5**-375
手动条目 **5**-378
寻址方案 **5**-376
自动条目 **5**-379
NRTP **10**-34, **10**-156
NSM
bulk-CLI **2**-436
报告事件 **3**-31, **3**-32
重启超时 **2**-436
初始连接建立 **3**-28
代理 **3**-27, **3**-30
定义 **3**-27
管理系统 **3**-27, **3**-30
管理选项 **3**-36
配置时戳 **3**-35
配置同步 **3**-33
启用代理 **3**-29
UI **3**-27
NSRP
ARP **10**-57
ARP 广播 **10**-19
安全通信 **10**-7, **10**-19
备份 **10**-4
clear 集群命令 **10**-17, **10**-143
config sync **10**-34
debug 集群命令 **10**-17, **10**-143
DHCP **2**-379
DIP 组 **2**-285– **2**-288
电缆连接 **10**-46– **10**-49
端口故障切换 **10**-60
端口监控 **10**-120
二级路径 **10**-19, **10**-26
负载共享 **10**-130
概述 **10**-3
管理 IP **10**-122, **10**-159
HA 电缆连接，网络接口 **10**-48
HA 电缆连接，专用接口 **10**-46
HA 端口，冗余接口 **10**-60
HA 会话备份 **2**-308, **10**-22
HA 接口 **10**-40
HA LED **10**-26
集群 **10**-17– **10**-21, **10**-50
集群名称 **10**-18, **10**-143
接口监控 **10**-19
控制链接 **10**-39
控制消息 **10**-39, **10**-40
NAT 和 “路由” 模式 **10**-8

NSRP，已定义 **1**-A-X
NTP 同步 **2**-445，**10**-38
配置回滚 **2**-433
抢先模式 **10**-24
全网状配置 **10**-46，**10**-130
缺省设置 **10**-9，**10**-141
RTO **1**-A-XVI，**10**-22– **10**-23，**10**-50
RTO 状态 **10**-23
RTO，同步 **10**-35
冗余端口 **10**-39
冗余接口 **2**-54
数据包转发和动态路由选择 **10**-42
数据链接 **10**-41
数据消息 **10**-41
同步，PKI **10**-35
透明模式 **10**-8
VSD 组 **10**-5，**10**-24– **10**-28，**10**-50，**10**-159
VSD，已定义 **1**-A-XV
VSI **1**-A-XV，**2**-54，**10**-5
VSI，静态路由 **10**-29，**10**-65，**10**-66
文件，同步 **10**-35
虚拟系统 **10**-130– **10**-136
抑制时间 **10**-52，**10**-56
优先级编号 **10**-24
主设备 **10**-4
NSRP-Lite **10**-137– **10**-158
安全通信 **10**-144
电缆连接 **10**-148
端口监控 **10**-159
集群 **10**-140– **10**-143
禁用同步 **10**-158
配置同步 **10**-156
抢先模式 **10**-147
VSD 组 **10**-145– **10**-147
文件同步 **10**-157
NTP **2**-444– **2**-447
保护服务器 **2**-447
多台服务器 **2**-444
服务器 **2**-444
服务器配置 **2**-446
NSRP 同步 **2**-445，**10**-38
认证类型 **2**-447
最大时间调整 **2**-445
Null 接口 **5**-105
Null 接口，定义路由 **6**-17
Null 路由 **5**-105
内部闪存 **3**-74
内部网，定义 **1**-A-XI
内容过滤 **4**-75– **4**-129

O

OCSP (在线证书状态协议) **5**-44
客户端 **5**-44
响应方 **5**-44
OSPF
安全配置 **6**-95
按需电路 **6**-101
备份指定路由器 **6**-69
重新分配路由 **6**-83
点对点网络 **6**-69
点对多点 **6**-103
定义 **1**-A-VIII
定义区域 **6**-74
ECMP 支持 **6**-86
防止泛滥 **6**-99
负载均衡 **6**-50
广播网络 **6**-69
过滤邻居 **6**-97
hello 协议 **6**-69
汇总重新分配的路由 **6**-84
减少的 LSA 泛滥 **6**-101
接口参数 **6**-92
禁用路由拒绝限制 **6**-104
拒绝缺省路由 **6**-98
LSA 抑制 **6**-102
链接状态通告 **6**-67，**6**-70
邻居认证 **6**-95
路由器类型 **6**-68
路由器邻接关系 **6**-69
not so stubby 区域 **6**-68
配置步骤 **6**-71
区域 **6**-67
全局参数 **6**-86
stub 区域 **6**-68
设置 OSPF 链接类型 **6**-103
通道接口 **6**-101，**6**-103
为区域分配接口 **6**-76
虚拟链接 **1**-A-XV，**6**-88
在 VR 中创建实例 **6**-72
在接口上启用 **6**-78
指定路由器 **6**-69

P

P2P **4**-148
BitTorrent **4**-148
DC **4**-148
eDonkey **4**-148
FastTrack **4**-149
Gnutella **4**-148
KaZaa **4**-149
MLdonkey **4**-149
Skype **4**-149
SMB **4**-149
WinMX **4**-149
PAP **5**-305，**5**-308
PAT **2**-268，**7**-16
定义 **1**-A-III
PCMCIA **3**-74
PFS **5**-14，**5**-68，**5**-77
PIM-SM **6**-250
安全配置 **6**-277
创建实例 **6**-257
代理 RP **6**-284
汇聚点 **6**-252
IGMPv3 **6**-301
接口参数 **6**-281
配置 RP **6**-273
配置步骤 **6**-256
指定路由器 **6**-252
转发信息流 **6**-253
PIM-SSM **6**-302
ping
管理选项 **3**-36
Ping of Death **4**-69
PKI **5**-26
加密 **1**-A-VII
密钥 **3**-8
PPP **5**-303
PPPoE **2**-393– **2**-404
定义 **1**-A-XVI
多个实例 **2**-401
高可用性 **2**-404
每个接口上的多个会话 **2**-399
配置 **2**-398
设置 **2**-393
排除，地址 **2**-333
排除，深入检查 **4**-194

配置
保存 **2**-429
保存和导入 **2**-429
备份 **2**-429
回滚 **2**-431– **2**-432, **2**-433
加载 **2**-433
LKG **2**-431
锁定 **2**-434
添加注释 **2**-435
下载和上传 **2**-429
配置设置
查看配置状态 **3**-33
检索时戳 **3**-35
浏览器要求 **3**-3
配置散列信息 **3**-34

Q

QoS **1**-xxix, **2**-342
前缀，已定义 **1**-A-XI
抢先模式 **10**-24, **10**-147
桥接器 **1**-A-XI
区段 **2**-29– **2**-38
安全 **1**-A-I, **2**-32
第 2 层 **2**-105
定义 **1**-A-XI
global **2**-32, **7**-117
功能 **2**-38
共享 **9**-15
通道 **1**-A-XIII, **2**-33
VLAN **2**-38, **2**-105
vsys **9**-7
区域 **1**-A-XI
区域边界路由器 **1**-A-XI
区域范围 **1**-A-XI
全网状配置 **10**-130

R

RADIUS **3**-51, **8**-23– **8**-25
auth 服务器对象 **8**-32
对象属性 **8**-24
访问质询 **1**-A-IV
L2TP **5**-308
NetScreen 词典文件 **8**-3
port **8**-24
retry timeout **8**-24
shared secret **8**-24
record route IP 选项 **4**-14
RFC
(MD5) 1321 **5**-7
(SHA-1) 2404 **5**-7
791 **4**-12
791, "Internet Protocol" **4**-12, **4**-13, **4**-69, **4**-210
792, "Internet Control Message Protocol" **2**-154, **4**-69
793, "Transmission Control Protocol" **4**-18
959, "File Transfer Protocol (FTP)" **4**-II
1035, "Domain Names - Implementation and Specification" **4**-I
1038, Revised IP Security Option **4**-13
1112, Host Extensions for IP Multicasting **6**-206
1157, "A Simple Network Management Protocol" **3**-101
1213 **3**-36
1213, "Management Information Base for Network Management of TCP/IP-based internets MIB-II" **3**-101
1349, "Type of Service in the Internet Protocol Suite" **2**-310
1508, "Generic Security Service Application Program Interface" **4**-III
1583 **6**-81, **6**-86
1701, Generic Routing Encapsulation (GRE) **1**-A-XIII, **6**-199
1730, "Internet Message Access Protocol - Version 4" **4**-III
1731, "IMAP4 Authentication Mechanisms" **4**-III
1771 **6**-156
1777, "Lightweight Directory Access Protocol" **8**-30
1793 **6**-93, **6**-101
1901, "Introduction to Community-based SNMPv2" **3**-101
1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)" **3**-101
1906, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)" **3**-101
1918, "Address Allocation for Private Internets" **2**-65
1939, "Post Office Protocol - Version 3" **4**-III
1945, "Hypertext Transfer Protocol - HTTP/1.0" **4**-II
1965 **6**-168, **6**-183, **6**-184
1966 **6**-180
1997 **6**-186
2082 **6**-113
2091 **6**-143
2104 **5**-7
2132, "DHCP Options and BOOTP Vendor Extensions" **2**-378
2236, Internet Group Management Protocol, Version 2 **6**-206
2326 第 11 节 **2**-164
2326, "Real Time Streaming Protocol (RTSP)" **2**-169
2328 **6**-86
2338 **10**-122, **10**-159
2403 **5**-7
2407 **5**-3
2408 **5**-3
2453 **6**-113, **6**-137
2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" **2**-310
2821, "Simple Mail Transfer Protocol" **4**-IV
3065 **6**-183
3376, Internet Group Management Protocol, Version 3 **6**-206
3569, An Overview of Source-Specific Multicast (SSM) **6**-250
RIP
安全配置 **6**-130
按需电路配置 **6**-143
版本 **6**-137
备用路由 **6**-141
查看 RIP 接口详细信息 **6**-124
查看 RIP 邻居信息 **6**-123
查看 RIP 数据库 **6**-121
查看 RIP 协议详细信息 **6**-122
重新分配路由 **6**-118

点对多点 **6**-146
定义 **1**-A-IX
防止泛滥 **6**-134
负载均衡 **6**-50
过滤邻居 **6**-132
接口参数 **6**-128
拒绝缺省路由 **6**-133
邻居认证 **6**-130
配置按需电路 **6**-144
配置步骤 **6**-114
配置汇总路由 **6**-139
前缀汇总 **6**-139
全局参数 **6**-125
数据库 **6**-141
协议版本 **6**-137
协议概述 **6**-113
在 VR 中创建实例 **6**-115
在接口上启用 **6**-117
RSH ALG **2**-156
RTCP
定义 **1**-A-XII
RTO **10**-22– **10**-23
操作状态 **10**-23
RTO 对等方 **10**-25
RTP
定义 **1**-A-XII
RTSP ALG
公共域中的服务器 **2**-173
请求方法 **2**-166
已定义 **2**-164
专用域中的服务器 **2**-170
状态代码 **2**-168
认证
Allow Any **2**-308
策略 **2**-306
NSRP **10**-7, **10**-19
NSRP-Lite **10**-144
算法 **5**-7, **5**-66, **5**-71, **5**-75, **5**-79
WebAuth **8**-43
用户 **2**-306, **8**-41– **8**-74
认证，用户 **8**-15– **8**-74
admin **8**-3
auth 服务器 **8**-16
auth 用户 **8**-41
本地数据库 **8**-18– **8**-19
多类型 **8**-5
IKE 用户 **8**-16, **8**-76
L2TP 用户 **8**-105
类型和应用 **8**-2– **8**-5
认证点 **8**-2
使用不同登录 **8**-5
手动密钥用户 **8**-16
WebAuth **8**-16
XAuth 用户 **8**-81
用户类型 **8**-16
认证包头
请参阅 AH
认证证书 **2**-425– **2**-428
MD5 消息整理 **2**-426
容器 **5**-275
冗余网关 **5**-434– **5**-452
恢复过程 **5**-437
TCP SYN 标记检查 **5**-440
软件
更新 **2**-405
密钥， vsys **9**-15

S

SA **5**-10, **5**-11, **5**-13
定义 **1**-A-I
数据包流检查 **5**-84
SA 策略 **3**-134
SCEP (简单证书注册协议) **5**-38
SCP **3**-24
定义 **1**-A-I
客户端命令范例 **3**-24
启用 **3**-24
SCREEN
大型 ICMP 数据包，封锁 **4**-208
地址扫描 **4**-8
丢弃未知 MAC 地址 **4**-55
端口扫描 **4**-10
ICMP 泛滥 **4**-63
ICMP 碎片，封锁 **4**-206
IP 欺骗 **4**-26– **4**-34
IP 数据包碎片，封锁 **4**-214
IP 选项 **4**-12
Land 攻击 **4**-67
MGT 区段 **2**-32
Ping of Death **4**-69
SYN 泛滥 **4**-49– **4**-55
SYN 碎片，检测 **4**-216– **4**-217
SYN-ACK-ACK 代理泛滥 **4**-47
设置 SYN 和 FIN 标志 **4**-16
松散源路由 IP 选项，检测 **4**-37
Teardrop **4**-71
UDP 泛滥 **4**-65
VLAN 和 MGT 区段 **4**-3
WinNuke 攻击 **4**-73
未知协议，丢弃 **4**-212
无标志的 TCP 数据包，检测 **4**-20
严格源路由 IP 选项，检测 **4**-37
有 FIN 但无 ACK **4**-22
有 FIN 但无 ACK 标志，丢弃 **4**-18
有害 IP 选项，丢弃 **4**-210
源路由 IP 选项，拒绝 **4**-37
ScreenOS **1**-xxx
安全区段 **2**-2, **2**-32
安全区段， global **2**-2
安全区段，预定义 **2**-2
安全区段接口 **2**-3
策略 **2**-3
端口模式 **2**-39
global 区段 **2**-32
概述 **2**-1– **2**-28
更新 **2**-405
功能区段 **2**-38
Home-Work 区段 **2**-47
区段 **2**-29– **2**-38
数据包流 **2**-12– **2**-14
通道区段 **2**-33
物理接口 **2**-3
虚拟系统 **2**-11
虚拟系统，区段 **9**-7
虚拟系统， VR **9**-6
子接口 **2**-4
SDP **2**-199– **2**-200
定义 **1**-A-VI
SecurID **8**-28– **8**-29
ACE 服务器 **8**-28
auth 服务器对象 **8**-35
authentication port **8**-29
cient retries **8**-29
client timeout **8**-29
duress **8**-29
encryption type **8**-29
L2TP **5**-308

令牌代码 **8**-28
认证器 **8**-28
用户类型支持 **8**-29
security IP 选项 **4**-14
self 日志 **3**-87
SHA-1 **5**-7
定义 **1**-A-XI
SIBR **6**-42
SIP **2**-195– **2**-205
ALG **2**-199, **2**-203
定义 **1**-A-VI
多媒体会话 **2**-195
会话静止超时 **2**-203
静止超时 **2**-203
连接信息 **2**-200
媒体静止超时 **2**-203, **2**-205
媒体声明 **2**-200
请求方法 **2**-196
请求方法的类型 **2**-196
RTCP **2**-200
RTP **2**-200
SDP **2**-199– **2**-200
响应 **2**-198
响应代码 **2**-198
消息 **2**-195
信号发送 **2**-199
信号发送静止超时 **2**-203, **2**-205
已定义 **2**-195
针孔 **2**-199
SIP NAT
DMZ 中的代理 **2**-237
公用区段中的代理 **2**-233
呼叫设置 **2**-207, **2**-213
内向，使用 MIP **2**-222, **2**-226
使用 DIP 池 **2**-222
使用接口 DIP **2**-218
使用内向 DIP **2**-216
使用全网状 VPN **2**-253
私有区段中的代理 **2**-229
trust 内部区段 **2**-249
untrust 内部区段 **2**-243
已定义 **2**-207
SMB
NetBIOS **4**-149
SMTP 服务器 IP **3**-96
SNMP **3**-36, **3**-101
公共组，公开 **3**-105
公共组，私有 **3**-105
管理选项 **3**-36
加密 **3**-104, **3**-107
冷启动陷阱 **3**-101
流量报警陷阱 **3**-101
MIB 文件 **3**-A-I
MIB 文件，导入 **5**-373
MIB 文件夹，一级 **3**-A-II
配置 **3**-105
VPN 监控 **5**-373
系统报警陷阱 **3**-101
陷阱 **3**-101
陷阱类型 **3**-102
执行 **3**-104
SNMP 陷阱
100，硬件问题 **3**-102
200，防火墙问题 **3**-102
300，软件问题 **3**-102
400，流量问题 **3**-102
500，VPN 问题 **3**-102
允许或拒绝 **3**-104
SPI
定义 **1**-A-I
SSH **3**-15– **3**-21, **3**-36
定义 **1**-A-II
服务器密钥 **3**-16
会话密钥 **3**-16
加载公开密钥，CLI **3**-20
加载公开密钥，TFTP **3**-20, **3**-23
加载公开密钥，WebUI **3**-20
连接过程 **3**-16
密码认证 **3**-19
PKA **3**-20
PKA 密钥 **3**-16
PKA 认证 **3**-19
强制仅使用 PKA 认证 **3**-21
认证方法优先级 **3**-21
主机密钥 **3**-16
自动登录 **3**-23
SSL **3**-7
管理选项 **3**-36
与 WebAuth **8**-70
SSL 握手协议
请参阅 SSLHP
SSLHP **3**-7
stream ID IP 选项 **4**-14
Sun RPC ALG
调用场景 **2**-156
服务 **2**-157
已定义 **2**-156
SurfControl **4**-107, **4**-121
SYN 泛滥 **4**-49– **4**-55
超时 **4**-55
丢弃未知 MAC 地址 **4**-55
队列长度 **4**-55
攻击 **4**-49
攻击临界值 **4**-53
警告临界值 **4**-53
临界值 **4**-50
目标临界值 **4**-54
源临界值 **4**-54
SYN 检查 **4**-22, **4**-23– **4**-25
非对称路由 **4**-24
会话表泛滥 **4**-25
会话中断 **4**-24
侦查漏洞 **4**-25
SYN 碎片 **4**-216– **4**-217
SYN-ACK-ACK 代理泛滥 **4**-47
三方握手 **1**-A-XII, **4**-49
三重 DES
请参阅 3DES
上次已知正确的配置
请参阅 LKG 配置
设备故障切换 **10**-116
设置 SYN 和 FIN 标志 **4**-16
深入检查 **4**-153– **4**-188
重新启用攻击对象 **4**-157
定义 **1**-A-XII
定制服务 **4**-173– **4**-180
定制攻击对象 **4**-181
定制签名 **4**-182– **4**-188
概述 **4**-133
更改严重性 **4**-153
攻击操作 **4**-158– **4**-169
攻击对象 **4**-134
攻击对象排除 **4**-194
攻击对象数据库 **4**-137– **4**-144
攻击对象组 **4**-153
攻击对象，已定义 **1**-A-IV
规则表达式 **4**-182– **4**-184

环境 **4**-I
记录攻击对象组 **4**-170
禁用攻击对象 **4**-157
流式签名 **4**-152
认证下载 **2**-425– **2**-428
协议异常 **4**-152
状态式签名 **4**-151
失败模式 **4**-103
时戳 IP 选项 **4**-14
时戳检索 **3**-35
时戳配置 **3**-35
时间表 **2**-289, **2**-309
时区 **2**-443
时钟，系统 **2**-443– **2**-447
*另请参阅*系统时钟
实时传输控制协议
请参阅 RTCP
实时传输协议
请参阅 RTP
事件日志 **3**-75
手动密钥 **5**-162, **5**-173
管理 **5**-9
VPN **3**-58, **3**-108
数据包 **3**-135
不可路由 **3**-134
冲突 **3**-131, **3**-132
地址欺骗攻击 **3**-132
点对点通道协议 (PPTP) **3**-133
丢弃的 **3**-134, **3**-135
IPSec **3**-133
拒绝的 **3**-134
Land 攻击 **3**-133
内向 **3**-131
破碎 **3**-135
收到的 **3**-131, **3**-132, **3**-133, **3**-134
网络地址转换 (NAT) **3**-134
无法接收的 **3**-131, **3**-132
已传送的欠载 **3**-132
因特网控制信息协议 (ICMP) **3**-130, **3**-133
数据包过滤 **1**-A-V
数据包流 **2**-12– **2**-14
出站 VPN **5**-83– **5**-84
基于策略的 VPN **5**-87
基于路由的 VPN **5**-82– **5**-86
NAT-dst **7**-36– **7**-39
入站 VPN **5**-85– **5**-86
数据加密标准
请参阅 DES
数据消息 **10**-41
数字签名 **5**-24
双 Untrust 接口 **10**-69
私有地址 **2**-65
松散源路由 IP 选项 **4**-13, **4**-35– **4**-37
碎片重组 **4**-77– **4**-80

T

TCP
代理 **3**-135
会话超时 **4**-45
流式签名 **4**-189
SYN 标记检查 **5**-440
三方握手 **1**-A-XII
无标志的数据包 **4**-20
TCP/IP，定义 **1**-A-II
Teardrop 攻击 **4**-71
Telnet **3**-13, **3**-36
timestamp IP 选项 **4**-14
trace-route **2**-110, **2**-113
traffic
priority **2**-310
Trust 区段，定义 **1**-A-XIII
探查
操作系统 **4**-16– **4**-20
开放端口 **4**-10
网络 **4**-8
逃避 **4**-22– **4**-37
提议
第 1 阶段 **5**-11
第 2 阶段 **5**-13
阶段 1 **5**-88
阶段 2 **5**-88
调制解调器端口 **3**-26
同步
查看状态 **3**-33
PKI 对象 **10**-35
配置 **3**-33, **10**-34
配置散列信息检索 **3**-34
RTO **10**-35
文件 **10**-35
通道接口 **2**-56
定义 **1**-A-XIII, **2**-56
基于策略的 NAT **2**-56
通道模式 **5**-5
通道区段，定义 **1**-A-XIII
通告 **1**-A-XIII
通配符 **5**-274
通讯簿
编辑组条目 **2**-145
*另请参阅*地址
添加地址 **2**-140
条目 **2**-140
修改地址 **2**-141
移除地址 **2**-146
组 **2**-142
统计信息
向 NSM 报告 **3**-31
透明模式 **2**-104– **2**-121
ARP/trace-route **2**-108
单播选项 **2**-108
丢弃未知 MAC 地址 **4**-55
泛滥 **2**-108
管理选项 **3**-37
广播信息流 **2**-106
路由 **2**-106
阻止非 ARP 信息流 **2**-106
阻止非 IP 信息流 **2**-106
图标
策略 **2**-312
定义的 **2**-312
图表，历史记录 **2**-309

U

UDP
定义 **1**-A-XVI
会话超时 **4**-45
NAT-T 封装 **5**-345
校验和 **5**-351
UDP 泛滥 **4**-65
Untrust 区段，定义 **1**-A-XIII
URL 过滤 **2**-308, **4**-106, **4**-121– **4**-129
blocked URL message type **4**-125
communication timeout **4**-124
策略级应用 **4**-126
重新定向 **4**-121
服务器状态 **4**-126
高速缓存 **4**-120
集成 **4**-107

路由 **4**-127
每个 vsys 的服务器 **4**-123
NetScreen blocked URL message **4**-125
配置文件 **4**-112
SurfControl CPA 服务器 **4**-107
SurfControl 服务器 **4**-119
SurfControl SCFP **4**-123
SurfControl server name **4**-124
SurfControl server port **4**-124
设备级激活 **4**-126
输入环境 **4**-108
Websense server name **4**-124
Websense server port **4**-124
URL 类别 **4**-110
应用配置文件到策略 **4**-115
URL 过滤服务 **2**-440, **2**-441
URL，定义 **1**-A-XIII
UTP，定义 **1**-A-IV

V

Verisign **5**-44
VIP **2**-13
必需的信息 **7**-116
编辑 **7**-120
从其它区段可到达 **7**-117
定义 **1**-A-XV, **7**-8
定制服务，低端口号 **7**-116
定制和多端口服务 **7**-121– **7**-127
global 区段 **7**-117
流向带有基于接口的 NAT 的区段 **2**-124
配置 **7**-117
虚拟系统 **9**-10
移除 **7**-120
VLAN
标记 **1**-XVII, **2**-4, **9**-23, **9**-24
创建 **9**-25– **9**-27
定义 **1**-A-XV
基于 VLAN 的信息流分类 **9**-21
透明模式 **9**-22, **9**-23
与另一个 VLAN 通信 **9**-28– **9**-32
中继 **9**-22
子接口 **9**-23
VLAN 区段 **2**-105
VLAN1
管理选项 **3**-37
接口 **2**-105, **2**-114
区段 **2**-105
VPN **1**-xxix
Aggressive 模式 **5**-12
策略 **2**-303
重叠地址的 NAT **5**-199– **5**-216
Diffie-Hellman 交换 **5**-13
Diffie-Hellman 组 **5**-13
代理 ID，匹配 **5**-88
第 1 阶段 **5**-11
第 2 阶段 **5**-13
定义 **1**-A-XVI
FQDN 别名 **5**-183
管理流量 **3**-107
回放攻击保护 **5**-14
基于路由和基于策略 **5**-80
加密选项 **5**-62– **5**-79
空闲时间 **8**-84
流向带有基于接口的 NAT 的区段 **2**-124
Main 模式 **5**-12
MIP **5**-199
每个通道接口多个通道 **5**-374– **5**-430
NAT-dst **5**-199
NAT-src **5**-202
配置技巧 **5**-88– **5**-89
冗余网关 **5**-434– **5**-452
冗余组，恢复过程 **5**-437
SA **5**-10
手动密钥 **3**-58, **3**-108
数据包流 **5**-82– **5**-87
通道区段 **2**-33
通道始终处于连接状态 **5**-356
通道，定义 **1**-A-XIII
VPN 监控和重定密钥 **5**-356
VPN 组 **5**-434
网关的 FQDN **5**-182– **5**-198
自动密钥 IKE **3**-58, **3**-108, **5**-9
VPN 监控 **5**-355– **5**-372
策略 **5**-359
重定密钥选项 **5**-356, **5**-379
ICMP 回应请求 **5**-373
路由设计 **5**-90
目标地址 **5**-357– **5**-360
目标地址，XAuth **5**-358
SNMP **5**-373
外向接口 **5**-357– **5**-360
状态更改 **5**-355, **5**-359
VR **6**-21– **6**-60
BGP **6**-159– **6**-169
创建共享 VR **9**-16
导出路由 **6**-60
导入路由 **6**-60
等值路由 **6**-50
定义 **1**-A-XV
定制 **6**-25
访问列表 **6**-56
共享 **9**-15
基于源的路由选择 **6**-38
基于源接口的路由选择 **6**-42
简介 **2**-5
路由表查找 **6**-44
路由度量 **6**-37
路由过滤 **6**-56
路由器 ID **6**-32
路由选择 **6**-35
路由映射 **6**-54
路由优先级 **6**-35
路由重新分配 **6**-53
OSPF **6**-71– **6**-100
RIP **6**-114– **6**-136
使用两个 VR **6**-21, **6**-22
修改 **6**-31
预定义的 **6**-21
在 vsys 上 **6**-27
在多个 VR 中的路由表查找 **6**-48
转发信息流的范围 **2**-5, **6**-22
最大路由表条目数 **6**-34
VRRP **10**-122, **10**-159
VSA **8**-25
attribute name **8**-25
attribute number **8**-25
attribute type **8**-25
vendor ID **8**-25
VSD 组 **10**-5, **10**-24– **10**-28, **10**-145– **10**-147
成员状态 **10**-25, **10**-145– **10**-146, **10**-159
故障切换 **10**-117
VSD，已定义 **1**-A-XV
心跳信号 **10**-19, **10**-26, **10**-146
抑制时间 **10**-52, **10**-56
优先级编号 **10**-24

VSI **10**-5, **10**-24, **10**-145
静态路由 **10**-29, **10**-65, **10**-66
每个 VSD 组有多个 VSI **10**-130
已定义 **1**-A-XV

W

Web 浏览器要求 **3**-3
Web 用户界面
请参阅 WebUI
WebAuth **8**-16
本地用户组 **8**-63
策略前认证过程 **2**-307
策略前认证进程 **8**-43
外部用户组 **8**-66
与 SSL (外部用户组) **8**-70
WebTrends **3**-74, **3**-99
定义 **1**-A-XIV
加密 **3**-99, **3**-107
消息 **3**-99
WebUI **3**-3, **3**-37, **3**-38
帮助文件 **3**-4
约定 **1**-xxxvi, **2**-ix, **3**-vii, **5**-vii, **6**-ix, **7**-v, **8**-v, **9**-v, **10**-v
WinNuke 攻击 **4**-73
WINS
定义 **1**-A-XIV
L2TP 设置 **5**-308
Work 区段 **2**-47
外部邻接路由器 **1**-A-XIV
外部网，定义 **1**-A-XIV
完全正向保密
请参阅 PFS
网关
路由 **1**-A-VI
网关 (路由器) **1**-A-XIV
网络，带宽 **2**-342
网络层可达到性信息 **1**-A-XIV
网络地址转换 (NAT) **3**-134
网络掩码 **2**-301
定义 **1**-A-XIV, **1**-A-XVII
用途 **2**-65
未标记的接口 **2**-400
未知单播选项 **2**-107– **2**-113
ARP **2**-110– **2**-113
泛滥 **2**-108– **2**-109
trace-route **2**-110, **2**-113
未知协议 **4**-212
无级路由 **1**-A-XV

X

XAuth
auth 和地址 **8**-97
bypass-auth **8**-82
本地用户 auth **8**-85
本地用户组 auth **8**-87
查询远程设置 **8**-82
地址超时 **8**-83
地址分配 **8**-81, **8**-83
定义 **1**-A-XV
IP 地址生存期 **8**-83– **8**-84
客户端认证 **8**-103
ScreenOS 作为客户端 **8**-103
生存期 **8**-84
TCP/IP 分配 **8**-82
VPN 监控 **5**-358
VPN 空闲时间 **8**-84
外部 auth 服务器查询 **8**-82
外部用户 auth **8**-89
外部用户组 auth **8**-92
虚拟适配器 **8**-81
已定义 **8**-81
用户认证 **8**-81
XAuth 用户 **8**-81– **8**-103
服务器支持 **8**-16
认证点 **8**-2
与 L2TP **8**-5
系统，参数 **2**-357– **2**-446
系统日志 **3**-74
安全设备 **3**-98, **3**-111, **3**-122
定义 **1**-A-XV
端口 **3**-98, **3**-111, **3**-122
加密 **3**-107
设备 **3**-98, **3**-111, **3**-122
消息 **3**-97
主机 **3**-97
主机名称 **3**-98, **3**-99, **3**-111, **3**-122
系统时钟 **2**-443– **2**-447
日期和时间 **2**-443
时区 **2**-443
与客户端同步 **2**-443
下一跳跃
定义 **1**-A-XV
消息
错误 **3**-75
关键 **3**-75
紧急 **3**-75
警告 **3**-75
警示 **3**-75
调试 **3**-75
通知 **3**-75
WebTrends **3**-99
信息 **3**-75
协议
CHAP **5**-305
NRTP **10**-34, **10**-156
NSRP **10**-1, **10**-137
PAP **5**-305
PPP **5**-303
VRRP **10**-122, **10**-159
协议散布
向 NSM 报告 **3**-31
协议异常 **4**-152
ALG **4**-149
基本网络协议 **4**-147
即时消息应用程序 **4**-148
P2P 应用程序 **4**-148
配置参数 **4**-192
支持的协议 **4**-147– **4**-150
信息流
分类，基于 IP **9**-33
分类，基于 VLAN **9**-21
计数 **2**-309
记录 **2**-309
整形 **2**-342
直通信息流， vsys 分类 **9**-11– **9**-13
信息流整形 **1**-xxix, **2**-341– **2**-355
服务优先级 **2**-349
接口要求 **2**-342
自动 **2**-342
许可密钥 **2**-437– **2**-438
虚拟 HA 接口 **2**-55, **10**-48
虚拟 IP
请参阅 VIP

虚拟安全接口
请参阅 VSI
虚拟安全设备组
请参阅 VSD 组
虚拟链接
定义 **1**-A-XV
虚拟路由器
请参阅 VR
虚拟适配器 **8**-81
定义 **1**-A-XV
虚拟系统 **2**-11, **9**-1– **9**-39
admin **9**-iii, **9**-1
admin 类型 **9**-3
重叠地址范围 **9**-25, **9**-34
重叠子网 **9**-25
创建 Vsys 对象 **9**-3
导出物理接口 **9**-19
导入物理接口 **9**-18
定义 **1**-A-XV
负载共享 **10**-130
更改 admin 的密码 **9**-3, **9**-38
共享 VR **9**-15
共享区段 **9**-15
故障切换 **10**-130
管理员 **3**-45
基本功能要求 **9**-3
基于 IP 的信息流分类 **9**-33– **9**-37
基于 VLAN 的信息流分类 **9**-21– **9**-32
接口 **9**-8
MIP **9**-10
NSRP **10**-130
区段 **9**-7
软件密钥 **9**-15
透明模式 **9**-22
VIP **9**-10
VR **9**-6
信息流分类 **9**-10– **9**-17
易管理性和安全性 **9**-34
只读 admin **3**-45
虚拟专用网
请参阅 VPN

Y

Yahoo! Messenger **4**-148
严格源路由 IP 选项 **4**-14, **4**-35– **4**-37
验证
IPSec **1**-A-XVI
以太网，已定义 **1**-A-XVI
映射 IP
请参阅 MIP
应用，策略中 **2**-303
应用程序层网关
请参阅 ALG
用户
多个管理用户 **3**-44
共享 IKE ID **5**-292– **5**-300
IKE **8**-76– **8**-80
IKE，组 **8**-79
组 IKE ID **5**-270– **5**-291
组，服务器支持 **8**-16
用户， admin **8**-3– **8**-4
auth 过程 **8**-4
超时 **8**-22
用户， IKE
定义 **8**-77
IKE ID **8**-76
组 **8**-76
用户， L2TP **8**-105– **8**-109
用户， XAuth **8**-81– **8**-103
有 FIN 但无 ACK 标志 **4**-18
优先级
定义 **1**-A-XVI
优先级排列 **2**-349
预共享密钥 **5**-9, **5**-231
域名系统
请参阅 DNS
远程认证拨号的用户服务
请参阅 RADIUS
源路由 **3**-135
约定
CLI **1**-xxxv, **2**-viii, **3**-vi, **4**-vi, **5**-vi, **6**-viii, **7**-iv, **8**-iv, **9**-iv, **10**-iv
插图 **1**-xxxviii, **2**-xi, **3**-ix, **4**-ix, **5**-ix, **6**-xi, **7**-vii, **8**-vii, **9**-vii, **10**-vii
名称 **1**-xxxix, **2**-xii, **3**-x, **4**-x, **5**-x, **6**-xii, **7**-viii, **8**-viii, **9**-viii, **10**-viii
WebUI **1**-xxxvi, **2**-ix, **3**-vii, **4**-vii, **5**-vii, **6**-ix, **7**-v, **8**-v, **9**-v, **10**-v
运行时认证 **2**-306, **8**-42

Z

zip 文件，封锁 **4**-202
Zombie 代理 **4**-39, **4**-41
侦查 **4**-7– **4**-37
地址扫描 **4**-8
端口扫描 **4**-10
FIN 扫描 **4**-22
IP 选项 **4**-12
设置 SYN 和 FIN 标志 **4**-16
无标志的 TCP 数据包 **4**-20
针孔 **2**-201
证书 **5**-10
本地 **5**-30
CA **5**-26, **5**-30
撤消 **5**-29, **5**-44
加载 **5**-34
申请 **5**-31
通过电子邮件 **5**-30
支持证书 **2**-441, **2**-442
执行对象
请参阅 RTO
质询握手认证协议
请参阅 CHAP
中继端口 **9**-23
定义 **1**-A-XVI
手动设置 **9**-22
已定义 **9**-22
主动调整时间 **4**-44– **4**-46
已定义 **1**-A-XVI
状态式检查 **4**-3
状态式签名 **4**-151
定义 **4**-151
自动密钥 IKE VPN **3**-58, **3**-108, **5**-9
管理 **5**-9
字符类型，ScreenOS 支持的 **1**-xxxix, **2**-xii, **3**-x, **4**-x, **5**-x, **6**-xii, **7**-viii, **8**-viii, **9**-viii, **10**-viii
子接口 **2**-4, **9**-23
创建 (根系统) **2**-70
创建 (vsys) **9**-23
定义 **9**-25
各 vsys 上的多个子接口 **9**-23
配置 (vsys) **9**-23
删除 **2**-71
已定义 **1**-A-XVII
子网掩码
定义 **1**-A-XVII

资源恢复日志 **3**-91
自治系统
已定义 **1**-A-XVII
自治系统边界路由器 **1**-A-XVII
自治系统路径 **1**-A-XVII
组
地址 **2**-142
服务 **2**-263
组 IKE ID
预共享密钥 **5**-283– **5**-291
证书 **5**-271– **5**-282
组 IKE ID 用户 **5**-270– **5**-291
预共享密钥 **5**-283
证书 **5**-271
组表达式 **8**-6– **8**-13
服务器支持 **8**-16
其它组表达式 **8**-7
用户 **8**-6
用户组 **8**-6
运算符 **8**-6
组播
策略 **6**-202
地址 **6**-194
反向路径转发 **6**-195
分布树 **6**-251
静态路由 **6**-198
路由表 **6**-196
组播策略
IGMP **6**-225
组播路由
IGMP **6**-205
PIM **6**-247