

NetScreen 概念与范例

ScreenOS 参考指南

第 1 卷：概述

ScreenOS 4.0.0

编号 093-0519-000-SC

版本 F

Copyright Notice

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies. Information in this document is subject to change without notice.

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

NetScreen Technologies, Inc.
350 Oakmead Parkway
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

第 1 卷：概述

目录.....	i
前言.....	xv
NetScreen 文档.....	xvii
概念与范例组织.....	xviii
约定.....	xxi
WebUI 导航约定.....	xxi
范例: Objects > Addresses > List > New.....	xxi

CLI 约定.....	xxii
相关性定义符.....	xxii
嵌套的相关性.....	xxii
CLI 命令及功能的可用性.....	xxiii

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
WebUI 导航约定.....	viii
范例: Objects > Addresses > List > New.....	viii
CLI 约定.....	ix
相关性定义符.....	ix
嵌套的相关性.....	ix
CLI 命令及功能的可用性.....	x
NetScreen 文档.....	xi

第 1 章 ScreenOS 体系结构.....	1
多个安全区段.....	2
安全区段接口.....	3
物理接口.....	3
子接口.....	4
虚拟路由器.....	5
路由重新分配.....	6
策略.....	7
VPN.....	8
虚拟系统.....	10
封包流序列.....	11

范例（第 1 部分）：具有六个区段的企业.....	14
范例（第 2 部分）：六个区段的接口.....	16
范例（第 3 部分）：具有两个路由选择域的企业 ...	20
范例（第 4 部分）：具有六个区段的企业 所用的策略.....	22
第 2 章 区段.....	29
安全区段	32
Global 区段.....	32
防火墙选项	33
范例：SYN 泛滥攻击.....	40
通道区段	45
配置安全区段和通道区段.....	46
创建区段	46
修改区段	47
删除区段	48
功能区段	49
Null 区段.....	49
MGT 区段	49
HA 区段	49
Self 区段	49
第 3 章 路由和虚拟路由器.....	51
路由选择过程	52
路由表	56
路由选择协议	57
路由度量	57
路由优选级	57
CLI 中的环境相关命令	58
命令的级别	58
在根级执行命令	58
在环境级执行命令	59
NetScreen 设备上的虚拟路由器	61
配置虚拟路由器	61
范例：创建自定义虚拟路由器	62
范例：修改虚拟路由器	63
范例：将虚拟路由器绑定到区段	63
范例：移除虚拟路由器	64
路由表.....	65
路由表配置	65
范例：配置路由表	67
范例：设置通过通道接口到达远程网络的路由	72
路由重新分配	74
配置路由图	74
范例：路由图创建	75
路由导出和导入	76
范例：移除路由导出规则	77
范例：创建路由导入规则	77
范例：删除路由导入规则	78
配置访问列表	79
范例：访问列表配置	79
设置路由优选级	80
范例：设置路由优选级	80
第 4 章 接口	81
接口类型	83
安全区段接口	83
物理.....	83
子接口	83
聚合接口	84

冗余接口	84
虚拟安全接口	84
功能区段接口	85
管理接口	85
HA 接口	85
通道接口	86
查看接口	87
接口表	87
配置安全区段接口	89
将接口绑定到安全区段	89
范例：绑定接口	89
为 L3（第 3 层）安全区段接口定义地址	90
公开 IP 地址	90
私有 IP 地址	91
范例：编址接口	92
从安全区段解除接口绑定	93
范例：解除接口绑定	93
修改接口	94
范例：修改接口上的设置	94
创建子接口	95
范例：在根系统中创建子接口	95
删除子接口	96
范例：删除安全区段接口	96
二级 IP 地址	97
二级 IP 地址属性	97
范例：创建二级 IP 地址	98
映射 IP 地址	99
MIP 和 Global 区段	100
范例：将 MIP 添加到 Untrust 区段接口	101

范例：从不同区段到达 MIP	104
范例：将 MIP 添加到 Tunnel 接口	109
MIP-Same-as-Untrust	110
范例：Untrust 接口上的 MIP	111
虚拟 IP 地址	113
VIP 和 Global 区段	115
范例：配置虚拟 IP 服务器	115
范例：编辑 VIP 配置	117
范例：移除 VIP 配置	118
范例：具有定制和多端口服务的 VIP	118
动态 IP 地址	125
端口地址转换	126
范例：创建带有 PAT 的 DIP 池	126
范例：修改 DIP 池	128
扩展接口和 DIP	129
范例：在不同子网中使用 DIP	129
DIP 组	137
范例：DIP 组	139
附着 DIP 地址	141
第 5 章 接口模式	143
透明模式	144
接口设置	145
VLAN1 接口	145
VLAN1 区段	145
未知 Unicast 选项	146
泛滥方法	147
ARP/Trace-Route 方法	148
范例：定义 VLAN1 接口	152
范例：透明模式	155

NAT 模式	160
接口设置	162
范例：NAT 模式	163
路由模式	167
接口设置	168
范例：路由模式	169
基于策略的 NAT	173
网络信息流的基于策略的 NAT	173
范例：外向网络信息流上的 NAT	174
第 6 章 为策略构建块	177
地址	178
地址条目	179
范例：添加地址	179
范例：修改地址	180
范例：删除地址	181
地址组	181
范例：创建地址组	183
范例：编辑组地址条目	184
范例：移除地址组成员和组	185
服务	186
范例：查看服务簿	187
范例：添加定制服务	188
范例：修改定制服务	189
范例：移除定制服务	190
IP 语音通信的 H.323 协议	190
范例：Trust 区段中的关守设备 （透明或路由模式）	191
范例：Trust 区段中的关守设备（NAT 模式）	193
范例：Untrust 区段中的关守设备 （Trust 区段处于透明或路由模式）	199
范例：Untrust 区段中的关守设备 （Trust 区段处于 NAT 模式）	201
服务组	206
范例：创建服务组	207
范例：修改服务组	208
范例：移除服务组	209
时间表	210
范例：循环时间表	210
第 7 章 策略	215
基本元素	216
三种类型的策略	217
区段间策略	217
区段内部策略	218
全局策略	218
策略组列表	219
策略定义	220
策略和规则	220
策略的结构	221
区段	222
地址	222
服务	222
动作	223
VPN 通道确定	223
L2TP 通道确定	224
定位在顶部	224
网络地址转换 (NAT)	224
用户认证	225
HA 会话备份	227
记录	227
计数	227
信息流报警临界值	228

时间表.....	228	SecurID.....	260
信息流整形.....	228	SecurID Auth 服务器对象属性.....	261
策略应用.....	230	支持的用户类型和功能.....	261
查看策略.....	230	LDAP.....	262
策略图标.....	230	LDAP Auth 服务器对象属性.....	263
创建策略.....	231	支持的用户类型和功能.....	263
策略位置.....	231	定义 Auth 服务器对象.....	264
范例：区段间策略.....	232	范例：为 RADIUS 定义 Auth 服务器对象.....	264
范例：区段间策略设置.....	233	范例：为 SecurID 定义 Auth 服务器对象.....	267
范例：区段内部策略.....	241	范例：为 LDAP 定义 Auth 服务器对象.....	269
范例：全局策略.....	244	定义缺省 Auth 服务器.....	271
修改和禁用策略.....	245	范例：更改缺省 Auth 服务器.....	271
重新排序策略.....	246	认证类型及应用.....	273
移除策略.....	247	Auth 用户和用户组.....	274
第 8 章 用户认证.....	249	在策略中引用 Auth 用户.....	274
认证服务器.....	250	在策略中引用 Auth 用户组.....	277
本地数据库.....	252	范例：运行时认证（本地用户）.....	278
支持的用户类型和功能.....	252	范例：运行时认证（本地用户组）.....	281
范例：设置本地数据库超时.....	253	范例：运行时认证（外部用户）.....	284
外部 Auth 服务器.....	254	范例：运行时认证（外部用户组）.....	287
Auth 服务器对象属性.....	255	范例：WebAuth（本地用户组）.....	291
Auth 服务器类型.....	257	范例：WebAuth（外部用户组）.....	294
RADIUS.....	257	范例：WebAuth + SSL（外部用户组）.....	298
RADIUS Auth 服务器对象属性.....	258	IKE 用户和用户组.....	303
支持的用户类型和功能.....	258	范例：定义 IKE 用户.....	304
NetScreen 词典文件.....	259	范例：创建 IKE 用户组.....	306
		在网关中引用 IKE 用户.....	307
		XAuth 用户和用户组.....	308
		在网关中引用 XAuth 用户.....	308

范例：XAuth 认证（本地用户）.....	310
范例：XAuth 认证（本地用户组）.....	312
范例：XAuth 认证（外部用户）.....	314
范例：XAuth 认证（外部用户组）.....	317
范例：XAuth 认证和地址分配（本地用户组）.....	322
手动密钥用户和用户组	328
范例：手动密钥用户.....	329
范例：手动密钥用户组	332
L2TP 用户和用户组	335
范例：本地和外部 L2TP Auth 服务器	336
Admin 用户	340
多类型用户	342
组表达式	343
范例：组表达式 (AND).....	345
范例：组表达式 (OR).....	347
范例：组表达式 (NOT)	349
标题自定义.....	351
范例：自定义 WebAuth 成功消息	351
第 9 章 信息流整形	353
应用信息流整形.....	354
在策略级管理带宽	354
范例：信息流整形	355
设置服务优先级.....	361
范例：优先级排列	362

第 10 章 系统参数	369
域名系统支持	370
DNS 查找.....	371
DNS 状态表	372
范例：定义 DNS 服务器地址并安排查找计划	373
DHCP	374
DHCP 服务器	376
范例：NetScreen 设备作为 DHCP 服务器	377
DHCP 中继代理.....	382
范例：NetScreen 设备作为 DHCP 中继代理.....	383
DHCP 客户端	387
范例：NetScreen 设备作为 DHCP 客户端	387
TCP/IP 设置传播.....	389
范例：转发 TCP/IP 设置.....	390
PPPoE.....	392
范例：设置 PPPoE	392
URL 过滤配置.....	396
下载 / 上传设置和软件	398
保存和导入设置	398
上传和下载软件	400
许可密钥	401
范例：扩大用户容量	402
系统时钟	403
范例：设置系统时钟	403
索引	IX-I

第 3 卷：管理

目录.....	i
前言.....	iii
约定	iv
WebUI 导航约定	iv
范例：Objects > Addresses > List > New	iv
CLI 约定.....	v
相关性定义符	v
嵌套的相关性	v
CLI 命令及功能的可用性.....	vi
NetScreen 文档.....	vii
第 1 章 管理.....	1
管理方法及工具.....	2
Web 用户界面	3
WebUI 导航级别图.....	4
WebUI 帮助	7
HTTP	8
安全套接字层	9
命令行界面	11
Telnet.....	11
安全命令外壳	13
范例：SCS 使用 PKA 进行自动登录	16
串行控制台	17
NetScreen-Global PRO	18
范例：设置 NACN	21

管理接口选项	25
管理的级别	27
根管理员	27
可读 / 写管理员	27
只读管理员	28
虚拟系统网络管理员	28
虚拟系统只读管理员	28
定义 Admin 用户	29
范例：添加只读 Admin	29
范例：修改 Admin	30
范例：删除 Admin	30
保证管理流量的安全.....	31
更改端口号	32
范例：更改端口号	32
更改 Admin 登录名和密码.....	33
范例：更改 Admin 用户的登录名和密码.....	34
范例：更改自己的密码.....	35
重置设备到出厂缺省设置	36
限制管理访问	37
范例：限制对单一工作站的管理.....	37
范例：限制对子网的管理	38
管理 IP	39
范例：设置多个接口的管理 IP	39
管理区段接口	42
范例：通过 MGT 接口进行管理	42

虚拟专用网	43
范例: 通过 IPSec 通道发送 SNMP 和 系统日志报告	44
范例: 从 Trust 区段通过 VPN 通道进行管理	49
第 2 章 监控 NetScreen 设备	55
存储日志信息	56
事件日志	57
查看事件日志	58
范例: 下载关键事件的事件日志	59
信息流日志	60
范例: 下载信息流日志	61
SELF 日志	62
范例: 下载 Self 日志	62
系统日志	63
WebTrends	63

范例: 启用通知事件的系统日志和 WebTrends	64
SNMP	66
执行概述	68
范例: 设置 SNMP 公共组	69
VPN 监控	71
计数器	74
范例: 查看屏幕和流量计数器	80
资源恢复日志	81
范例: 下载“系统恢复日志”	81
流量报警	82
范例: 基于策略的入侵检测	83
范例: 折衷系统通知	84
范例: 发送电子邮件警示	86
附录 A SNMP MIB 文件	A-I
索引	IX-I

第 4 卷: VPN

目录	i
前言	v
约定	vi
WebUI 导航约定	vi
范例: Objects > Addresses > List > New	vi
CLI 约定	vii
相关性定义符	vii
嵌套的相关性	vii

CLI 命令及功能的可用性	viii
NetScreen 文档	ix
第 1 章 IPSec	1
VPN 的简介	2
IPSec 概念	3
模式	4
传送模式	4
通道模式	5

协议	7	范例: 加载证书和 CRL	34
AH	7	范例: 为 CA 证书配置 CRL 设置	36
ESP	8	自动获取本地证书	38
密钥管理	9	范例: 自动申请本地证书	39
手动密钥	9	使用 OCSP 检查撤消	43
自动密钥 IKE	9	配置 OCSP	43
安全联盟	10	指定 CRL 或 OCSP 以用于撤消检查	44
通道协商	11	显示证书撤消状态属性	44
第 1 阶段	11	指定证书的“OCSP 响应方” URL	44
Main mode / Aggressive mode		删除证书撤消检查属性	45
(主模式和主动模式)	12	第 3 章 基于路由的 VPN	47
Diffie-Hellman 交换	13	通道接口	48
第 2 阶段	13	范例: 绑定到通道接口的通道	49
完全正向保密	14	删除通道接口	57
回放攻击保护	14	范例: 删除通道接口	57
封包流: 基于策略的 LAN 到 LAN VPN	15	LAN 到 LAN 的 VPN	58
IPSec NAT 穿透	17	范例: 基于路由的 LAN 到 LAN 的 VPN,	
穿透 NAT 设备	18	手动密钥	59
UDP 校验和	19	范例: 基于路由的 LAN 到 LAN 的 VPN,	
激活频率值	19	自动密钥 IKE	70
IPSec NAT 穿透和发起方 / 响应方对称	20	范例: 基于路由的 LAN 到 LAN 的 VPN,	
范例: 启用 NAT 穿透	21	动态对等方	76
第 2 章 公开密钥密码术	23	拨号到 LAN 的 VPN, 动态对等方	92
公开密钥密码术简介	24	范例: 基于路由的拨号到 LAN 的 VPN,	
PKI	26	动态对等方	93
证书和 CRL	29	集中星型 VPN	103
手动获取证书	30	范例: 集中星型 VPN	104
范例: 手动申请证书	31	背对背的 VPN	111
		范例: 背对背的 VPN	112

第 4 章 基于策略的 VPN	123
LAN 到 LAN 的 VPN	124
通道接口	125
范例: 基于策略的 LAN 到 LAN 的 VPN, 手动密钥	127
范例: 基于策略的 LAN 到 LAN 的 VPN, 自动密钥 IKE	136
范例: 基于策略的 LAN 到 LAN 的 VPN, 动态对等方	142
拨号到 LAN 的 VPN	156
范例: 基于策略的拨号到 LAN 的 VPN, 手动密钥	157
范例: 基于策略的拨号到 LAN 的 VPN, 自动密钥 IKE	163
范例: 基于策略的拨号到 LAN 的 VPN, 动态对等 ..	171
组 IKE ID	180
具有证书的组 IKE ID	181
通配符和容器 ASN1-DN IKE ID 类型	183
范例: 组 IKE ID (证书)	186
具有预共享密钥的组 IKE ID	193
范例: 组 IKE ID (预共享密钥)	195

Tunnel 区段和基于策略的 NAT	202
范例: 具有 MIP 和 DIP 的 Tunnel 接口	204
冗余 VPN 网关	213
VPN 组	214
监控机制	215
IKE 心跳信号	215
IKE 恢复过程	216
TCP SYN 标记检查	219
范例: 冗余 VPN 网关	220
第 5 章 L2TP (Layer 2 Tunneling Protocol, 第 2 层通道协议)	233
L2TP 简介	234
封包的封装和解封	238
封装	238
解封	239
L2TP 参数	240
范例: 配置 IP 池和 L2TP 缺省设置	241
L2TP 和 IPSec 上的 L2TP	243
范例: 配置 L2TP	244
范例: 配置 IPSec 上的 L2TP	250
索引	IX-I

第 5 卷：动态路由

目录.....	i
前言.....	v
约定.....	vi
WebUI 导航约定.....	vi
范例：Objects > Addresses > List > New.....	vi
CLI 约定.....	vii
相关性定义符.....	vii
嵌套的相关性.....	vii
CLI 命令及功能的可用性.....	viii
NetScreen 文档.....	ix
第 1 章 OSPF 任务参考.....	1
OSPF 概述.....	3
区域.....	3
路由器分类.....	4
Hello 协议.....	5
网络类型.....	5
广播网络.....	5
非广播网络.....	6
点对点网络.....	6
链接状态通告.....	7
NetScreen 设备上的 OSPF.....	8
VPN 通道上的 OSPF 支持.....	8
OSPF 认证.....	8
OSPF 接口特征.....	9

OSPF 命令.....	10
OSPF 环境启动.....	10
基本 OSPF 配置任务.....	11
在虚拟路由器级启用 OSPF 实例.....	11
范例：启动 OSPF 实例.....	11
移除 OSPF 虚拟路由实例.....	12
范例：禁用 OSPF.....	12
创建 OSPF 区域.....	13
范例：创建 OSPF 区域.....	13
指定到区域的接口.....	14
范例：为 OSPF 区域指定接口.....	14
重新分配路由.....	15
范例：将 BGP 路由重新分配到 OSPF 中.....	16
OSPF 接口配置.....	17
显示 OSPF 接口详细信息.....	17
范例：显示 OSPF 接口信息.....	17
在接口上设置明文密码.....	18
范例：配置明文密码认证方法.....	18
在接口上设置 MD5 密码.....	19
范例：配置 MD5 密码认证方法.....	19
为 OSPF 接口设置开销值.....	20
范例：为 OSPF 接口配置开销.....	20
为 OSPF 接口设置不工作间隔.....	21
范例：配置不工作间隔.....	21
为 OSPF 接口设置 Hello 间隔.....	22
范例：配置 Hello 间隔.....	22

为 OSPF 接口设置 Neighbor List（邻接方列表）.....	23	OSPF 信息	35
范例：配置 Neighbor List（邻接方列表）.....	23	显示 OSPF 路由实例的统计信息.....	35
为 OSPF 接口设置重新传输间隔	24	范例：显示 OSPF 统计信息	35
范例：配置重新传输间隔.....	24	显示重新分配条件的详细信息	37
在 OSPF 接口上设置优先级值.....	25	范例：显示重新分配条件	37
范例：配置优先级值.....	25	显示已重新分配路由的详细信息	38
在 OSPF 接口上设置传输延迟值	26	范例：显示已重新分配路由的详细信息	38
范例：配置传输延迟.....	26	显示 OSPF 数据库中的对象.....	39
OSPF 虚拟链接配置	27	范例：显示 OSPF 数据库对象.....	39
创建虚拟链接	27	显示剩余区域详细信息	40
范例：创建到中枢区域的虚拟链接.....	27	范例：显示剩余区域详细信息	40
自动创建虚拟链接	28	显示 OSPF 配置	41
范例：创建自动虚拟链接.....	28	范例：列出 OSPF 配置命令	41
为虚拟链接创建消息整理	29	其它 OSPF 配置	42
范例：创建使用 MD5 认证的虚拟链接.....	29	将 OSPF 绑定到通道接口	42
为虚拟链接创建明文密码.....	30	范例：将通道绑定到 OSPF 路由实例	42
范例：创建具有明文密码的虚拟链接	30	通告所有区域中的缺省路由	43
为虚拟链接邻接方创建不工作间隔	31	范例：通告缺省路由	43
范例：配置虚拟链接邻接方不工作间隔.....	31	配置汇总路由	44
为虚拟链接创建 Hello 间隔	32	范例：汇总重新分配的路由.....	45
范例：配置虚拟链接 Hello 间隔.....	32	移除缺省路由	46
为虚拟链接创建重新传输间隔	33	范例：从路由表移除缺省路由	46
范例：配置虚拟链接重新传输间隔.....	33	设置区域范围	47
为虚拟链接配置传输延迟值	34	范例：配置区域范围	47
范例：配置虚拟链接传输延迟.....	34	设置 Hello 泛滥攻击临界值.....	48
		范例：配置 Hello 临界值.....	48
		设置 LSA 临界值	49
		范例：配置 LSA 临界值	49

配置 RFC-1583 环境	50	范例：忽略缺省路由通告	66
范例：改变到 RFC-1583 环境	50	高级 BGP 配置任务	67
第 2 章 BGP 任务参考	51	将路由图应用到来自指定邻接方的路由	67
BGP 命令	53	范例：应用路由图	67
启动环境	53	为路径指定 Weight（权）	68
基本 BGP 命令介绍	54	范例：指定权值	68
基本 BGP 配置任务	57	设置 AS 路径访问列表	69
创建虚拟路由器的 BGP 实例	57	范例：创建 AS 路径访问列表中的条目	69
范例：启动虚拟路由实例	57	配置公共组列表	70
指定从 AS 可到达的网络	58	范例：创建公共组列表	70
范例：创建从本地虚拟路由器可到达的网络	58	设置本地优先	73
启用聚合路由	59	范例：设置本地优先	73
范例：创建聚合路由条目	59	设置多出口点识别器 (MED)	74
启用重新分配	60	范例：设置 MED	74
范例：创建重新分配规则	60	设置多出口点识别器 (MED) 比较	75
配置 BGP 邻接方	61	范例：设置 MED 比较	75
范例：配置邻接方的虚拟路由器	61	配置路由反射器	76
启用带有 IP 地址的 BGP 对等方	62	范例：指定路由反射器	76
范例：启用 BGP 对等方连接	62	将邻接方设置为路由反射器客户机	77
配置等待时间计时器	63	范例：配置 IBGP 邻接方	77
范例：设置等待时间值	63	配置联合	78
配置 Keepalive 计时器	64	范例：创建联合	78
范例：设置 Keepalive 计时器	64	添加 AS 成员到联合中	79
启用路由 Flap 衰减	65	范例：添加新联合	79
范例：启用 Flap 衰减	65	索引	IX-I
废除来自对等路由器的缺省路由通告	66		

第 6 卷：虚拟系统

目录.....	i
前言.....	iii
约定.....	iv
WebUI 导航约定.....	iv
范例：Objects > Addresses > List > New.....	iv
CLI 约定.....	v
相关性定义符.....	v
嵌套的相关性.....	v
CLI 命令及功能的可用性.....	vi
NetScreen 文档.....	vii
第 1 章 虚拟系统.....	1
创建 Vsys 对象.....	3
范例：创建 Vsys 对象和 Vsys Admin.....	3
虚拟路由器.....	6
区段.....	7
接口.....	7
通信流分类.....	9
发往 NetScreen 设备的通信流.....	9
直通信息.....	10

专用和共享接口.....	12
专用接口.....	12
共享接口.....	12
导入和导出物理接口.....	15
范例：将物理接口导入到虚拟系统.....	15
范例：从虚拟系统导出物理接口.....	16
基于 VLAN 的通信流分类.....	17
VLAN.....	18
定义子接口和 VLAN 标记.....	19
范例：定义三个子接口和 VLAN 标记.....	21
VLAN 之间的通信.....	24
范例：VLAN 间的通信.....	24
基于 IP 的通信流分类.....	28
范例：配置基于 IP 的通信流分类.....	30
以 Vsys Admin 身份登录.....	33
范例：登录并更改密码.....	33
索引.....	IX-I

第 7 卷 : NSRP

目录.....	i
前言.....	iii
约定.....	iv
WebUI 导航约定.....	iv
范例: Objects > Addresses > List > New.....	iv
CLI 约定.....	v
相关性定义符.....	v
嵌套的相关性.....	v
CLI 命令及功能的可用性.....	vi
NetScreen 文档.....	vii
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.....	15
集群名称.....	17
范例: 创建 NSRP 集群.....	18
执行对象.....	21
RTO 镜像状态.....	22
VSD 组.....	23
抢先选项.....	23
VSD 组成员状态.....	24
心跳信号消息.....	25
范例: 创建两个 VSD 组.....	26

VSI 和静态路由.....	28
范例: Trust 和 Untrust 区段 VSI.....	29
配置、文件和 RTO 同步.....	33
同步配置.....	33
同步文件.....	34
同步 RTO.....	34
范例: 手动重新同步 RTO.....	35
范例: 将设备添加到活动的 NSRP 集群.....	36
冗余接口.....	37
双 HA 接口.....	37
控制消息.....	38
数据消息 (封包交换).....	39
安全区段冗余接口.....	41
范例: 为 VSI 创建冗余接口.....	42
设置过程.....	47
全网状配置的电缆连接.....	47
NSRP 配置.....	51
范例: 双主动配置的 NSRP.....	51
虚拟系统支持.....	60
范例: 虚拟系统间负载共享的 VSI.....	60
路径监控.....	68
设置临界值.....	69
对跟踪的 IP 地址加权.....	69
范例: 配置路径跟踪.....	70
索引.....	IX-I

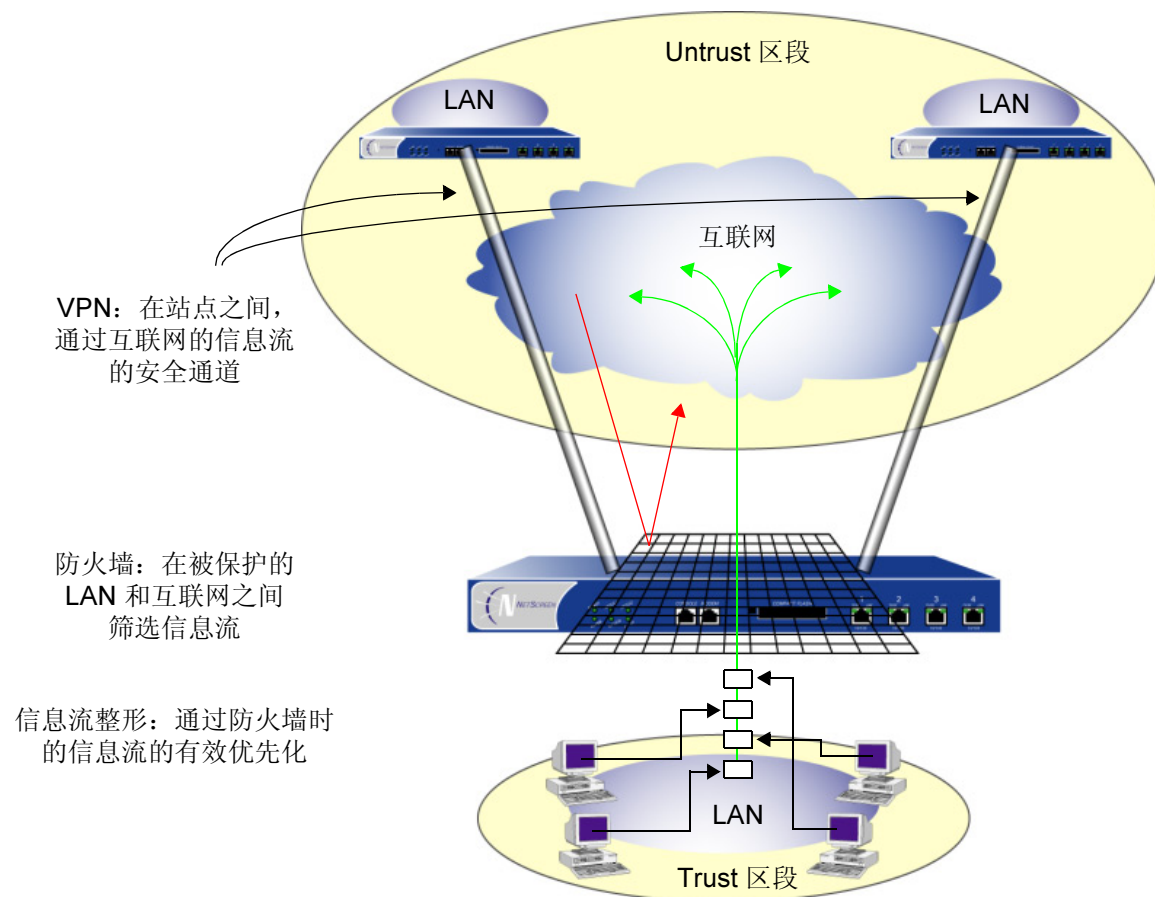
前言

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) 或隔离区段 (DMZ) 提供灵活的保护。

- **防火墙：**防火墙筛选通过专用 LAN 和公用网（如互联网）之间边界的信息流。
- **VPN：**VPN 提供一个在两个或多个远程网络装置之间的安全通道。
- **信息流整形：**信息流整形功能允许对通过 NetScreen[®] 防火墙的信息流进行管理监控和控制，来维护网络的服务质量 (QoS) 级别。

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 文档 CD-ROM 上适用于各个平台的 NetScreen Cryptographic Module Security Policy 文档。

1. “互联网计算机安全联盟” (ICSA) 是一个组织，它致力于连接到互联网上公司的所有类型的网络安全。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 和加密技术。ICSA 已经认证了 NetScreen 有关防火墙和 IPSec 的所有产品。



NetScreen ScreenOS 是这样的一个操作系统，它提供需要设置和管理任何 NetScreen 安全设备或系统的所有功能。
“*NetScreen 概念与范例 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。

NETSCREEN 文档

欲获得任何 NetScreen 产品的技术资料, 请浏览 www.netscreen.com/support/manuals.html。欲访问最新的 NetScreen 文档, 请参阅 **Current Manuals** 部分。欲从以前的版本中访问已存档的资料, 请参阅 **Archived Manuals** 部分。

欲获得 NetScreen 产品版本上的最新技术信息, 请参阅该版本的记录资料。欲获得版本注释, 请浏览 www.netscreen.com/support 并选定 **Software Download**。选定产品及其版本, 然后单击 **Go**。(欲执行此下载任务, 您必须是注册用户。)

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@netscreen.com

概念与范例组织

“*NetScreen 概念与范例 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 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 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 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 “USGA（Universal Security Gateway Architecture，通用安全网关体系结构）” 的基本元素，NetScreen ScreenOS 中的体系结构，同时用一个包含四部分的范例来举例说明一种基于企业的配置，该配置中结合了这些元素中的大部分。在本章及以后所有各章中，每个概念都附有说明性的范例。
- 第 2 章，“区段” 解释安全区段、通道区段和功能区段。
- 第 3 章，“路由和虚拟路由器” 介绍虚拟路由器的概念，并解释如何在 NetScreen 设备上配置虚拟路由器。它还包含有关路由表条目的信息。
- 第 4 章，“接口” 说明 NetScreen 设备上的各种物理的、逻辑的和虚拟的接口，而且包含各种防火墙攻击的信息，以及 NetScreen 提供的阻拦攻击选项。
- 第 5 章，“接口模式” 解释 “透明”、“网络地址转换” (NAT) 和 “路由器” 接口操作模式的概念。
- 第 6 章，“为策略构建块” 讨论有关创建策略和虚拟专用网 (VPN) 的各个元素：地址（包括 VIP 地址）、用户和服务。它还介绍了几个支持 H.323 协议的配置的范例。
- 第 7 章，“策略” 探究策略的组成及功能，而且给他们的创建和应用提供指导。

- 第 8 章，“用户认证”详述 NetScreen 支持的各种认证方法和用途。
- 第 9 章，“信息流整形”说明如何管理接口带宽、策略级别和优先化服务。
- 第 10 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)”去分配或传递 TCP/IP 设置；URL 过滤；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”说明本地和远程管理 NetScreen 设备的各种不同的可用方法。本章还解释了属于可被定义四个网络管理员级别中的每一个级别的权限。最后，它说明了如何确保本地和远程管理信息流的安全。
- 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，“VPN”

- 第 1 章，“IPSec”提供有关 IPSec 的背景信息，介绍一个以主动模式和主模式 IKE（因特网密钥交换）协商的“阶段 1”流序列，最后介绍了有关“NAT 穿透”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销列表 (CRL) 的信息。
- 第 3 章，“基于路由的 VPN”提供基于路由的 VPN 配置的多方面的范例，包括集中星型和背对背通道设计。
- 第 4 章，“基于策略的 VPN”提供有关基于策略的 VPN 配置的多方面的范例，这些配置是关于 LAN 到 LAN 和客户端到 LAN 的通信的，而这些通信使用“手动密钥”和“自动密钥”IKE 机制。它还详细说明了，如何使用通道接口，去提供基于策略的 NAT，这个 NAT 是有关通过站点之间的 VPN 通道的信息流的，在这些站点之间有使用一个重叠的地址空间的可信任网络。
- 第 5 章，“L2TP（Layer 2 Tunneling Protocol，第 2 层通道协议）”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 5 卷，“动态路由”

- 第 1 章，“OSPF 任务参考”介绍路由的基本原理、概念及路由如何适配安全设备（重点强调 **NetScreen** 设备）。
- 第 2 章，“BGP 任务参考”提供了基本路由概念和术语。

第 6 卷，“虚拟系统”

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

第 7 卷，“NSRP”

- 第 1 章，“**NSRP**”说明如何对冗余组中的 **NetScreen** 设备布线、配置和管理，以便提供使用“**NetScreen** 冗余协议 (**NSRP**)”的高可用性。

约定

本书介绍了配置 NetScreen 设备的两种管理方法: Web 用户界面 (WebUI) 和命令行界面 (CLI)。以下介绍这两种界面使用的约定。

WebUI 导航约定

本书中用一个尖角符号 (>) 来指示在 WebUI 中的导航, 其方法是单击菜单选项和链接。

范例: Objects > Addresses > List > New

为访问新的地址配置对话框, 请执行以下操作:

1. 在菜单栏中, 单击 **Objects**。
Objects 菜单选项展开, 显示出一个对象选项子菜单。
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, 显示出一个 Addresses 选项子菜单。
3. 单击 **List**。
出现通讯簿列表。
4. 在右上角单击 **New** 链接。
出现新的地址配置对话框。

CLI 约定

手册中每一条 CLI 命令的说明，都会介绍命令语法的某些方面。此语法可包括选项、开关、参数及其它功能。为了阐明语法规则，一些命令的说明使用 *相关性定义符*。这种定义符指出，哪些命令功能是强制性的，和适用于哪些环境中。

相关性定义符

每个语法说明使用特殊字符来显示命令功能之间的相关性。

- { 和 } 符号表示一个强制性的功能。包含在这些符号中的功能，对执行命令非常重要。
- [和] 符号表示一个任选功能。包含在这些符号中的功能，尽管省略它们可能使命令执行后得到相反的结果，但它们对命令执行并不重要。
- | 符号表示两个功能之间的一个“或”关系。当这个符号出现在同一行上的两个功能之间时，可使用两个功能中的任一个（但不能两个都使用）。当这个符号出现在行尾时，可使用该行上的功能，或下一行上的功能。

嵌套的相关性

多数 CLI 命令有 *嵌套* 的相关性，这使得功能在某些环境中是可以选择的，而在另一些环境中，则是强制性的。三个假设的功能显示如下，以对这种原则进行示范。

```
[ feature_1 { feature_2 | feature_3 } ]
```

定义符 [和] 包围整个子句。因此，可省略 **feature_1**、**feature_2** 和 **feature_3**，而且，还能成功地执行这条命令。可是，因为 { 和 } 定义符包围 **feature_2** 和 **feature_3**，所以如果包括了 **feature_1**，则必须包括 **feature_2** 或 **feature_3** 中的任一个。否则，将不能成功执行该命令。

以下范例说明一些 **set interface** 命令功能的相关性。

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

这个 { 和 } 括号说明指定的任一个 **flood** 或 **arp** 是强制性的。但是，[和] 括号说明，对于 **arp** 而言，**trace-route** 选项是非强制性的。因而，这条命令可以采取以下任一种格式：

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

CLI 命令及功能的可用性

用本手册中的语法说明执行 CLI 命令，可能发现某些命令及其功能对于您的 NetScreen 设备型号是无效的。

因为 NetScreen 设备将未提供的命令功能视为语法不当，所以，试图使用这样的功能，通常将产生 **unknown keyword** 错误信息。出现这个信息时，用 **?** 开关确认该功能的可用性。比如，以下命令列出了 **set vpn** 命令的可用选项：

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```


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 325 英尺（100 米），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封包。

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。

原子聚合: 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封包。

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。

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域对资源进行保护，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。

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。

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 发送方与其邻接方之间消息传输的时间长度。

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”。

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 来指封包、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。

防火墙: 是为信息流输入及提供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配备安全装置的专用计算机，也可以是基于软件的保护。

访问列表: 要限制路由器获悉或发出的路由信息，可根据发到或来自某一相邻路由器的路由更新信息进行过滤。过滤器由一个访问列表组成，该列表适用于发到或来自相邻路由器的更新信息。可按每个相邻路由器或每个对等组过滤路由信息。

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工作映射（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。

隔离区段 (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。

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

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。以太网就是广播网络中的一个范例。

动态过滤: 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: 获准将封包发送到当前路由域的一个 IP 地址列表。

Hello 间隔: “Hello 封包”实例之间的时间长度。

Hello 封包: 是通告信息（例如，它的存在与可用性）的封包，它将信息通告给生成封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** 使用 **IP** 的基本支持，似乎是更高级别的协议，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。

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：

表 0-1

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”表示网络编号位，“h”表示主机编号位，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 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。

Keep Alive: 两激活封包之间的时间长度（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: 封包在通过 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，使得封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。

局部优先级: 为了比“多出口区分符” (MED) 值为封包路径选择提供更好的信息，BGP 提供了一种称为 LOCAL_PREF 或局部优先级值的属性。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。

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 **LAN** 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。**LAN** 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，或以封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。

连接状态: 当发自某一路由器的封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。

联合体: **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。

邻接方: 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接方。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接方。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。

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**。

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封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。

路由图：路由图和 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。路由图包含一个路由图条目的列表，每个条目包含一个序列号、一个匹配项和一个设置值。路由图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图。找到匹配项后，路由图会执行对该条目的许可或拒绝操作。如果路由图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，可以阻拦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。

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。

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 LAN 或其它网络中，MAC 地址是计算机的唯一硬件编号（在以太网 LAN 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 LAN 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、认证、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。

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：一个区段可以是一个应用了安全措施的网络空间段（安全区段）、一个绑定了 VPN 通道接口的逻辑片段（通道区段），或者是一个执行特定功能的物理或逻辑实体（功能区段）。

区域：OSPF 是路由协议中最基本的排序方法。OSPF 区域将互连网络划分成更小、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它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。

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；将计算机连接到局域网 (LAN) 或电话机。

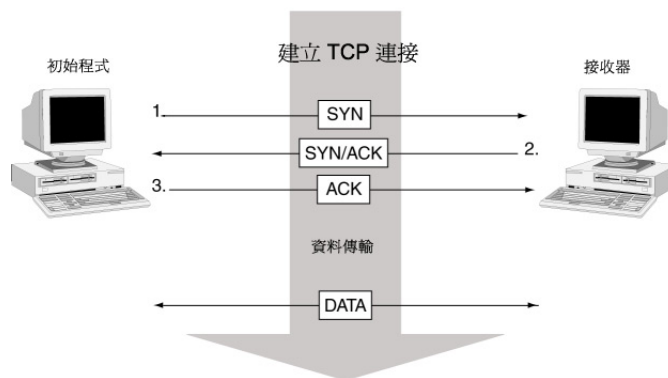
认证：认证可确保将数字数据传输到预定的接收方。认证还可向接收方确保信息及其来源（来自何处）的完整性。最简单的认证形式要求有获准访问特定帐户的用户名和密码。认证协议可以根据私有密钥加密，例如 DES 或 3DES，也可以根据使用数字签名的公开密钥系统进行加密。

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



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 - 密码块链 (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, 密文与明文进行“异或”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。

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: 通道接口是出口或入口, 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: 通道区段是安装有一个或多个通道接口的逻辑段。通道区段与作为其传输工具的安全区段相关联。

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。

通用安全网关体系结构 (USGA): 是一种 ScreenOS 体系结构, 提供管理员能自定义并绑定到预定义和用户定义的安全区段的通用接口。

统一资源定位 (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 语法为协议://地址。例如，<http://www.srl.rmit.edu.au/pd/index.html> 表明协议为 http 协议，地址是 www.srl.rmit.edu.au/pd/index.html。

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

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

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。

外部邻接路由器: 两个不同的自治系统中的两个对等 BGP 路由器。

网关: 驻留在当前路由域进入点的路由器，通常被称为缺省网关。

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、尽力而为的传输系统中。“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): 用于将安全 IP 地址从地址池中转换为临时的外部注册 IP 地址的标准。这允许具有秘密指定的 IP 地址的“可信”网络获得对互联网的访问权。它还意味着您不必为网络中的每一台机器都获取注册的 IP 地址。

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。

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封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。如果存在故障切换设备, 并且它成为新的主设备, 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: 不信任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。采用这种方法, 企业的远程办公人员和流动的专业人员可通过本地拨号访问企业网或另一“互联网服务提供商”。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。

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 技术的尽力而为的传输系统。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。

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重复检测时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。

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 (SA) 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, 并按封包的帧报头中的 VLAN 标识符 (VID) 对封包进行排序。

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封包。该组还使用外部网关协议 (**EGP**) 向其它 **AS** 发送封包。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。

索引

数字

100BaseT, 已定义 1-A-I

10BaseT, 已定义 1-A-I

3DES 4-8

A

ACL 4-16

Address Sweep Attack (地址扫描攻击) 2-36

admin 用户 2-340 – 2-341

auth 过程 2-341

超时 2-256

服务器支持 2-250

来自 RADIUS 的权限 2-340

AES (高级加密标准) 4-8

Aggressive mode (主动模式) 4-12

AH 4-3, 4-7

ARP 2-146, 7-58, 7-68

入口 IP 地址 2-148

ARP 广播 7-18

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

asset recovery log 3-81

attacks

ICMP fragments (ICMP 碎片) 2-36

large ICMP packets (大的 ICMP 封包) 2-36

SYN and FIN bits set

(SYN 和 FIN 位的封包) 2-35

SYN fragment (SYN 碎片) floods 2-35

unknown MAC addresses 2-44

auth 服务器 2-250

备份服务器 2-255

策略中 2-272

超时 2-255

地址 2-255

定义 2-264 – 2-272

对象名 2-255

对象属性 2-255

多种用户类型 2-251

功能支持 2-250

ID 号 2-255

IKE 网关中 2-272

LDAP 2-262 – 2-263

LDAP, 定义 2-269

类型 2-255

缺省 2-271

RADIUS 2-257 – 2-259

RADIUS, 定义 2-264

RADIUS, 用户类型支持 2-258

认证过程 2-254

SecurID 2-260 – 2-261

SecurID, 定义 2-267

外部 2-254

用户类型支持 2-250

最大数量 2-251

auth 用户 2-274 – 2-302

策略前 auth 2-276

策略前认证 2-226

策略中 2-274

超时 2-255

服务器支持 2-250

认证点 2-273

WebAuth 2-226, 2-276

WebAuth + SSL (外部用户组) 2-298

WebAuth (本地用户组) 2-291

WebAuth (外部用户组) 2-294

运行认证 2-275

运行时认证过程 2-225, 2-275

运行时 (本地用户组) 2-281

运行时 (本地用户) 2-278

运行时 (外部用户) 2-284

执行时认证 2-225

执行时 (外部用户组) 2-287

组 2-274, 2-277

安全联盟

请参阅 SA

安全联盟 (SA) 3-79

安全区段 2-2, 2-62

Global 2-2

接口 2-3, 2-83

目的区段确定 2-12

请参阅区段

物理接口 2-83

预定义的 2-2

源区段确定 2-12

子接口 2-83

安全区域 1-A-I

安全散列算法 1

请参阅 SHA-1

安全套接字层

请参阅 SSL

B

Bad IP Option（坏的 IP 选项） 2-37

BGP 1-A-I

AS 路径访问列表 5-54, 5-69

本地优先 5-55, 5-73

等待时间 5-55

等待时间计时器 5-63

多出口点识别器 (MED) 5-54, 5-56, 5-75

flap-damping 5-55

公共组列表 5-54

聚合 5-54, 5-59

Keepalive 计时器 5-64

Keepalive（激活） 5-55

可到达的网络 5-56, 5-58

联合 5-55, 5-78, 5-79

邻接方 5-56

路由反射器 5-56, 5-76, 5-77

路由图 5-67

启用对等方 5-55, 5-62

缺省路由 5-55

同步 5-56

通告 5-55

Weight 权 5-68

虚拟路由实例 5-57

重新分配 5-56

报警

临界值 2-228

本地数据库 2-252 – 2-253

超时 2-253

IKE 用户 2-303

支持的用户类型 2-252

本地证书 4-30

比特流 3-75

编辑

策略 2-245

地址组 2-184

区段 2-47

标题, 定制 2-351

不工作间隔 1-A-I

不信任 1-A-XI

C

CA 证书 4-26, 4-30

CHAP 2-323, 4-237, 4-240

CLI 3-11, 3-42

save 2-400

set arp always-on-dest 7-58

set traffic-shaping mode auto 2-360

set vip multi -port 2-114

CLI 约定 1-xxii, 2-ix, 3-v, 4-vii, 5-vii, 6-v, 7-v

CompactFlash 3-56

Console（控制台） 3-56

Container（容器） 4-185

CRL（证书撤消列表） 4-28, 4-43

加载 4-28

操作系统 3-11

策略 2-3, 2-7, 2-217

报警 2-228

策略组列表 2-219

查询顺序 2-219

deny 2-223

DIP 组 2-138

地址 2-222

地址组 2-222

定位在顶部 2-224, 2-246

定义 1-A-II

动作 2-223

服务簿 2-187

服务于 2-186, 2-222

服务组 2-206

根系统 2-220

更改 2-245

功能 2-215

管理 2-230

管理带宽 2-354

计数 2-227

进度表 2-228

L2TP 2-224

permit 2-223

区段间 2-219, 2-231, 2-232

区段内部 2-219, 2-231, 2-241

全局 2-219, 2-231, 2-244

认证 2-225

双向 VPN 2-223, 2-230, 4-128

顺序 2-246

通道 2-223

图标 2-230

VPN 拨号用户组 2-222

位置 2-231

信息流记录 2-227

虚拟系统 2-220

移除 2-247

重新排序 2-246

最大限制 2-182

差异服务 2-229

超时

admin 用户 2-256

auth 用户 2-255

超文本传输协议

请参阅 HTTP

串行电缆 3-17

创建

地址组 2-183

服务组 2-207

MIP 地址 2-101
密钥 3-9
区段 2-46
词典文件 2-259, 2-340
存取策略
 请参阅策略

D

DES 4-8
DES-CBC, 已定义 1-A-X
DES, 已定义 1-A-X
DHCP 2-164, 2-170, 2-392
 HA 2-376
 客户端 2-374
 中继代理 2-374
Diffie-Hellman 交换 4-13
Diffie-Hellman 组 4-13
DiffServ
 请参阅DS 码点标记
DIP 2-125 – 2-141, 2-168, 3-79
 池 2-224
 附着 DIP 2-141
 固定端口 2-127
 PAT 2-126
 修改 DIP 池 2-128
 组 2-137 – 2-140
DIP 池
 基于策略的 NAT 4-202 – 4-212
 扩展的接口 4-202
Distinguished name (识别名称) 2-263
DMZ, 定义 1-A-III
DN (识别名称) 4-180
DNS 2-370
 查找 2-371
 服务器 2-393
 L2TP 设置 4-240
 状态表 2-372
DoS 2-36
DS 码点标记 2-354, 2-364, 2-365
DSL 2-387, 2-393
带宽 2-228
 保障 2-228
 保证的 2-354, 2-362
 管理 2-354
 缺省优先级 2-361
 未限定最大值 2-354
 优先级 2-361
 优先级排列 2-361
 最大 2-228, 2-362
 最大规格 2-354
代理服务器 1-A-II
等待时间 1-A-II
登录
 vsys 6-28, 6-33
第 1 阶段 4-11
 提议 4-11
 提议, 预定义 4-11
第 2 阶段 4-13
 提议 4-13
 提议, 预定义 4-14
第二层通道协议
 请参阅L2TP
地址
 策略中 2-222
 定义 2-222
 通讯簿条目 2-179
地址组 2-181, 2-222
 编辑 2-184
 创建 2-183
 选项 2-182
 移除条目 2-185
点对点通道协议 (PPTP) 3-79
点对点协议
 请参阅PPP
电缆, 串行 3-17
电子邮件警示通知 3-64, 3-65, 3-86
定期重置 3-25
定义
 区段 2-46
 子接口 6-21
动态 IP
 请参阅DIP
动态 IP 池
 请参阅DIP 池
动态路由 1-A-II
端口
 端口故障切换 7-41
 端口号 2-122
 二级可信和不可信 7-41
 HA 7-7
 监控 7-18, 7-68
 冗余 7-37 – 7-46
 中继 6-19
 中继端口 1-A-XII
 主可信和不可信 7-41
端口地址转换
 请参阅PAT
短缺错误 3-76
对等方 1-A-II
多出口区分符 1-A-II
多类型用户 2-342

E

ESP 4-3, 4-7, 4-8
恶意 URL 2-39
二级 IP 地址 2-97
二级路径 7-18, 7-25

F

Filter IP Source Route Option

(过滤 IP 源路由选项) 2-36

FIN Bit With No ACK Bit

(有 FIN 位无 ACK 位) 2-36

FIPS 1-xv

firewall

drop unknown MAC (丢弃未知的 MAC)
addresses 2-44

ICMP fragments (ICMP 碎片) 2-36

large ICMP packets (大的 ICMP 封包) 2-36

session limiting (限制会话) 2-35

SYN and FIN bits set

(SYN 和 FIN 位的封包) 2-35

SYN fragment (SYN 碎片) floods 2-35

防火墙

Address Sweep Attack (地址扫描攻击)
2-36

Bad IP Option (坏的 IP 选项) 2-37

恶意 URL 2-39

Filter IP Source Route Option

(过滤 IP 源路由选项) 2-36

FIN Bit With No ACK Bit

(有 FIN 位无 ACK 位) 2-36

封锁 Java/ActiveX/.zip/.exe 组件 2-39

ICMP Flood (ICMP 泛滥) 2-34

记录路由选项 2-36

IP Security Option (IP 安全性选项) 2-37

IP Spoofing (IP 欺骗) 2-37

IP Stream Option (IP 流选项) 2-37

IP Strict Source Route Option

(IP 严格源路由选项) 2-37

IP 碎片攻击 2-39

IP Timestamp Option (IP 时戳选项) 2-37

拒绝服务 2-36

Loose Source Route Option

(松散源路由选项) 2-37

陆地攻击 2-38

Ping of Death 2-35

Port Scan Attack (端口扫描攻击) 2-34

SYN Attack (SYN 攻击) 2-34

设置 2-33 – 2-44

TCP Packet Without Flag

(无标志的 TCP 封包) 2-35

Tear Drop Attack (撕毁攻击) 2-36

UDP Flood (UDP 泛滥) 2-34

WinNuke Attack (WinNuke 攻击) 2-38

未知协议 2-37

防火墙, 定义 1-xv, 1-A-III

访问列表 1-A-III, 2-79

配置 2-79

非活动 SA 3-79

封包 3-78

不可路由 3-79

冲突 3-75

地址欺骗攻击 3-79

点对点通道协议 (PPTP) 3-79

定义的 3-79

丢弃的 3-79

非法 3-79

IPSec 3-78

陆地攻击 3-79

内向 3-75

破碎 3-78

欠载传输 3-75

收到的 3-75, 3-77

网络地址转换 (NAT) 3-79

未知 3-76

无法接收的 3-75

因特网控制信息协议 (ICMP) 3-74, 3-78

封包流 2-11 – 2-13

封锁 Java/ActiveX/.zip/.exe 组件 2-39

封装安全性负荷

请参阅 ESP

父级连接 3-78

服务 2-186

策略中 2-222

定义 2-222

下拉式列表 2-187

服务簿

查看 (CLI) 2-187

定制服务 2-187

定制服务 (CLI) 2-188

服务组 (Web 用户界面) 2-206

添加服务 2-188

修改条目 (CLI) 2-189

修改条目 (Web 用户界面) 2-208

移除条目 (CLI) 2-190

预配置服务 2-187

服务质量

请参阅 QoS

服务组 2-206 – 2-209

创建 2-207

删除 2-209

修改 2-208

负载共享 7-60

负载均衡

定义 1-A-III

G

Global 区段 2-115

高可用性

请参阅 HA

公共组 1-A-III

攻击

- Address Sweep (地址扫描) 2-36
- Bad IP Option (坏的 IP 选项) 2-37
- 恶意 URL 2-39
- Filter IP Source Route Option
(过滤 IP 源路由选项) 2-36
- FIN Bit With No ACK Bit
(有 FIN 位无 ACK 位) 2-36
- 封锁 Java/ActiveX/.zip/.exe 组件 2-39
- 回复 4-14
- ICMP Flood (ICMP 泛滥) 2-34
- 记录路由选项 2-36
- IP Security Option (IP 安全性选项) 2-37
- IP Spoofing (IP 欺骗) 2-37
- IP Stream Option (IP 流选项) 2-37
- IP Strict Source Route Option
(IP 严格源路由选项) 2-37
- IP 碎片 2-39
- IP Timestamp Option (IP 时戳选项) 2-37
- 检测 2-40
- 拒绝服务 2-36
- Loose Source Route Option
(松散源路由选项) 2-37
- 陆地攻击 2-38
- Ping of Death 2-35
- Port Scan (端口扫描) 2-34
- SYN Attack (SYN 攻击) 2-34
- TCP Packet Without Flag
(无标志的 TCP 封包) 2-35
- Tear Drop (撕毁) 2-36
- 特洛伊木马病毒 2-39
- UDP Flood (UDP 泛滥) 2-34
- WinNuke 2-38
- 未知协议 2-37
- 攻击继续 2-44
- 公开 / 私有密钥对 4-27

公开密钥基础

请参阅 PKI

功能区段接口 2-85

管理接口 2-85

HA 接口 2-85

供应商专用属性

请参阅 VSA

管理

CLI 3-11

WebUI 3-3

vsys admin 6-33

限制 3-37, 3-38

管理 IP 3-39

VSD 组 0 7-8

管理方法

CLI 3-11

控制台 3-17

SSL 3-9

Telnet 3-11

WebUI 3-3

管理接口

请参阅 MGT 接口

管理客户端 IP 地址 3-37

管理流量 3-42

管理区域, 接口 3-42

管理信息库 II

请参阅 MIB II

管理选项

NetScreen-Global PRO 3-26

ping 3-26

SCS 3-25

SSL 3-26

WebU 3-25

关守设备 2-190

广播网络 1-A-III

过滤器列表 1-A-III

过滤源路由 3-79

过滤, 封包, 封包过滤 1-A-III

H

H.323 协议 2-190

HA 7-1 – 7-59

DHCP 2-376

电缆连接 7-47 – 7-50

二级路径 7-25

HA LED 7-25

IP 跟踪 7-68

控制链接 7-37

路径监控 7-68

冗余 HA 端口 7-7

冗余接口 7-41

数据链路 7-39

双主动故障切换 7-6

消息 7-39

虚拟 HA 接口 2-85

以 HA 链接来连接网络接口 7-49

主动 / 被动故障切换 7-4

专用 HA 接口的电缆连接 7-47

hello 封包 1-A-III

hello 间隔 1-A-III

HMAC 4-7

HTTP 3-8

后备存储器 3-76

互联网密钥交换

请参阅 IKE

互联网, 定义 1-A-IV

回放攻击保护 4-14

恢复日志 3-81

会话, 空闲超时 2-255

- I
- ICMP
 - fragments (ICMP 碎片) 2-36
 - large packets (大的 ICMP 封包) 2-36
- ICMP Flood (ICMP 泛滥) 2-34
- ICMP, 定义 1-A-IV
- Ident-Reset 3-26
- IEEE 802.1Q VLAN 标准 6-17
- IKE 4-9, 4-70, 4-136, 4-163
 - 第 1 阶段提议, 预定义 4-11
 - 第 2 阶段提议, 预定义 4-14
 - hello 消息 4-215
 - IKE ID 2-303, 2-322
 - IKE ID, Windows 2000 4-252
- ISAKMP 1-A-V
 - 冗余网关 4-213 – 4-231
 - 心跳信号 4-215
 - 用户 2-303 – 2-307
 - 用户组, 定义 2-306
 - 用户, 定义 2-304
 - 用户, 组 2-303
 - 组 IKE ID 用户 4-180 – 4-201
 - 组 IKE ID, Container (容器) 4-185
 - 组 IKE ID, Wildcard (通配符) 4-184
- IKE 用户
 - 服务器支持 2-250
 - IKE ID 2-273, 2-303
 - 与其它用户类型 2-342
- IKE (互联网密钥交换)
 - 密钥管理 1-A-VIII
- 记录 2-227
- 记录路由选项 2-36
- IP 安全性
 - 请参阅 IPSec
- IP 池
 - 请参阅 DIP 池
- IP 地址
 - 定义 1-A-IV
 - 定义每一个端口 2-179
 - 二级 2-97
 - 公开 2-90
 - 管理 IP 3-39
 - 扩展的 4-202
 - Layer 3 (第 3 层) 安全区段 2-90 – 2-91
 - 私有 2-90
 - 私有地址范围 2-91
 - 网络 ID 2-91
 - 虚拟 2-113
 - 主机 ID 2-91
- IP 跟踪 7-68
 - 跟踪的 IP 故障临界值 7-69
 - ping 和 ARP 7-68
 - 权重 7-69
 - 设备故障切换临界值 7-69
- IP Security Option (IP 安全性选项) 2-37
- IP Spoofing (IP 欺骗) 2-37
- IP Stream Option (IP 流选项) 2-37
- IP Strict Source Route Option (IP 严格源路由选项) 2-37
- IP 碎片攻击 2-39
- IP Timestamp Option (IP 时戳选项) 2-37
- IP 语音通信 2-190
- IPSec 4-3
 - AH 4-2
 - AH, 已定义 1-A-III
 - 定义 1-A-IV
 - ESP 4-2
 - ESP, 已定义 1-A-III
 - 加密 1-A-V
 - 认证 1-A-IX
 - SA 1-A-I, 4-2, 4-10, 4-11, 4-13
 - SPI 4-2
 - SPI, 定义 1-A-I
 - 数字签名 4-24
 - 通道 4-2
 - 通道模式 4-5
 - 通道协商 4-11
 - 传送模式 4-4, 4-237, 4-243, 4-250
- IPSec 上的 L2TP 4-4, 4-243, 4-250
 - 通道 4-243
- IP, 定义 1-A-XI
- ISAKMP 1-A-V
- J
- 集群 1-A-V, 7-16 – 7-20, 7-51
- 集群列表 1-A-V
- 集群名称, NSRP 7-17
- 计数 2-227
- 集线器, 定义 1-A-V
- 基于 IP 的通信流分类 6-28
- 基于策略的 NAT 2-167, 2-173 – 2-176, 2-224, 4-202 – 4-212
 - 通道接口 2-86
- 基于散列的信息认证代码
 - 请参阅 HMAC
- 加密
 - NSRP 7-7, 7-18
- 加密, 定义 1-A-V
- 接口
 - 绑定到区段 2-89
 - 编址 2-90
 - CLI 接口表 2-88
 - 查看接口表 2-87
 - 从 vsys 导出 6-16
 - 从区段解除绑定 2-93
 - DIP 2-125
 - 导入到 vsys 6-15

- 二级 IP 地址 2-97
- 共享 6-12, 6-28
- 管理选项 3-25 – 3-26
- HA 2-85
- HA 双端口 7-37 – 7-40
- 聚合 2-84
- 扩展的 4-202
- Layer 3（第 3 层）安全区段 2-90
- MGT 2-85, 3-42
- MIP 2-99
- 缺省 2-92, 3-43
- 冗余 2-84, 7-41
- 通道 2-72, 2-86, 4-48 – 4-57, 4-204
- 通道, 定义 1-A-X
- WebUI 接口表 2-88
- VIP 2-113
- VSI 2-84, 7-28
- 物理 2-3
- 修改 2-94
- 虚拟 HA 2-85
- 虚拟的 HA 7-49
- 专用的 6-12, 6-28
- 进度表 2-228
- 警告
 - 电子邮件警示 3-82
 - 临界值 3-82
 - 流量 3-82 – 3-86
- 静态路由 1-A-V
- 局部优先级 1-A-V
- 聚合 1-A-VI
- 聚合接口 2-84
- 聚合器 1-A-VI
- 聚合状态 1-A-VI
- 距离向量 1-A-VI

K

- Keep Alive 1-A-V
- Keep Alive（激活）
 - L2TP 4-247
 - 频率, NAT-T 4-19
- 空闲会话超时 2-255
- 控制消息 7-37
 - HA 物理链接心跳信号 7-38
 - HA 信息 7-39
 - RTO 心跳信号 7-39
 - VSD 心跳信号 7-38

L

- L2TP 4-233 – 4-261
 - 本地数据库 2-336
 - 操作模式 4-237
 - 策略 2-224
 - 存取集中器
 - 请参阅 LAC
 - 地址分配 2-335
 - 封装 4-238
 - hello 信号 4-247
 - 解封 4-239
 - Keep Alive（激活） 4-247
 - 强制的配置 4-234
 - 缺省参数 4-240
 - RADIUS 服务器 4-240
 - ScreenOS 支持 4-237
 - SecurID 服务器 4-240
 - 通道 4-243
 - Windows 2000 4-254
 - Windows 2000 通道认证 4-247
 - 外部 auth 服务器 2-336

- 网络服务器

- 请参阅 LNS

- 用户认证 2-335
- 在 Windows 2000 中仅使用 L2TP 4-237
- 自愿的配置 4-234
- L2TP 用户 2-335 – 2-339
- 服务器支持 2-250
- 认证点 2-273
- 与 XAuth 2-342
- LAC 4-234
 - NetScreen-Remote 5.0 4-234
 - Windows 2000 4-234
- LAN, 定义 1-A-VI
- Layer 2 通道协议
 - 请参阅 L2TP
- LDAP 2-262 – 2-263
 - auth 服务器对象 2-269
 - Distinguished name（识别名称） 2-263
 - 服务器端口 2-263
 - 结构 2-262
 - 通用名称标识符 2-263
 - 支持的用户类型 2-263
- LED 指示器, HA 7-25
- LNS 4-234
- logging
 - asset recovery log 3-81
- Loose Source Route Option
 - （松散源路由选项） 2-37
- 历史记录图表 2-227
- 联合体 1-A-VI
- 连接器
 - GBIC, 定义 1-A-III
 - RJ-45, 定义 1-A-IX
- 连接状态 1-A-VI
- 链接状态 1-A-VI
- 链接状态通告 1-A-VI

- 邻接方 1-A-VI
- 邻接设备 1-A-VII
- 令牌代码 2-260
- 陆地攻击 2-38
- 浏览器要求 3-3
- 流量
 - 警告 3-82 – 3-86
- 路径监控 7-68
- 路由
 - 二级 IP 地址之间 2-97
 - 路由导出 2-76
- 路由表 1-A-VII
 - 度量声明 2-67
 - 静态路由 2-66
 - 通道接口 2-72
- 路由度量 2-57
- 路由反射器 1-A-VII
- 路由模式 2-167 – 2-172
 - 基于策略的 NAT 2-167
 - 接口设置 2-168
- 路由器, 定义 1-A-VII
- 路由图 1-A-VII, 2-74
 - 配置 2-75
- 路由文件布置和分配程序衰减 1-A-VII
- 路由选择
 - BGP 2-57
 - 过程 2-52
 - 路由表 2-56, 2-65
 - 路由表配置 2-65, 2-67
 - 路由度量 2-57
 - 路由选择协议 2-57
 - 路由优先级 2-57, 2-80
 - 路由重新分配 2-74
 - OSPF 2-57
 - 通道接口 2-72
 - 重新分配 2-76

- 路由优先级 2-67
- 路由重新分配 1-A-VII

M

- MAC 地址
 - 定义 1-A-VIII
- Main mode (主模式) 4-12
- MD5 4-7
 - 定义 1-A-VII
- MED 比较 1-A-VIII
- MGT 接口 2-85
- MIB II 3-26, 3-66
- MIB 文件 3-A-I
- MIB 文件夹
 - 一级 3-A-II
- MIP 2-12, 2-99
 - 创建地址 2-101
 - 从其它区段可到达 2-104
 - 地址范围 2-103
 - 定义 1-A-XII
 - Global 区段 2-100
 - 流向带有基于接口的 NAT 的区段 2-161
 - NAT 2-224
 - 缺省网络掩码 2-103
 - 缺省虚拟路由器 2-103
 - same-as-untrust 接口 2-110 – 2-112
 - 信息流整形 2-100
 - 虚拟系统 6-9
 - 在区段接口上创建 2-101
 - 在通道接口上创建 2-109
- 密码
 - vsys admin 6-33
 - 遗忘 3-33
- 密码认证协议
 - 请参阅 PAP

- 密钥
 - 创建 3-9
 - 管理 1-A-VIII
- 命令
 - set admin 5-69, 5-70, 5-75
- 命令级别 2-58
 - 根级 2-58
 - 环境级 2-59
- 命令行界面
 - 请参阅 CLI
- 模数 4-13

N

- NAT
 - 定义 1-A-XI
 - IPSec 和 NAT 4-17
 - NAT 服务器 4-17
- NAT 穿透
 - 请参阅 NAT-T
- NAT 模式 2-160 – 2-166
 - 接口设置 2-162
 - 流向 Untrust 区段的信息流 2-143, 2-161
- NAT 向量错误 3-79
- NAT-T 4-17
 - 激活频率 4-19
 - 启用 4-21
- NAT, 基于策略的 2-167, 2-224
- NetInfo 2-375
- NetScreen 词典文件 2-259
- NetScreen 可靠传输协议
 - 请参阅 NSTP
- NetScreen 冗余协议
 - 请参阅 NSRP

NetScreen-Global PRO 3-18, 3-56

管理选项 3-26

Policy Manager 3-18

Report Manager 3-18

NetScreen-Global PRO Express 3-18

实时监控器 3-18

NetScreen-Remote

动态对等 4-171

动态对等方 4-93

NAT-T 选项 4-17

手动密钥 VPN 4-157

自动密钥 IKE VPN 4-163

NSRP 7-1 – 7-73

ARP 7-58

ARP 广播 7-18

安全通信 7-7, 7-18

备份 7-4

DHCP 2-376

DIP 组 2-137 – 2-140

电缆连接 7-47 – 7-50

调试集群命令 7-16

端口故障切换 7-41

端口监控 7-18, 7-68

二级路径 7-18, 7-25

负载共享 7-60

概述 7-3

管理 IP 7-68

HA 电缆连接, 网络接口 7-49

HA 电缆连接, 专用接口 7-47

HA 端口, 冗余接口 7-41

HA 会话备份 2-227, 7-21

HA 接口 7-38

HA LED 7-25

HA 配置 7-51

集群 7-16 – 7-20, 7-51

集群名称 7-17

控制链接 7-37

控制消息 7-37, 7-38

NAT 和“路由”模式 7-8

NSRP, 已定义 1-A-VIII

抢先模式 7-23

清除集群命令 7-16

全网状配置 7-47, 7-60

缺省设置 7-9

RTO 1-A-XII, 7-21 – 7-22, 7-51

RTO 状态 7-22

RTO, 重新同步 7-34

冗余端口 7-37 – 7-46

冗余接口 2-84

数据链路 7-39

数据消息 7-39

VSD 组 7-5, 7-23 – 7-27, 7-51, 7-68

VSD, 已定义 1-A-XII

VSI 1-A-XII, 2-84, 7-5

VSI, 静态路由 7-28, 7-45, 7-46

虚拟系统 7-60 – 7-67

抑制时间 7-53, 7-57

优先级编号 7-23

主设备 7-4

“透明”模式 7-8

NSTP 7-33

内部闪存存储器 3-56

内部网, 定义 1-A-VIII

O

OSPF

AS 边界路由器 5-4

备份指定路由器 5-5

不工作间隔 5-21, 5-31

不完全剩余区域 5-4

点对点网络 5-6

非广播网络 5-6

概述 5-3

广播网络 5-5

hello 间隔 5-22, 5-32

hello 临界值 5-48

hello 协议 5-5

环境 5-10

汇总路由 5-44

接口 5-14, 5-17

接口特征 5-9

开销 5-20

LSA 临界值 5-49

链接状态数据库 5-3

链接状态通告 5-3, 5-7

邻接 5-5

邻接路由器 5-5

路由实例, 创建 5-11

路由重新分配 5-15, 5-38

路由重新分配规则 5-37

MD5 密码 5-19, 5-29

明文密码 5-18, 5-30

Neighbor List (邻接方列表) 5-23

内部路由器 5-4

配置命令 5-41

区域 5-3, 5-13

区域边界路由器 5-4

区域范围 5-47

缺省路由 5-43, 5-46

RFC 1538 5-8

RFC 1583 5-50

RFC 2328 5-8

认证方法 5-8

剩余区域 5-4, 5-40

实例 5-8, 5-11, 5-12

数据库 5-39

通道接口 5-42

统计信息 5-35
VPN 通道支持 5-8
完全剩余区域 5-4
网络类型 5-5
虚拟链接 5-27, 5-28
优先级 5-25
指定路由器 5-5
中枢路由器 5-4
中枢区域 5-3
重新传输间隔 5-24, 5-33
传输延迟 5-26, 5-34

P

PAP 4-237, 4-240
PAT 2-126
PC 卡 2-398, 2-400
PCMCIA 3-56
PFS 4-14
ping 3-72
 管理选项 3-26
Ping of Death 2-35
PKI 4-26
 加密 1-A-V
 密钥 3-9
Policy Manager 3-18
Port Scan Attack（端口扫描攻击） 2-34
PPP 4-235
PPPoE 2-164, 2-170, 2-392
 已定义 2-392
配置设置
 浏览器要求 3-3
 上传 2-398
 下载 2-398

Q

QoS 1-xv, 2-354
前缀
 已定义 1-A-VIII
抢先模式 7-23
桥接器 1-A-VIII
轻量目录访问协议
 请参阅 LDAP
区段 2-29 – 2-49
 安全 2-32
 Global 2-32, 2-115
 功能 2-49
 共享 6-12
 通道 2-45, 4-202, 4-204
 VR 绑定 2-62
 vsys 6-7
区域 1-A-VIII
 安全 1-A-I
 定义 1-A-VIII
 MGT 3-42
 通道 1-A-X
区域边界路由器 1-A-VIII
区域范围 1-A-IX
全网状配置 7-60

R

RADIUS 2-257 – 2-259
 auth 服务器对象 2-264
 端口 2-258
 对象属性 2-258
 共享机密 2-258
 L2TP 4-240
 NetScreen 词典文件 2-259, 2-340
RADIUS（用户服务远程认证拨号） 3-33
Report Manager 3-18

RFC

1349, “网际协议套件中的服务类型” 2-229
1777, “轻量目录访问协议” 2-262
1918, “Address Allocation for Private Internets” 2-91
2474, “IPv4 和 IPv6 头中差异服务字段（DS 字段）的定义” 2-229

RTO 7-21 – 7-22

操作状态 7-22
RTO 对等方 7-24

认证

Allow Any 2-227
策略 2-225
IPSec 1-A-IX
NSRP 7-7, 7-18
用户 2-225, 2-249 – 2-351

认证包头

请参阅 AH

认证, 用户 2-249 – 2-351

auth 服务器 2-250
本地数据库 2-252 – 2-253
多类型 2-342
IKE 用户 2-250
类型和应用 2-273 – 2-342
配置文件 2-249
认证点 2-273
使用不同登录 2-342
手动密钥用户 2-250
WebAuth 2-250
用户类型 2-250
帐户 2-249

日志 3-56 – 3-81

CompactFlash (PCMCIA) 3-56
Console（控制台） 3-56
Email（电子邮件） 3-56
恢复日志 3-81

- Internal（内部） 3-56
- NetScreen-Global PRO 3-56
- self 日志 3-62
- SNMP 3-56, 3-66
- Syslog（系统日志） 3-56
- WebTrends 3-56, 3-63
- 系统日志 3-63
- 冗余网关 4-213 – 4-231
 - 恢复过程 4-216
- TCP SYN 标记检查 4-219
- 软件
 - 更新 2-400
 - 密钥, vsys 6-12
 - 上传和下载 2-400

S

- SA 4-10, 4-11, 4-13
 - 定义 1-A-I
- SA 策略 3-79
- SCEP（简单证书注册协议） 4-38
- ScreenOS 1-xvi
 - 安全区段 2-2, 2-32
 - 安全区段接口 2-3
 - 安全区段, Global 2-2
 - 安全区段, 预定义 2-2
 - 策略 2-3, 2-7
 - 封包流 2-11 – 2-13
 - Global 区段 2-32
 - 概述 2-1 – 2-27
 - 更新 2-400
 - 功能区段 2-49
 - 区段 2-29 – 2-49
 - 通道区段 2-45
 - 物理接口 2-3
 - 虚拟系统 2-10

- 虚拟系统, 区段 6-7
- 虚拟系统, VR 6-6
- 子接口 2-4
- SCS 3-13 – 3-16, 3-25
 - 服务器密钥 3-14
 - 会话密钥 3-14
 - 加载公开密钥, CLI 3-15
 - 加载公开密钥, TFTP 3-15, 3-16
 - 加载公开密钥, WebUI 3-15
 - 连接过程 3-14
 - 密码认证 3-13
 - PKA 3-15
 - PKA 密钥 3-14
 - PKA 认证 3-13
 - 强制仅使用 PKA 认证 3-16
 - 认证方法优先级 3-16
 - 主机密钥 3-14
 - 自动登录 3-16
- SCS（安全命令外壳） 3-26
- SecurID 2-260 – 2-261
 - ACE 服务器 2-260
 - auth 服务器对象 2-267
 - Authentication Port（认证端口） 2-261
 - Client Retries（客户端重试次数） 2-261
 - Client Timeout（客户端超时） 2-261
 - Encryption Type（加密类型） 2-261
 - L2TP 4-240
 - 令牌代码 2-260
 - 强迫 2-261
 - 认证器 2-260
 - 用户类型支持 2-261
- self 日志 3-62
- session limiting（限制会话） 2-35
- set 命令
 - admin 5-69, 5-70, 5-75

- SHA-1 4-7
 - 定义 1-A-IX
- SMTP 服务器 IP 3-86
- SNMP 3-26, 3-66
 - 公共组, 公开 3-69
 - 公共组, 私有 3-69
 - 加密 3-43, 3-68
 - 冷启动陷阱 3-66
 - 流量报警陷阱 3-66
 - MIB 文件 3-A-I
 - MIB 文件夹, 一级 3-A-II
 - 配置 3-69
 - 认证故障陷阱 3-66
 - VPN 监控 3-71 – 3-72
 - 系统报警陷阱 3-66
 - 陷阱 3-66
 - 陷阱类型 3-67
 - 执行 3-68
- SNMP 陷阱
 - 100, 硬件问题 3-67
 - 200, 防火墙问题 3-67
 - 300, 软件问题 3-67
 - 400, 流量问题 3-67
 - 500, VPN 问题 3-67
 - 允许或拒绝 3-68
- SPI, 定义 1-A-I
- SSL 3-9
 - 管理选项 3-26
 - 与 WebAuth 2-298
- SSL 握手协议
 - 请参阅 SSLHP
- SSLHP 3-9
- SYN
 - Alarm Threshold（警报临界值） 2-44
 - Attack Threshold（攻击临界值） 2-43
 - destination threshold（目的临界值） 2-44

- drop unknown MAC addresses
 - (丢弃未知的 MAC) 2-44
- 泛滥攻击 2-40
- 攻击 2-34
- 临界值 2-41
- Queue size (队列长度) 2-43
- source threshold (源临界值) 2-44
- Timeout (超时) 2-43
- Syslog (系统日志) 3-56
- 三方握手 2-40
- 三重 DES
 - 请参阅 3DES
- 设置
 - 保存 2-398
 - 导入 2-398
 - 上传 2-398
 - 下载 2-398
- 时间表 2-210
- 实时监控器 3-18
- 时钟 2-403
- 手动密钥 4-59, 4-127
 - 管理 4-9
 - VPN 3-43
- 手动密钥用户 2-328 – 2-334
 - 定义 2-329
 - 服务器支持 2-250
 - 组, 定义 2-332
- 数据加密标准
 - 请参阅 DES
- 数据消息 7-39
- 数字签名 4-24
- 碎片攻击 2-39

T

- TCP
 - 代理 3-78
 - SYN 标记检查 4-219
 - 三方握手 1-A-IX
- TCP Packet Without Flag (无标志的 TCP 封包) 2-35
- TCP/IP, 定义 1-A-II
- Tear Drop Attack (撕毁攻击) 2-36
- Telnet 3-11, 3-25
- TFTP 服务器 2-398, 2-400
- trace-route 2-149, 2-151
- Transparent mode
 - drop unknown MAC (丢弃未知的 MAC) addresses 2-44
- 提议
 - 第 1 阶段 4-11
 - 第 2 阶段 4-13
- 通道接口 2-72, 2-86, 4-204
 - 定义 1-A-X, 2-86
 - 基于策略的 NAT 2-86
 - 一个接口, 多个通道 2-86
- 通道模式 4-5
- 通道区 1-A-X
- 通道区段 4-202, 4-204
 - 绑定 4-125, 4-127
- 通道区域
 - 定义 1-A-X
- 通告 1-A-X
- 通信流
 - 分类, 基于 IP 6-28
 - 分类, 基于 VLAN 6-17
 - 直通信息, vsys 分类 6-10 – 6-11
- 通讯簿
 - 编辑组的条目 2-184
 - 另请参阅 地址

- 添加地址 2-179
- 条目 2-179
- 修改地址 2-180
- 移除地址 2-185
- 组 2-181

- 通用名称 2-263
- 透明模式 2-144 – 2-159
 - ARP/trace-route 2-146
- 泛滥 2-146
- unicast 选项 2-146

图标

- 策略 2-230
- 定义 2-230

- 图表, 历史记录 2-227

U

- UDP
 - 定义 1-A-XII
 - NAT-T 封装 4-17
 - 校验和 4-19
- UDP Flood (UDP 泛滥) 2-34
- URL 过滤
 - 封锁的 URL 消息类型 2-397
 - 服务器状态 2-396
 - NetScreen 封锁的 URL 消息 2-397
 - 通信超时 2-396
 - Websense 服务器端口 2-396
 - Websense 服务器名称 2-396
- URL, 定义 1-A-XI

V

- VIP 2-12
 - 必需的信息 2-114
 - 编辑 2-117
 - 从其它区段可到达 2-115

- 定义 1-A-XI
- 定制服务, 低端口号 2-114
- 定制和多端口服务 2-118 – 2-124
- Global 区段 2-115
- 流向带有基于接口的 NAT 的区段 2-161
- 配置 2-115
- 虚拟系统 6-9
- 移除 2-118
- VLAN
 - 标记 2-4, 6-19, 6-20
 - 创建 6-21 – 6-23
 - 定义 1-A-XII
 - 基于 VLAN 的通信流分类 6-17
 - 透明模式 6-18, 6-19
 - 与另一 VLAN 通信 6-24 – 6-27
 - 中继 6-18
 - 子接口 6-19
- VLAN1
 - 接口 2-145, 2-152
 - MGT 区域 3-42
 - 区段 2-145
- VLAN (虚拟局域网)
 - 标记 1-A-XIII
- VPN 1-xv
 - Aggressive mode (主动模式) 4-12
 - 不同的 ScreenOS 版本 4-49, 4-204
 - 策略 2-223
 - Diffie-Hellman 交换 4-13
 - Diffie-Hellman 组 4-13
 - 第 1 阶段 4-11
 - 第 2 阶段 4-13
 - 定义 1-A-XII
 - 回放攻击保护 4-14
 - 基于策略的 NAT 4-202
 - 监控 3-86
 - 流向带有基于接口的 NAT 的区段 2-161
 - Main mode (主模式) 4-12
 - 冗余网关 4-213 – 4-231
 - 冗余组、恢复过程 4-216
 - SA 4-10
 - 手动密钥 3-43
 - 通道接口 2-72, 4-204
 - 通道区段 2-45, 4-202
 - 通道区段, 绑定 4-125, 4-127
 - 通道, 定义 1-A-X
 - VPN 组 4-213
 - 用于管理流量 3-43
 - 自动密钥 IKE 3-43, 4-9
 - “Untrust_Tun” 通道区段 4-125, 4-127
- VR 2-61 – 2-73
 - 创建共享 VR 6-13
 - 定义 1-A-XII
 - 共享 6-12
 - 简介 2-5 – 2-6
 - 路由表 2-6
 - 路由重新分配 2-6
 - 配置 2-61
 - 删除 2-62
 - 修改 2-61
- VRRP 7-68
- VSA 2-259
 - Attribute Name (属性名) 2-259
 - Attribute Number (属性编号) 2-259
 - Attribute Type (属性类型) 2-259
 - Vendor ID (供应商 ID) 2-259
- VSD 组 7-5, 7-23 – 7-27
 - 成员状态 7-24, 7-68
 - VSD, 已定义 1-A-XII
 - 心跳信号 7-18, 7-25
 - 抑制时间 7-53, 7-57
 - 优先级编号 7-23
- USGA
 - 安全区域 1-A-I
 - 已定义 1-A-X
- USGA (通用安全网关体系结构)
 - 通道区 1-A-X
- VSI 7-5, 7-23
 - 静态路由 7-28
 - 每个 VSD 组有多个 VSI 7-60
 - 已定义 1-A-XII
- W
 - Web 浏览器要求 3-3
 - Web 用户界面
 - 请参阅 WebUI
 - WebAuth 2-250
 - 本地用户组 2-291
 - 策略前认证进程 2-226, 2-276
 - 外部用户组 2-294
 - 与 SSL (外部用户组) 2-298
 - Websense 2-396
 - WebTrends 3-56, 3-63
 - 加密 3-43, 3-63
 - 消息 3-64
 - WebUI 3-3, 3-42
 - WebUI, 约定 1-xxi, 2-viii, 3-iv, 4-vi, 5-vi, 6-iv, 7-iv
 - Wildcard (通配符) 4-184
 - WinNuke Attack (WinNuke 攻击) 2-38
 - WINS
 - 定义 1-A-XI
 - L2TP 设置 4-240
 - 外部邻接路由器 1-A-XI
 - 外部网, 定义 1-A-XI
 - 完全正向保密
 - 请参阅 PFS

网关 1-A-XI
网关, 定义 1-A-IV
网络层可达到性信息 1-A-XI
网络地址转换 (NAT) 3-79
网络服务器 4-234
网络掩码 2-222
 定义 1-A-XI, 1-A-XIII
 用途 2-91
网络, 带宽 2-354
未知 Unicast 选项 2-146 – 2-151
 ARP 2-148 – 2-151
 泛滥 2-147 – 2-148
 trace-route 2-149, 2-151
未知协议 2-37
无级路由 1-A-XI

X

XAuth

 auth 和地址 2-322
 本地用户 auth 2-310
 本地用户组 auth 2-312
 地址超时 2-309
 地址分配 2-308, 2-309
 认证点 2-308
 外部用户 auth 2-314
 外部用户组 auth 2-317
 虚拟适配器 2-308
 用户认证 2-309
XAuth 用户 2-308 – 2-328
 服务器支持 2-250
 认证点 2-273
 与 L2TP 2-342
系统日志
 安全设备 3-64
 加密 3-43, 3-63

 设备 3-64
 消息 3-63
 主机 3-63
 主机名称 3-64, 3-65
系统, 参数 2-369 – 2-404
消息
 错误 3-57
 调试 3-57
 关键 3-57
 紧急 3-57
 警告 3-57
 警示 3-57
 通知 3-57
 WebTrends 3-64
 信息 3-57

协议

 CHAP 4-237
 NSRP 7-1
 NSTP 7-33
 PAP 4-237
 PPP 4-235
 VRRP 7-68

信任 1-A-XI

信息流

 记录 2-227
 计数 2-227
 优先级 2-229
 整形 2-354
信息流整形 1-xv, 2-353 – 2-368
 服务优先级 2-361
 自动 2-354
 自动模式 2-360
“信息整理” 版本 5
 请参阅 MD5
虚拟 HA 接口 2-85, 7-49

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

虚拟路由器

 配置 2-61

 请参阅 VR

虚拟适配器 2-308

 定义 1-A-XII

虚拟系统 2-10, 6-1 – 6-34

 admin 6-iii

 admin 类型 6-3

 admins 6-1

 创建 Vsys 对象 6-3

 导出物理接口 6-16

 导入物理接口 6-15

 定义 1-A-XII

 负载共享 7-60

 更改 admin 的密码 6-3, 6-33

 共享 VR 6-12

 共享区段 6-12

 管理员 3-28

 基本功能要求 6-3

 基于 IP 的通信流分类 6-28 – 6-32

 基于 VLAN 的通信流分类 6-17 – 6-27

 接口 6-7

 MIP 6-9

 NSRP 7-60

 区段 6-7

 软件密钥 6-12

 通信流分类 6-9 – 6-14

 透明模式 6-18

 VIP 6-9

 VR 6-6

- 易管理性和安全性 6-29
- 只读管理员 3-28
- 重叠地址范围 6-21, 6-29
- 重叠子网 6-21
- 虚拟专用网
 - 请参阅VPN

Y

- 以太网, 已定义 1-A-XII
- 映射 IP
 - 请参阅MIP
- 用户
 - 多个管理用户 3-27
 - IKE 2-303 – 2-307
 - IKE, 组 2-306
 - 组 IKE ID 4-180 – 4-201
 - 组, 服务器支持 2-250
- 用户认证
 - 请参阅认证, 用户
- 用户, admin 2-340 – 2-341
 - auth 过程 2-341
 - 超时 2-256
- 用户, IKE
 - 定义 2-304
 - IKE ID 2-303
 - 组 2-303
- 用户, L2TP 2-335 – 2-339
- 用户, 手动密钥 2-328 – 2-334
- 用户, XAuth 2-308 – 2-328
- 优先级排列 2-361
- 预共享密钥 4-9, 4-163
- 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 3-79
- 原子聚合 1-A-I
- 约定
 - CLI 1-xxii, 2-ix, 3-v, 4-vii, 5-vii, 6-v, 7-v
 - WebUI 1-xxi, 2-viii, 3-iv, 4-vi, 5-vi, 6-iv, 7-iv
- 运行认证 2-275
- 运行时认证 2-225

Z

- 证书 4-10
 - 本地 4-30
 - CA 4-26, 4-30
 - 撤消 4-29, 4-43
 - 加载 4-34
 - 请求 4-31
 - 通过电子邮件 4-30
- 执行对象
 - 请参阅RTO
- 质询握手认证协议
 - 请参阅CHAP
- 中继端口 6-19
 - 手动设置 6-18
 - 已定义 6-18
- 中继端口, 定义 1-A-XII
- 重新分配 1-A-II
- 重新分配列表 1-A-II
- 重置
 - 定期 3-25
 - 至出厂缺省值 3-36
- 传送模式 4-4, 4-237, 4-243, 4-250
- 状态式检查 2-34
- 自动密钥 IKE VPN 3-43, 4-9
 - 管理 4-9
- 子接口 2-4, 6-19
 - 创建 (vsys) 6-19
 - 创建 (根系统) 2-95
 - 定义 6-21
 - 各 vsys 上的多个子接口 6-19
 - 配置 (vsys) 6-19
 - 删除 2-96
 - 已定义 1-A-XIII
- 子网掩码
 - 定义 1-A-XIII
- 自治系统
 - 已定义 1-A-XIII
- 自治系统边界路由器 1-A-XIII
- 自治系统路径 1-A-XIII
- 组
 - 地址 2-181
 - 服务 2-206
- 组 IKE ID
 - 预共享密钥 4-193 – 4-201
 - 证书 4-181 – 4-192
- 组 IKE ID 用户 4-180 – 4-201
 - 预共享密钥 4-193
 - 证书 4-181
- 组表达式 2-343 – 2-350
 - 服务器支持 2-250
 - 其它组表达式 2-344
 - 用户 2-343
 - 用户组 2-343
 - 运算符 2-343

