

NetScreen 概念与范例

ScreenOS 参考指南

第 2 卷：基本原理

ScreenOS 5.0.0

编号 093-0925-000-SC

修订本 E

Copyright Notice

Copyright © 2004 NetScreen Technologies, Inc. All rights reserved.

NetScreen, NetScreen Technologies, GigaScreen, NetScreen-Global PRO, ScreenOS and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. in the United States and certain other countries. NetScreen-5GT, NetScreen-5GT Extended, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-500 GPRS, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-IDP 1000, NetScreen-SA 1000, NetScreen-SA 3000, NetScreen-SA 5000, NetScreen-SA Central Manager, NetScreen-SM 3000, NetScreen-Security Manager, NetScreen-Security Manager 2004, NetScreen-Hardware Security Client, NetScreen ScreenOS, NetScreen Secure Access Series, NetScreen Secure Access Series FIPS, NetScreen-IDP Manager, GigaScreen ASIC, GigaScreen-II ASIC, Neoteris, Neoteris Secure Access Series, Neoteris Secure Meeting Series, Instant Virtual Extranet, and Deep Inspection are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

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

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

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance

with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

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

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

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

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

Disclaimer

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

目录

前言	ix
约定	x
CLI 约定	x
WebUI 约定	xi
插图约定	xiii
命名约定和字符类型	xiv
NetScreen 文档	xv
第 1 章 ScreenOS 体系结构	1
安全区	2
安全区接口	3
物理接口	3
子接口	4
虚拟路由器	5
策略	6
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): 两个路由选择域	20
范例 (第 4 部分): 策略	22
第 2 章 路由表和静态路由	29
路由基本原理	30

路由方法	30
静态路由	30
动态路由	30
路由表	31
使用静态路由进行路由选择	33
NetScreen 设备上的虚拟路由器	35
配置静态路由的时机	36
配置静态路由	38
范例: 静态路由	39
范例: 用于通道接口的路由	43
第 3 章 区段	45
安全区	48
Global 区段	48
SCREEN 选项	48
通道区段	49
范例: 将通道接口绑定到 Tunnel 区段	50
配置安全区和 Tunnel 区段	51
创建区段	51
修改区段	52
删除区段	53
功能区段	54
Null 区段	54
MGT 区段	54
HA 区段	54
Self 区段	54
VLAN 区段	54

端口模式	55	修改接口	83
设置端口模式	60	范例：修改接口设置	83
范例：Home-Work 端口模式	61	跟踪 IP 地址	84
Home 区段 /Work 区段	62	IP 跟踪重新路由信息流	85
范例：Home 和 Work 区段	64	出口接口上的失败	86
第 4 章 接口	67	入口接口上的失败	89
接口类型	68	配置 IP 跟踪	93
安全区接口	68	范例：配置接口 IP 跟踪	95
物理	68	创建子接口	99
子接口	68	范例：根系统中的子接口	99
聚合接口	69	删除子接口	100
冗余接口	69	范例：删除安全区接口	100
虚拟安全接口	69	二级 IP 地址	101
功能区段接口	70	二级 IP 地址属性	101
管理接口	70	范例：创建二级 IP 地址	102
HA 接口	70	回传接口	103
通道接口	71	范例：创建回传接口	103
删除通道接口	74	使用回传接口	104
范例：删除通道接口	74	范例：用于管理的回传接口	104
查看接口	76	范例：回传接口上的 BGP	105
接口表	76	范例：回传接口上的 VSI	105
配置安全区接口	78	范例：回传接口作为源接口	106
将接口绑定到安全区	78	第 5 章 接口模式	107
范例：绑定接口	78	透明模式	108
为 L3 安全区接口寻址	79	区段设置	109
公开 IP 地址	79	VLAN 区段	109
私有 IP 地址	80	预定义的第 2 层区段	109
范例：编址接口	81	信息流转发	110
从安全区解除接口绑定	82		
范例：解除接口绑定	82		

未知 Unicast 选项	111	ICMP 服务	155
泛滥方法	112	范例：定义 ICMP 服务	156
ARP/Trace-Route 方法	114	RSH ALG	156
范例：用于管理的 VLAN1 接口	118	IP 语音通信的 H.323 协议	157
范例：透明模式	121	范例：Trust 区段中的关守设备 (透明或路由模式)	157
NAT 模式	126	范例：Trust 区段中的关守设备 (NAT 模式)	159
入站和出站 NAT 信息流	128	范例：Untrust 区段中的关守设备 (透明或路由模式)	164
接口设置	129	范例：Untrust 区段中的关守设备 (NAT 模式)	167
范例：NAT 模式	130	SIP – 会话启动协议	172
路由模式	134	SIP 请求方法	173
接口设置	135	SIP 响应的类别	173
范例：路由模式	136	ALG – 应用程序层网关	175
第 6 章 为策略构建块	141	SDP	176
地址	142	针孔创建	177
地址条目	143	会话静止超时	179
范例：添加地址	143	范例：创建策略以允许 SIP	180
范例：修改地址	144	范例：信号发送与媒体静止超时	182
范例：删除地址	145	服务组	183
地址组	145	范例：创建服务组	184
范例：创建地址组	147	范例：修改服务组	185
范例：编辑地址组条目	148	范例：移除服务组	186
范例：移除成员和组	149	DIP 池	187
服务	150	端口地址转换	188
预定义的服务	150	范例：创建带有 PAT 的 DIP 池	188
范例：设置服务超时	152	范例：修改 DIP 池	190
定制服务	152	附着 DIP 地址	190
范例：添加定制服务	152	扩展接口和 DIP	191
范例：修改定制服务	154	范例：在不同子网中使用 DIP	191
范例：移除定制服务	154		

回传接口和 DIP	199	URL 过滤	229
范例：回传接口上的 DIP	200	记录	229
DIP 组	205	计数	229
范例：DIP 组	207	信息流报警临界值	229
时间表	209	时间表	230
范例：循环时间表	209	防病毒扫描	230
第 7 章 策略	213	信息流整形	231
基本元素	215	策略应用	232
三种类型的策略	216	查看策略	232
区段内部策略	216	策略图标	232
区段内部策略	217	创建策略	233
全局策略	217	策略位置	234
策略组列表	218	范例：区段内部策略邮件服务	234
策略定义	219	范例：区段内部策略设置	239
策略和规则	219	范例：区段内部策略	247
策略的结构	221	范例：全局策略	250
ID	222	输入策略环境	251
区段	222	每个策略组件含多个条目	252
地址	222	地址排除	253
服务	222	范例：目的地址排除	253
动作	223	修改和禁用策略	257
应用	223	策略验证	258
名称	224	重新排序策略	259
VPN 通道确定	224	移除策略	260
L2TP 通道确定	225	第 8 章 地址转换	261
深层检测	225	地址转换简介	262
策略列表顶部位置	225	基于策略的转换选项	269
源地址转换	226	NAT-Src 和 NAT-Dst 的方向特性	273
目的地址转换	226	源网络地址转换	275
用户认证	226	来自 DIP 池 (启用 PAT) 的 NAT-Src	276
HA 会话备份	228	范例：带有 PAT 的 NAT-Src	277

来自 DIP 池 (禁用 PAT) 的 NAT-Src	280
范例：禁用 PAT 的 NAT-Src	280
来自 DIP 池 (带有地址变换) 的 NAT-Src	283
范例：带有地址变换的 NAT-Src	284
来自出口接口 IP 地址的 NAT-Src	289
范例：无 DIP 的 NAT-Src	289
目的网络地址转换	292
目的地址转换的封包流	294
目的地址转换的路由	298
连接到一个接口的地址	299
连接到一个接口但被路由器分隔的地址	300
由接口分隔的地址	301
NAT-Dst: 一对一映射	302
范例：一对一目的地址转换	303
从一个地址到多个地址的转换	307
范例：一对多目的地址转换	307
NAT-Dst: 多对一映射	311
范例：多对一目的地址转换	311
NAT-Dst: 多对多映射	316
范例：多对多目的地址转换	317
带有端口映射的 NAT-Dst	321
范例：带有端口映射的 NAT-Dst	321
同一策略中的 NAT-Src 和 NAT-Dst	326
范例：结合 NAT-Src 和 NAT-Dst	326
映射 IP 地址	347
MIP 和 Global 区段	348
范例：Untrust 区段接口上的 MIP	349

范例：从不同区段到达 MIP	352
范例：将 MIP 添加到 Tunnel 接口	357
MIP-Same-as-Untrust	358
范例：Untrust 接口上的 MIP	359
MIP 和回传接口	362
范例：两个通道接口的 MIP	363
虚拟 IP 地址	372
VIP 和 Global 区段	375
范例：配置虚拟 IP 服务器	375
范例：编辑 VIP 配置	378
范例：移除 VIP 配置	378
范例：具有定制和多端口服务的 VIP	379
第 9 章 用户认证	387
认证服务器	388
本地数据库	390
支持的用户类型和功能	390
范例：本地数据库超时	391
外部 Auth 服务器	392
Auth 服务器对象属性	393
Auth 服务器类型	395
RADIUS	395
RADIUS Auth 服务器对象属性	396
支持的用户类型和功能	396
NetScreen 词典文件	397
RADIUS 访问质询	398
SecurID	400
SecurID Auth 服务器对象属性	401
支持的用户类型和功能	401
LDAP	402

LDAP Auth 服务器对象属性	403	范例：XAuth 认证 (本地用户组)	458
支持的用户类型和功能	403	范例：XAuth 认证 (外部用户)	460
定义 Auth 服务器对象	404	范例：XAuth 认证 (外部用户组)	463
范例：RADIUS Auth 服务器	404	范例：XAuth 认证和地址分配 (本地用户组)	468
范例：SecurID Auth 服务器	407	XAuth 客户端	474
范例：LDAP Auth 服务器	409	范例：NetScreen 设备作为 XAuth 客户端	475
定义缺省 Auth 服务器	411	L2TP 用户和用户组	476
范例：更改缺省 Auth 服务器	411	范例：本地和外部 L2TP Auth 服务器	477
认证类型及应用	413	Admin 用户	481
Auth 用户和用户组	414	多类型用户	483
在策略中引用 Auth 用户	414	组表达式	484
在策略中引用 Auth 用户组	418	范例：组表达式 (AND)	486
范例：运行时认证 (本地用户)	419	范例：组表达式 (OR)	488
范例：运行时认证 (本地用户组)	422	范例：组表达式 (NOT)	490
范例：运行时认证 (外部用户)	425	标题自定义	492
范例：运行时认证 (外部用户组)	428	范例：自定义 WebAuth 标题	492
范例：多个组中的本地 Auth 用户	432	第 10 章 信息流整形	493
范例：WebAuth (本地用户组)	436	应用信息流整形	494
范例：WebAuth (外部用户组)	439	在策略级管理带宽	494
范例：WebAuth + SSL (外部用户组)	443	范例：信息流整形	495
IKE 用户和用户组	447	设置服务优先级	501
范例：定义 IKE 用户	448	范例：优先级排列	502
范例：创建 IKE 用户组	450	第 11 章 系统参数	509
在网关中引用 IKE 用户	451	域名系统支持	511
XAuth 用户和用户组	452	DNS 查找	512
IKE 协商中的 XAuth 用户	453		
范例：XAuth 认证 (本地用户)	456		

DNS 状态表.....	513
范例：DNS 服务器和刷新进度	514
范例：设置 DNS 刷新时间间隔	515
DHCP	516
DHCP 服务器	518
范例：NetScreen 设备作为 DHCP 服务器	518
NSRP 集群中的 DHCP 服务器	524
DHCP 服务器检测	524
范例：打开 DHCP 服务器检测	525
范例：关闭 DHCP 服务器检测	525
DHCP 中继代理	526
范例：NetScreen 设备作为 DHCP 中继代理	527
DHCP 客户端	532
范例：NetScreen 设备作为 DHCP 客户端	532
TCP/IP 设置传播	534
范例：转发 TCP/IP 设置	535
PPPoE	537
范例：设置 PPPoE	537
范例：在主 Untrust 接口和备份 Untrust 接口上配置 PPPoE	542
下载 / 上传设置和固件	544
保存和导入设置	544
上传和下载固件	546

配置回滚	547
上次已知正确的配置	547
自动与手动配置回滚	547
加载新的配置文件	549
锁定配置文件	550
向配置文件添加注释	551
许可密钥	552
范例：扩大用户容量	553
签名服务的注册与激活	554
临时服务	554
在新设备上捆绑 AV 和 DI 服务	554
与 DI 一起更新 AV 服务	555
只更新 DI 服务	556
系统时钟	557
日期和时间	557
时区	557
NTP	558
多个 NTP 服务器	558
最大时间调整	558
NTP 与 NSRP	559
范例：配置 NTP 服务器和最大时间差值	560
保护 NTP 服务器	561
索引	IX-I

前言

第 2 卷的“基本原理”介绍了 ScreenOS 的体系结构及其组成元素，包括配置不同元素的范例。本卷介绍以下内容：

- 安全性、通道和功能区段
- 路由基础，包括路由表和配置静态路由的方式。
- 各种接口类型，如物理接口、子接口、虚拟安全接口 (VSI)、冗余接口、聚合接口和 VPN 通道接口
- 源网络地址转换和网络地址转换 (NAT-src 和 NAT-dst)、映射 IP (MIP) 地址、虚拟 IP (VIP) 地址、动态 IP (DIP) 地址
- NetScreen 接口可以在其下运行的接口模式：网络地址转换 (NAT)、路由和透明
- 用来控制流过接口的信息流的策略，以及用来创建策略和虚拟专用网的元素，如地址、用户和服务
- NetScreen 设备可用的用户认证方法以及如何配置用户帐户和用户组
- 信息流管理方面的概念
- 下列功能的系统参数：
 - “域名系统” (DNS) 寻址
 - 用于分配或转递 TCP/IP 设置的“动态主机配置协议” (DHCP)
 - URL 过滤
 - 向 NetScreen 设备上传以及从 NetScreen 设备下载配置设置和软件
 - 用来扩充 NetScreen 设备功能的许可密钥
 - 系统时钟配置

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 xi 页上的 “WebUI 约定”
- 第 xiii 页上的 “插图约定”
- 第 xiv 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：

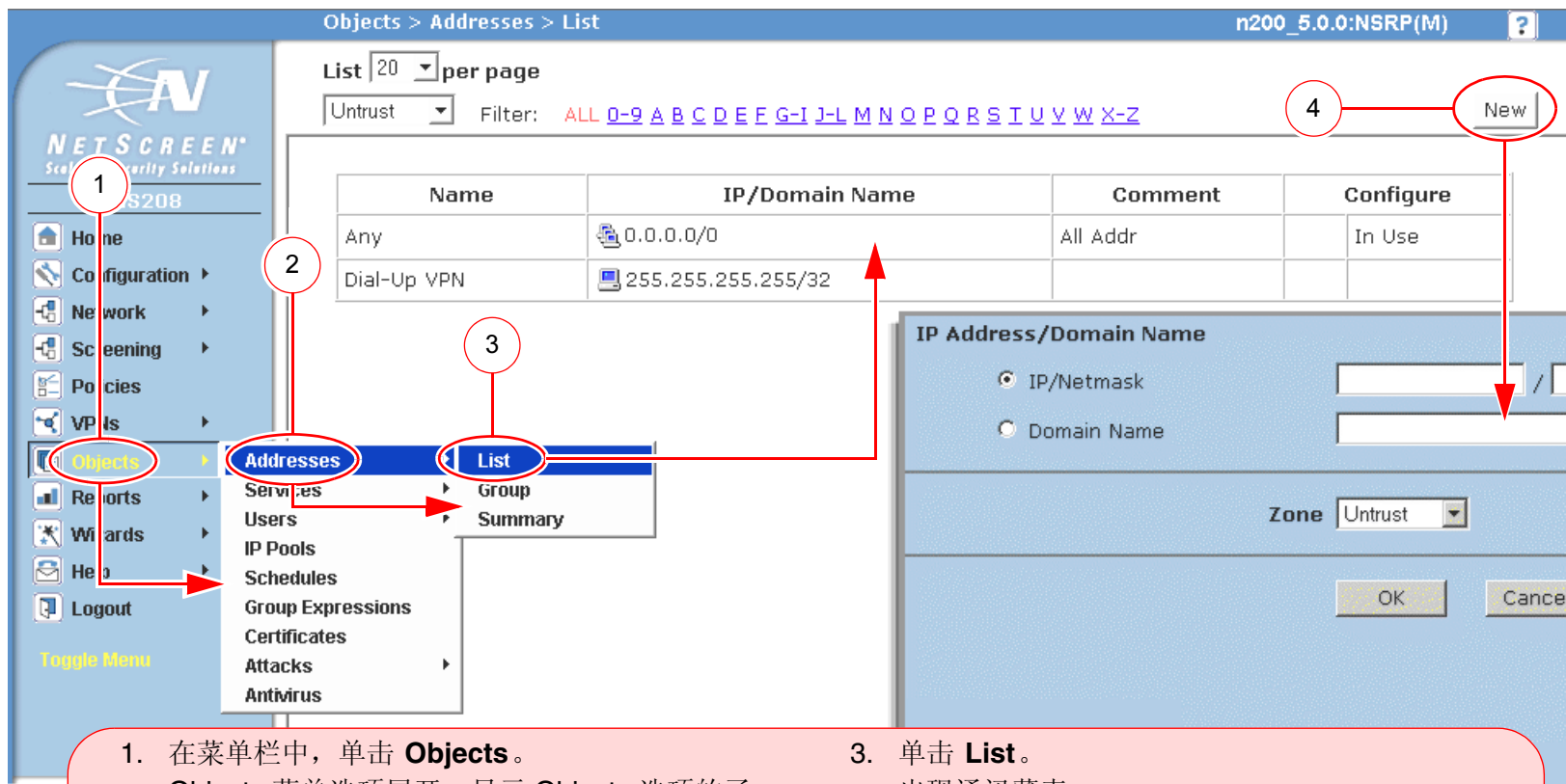
- 在中括号 [] 中的任何内容都是可选的。
- 在大括号 { } 中的任何内容都是必需的。
- 如果选项不止一个，则使用管道 (|) 分隔每个选项。例如，
`set interface { ethernet1 | ethernet2 | ethernet3 } manage`
意味着 “设置 **ethernet1**、**ethernet2** 或 **ethernet3** 接口的管理选项”。
- 变量以斜体方式出现。例如：
`set admin user name password`

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，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

The screenshot shows the NetScreen WebUI configuration page for creating a new address object. The breadcrumb path at the top is "Objects > Addresses > Configuration". The page title is "n200_5.0.0:NSRP(M)". The left sidebar shows the navigation menu with "Configuration" selected. The main content area is titled "Address Name: addr_1" and "Comment". The "IP Address/Domain Name" section has two radio buttons: "IP/Netmask" (selected) and "Domain Name". The "IP/Netmask" field is set to "10.2.2.5 / 32". The "Zone" dropdown menu is set to "Untrust". At the bottom, there are "OK" and "Cancel" buttons. A red box on the right contains the text: "注意：由于没有 Comment 字段的说明，请保持其内容不变。". Red circles and lines highlight the configuration steps: "Address Name: addr_1", "IP Address Name/Domain Name: IP/Netmask: (选择), 10.2.2.5/32", "Zone: Untrust", and the "OK" button.

Address Name: addr_1

Comment

IP Address/Domain Name

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

单击 **OK**。

注意：由于没有 Comment 字段的说明，请保持其内容不变。

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：



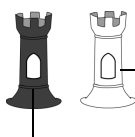
通用 NetScreen 设备



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)



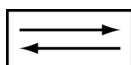
通道接口



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，则整个名称字符串的两边必须用双引号 (“ ”) ；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 将多个连续的空格处理为单个空格。
- 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、欧洲语和希伯来语。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。*

- ASCII 字符从 32 (十六进制 0x20) 到 255 (0xff)，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 NetScreen 产品的技术文档，请访问 www.netscreen.com/resources/manuals/。

要获取 NetScreen 软件的最新版本，请访问 www.netscreen.com。您必须先注册成为经过授权的用户，然后才能执行此类下载。

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

ScreenOS 体系结构

NetScreen ScreenOS 体系结构为网络安全布局的设计提供了极大的灵活性。在具有两个以上接口的 NetScreen 设备上，可以创建多个安全区并配置策略以调节区段内部及区段之间的信息流。可以为每个区段绑定一个或多个接口，并在每个区段上启用一组唯一的管理和防火墙攻击屏蔽选项。实际上，利用 ScreenOS 可以创建网络环境所需的区段数，分配每个区段所需的接口数，并且可以根据自己的特殊要求来设计每个接口。

本章对 ScreenOS 进行了简要介绍，包括以下几个主要内容：

- 第 2 页上的“安全区”
- 第 3 页上的“安全区接口”
- 第 5 页上的“虚拟路由器”
- 第 6 页上的“策略”
- 第 8 页上的“VPN”
- 第 10 页上的“虚拟系统”

此外，要更好地了解 ScreenOS 处理信息流的机制，请参阅第 11 页上的“封包流序列”中的内向封包的流序列。

本章结束时给出了一个由四部分组成的范例，它例举了使用 ScreenOS 的 NetScreen 设备的基本配置：

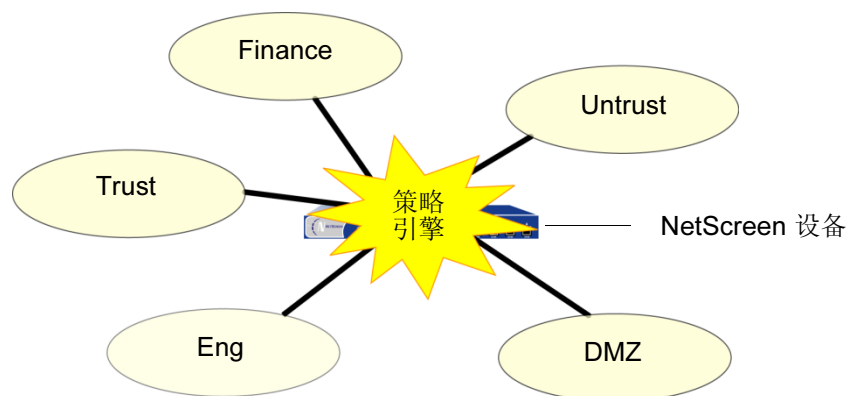
- 第 14 页上的“范例 (第 1 部分): 具有六个区段的企业”
- 第 16 页上的“范例 (第 2 部分): 六个区段的接口”
- 第 20 页上的“范例 (第 3 部分): 两个路由选择域”
- 第 22 页上的“范例 (第 4 部分): 策略”

安全区

安全区是由一个或多个网段组成的集合，需要通过策略来对入站和出站信息流进行调整（参见第 6 页上的“策略”）¹。安全区是绑定了一个或多个接口的逻辑实体。通过多种类型的 NetScreen 设备，您可以定义多个安全区，确切数目可根据网络需要来确定。除用户定义的区段外，您还可以使用预定义的区段：Trust、Untrust 和 DMZ（用于第 3 层操作），或者 V1-Trust、V1-Untrust 和 V1-DMZ（用于第 2 层操作）²。如果愿意，可以继续使用这些预定义区段。也可以忽略预定义区段而只使用用户定义的区段³。另外，您还可以同时使用这两种区段——预定义和用户定义。利用区段配置的这种灵活性，您可以创建能够最好地满足您的具体需要的网络设计。

配置了 5 个安全区的网络 — 3 个缺省区段 (Trust、Untrust、DMZ)，和两个用户定义的区段 (Finance、Eng)

信息流（以黑线表示）只有在策略允许时才能由一个安全区传递到另一区段。



1. 无需任何网段的安全区是全域区段。（有关详细信息，请参阅 Global 区段第 48 页上的“Global 区段”。）另外，任何区段，如果既没有绑定到它的接口也没有通讯簿条目，则也可以说它不包含任何网段。
2. 如果是从 ScreenOS 的早期版本进行升级，则这些区段的所有配置将保持不变。
3. 不能删除预定义安全区。但是，可以删除用户定义的安全区。删除安全区时，还会同时自动删除为该区段配置的所有地址。

安全区接口

安全区的接口可以视为一个入口，TCP/IP 信息流可通过它在该区段和其它任何区段之间进行传递。

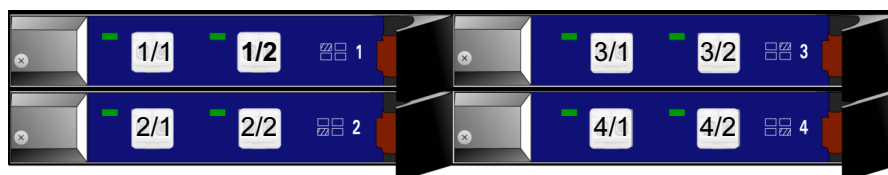
通过定义的策略，可以使两个区段间的信息流向一个或两个方向流动⁴。利用定义的路由，可指定信息流从一个区段到另一个区段必须使用的接口。由于可将多个接口绑定到一个区段上，所以您制定的路由对于将信息流引向您所选择的接口十分重要。

要允许信息流从一个区段流到另一个区段，需要将一个接口绑定到该区段，而且要 — 对于“路由”或 NAT 模式的接口 (参见第 5 章，“接口模式”) — 为该接口分配一个 IP 地址。两种常见的接口类型为物理接口和 — 对于那些具有虚拟系统支持的设备 — 子接口 (即，物理接口在第 2 层的具体体现)。有关详细信息，请参阅第 4 章，“接口”。

物理接口

物理接口与 NetScreen 设备上实际存在的组件有关。接口命名约定因设备而异。例如，在 NetScreen-500 上，物理接口由接口模块的位置及该模块上的以太网端口标识。例如，接口 *ethernet1/2* 表示接口模块在**第一槽位** (*ethernet1/2*)和**第二个端口** (*ethernet1/2*)。

物理接口分配



注意：要了解具体的 NetScreen 设备的命名约定，请参阅该设备的“用户指南”。

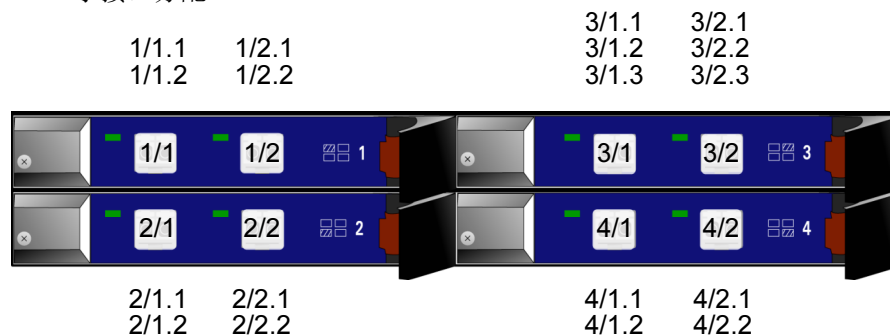
4. 对于在绑定到同一区段的两个接口间流动的信息流，因为两个接口具有相同的安全级别，所以不需要策略。ScreenOS 对于两个区段间的信息流需要策略，如果是在一个区段内，则不需要。

子接口

在支持虚拟 LAN (VLAN) 的设备上，可以在逻辑上将一个物理接口分为几个虚拟的子接口，每个子接口都从它来自的物理接口借用需要的带宽。子接口是一个抽象的概念，但它在功能上与物理接口相同，子接口由 802.1Q VLAN 标记⁵进行区分。NetScreen 设备子接口通过它的 IP 地址和 VLAN 标记来指引信息流流入和流出区段。为方便起见，网络管理员使用的 VLAN 标记号通常与子接口号相同。例如，使用 VLAN 标记 3 的接口 `ethernet1/2` 命名为 `ethernet1/2.3`。这表示接口模块在第一槽位，第二个端口在该模块上，子接口号为 3 (`ethernet1/2.3`)。

请注意，虽然子接口与物理接口共享部分标识，但是其绑定的区段并不依赖于物理接口绑定的区段。您可以将子接口 `ethernet1/2.3` 绑定到与物理接口 `ethernet1/2` 或 `ethernet1/2.2` 所绑定的不同区段上。同样，IP 地址的分配也没有限制。术语 *子接口* 并不意味着它的地址在物理接口的地址空间的子网中。

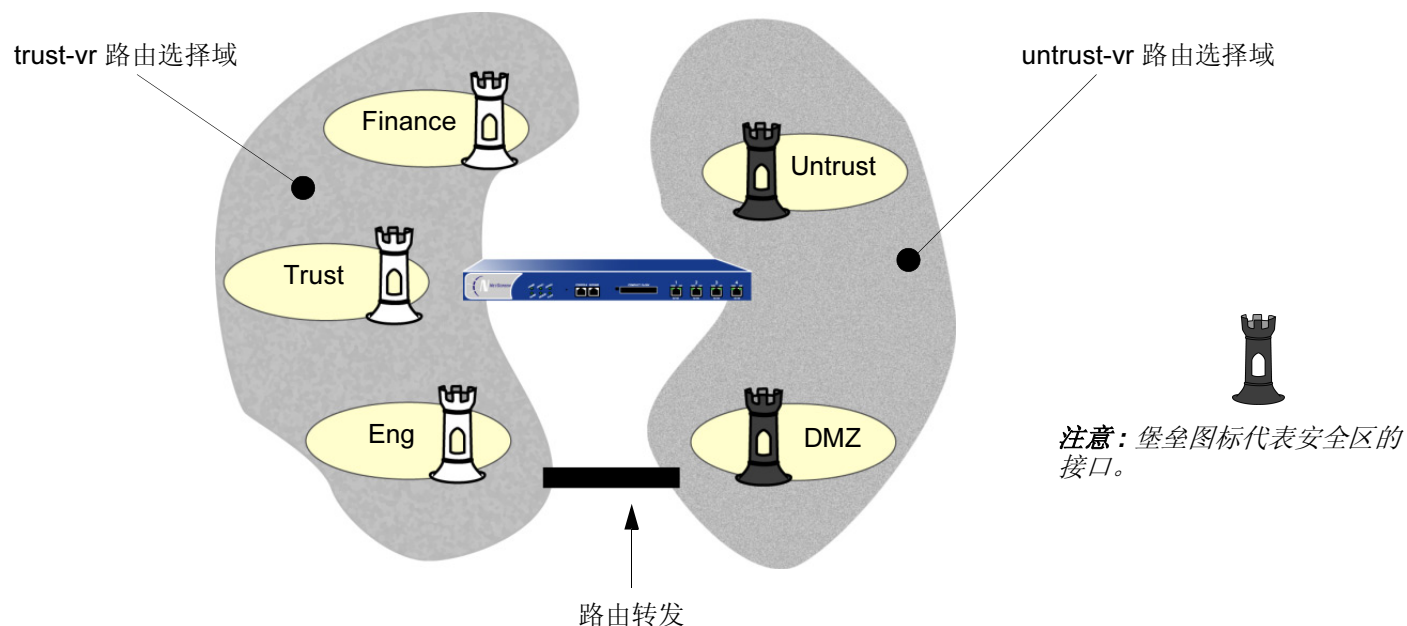
子接口分配



5. 802.1Q 是一个 IEEE 标准，它定义了实现虚拟桥接 LAN 的机制以及用来通过 VLAN 标记指示 VLAN 从属关系的以太网帧格式。

虚拟路由器

虚拟路由器 (VR) 的功能与路由器相同。它拥有自己的接口和路由表。在 ScreenOS 中，NetScreen 设备支持两个预定义的虚拟路由器，从而允许 NetScreen 设备维护两个单独的路由表，并隐藏虚拟路由器彼此之间的路由信息。例如，untrust-vr 通常用来与不可信方进行通信，并且不含有保护区段的任何路由信息。保护区段的路由信息由 trust-vr 进行维护。因此，通过从 untrust-vr 中秘密提取路由的方式，搜集不到任何内部网络信息。



NetScreen 设备上存在两个虚拟路由器时，即使存在允许信息流的策略，也不能在驻留于不同 VR 中的区段之间自动转发信息流。如果希望信息流在虚拟路由器之间传递，则需要导出 VR 之间的路由或在一个 VR 中配置静态路由将另一个 VR 定义为下一跳。有关使用两个虚拟路由器的详细信息，请参阅第 6 卷，“动态路由”。

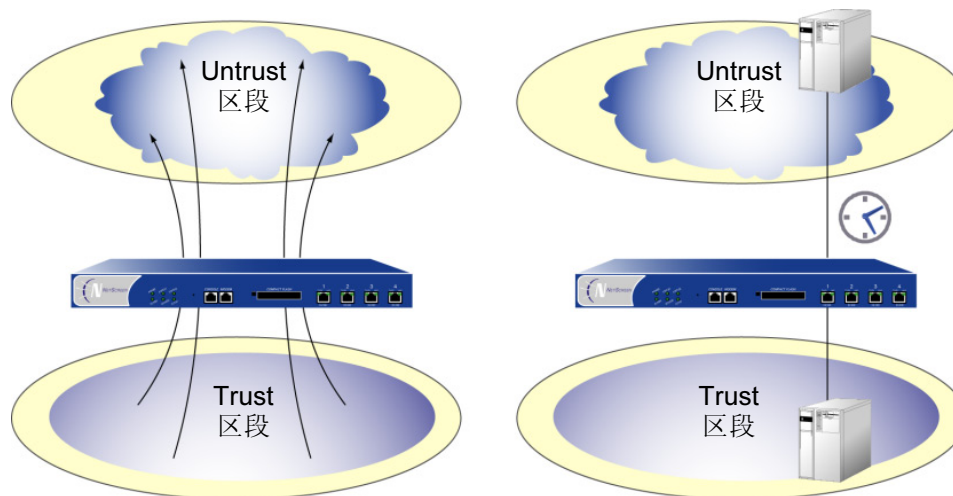
策略

NetScreen 设备用于保护网络的安全，具体做法是先检查要求从一个安全区到另一区段的通路的所有连接尝试，然后予以允许或拒绝。

在缺省情况下，**NetScreen** 设备拒绝所有方向的所有信息流⁶。通过创建策略，定义允许在预定时间通过指定源地点到达指定目的地点的信息流的种类，您可以控制区段间的信息流。范围最大时，可以允许所有类型的信息流从一个区段中的任何源地点到其它所有区段中的任何目的地点，而且没有任何预定时间限制。范围最小时，可以创建一个策略，只允许一种信息流在预定的时间段内、在一个区段中的指定主机与另一区段中的指定主机之间流动。

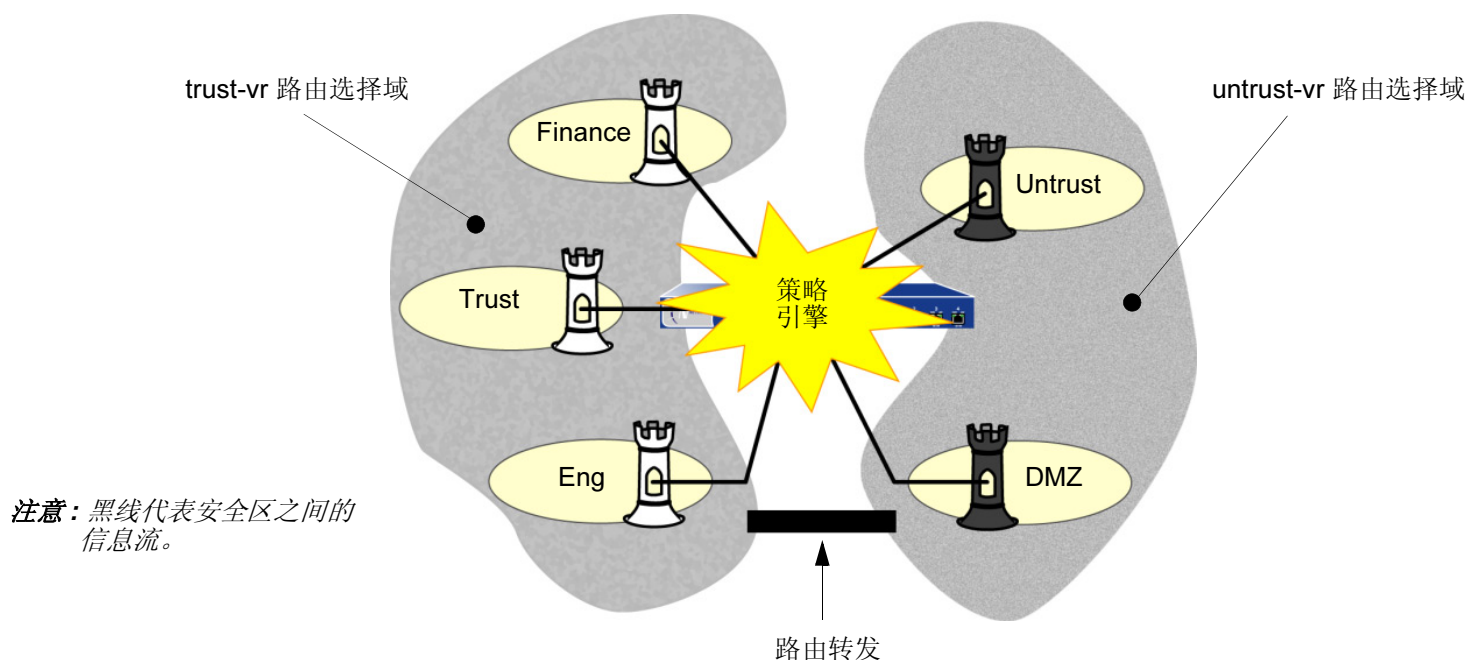
广义的互联网访问：任何服务可在任何时间、从 **Trust** 区段的任何一点到 **Untrust** 区段的任何一点

狭义的互联网访问：**SMTP** 服务从上午 5:00 点到下午 7:00 点、从 **Trust** 区段中的邮件服务器到 **Untrust** 区段中的邮件服务器



6. 某些 **NetScreen** 设备出厂时设置的缺省策略为允许所有从 **Trust** 区段到 **Untrust** 区段的出站信息流，但拒绝所有从 **Untrust** 区段到 **Trust** 区段的入站信息流。

每次当封包尝试从一个区段向另一区段或在绑定到同一区段的两个接口间传递时，NetScreen 设备会检查其策略组列表中是否有允许这种信息流的策略（请参阅第 218 页上的“策略组列表”）。要使信息流可以从一个安全区传递到另一个区段——例如，从区段 A 到区段 B——必须配置一个允许区段 A 发送信息流到区段 B 的策略。要使信息流向另一方向流动，则必须配置另一策略，允许信息流从区段 B 流向区段 A。对于从一个区段向另一区段传递的任何信息流，都必须有允许它的策略。同样，如果启用了内部区段阻塞，则必须要有允许信息流在该区段中从一个接口向另一个接口传递的策略。



注意：有关策略方面的详细信息，请参阅第 7 章，“策略”。

VPN

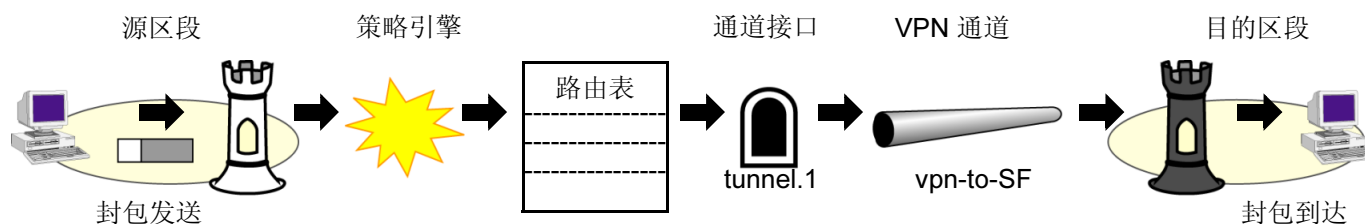
ScreenOS 支持多个虚拟专用网络 (VPN) 配置选项。两种主要类型如下：

- **基于路由的 VPN** – 路由查找确定 NetScreen 设备封装哪些信息流。策略允许或拒绝信息流到达路由中指定的目标。如果策略允许信息流并且路由引用绑定到 VPN 通道的通道接口，则 NetScreen 设备也封装该策略。此配置将策略的应用与 VPN 通道的应用分离。配置完成后，这些通道就成为可用的资源，用于保护一个安全区与另一区段之间传递的信息流。
- **基于策略的 VPN** – 策略查找确定：在策略引用特定 VPN 通道并将 “tunnel” 指定为操作时 NetScreen 设备封装哪些信息流。

对于站点到站点 VPN 配置来说，基于路由的 VPN 是一种很好的选择，因为您可以将多个策略应用到流经单个 VPN 通道的信息流。对于拨号 VPN 来说，基于策略的 VPN 是一种很好的选择，因为拨号客户端可能没有可以设置路由的内部 IP 地址。

以下步骤介绍基于路由的 VPN 配置中涉及到的主要元素：

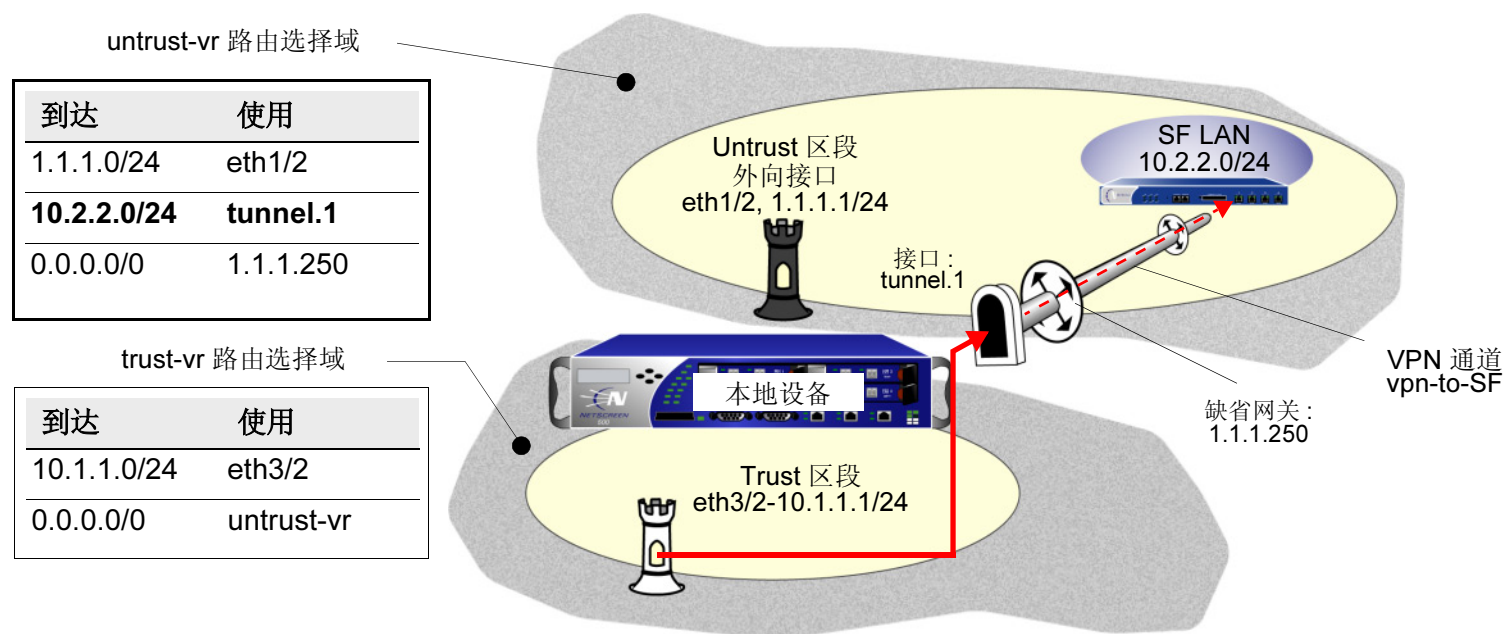
1. 配置 VPN 通道时 (例如, *vpn-to-SF*, 其中 *SF* 为目的或端实体), 将本地设备上的一个物理接口或子接口指定为外向接口。(远程对等方配置其远程网关时, 必须使用此接口的 IP 地址。)
2. 创建一个通道接口 (例如, *tunnel.1*), 将其绑定到一个安全区⁷。
3. 将通道接口 *tunnel.1* 绑定到 VPN 通道 *vpn-to-SF* 上。
4. 要引导信息流通过此通道, 请设置一个路由, 指明到 *SF* 的信息流必须使用 *tunnel.1*。



7. 不必将该通道接口绑定到 VPN 信息流发往的同一区段上。如果路由指向某通道接口，则到任何区段的信息流都可以访问该接口。

此时，该通道已就绪，为 SF 绑定的信息流可以从中通过。现在，您可以创建通讯簿条目，如“Trust LAN” (10.1.1.0/24) 和“SF LAN” (10.2.2.0/24)，并设置策略，允许或阻止不同类型的信息流从指定源 (如“Trust LAN”) 传递到指定目标 (如“SF LAN”)。

本地 NetScreen 设备将信息流通过 tunnel.1 接口从 Trust 区段发送到 Untrust 区段中的“SF LAN”。因为 tunnel.1 绑定到 VPN 通道“vpn-to-SF”上，所以 NetScreen 设备加密信息流并通过该通道将信息流发送到远程对方。



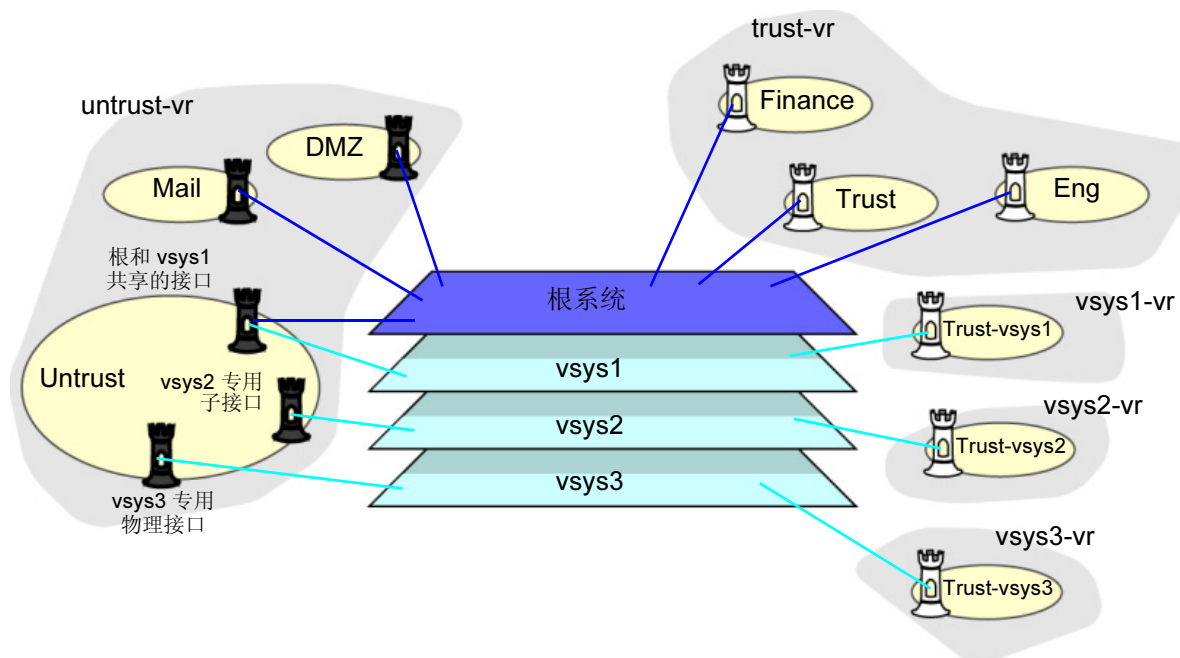
注意：有关 VPN 的详细信息，请参阅第 5 卷，“VPN”。

虚拟系统

一些 **NetScreen** 设备支持虚拟系统 (**vsys**)。虚拟系统是对主系统的细分, 在用户看来, 它就像是一个独立的实体。虚拟系统相对于同一 **NetScreen** 设备中的任何其它虚拟系统以及根系统是独立存在的。将 **ScreenOS** 应用于虚拟系统需要协调三个主要成员: 区段、接口和虚拟路由器。下面的图例从概念上简要说明 **ScreenOS** 如何同时在根级和 **vsys** 级上将这些成员紧密结合在一起。



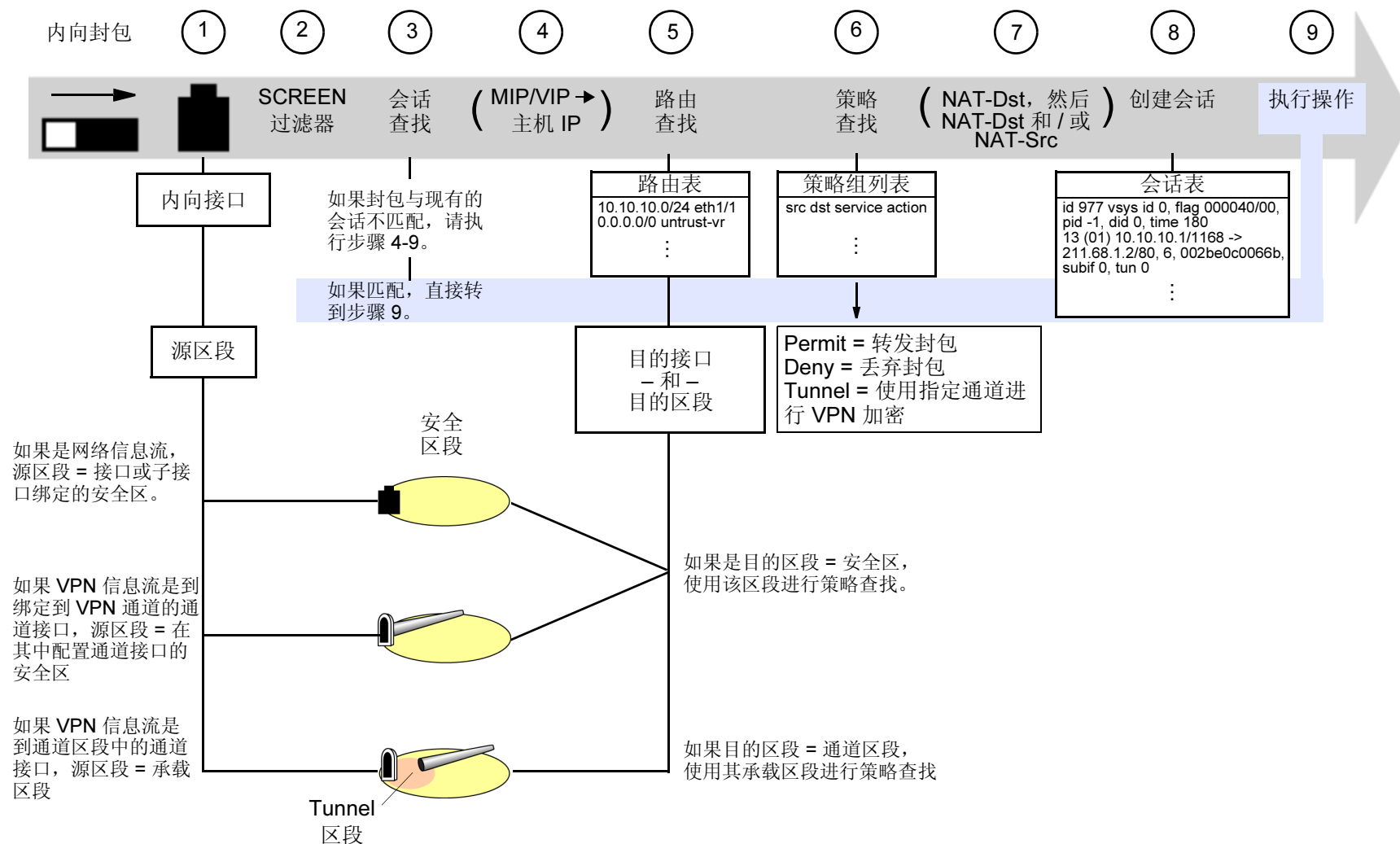
注意：堡垒图标代表安全区接口。



注意：有关虚拟系统以及在虚拟系统环境中应用区段、接口和虚拟路由器的详细信息，请参阅第 7 卷，“虚拟系统”。

封包流序列

在 ScreenOS 中，内向封包的流序列按如下所示的方式进行。



1. 接口模块识别内向接口，进而识别绑定到该接口的源区段。
源区段根据以下判别条件进行确定：
 - 如果包没有封装，源区段为内向接口或子接口绑定的安全区。
 - 如果包进行了封装并且通道接口绑定到 **VPN** 通道上，源区段为在其中配置通道接口的安全区。
 - 如果包进行了封装并且通道接口位于通道区段，源区段为该通道区段相应的承载区段 (携带通道区段的安全区)。
2. 此时，如果启用了源区段的 **SCREEN** 选项，则 **NetScreen** 设备激活 **SCREEN** 模块。**SCREEN** 检查可以生成下列三种结果之一：
 - 如果 **SCREEN** 机制检测到异常行为 (对此行为已配置 **NetScreen** 设备封锁该封包)，则 **NetScreen** 设备会丢弃该封包并在事件日志中生成一个条目。
 - 如果 **SCREEN** 机制检测到异常行为 (对此行为已配置 **NetScreen** 设备记录事件但不封锁该封包)，则 **NetScreen** 设备在入口接口的 **SCREEN** 计数器列表中记录该事件并继续下一步骤。
 - 如果 **SCREEN** 机制没有检测到异常行为，则 **NetScreen** 设备继续下一步骤。
3. 会话模块执行会话查找，尝试用现有会话与该数据包进行匹配。
如果该数据包与现有会话不匹配，**NetScreen** 设备会执行“首包处理”，该过程包括下面的步骤 4 到 9。
如果该包与现有会话匹配，**NetScreen** 设备会执行“快速处理”，用现有会话条目中可用的信息来处理该封包。“快速处理”会跳过步骤 4 到 8，因为这些步骤产生的信息已经在会话的首包处理期间获得。
4. 如果使用映射 IP (MIP) 或虚拟 IP (VIP) 地址，地址映射模块会对 MIP 或 VIP 进行解析以便路由表能查找到实际的主机地址。

5. 路由表查找程序寻找指向目的地址的接口。同时，接口模块识别该接口绑定的目的区段。

目的区段根据以下判别条件进行确定：

- 如果目的区段是安全区，请使用该区段进行策略查找。
 - 如果目的区段是通道区段，请使用相应的承载区段进行策略查找。
6. 策略引擎搜寻策略组列表，以便在识别出来的源和目的区段中的地址之间查找策略。
在策略中配置的操作决定 NetScreen 防火墙将会对包执行的动作：
 - 如果操作为 **Permit**, NetScreen 设备会决定将封包转发到其目标地点。
 - 如果操作为 **Deny**, NetScreen 设备会决定将封包丢弃。
 - 如果操作为 **Tunnel**, NetScreen 设备会决定将封包转发给 VPN 模块，该模块对封包进行封装并用指定的 VPN 通道设置进行传送。
 7. 如果策略中指定了目的地址转换 (NAT-dst)，则 NAT 模块会将 IP 封包包头中的初始目的地址转换成一个不同的地址。

如果指定了源地址转换 (基于接口的 NAT 或基于策略的 NAT-src)，则 NAT 模块会在将 IP 封包包头中的源地址转发到目标地点或 VPN 模块前对其进行转换。

(如果同一策略中同时指定了 NAT-dst 和 NAT-src，则 NetScreen 设备会首先执行 NAT-dst，然后执行 NAT-src。)

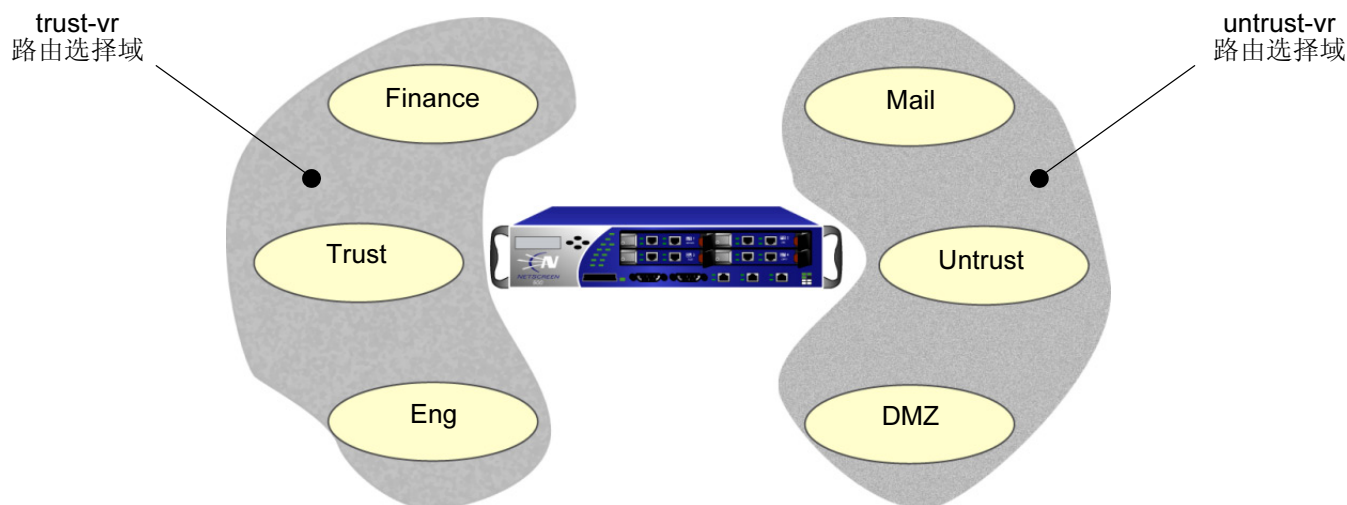
8. 会话模块在会话表中创建一个新条目，其中包含步骤 1 到 7 的结果。
随后，NetScreen 设备使用该会话条目中所含的信息来处理同一会话的后续数据包。
9. NetScreen 设备执行在会话中指定的操作。
典型的操作有源地址转换、VPN 通道选择、加密、解密和包转发。

范例 (第 1 部分): 具有六个区段的企业

共有四部分范例，这是第一部分范例，目的是为了说明前面几节介绍的部分概念。在第二部分中将设置每个区段的接口，请参阅第 16 页上的“范例 (第 2 部分): 六个区段的接口”。在这里为企业配置以下六个区段：

- Finance
- Trust
- Eng
- Mail
- Untrust
- DMZ

Trust、Untrust 和 DMZ 区段是预先配置的。您必须对 Finance、Eng 和 Mail 区段进行定义。在缺省情况下，用户定义的区段位于 **trust-vr** 路由选择域中。因而，不必为 Finance 和 Eng 区段指定虚拟路由器。但是，除了配置 Mail 区段外，您还需要指定它在 **untrust-vr** 路由选择域中。还必须将 Untrust 和 DMZ 区段的虚拟路由器绑定设置从 **trust-vr** 转移到 **untrust-vr**⁸。



8. 有关虚拟路由器及其路由选择域的详细信息，请参阅第 2 章，“路由表和静态路由”。

WebUI

Network > Zones > New: 输入以下内容，然后单击 **OK**:

Zone Name: Finance

Virtual Router Name: trust-vr

Zone Type: Layer 3: (选择)

Network > Zones > New: 输入以下内容，然后单击 **OK**:

Zone Name: Eng

Virtual Router Name: trust-vr

Zone Type: Layer 3: (选择)

Network > Zones > New: 输入以下内容，然后单击 **OK**:

Zone Name: Mail

Virtual Router Name: untrust-vr

Zone Type: Layer 3: (选择)

Network > Zones > Edit (对于 Untrust): 在 Virtual Router Name 下拉列表中选择 **untrust-vr**，然后单击 **OK**。

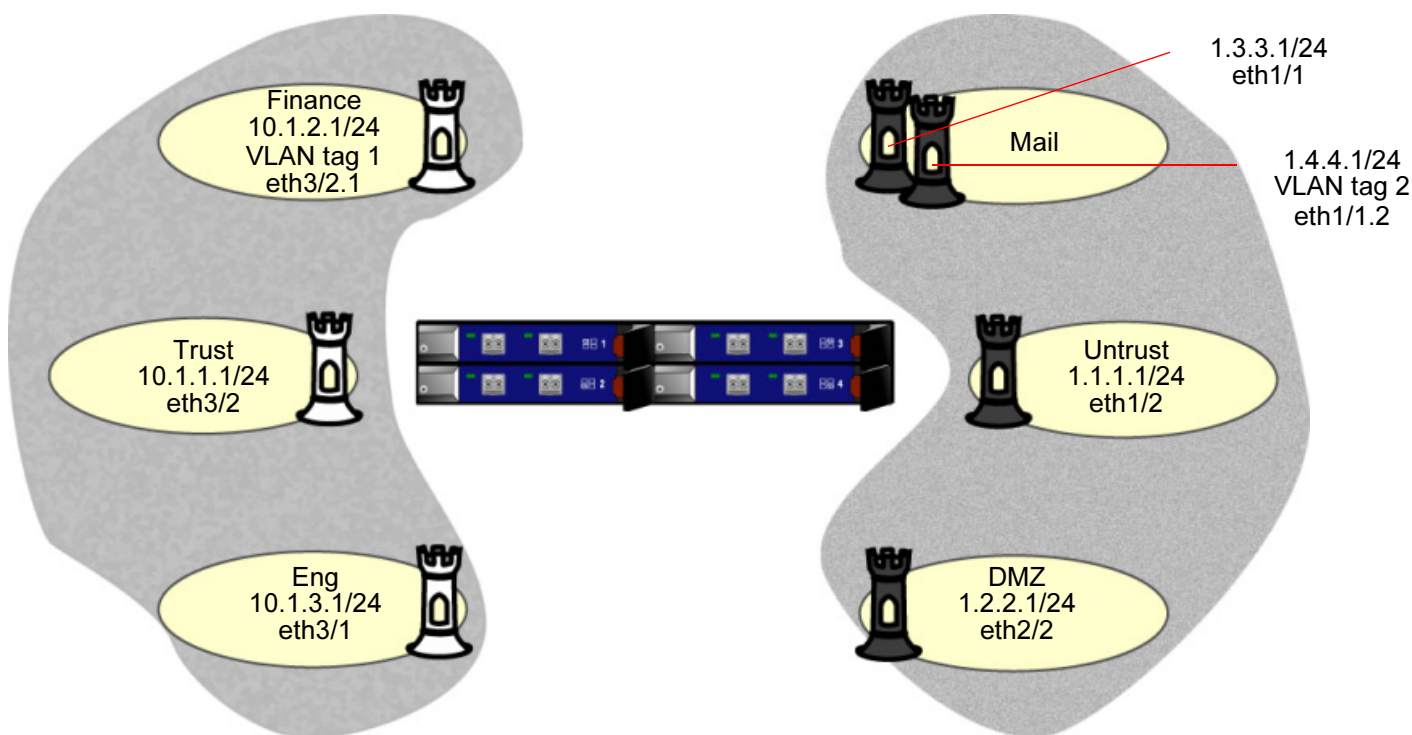
Network > Zones > Edit (对于 DMZ): 在 Virtual Router Name 下拉列表中选择 **untrust-vr**，然后单击 **OK**。

CLI

```
set zone name finance
set zone name eng
set zone name mail
set zone mail vrouter untrust-vr
set zone untrust vrouter untrust-vr
set zone dmz vrouter untrust-vr
save
```

范例 (第 2 部分): 六个区段的接口

这是一个渐进式范例的第二部分。在第一部分中，对区段进行了配置，请参阅第 14 页上的“范例 (第 1 部分): 具有六个区段的企业”。在下一部分中，将对虚拟路由器进行配置，请参阅第 20 页上的“范例 (第 3 部分): 两个路由选择域”。范例的这一部分演示了如何将接口绑定到区段上并为其配置 IP 地址和各种管理选项。



WebUI

1. 接口 ethernet3/2

Network > Interfaces > Edit (对于 ethernet3/2): 输入以下内容, 然后单击 **OK**:

Zone Name: Trust

Static IP: (有此选项时将其选定)

IP Address/Netmask: 10.1.1.1/24

Manageable: (选择)

Management Services: WebUI, Telnet, SNMP, SSH (选择)

Other Services: Ping (选择)

2. 接口 ethernet3/2.1

Network > Interfaces > Sub-IF New: 输入以下内容, 然后单击 **OK**:

Interface Name: ethernet3/2.1

Zone Name: Finance

Static IP: (有此选项时将其选定)

IP Address/Netmask: 10.1.2.1/24

VLAN Tag: 1

Other Services: Ping (选择)

3. 接口 ethernet3/1

Network > Interfaces > Edit (对于 ethernet3/1): 输入以下内容, 然后单击 **OK**:

Zone Name: Eng

Static IP: (有此选项时将其选定)

IP Address/Netmask: 10.1.3.1/24

Other Services: Ping (选择)

4. 接口 ethernet1/1

Network > Interfaces > Edit (对于 ethernet1/1): 输入以下内容, 然后单击 **OK**:

Zone Name: Mail

Static IP: (有此选项时将其选定)

IP Address/Netmask: 1.3.3.1/24

5. 接口 ethernet1/1.2

Network > Interfaces > Sub-IF New: 输入以下内容, 然后单击 **OK**:

Interface Name: ethernet1/1.2

Zone Name: Mail

Static IP: (有此选项时将其选定)

IP Address/Netmask: 1.4.4.1/24

VLAN Tag: 2

6. 接口 ethernet1/2

Network > Interfaces > Edit (对于 ethernet1/2): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (有此选项时将其选定)

IP Address/Netmask: 1.1.1.1/24

Manageable: (选择)

Management Services: SNMP (选择)

7. 接口 ethernet2/2

Network > Interfaces > Edit (对于 ethernet2/2): 输入以下内容, 然后单击 **OK**:

Zone Name: DMZ

Static IP: (选择)

IP Address/Netmask: 1.2.2.1/24

CLI

1. 接口 ethernet3/2

```
set interface ethernet3/2 zone trust
set interface ethernet3/2 ip 10.1.1.1/24
set interface ethernet3/2 manage ping
set interface ethernet3/2 manage webui
set interface ethernet3/2 manage telnet
set interface ethernet3/2 manage snmp
set interface ethernet3/2 manage ssh
```

2. 接口 ethernet3/2.1

```
set interface ethernet3/2.1 tag 1 zone finance
set interface ethernet3/2.1 ip 10.1.2.1/24
set interface ethernet3/2.1 manage ping
```

3. 接口 ethernet3/1

```
set interface ethernet3/1 zone eng
set interface ethernet3/1 ip 10.1.3.1/24
set interface ethernet3/1 manage ping
```

4. 接口 ethernet1/1

```
set interface ethernet1/1 zone mail
set interface ethernet1/1 ip 1.3.3.1/24
```

5. 接口 ethernet1/1.2

```
set interface ethernet1/1.2 tag 2 zone mail
set interface ethernet1/1.2 ip 1.4.4.1 /24
```

6. 接口 ethernet1/2

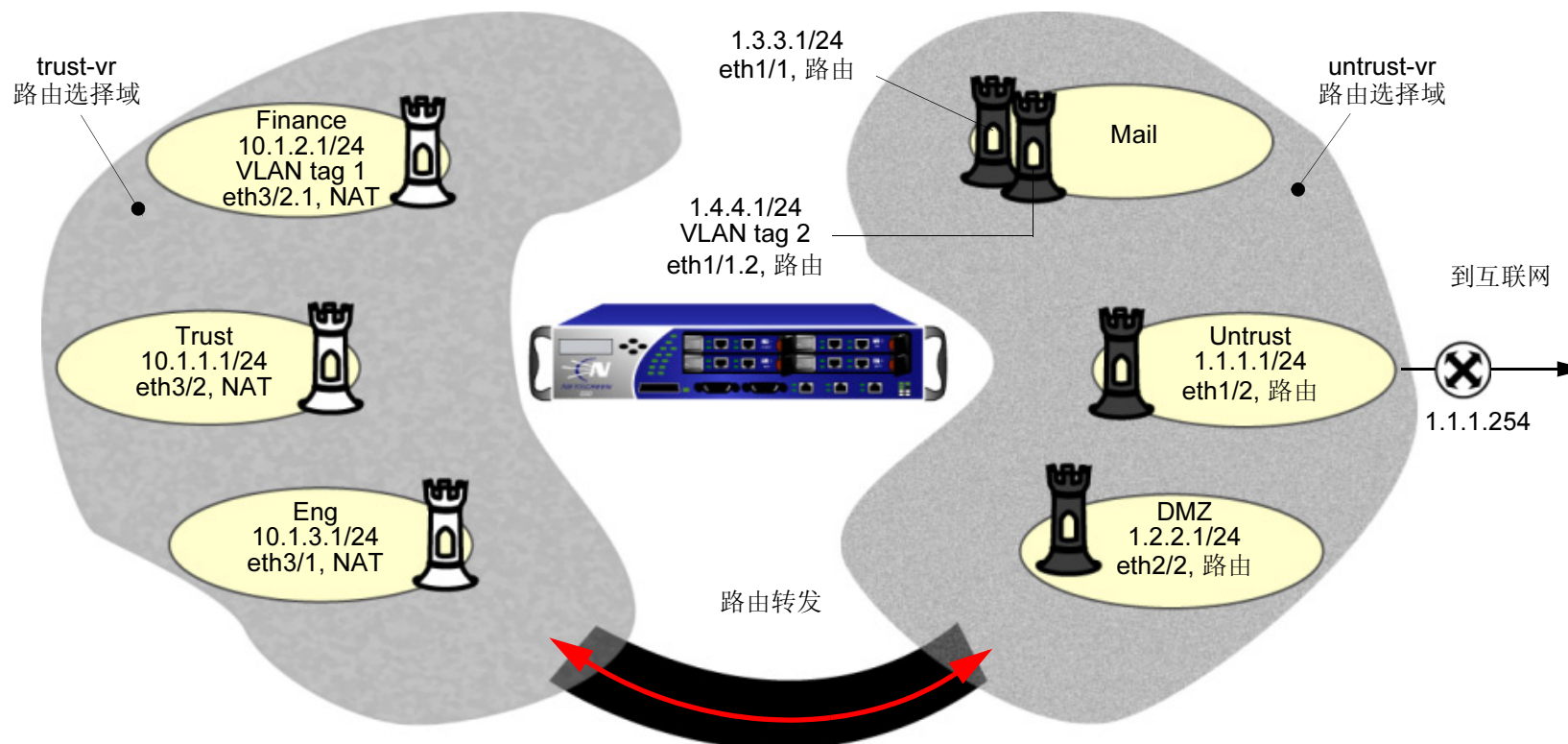
```
set interface ethernet1/2 zone untrust
set interface ethernet1/2 ip 1.1.1.1/24
set interface ethernet1/2 manage snmp
```

7. 接口 ethernet2/2

```
set interface ethernet2/2 zone dmz
set interface ethernet2/2 ip 1.2.2.1/24
save
```

范例 (第 3 部分): 两个路由选择域

这是一个渐进式范例的第三部分。在上一部分中，对多个安全区的接口进行了定义，请参阅第 16 页上的“范例 (第 2 部分): 六个区段的接口”。在下一部分中，将对策略进行设置，请参阅第 22 页上的“范例 (第 4 部分): 策略”。在本例中，您只须为连接到互联网的缺省网关配置路由。其它路由在您创建接口 IP 地址时由 NetScreen 设备自动创建。



WebUI

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (选择); untrust-vr

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet1/2

Gateway IP Address: 1.1.1.254

CLI

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface eth1/2 gateway 1.1.1.254
save
```

NetScreen 设备自动创建以下路由 (黑色):

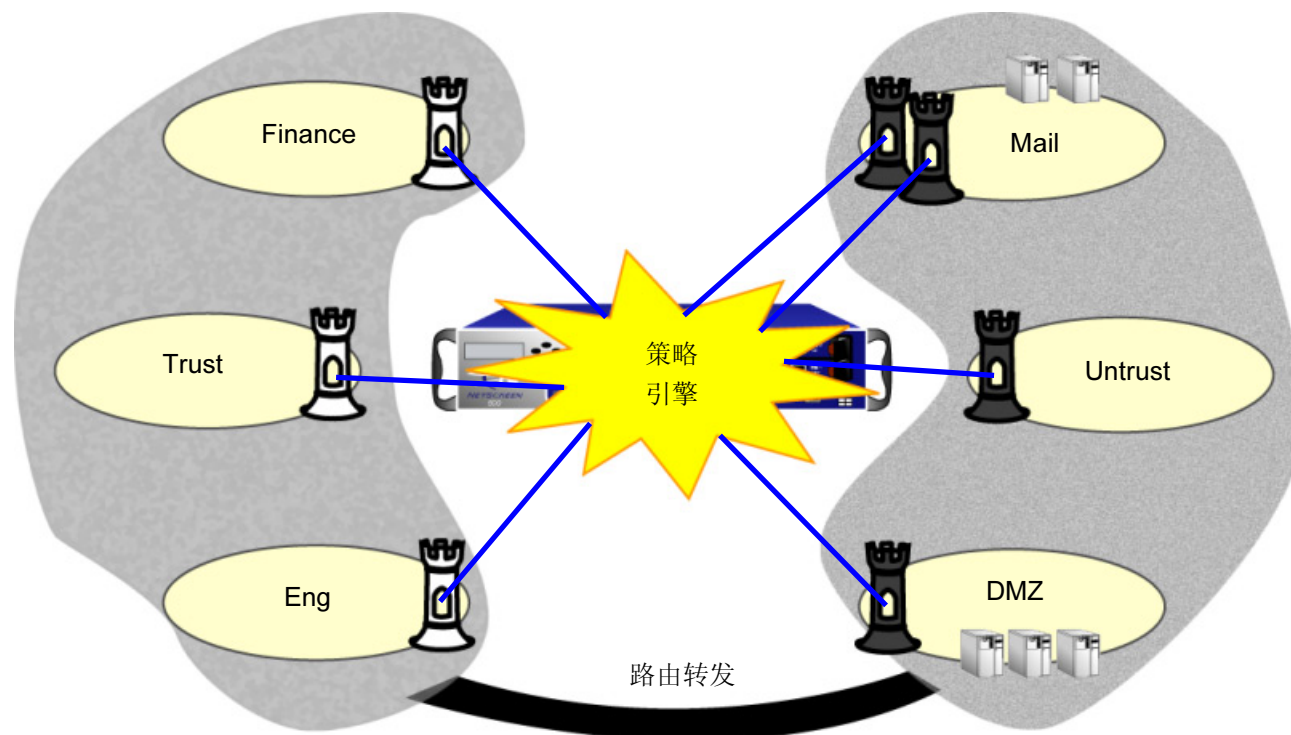
trust-vr		
到达 :	使用接口 :	使用网关 /Vrouter:
0.0.0.0/0	n/a	untrust-vr
10.1.3.0/24	eth3/1	0.0.0.0
10.1.1.0/24	eth3/2	0.0.0.0
10.1.2.0/24	eth3/2.1	0.0.0.0

untrust-vr		
到达 :	使用接口 :	使用网关 /Vrouter:
1.2.2.0/24	eth2/2	0.0.0.0
1.1.1.0/24	eth1/2	0.0.0.0
1.4.4.0/24	eth1/1.2	0.0.0.0
1.3.3.0/24	eth1/1	0.0.0.0
0.0.0.0/0	eth1/2	1.1.1.254

注意: 只有这些
条目由用户配置。

范例 (第 4 部分): 策略

这是一个渐进式范例的最后一部分。上一部分为第 20 页上的“范例 (第 3 部分): 两个路由选择域”。范例的这一部分演示如何配置新的策略。



为达到本例的目的，在开始配置新策略前，您需要创建新的服务组。

注意：创建区段时，NetScreen 设备自动为该区段内的所有主机创建地址 **Any**。本例对所有主机使用地址 **Any**。

WebUI

1. 服务组

Objects > Services > Groups > New: 输入以下内容，然后单击 **OK**:

Group Name: Mail-Pop3

选择 **Mail**，利用按钮 << 将服务从 Available Members 栏移动到 Group Members 栏。

选择 **Pop3**，利用按钮 << 将服务从 Available Members 栏移动到 Group Members 栏。

Objects > Services > Groups > New: 输入以下内容，然后单击 **OK**:

Group Name: HTTP-FTPGet

选择 **HTTP**，利用按钮 << 将服务从 Available Members 栏移动到 Group Members 栏。

选择 **FTP-Get**，利用按钮 << 将服务从 Available Members 栏移动到 Group Members 栏。

2. 策略

Policies > (From: Finance, To: Mail) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

Policies > (From: Trust, To: Mail) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

Policies > (From: Eng, To: Mail) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

Policies > (From: Untrust, To: Mail) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail

Action: Permit

Policies > (From: Finance, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

Policies > (From: Finance, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

Policies > (From: Eng, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

Policies > (From: Eng, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: FTP-Put

Action: Permit

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

CLI

1. 服务组

```
set group service mail-pop3 add mail
set group service mail-pop3 add pop3
set group service http-ftpget add http
set group service http-ftpget add ftp-get
```

2. 策略

```
set policy from finance to mail any any mail-pop3 permit
set policy from trust to mail any any mail-pop3 permit
set policy from eng to mail any any mail-pop3 permit
set policy from untrust to mail any any mail permit
set policy from finance to untrust any any http-ftpget permit
set policy from finance to dmz any any http-ftpget permit
set policy from trust to untrust any any http-ftpget permit
set policy from trust to dmz any any http-ftpget permit
set policy from eng to untrust any any http-ftpget permit
set policy from eng to dmz any any http-ftpget permit
set policy from eng to dmz any any ftp-put permit
set policy from untrust to dmz any any http-ftpget permit
save
```


路由表和静态路由

为方便 NetScreen 设备将封包从一个网络转发到另一个网络，ScreenOS 需要维护包含所有已知网络地址条目的路由表。路由表通常包含一个或多个静态路由，它们多为手动输入的配置信息，定义指向特定目的地址的路径。

本章介绍 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。本章包括以下部分：

- 第 30 页上的“路由基本原理”
 - 第 30 页上的“路由方法”
 - 第 31 页上的“路由表”
 - 第 33 页上的“使用静态路由进行路由选择”
- 第 35 页上的“NetScreen 设备上的虚拟路由器”
- 第 36 页上的“配置静态路由的时机”
- 第 37 页上的“配置静态路由”

注意：有关在 NetScreen 设备上配置动态路由（含动态路由协议）的信息，请参阅第 6 卷，“动态路由”。

路由基本原理

路由是将封包从一个网络转发到另一个最终目的地的过程。路由器是一个网络与另一个网络之间的汇合点。**NetScreen** 安全设备提供集成的路由功能，让 **ScreenOS** 将受保护的信息流有效地转发到目的地。

路由方法

在 **NetScreen** 设备上，可以配置两种路由类型：静态和动态。网络使用静态路由时，管理员必须手动配置路由并维护路由器上的路由表。如果该网络与其它许多网络相连，或者经常更改内部网络的连接，则应使用动态路由协议自动更新路由表。动态路由选择协议允许路由器在本地网络拓扑结构改变时，或在邻接路由器通告远处网络发生变化时，自动更新它们的路由表。

静态路由

静态路由是从 IP 网络地址到在第 3 层转发设备（如路由器）上定义的下一跳跃¹ 目的地的映射。只要不改变这些映射，它们就不会更改。如果该网络与其它网络之间的连接很少，或内部网络连接相对稳定，则定义静态路由通常比设置动态路由更为有效。除非您明确删除静态路由，否则 **ScreenOS** 会将其保留。但是，必要时可以用动态路由信息覆盖静态路由。

动态路由

动态路由包含路由器交换网络与子网可达性的信息，以及路由器通过分析内向路由更新消息以调整路由表。这些消息驻留在网络中，用来引导路由器重新计算路由，并对路由表做出相应更改。有关动态路由协议以及在 **NetScreen** 设备上配置动态路由的信息，请参阅第 6 卷，“动态路由”。

1. 下一跳跃目的地是路由器。

路由表

路由器通常与多个网络相连，负责引导信息流通过这些网络。每个路由器维护一个路由表，该表是已知网络以及如何到达这些网络的指令的列表。在 NetScreen 设备上处理内向封包时，ScreenOS 会执行路由表查找，以找出通向目的地址的相应接口。有关 ScreenOS 中封包流序列的详细信息，请参阅第 1 章，“ScreenOS 体系结构”。

信息流被转发到的目的网络能够识别路由表中的每个条目（称为*路由条目*或简称为*路由*）。目的网络以 IP 地址和网络掩码的形式给出，可以是 IP 网络、子网、SuperNet 或主机。ScreenOS 路由表的条目可能有以下几种来源：

- 直接相连的网络（目的网络是分配给“路由”模式接口的 IP 地址）²
- 动态路由协议，如 OSPF、BGP 或 RIP
- 从其它路由器或虚拟路由器导入的路由
- 静态配置的路由

2. 为“路由”模式的接口设置 IP 地址时，路由表会自动创建指向相邻子网的已连接路由，让信息流通过该接口。

下面是一个 ScreenOS 路由表的范例：

C - Connected, S - Static, A - Auto-Exported, I - Imported
iB - IBGP, eB - EBGP, R - RIP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2

Total 8 entries

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
缺省路由	* 9	0.0.0.0/0	eth3	10.31.1.1	eB	40	100	root
	* 11	192.168.1.100/32	eth2	10.3.3.100	iB	250	0	root
	* 10	1.1.0.0/16	eth3	10.31.1.1	eB	40	100	root
	* 4	10.1.1.1/32	eth3	10.2.2.250	S	20	1	root
	* 1	192.168.1.1/32	eth1	0.0.0.0	C	0	0	root
	* 5	2.2.0.0/16	eth3	10.2.2.250	S	20	1	root
	* 2	10.3.3.0/24	eth2	0.0.0.0	C	0	0	root
	* 3	10.2.2.0/24	eth3	0.0.0.0	C	0	0	root
		目的网络	转发数据的接口	下一跳跃	协议	优先级	度量	Vsys

对于每个目的网络，路由表包含以下信息：

- **NetScreen** 设备上的接口，用于转发流向目的网络的信息流。
- 下一跳跃，既可以是 **NetScreen** 设备上的另一个虚拟路由器，也可以是网关的 IP 地址（通常为路由器的地址）。
- 产生该路由的协议。
- **优先级**，当存在多个路由指向同一目的网络时，可使用优先级来选择要使用的路由。该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。

对每个虚拟路由器，可以修改每项协议或路由来源的优先级值。有关详细信息，请参阅第 6 卷中的“虚拟路由器”一章。

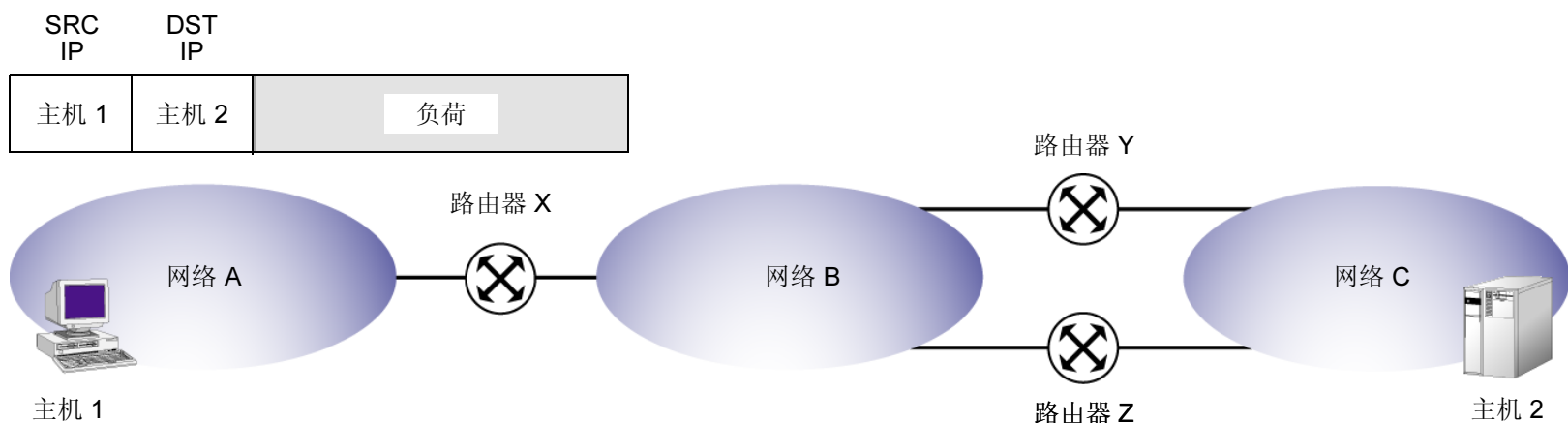
- **度量**，当存在多个路由指向同一目的网路且优先级相同时，还可以使用度量来选择要使用的路由。已连接路由的度量值始终为 0。静态路由的缺省度量值为 1，但可以在定义静态路由时指定其它值。
- 此路由所属的虚拟系统 (vsys)。有关虚拟路由器和虚拟系统的详细信息，请参阅第 6 卷中的“虚拟路由器”一章。

大多数路由表都包含一个**缺省路由**（网络地址为 0.0.0.0/0），对于发往网络的封包，缺省路由无疑是整个路由表中应用最广的条目。

使用静态路由进行路由选择

当某一主机向位于不同网络的另一台主机发送封包时，每个封包包头都含有目的主机的地址。当路由器收到封包时，会将该目的地址与其路由表中的所有地址进行比较。路由器先在路由表中选择一个最具体的³指向目的地址的路由，再根据选定的路由条目决定转发封包的下一跳跃。

下面的示意图展示了一个采用静态路由选择的网络。为了便于说明，假设网络 A 中主机 1 的信息发送到网络 C 中的主机 2，因此创建了包头中包含下列信息的封包：



3. 确定最具体路由的方法是，先对路由表中每个条目的目的地址和网络掩码执行位逻辑 AND 运算。例如，IP 地址 10.1.1.1 与子网掩码 255.255.255.0 进行位逻辑 AND 运算的结果为 10.1.1.0。最具体的路由就是子网掩码中最高位置为 1 的路由（也称作“最长匹配路由”）。

以下说明每个路由器上的路由表。

路由表					
路由器 X		路由器 Y		路由器 Z	
网络	网关	网络	网关	网络	网关
网 A	已连接	网 A	路由器 X	网 A	路由器 X
网 B	已连接	网 B	已连接	网 B	已连接
网 C	路由器 Y	网 C	已连接	网 C	已连接

在上例中，路由器 X 有一个为网络 C 配置的静态路由，相应网关 (下一跳跃) 为路由器 Y。当路由器 X 收到发往网络 C 中主机 2 的封包时，先将封包中的目的地址与其路由表进行比较，然后会发现表中的最后一个路由条目是最具体的指向目的地址的路由。最后一条路由条目指定将发往网络 C 的信息流发送到路由器 Y 进行传送。路由器 Y 接收封包，而且由于它知道网络 C 是直接连接的，所以它会通过连接到该网络的接口来发送封包。

注意，如果路由器 Y 发生故障，或者路由器 Y 与网络 C 之间的链接不可用，则无法将封包送到主机 2。虽然还有一条通过路由器 Z 到达网络 C 的路由，但由于尚未在路由器 X 上配置该静态路由，因此路由器 X 并不知道这条备用路由。

NETSCREEN 设备上的虚拟路由器

ScreenOS 可以将其路由选择组件分成两个或多个虚拟路由器。虚拟路由器同时支持静态和动态路由协议，这样可以在一个虚拟路由器上同时启用二者。NetScreen 设备上预先定义了两个虚拟路由器：

- **trust-vr**，在缺省情况下包含所有预定义安全区和所有用户定义区段
- **untrust-vr**，在缺省情况下不含任何安全区

一些 NetScreen 设备还允许创建其它自定义的虚拟路由器。通过将路由选择信息分给两个 (或多个) 虚拟路由器，可以控制给定路由域中对其它路由域可见的信息。例如，可以将企业网内部所有安全区的路由选择信息保留在预定义的虚拟路由器 **trust-vr** 中，而将企业网外部所有区段的路由选择信息保留在另一预定义的虚拟路由器 **untrust-vr** 中。由于虚拟路由器路由表中的信息对于其它路由器是不可见的，所以您可以将内部网的路由选择信息与公司外部的不可信源分离开来。也就是说，从一个虚拟路由器的区段发出的信息流不能自动转发到另一个虚拟路由器中的区段，即使存在策略允许这样转发信息流。如果希望信息流在虚拟路由器之间传递，则需要导出 VR 之间的路由或在将另一个 VR 定义为下一跳跃的 VR 中配置静态路由。

本章不包括创建自定义虚拟路由器、使用两个或多个虚拟路由器以及导出 VR 之间的路由等信息。有关虚拟路由器的详细信息，请参阅第 6 卷中的“虚拟路由器”。

配置静态路由的时机

路由表提供的信息可帮助虚拟路由器将信息流发送到不同的接口和子网。在 NetScreen 设备中，即使正在使用动态路由，仍可能需要定义静态路由。在以下情况中，需要定义静态路由：

- 如果网络没有直接连接到 NetScreen 设备，但可以通过虚拟路由器的接口上的路由器访问网络，则需要使用该路由器的 IP 地址定义网络的静态路由。例如，Untrust 区段接口所在的子网可能有两个路由器，每个路由器连接到不同的 Internet 连接，此时必须定义使用哪个路由器将信息流转发到特定的 ISP。
- 您需要定义一个静态路由，将缺省路由 (0.0.0.0/0) 添加到虚拟路由器的路由表中。例如，如果正在使用的两个虚拟路由器在同一 NetScreen 设备上，则 trust-vr 路由表可包含一个缺省路由，将 untrust-vr 指定为下一跳跃。这样即可将目的地不在 trust-vr 路由表中的信息流路由到 untrust-vr。还可以在 untrust-vr 中定义一个缺省路由，将目的地不在 untrust-vr 路由表中的信息流路由到特定路由器的 IP 地址。
- 如果正在使用的两个虚拟路由器在同一 NetScreen 设备上，且目的地为连接到 trust-vr 接口的网络的入站信息流到达 untrust-vr 接口，则需要在 untrust-vr 路由表中定义一个静态条目，将连接到 trust-vr 接口的目的网络指定为下一跳跃。（注意，如果 trust-vr 中的路由表条目被导出到 untrust-vr 中，则不需要定义此静态路由。）
- 当设备处于“透明”模式时，必须定义静态路由，将源自设备本身的管理信息流（与经过防火墙的用户信息流方向相反）发送到远程目的地。例如，需要定义静态路由，将 syslog、SNMP、WebTrends 等消息发送到远程管理员地址。还必须定义路由，将认证请求发往 RADIUS、SecurID 和 LDAP 服务器，并将 URL 检查信息发往 Websense 服务器。

注意：当 NetScreen 设备处于“透明”模式时，必须为来自设备的管理信息流定义静态路由，即使目标与该设备位于同一子网中。要指定发送信息流所通过的接口，此路由是必需的。

- 对于出站 VPN 信息流，如果有多个外向接口指向目的地址，则需要设置路由，让出站信息流通过预期接口发送到外部路由器。
- 如果 trust-vr 路由域中的安全区接口的运行模式为 NAT，且在该接口上配置了 MIP 或 VIP 以接收来自 untrust-vr 路由选择域中的信息源的内向信息流，则必须创建到 untrust-vr 中的 MIP 或 VIP 的路由，该路由指向 trust-vr 作为网关。

配置静态路由

要创建静态路由，需要定义以下内容：

- 可添加路由的虚拟路由器。
- 目的网络的 IP 地址和网络掩码。
- 路由的下一跳跃，既可以是 NetScreen 设备上的另一个虚拟路由器，也可以是网关（路由器）的 IP 地址。
- 如果要指定另一个虚拟路由器，请确保该虚拟路由器的路由表中存在目的网络条目。
- 转发被路由的信息流的接口。接口可以是支持 ScreenOS 的任何接口，如物理接口（例如 ethernet1/2）或通道接口。
- 此外，还可以指定路由度量和 / 或路由标记。当存在多个路由指向同一目的网路且优先级相同时，使用路由度量来选择活动路由。静态路由的缺省度量值为 1。路由标记是一个值，在重新分配路由时可用作过滤器。例如，可以只导入包含特定标记值的路由。

范例：静态路由

在下例中，NetScreen 设备负责保护一个多级网络，设备 Trust 区段的接口处于 NAT 模式。本例中既有本地管理又有远程管理（通过 NetScreen-Security Manager）。NetScreen 设备向本地管理员（位于 Trust 区段中的某一网络）发送 SNMP 陷阱和 syslog 报告，并向远程管理员（位于 Untrust 区段中的某一网络）发送 NetScreen-Security Manager 报告。该设备通过 DMZ 区段中的 SecurID 服务器来认证用户，通过 Trust 区段中的 Websense 服务器执行 URL 过滤。

Trust-vr 和 untrust-vr 路由表必须包含指向以下目的地的路由（以下数字对应 39 页上的图示）：

untrust-vr

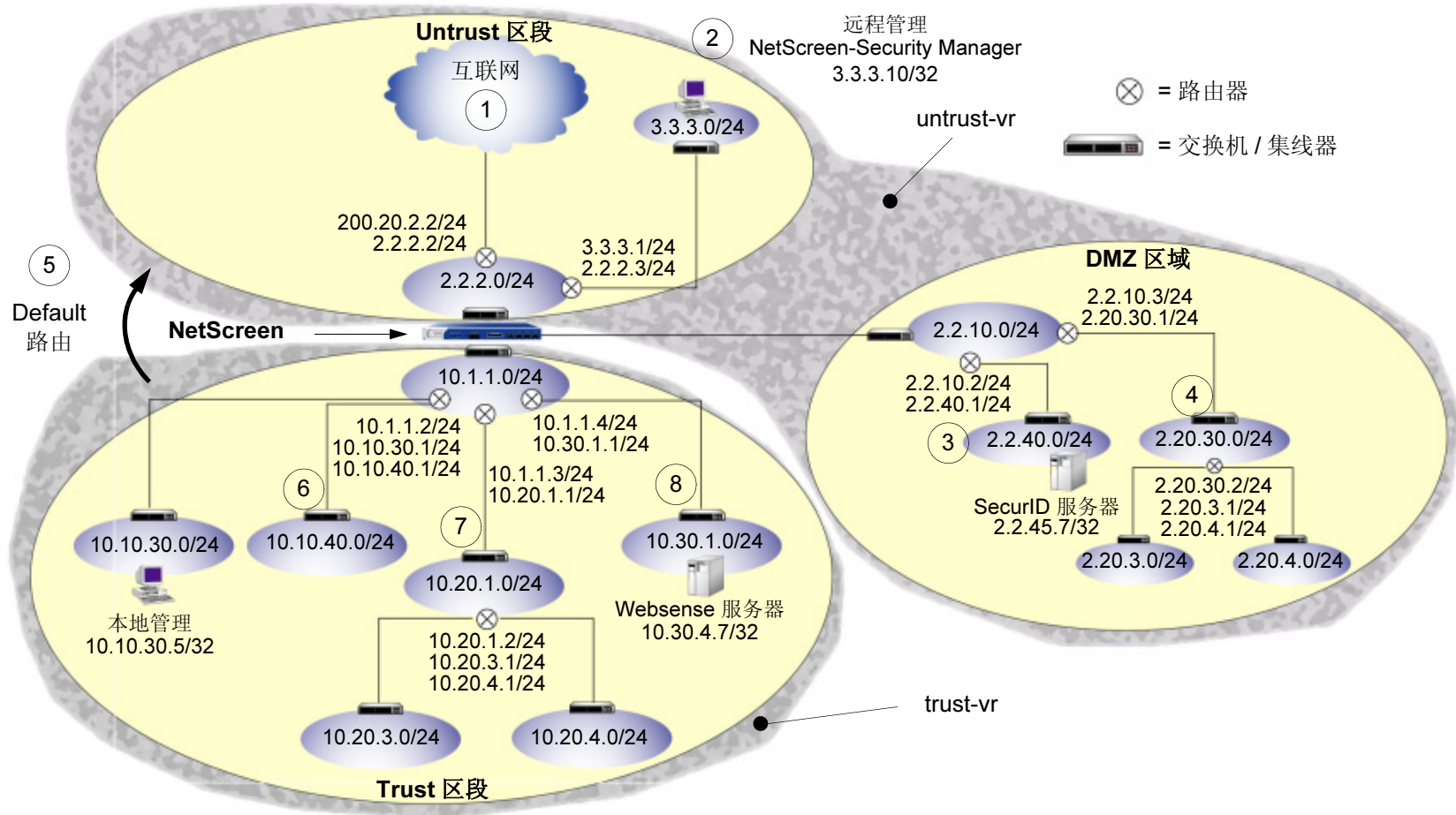
1. 连接到 Internet 的缺省网关（这是虚拟路由器的缺省路由）
2. 3.3.3.0/24 子网中的远程管理员
3. DMZ 区段中的 2.2.40.0/24 子网
4. DMZ 区段中的 2.20.0.0/16 子网

trust-vr

5. 与未在 trust-vr 路由表中找到的所有地址相对应的 untrust-vr（这是虚拟路由器的缺省路由）
6. Trust 区段中的 10.10.0.0/16 子网
7. Trust 区段中的 10.20.0.0/16 子网
8. Trust 区段中的 10.30.1.0/24 子网

注意：下面的例子假设已经将 ethernet1 绑定到 Trust 区段、将 ethernet2 绑定到 DMZ 区段、将 ethernet3 绑定到 Untrust 区段。接口 IP 地址分别为 10.1.1.1/24、2.2.10.1/24 和 2.2.2.1/24。

静态路由配置



WebUI

1. untrust-vr

Network > Routing > Routing Entries > untrust-vr New: 输入以下内容创建缺省不信任不可信网关，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.2

Network > Routing > Routing Entries > untrust-vr New: 输入下列内容将 NetScreen 设备产生的系统报告发往远程管理，然后单击 **OK**:

Network Address/Netmask: 3.3.3.0/24

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.3

Network > Routing > Routing Entries > untrust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 2.2.40.0/24

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 2.2.10.2

Network > Routing > Routing Entries > untrust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 2.20.0.0/16

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 2.2.10.3

2. trust-vr

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (选择); untrust-vr

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.10.0.0/16

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.2

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.20.0.0/16

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.3

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.30.1.0/32

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.4

注意：要移除条目，请单击 **Remove**。会出现一条“系统消息”，提示您确认移除操作。单击 **OK** 继续，或单击 **Cancel** 取消操作。

CLI

1. untrust-vr

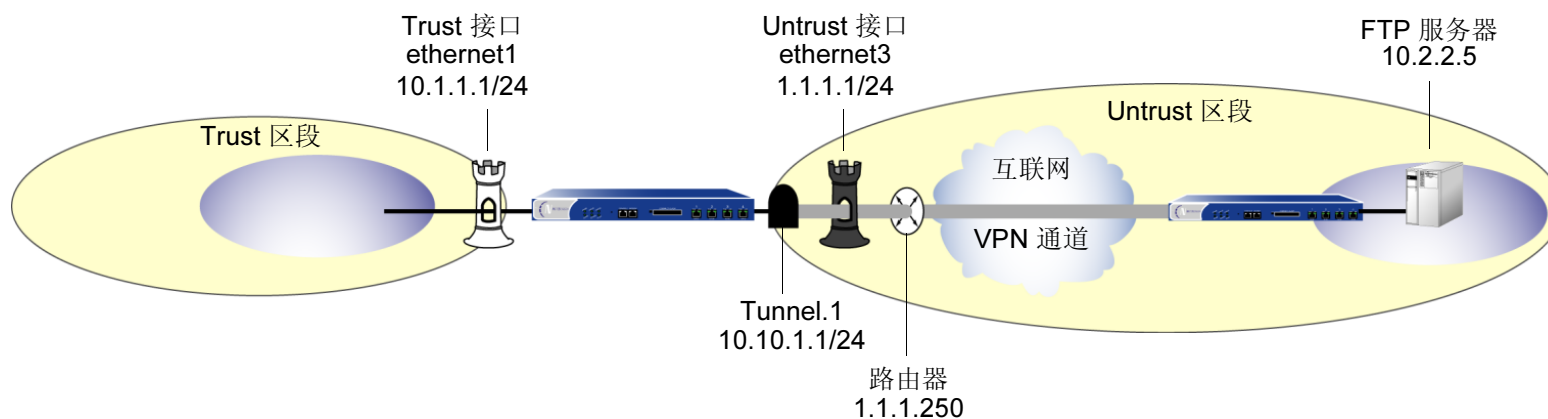
```
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
set vrouter untrust-vr route 3.3.3.0/24 interface ethernet3 gateway 2.2.2.3
set vrouter untrust-vr route 2.2.40.0/24 interface ethernet2 gateway 2.2.10.2
set vrouter untrust-vr route 2.20.0.0/16 interface ethernet2 gateway 2.2.10.3
```

2. trust-vr

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter trust-vr route 10.10.0.0/16 interface ethernet1 gateway 10.1.1.2
set vrouter trust-vr route 10.20.0.0/16 interface ethernet1 gateway 10.1.1.3
set vrouter trust-vr route 10.30.1.0/24 interface ethernet1 gateway 10.1.1.4
save
```

范例：用于通道接口的路由

在本例中，信任主机与信任接口处在不同的子网中。FTP 服务器通过 VPN 通道接收入站信息流。您需要设置一个路由，将离开通道接口的信息流引向通往服务器所在子网的内部路由器。



WebUI

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.2.2.5/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

注意：若要为了 **tunnel.1** 出现在 **Interface** 下拉列表中，您必须先创建 **tunnel.1** 接口。

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

CLI

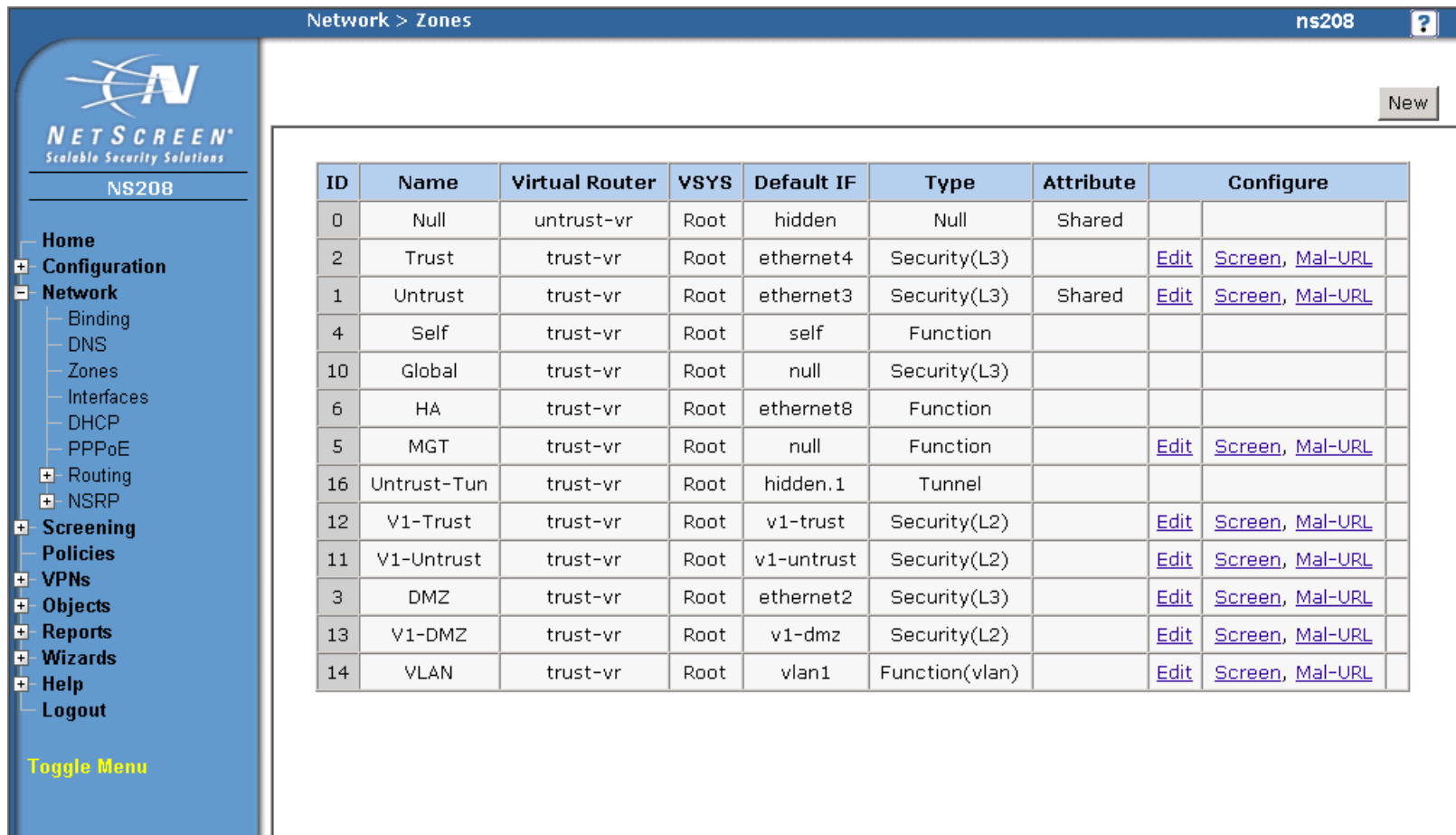
```
set vrouter trust-vr route 10.2.2.5/32 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```


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)、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)。本章研究各种类型的区段，特别将重点放在安全区上。本章由以下几节组成：

- 第 48 页上的 “安全区”
 - 第 48 页上的 “Global 区段”
 - 第 48 页上的 “SCREEN 选项”
- 第 49 页上的 “通道区段”
- 第 51 页上的 “配置安全区和通道区段”
 - 第 51 页上的 “创建区段”
 - 第 52 页上的 “修改区段”
 - 第 53 页上的 “删除区段”
- 第 54 页上的 “功能区段”
 - 第 54 页上的 “Null 区段”
 - 第 54 页上的 “MGT 区段”
 - 第 54 页上的 “HA 区段”
 - 第 54 页上的 “Self 区段”
 - 第 54 页上的 “VLAN 区段”
- 第 55 页上的 “端口模式”
 - 第 60 页上的 “设置端口模式”
 - 第 62 页上的 “Home 区段 / Work 区段”

首次启动 NetScreen 设备时，可以看到若干预定义的区段。在 WebUI 中，单击左侧菜单栏中的 **Network > Zones**。在 CLI 中，使用 **get zone** 命令。



Network > Zones ns208 ?

New

ID	Name	Virtual Router	VSYS	Default IF	Type	Attribute	Configure
0	Null	untrust-vr	Root	hidden	Null	Shared	
2	Trust	trust-vr	Root	ethernet4	Security(L3)		Edit Screen , Mal-URL
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	Edit Screen , Mal-URL
4	Self	trust-vr	Root	self	Function		
10	Global	trust-vr	Root	null	Security(L3)		
6	HA	trust-vr	Root	ethernet8	Function		
5	MGT	trust-vr	Root	null	Function		Edit Screen , Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel		
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)		Edit Screen , Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)		Edit Screen , Mal-URL
3	DMZ	trust-vr	Root	ethernet2	Security(L3)		Edit Screen , Mal-URL
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)		Edit Screen , Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)		Edit Screen , Mal-URL

get zone 命令的输出为：

ns500-> get zone
Total of 13 zones in vsys root

ID	Name	Type	Attr	VR	Default-IF	VSYS
0	Null	Null	Shared	untrust-vr	null	Root
1	Untrust	Sec(L3)	Shared	trust-vr	ethernet1/2	Root
2	Trust	Sec(L3)		trust-vr	ethernet3/2	Root
3	DMZ	Sec(L3)		trust-vr	ethernet2/2	Root
4	Self	Func		trust-vr	self	Root
5	MGT	Func		trust-vr	mgt	Root
6	HA	Func		trust-vr	ha1	Root
10	Global	Sec(L3)		trust-vr	null	Root
11	V1-Untrust	Sec(L2)		trust-vr	v1-untrust	Root
12	V1-Trust	Sec(L2)		trust-vr	v1-trust	Root
13	V1-DMZ	Sec(L2)		trust-vr	v1-dmz	Root
14	VLAN	Func		trust-vr	vlan1	Root
16	Untrust-Tun	Tun		trust-vr	null	Root

根和虚拟系统共享这些区段。

这些区段没有也不能包含接口。

如果从早于 ScreenOS 3.1.0 的版本升级 — 对于 NAT 或路由模式下的设备版本高于 3、对于透明模式下的设备版本低于 3，这些区段具有向下兼容性。

保留区段 ID number 7-9 和 15 以备将来使用。

在缺省情况下，VPN 通道接口绑定到 Untrust-Tun 区段，其承载区段为 Untrust 区段。(升级时，现有通道绑定到 Untrust-Tun 区段。)

上述预定义区段可分为三种不同类型：

安全区：Untrust、Trust、DMZ、Global、V1-Untrust、V1-Trust、V1-DMZ

通道区段：Untrust-Tun

功能区段：Null、Self、MGT、HA、VLAN

安全区

在单个 NetScreen 设备上，可以配置多个安全区，将网络分成多段，可对这些网段应用各种安全选项以满足各段的需要。必须最少定义两个安全区，以便在网络的不同区段间分开提供基本的保护。在某些 NetScreen 平台上，您可以定义多个安全区，使网络安全设计具有更高的精确度 — 而且这样做无需配置多个安全设备。

Global 区段

您可以识别安全区，因为它有地址簿而且可以在策略中引用。Global 区段满足这些条件。但是，它不具有其它安全区都具有的一种元素 — 接口。Global 区段可充当映射 IP (MIP) 和虚拟 IP (VIP) 地址的存储区域。预定义 Global 区段地址 “Any” 应用于 Global 区段中所有 MIP、VIP 和其它用户定义的地址组。因为转向这些地址的信息流被映射到其它地址，所以 Global 区段不需要用于使信息流从中流过的接口。

Global 区段还包含全域策略中使用的地址。有关全域策略的详细信息，请参阅第 217 页上的“全局策略”。

注意：任何以 Global 区段作为其目的区段的策略均不支持 NAT 或信息流整形。

SCREEN 选项

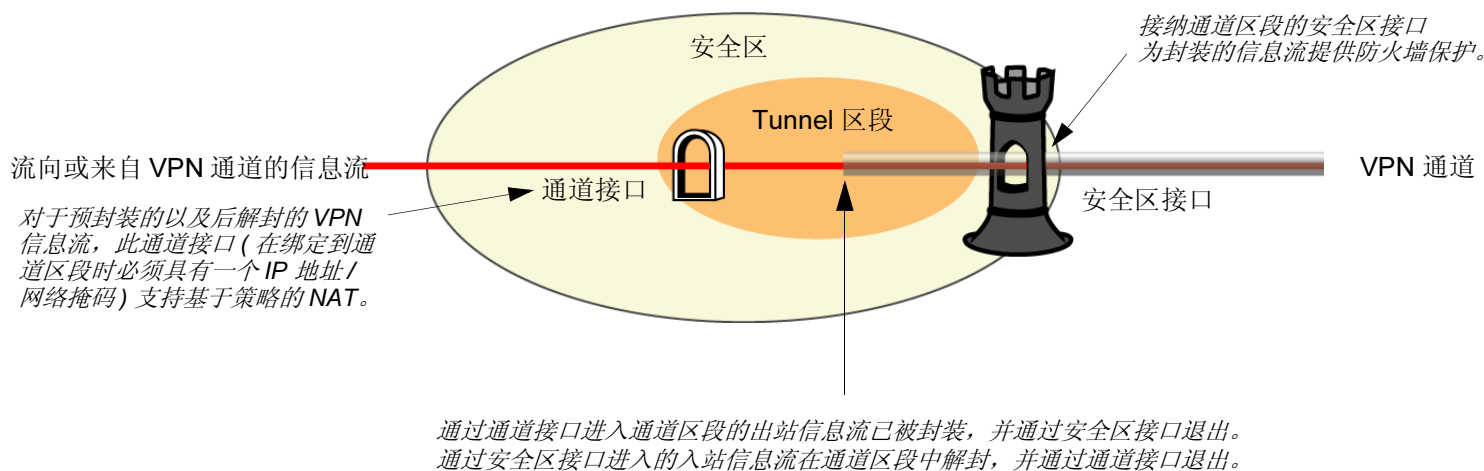
NetScreen 防火墙用于保护网络的安全，具体做法是先检查要求从一个安全区到另一区段的通路的所有连接尝试，然后予以允许或拒绝。对于每个安全区和 MGT 区段，可启用一组预定义的 SCREEN 选项，检测并阻塞 NetScreen 确定为潜在有害的各种信息流。有关 SCREEN 的多个可用选项的详细信息，请参阅第 4 卷，“攻击检测和防御机制”。

通道区段

通道区段是一个或多个通道接口的宿主逻辑网段。通道区段在概念上以一种“子父”关系附属于安全区。安全区充当“父”，您也可以将其想象为载体区段，该区段对封装的信息流提供防火墙保护。通道区段提供封包封装 / 解封，还提供基于策略的 NAT 服务（通过支持具有可以接纳映射 IP (MIP) 地址和动态 IP (DIP) 池的 IP 地址和网络掩码的通道接口）。

NetScreen 设备使用路由信息使承载区段将信息流引向通道端点。缺省的通道区段为 **Untrust-Tun**，它与 **Untrust** 区段相关联。您可以创建其它通道区段并将其绑定到其它安全区，每个虚拟系统上的每个承载区段最多只能有一个通道区段¹。

在缺省情况下，通道区段在 **trust-vr** 路由选择域中，但是也可以将通道区段移动到其它路由选择域中。



当从 3.1.0 以下版本的 ScreenOS 升级时，在缺省情况下，现有的通道接口被绑定到预配置的 **Untrust-Tun** 通道区段，该区段是预配置的 **Untrust** 安全区的“子”区段。可以将多个通道区段绑定到同一个安全区，但是不可以将一个通道区段绑定到另一个通道区段。

1. 根系统与所有虚拟系统可以共享 **Untrust** 区段。但是，各系统拥有自己单独的 **Untrust-Tun** 区段。

范例：将通道接口绑定到 Tunnel 区段

在本例中，将创建一个通道接口，并将其命名为 `tunnel.3`。将其绑定到 `Untrust-Tun` 区段，并将其 IP 地址指派为 `3.3.3.3/24`。然后定义 `tunnel.3` 上的映射 IP (MIP) 地址，将 `3.3.3.5` 转换为 `10.1.1.5` (Trust 区段中某服务器的地址)。Untrust 区段 (Untrust-Tun 区段的承载区段) 和 Trust 区段都在 `trust-vr` 路由选择域中。

WebUI

1. 通道接口

Network > Interfaces > New Tunnel IF: 输入以下内容，然后单击 **OK**:

Tunnel Interface Name: `tunnel.3`

Zone (VR): `Untrust-Tun (trust-vr)`

Fixed IP: (选择)

IP Address/Netmask `3.3.3.3/24`

2. MIP

Network > Interfaces > Edit (对于 `tunnel.3`) > MIP > New: 输入以下内容，然后单击 **OK**:

Mapped IP: `3.3.3.5`

Netmask: `255.255.255.255`

Host IP Address: `10.1.1.5`

Host Virtual Router Name: `trust-vr`

CLI

1. 通道接口

```
set interface tunnel.3 zone Untrust-Tun
set interface tunnel.3 ip 3.3.3.3/24
```

2. MIP

```
set interface tunnel.3 mip 3.3.3.5 host 10.1.1.5
save
```


配置安全区和通道区段

第 3 层或第 2 层安全区及通道区段的创建、修改和删除十分相似。

注意：您不能删除预定义的安全区或预定义的通道区段，但是可以编辑它们。

创建区段

要创建第 3 层或第 2 层安全区或通道区段，请使用 WebUI 或 CLI:

WebUI

Network > Zones > New: 输入以下内容，然后单击 **OK**:

Zone Name: 键入区段名称²。

Virtual Router Name: 选择要在其路由选择域中放置区段的虚拟路由器。

Zone Type: 选择 **Layer 3** 创建一个区段，可以将处于 NAT 或“路由”模式的接口绑定到该区段。选择 **Layer 2** 创建一个区段，可以将处于“透明”模式的接口绑定到该区段。创建通道区段并将其绑定到承载区段时，请选择 **Tunnel Out Zone**，然后从下拉列表中选择具体的承载区段。

Block Intra-Zone Traffic: 选择此选项可封锁同一安全区中主机之间的信息流。在缺省情况下，禁用区段内部封锁。

CLI

```
set zone name zone [ l2 vlan_id_num3 | tunnel sec_zone ]
set zone zone block
set zone zone vrouter name_str
```

-
- 第 2 层安全区的名称必须以“L2-”开头；例如，“L2-Corp”或“L2-Xnet”。
 - 创建第 2 层安全区时，VLAN ID number 必须为 1 (对于 VLAN1)。

修改区段

要修改安全区或通道区段的名称，或更改通道区段的承载区段，必须先删除该区段⁴，然后再以修改值重新创建它。您可以更改现有区段上的区段内部封锁选项和虚拟路由器⁵。

WebUI

1. 修改区段名称

Network > Zones: 单击 **Remove** (对于要更改其名称的安全区或通道区段，或对于要更改其承载区段的通道区段)。

当出现提示，请求对删除操作进行确认时，单击 **Yes**。

Network > Zones > New: 输入更改后的区段设置，然后单击 **OK**。

2. 更改区段内部封锁选项或虚拟路由器

Network > Zones > Edit (对于要修改的区段): 输入以下内容，然后单击 **OK**:

Virtual Router Name: 从下拉列表中，选择要将区段移动到其路由选择域中的虚拟路由器。

Block Intra-Zone Traffic: 启用时，选中此复选框。禁用时，将其清除。

CLI

1. 修改区段名称

```
unset zone zone
set zone name zone [ l2 vlan_id_num | tunnel sec_zone ]
```

2. 更改区段内部封锁选项或虚拟路由器

```
{ set | unset } zone zone block
set zone zone vrouter name_str
```

4. 删除区段前，必须先解除所有绑定到它的接口。

5. 更改区段的虚拟路由器之前，必须先删除绑定到该区段的所有接口。

删除区段

要删除安全区或通道区段，执行以下任一操作⁶：

WebUI

Network > Zones: 单击 **Remove** (对于要删除的区段)。

当出现提示，请求对删除操作进行确认时，单击 **Yes**。

CLI

```
unset zone zone
```

6. 删除区段前，必须先解除所有绑定到它的接口。要解除接口与区段间的绑定，请参阅第 78 页上的“将接口绑定到安全区”。

功能区段

共有五个功能区段，分别是 **Null**、**MGT**、**HA**、**Self** 和 **VLAN**。每个区段的存在都有其专门的目的，如下所示。

Null 区段

此区段用于临时存储没有绑定到任何其它区段的接口。

MGT 区段

此区段是带外管理接口 **MGT** 的宿主区段。可以在此区段上设置防火墙选项以保护管理接口，使其免受不同类型的攻击。有关防火墙选项的详细信息，请参阅第 4 卷，“攻击检测和防御机制”。

HA 区段

此区段是高可用性接口 **HA1** 和 **HA2** 的宿主区段。尽管可以为 **HA** 区段设置接口，但是此区段本身是不可配置的。

Self 区段

此区段是远程管理连接接口的宿主区段。当您通过 **HTTP**、**SCS** 或 **Telnet** 连接到 **NetScreen** 设备时，就会连接到 **Self** 区段。

VLAN 区段

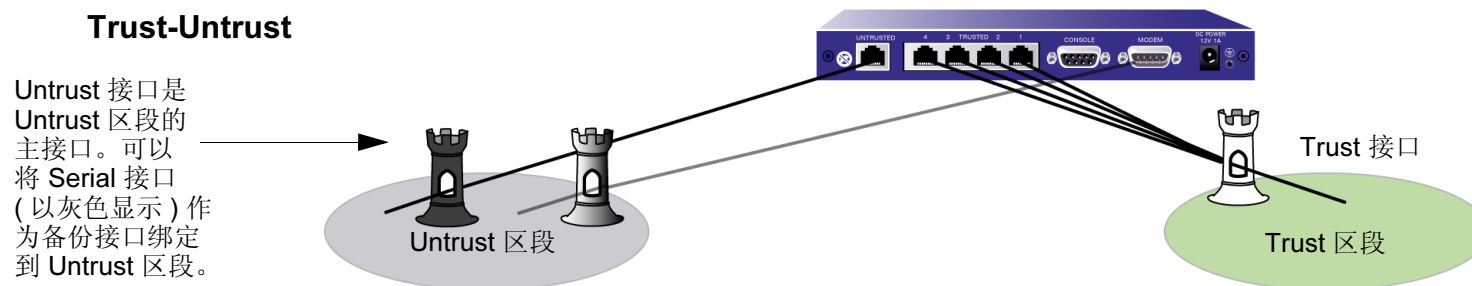
此区段是 **VLAN1** 接口的宿主区段，可用于管理设备，并在设备处于“透明”模式时终止 **VPN** 信息流，也可在此区段上设置防火墙选项以保护 **VLAN1** 接口，使其免受各种攻击。

端口模式

可以为某些 NetScreen 设备选择*端口模式*。端口模式自动为设备设置不同的端口、接口和区段绑定⁷。在 NetScreen-5XT 和 NetScreen-5GT 上，可以配置下列端口模式之一：

警告：更改端口模式会删除 NetScreen 设备上任何现有的配置，并要求系统重置。

- Trust-Untrust 模式是缺省端口模式。此模式提供下列端口、接口和区段绑定：
 - 将 Untrusted 以太网端口绑定到 Untrust 接口，该接口被绑定到 Untrust 安全区
 - 将 MODEM 端口绑定到 Serial 接口，可以将其作为备份接口绑定到 Untrust 安全区
 - 将以太网端口 1 到 4 绑定到 Trust 接口，该接口被绑定到 Trust 安全区



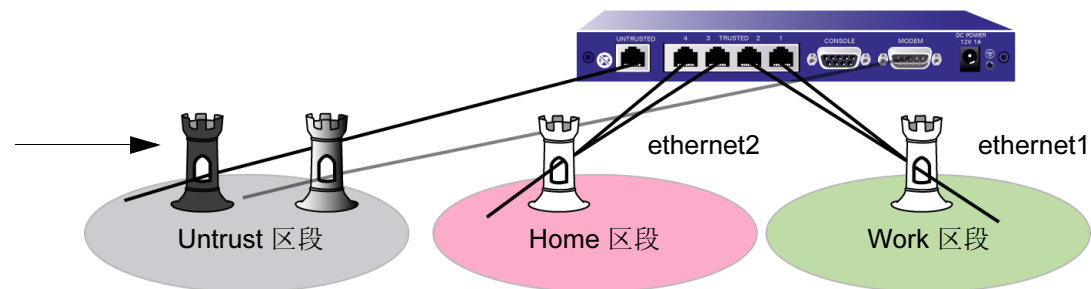
注意：“初始配置向导”仅在 Trust-Untrust 端口模式下运行。

7. 在端口模式环境中，*端口*指的是 NetScreen 设备背面的物理接口。端口被其标签引用：Untrusted、1-4、Console 或 Modem。术语*接口*指的是可以通过 WebUI 或 CLI 配置的逻辑接口。每个端口只能绑定到一个接口，但是多个端口可以绑定到一个接口。

- **Home-Work 模式**将接口绑定到 **Untrust** 安全区及新的 **Home** 和 **Work** 安全区。**Work** 和 **Home** 区段允许隔离每个区段中的用户和资源。在此模式下，缺省策略允许信息流和连接从 **Work** 区段到 **Home** 区段，但不允许信息流从 **Home** 区段流到 **Work** 区段。在缺省情况下，从 **Home** 区段到 **Untrust** 区段的信息流不受到任何限制。此模式提供下列端口、接口和区段绑定：
 - 将以太网端口 **1** 和 **2** 绑定到 **ethernet1** 接口，该接口被绑定到 **Work** 安全区
 - 将以太网端口 **3** 和 **4** 绑定到 **ethernet2** 接口，该接口被绑定到 **Home** 安全区
 - 将 **Untrusted** 以太网端口绑定到 **ethernet3** 接口，该接口被绑定到 **Untrust** 安全区
 - 将 **Modem** 端口绑定到 **Serial** 接口，可以将其作为备份接口绑定到 **Untrust** 安全区

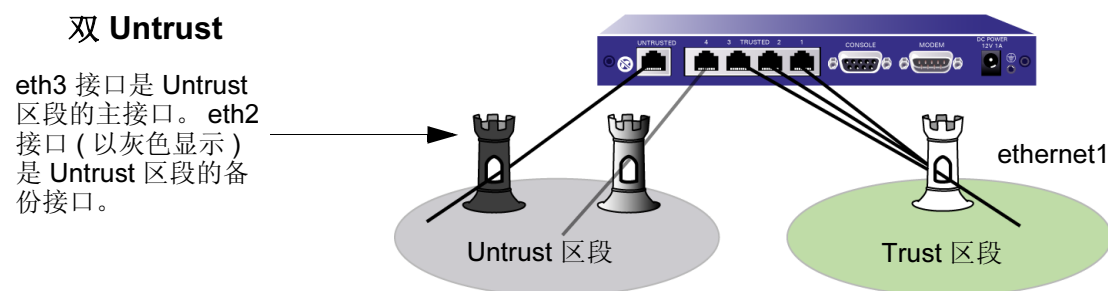
Home-Work

ethernet3 接口是 Untrust 区段的主接口。可以将 Serial 接口 (以灰色显示) 作为备份接口绑定到 Untrust 区段。



有关配置和使用 Home-Work 模式的详细信息，请参阅第 62 页上的“Home 区段 / Work 区段”。

- “双 Untrust”模式将两个接口（一个主接口和一个备份接口）绑定到 Untrust 安全区。主接口用于传递进出 Untrust 区段的信息流，而备份接口仅在主接口出现故障时才使用。此模式提供下列端口、接口和区段绑定：
 - 将 Untrusted 以太网端口绑定到 ethernet3 接口，该接口被绑定到 Untrust 安全区
 - 将以太网端口 4 绑定到 ethernet2 接口，该接口作为备份接口被绑定到 Untrust 安全区（ethernet3 接口是 Untrust 安全区的主接口）
 - 将以太网端口 1、2 和 3 绑定到 ethernet1 接口，该接口被绑定到 Trust 安全区



注意：Serial 接口在“双 Untrust”端口模式下不可使用。

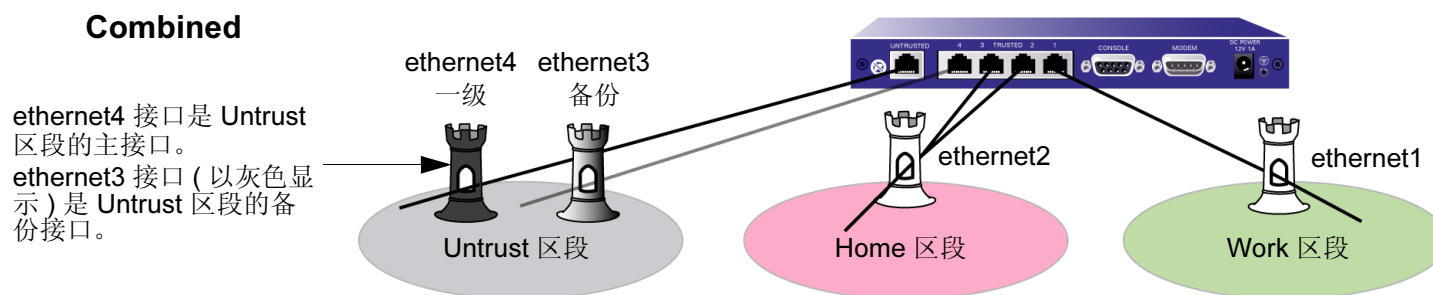
有关配置和使用“双 Untrust”模式的详细信息，请参阅第 8 卷，“高可用性”。

- Combined 模式允许互联网的主接口和备份接口及 Work 和 Home 区段中用户和资源的隔离。

注意：对于 NetScreen-5XT，只有 NetScreen-5XT Elite (不受限制的用户) 平台支持 Combined 端口模式。

此模式提供下列端口、接口和区段绑定：

- 将 Untrusted 以太网端口绑定到 ethernet4 接口，该接口被绑定到 Untrust 区段
- 将以太网端口 4 绑定到 ethernet3 接口，该接口作为备份接口被绑定到 Untrust 区段 (ethernet4 接口是 Untrust 安全区的主接口)
- 将以太网端口 3 和 2 绑定到 ethernet2 接口，该接口被绑定到 Home 区段
- 将以太网端口 1 绑定到 ethernet1 接口，该接口被绑定到 Work 区段



注意：Serial 接口在 Combined 端口模式下不可使用。

有关配置和使用 Combined 模式的详细信息，请参阅第 8 卷，“高可用性”和第 62 页上的“Home 区段 / Work 区段”。

- Trust/Untrust/DMZ 模式将接口绑定到 Untrust、Trust 和 DMZ 安全区，允许将 web、电子邮件或其它应用程序服务器与内部网络分开。

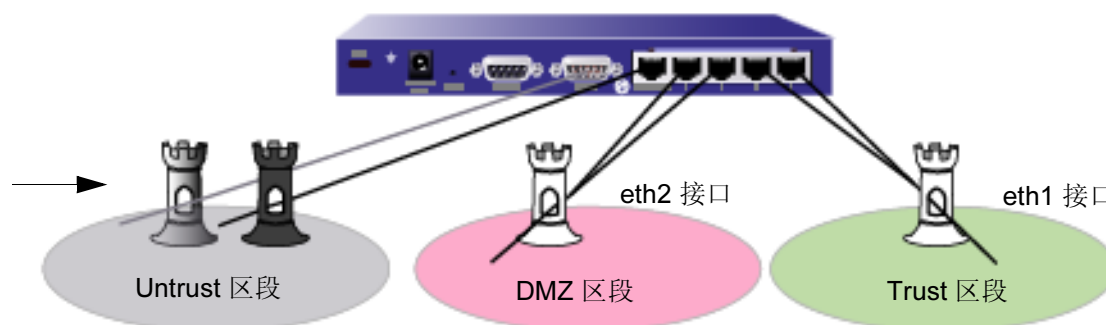
注意：只有 NetScreen-5GT Extended 平台支持 Trust/Untrust/DMZ 端口模式。

此模式提供下列端口、接口和区段绑定：

- 将以太网端口 1 和 2 绑定到 ethernet1 接口，该接口被绑定到 Trust 安全区
- 将以太网端口 3 和 4 绑定到 ethernet2 接口，该接口被绑定到 DMZ 安全区
- 将 Untrusted 以太网端口绑定到 ethernet3 接口，该接口被绑定到 Untrust 安全区
- 将 Modem 端口绑定到 Serial 接口，可以将其作为备份接口绑定到 Untrust 安全区

Trust/Untrust/DMZ

eth3 接口是 Untrust 区段的主接口。可以将 Serial 接口 (以灰色显示) 作为备份接口绑定到 Untrust 区段。



设置端口模式

下表对 ScreenOS 端口模式提供的端口、接口和区段绑定加以汇总：

端口*	Trust-Untrust 模式†		Home-Work 模式		双 Untrust 模式		Combined 模式		Trust/Untrust/DMZ 模式	
	接口	区段	接口	区段	接口	区段	接口	区段	接口	区段
Untrusted	Untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust	ethernet4	Untrust	ethernet3	Untrust
1	Trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet1	Work	ethernet1	Trust
2	Trust	Trust	ethernet1	Work	ethernet1	Trust	ethernet2	Home	ethernet1	Trust
3	Trust	Trust	ethernet2	Home	ethernet1	Trust	ethernet2	Home	ethernet2	DMZ
4	Trust	Trust	ethernet2	Home	ethernet2	Untrust	ethernet3	Untrust	ethernet2	DMZ
Modem	串行	Null	串行	Null	无	无	无	无	串行	Null

* 如 NetScreen 设备底盘上标注。

† 缺省端口模式

通过 WebUI 或 CLI 更改 NetScreen 设备上的端口模式设置。设置端口模式之前，请注意以下方面：

- 更改端口模式会 **删除** NetScreen 设备上任何现有的配置，并要求系统重置。
- 发布 **unset all** CLI 命令不影响 NetScreen 设备上的端口模式设置。例如，如果要将端口模式设置从 Combined 模式更改回缺省 Trust-Untrust 模式，发布 **unset all** 命令会删除现有配置，但不会将设备设置为 Trust-Untrust 模式。

范例 : Home-Work 端口模式

在本例中，将 NetScreen-5XT 上的端口模式设置为 Home-Work 模式。

注意：更改端口模式会删除 NetScreen 设备上任何现有的配置，并要求系统重置。

WebUI

Configuration > Port Mode > Port Mode: 从下拉列表中选择 Home-Work，然后单击 **Apply**。

在下列提示下，单击 **OK**：

Operational mode change will erase current configuration and reset the device, continue?

CLI

```
exec port-mode home-work
```

在下列提示下，输入 **y** (代表 yes)：

Change port mode from <trust-untrust> to <home-work> will erase system configuration and reboot box

Are you sure y/[n] ?

要查看 NetScreen 设备上的当前端口模式设置：

WebUI

Configuration > Port Mode

CLI

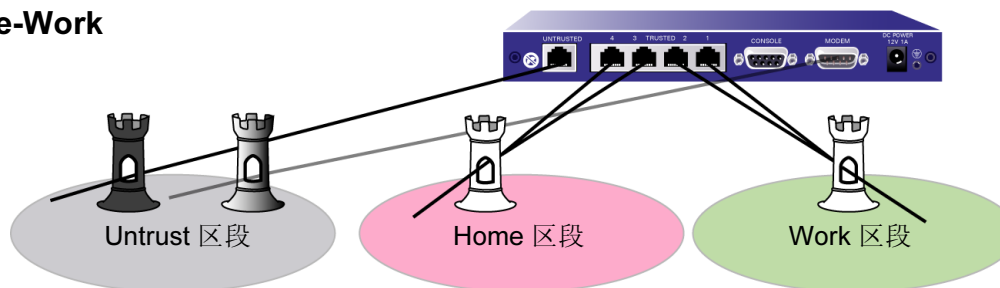
```
get system
```

Home 区段 / Work 区段

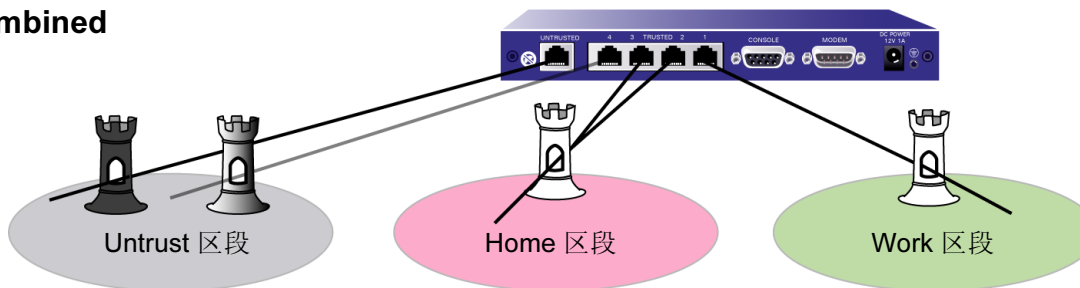
职员远程办公和家用网络成为常见的事时，会发生安全冲突。远程工作者和家庭成员使用的家用网络会成为企业网络的危险途径，由非职员携带威胁（如蠕虫病毒）并允许访问企业资源（如服务器和网络）。

Home-Work 和 Combined 端口模式⁸将 ScreenOS 接口绑定到具体的 Work 和 Home 区段。这样就允许商业及家庭用户和资源的隔离，同时允许 Home 和 Work 区段内的用户访问 Untrust 区段。

Home-Work



Combined



8. 可以仅在某些 NetScreen 设备上设置端口模式。请参阅第 55 页上的“端口模式”。

Home-Work 端口模式也将 MODEM 端口绑定到 Serial 接口，可以将其作为备份接口绑定到 Untrust 安全区。有关使用 Serial 接口作为 Untrust 安全区的备份接口的详细信息，请参阅第 8 卷，“高可用性”。

Combined 端口模式也将 Trusted4 以太网端口作为备份接口 (ethernet3) 绑定到 Untrust 安全区。仅当 Untrust 区段的主接口出现故障时，才使用备份接口。有关使用 ethernet3 接口作为 Untrust 安全区的备份接口的详细信息，请参阅第 8 卷，“高可用性”。

在缺省情况下，NetScreen-5XT 充当“动态主机配置协议” (DHCP) 服务器，为 Work 区段中的 DHCP 客户端分配动态 IP 地址。(有关 DHCP 服务器的详细信息，请参阅第 518 页上的“DHCP 服务器”。)

可以仅使用 Work 区段的 Telnet 连接或 WebUI 配置 NetScreen 设备。不能配置 Home 区段的 NetScreen 设备。不能使用 Home 区段接口上的任何管理服务，包括 ping。Work 区段接口 (ethernet1) 的缺省 IP 地址为 192.168.1.1/24。

Home-Work 和 Combined 端口模式中的缺省策略提供区段间的下列信息流控制：

- 允许所有信息流从 Work 区段流向 Untrust 区段
- 允许所有信息流从 Home 区段流向 Untrust 区段
- 允许所有信息流从 Work 区段流向 Home 区段
- 阻塞所有信息流从 Home 区段流向 Work 区段 (不能删除此策略)

可以为从 Work 区段流向 Untrust 区段、从 Home 区段流向 Untrust 区段及从 Work 区段流向 Home 区段的信息流创建新的策略。也可以删除允许所有从 Work 区段流向 Untrust 区段、从 Home 区段流向 Untrust 区段及从 Work 区段流向 Home 区段的信息流的缺省策略。但是，请注意不能创建允许信息流从 Home 区段流向 Work 区段的策略。

范例 : Home 和 Work 区段

在本例中，首先设置 Home-Work 端口模式下的 NetScreen-5XT 设备，然后配置仅允许 FTP 信息流从 Home 区段流向 Untrust 区段的策略，并删除允许所有信息流从 Home 区段流向 Untrust 区段的缺省策略。在本例中，缺省策略 (允许任意服务的信息流从任意源地址流向任意目的地址) 的 ID 为 2。

警告：更改端口模式会删除 NetScreen 设备上任何现有的配置，并要求系统重置。

WebUI

Configuration > Port Mode > Port Mode: 从下拉列表中选择 Home-Work，然后单击 **Apply**。

在下列提示下，单击 **OK**:

Operational mode change will erase current configuration and reset the device, continue?

Policies > (From: Home, To: Untrust) > New: 输入以下内容，然后单击 **OK**。

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: FTP

Action: Permit

Policies: 在 “From Home to Untrust” 策略列表中，在 ID 为 2 的策略的 Configure 栏中单击 **Remove**。

CLI

```
exec port-mode home-work
```

在下列提示下，输入 **y** (代表 yes)：

```
Change port mode from <trust-untrust> to <home-work> will erase system  
configuration and reboot box
```

```
Are you sure y/[n] ?
```

```
set policy from home to untrust any any ftp permit
```

```
unset policy 2
```

```
save
```


接口

信息流可通过物理接口和子接口 (如入口) 进出安全区。为了使网络信息流能流入和流出安全区, 必须将一个接口绑定到该区段, 如果它是第 3 层区段, 给它分配一个 IP 地址。然后, 必须配置允许信息流在区段之间从接口传递到接口的策略。可将多个接口指派给一个区段, 但是不能将单个接口分配给多个区段。

本章包括以下部分:

- 第 68 页上的 “接口类型”
 - 第 68 页上的 “安全区接口”
 - 第 70 页上的 “功能区段接口”
 - 第 71 页上的 “通道接口”
- 第 76 页上的 “查看接口”
- 第 78 页上的 “配置安全区接口”
 - 第 78 页上的 “将接口绑定到安全区”
 - 第 79 页上的 “为 L3 安全区接口寻址”
 - 第 82 页上的 “从安全区解除接口绑定”
 - 第 83 页上的 “修改接口”
 - 第 84 页上的 “跟踪 IP 地址”
 - 第 99 页上的 “创建子接口”
 - 第 100 页上的 “删除子接口”
- 第 101 页上的 “二级 IP 地址”
 - 第 101 页上的 “二级 IP 地址属性”
- 第 103 页上的 “回传接口”

接口类型

本部分描述安全区、功能区段及通道接口。有关如何查看所有这些接口的表，请参阅[第 76 页上的“查看接口”](#)。

安全区接口

物理接口和子接口的目的是提供一个开口，网络信息流可通过它在区段之间流动。

物理

NetScreen 设备上的每个端口表示一个物理接口，且该接口的名称是预先定义的。物理接口的名称由介质类型、插槽号 (对于某些 NetScreen 设备) 及端口号组成，例如， *ethernet3/2* 或 *ethernet2* (另请参阅[第 3 页上的“安全区接口”](#))。可将物理接口绑定到充当入口的任何安全区，信息流通过该入口进出区段。没有接口，信息流就无法访问或退出区段。

在支持对“接口至区段绑定”进行修改的 NetScreen 设备上，三个物理以太网接口被预先绑定到各特定第 2 层安全区 — V1-Trust、V1-Untrust 和 V1-DMZ。哪个接口绑定到哪个区段根据每个平台而定。(有关安全区的详细信息，请参阅[第 2 页上的“安全区”](#)。)

子接口

子接口，与物理接口相似，充当信息流进出安全区的开口。逻辑上，可将物理接口分成几个虚拟子接口。每个虚拟子接口都从自己来源的物理接口借用所需的带宽，因此其名称是物理接口名称的扩展，例如， *ethernet3/2.1* 或 *ethernet2.1*。(另请参阅[第 3 页上的“安全区接口”](#)。)

可以将子接口绑定到任何区段。还可将子接口绑定到其物理接口的相同区段，或将其绑定到不同区段。(有关详细信息，请参阅[第 78 页上的“将接口绑定到安全区”](#)和[第 7-23 页上的“定义子接口和 VLAN 标记”](#)。)

聚合接口

NetScreen-5000 Series 支持聚合接口。聚合接口是两个或多个物理接口的聚集，其中每个物理接口都平均分担流向聚合接口 IP 地址的信息流负载。通过使用聚合接口，可以增加单个 IP 地址可用的总带宽。同时，如果聚合接口的一个成员失败，其它成员可以继续处理信息流—虽然可用的带宽比以前少。

注意：有关聚合接口的详细信息，请参阅第 8-57 页上的“接口冗余”。

冗余接口

可以将两个物理接口绑定在一起来创建一个冗余接口，然后再将其绑定到安全区。两个物理接口的其中一个接口充当主接口，并处理流向冗余接口的所有信息流。另一个物理接口充当辅助接口以及活动接口失效时的备用接口。如果发生故障，流向冗余接口的信息流切换至辅助接口，该接口成为新的主接口。冗余接口的使用提供了升级到设备级故障切换前的首行冗余。

注意：有关冗余接口的详细信息，请参阅第 8 卷，“高可用性”中的“冗余接口”一章。

虚拟安全接口

虚拟安全接口 (VSI) 是在高可用性 (HA) 模式运行时，两个 **NetScreen** 设备形成虚拟安全设备 (VSD) 共享的虚拟接口。网络和 VPN 信息流使用 VSI 的 IP 地址和虚拟 MAC 地址。然后，VSD 将信息流映像到之前已经将该 VSI 绑定到其上的物理接口、子接口或冗余接口。两个 **NetScreen** 设备在 HA 模式运行时，必须将要在设备发生故障切换时提供不间断服务的安全区接口绑定到一个或多个虚拟安全设备 (VSD)。将接口绑定到 VSD 后，就会得到虚拟安全接口 (VSI)。

注意：有关 VSI 及其如何与 HA 集群中 VSD 一起使用的详细信息，请参阅第 8 卷，“高可用性”。

功能区段接口

功能区段接口，例如，“管理”和 HA，都有专用目的。

管理接口

在一些 NetScreen 设备上，可以通过独立的物理接口 — 管理 (MGT) 接口 — 管理设备，将管理信息流从常规网络用户信息流中分出。将管理信息流从网络用户信息流中分出，大大增加了管理安全性，并确保稳定的管理带宽。

注意：有关配置管理设备的信息，请参阅第 3-1 页上的“管理”。

HA 接口

HA 接口是专用于 HA 功能的物理端口。使用具有专用“高可用性”(HA)接口的 NetScreen 设备，可将两个设备链接在一起，组成冗余组或集群。在冗余组中，一个设备充当主设备，执行网络防火墙、VPN 和信息流整形功能，而另一个设备充当备份设备，通常在主设备发生故障时接替防火墙功能。这是一种主动 / 被动配置。还可以将集群的两个成员都设置为彼此的主设备和备份设备。这是一种主动 / 主动配置。这两种配置在第 8 卷，“高可用性”中都有详尽说明。

虚拟 HA 接口

在没有专用 HA 接口的 NetScreen 设备上，虚拟高可用性 (HA) 接口提供相同的功能。由于没有 HA 信息流专用的独立物理端口，因此必须将“虚拟 HA”接口绑定到物理以太网端口之一。使用和将网络接口绑定到安全区相同的方法，将网络接口绑定到 HA 区段 (请参阅第 78 页上的“将接口绑定到安全区”)。

注意：有关 HA 接口的详细信息，请参阅第 8-38 页上的“双 HA 接口”。

通道接口

通道接口充当 VPN 通道的入口。信息流通过通道接口进出 VPN 通道。

将通道接口绑定到 VPN 通道时，即可在到达特定目标的路由中引用该通道接口，然后在一个或多个策略中引用该目标。利用这种方法，可以精确控制通过该通道的信息流的信息流。它还提供 VPN 信息流的动态路由支持。如果没有通道接口绑定到 VPN 通道，则必须在策略中指定通道并选择 **tunnel** 作为操作。因为操作 **tunnel** 意味着允许，所以不能明确拒绝来自 VPN 通道的信息流。

可使用在通道接口的相同子网中的动态 IP (DIP) 地址池对外向或内向信息流上执行基于策略的 NAT。对通道接口使用基于策略的 NAT 的主要原因是为了避免 IP 地址在 VPN 通道端两个站点间发生冲突。

必须将基于路由的 VPN 通道绑定到通道接口，以便 NetScreen 设备可以路由信息流入出设备。可将基于路由的 VPN 通道绑定到一个有编号 (具有 IP 地址 / 网络掩码) 或没有编号 (没有 IP 地址 / 网络掩码) 的通道接口。如果通道接口没有编号，则必须指定它借用 IP 地址的接口。NetScreen 设备自行启动通过通道的信息流 — 如 OSPF 消息时，NetScreen 设备仅使用借用的 IP 地址作为源地址。通道接口可以从相同或不同安全区的接口借用 IP 地址，只要这两个区段位于同一个路由选择域中。

可以对 VPN 信息流路由进行非常安全的控制，方法是将所有没有编号的通道接口绑定到一个区段 (该区段位于其自身的虚拟路由选择域中)，并且从绑定到同一区段的回传接口借用 IP 地址。例如，可以将所有没有编号的通道接口绑定到一个名为 “VPN” 的用户定义的区段，并且对这些接口进行配置，以便从 **loopback.1** 接口借用 IP 地址，也可绑定到 VPN 区段。VPN 区段位于名为 “vpn-vr” 的用户定义的路由选择域中。将通道通向的所有目标地址放置在 VPN 区段中。对这些地址的路由指向通道接口，策略则控制其他区段和 VPN 区段之间的 VPN 信息流。

```

set vrouter name vpn-vr
set zone name vpn vrouter vpn-vr
set interface loopback.1 zone vpn
set interface loopback.1 ip 172.16.1.1/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip unnumbered loopback.1

```

为 src-1 和 dst-1 配置地址。
配置 VPN 通道并将其绑定到 tunnel.1。

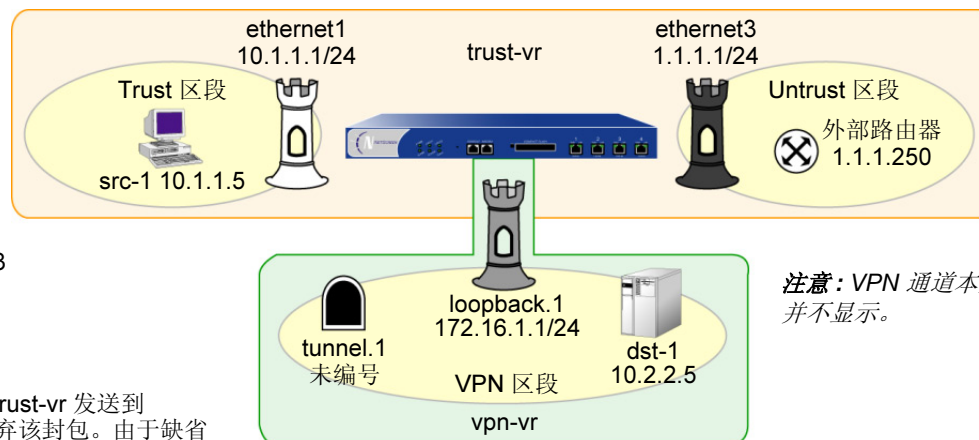
```

set vrouter trust-vr route 10.2.2.5/32 vrouter vpn-vr
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3
gateway 1.1.1.250
set vrouter vpn-vr route 10.2.2.5 interface tunnel.1

```

```
set policy from trust to vpn src-1 dst-1 any permit
```

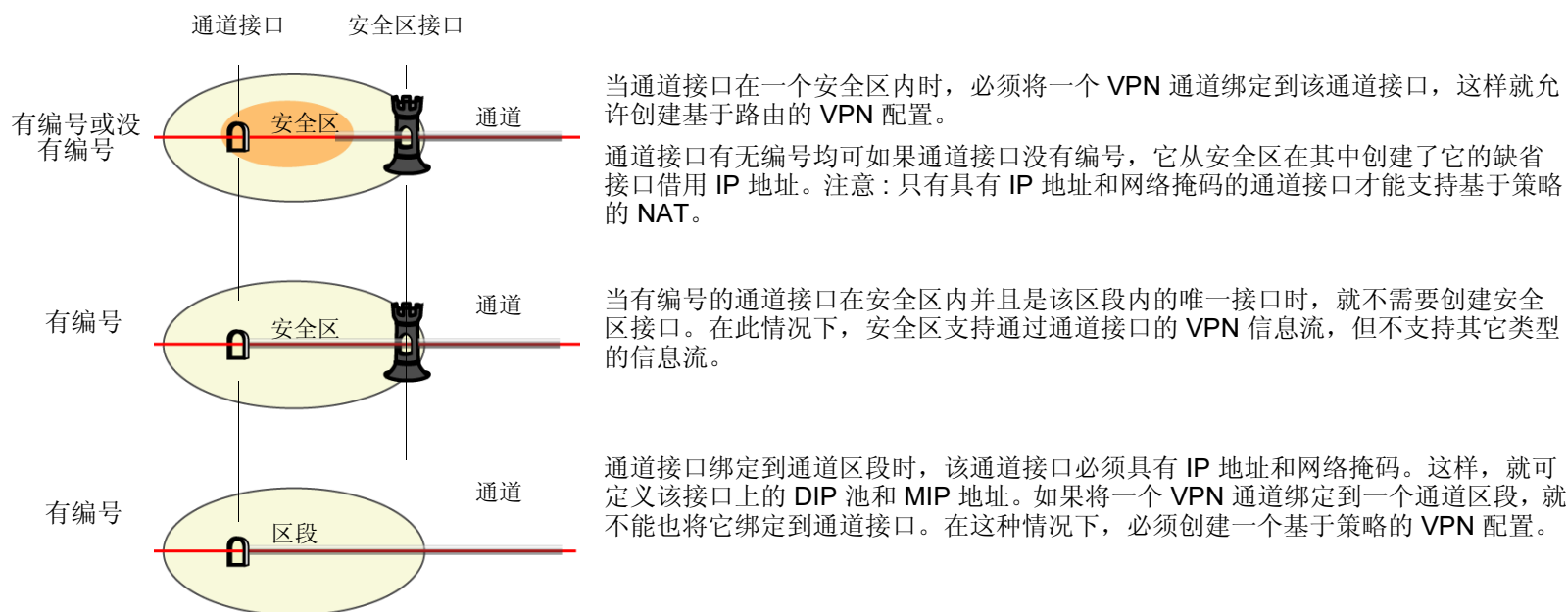
NetScreen 设备将目的地为 10.2.2.5/32 的信息流从 trust-vr 发送到 vpn-vr。如果 tunnel.1 被禁用，NetScreen 设备就丢弃该封包。由于缺省路由 (到 0.0.0.0/0) 仅在 trust-vr 中，因此 NetScreen 设备并不试图将封包以纯文本格式发送出 ethernet3。



将所有通道接口放置在这样的区段中非常安全，因为 VPN 不会由于出现故障 (这样会使通往相关通道接口的路由变成非活动状态) 而重新定向原本让通道使用非通道路由 (如缺省路由) 的信息流。(有关如何避免出现这类问题的两种建议，请参阅第 5-323 页上的“对基于路由的 VPN 设计的安全注意事项”。)

还可将一个通道接口绑定到 Tunnel 区段。这时，必须有一个 IP 地址。将通道接口绑定到 Tunnel 区段的目的是让基于策略的 VPN 通道能够使用 NAT 服务¹。

1. 网络地址转换 (NAT) 服务包括在与接口相同的子网中定义动态 IP (DIP) 池和映射 IP (MIP) 地址。



从概念上讲, 可将 VPN 通道当作铺设的管道。它们从本地设备延伸到远程网关, 而通道接口就是这些管道的开口。管道始终存在, 只要路由引擎将信息流引导到接口之一就可随时使用。

通常, 如果希望接口支持源地址转换 (NAT-src) 的一个或多个动态 IP (DIP) 池和目标地址转换 (NAT-dst) 的映射 IP (MIP) 地址, 请为该通道接口分配一个 IP 地址。有关 VPN 和地址转换的详细信息, 请参阅第 5-168 页上的“具有重叠地址的 VPN 站点”。可以在安全区或通道区段创建具有 IP 地址和网络掩码的通道接口。

如果通道接口不需要支持地址转换, 并且配置不要求将通道接口绑定到一个 Tunnel 区段, 则可以将该接口指定为无编号。必须将一个没有编号的通道接口绑定到安全区; 同时不能将其绑定到 Tunnel 区段。还必须指定一个具有 IP 地址的接口, 该接口位于与绑定没有编号接口的安全区相同的虚拟路由选择域中。无编号的通道接口借用该接口的 IP 地址。

注意: 有关显示如何将通道接口绑定到通道的范例, 请参阅第 5-69 页上的“站点到站点 VPN”和第 5-199 页上的“拨号 VPN”中基于路由的 VPN 范例。

删除通道接口

不能立即删除拥有映射 IP 地址 (MIP) 或 “动态 IP (DIP)” 地址池的通道接口。删除拥有这些特征的通道接口前，必须首先删除引用它们的所有策略。然后必须删除通道接口上的 MIP 和 DIP 池。如果基于路由的 VPN 配置引用一个通道接口，则必须首先删除 VPN 配置，然后删除通道接口。

范例：删除通道接口

在本范例中，通道接口 `tunnel.2` 被链接到 DIP 池 8。通过名为 `vpn1` 的 VPN 通道，从 Trust 区段到 Untrust 区段的 VPN 信息流的策略 (ID 10) 引用 DIP 池 8。要删除该通道接口，必须首先删除该策略 (或从该策略中删除引用的 DIP 池 8)，然后删除 DIP 池。然后，必须解除 `tunnel.2` 到 `vpn1` 的绑定。删除依赖通道接口的所有配置后，即可删除该通道接口。

WebUI

1. 删除引用 DIP 池 8 的策略 10

Policies (From: Trust, To: Untrust): 单击策略 ID 10 的 **Remove**。

2. 删除链接到 Tunnel.2 的 DIP 池 8

Network > Interfaces > Edit (对于 `tunnel.2`) > DIP: 单击 DIP ID 8 的 **Remove**。

3. 解除来自 `vpn1` 的 `tunnel.2` 绑定

VPNs > AutoKey IKE > Edit (对于 `vpn1`) > Advanced: 在 Bind to: Tunnel Interface 下拉列表中选择 **None**，单击 **Return**，然后单击 **OK**。

4. 删除 Tunnel.2

Network > Interfaces: 单击 `tunnel.2` 的 **Remove**。

CLI

1. 删除引用 DIP 池 8 的策略 10

```
unset policy 10
```

2. 删除链接到 Tunnel.2 的 DIP 池 8

```
unset interface tunnel.2 dip 8
```

3. 解除来自 vpn1 的 Tunnel.2 绑定

```
unset vpn vpn1 bind interface
```

4. 删除 Tunnel.2

```
unset interface tunnel.2  
save
```

查看接口

可查看列出 NetScreen 设备上所有接口的表。因为物理接口是预定义的，所以不管是否配置，它们都会列出。而对于子接口和通道接口来说，只有在创建和配置后才列出。

要在 WebUI 中查看接口表，请单击 **Network > Interfaces**。可指定接口类型从 **List Interfaces** 下拉菜单显示。

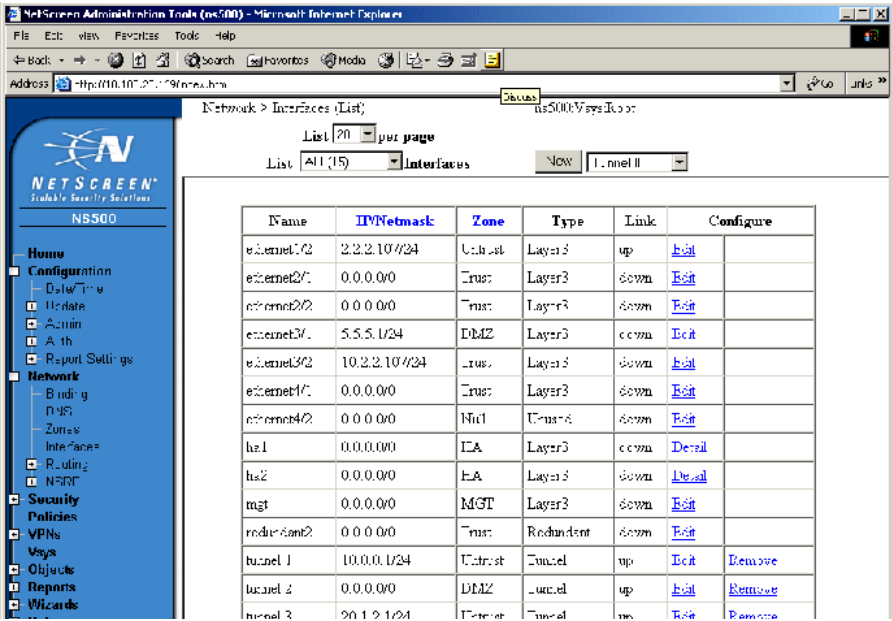
要在 CLI 中查看接口表，请使用 **get interface** 命令。

接口表

接口表显示每个接口的下列信息：

- **Name:** 此字段确定接口的名称。
- **IP/Netmask:** 此字段确定接口的 IP 地址和网络掩码地址。
- **Zone:** 此字段确定将接口绑定到的区段。
- **Type:** 此字段指出接口类型：Layer 2（第 2 层）、Layer 3（第 3 层）、tunnel（通道）、redundant（冗余）、aggregate（聚合）、VSI。
- **Link:** 此字段确定接口是否为活动 (Up) 或非活动 (Down)。
- **Configure:** 此字段允许修改或移除接口。

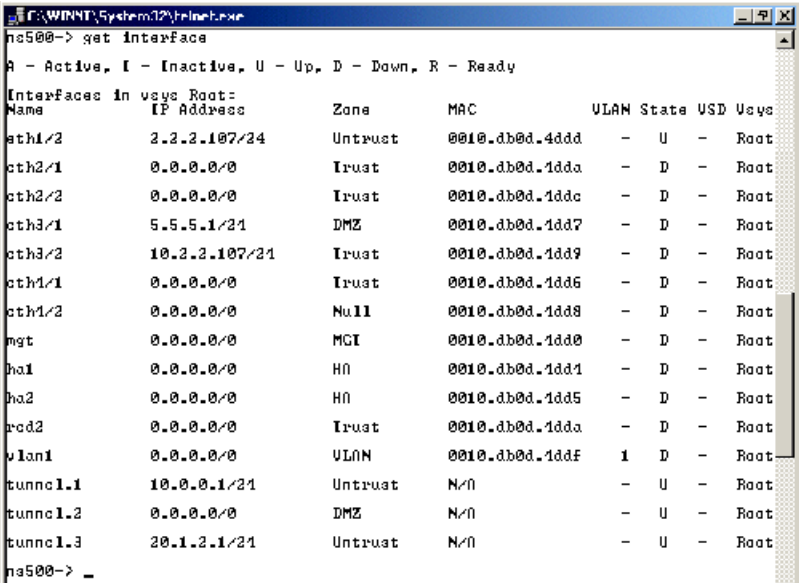
WebUI 接口表



The screenshot shows the NetScreen Administration Tools (ns500) WebUI. The left sidebar contains a navigation menu with options like Home, Configuration, Network, Security, and VPNs. The main content area displays a table of interfaces. The table has columns for Name, IPvNetmask, Zone, Type, Link, and Configure. The interfaces listed include ethernet1/2, ethernet2/1, ethernet2/2, ethernet3/1, ethernet3/2, ethernet4/1, ethernet4/2, hsa1, hsa2, mgt, router2, tunnel1, tunnel2, and tunnel3.

Name	IPvNetmask	Zone	Type	Link	Configure
ethernet1/2	2.2.2.107/24	Untrust	Layer3	up	Edit
ethernet2/1	0.0.0.0/0	Trust	Layer3	down	Edit
ethernet2/2	0.0.0.0/0	Trust	Layer3	down	Edit
ethernet3/1	5.5.5.1/24	DMZ	Layer3	down	Edit
ethernet3/2	10.2.2.107/24	Trust	Layer3	down	Edit
ethernet4/1	0.0.0.0/0	Trust	Layer3	down	Edit
ethernet4/2	0.0.0.0/0	Null	Trust	down	Edit
hsa1	0.0.0.0/0	HA	Layer3	down	Detail
hsa2	0.0.0.0/0	HA	Layer3	down	Detail
mgt	0.0.0.0/0	MGT	Layer3	down	Edit
router2	0.0.0.0/0	Trust	Redundant	down	Edit
tunnel1	10.0.0.1/24	Untrust	Tunnel	up	Edit Remove
tunnel2	0.0.0.0/0	DMZ	Tunnel	up	Edit Remove
tunnel3	20.1.2.1/24	Untrust	Tunnel	up	Edit Remove

CLI 接口表



The screenshot shows the NetScreen CLI interface. The command 'get interface' has been executed, and the output displays a table of interfaces with columns for Name, IP Address, Zone, MAC, VLAN, State, USD, and Usage. The interfaces listed include eth1/2, eth2/1, eth2/2, eth3/1, eth3/2, eth4/1, eth4/2, mgt, hsa1, hsa2, router2, vlan1, tunnel1.1, tunnel1.2, and tunnel1.3.

Name	IP Address	Zone	MAC	VLAN	State	USD	Usage
eth1/2	2.2.2.107/24	Untrust	0010.db0d.4ddd	-	U	-	Root
eth2/1	0.0.0.0/0	Trust	0010.db0d.1dda	-	D	-	Root
eth2/2	0.0.0.0/0	Trust	0010.db0d.1ddc	-	D	-	Root
eth3/1	5.5.5.1/24	DMZ	0010.db0d.1dd7	-	D	-	Root
eth3/2	10.2.2.107/24	Trust	0010.db0d.1dd9	-	D	-	Root
eth4/1	0.0.0.0/0	Trust	0010.db0d.1dd6	-	D	-	Root
eth4/2	0.0.0.0/0	Null	0010.db0d.1dd8	-	D	-	Root
mgt	0.0.0.0/0	MGT	0010.db0d.1dd0	-	D	-	Root
hsa1	0.0.0.0/0	HA	0010.db0d.1dd1	-	D	-	Root
hsa2	0.0.0.0/0	HA	0010.db0d.1dd5	-	D	-	Root
router2	0.0.0.0/0	Trust	0010.db0d.1dda	-	D	-	Root
vlan1	0.0.0.0/0	VLAN	0010.db0d.1ddf	1	D	-	Root
tunnel1.1	10.0.0.1/24	Untrust	N/A	-	U	-	Root
tunnel1.2	0.0.0.0/0	DMZ	N/A	-	U	-	Root
tunnel1.3	20.1.2.1/24	Untrust	N/A	-	U	-	Root

配置安全区接口

本部分描述如何配置安全区接口的以下方面：

- 将接口绑定到安全区及解除绑定
- 将地址分配到 L3 (第 3 层) 安全区接口
- 修改物理接口和子接口
- 创建子接口
- 删除子接口

注意：有关为接口设置信息流带宽的信息，请参阅第 10 章，“信息流整形”。有关每种接口可用的管理及其它可用服务选项的详细信息，请参阅第 3-29 页上的“控制管理信息流”。

将接口绑定到安全区

可将任何物理接口绑定到 L2 (第 2 层) 或 L3 (第 3 层) 安全区。由于子接口需要 IP 地址，因此仅可将子接口绑定到 L3 (第 3 层) 安全区。将接口绑定到 L3 安全区后，才能将 IP 地址指定给接口。

范例：绑定接口

在本例中，将 ethernet5 绑定到 Trust 区段。

WebUI

Network > Interfaces > Edit (对于 ethernet5): 从 Zone Name 下拉列表中选择 **Trust**，然后单击 **OK**。

CLI

```
set interface ethernet5 zone trust
save
```

为 L3 安全区接口寻址

定义 L3 (第 3 层) 安全区接口或子接口时，必须给它分配 IP 地址和网络掩码。如果将接口绑定到 **trust-vr** 中的区段，则还可指定接口模式为 **NAT** 或 **Route** (路由)。(如果将接口绑定到的区段在 **untrust-vr** 中，则接口模式始终是 **Route** (路由)。)

注意：有关 **NAT** 和 **Route** (路由) 模式的配置，请参阅第 5 章，第 107 页上的“接口模式”。

进行接口地址分配时，要考虑的两种基本类型的 IP 地址如下：

- 公开地址，由互联网服务提供商 (ISP) 提供的地址，用于公用网络 (如互联网) 并且必须是唯一的
- 私有地址，由本地网络管理员分配，用于私有网络并且其它管理员也可分配用于其私有网络

注意：将 IP 地址添加到接口后，**NetScreen** 设备将通过 **ARP** 请求进行检查，以确保本地网络中不存在该 IP 地址。(此时物理链接必须为工作中状态。) 如果 IP 地址已存在，则会显示警告。

公开 IP 地址

连接到公开网络的接口必须有公开 IP 地址。同样，如果 **untrust-vr** 中的 **Layer** (第 3 层) 安全区连接到公开网络，并且 **trust-vr** 中区段的接口模式为 **Route** (路由)，那么 **trust-vr** 的区段中所有地址 (包括接口和主机的地址) 也必须为公开地址。公开 IP 地址分成三类，**A**、**B** 和 **C**²，显示如下：

地址类别	地址范围	排除的地址范围
A	0.0.0.0 – 127.255.255.255	10.0.0.0 – 10.255.255.255, 127.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.31.255.255
C	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255

2. 还有 **D** 和 **E** 类地址，保留为专用。

IP 地址由四个八位位组组成，每个八位位组长为 8 位。在 A 类地址中，前 8 位表示网络 ID，后 24 位表示主机 ID (nnn.hhh.hhh.hhh)。在 B 类地址中，前 16 位表示网络 ID，后 16 位表示主机 ID (nnn.nnn.hhh.hhh)。在 C 类地址中，前 24 位表示网络 ID，后 8 位表示主机 ID (nnn.nnn.nnn.hhh)。

通过应用子网掩码 (或网络掩码)，可进一步划分网络。实际上，网络掩码掩蔽了主机 ID 的一部分，以便使掩蔽的部分成为网络 ID 的子网。例如，地址 10.2.3.4/24 中的 24 位掩码³指出，前 8 位 (即第一个 8 位位组 — 010) 识别此 A 类私有地址的网络部分，中间 16 位 (即第二个和第三个 8 位位组 — 002.003) 识别地址的子网络部分，最后 8 位 (最后一个 8 位位组 — 004) 识别地址的主机部分。使用子网可将大的网络地址空间缩小为较小的子部分，这样大大增强了 IP 数据报的传输效率。

私有 IP 地址

如果将接口连接到私有网络，那么本地网络管理员可将任何地址分配给它，虽然通常是使用私有地址保留范围中的地址 — 10.0.0.0/8，172.16.0.0 – 172.31.255.255，192.168.0.0/16— 如 RFC 1918，“Address Allocation for Private Internets (私有互联网地址分配)”中定义。

如果将 untrust-vr 中的第 3 层安全区连接到公开网络，并且 trust-vr 中绑定到各区段的各接口模式为 NAT，那么 trust-vr 的区段中所有地址 (包括接口和主机的地址) 都可为私有地址。

3. 24 位掩码的十进制点格式等值为 255.255.255.0。

范例：编址接口

在本例中，将给 **ethernet5** 分配 IP 地址 **210.1.1.1/24**、“管理 IP”地址 **210.1.1.5**。（请注意，“管理 IP”地址必须在与安全区接口 IP 地址相同的子网中。）最后，将接口模式设置为 **NAT**，将所有内部 IP 地址转换至绑定到其它安全区的缺省接口⁴。

WebUI

Network > Interfaces > Edit (对于 **ethernet5**): 输入以下内容，然后单击 **OK**:

IP Address/Netmask: **210.1.1.1/24**

Manage IP: **210.1.1.5**

CLI

```
set interface ethernet5 ip 210.1.1.1/24
set interface ethernet5 manage-ip 210.1.1.5
save
```

4. 安全区的缺省接口是绑定到该区段的第一个接口。要查明哪个接口是区段的缺省接口，请在 WebUI 中查看 **Network > Zones** 页中的 **Default IF** 栏，或在 CLI 中查看 **get zone** 命令输出内容中的 **Default-If** 栏。

从安全区解除接口绑定

如果接口未编号，那么可解除其到一个安全区的绑定，然后绑定到另一个安全区。如果接口已编号，则必须首先将其 IP 地址和网络掩码设置为 0.0.0.0。然后，可解除其到一个安全区的绑定，然后绑定到另一个安全区，并 (可选) 给它分配 IP 地址 / 网络掩码。

范例：解除接口绑定

在本例中，**ethernet3** 的 IP 地址为 **210.1.1.1/24** 并且被绑定到 **Untrust** 区段。将其 IP 地址和网络掩码设置为 **0.0.0.0/0** 并将其绑定到 **Null** 区段。

WebUI

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Null

IP Address/Netmask: 0.0.0.0/0

CLI

```
set interface ethernet3 ip 0.0.0.0/0
set interface ethernet3 zone null
save
```


修改接口

配置物理接口、子接口、冗余接口、聚合接口或“虚拟安全接口”(VSI)后,需要时可更改下列任何设置:

- IP 地址和网络掩码
- 管理 IP 地址
- (第 3 层区段接口)管理和网络服务
- (子接口)子接口 ID 号和 VLAN 标记号
- (trust-vr 中绑定到 L3 (第 3 层)安全区的接口)接口模式 — NAT 或“路由”
- (物理接口)信息流带宽设置(请参阅第 10 章,第 493 页上的“信息流整形”)
- (物理、冗余和聚合接口)最大传输单位(MTU)大小
- (第 3 层接口)阻止进出相同接口的信息流,包括主子网和辅助子网之间或两个辅助子网之间的信息流(通过含有 **route-deny** 选项的 CLI **set interface** 命令来完成)

对于某些 NetScreen 设备上的物理接口,可以强迫物理链接状态处于不在工作中或工作中状态。如果强迫物理链接状态处于不在工作中状态,则可模拟电缆与接口端口的断开。(通过含有 **phy link-down** 选项的 CLI **set interface** 命令来完成。)

范例:修改接口设置

在本例中,对 **ethernet1** 进行一些修改,它是一个绑定到 **Trust** 区段的接口。将“管理 IP”地址从 10.1.1.2 更改为 10.1.1.12。为了确保管理信息流的绝对安全,还更改了管理服务选项,启用 **SCS** 和 **SSL** 并禁用 **Telnet** 和 **WebUI**。

WebUI

Network > Interfaces > Edit (对于 ethernet1): 进行以下修改,然后单击 **OK**:

Manage IP: 10.1.1.12

Management Services: (选择) SSH, SSL; (清除) Telnet, WebUI

CLI

```
set interface ethernet1 manage-ip 10.1.1.12
set interface ethernet1 manage ssh
set interface ethernet1 manage ssl
unset interface ethernet1 manage telnet
unset interface ethernet1 manage web
save
```

跟踪 IP 地址

NetScreen 设备可以通过接口跟踪指定的 IP 地址，所以，如果一个或多个 IP 地址不可达，**NetScreen** 设备就可以禁用所有与该接口相关联的路由，即使物理链接仍处于活动状态⁵。在 **NetScreen** 设备与这些 IP 地址重新取得联系后，禁用的路由就恢复为活动路由。

类似于 **NSRP** 中使用的功能，**NetScreen** 使用第 3 层路径监控或 *IP 跟踪* 监控经过接口的指定 IP 地址的可达性。例如，如果接口直接连接到路由器，则可跟踪接口的下一跳跃地址，以确定该路由器是否仍旧可达。在配置接口上的 IP 跟踪时，**NetScreen** 设备在接口上向最多 4 个目标 IP 地址以用户定义的时间间隔发送 ping 请求。**NetScreen** 设备监控这些目标以确定是否能接收到响应。如果目标在指定的次数内未响应，则视该 IP 地址为不可达。不能引发一个或多个目标响应时，会导致 **NetScreen** 设备禁用与该接口相关联的路由。如果存在另外一个连接同一目标的路由，**NetScreen** 设备就会重新定向信息流以使用新路由。

5. 对于某些 **ScreenOS** 设备，此操作还会引起到备份接口（该备份接口绑定到与配置了 IP 跟踪的接口相同的区段上）的故障切换（请参阅第 8-69 页上的“确定接口故障切换”）。

IP 跟踪重新路由信息流

如果经过一个接口不可到达某个 IP 地址，则配置接口上的 IP 跟踪可以使 NetScreen 经过另一个接口重新路由外向信息流。虽然 NetScreen 设备可能会因为 IP 跟踪失败而禁用与接口相关联的路由，但是该接口仍然处于物理活动状态并仍然能够发送和接收信息流。例如，NetScreen 设备继续处理现存会话的内向信息流，而该信息流可能会到达 IP 跟踪已失败的初始接口。此外，NetScreen 设备继续使用该接口向目标 IP 地址发送 ping 请求以确定目标是否重新变为可达。在这些情况下，信息流仍然会经过 IP 跟踪已失败并且 NetScreen 设备已禁用其路由的接口。NetScreen 设备处理此类接口上的会话信息流的方法取决于下列情况：

- 如果配置 IP 跟踪的接口是会话的出口接口，则会话回复可能会继续到达该接口，NetScreen 设备也仍然会处理该回复。
- 如果配置 IP 跟踪的接口是会话的入口接口，则使用命令 **set arp always-on-dest** 可使 NetScreen 设备重新路由会话回复至另一个接口。如果不设置此命令，则 NetScreen 设备经过 IP 跟踪已失败的接口转发会话回复，即使 NetScreen 设备已经禁用使用该接口的路由。（在缺省情况下，此命令未设置。）

在缺省情况下，NetScreen 设备在接收到新会话的初始封包时缓存会话发起方的 MAC 地址。如果输入 CLI 命令 **set arp always-on-dest**，则 NetScreen 设备不缓存会话发起方的 MAC 地址。相反地，NetScreen 设备在处理初始封包的回复时执行 ARP 查找。如果发起方的 MAC 地址在 ARP 表中，则 NetScreen 设备使用该地址。如果 MAC 地址不在 ARP 表中，则 NetScreen 设备向目的 MAC 地址发送 ARP 要求，然后将接收到的 MAC 地址添加到 ARP 表中。只要发生路由变更，NetScreen 设备就执行一次 ARP 查找。

下节分别说明出口接口和入口接口上 IP 跟踪失败的情况；以及对于后者，使用命令 **set arp always-on-dest** 时发生的情况。

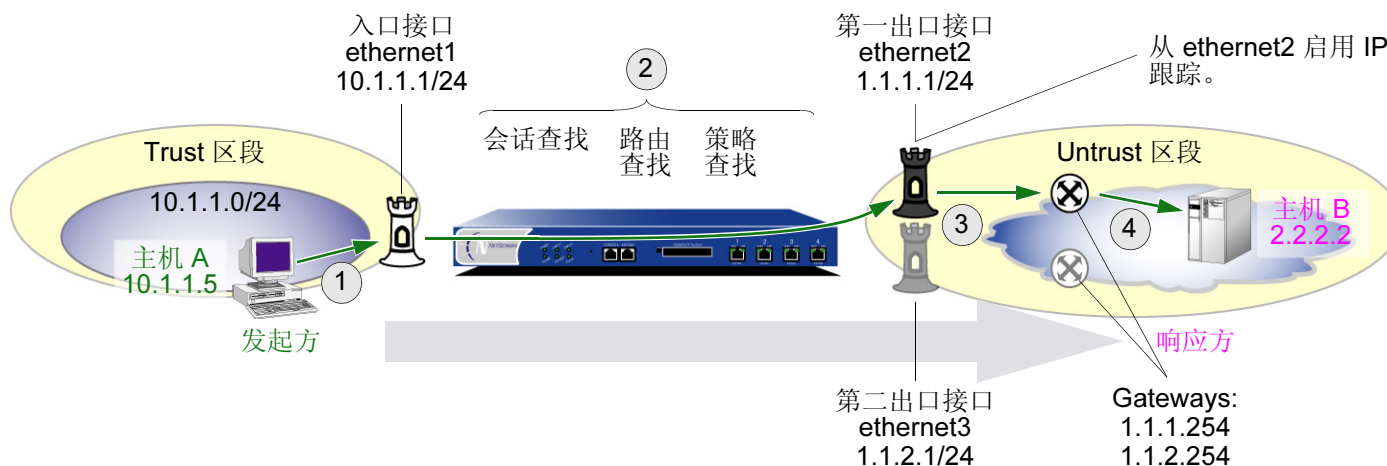
注意：下节说明 IP 跟踪如何触发路由变更以及这些变更如何影响经过所有 NetScreen 设备 (NetScreen-5XT 和 -5GT 除外) 的封包流。对于这些设备，IP 跟踪失败触发接口故障切换。有关详细信息，请参阅第 8-67 页上的“双 Untrust 接口”。

出口接口上的失败

在下述情况中，在 **ethernet2** (主机 A 与主机 B 之间会话的入口接口) 上配置 IP 跟踪。主机 A 通过向主机 B 发送封包发起会话，如下所示。

注意：首先必须创建两个通往主机 B 的路由并且两个出口接口必须在同一区段，以便让同一策略应用于重新路由发生前后。

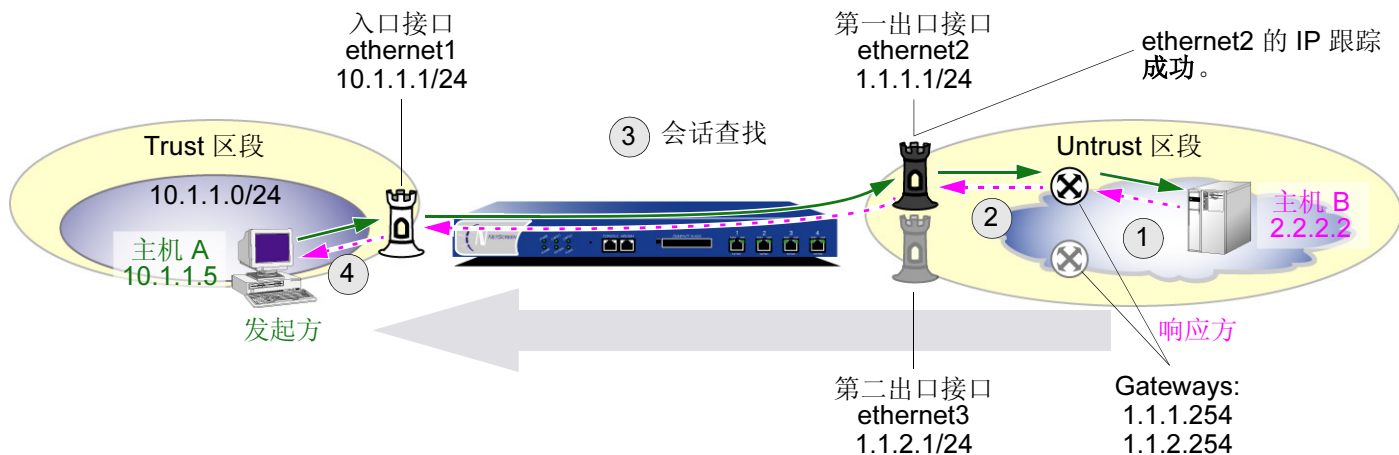
从主机 A 到主机 B 的信息流 – 请求 (发起会话)



1. 位于 10.1.1.5 的主机 A 将目的地为位于 2.2.2.2 的主机 B 的封包发送至 ethernet1 (10.1.1.1)。
2. NetScreen 设备执行以下任务：
 - 2.1 **会话查找** – 如果这是第一个封包，NetScreen 设备创建一个会话。如果该封包属于现有会话，则会刷新会话表条目。
 - 2.2 **路由查找** – NetScreen 设备对会话的第一个封包执行路由查找，如果路由发生变更，则再次进行路由查找。经过路由查找，找到以下路由：要到达 0.0.0.0/0，请从接口 ethernet2 发送封包至网关 1.1.1.254。
 - 2.3 **策略查找** – 对于主机 A 所发送的信息流类型，NetScreen 设备对从 Trust 区段的主机 A 到 Untrust 区段的主机 B 的区段内部信息流加强安全策略。
3. NetScreen 设备经过 ethernet2 将封包转发到网关 1.1.1.254。
4. 网关 1.1.1.254 将封包转发到下一跳跃。路由一直继续到主机 B 接收到封包。

当主机 B 回复主机 A 时，返回的信息流经过 NetScreen 设备沿着类似的路径传回，如下所示。

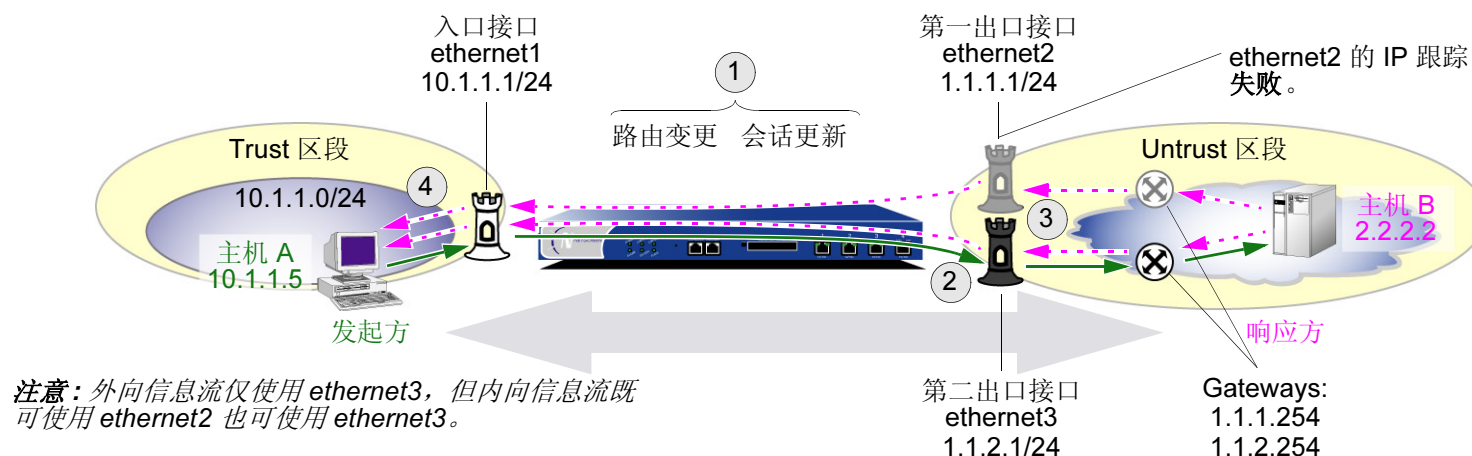
从主机 A 到主机 B 的信息流 – 回复



1. 位于 2.2.2.2 的主机 B 向位于 10.1.1.5 的主机 A 回复一个封包 (为了清楚起见, 省略 NAT)。
2. 当网关 1.1.1.254 收到回复时, 将回复转发至下一跳跃, 即 ethernet2 的 IP 地址 1.1.1.1。
3. NetScreen 设备执行会话查找。因为这是一个回复, NetScreen 设备将其与现有会话进行匹配并刷新会话表条目。
4. 利用主机 A 的缓存 MAC 地址或通过 ARP 查找找到主机 A 的 MAC 地址, NetScreen 设备经过 ethernet1 将封包转发至主机 A。

如果 ethernet2 上的 IP 跟踪失败，NetScreen 设备就禁用使用 ethernet2 的路由，然后使用 ethernet3 向主机 B 发出出站信息流。但是，从主机 B 发送至主机 A 的回复既可经过 ethernet2 也可经过 ethernet3 到达，NetScreen 设备经过 ethernet1 将回复转发至主机 A。

从主机 A 到主机 B 的信息流 – IP 跟踪失败触发重新路由

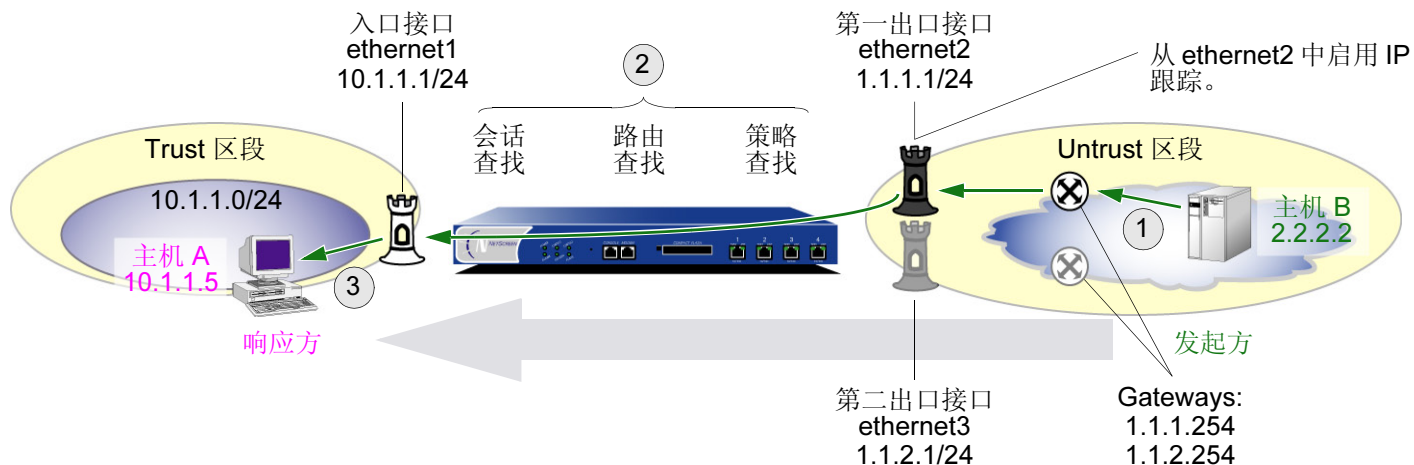


1. 当 ethernet2 上的 IP 跟踪失败时，NetScreen 设备执行以下任务：
 - 1.1 路由变更 – NetScreen 设备禁用所有使用 ethernet2 的路由。NetScreen 设备进行路由查找，以使用 ethernet3 和网关 1.1.2.254 的路由替换使用 ethernet2 和网关 1.1.1.254 的通往 2.2.2.2 的路由。
 - 1.2 会话更新 – NetScreen 设备扫描会话表中所有使用 ethernet2 的条目，然后将这些条目经过 ethernet3 重新路由到网关 1.1.2.254。
2. 现在，NetScreen 设备将来自主机 A 的信息流从 ethernet3 改发到 1.1.2.254。
3. 来自主机 B 的回复既可到达 ethernet2 也可到达 ethernet3。NetScreen 设备执行会话查找并将封包与现有会话进行匹配。不论封包到达哪个接口，NetScreen 设备都经过 ethernet1 将封包转发到主机 A。
4. NetScreen 设备经过 ethernet1 将封包转发到主机 A。

入口接口上的失败

在下述情况中，再次在 **ethernet2** 上配置 IP 跟踪，但是，这次 **ethernet2** 是 NetScreen 设备上从主机 B 到主机 A 的会话的入口接口。主机 A 通过向主机 B 发送封包发起会话，如下所示。

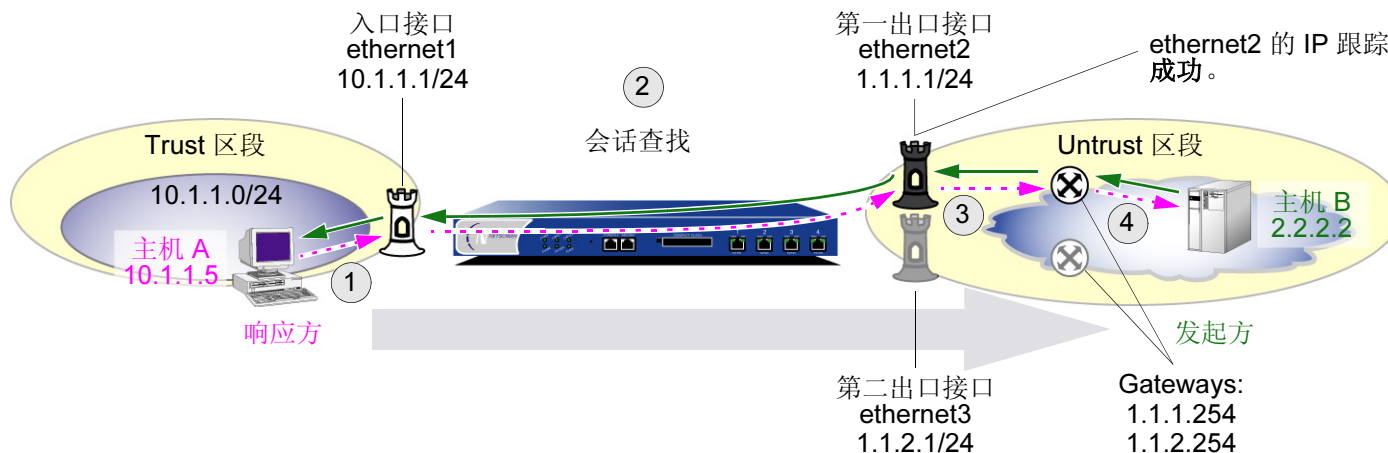
从主机 B 到主机 A 的信息流 – 请求 (发起会话)



1. 位于 2.2.2.2 的主机 B 向位于 10.1.1.5 的主机 A 发送一个封包 (为了清楚起见, 省略 NAT)。
2. 当封包到达 **ethernet2** 时, NetScreen 设备执行以下任务:
 - 2.1 会话查找 (由于这是会话的第一个封包, 所以创建一个新的会话表条目)
 - 2.2 路由查找
 - 2.3 策略查找
3. NetScreen 设备经过 **ethernet1** 将封包转发到位于 10.1.1.5 的主机 A。

主机 A 回复主机 B 时，返回的信息流经过 NetScreen 设备沿着类似的路径传回，如下所示。

从主机 B 到主机 A 的信息流 – 回复



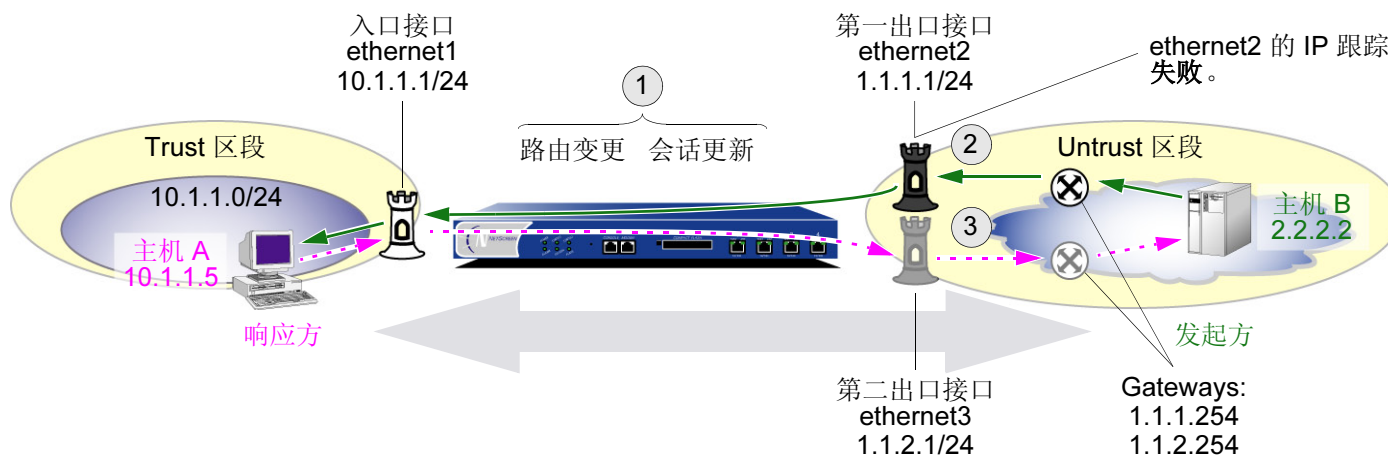
1. 位于 10.1.1.5 的主机 A 将目的地为位于 2.2.2.2 的主机 B 发送至位于 10.1.1.1 的 ethernet1。
2. NetScreen 设备执行会话查找。因为这是一个回复，NetScreen 设备将其与现有会话进行匹配并刷新会话表条目。
3. 利用网关 1.1.1.254 的缓存 MAC 地址或通过 ARP 查找找到网关的 MAC 地址，NetScreen 设备经过 ethernet2 将封包转发至该网关。
4. 当网关 1.1.1.254 接收到回复时，将回复转发到下一跳跃。路由会一直继续到主机 B 接收到回复。

如果 ethernet2 上的 IP 跟踪失败，NetScreen 设备禁用使用 ethernet2 的路由，然后使用 ethernet3 向主机 B 发送出站信息流。但是，主机 B 发送至主机 A 的请求仍可经过 ethernet2 到达，NetScreen 设备也依然经过 ethernet1 将请求转发至主机 A。从主机 B 到主机 A 的请求数据流在 IP 跟踪失败前后显示相同。但是，根据命令 **set arp always-on-dest** 的应用，主机 A 的回复可经过两个不同的路径传送。

如果设置命令 **set arp always-on-dest**，NetScreen 设备在处理会话的第一个封包的回复时或路由发生变更时，向目的 MAC 地址发送 ARP 请求。(未设置此命令时，NetScreen 设备缓存会话发起方的 MAC 地址并在处理回复时使用该地址。在缺省情况下，此命令未设置。)

当 ethernet2 上的 IP 跟踪失败时，NetScreen 设备首先禁用所有使用 ethernet2 的路由，然后进行路由查找。NetScreen 设备找到另一条经过 ethernet3 和网关 1.1.2.254 而到达主机 B 的路由。然后，NetScreen 设备扫描会话表，将全部会话改发至新路由。如果启用命令 **set arp always-on-dest**，NetScreen 设备在接收到主机 A 的下一个封包时进行 ARP 查找，因为该封包位于受路由变更影响的会话。不论来自主机 B 的封包达到哪个入口接口，NetScreen 设备都经过 ethernet3 将主机 A 的全部后续回复发送至网关 1.1.2.254。

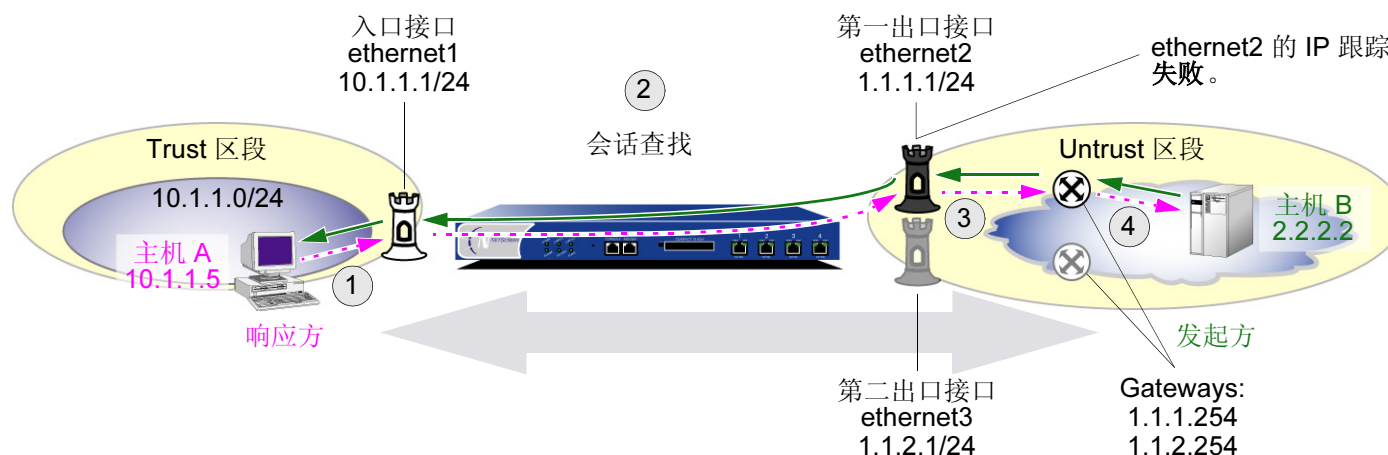
从主机 B 到主机 A 的信息流 – IP 跟踪失败触发重新路由



1. 当 ethernet2 上的 IP 跟踪失败时，NetScreen 设备执行以下任务：
 - 1.1 路由变更 – NetScreen 设备禁用所有使用 ethernet2 的路由。NetScreen 设备用一条经过 ethernet3 和网关 1.1.2.254 的路由替换经过 ethernet2 和网关 1.1.2.254 的通往 2.2.2.2 的路由。
 - 1.2 会话更新 – NetScreen 设备扫描会话表中所有使用 ethernet2 的条目，然后将这些条目经过 ethernet3 重新路由到网关 1.1.2.254。
2. 来自主机 B 的请求可能仍然到达 ethernet2，也可能被路由结构改发到 ethernet3。NetScreen 设备执行会话查找并将封包与现有会话进行匹配。
3. 由于已输入命令 **set arp always-on-dest**，所以 NetScreen 设备对主机 A 的回复进行 ARP 查找，并经过 ethernet3 将其发送到网关 1.1.2.254。

如果未输入命令 **set arp always-on-dest** (这是缺省配置), NetScreen 设备使用主机 B 发送初始会话封包时缓存的网关 1.1.1.1 的 MAC 地址。NetScreen 设备继续经过 ethernet2 发送会话回复。在这种情况下, IP 跟踪失败不会导致经过 NetScreen 设备的数据流的改变。

从主机 B 到主机 A 的信息流 – IP 跟踪失败不触发重新路由



- 当 ethernet2 上的 IP 跟踪失败时, NetScreen 设备执行以下任务:
 - 路由变更** – NetScreen 设备禁用所有使用 ethernet2 的路由。NetScreen 设备用一条经过 ethernet3 和网关 1.1.2.254 的路由替换经过 ethernet2 和网关 1.1.2.254 的通往 2.2.2.2 的路由。
 - 会话更新** – NetScreen 设备扫描会话表中所有使用 ethernet2 的条目,然后将这些条目经过 ethernet3 重新路由至网关 1.1.2.254。但是,由于 NetScreen 设备缓存了网关 1.1.1.254 的 MAC 地址,所以,对于主机 A 的回复,NetScreen 设备继续使用该 MAC 地址。
- 来自主机 B 的请求仍可到达 ethernet2。NetScreen 设备执行会话查找,将封包与现有会话进行匹配,然后经过 ethernet1 将封包转发至位于 10.1.1.5 的主机 A。
- 当主机 A 回复时,NetScreen 设备经过 ethernet2 将回复转发到网关 1.1.1.254。因为命令 **set arp always-on-dest** 未设置,所以会话表中的 MAC 地址仍保持条目的初始创建状态不变。

配置 IP 跟踪

可在以下已配置了管理 IP 地址的第 3 层接口上定义 IP 跟踪：

- 物理接口
- 子接口
- 冗余接口
- 聚合接口

注意：虽然接口可以是冗余接口或聚合接口，但不能是冗余接口或聚合接口的成员。

不能在第 2 层接口或绑定到 HA 或 MGT 功能区段的接口上定义 IP 跟踪。

在支持虚拟系统的设备上，设置 IP 跟踪的接口可以属于根系统或虚拟系统 (vsys) 并且可同时在根级和 vsys 级上运行。

可为每个接口配置最多 4 个 IP 地址，以便 NetScreen 设备进行跟踪。在一个设备上，可以配置最多 64 个跟踪 IP 地址。这包括所有的跟踪 IP 地址，无论是基于接口的 IP 跟踪，还是基于 NSRP 的 IP 跟踪；无论是根级跟踪，还是 vsys 级跟踪。

被跟踪的 IP 地址不必与接口在同一个子网上。对于每个被跟踪的 IP 地址，可指定以下信息：

- ping 发送到指定 IP 地址的时间间隔，以秒为单位。
- 经过多少次连续失败的 ping 尝试后认为到指定 IP 地址的连接失败。
- 失败 IP 连接的权重 (所有失败 IP 连接的权重之和一旦超过指定临界值，与接口相关联的路由就会被禁用)。

也可以配置 NetScreen 设备跟踪接口的缺省网关。此选项对于该接口的 PPPoE 或 DHCP 连接特别有用。注意：当配置供 NetScreen 设备跟踪 IP 地址时，NetScreen 设备不会将该 IP 地址的主机路由添加到路由表中。

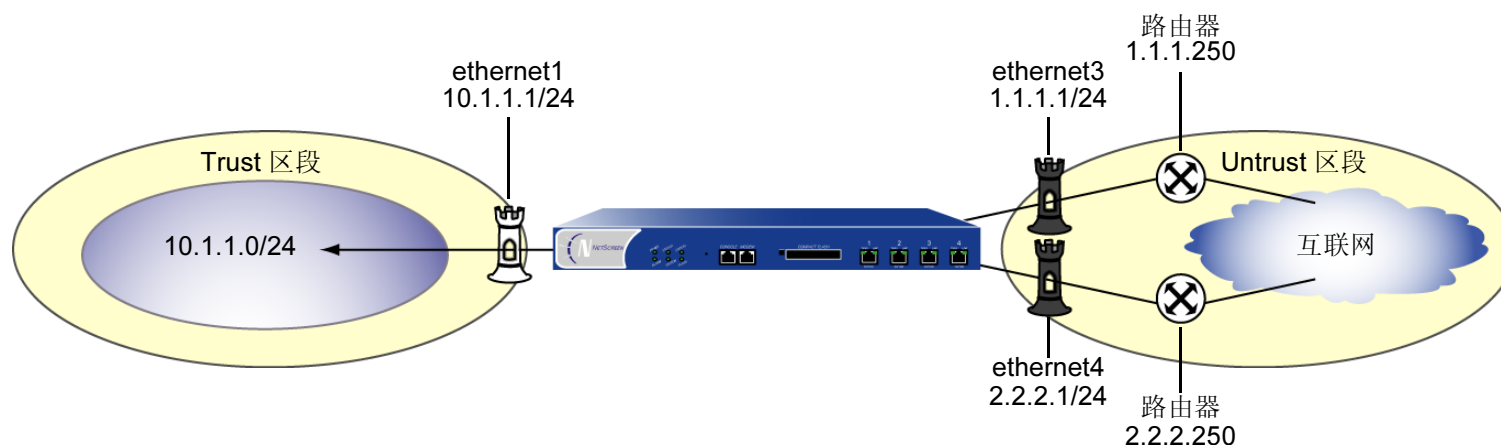
在配置跟踪 IP 地址时有两种类型的临界值：

- 特定被跟踪 IP 地址的失败临界值 — 引发特定 IP 地址发出 ping 响应的连续失败次数，超过此临界值则构成一次到达 IP 地址的失败尝试。不超过临界值表示可以接受该地址的连通性；超过临界值则表示不可以接受。可以将每个 IP 地址的此临界值设置为 1 到 200 之间的任意值，缺省值为 3。
- 接口上的 IP 跟踪的失败临界值 — 到达接口上 IP 地址的累积失败尝试的总权重值，超过此临界值则导致与接口相关联的路由被禁用。可以将此临界值设置为 1 — 255 之间的任意值。缺省值为 1，这就是说，到达任何已配置的被跟踪 IP 地址的一次失败会导致与接口相关联的路由被禁用。

通过在被跟踪 IP 地址上应用权重或权值，可以调整该地址连通性的重要程度（与其它被跟踪 IP 地址相比）。可以将较大的权重分配给相对重要的地址，将较小的权重分配给相对次要的地址。注意，仅当达到特定被跟踪 IP 地址的失败临界值时，分配的权重才会起作用。例如，如果一个接口上的 IP 跟踪的失败临界值是 3，权重为 3 的一个被跟踪 IP 地址的失败就达到该接口上 IP 跟踪的失败临界值，从而导致与接口相关联的路由被禁用。权重为 1 的一个被跟踪 IP 地址的失败没有达到该接口上 IP 跟踪的失败临界值，因而与接口相关联的路由仍然处于活动状态。

范例：配置接口 IP 跟踪

在下例中，接口 **ethernet1** 绑定到 **Trust** 区段并分配到网络地址 **10.1.1.1/24**。接口 **ethernet3** 和 **ethernet4** 绑定到 **Untrust** 区段。接口 **ethernet3** 分配到网络地址 **1.1.1.1/24**，并与位于 **1.1.1.250** 的路由连接。接口 **ethernet4** 分配到网络地址 **2.2.2.1/24**，并与位于 **2.2.2.250** 的路由连接。



有两个已配置的缺省路由：一个路由将 **ethernet3** 用作出站接口，将路由器地址 **1.1.1.250** 作为网关；另一个路由将 **ethernet4** 用作出站接口，将路由器地址 **2.2.2.250** 作为网关，并用度量值 **10** 进行配置。使用 **ethernet3** 的缺省路由是首选路由，因为它的度量值较低（静态路由的缺省度量值是 **1**）。命令 **get route** 的下列输出内容显示 **trust-vr** 的四个活动路由（活动路由用 ***** 表示）。经过 **ethernet3** 的缺省路由处于活动状态，而经过 **ethernet4** 的缺省路由处于非活动状态，因为它的优先级低。

```
ns-> get route
untrust-vr (0 entries)
-----
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
-----
```

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	4	0.0.0.0/0	eth3	1.1.1.250	S	20	1	Root
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	Root
	3	0.0.0.0/0	eth4	2.2.2.250	S	20	10	Root
*	6	2.2.2.0/24	eth4	0.0.0.0	C	0	1	Root
*	5	10.1.1.0/24	eth1	0.0.0.0	C	20	1	Root

如果经过 **ethernet3** 的路由变为不可用，则经过 **ethernet4** 的缺省路由会变为活动路由。启用并配置 **ethernet3** 接口上的 IP 跟踪监控路由器地址 **1.1.1.250**。如果 IP 跟踪不能到达 **1.1.1.250**，**NetScreen** 设备上与 **ethernet3** 接口相关的所有路由变为非活动路由。因此，经过 **ethernet4** 的缺省路由变为活动路由。当 IP 跟踪能够重新到达 **1.1.1.250** 时，经过 **ethernet3** 的缺省路由变为活动路由，同时，经过 **ethernet4** 的缺省路由变为非活动路由，因为它的优先级低于经过 **ethernet3** 的缺省路由。

以下操作启用接口失败临界值为 **5** 的 IP 跟踪并配置 **ethernet3** 接口上的 IP 跟踪，监控路由 IP 地址 **1.1.1.250** (其权重为 **10**)。

WebUI

Network > Interfaces > Edit (对于 ethernet3) > Track IP Options: 输入以下内容, 然后单击 **Apply**:

Enable Track IP: (选择)

Threshold: 5

> Track IP: 输入以下内容, 然后单击 **Add**:

Static: (选择)

Track IP: 1.1.1.250

Weight: 10

CLI

```
set interface ethernet3 track-ip
set interface ethernet3 track-ip threshold 5
set interface ethernet3 track-ip ip 1.1.1.250 weight 10
save
```

在范例中, 目标地址的失败临界值设为缺省值 3。即, 如果目标不响应三次连续 ping, 将对接口上 IP 跟踪的失败临界值应用权重 10。由于接口上 IP 跟踪的失败临界值是 5, 权重 10 会导致 NetScreen 设备上与该接口相关联的路由被禁用。

可以通过发出 CLI 命令 **get interface ethernet3 track-ip** 来检查接口上 IP 跟踪的状态, 如下所示:

```
ns-> get interface ethernet3 track-ip
ip address interval threshold wei gateway fail-count success-rate
1.1.1.250 1 1 10 0.0.0.0 343 46%
threshold: 5, failed: 1 ip(s) failed, weighted sum = 10
```

get route 命令显示经过 **ethernet4** 的缺省路由现在处于活动状态，而经过 **ethernet3** 的所有路由不再处于活动状态。

```
ns-> get route
untrust-vr (0 entries)
-----
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
-----
```

ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
4	0.0.0.0/0	eth3	1.1.1.250	S	20	1	Root
2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	Root
* 3	0.0.0.0/0	eth4	2.2.2.250	S	20	10	Root
* 6	2.2.2.0/24	eth4	0.0.0.0	C	0	1	Root
* 5	10.1.1.0/24	eth1	0.0.0.0	C	20	1	Root

注意，即使经过 **ethernet3** 的路由不再处于活动状态，IP 跟踪仍然继续使用与 **ethernet3** 相关联的路由向目标 IP 地址发送 **ping** 请求。当 IP 跟踪能够重新到达 **1.1.1.250** 时，NetScreen 设备上经过 **ethernet3** 接口的缺省路由重新变为活动路由。同时，经过 **ethernet4** 的缺省路由变为非活动路由，因为它的优先级低于经过 **ethernet3** 的缺省路由。

创建子接口

可在根系统或虚拟系统中的任何物理接口⁶上创建子接口。子接口使用 **VLAN** 标记区别绑定到该子接口的信息流与绑定到其它接口的信息流。请注意虽然子接口源自物理接口，并借用其需要的带宽，但是可将子接口绑定到任何区段，不必绑定到其“父级”接口绑定到的区段。此外，子接口的 **IP** 地址必须在不同于所有其它物理接口和子接口的 **IP** 地址的子网中。

范例：根系统中的子接口

在本例中，将在根系统中为 **Trust** 区段创建子接口。配置绑定到 **Trust** 区段的 **ethernet1** 的子接口，将子接口绑定到用户定义的区段，名为“**accounting**”（在 **trust-vr** 中）。为其分配子接口 ID 3、IP 地址 **10.2.1.1/24** 和 **VLAN** 标记 ID 3。接口模式为 **NAT**。

WebUI

Network > Interfaces > New Sub-IF: 输入以下内容，然后单击 **OK**:

Interface Name: ethernet1.3

Zone Name: accounting

IP Address/Netmask: 10.2.1.1/24

VLAN Tag: 3

CLI

```
set interface ethernet1.3 zone accounting
set interface ethernet1.3 ip 10.2.1.1/24 tag 3
save
```

6. 还可配置冗余子接口和 **VSI** 上的子接口。有关配置冗余接口上子接口的范例，请参阅第 **8-108** 页上的“虚拟系统故障切换”。

删除子接口

不能立即删除映射 IP 地址 (MIP)、虚拟 IP 地址 (VIP) 或 “动态 IP” (DIP) 地址池的宿主子接口。删除任何这些地址的宿主子接口前，必须首先删除所有引用它们的策略或 IKE 网关。然后必须删除子接口上的 MIP、VIP 和 DIP 池。

范例：删除安全区接口

在本例中，将删除子接口 `ethernet1:1`。

WebUI

Network > Interfaces: 单击 **Remove** (对于 `ethernet1:1`)。

会出现一条系统消息，提示您确认移除。

单击 **Yes** 删除子接口。

CLI

```
unset interface ethernet1:1
save
```

二级 IP 地址

每个 NetScreen 接口都有一个唯一的主 IP 地址，但是，某些情况要求一个接口有多个 IP 地址。例如，机构可能分配额外的 IP 地址，但不希望添加路由器来适应其需要。此外，机构拥有的网络设备可能比其子网所能处理的多，如有多于 254 台的主机连接到 LAN。要解决这样的问题，可将二级 IP 地址添加到 Trust、DMZ 或用户定义区段中的接口。

注意：不能为 Untrust 区段中的接口设置多个二级 IP 地址。

二级 IP 地址属性

二级地址具有某些属性，这些属性会影响如何实施此类地址。这些属性如下：

- 任何两个二级 IP 地址之间不能有子网地址重迭。此外，NetScreen 设备上二级 IP 和任何现有子网间不能有子网地址重迭。
- 通过二级 IP 地址管理 NetScreen 设备时，该地址总是具有与主 IP 地址相同的管理属性。因此，不能为二级 IP 地址指定独立的管理配置。
- 不能为二级 IP 地址配置网关。
- 创建新的二级 IP 地址时，NetScreen 设备会自动创建相应的路由选择表条目。删除二级 IP 地址时，设备会自动删除其路由选择表条目。

启用或禁用两个二级 IP 地址之间的路由选择不会使路由选择表发生改变。例如，如果禁用两个此类地址之间的路由选择，NetScreen 设备会丢弃从一个接口到另一个接口的任何封包，但是路由选择表没有改变。

范例：创建二级 IP 地址

在本例中，为 **ethernet1** 设置一个二级 IP 地址 — 192.168.2.1/24，接口 **ethernet1** 的 IP 地址为 10.1.1.1/24 并且绑定到 **Trust** 区段。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > Secondary IP: 输入以下内容，然后单击 **Add**:
IP Address/Netmask: 192.168.2.1/24

CLI

```
set interface ethernet1 ip 192.168.2.1/24 secondary
save
```

回传接口

回传接口是一个逻辑接口，它模拟 NetScreen 设备上的物理接口。然而，与物理接口不同的是，只要其所在的设备开启，该接口始终处于工作中状态。回传接口的名称为 `loopback.id_num`，其中 `id_num` 是大于或等于 1^7 的数字，表示设备上唯一的回传接口。与物理接口相似，必须给回传接口分配 IP 地址，并将其绑定到安全区。

定义回传接口后，即可定义其它接口作为其组的成员。如果信息流通过其组的一个接口到达，则可达到回传接口。任何接口类型都可以是回传接口组的成员 — 物理接口、子接口、通道接口、冗余接口或 VSI。

范例：创建回传接口

在下例中，将创建回传接口 `loopback.1`，将其绑定到 Untrust 区段并为其分配 IP 地址 `1.1.1.27/24`。

WebUI

Network > Interfaces > New Loopback IF: 输入以下内容，然后单击 **OK**:

Interface Name: `loopback.1`

Zone: Untrust (选择)

IP Address/Netmask: `1.1.1.27./24`

CLI

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.1.27
save
```

注意：无法从网络或驻留在其它区段中的主机直接访问回传接口。必须定义策略，以允许进出接口的信息流。

7. 可以指定的最大 `id_num` 值根据平台而定。

使用回传接口

采用和物理接口相同的多种方式，可以使用回传接口。本节说明如何配置回传接口的范例。

注意：不能将回传接口绑定到 HA 区段，也不能为第 2 层操作配置回传接口，或者将回传接口配置为冗余 / 聚合接口。不能配置回传接口的以下功能：NTP、DNS、VIP、二级 IP、跟踪 IP 或 Webauth。

可以定义回传接口上的 MIP。这样，接口组就可访问 MIP，此功能为回传接口所特有。有关使用带有 MIP 的回传接口的信息，请参阅第 362 页上的“MIP 和回传接口”。

使用回传接口的 IP 地址或分配给回传接口的管理 IP 地址，可以管理 NetScreen 设备。

范例：用于管理的回传接口

在下例中，将先前定义的 loopback.1 接口配置为设备的管理接口。

WebUI

Network > Interfaces > loopback.1 > Edit: 选择所有管理选项，然后单击 **OK**。

CLI

```
set interface loopback.1 manage
save
```

范例：回传接口上的 BGP

回传接口支持 NetScreen 设备上的 BGP 动态路由选择协议。在下例中，将启用 loopback.1 接口上的 BGP。

注意：要启用回传接口上的 BGP，必须首先为想要在其中绑定接口的虚拟路由器创建一个 BGP 实例。关于配置 NetScreen 设备上的 BGP 的信息，请参阅第 6 卷，“动态路由”。

WebUI

Network > Interfaces > loopback.1 > Edit: 选择 **Protocol BGP**，然后单击 **OK**。

CLI

```
set interface loopback.1 protocol bgp
save
```

范例：回传接口上的 VSI

可以在回传接口上为 NSRP 配置“虚拟安全接口 (VSI)”。回传接口上的 VSI 物理状态始终为工作中。接口可以是活动或非活动状态，具体取决于该接口所属的 VSD 组的状态。

WebUI

Network > Interfaces > New VSI IF: 输入以下内容，然后单击 **OK**:

Interface Name: VSI Base: loopback.1

VSD Group: 1

IP Address/Netmask: 1.1.1.1/24

CLI

```
set interface loopback.1: 1 ip 1.1.1.1/24
save
```

范例：回传接口作为源接口

可以使用回传接口作为来自 **NetScreen** 设备的某信息流的源接口。(定义应用程序的源接口后，即可使用指定的源接口地址与外部设备进行通信，而不是使用出站接口地址。) 在下例中，将指定 **NetScreen** 设备使用先前定义的 **loopback.1** 接口发送系统日志封包。

WebUI

Configuration > Report Settings > Syslog: 输入以下内容，然后单击 **Apply**:

Enable Syslog Messages: (选择)

Source Interface: loopback.1 (选择)

Syslog Servers:

No.: 1 (选择)

IP/Hostname: 10.1.1.1

Traffic Log: (选择)

Event Log: (选择)

CLI

```
set syslog config 10.1.1.1 log all
set syslog src-interface loopback.1
set syslog enable
save
```


接口模式

接口能以三种不同模式运行，分别是：网络地址转换 (NAT)、路由和透明。如果绑定到第 3 层区段的接口具有 IP 地址，则可为该接口定义 NAT¹ 或路由操作模式。绑定到第 2 层区段 (如预定义的 v1-trust、v1-untrust 和 v1-dmz，或用户定义的第 2 层区段) 的接口必须为透明模式。在配置接口时选择操作模式。

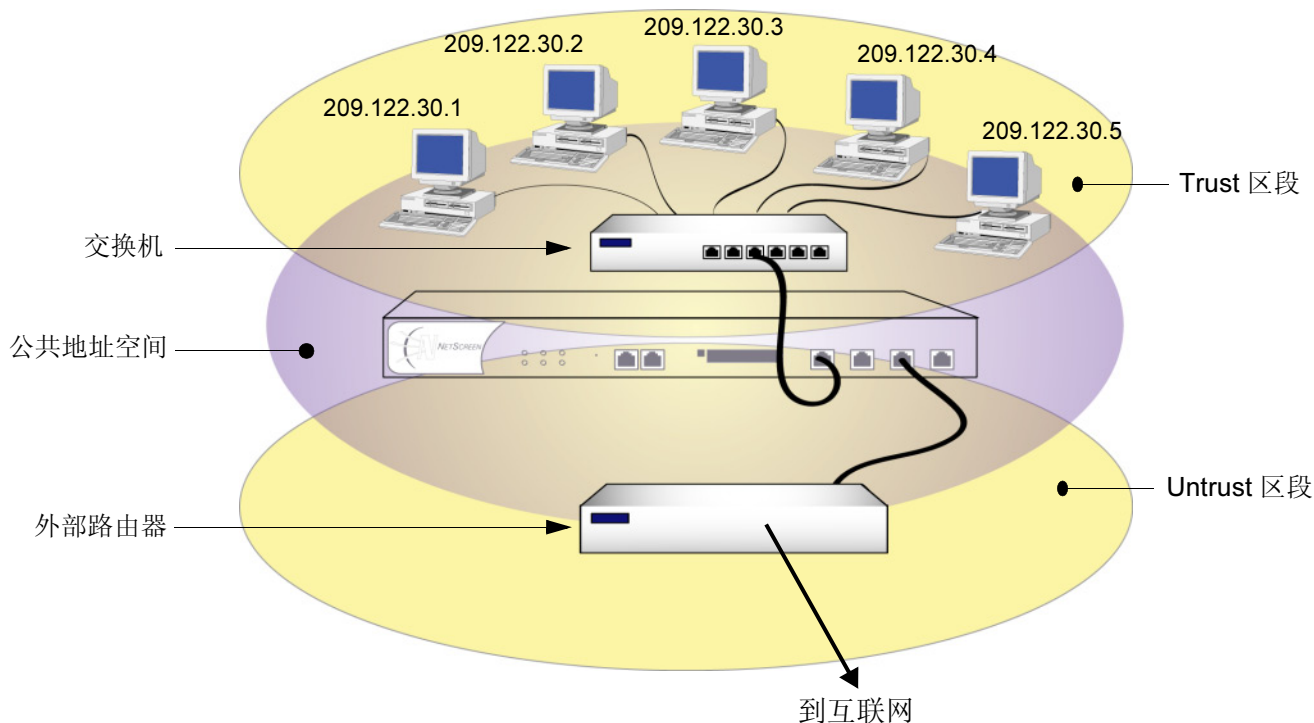
本章包括以下部分：

- 第 108 页上的“透明模式”
 - 第 109 页上的“区段设置”
 - 第 110 页上的“信息流转发”
 - 第 111 页上的“未知 Unicast 选项”
- 第 126 页上的“NAT 模式”
 - 第 128 页上的“入站和出站 NAT 信息流”
 - 第 129 页上的“接口设置”
- 第 134 页上的“路由模式”
 - 第 135 页上的“接口设置”

1. 尽管可以将绑定到任意第 3 层区段的接口的操作模式定义为 NAT，但是，NetScreen 设备只对通过该接口传递到 Untrust 区段的信息流执行 NAT。对于通往 Untrust 区段之外的其它任意区段的信息流，NetScreen 不执行 NAT。还要注意，NetScreen 允许您将 Untrust 区段接口设置为 NAT 模式，但是这样做并不会激活任何 NAT 操作。

透明模式

接口为透明模式时，**NetScreen** 设备过滤通过防火墙的封包，而不会修改 IP 封包包头中的任何源或目的地信息。所有接口运行起来都像是同一网络中的一部分，而 **NetScreen** 设备的作用更像是第 2 层交换机或桥接器。在透明模式下，接口的 IP 地址被设置为 0.0.0.0，使得 **NetScreen** 设备对于用户来说是可视或“透明”的。



透明模式是一种保护 **Web** 服务器，或者主要从不可信源接收信息流的其它任意类型服务器的方便手段。使用透明模式有以下优点：

- 不需要重新配置路由器或受保护服务器的 IP 地址设置
- 不需要为到达受保护服务器的内向信息流创建映射或虚拟 IP 地址

区段设置

在缺省情况下，ScreenOS 会创建一个功能区段、VLAN 区段和三个第 2 层安全区：V1-Trust、V1-Untrust 和 V1-DMZ。

VLAN 区段

VLAN 区段是 VLAN1 接口的宿主区段，VLAN1 接口具有与物理接口相同的配置和管理能力。NetScreen 设备处于透明模式时，使用 VLAN1 接口来管理设备和终止 VPN 信息流。可将 VLAN1 接口配置为允许第 2 层安全区中的主机来管理设备。为此，必须将 VLAN1 接口的 IP 地址设置为与第 2 层安全区中的主机在同一子网中。

对于管理信息流，VLAN1 管理 IP 优先于 VLAN1 接口 IP。可为管理信息流设置“VLAN1 管理 IP”，并将 VLAN1 接口 IP 专用于 VPN 通道终端。

预定义的第 2 层区段

在缺省情况下，ScreenOS 提供三个第 2 层安全区，分别是：V1-Trust、V1-Untrust 和 V1-DMZ。这三个区段共享同一个第 2 层域。在其中一个区段中配置接口时，它被添加到由所有第 2 层区段中的所有接口共享的第 2 层域中。第 2 层区段中的所有主机必须在同一子网上以进行通信。

如上一节所述，设备处于透明模式时，用户使用 VLAN1 接口管理设备。对于要到达 VLAN1 接口的管理信息流，必须启用 VLAN1 接口和管理信息流通过的区段上的管理选项。在缺省情况下，启用 V1-Trust 区段中的所有管理选项。要在其它区段中启用主机以管理设备，必须设置它们所属的区段上的那些选项。

注意：要了解哪个物理接口被预先绑定到每个 NetScreen 平台的第 2 层区段，请参阅该平台的安装程序指南。

信息流转发

在第 2 层 (L2) 工作的 NetScreen 设备不允许区段间的任何信息流，除非在该设备上配置了相应的策略。有关如何设置策略的详细信息，请参阅第 213 页上的“策略”。在 NetScreen 设备上配置了策略后，该策略执行以下任务：

- 允许或拒绝策略中指定的信息流
- 允许 ARP 和第 2 层非 IP 多点传送并广播信息流。然后，NetScreen 设备可以接收和通过生成树协议的第 2 层广播信息流。
- 继续阻止所有非 IP 和非 ARP 单点传送信息流及 IPSec 信息流

可以按如下所述更改设备的转发行为：

- 要阻止所有第 2 层非 IP 和非 ARP 信息流，包括多点传送和广播信息流，请输入 **unset interface vlan1 bypass-non-ip-all** 命令。
- 要允许所有第 2 层非 IP 信息流通过设备，请输入 **set interface vlan1 bypass-non-ip** 命令。
- 要恢复设备的缺省行为 (阻止所有非 IP 和非 ARP 单点传送信息流)，请输入 **unset interface vlan1-bypass-non-ip** 命令。
 - 请注意，这两种命令都在配置文件中时，**unset interface vlan1 bypass-non-ip-all** 命令始终覆盖 **unset interface vlan1 bypass-non-ip** 命令。因此，如果先前已经输入 **unset interface vlan1 bypass-non-ip-all** 命令，而现在希望设备恢复其缺省行为 (仅阻止非 IP 和非 ARP 单点传送信息流)，则应该首先输入 **set interface vlan1 bypass-non-ip** 命令以允许所有非 IP 信息流通过设备。然后，必须输入 **unset interface vlan1-bypass-non-ip** 命令以仅阻止非 IP、非 ARP 单点传送信息流。
- 要允许 NetScreen 设备通过 IPSec 信息流而不试图终止它，请使用 **set interface vlan1 bypass-others-ipsec** 命令。然后，NetScreen 设备允许 IPSec 信息流通过以到达其它 VPN 终止点。

注意：具有处于透明模式接口的 NetScreen 设备需有路由，其用途有两个：引导自行生成的信息流 (如 SNMP 陷阱) 及封装或解封 VPN 信息流后进行转发。

未知 Unicast 选项

当主机或任意类型的网络设备不知道与其它设备的 IP 地址相关的 MAC 地址时，将使用“地址解析协议 (ARP)”来获得该地址。请求方将 ARP 查询 (arp-q) 广播到同一子网中的所有其它设备。arp-q 请求指定目的地 IP 地址处的设备发回 ARP 回复 (arp-r)，为请求方提供回复方的 MAC 地址。子网中的所有其它设备收到 arp-q 时，会检查目的地 IP 地址，并且由于它不是它们的 IP 地址而将该封包丢弃。只有具有指定 IP 地址的设备才返回 arp 回复。设备将 IP 地址与 MAC 地址相匹配后，将信息存储在其 ARP 高速缓存中。

ARP 信息流通过透明模式下的 NetScreen 设备时，设备记录每个封包中的源 MAC 地址，并且可以获知哪个接口通向该 MAC 地址。实际上，NetScreen 设备通过记录收到的所有封包中的源 MAC 地址，来了解哪个接口通向哪个 MAC 地址。然后将此信息存储在其转发表中。

注意：透明模式下的 NetScreen 设备不允许区段间的任何信息流，除非在该设备上配置了策略。有关透明模式下的设备如何转发信息流的详细信息，请参阅第 110 页上的“信息流转发”。

当设备发送带有目的地 MAC 地址的 unicast 封包 (地址在其 ARP 高速缓存中), 但 NetScreen 设备的转发表中没有该地址时, 会出现这种情况。例如, NetScreen 设备每次重新启动时, 都清除其发送表。(也可用 CLI 命令 **clear arp** 来清除转发表。) 透明模式下的 NetScreen 设备收到在其转发表中没有其条目的 unicast 封包时, 可执行以下两个过程之一:

- 执行策略查找来确定允许接收来自源地址的信息流的区段后, 将初始封包大量发送出绑定到这些区段的接口, 然后使用收到回复的任意接口继续。这就是缺省启用的 **Flood** 选项。
- 丢弃初始封包, 将 ARP 查询 (和 / 或 trace-route 封包, 活动时间值设置为 1 的 ICMP 回应请求) 大量发送出所有接口 (封包已到达的接口除外), 然后通过从路由器或主机 (其 MAC 地址与初始封包中的目的地 MAC 地址匹配) 收到 ARP (或 trace-route) 回复的任意接口发送后续封包。目的地 IP 地址在非邻近子网中时, trace-route 选项允许 NetScreen 设备发现目的地 MAC 地址。

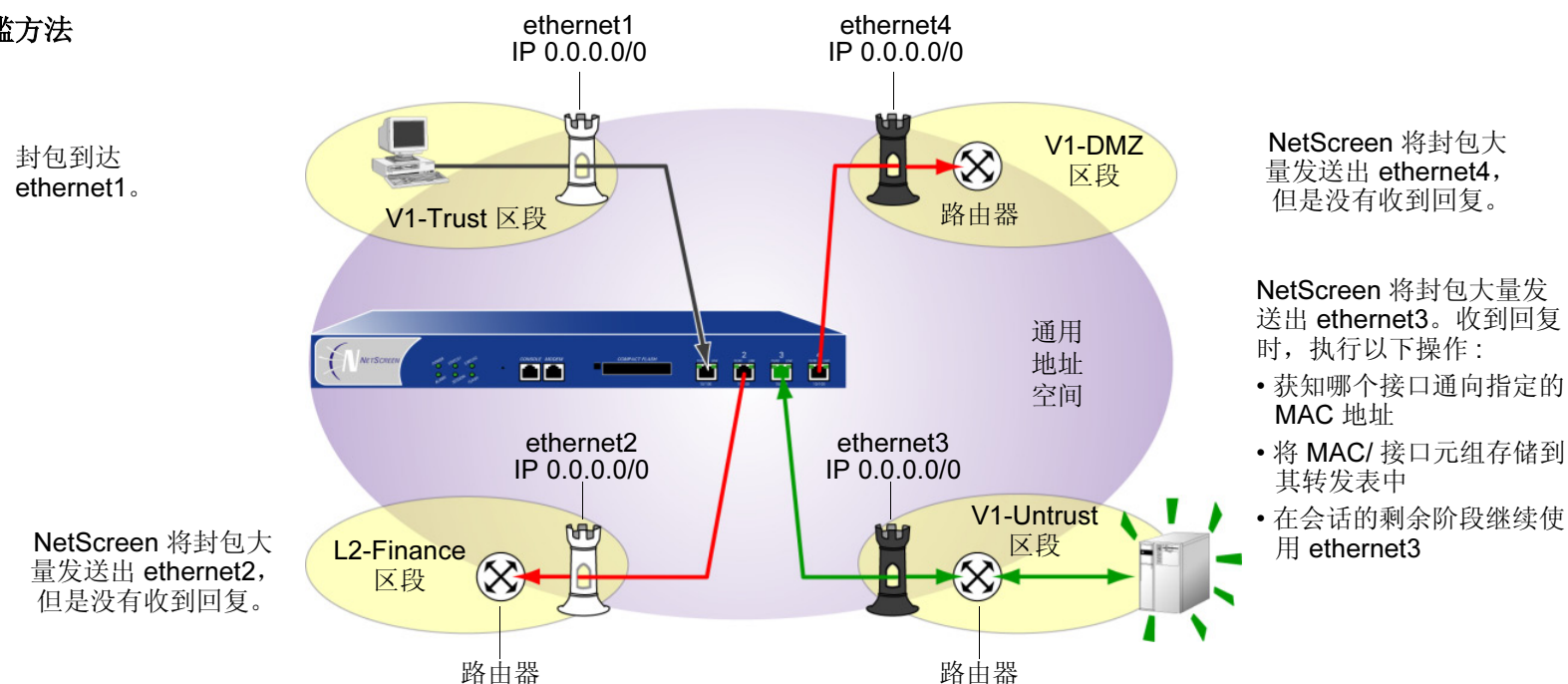
注意: 泛滥和 ARP/trace-route 这两种方法中, ARP/trace-route 更安全, 因为 NetScreen 设备将 ARP 查询和 trace-route 封包 (而非初始封包) 大量发送出所有接口。

泛滥方法

泛滥方法用与多数第 2 层交换机相同的方式发送封包。交换机维护转发表, 它包含 MAC 地址和每个第 2 层域的相关端口。该表还包含相应的接口, 通过该接口, 交换机能将信息流转发到每个设备。每次在其帧包头中带有新的源 MAC 地址的封包到达时, 交换机都会将该 MAC 地址添加到其转发表中。它还跟踪封包到达的接口。如果交换机不知道目的地 MAC 地址, 交换机将复制封包并将其大量发送出所有接口 (封包到达的接口除外)。当带有那个 MAC 地址的回复到达这些接口之一时, 它即获知先前未知的 MAC 地址及其相应接口。

启用泛滥方法后, 当 NetScreen 设备收到目的地 MAC 地址未在 NetScreen 设备 MAC 表中列出的以太网帧时, 它将该封包大量发送出所有接口。

泛滥方法



要启用泛滥方法来处理未知的 unicast 封包，请执行以下操作之一：

WebUI

Network > Interface > Edit (对于 VLAN1): 对于广播选项，选择 **Flood**，然后单击 **OK**。

CLI

```
set interface vlan1 broadcast flood
save
```


ARP/Trace-Route 方法

启用带有 `trace-route` 选项² 的 ARP 方法后，如果 NetScreen 设备收到目的地 MAC 地址未在其 MAC 表中列出的以太网帧时，NetScreen 设备执行以下系列操作：

1. NetScreen 设备记录初始封包中的目的地 MAC 地址（而且，如果转发表中没有此地址，则将源 MAC 地址及其相应的接口添加到其转发表中）。
2. NetScreen 设备丢弃初始封包。
3. NetScreen 设备生成两个封包 —ARP 查询 (`arp-q`) 和活动时间 (TTL) 字段为 1 的 `trace-route` (ICMP 回应请求或 PING)，并将这些封包大量发送出所有接口，初始封包到达的接口除外。对于 `arp-q` 封包和 ICMP 回应请求，NetScreen 设备使用初始封包的源和目的地 IP 地址。对于 `arp-q` 封包，NetScreen 设备用 VLAN1 的 MAC 地址替换初始封包的源 MAC 地址，用 `ffff.ffff.ffff` 替换初始封包的目的地 MAC 地址。对于 `trace-route` 选项，NetScreen 设备在其广播的 ICMP 回应请求中使用初始封包的源和目的地 MAC 地址。

如果目的地 IP 地址属于与入口 IP 地址³ 在同一子网中的设备，则主机返回一条带有其 MAC 地址的 ARP 回复 (`arp-r`)，从而指示出 NetScreen 设备必须通过它转发以该地址为目的地的信息流的接口。（请参阅第 116 页上的“ARP 方法”。）

如果目的地 IP 地址属于入口 IP 地址所在子网外的其它子网中的设备，则 `trace-route` 返回通向目的地⁴ 的路由器的 IP 和 MAC 地址，尤其重要的是，指出了 NetScreen 设备必须通过它转发流向该 MAC 地址的信息流的接口。（请参阅第 117 页上的“Trace-Route”。）

-
2. 启用 ARP 方法时，在缺省情况下 `trace-route` 选项启用。也可启用不带 `trace-route` 选项的 ARP 方法。但是，如果目的地 IP 地址与入口 IP 地址在同一子网中，则该方法只允许 NetScreen 设备发现 `unicast` 封包的目的地 MAC 地址。（关于入口 IP 地址的详细信息，请参阅下一脚注。）
 3. 入口 IP 地址指将封包发送到 NetScreen 设备的最后设备的 IP 地址。此设备可能是发送封包的源，或者是转发封包的路由器。
 4. 实际上，`trace-route` 返回子网中所有路由器的 IP 和 MAC 地址。NetScreen 设备于是将初始封包的目的地 MAC 地址与 `arp-r` 封包中的源 MAC 地址相匹配，来确定指向哪个路由器，并进而确定使用哪个接口到达该目的地。

4. NetScreen 设备将从初始封包中收集的目的地 MAC 地址与通向该 MAC 地址的接口相结合，添加新的条目到其转发表中。
5. NetScreen 设备将其收到的所有后续封包转发出正确接口，到达目的地。

要启用 ARP/trace-route 方法来处理未知的 unicast 封包，请执行以下操作之一：

WebUI

Network > Interface > Edit (对于 VLAN1): 对于广播选项，选择 **ARP**，然后单击 **OK**。

CLI

```
set interface vlan1 broadcast arp
save
```

注意：trace-route 选项缺省启用。如果要使用不带 trace-route 选项的 ARP，请输入以下命令：**unset interface vlan1 broadcast arp trace-route**。此命令取消设置 trace-route 选项，但是不取消将 ARP 作为处理未知 unicast 封包的方法的设置。

下图显示了目的地 IP 地址在邻近的子网中时，ARP 方法如何查找目的地 MAC。

ARP 方法

注意：以下仅显示封包包头的相关元素和 MAC 地址中的最后四位数字。

如果下列封包

以太网帧		IP 数据报			
目的地	源	类型	源	目的地	
11bb	11aa	0800	210.1.1.5	210.1.1.75	

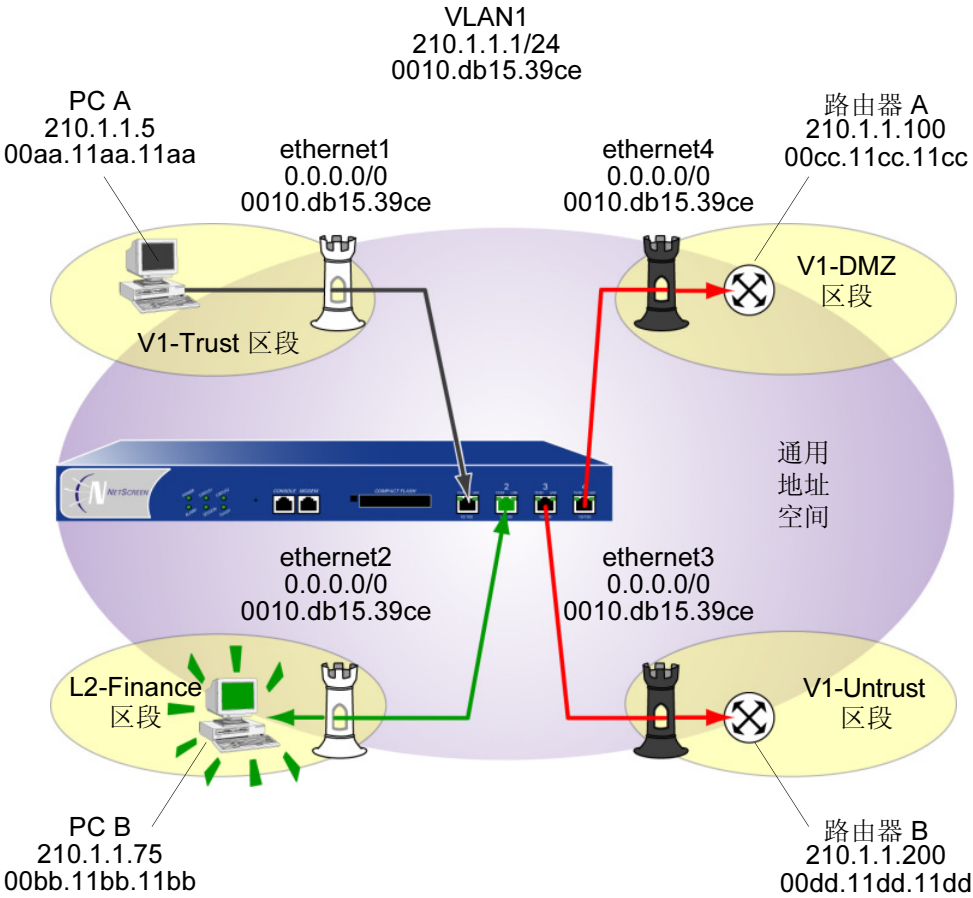
到达 ethernet1，并且转发表中没有 MAC 地址 00bb.11bb.11bb 的条目，NetScreen 设备将以下 arp-q 封包大量发送出 eth2、eth3 和 eth4。

以太网帧		ARP 消息			
目的地	源	类型	源	目的地	
ffff	39ce	0806	210.1.1.5	210.1.1.75	

当 NetScreen 设备在 eth2 收到以下 arp-r 时，

以太网帧		ARP 消息			
目的地	源	类型	源	目的地	
39ce	11bb	0806	210.1.1.75	210.1.1.5	

它现在能将 MAC 地址与通向该地址的接口相关联。



下图显示了目的地 IP 地址在非邻近的子网中时， trace-route 选项如何查找目的地 MAC。

Trace-Route

注意：以下仅显示封包包头的相关元素和 MAC 地址中的最后四位数字。

如果下列封包

以太网帧		IP 数据报			
目的地	源	类型	源	目的地	
11dd	11aa	0800	210.1.1.5	195.1.1.5	

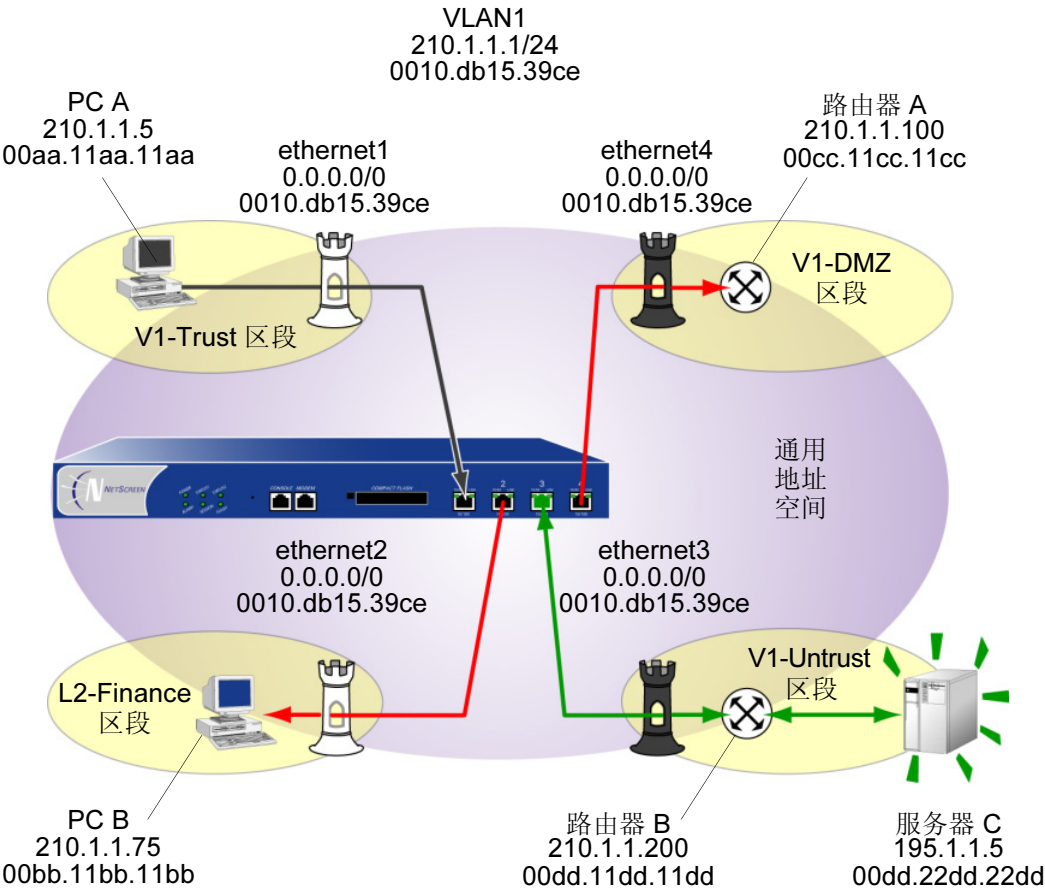
到达 ethernet1，并且转发表中没有 MAC 地址 00dd.11dd.11dd 的条目，NetScreen 设备将以下 trace-route 封包大量发送出 eth2、eth3 和 eth4。

以太网帧		ICMP 消息			
目的地	源	类型	源	目的地	TTL
11dd	11aa	0800	210.1.1.5	195.1.1.5	1

NetScreen 设备在 eth3 收到以下回应时，

以太网帧		ICMP 消息			
目的地	源	类型	源	目的地	消息
11aa	11dd	0800	210.1.1.200	210.1.1.5	超时

它现在能将 MAC 地址与通向该地址的接口相关联。



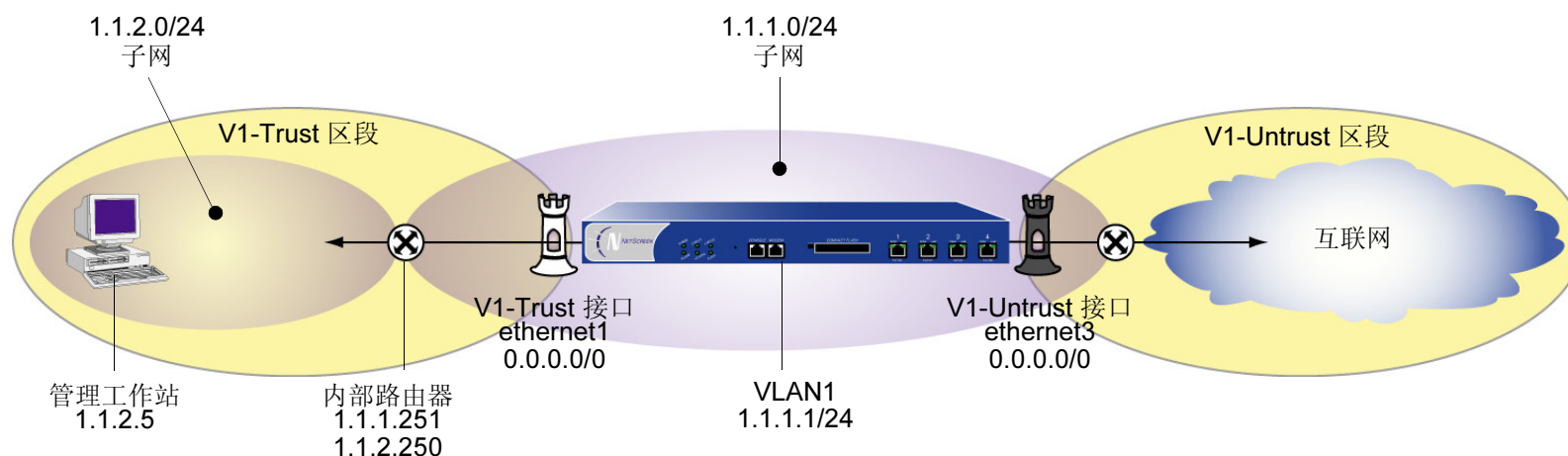
范例：用于管理的 VLAN1 接口

在本例中，将按下述内容配置 NetScreen 设备来管理其 VLAN1 接口：

- 为 VLAN1 接口分配 IP 地址 1.1.1.1/24。
- 在 VLAN1 接口和 V1-Trust⁵ 安全区上启用 Web、Telnet、SSH 和 Ping。

注意：要从第 2 层安全区管理设备，必须在 VLAN1 接口和第 2 层安全区上设置相同的管理选项。

- 在信任虚拟路由器中（所有的 Layer 2（第 2 层）安全区都在 trust-vr 路由选择域中）添加路由，使管理信息流能在 NetScreen 设备和管理工作站（该工作站在 NetScreen 设备的紧邻子网外）之间流动。所有安全区域都在 trust-vr 路由选择域中。



5. 在缺省情况下，NetScreen 启用 VLAN1 接口和 V1-Trust 安全区的管理选项。本例中包括了对这些选项的启用，仅用于说明目的。除非先前已经禁用了它们，否则不需要手动启动。

WebUI

1. VLAN1 接口

Network > Interfaces > Edit (对于 VLAN1): 输入以下内容, 然后单击 **OK**:

IP Address/Netmask: 1.1.1.1/24

Management Services: WebUI, Telnet, SSH (选择)

Other Services: Ping (选择)

2. V1-Trust 区段

Network > Zones > Edit (对于 V1-Trust): 选择以下内容, 然后单击 **OK**:

Management Services: WebUI, Telnet, SSH

Other Services: Ping

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 1.1.2.0/24

Gateway: (选择)

Interface: vlan1(trust-vr)

Gateway IP Address: 1.1.1.251

Metric: 1

CLI

1. VLAN1 接口

```
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ssh
set interface vlan1 manage ping
```

2. V1-Trust 区段

```
set zone v1-trust manage web
set zone v1-trust manage telnet
set zone v1-trust manage ssh
set zone v1-trust manage ping
```

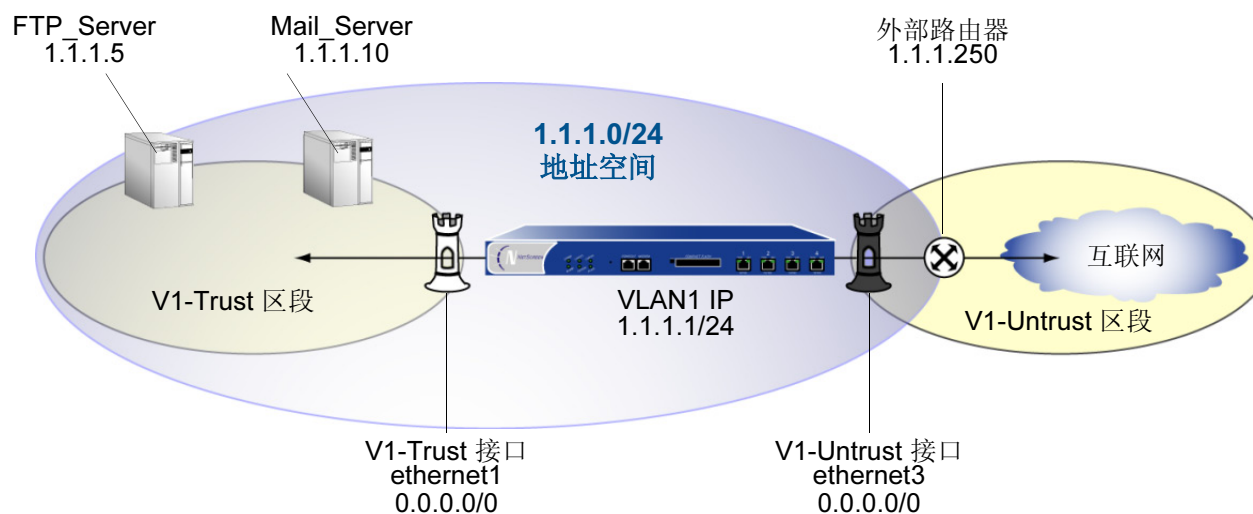
3. 路由

```
set vrouters trust-vr route 1.1.2.0/24 interface vlan1 gateway 1.1.1.251 metric 1
save
```

范例：透明模式

以下范例说明了受处于透明模式的 NetScreen 设备保护的单独 LAN 的基本配置。策略允许 V1-Trust 区段中所有主机的外向信息流、邮件服务器的内向 SMTP 服务，以及 FTP 服务器的内向 FTP-GET 服务。

为了提高管理信息流的安全性，将 WebUI 管理的 HTTP 端口号从 80 改为 5555，将 CLI 管理的 Telnet 端口号从 23 改为 4646。使用 VLAN1 IP 地址 1.1.1.1/24 来管理 V1-Trust 安全区的 NetScreen 设备。定义 FTP 和邮件服务器的地址。也可配置到外部路由器的缺省路由（于 1.1.1.250 处），以便 NetScreen 设备能向其发送出站 VPN 信息流⁶。（V1-Trust 区段中所有主机的缺省网关也是 1.1.1.250。）



6. 关于为接口处于透明模式的 NetScreen 设备配置 VPN 通道的范例，请参阅第 5-186 页上的“透明模式 VPN”。

WebUI

1. VLAN1 接口

Network > Interfaces > Edit (对于 VLAN1 接口): 输入以下内容, 然后单击 **OK**:

IP Address/Netmask: 1.1.1.1/24

Management Services: WebUI, Telnet (选择)

Other Services: Ping (选择)

2. HTTP 端口

Configuration > Admin > Management: 在 HTTP Port 字段中, 键入 5555⁷, 然后单击 **Apply**。

3. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **OK**:

Zone Name: V1-Trust

IP Address/Netmask: 0.0.0.0/0

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: V1-Untrust

IP Address/Netmask: 0.0.0.0/0

4. V1-Trust 区段

Network > Zones > Edit (对于 v1-trust): 选择以下内容, 然后单击 **OK**:

Management Services: WebUI, Telnet

Other Services: Ping

7. 缺省端口号为 80。建议将此号码改为 1024 和 32,767 间的数值, 以阻止对配置的未授权访问。以后登录以管理设备时, 请在 Web 浏览器的 URL 区输入以下内容: http://1.1.1.1: 5555。

5. 地址

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

Address Name: FTP_Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/32

Zone: V1-Trust

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

Address Name: Mail_Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.10/32

Zone: V1-Trust

6. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: vlan1(trust-vr)

Gateway IP Address: 1.1.1.250

Metric: 1

7. 策略

Policies >(From: V1-Trust, To: V1-Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

Policies >(From: V1-Untrust, To: V1-Trust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Mail_Server

Service: Mail

Action: Permit

Policies > (From: V1-Untrust, To: V1-Trust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), FTP_Server

Service: FTP-GET

Action: Permit

CLI

1. VLAN1

```
set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ping
```

2. Telnet

```
set admin telnet port 46468
```

3. 接口

```
set interface ethernet1 ip 0.0.0.0/0
set interface ethernet1 zone vl-trust
set interface ethernet3 ip 0.0.0.0/0
set interface ethernet3 zone vl-untrust
```

4. V1-Trust 区段

```
set zone vl-trust manage web
set zone vl-trust manage telnet
set zone vl-trust manage ping
```

5. 地址

```
set address vl-trust FTP_Server 1.1.1.5/32
set address vl-trust Mail_Server 1.1.1.10/32
```

6. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250 metric 1
```

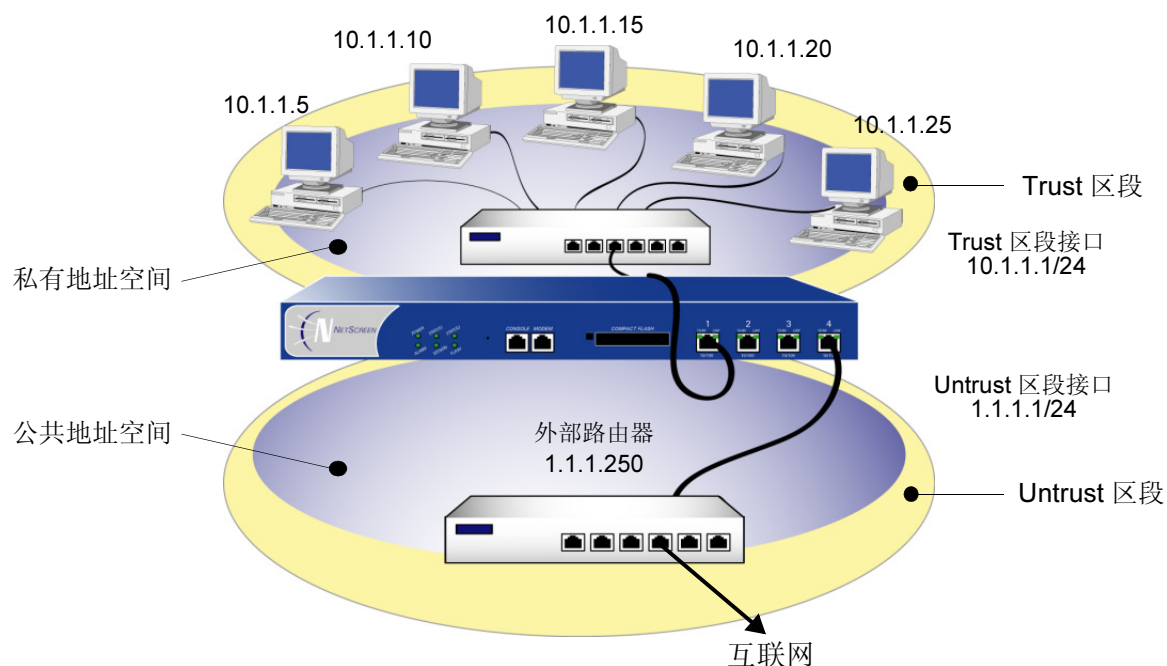
7. 策略

```
set policy from vl-trust to vl-untrust any any any permit
set policy from vl-untrust to vl-trust any Mail_Server mail permit
set policy from vl-untrust to vl-trust any FTP_Server ftp-get permit
save
```

8. Telnet 的缺省端口号为 23。建议将此号码改为介于 1024 和 32,767 间的数值，以阻止对配置的未授权访问。以后登录 Telnet 来管理设备时，输入以下地址：1.1.1.1 4646。

NAT 模式

入口接口处于“网络地址转换 (NAT)”模式下时，NetScreen 设备的作用与第 3 层交换机 (或路由器) 相似，将通往 Untrust 区段的外向 IP 封包包头中的两个组件进行转换：其源 IP 地址和源端口号。NetScreen 设备用 Untrust 区段接口的 IP 地址替换发端主机的源 IP 地址。另外，它用另一个由 NetScreen 设备生成的任意端口号替换源端口号。



当回复封包到达 NetScreen 设备时，该设备转换内向封包的 IP 包头中的两个组件：目的地地址和端口号，它们被转回初始号码。NetScreen 设备于是将封包转发到其目的地。

NAT 添加透明模式中未提供的一个安全级别：通过 NAT 模式下的入口接口（如 Trust 区段接口）发送信息流的主机地址决不对出口区段（如 Untrust 区段）中的主机公开，除非这两个区段在相同的虚拟路由选择域中并且 NetScreen 设备通过动态路由选择协议 (DRP) 向对等方通告路由。尽管这样，如果有策略允许入站信息流到达，也仅仅可到达 Trust 区段地址。（如果希望在使用 DRP 时隐藏 Trust 区段地址，则可将 Untrust 区段放置在 untrust-vr 中，将 Trust 区段放置在 trust-vr 中，并且不将 trust-vr 中外部地址的路由导出到 untrust-vr。）

如果 NetScreen 设备使用静态路由选择并且仅有一个虚拟路由器，由于基于接口的 NAT，内部地址在信息流出站时保持隐藏。配置的策略控制入站信息流。如果仅使用映射 IP (MIP) 和虚拟 IP (VIP) 地址作为入站策略中的目的地，则内部地址仍保持隐藏。

另外，NAT 还保留对公共 IP 地址的使用。在许多环境中，资源不可用，不能为网络上的所有设备提供公共 IP 地址。NAT 服务允许多个私有 IP 地址通过一个或几个公共 IP 地址访问互联网资源。以下 IP 地址范围保留给私有 IP 网络，并且不必在互联网上设定路由：

10.0.0.0 – 10.255.255.255

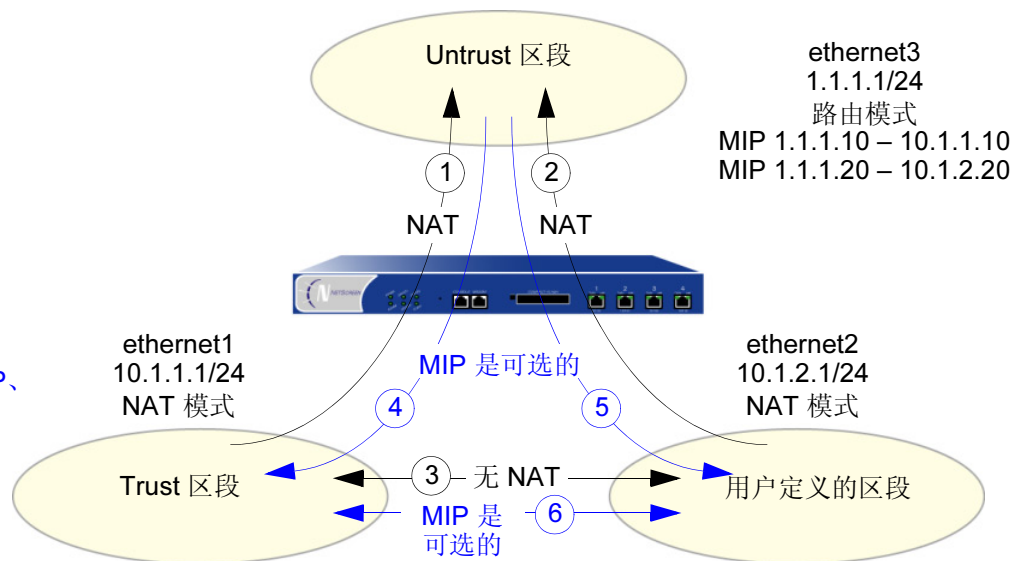
172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

入站和出站 NAT 信息流

通过 NAT 模式下的接口发送信息流的区段内的主机，能够发出流向 Untrust 区段的信息流（假定策略允许）。在 ScreenOS 5.0.0 之前的版本中，NAT 模式下的接口后的主机无法接收 Untrust 区段的信息流，除非为它设置了“映射 IP (MIP)”、“虚拟 IP (VIP)”或 VPN 通道⁹。不过，在 ScreenOS 5.0.0 版本中，从任意区段（包括 Untrust 区段）向拥有已启用 NAT 的接口的区段发送信息流时，不需要使用 MIP、VIP 或 VPN。如果要保护地址的私密性或使用不在公开网络（如互联网）上出现的私有地址，仍可为到达他们的信息流定义 MIP、VIP 或 VPN。不过，如果不关注私密性和私有 IP 地址的问题，则 Untrust 区段的信息流可直接到达 NAT 模式接口后的主机，而不必使用 MIP、VIP 或 VPN。

1. 从 Trust 区段到 Untrust 区段的信息流上的基于接口的 NAT。
2. 从用户定义区段到 Untrust 区段的信息流上的基于接口的 NAT。
(注意：只有用户定义区段和 Untrust 区段在不同的虚拟路由选择域中时，这种情况才有可能发生。)
3. Trust 区段和用户定义区段之间的信息流上**没有**基于接口的 NAT。
- 4 和 5. 可以对从 Untrust 区段到达 Trust 区段或用户定义区段的信息流使用 MIP、VIP 或 VPN，但它们**不是必需的**。
6. Trust 区段和用户定义区段之间的信息流也**不需要**MIP 和 VPN。



注意：有关 MIP 的详细信息，请参阅第 347 页上的“映射 IP 地址”。有关 VIP 的详细信息，请参阅第 372 页上的“虚拟 IP 地址”。

9. 可以仅在绑定到 Untrust 区段的接口上定义虚拟 IP (VIP) 地址。

接口设置

对于 NAT 模式，定义以下接口设置，其中 *ip_addr1* 和 *ip_addr2* 代表 IP 地址中的数字，*mask* 代表网络掩码中的数字，*vlan_id_num* 代表 VLAN 标记的编号，*zone* 代表区段名称，*number* 代表以 kbps 为单位的带宽大小：

区段接口	设置	区段子接口
使用 NAT 的 Trust、DMZ 和用户定义的区段	IP: <i>ip_addr1</i> Netmask: <i>mask</i> Manage IP [*] : <i>ip_addr2</i> Traffic Bandwidth [†] : <i>number</i> NAT [‡] : (选择)	IP: <i>ip_addr1</i> Netmask: <i>mask</i> VLAN Tag: <i>vlan_id_num</i> Zone Name: <i>zone</i> NAT [†] : (选择)
Untrust ^{**}	IP: <i>ip_addr1</i> Netmask: <i>mask</i> Manage IP [*] : <i>ip_addr2</i> Traffic Bandwidth [†] : <i>number</i>	IP: <i>ip_addr1</i> Netmask: <i>mask</i> VLAN Tag: <i>vlan_id_num</i> Zone Name: <i>zone</i>

^{*} 可在每个接口的基础上设置管理 IP 地址。主要目的是为从网络信息流中分离出来的管理信息流提供 IP 地址。当某特定设备具备高可用性配置时，也可使用管理 IP 地址来访问它。

[†] 用于信息流整型的可选设置。

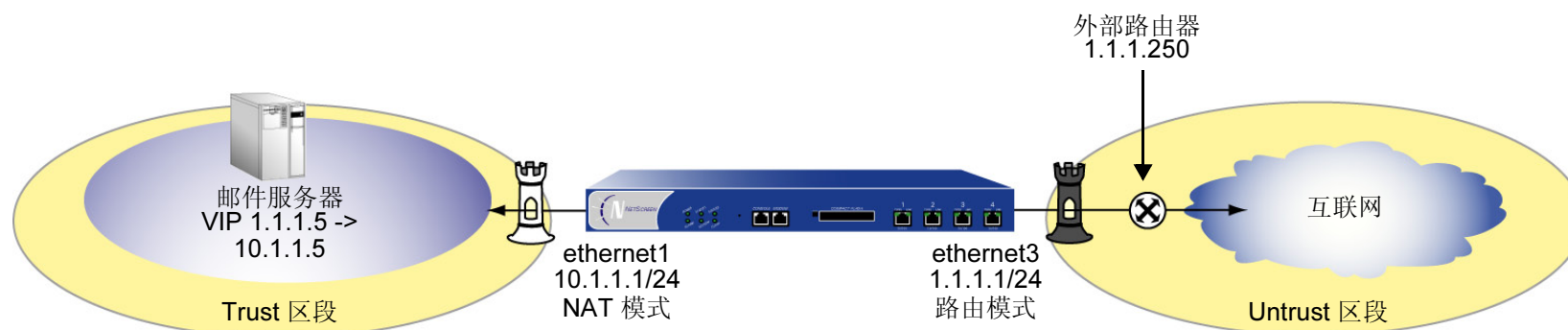
[‡] 选择 NAT 可将接口模式定义为 NAT。选择“路由”可将接口模式定义为“路由”。

^{**} 尽管能选择 NAT 作为绑定到 Untrust 区段的接口模式，但是，NetScreen 设备不在该接口上执行任何 NAT 操作。

范例 : NAT 模式

以下范例说明了 Trust 区段中有单独子网的 LAN 的简单配置。LAN 受 NAT 模式下的 NetScreen 设备保护。策略允许 Trust 区段中所有主机的外向信息流和邮件服务器的内向邮件。内向邮件通过虚拟 IP 地址被发送到邮件服务器。Trust 和 Untrust 区段都在 trust-vr 路由选择域中。

注意：将此范例与 136 页上“路由”模式的范例比较。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容, 然后单击 **OK**:

Interface Mode: NAT¹⁰

10. 在缺省情况下, 绑定到 Trust 区段的任意接口都处于 NAT 模式。因此, 对于绑定到 Trust 区段的接口, 此选项已经启用。

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask¹¹ : 1.1.1.1/24

Interface Mode: 路由

2. VIP¹²

Network > Interfaces > Edit (对于 ethernet3) > VIP: 输入以下内容, 然后单击 **Add**:

Virtual IP Address: 1.1.1.5

Network > Interfaces > Edit (对于 ethernet3) > VIP > New VIP Service: 输入以下内容, 然后单击 **OK**:

Virtual Port: 25

Map to Service: Mail

Map to IP: 10.1.1.5

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

11. 如果 NetScreen 设备上 Untrust 区段中的 IP 地址由 ISP 动态分配, 则保留 IP 地址和 netmask 字段为空, 并选择 **Obtain IP using DHCP**。如果 ISP 使用“以太网点对点传输协议”, 则选择 **Obtain IP using PPPoE**, 然后单击 **Create new PPPoE settings** 链接, 并输入名称和密码。

12. 有关虚拟 IP (VIP) 地址的信息, 请参阅第 372 页上的“虚拟 IP 地址”。

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Policies > (From: Untrust, To: Global) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.5)

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat13
```

```
set interface ethernet3 zone untrust14
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. VIP

```
set interface ethernet3 vip 1.1.1.5 25 mail 10.1.1.5
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

4. 策略

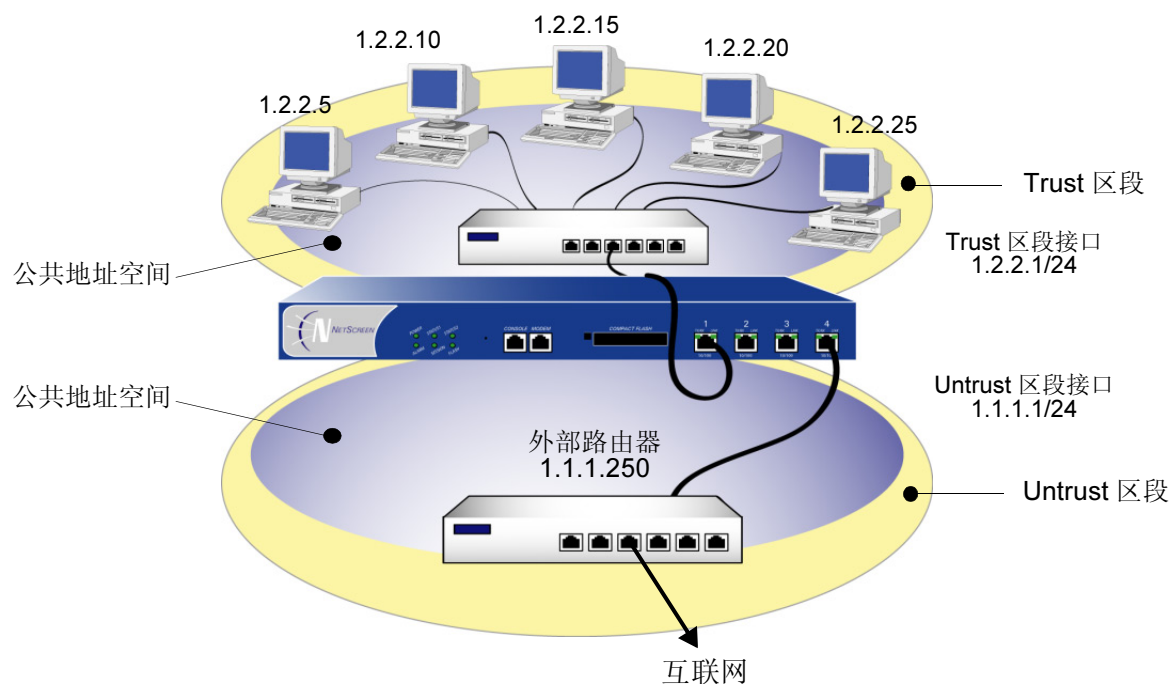
```
set policy from trust to untrust any any any permit
set policy from untrust to global any vip(1.1.1.5) mail permit
save
```

13. **set interface ethernetn nat** 命令确定 NetScreen 设备在 NAT 模式下运行。

14. 如果 NetScreen 设备上 Untrust 区段中的 IP 地址由 ISP 动态分配，则使用以下命令：**set interface untrust dhcp**。如果 ISP 使用“以太网点对点传输协议”，则使用 **set pppoe** 和 **exec pppoe** 命令。详细信息请参阅 *NetScreen CLI Reference Guide*。

路由模式

接口为路由模式时，NetScreen 设备在不同区段间转发信息流时不执行源 NAT (NAT-src)；即，当信息流穿过 NetScreen 设备时，IP 封包包头中的源地址和端口号保持不变。与 NAT-src 不同，目的地区段接口为路由模式时，不需要为了允许入站信息流到达主机而建立映射 IP (MIP) 和虚拟 IP (VIP) 地址。与透明模式不同，每个区段内的接口都在不同的子网中。



不必在接口级应用源网络地址转换 (“NAT-src”), 这样做会使发出外向信息流的所有源地址都被转换为目的地区段接口的 IP 地址。相反，可以在策略级选择性地执行 NAT-src。通过为内向或外向信息流上的指定源地址创建启用 NAT-src 的策略，可确定要确定路由的信息流，以及对哪些信息流执行 NAT-src。对于网络信息流，NAT 可使用 IP 地址或

动态 IP (DIP) 池的目的地区段接口地址，动态 IP 池与目的地区段接口在同一子网中。对于 VPN 信息流，NAT 可使用通道接口 IP 地址或与其关联的 DIP 池的地址。

注意：关于配置基于策略的 NAT-src 的详细信息，请参阅第 275 页上的“源网络地址转换”。

接口设置

对于路由模式，定义以下接口设置，其中 *ip_addr1* 和 *ip_addr2* 代表 IP 地址中的数字，*mask* 代表网络掩码中的数字，*vlan_id_num* 代表 VLAN 标记的编号，*zone* 代表区段名称，*number* 代表以 kbps 为单位的带宽大小：

区段接口	设置	区段子接口
Trust、Untrust、DMZ 和用户定义的区域	IP: <i>ip_addr1</i> Netmask: <i>mask</i> Manage IP*: <i>ip_addr2</i> Traffic Bandwidth†: <i>number</i> Route‡: (选择)	IP: <i>ip_addr1</i> Netmask: <i>mask</i> VLAN Tag: <i>vlan_id_num</i> Zone Name: <i>zone</i> Route†: (选择)

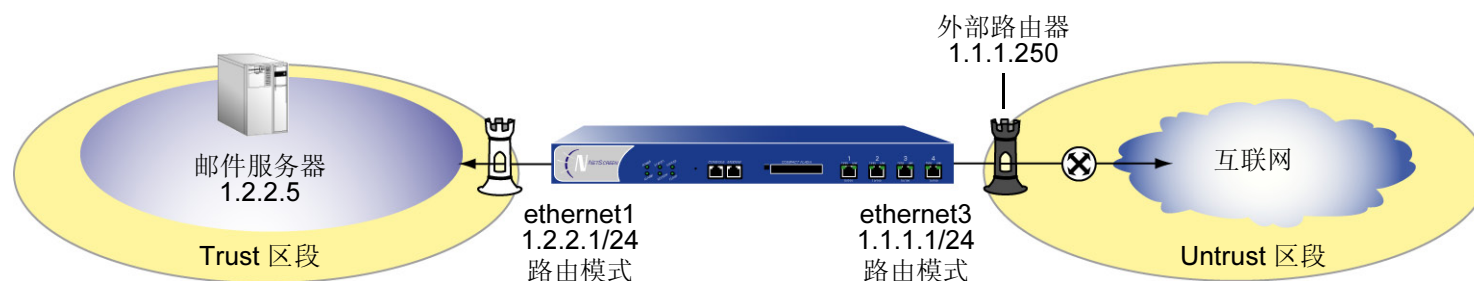
* 可在每个接口的基础上设置管理 IP 地址。主要目的是为从网络信息流中分离出来的管理信息流提供 IP 地址。当某特定设备具备高可用性配置时，也可使用管理 IP 地址来访问它。

† 用于信息流整型的可选设置。

‡ 选择“路由”可将接口模式定义为“路由”。选择 NAT 可将接口模式定义为 NAT。

范例：路由模式

在上一范例第 130 页上的“范例：NAT 模式”中，Trust 区段 LAN 中的主机具有私有 IP 地址和邮件服务器的映射 IP。在以下相同网络（受运行在路由模式下的 NetScreen 设备保护）的范例中，要注意，主机具有公共 IP 地址，且邮件服务器不需要 MIP。所有安全区都在 trust-vr 路由选择域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: Route¹⁵

15. 选择 **Route**，确定 NetScreen 设备在“路由”模式下运行，而不对进出 Trust 区段的信息流执行 NAT。

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask¹⁶ : 1.1.1.1/24

2. 地址

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

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: Trust

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

16. 如果 NetScreen 设备上 Untrust 区段中的 IP 地址由 ISP 动态分配, 则保留 IP 地址和 netmask 字段为空, 并选择 **Obtain IP using DHCP**。如果 ISP 使用“以太网点对点传输协议”, 则选择 **Obtain IP using PPPoE**, 然后单击 **Create new PPPoE settings** 链接, 并输入名称和密码。

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Mail Server

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 1.2.2.1/24
set interface ethernet1 route17
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. 地址

```
set address trust mail_server 1.2.2.5/24
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

4. 策略

```
set policy from trust to untrust any any any permit
set policy from untrust to trust any mail_server mail permit
save
```

17. **set interface ethernet *number* route** 命令确定 NetScreen 设备在路由模式下运行。

为策略构建块

本章讨论了可以在策略中引用的组件或构建块。讨论的具体主题如下：

- 第 142 页上的 “地址”
 - 第 143 页上的 “地址条目”
 - 第 145 页上的 “地址组”
- 第 150 页上的 “服务”
 - 第 150 页上的 “预定义的服务”
 - 第 152 页上的 “定制服务”
 - 第 155 页上的 “ICMP 服务”
 - 第 156 页上的 “RSH ALG”
 - 第 157 页上的 “IP 语音通信的 H.323 协议”
 - 第 172 页上的 “SIP – 会话启动协议”
 - 第 183 页上的 “服务组”
- 第 187 页上的 “DIP 池”
 - 第 190 页上的 “附着 DIP 地址”
 - 第 191 页上的 “扩展接口和 DIP”
 - 第 199 页上的 “回传接口和 DIP”
 - 第 205 页上的 “DIP 组”
- 第 209 页上的 “时间表”

注意：有关用户认证的信息，请参阅第 9 章，第 387 页上的 “用户认证”。

地址

NetScreen ScreenOS 通过位置和网络掩码对所有其它设备的地址进行分类。每个区段都具有自己的地址和地址组列表。

单个主机只定义一个单一的 IP 地址，因此，必须具有设置为 255.255.255.255 的网络掩码 (它掩蔽除该主机以外的所有其它设备)。

子网有 IP 地址和网络掩码 (例如， 255.255.255.0 或 255.255.0.0)。

必须先按区段组织的 NetScreen 地址列表中为其构造条目，才能配置允许、拒绝或导向出入单个主机和子网的信息流策略。

注意：不必为 “Any” 构建地址条目。此术语自动应用到实际位置在它们各自区段中的所有设备。

地址条目

需要先在一个或多个地址列表中定义地址，才能设置许多 **NetScreen** 防火墙、VPN 和信息流整形功能。安全区的地址列表包含主机或子网的 IP 地址或域名¹，这些主机或子网的信息流将被允许、阻塞、加密或进行用户验证。

注意：有关 **ScreenOS** 命名约定的信息 — 应用于为地址创建的名称 — 请参阅第 xiv 页上的“命名约定和字符类型”。

范例：添加地址

在本例中，将 IP 地址为 10.1.10.0/24 的子网 “Sunnyvale_Eng” 添加为 **Trust** 区段中的地址，并将地址 **www.firenet.com** 添加为 **Untrust** 区段中的地址。

WebUI

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: Sunnyvale_Eng

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.10.0/24

Zone: Trust

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: FireNet

IP Address/Domain Name:

Domain Name: (选择), www.firenet.com

Zone: Untrust

1. 必须为 **NetScreen** 设备配置 “域名系统 (DNS)” 服务，才能使用地址条目的域名。有关 DNS 配置的信息，请参阅第 511 页上的“域名系统支持”。

CLI

```
set address trust Sunnyvale_Eng 10.1.10.0/24
set address untrust FireNet www.firenet.com
save
```

范例：修改地址

在本例中，将更改地址 “Sunnyvale_Eng” 的地址条目，以反映此部门特别用于软件工程，并具有不同的 IP 地址 — 10.1.40.0/24。

WebUI

Objects > Addresses > List > Edit (对于 Sunnyvale_Eng): 将名称和 IP 地址更改为以下内容，然后单击 **OK**:

Address Name: Sunnyvale_SW_Eng

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.40.0/24

Zone: Trust

CLI

```
unset address trust Sunnyvale_Eng
set address trust Sunnyvale_SW_Eng 10.1.40.0/24
save
```

注意：在定义地址或地址组并将其与策略相关联后，不能将地址位置更改到其它区段（例如，从 **Trust** 区段更改到 **Untrust** 区段）。要更改它的位置，必须首先将其从底层策略中分离。

范例：删除地址

在本例中，将移除地址 “Sunnyvale_SW_Eng” 的地址条目。

WebUI

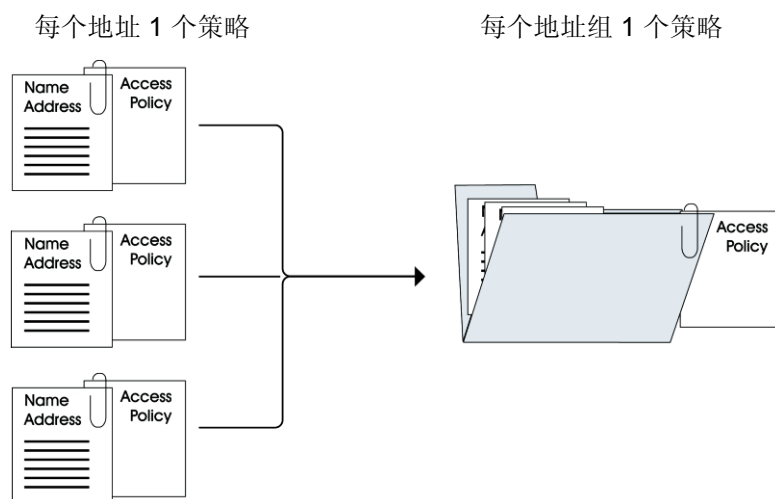
Objects > Addresses > List: 在 Sunnyvale_SW_Eng 的 Configure 栏中，单击 **Remove**。

CLI

```
unset address trust "Sunnyvale_SW_Eng"  
save
```

地址组

上一节说明了如何创建、修改和删除单个主机和子网的通讯簿条目。将地址添加到地址列表后，将很难控制策略如何影响每个地址条目。**NetScreen** 允许创建地址组，这样可以仅管理少数的组，而不用管理大量的地址条目。对组的更改将应用到组中的每个地址条目。



地址组选项具有下列功能：

- 可以在任何区段中创建地址组。
- 可以创建有现有用户的地址组，或者可以创建空的地址组并在以后使用用户填充它们。
- 一个地址组可以是其他地址组的成员²。
- 可以在策略中引用地址组条目，如同单个通讯簿条目一样。
- **NetScreen** 通过在内部为每个组成员创建单个策略，将策略应用到组的每个成员。只需为组创建一个策略，**NetScreen** 实际上为组中的每个成员（以及为每个用户配置的每项服务）都创建了一个内部策略。³
- 从通讯簿中删除单个通讯簿条目时，**NetScreen** 设备将会从它属于的所有组中自动将它移除。

地址组适用以下限制：

- 地址组只能包含属于同一区段的地址。
- 地址名称不能与组的名称相同。如果名称“Paris”用于单个地址条目，则它不能用作组名称。
- 如果地址组被某策略引用，则不能移除该地址组，但是可以进行编辑。
- 将单个策略指派给地址组时，它将独立地应用到每个组成员，并且 **NetScreen** 设备将为访问控制列表 (ACL) 中的每个成员构建一个条目。如果处理不够慎重，可能会超过可用策略资源的数量，尤其是在源地址和目标地址都是地址组，而且指定服务是服务组时。
- 不能将预定义的地址：“Any”、“All Virtual IPs”和“Dial-Up VPN”添加到组中。

2. 要确保一个组不会意外地将自身当作成员包含在组内，将该组添加到其他组时，**NetScreen** 设备将执行运行状况检查。例如，如果将组 A 作为成员添加到组 B，**NetScreen** 设备会自动检查 A 没有将 B 当作其成员包含在内。

3. 由于 **NetScreen** 设备自动将策略应用到每个地址组成员，因此无需逐个为每个地址创建策略。此外，**NetScreen** 还将这些策略写入 ASIC，使查询的运行速度非常快。

范例：创建地址组

下例中，将创建名为“HQ 2nd Floor”的组，该组包括“Santa Clara Eng”和“Tech Pubs”两个地址，它们都已输入 Trust 区段的通讯簿。

WebUI

Objects > Addresses > Groups > (对于 Zone: Trust) New: 输入以下组名称，移动以下地址，然后单击 **OK**:

Group Name: HQ 2nd Floor

选择 **Santa Clara Eng**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **Tech Pubs**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

CLI

```
set group address trust "HQ 2nd Floor" add "Santa Clara Eng"  
set group address trust "HQ 2nd Floor" add "Tech Pubs"  
save
```

范例：编辑地址组条目

在本例中，将 “Support” (已输入通讯簿中的一个地址) 添加到 “HQ 2nd Floor” 地址组中。

WebUI

Objects > Addresses > Groups > (对于 Zone: Trust) Edit (对于 HQ 2nd Floor): 移动以下地址，然后单击 **OK**:

选择 **Support**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

CLI

```
set group address trust "HQ 2nd Floor" add Support
save
```

范例：移除成员和组

在本例中，从 HQ 2nd Floor 地址组中移除成员 “Support”，并删除先前已创建的 “Sales” 地址组。

WebUI

Objects > Addresses > Groups > (对于 Zone: Trust) Edit (对于 HQ 2nd Floor): 移动以下地址，然后单击 **OK**:

选择 **Support**，并使用 **>>** 按钮将地址从 Group Members 栏移动到 Available Members 栏中。

Objects > Addresses > Groups > (Zone: Trust): 在 Sales 的 Configure 栏中，单击 **Remove**。

CLI

```
unset group address trust "HQ 2nd Floor" remove Support
unset group address trust Sales
save
```

注意：NetScreen 设备不会自动删除已经移除其中所有名称的组。

服务

服务是 IP 信息流的类型，它们有相应的协议标准。每个服务都有一个端口号与之相关联，如 FTP 的端口号为 21，Telnet 的端口号为 23。创建策略时，必须为它指定服务。可以从服务簿中选择一个预定义的服务、创建的定制服务或服务组。通过查看 Policy Configuration 对话框中的 Service 下拉列表 (WebUI)，或使用 **get service** 命令 (CLI)，可以查看能够在策略中使用的服务。

预定义的服务

ScreenOS 支持大量预定义的服务。在本节后续部分，可以发现有关这些服务的更详细信息，即：

- [第 155 页上的 “ICMP 服务”](#)
- [第 156 页上的 “RSH ALG”](#)
- [第 157 页上的 “IP 语音通信的 H.323 协议”](#)
- [第 172 页上的 “SIP – 会话启动协议”](#)

使用 WebUI 或 CLI 可以查看 NetScreen 设备的预定义服务、定制服务或服务组的列表。

使用 WebUI:

Objects > Services > Predefined

Objects > Services > Custom

Objects > Services > Groups

使用 CLI:

```
get service [ group | predefined | user ]
```

get service pre-defined CLI 的输出与如下所示内容类似：

Name	Proto	Port	Group	Timeout (分钟)	Flag
ANY	0	0/65535	other	1	Pre-defined
AOL	6	5190/5194	remote	30	Pre-defined
BGP	6	179	other	30	Pre-defined
DHCP-Relay	17	67	info seeking	1	Pre-defined
DNS	17	53	info seeking	1	Pre-defined
FINGER	6	79	info seeking	30	Pre-defined
FTP	6	21	remote	30	Pre-defined
FTP-Get	6	21	remote	30	Pre-defined
FTP-Put	6	21	remote	30	Pre-defined
GOPHER	6	70	info seeking	30	Pre-defined
H.323	6	1720	remote	2160	Pre-defined
--- more ---					

注意：每个预定义服务的源端口范围都为 1-65535，包括所有有效端口号的条目集合。这样可阻止潜在的攻击者通过使用范围以外的源端口获得访问权。对于任何预定义的服务，如果需要使用不同的源端口范围，请创建一个定制服务。有关信息，请参阅第 152 页上的“定制服务”。

可以为预定义服务或定制服务设置超时临界值（以分钟为单位）。可以使用服务缺省超时、指定定制超时或完全不使用超时。

范例：设置服务超时

本例中，将 BGP 预定义服务的超时临界值更改为 75 分钟：

WebUI

Objects > Services > Predefined > Edit (BGP): 输入以下内容，然后单击 **OK**:

Service Timeout: Custom (选择), 75 (类型)

CLI

```
set service BGP timeout 75
save
```

定制服务

除了使用预定义服务之外，您也可以利用定制名称、端口号和传输协议轻松创建自己的服务。以下范例介绍如何添加、修改和移除定制服务。

注意：有关 ScreenOS 命名约定的信息 — 应用于为定制服务创建的名称 — 请参阅第 xiv 页上的“命名约定和字符类型”。

范例：添加定制服务

要将定制服务添加到服务簿中，需要以下信息：

- 服务的名称，本例中为 “cust-telnet”
- 源端口号范围：1 – 65535
- 接收服务请求的目标端口号范围，例如：23000 – 23000。
- 服务使用 TCP 协议还是使用 UDP 协议，或者使用互联网规范定义的其它一些协议。在本例中，为 TCP 协议。

WebUI

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: cust-telnet

Service Timeout: Custom (选择), 30 (类型)

Transport Protocol: TCP (选择)

Source Port Low: 1

Source Port High: 65535

Destination Port Low: 23000

Destination Port High: 23000

CLI

```
set service cust-telnet protocol tcp src-port 1-65535 dst-port 23000-23000
set service cust-telnet timeout 304
save
```

4. 超时值以分钟计。如果没有设置它，则定制服务的超时值为 180 分钟。如果不想服务超时，请输入 **never**。

范例：修改定制服务

在本例中，通过将目标端口范围更改为 23230-23230，修改定制服务 “cust-telnet”。

使用 **set service service_name clear** 命令，在不从服务簿中移除服务的情况下，移除定制服务的定义：

WebUI

Objects > Services > Custom > Edit (对于 cust-telnet): 输入以下内容，然后单击 **OK**:

Destination Port Low: 23230

Destination Port High: 23230

CLI

```
set service cust-telnet clear
set service cust-telnet + tcp src-port 1-65535 dst-port 23230-23230
save
```

范例：移除定制服务

在本例中，将移除定制服务 “cust-telnet”。

WebUI

Objects > Services > Custom: 在 “cust-telnet” 的 Configure 栏中，单击 **Remove**。

CLI

```
unset service cust-telnet
save
```


ICMP 服务

ScreenOS 支持 ICMP (因特网控制信息协议) 以及多种 ICMP 消息作为预定义或定制服务。配置定制 ICMP 服务时，必须定义类型和代码⁵。ICMP 内有不同的消息类型。例如：

- 类型 0 = 回应请求消息
- 类型 3 = 目标不可到达消息

ICMP 消息类型也可以有消息代码。此代码提供有关该消息的更具体信息。例如：

消息类型	消息代码
5 = 重新定向	0 = 重新定向网络 (或子网) 的数据报
	1 = 重新定向主机的数据报
	2 = 重新定向服务类型和网络的数据报
	3 = 重新定向服务类型和主机的数据报
11 = 超时代码	0 = 传输中超过的活动时间
	1 = 超过的碎片重组时间

ScreenOS 支持 0-255 范围内的任何类型或代码。

5. 有关 ICMP 类型和代码的详细信息，请参阅 RFC 792。

范例：定义 ICMP 服务

在本例中，将使用 **ICMP** 作为传输协议定义名为 “**host-unreachable**” 的定制服务。类型为 **3** (对于目标不可到达的服务) 而代码为 **1** (对于主机不可到达的服务)。将超时值设置为 **2** 分钟。

WebUI

Objects > Services > Custom: 输入以下内容，然后单击 **OK**:

Service Name: host-unreachable

Service Timeout: Custom (选择), 2 (类型)

Transport Protocol: ICMP (选择)

ICMP Type: 3

ICMP Code: 1

CLI

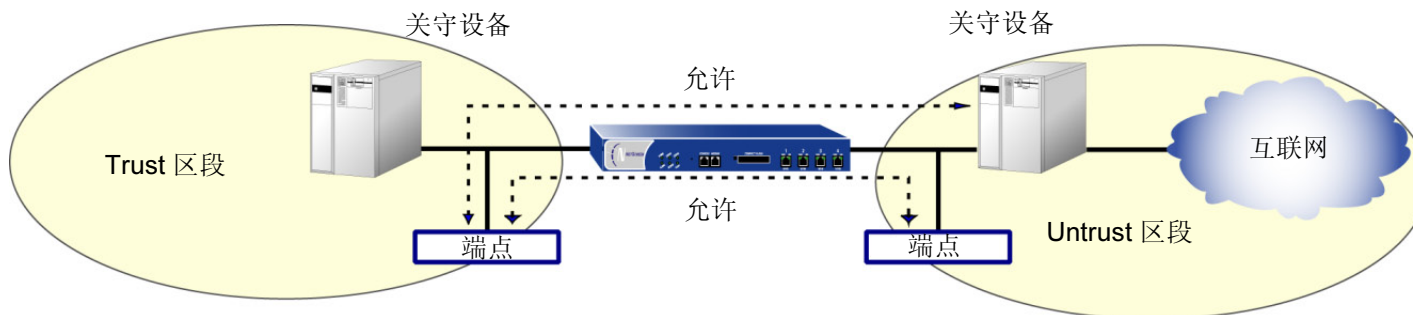
```
set service host-unreachable protocol icmp type 5 code 0
set service host-unreachable timeout 2
save
```

RSH ALG

利用 **RSH ALG** (远程外壳应用程序层网关)，认证用户可在远程主机上运行外壳命令。**NetScreen** 设备支持 “透明” (L2) 模式、“路由” (L3) 模式和 **NAT** 模式中的 **RSH** 服务，但不支持 **RSH** 信息流的端口转换。

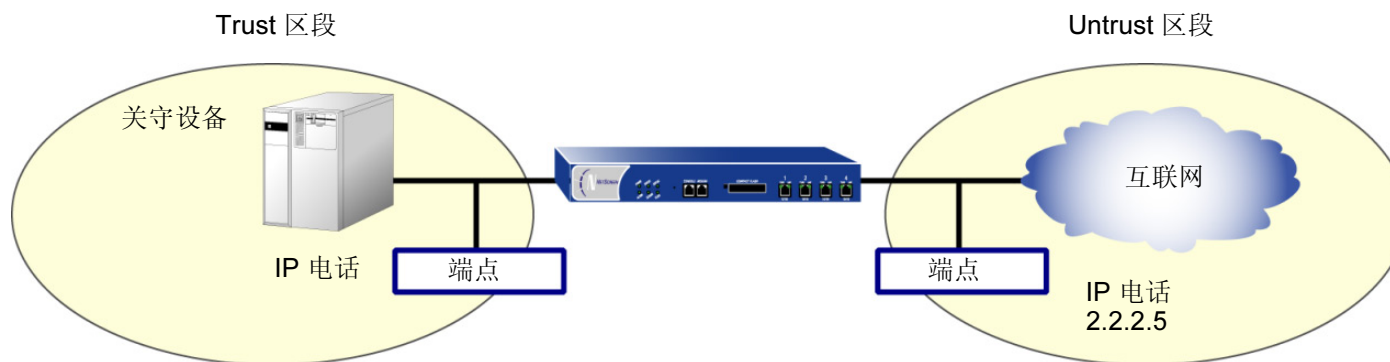
IP 语音通信的 H.323 协议

为了实现终端主机间的安全 IP 语音通信 (VoIP)，NetScreen 设备支持 H.323 协议。在该电话系统中，网关设备管理呼叫注册、许可和 VoIP 呼叫的呼叫状态。网关设备可驻留在两个不同的区段，或驻留在同一区段中。



范例：Trust 区段中的网关设备（透明或路由模式）

在以下范例中，将设置两个策略。这些策略共同允许 H.323 信息流在 IP 电话主机与 Trust 区段的网关设备以及 Untrust 区段的 IP 电话主机 (2.2.2.5) 间流动。在本例中，NetScreen 设备可处于透明模式或路由模式。Trust 和 Untrust 安全区都在 trust-vr 路由选择域中。



WebUI

1. 地址

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

Address Name: IP_Phone

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), IP_Phone

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone

Destination Address:

Address Book Entry: (选择), Any

Service: H.323

Action: Permit

CLI

1. 地址

```
set address untrust IP_Phone 2.2.2.5/32
```

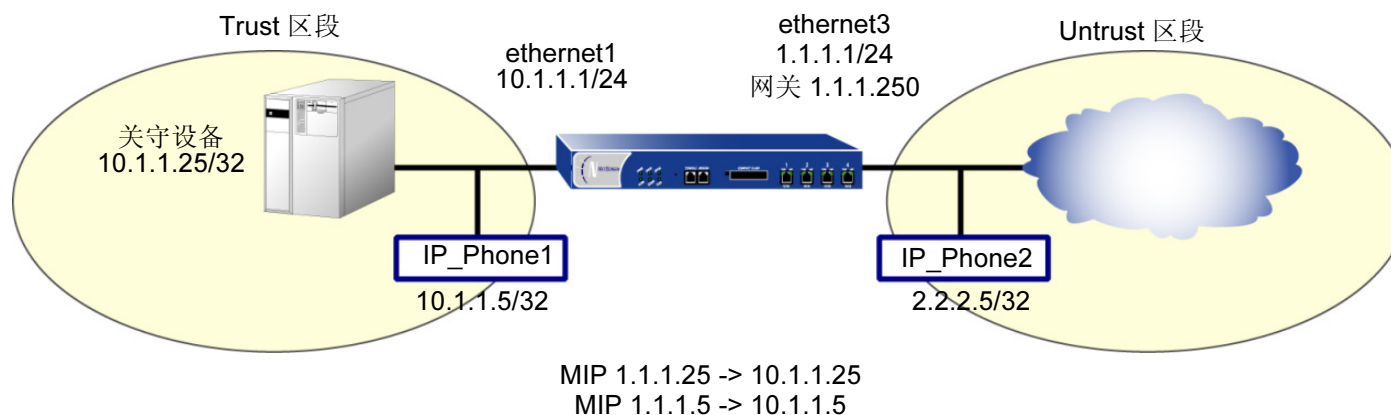
2. 策略

```
set policy from trust to untrust any IP_Phone h.323 permit  
set policy from untrust to trust IP_Phone any h.323 permit  
save
```

范例：Trust 区段中的关守设备 (NAT 模式)

NetScreen 设备处于 NAT 模式时，关守设备或端点设备驻留在 Trust 区段中时，被认为是私有的，驻留在 Untrust 区段中时被认为是公开的。将 NetScreen 设备设置到 NAT 模式时，必须将一个公共 IP 地址映射到每个私有设备。

在本例中，Trust 区段中的设备包括端点主机 (10.1.1.5/32) 和关守设备 (10.1.1.25/32)。IP_Phone2 (2.2.2.5/32) 在 Untrust 区段中。配置 NetScreen 设备以允许信息流在端点主机 IP_Phone1 和 Trust 区段中的关守设备，以及 Untrust 区段中的端点主机 IP_Phone2 间通过。Trust 和 Untrust 安全区都在 trust-vr 路由选择域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: IP_Phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.25/32

Zone: Trust

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

Address Name: IP_Phone2

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 映射 IP 地址

Network > Interfaces > Edit (对于 ethernet3) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

Network > Interfaces > Edit (对于 ethernet3) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 1.1.1.25

Netmask: 255.255.255.255

Host IP Address: 10.1.1.25

Host Virtual Router Name: trust-vr

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), Phone2

Service: H.323

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Gatekeeper

Destination Address:

Address Book Entry: (选择), Phone2

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.5)

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.25)

Service: H.323

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address trust IP_Phone1 10.1.1.5/32
set address trust gatekeeper 10.1.1.25/32
set address untrust IP_Phone2 2.2.2.5/32
```

3. 映射 IP 地址

```
set interface ethernet3 mip 1.1.1.5 host 10.1.1.5
set interface ethernet3 mip 1.1.1.25 host 10.1.1.25
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

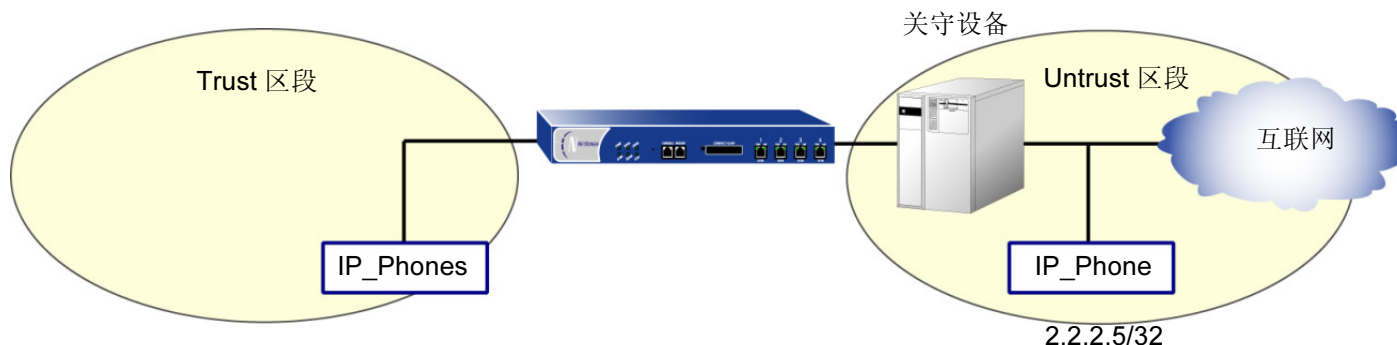
5. 策略

```
set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
set policy from trust to untrust gatekeeper IP_Phone2 h.323 permit
set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
set policy from untrust to trust IP_Phone2 mip (1.1.1.25) h.323 permit
save
```

范例：Untrust 区段中的关守设备（透明或路由模式）

由于透明模式和路由模式不需要任何类型的地址映射，因此在 Untrust 区段中关守设备的 NetScreen 设备配置，通常与 Trust 区段中关守设备的 NetScreen 设备配置相同。

在下例中，设置两个允许 H.323 信息流在 Trust 区段中的 IP 电话主机（和关守设备），与 Untrust 区段中 IP 地址为 2.2.2.5 的 IP 电话间流动的策略。设备可以处于透明或路由模式。Trust 和 Untrust 安全区都在 trust-vr 路由选择域中。



WebUI

1. 地址

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

Address Name: IP_Phone

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.10/32

Zone: Untrust

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), IP_Phone

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone

Destination Address:

Address Book Entry: (选择), Any

Service: H.323

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Gatekeeper

Service: H.323

Action: Permit

CLI

1. 地址

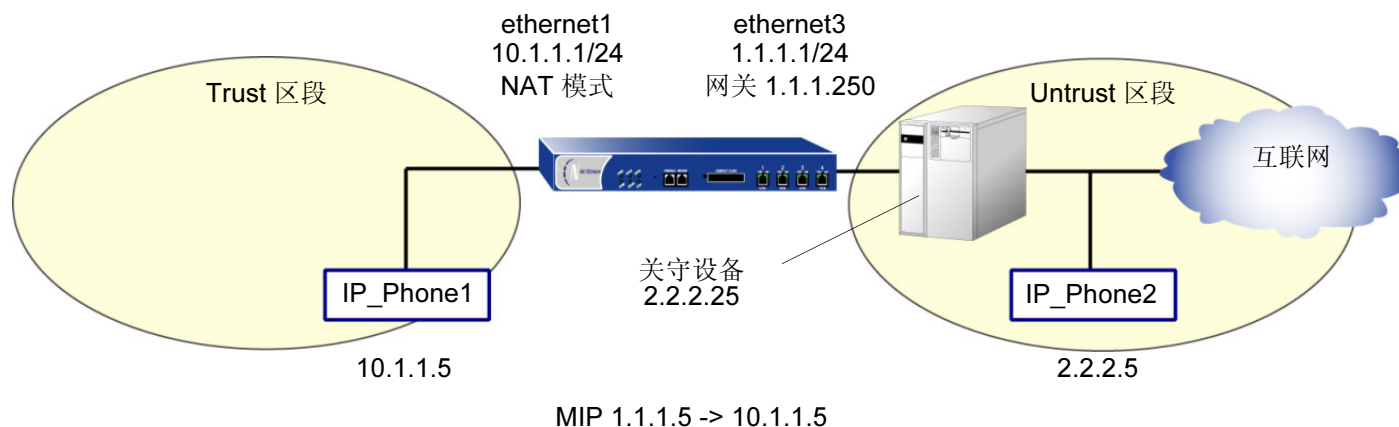
```
set address untrust IP_Phone 2.2.2.5/32
set address untrust gatekeeper 2.2.2.10/32
```

2. 策略

```
set policy from trust to untrust any IP_Phone h.323 permit
set policy from untrust to trust IP_Phone any h.323 permit
set policy from trust to untrust any gatekeeper h.323 permit
save
```

范例 : Untrust 区段中的关守设备 (NAT 模式)

本例中, 关守设备 (2.2.2.25) 和主机 IP_Phone2 (2.2.2.5) 都在 Untrust 区段中, 并且主机 IP_Phone1 (10.1.1.5) 在 Trust 区段中。配置 NetScreen 设备以允许信息流在 Trust 区段中的主机 IP_Phone1 和 Untrust 区段中的主机 IP_Phone2 (及关守设备) 间通过。Trust 和 Untrust 安全区都在 trust-vr 路由选择域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: IP_Phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.25/32

Zone: Untrust

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

Address Name: IP_Phone2

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 映射 IP 地址

Network > Interfaces > Edit (对于 ethernet3) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), IP_Phone2

Service: H.323

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), Gatekeeper

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.5)

Service: H.323

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Gatekeeper

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.5)

Service: H.323

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address trust IP_Phone1 10.1.1.5/32
set address untrust gatekeeper 2.2.2.25/32
set address untrust IP_Phone2 2.2.2.5/32
```

3. 映射 IP 地址

```
set interface ethernet3 mip 1.1.1.5 host 10.1.1.5
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. 策略

```
set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
set policy from trust to untrust IP_Phone1 gatekeeper h.323 permit
set policy from untrust to trust IP_Phone2 mip(1.1.1.5) h.323 permit
set policy from untrust to trust gatekeeper mip(1.1.1.5) h.323 permit
save
```

SIP – 会话启动协议

SIP (会话启动协议) 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。

NetScreen 设备支持将 **SIP** 作为服务并可以筛选 **SIP** 信息流, 根据所配置的策略允许并拒绝信息流。**SIP** 是 **ScreenOS** 中的预定义服务, 使用端口 **5060** 作为目标端口。请注意, **NetScreen** 设备当前不支持带有 **NAT** (网络地址转换) 的 **SIP**。

实际上, **SIP** 用于分配会话说明, 在会话期间用于协商和修改会话参数。**SIP** 还用于终止多媒体会话。

用户可将会话说明包括在 **INVITE** 或 **ACK** 请求中。会话说明指出会话的多媒体类型, 例如语音或视频。**SIP** 可使用不同的说明协议来说明会话, **NetScreen** 仅支持 **SDP** (会话说明协议)。

SDP 提供系统可以使用的信息, 以便与多媒体会话结合。**SDP** 可能包括如 **IP** 地址、端口号、时间和日期等信息。请注意, **SDP** 报头中的 **IP** 地址和端口号 (分别为 “**c=**” 和 “**m=**” 字段) 是客户端希望接收媒体流的地址和端口, 而不是发出 **SIP** 请求的 **IP** 地址和端口号 (尽管它们可能是相同的)。有关详细信息, 请参阅第 176 页上的 “**SDP**”。

SIP 消息由从客户端到服务器的请求和对从服务器到客户端的请求的响应组成, 目的是建立会话 (或呼叫)。**UA** (用户代理) 是运行在呼叫端点的应用程序, 由下列两部分组成: 代表用户发送 **SIP** 请求的 **UAC** (用户代理客户端) 及接听响应并在响应到达时通知用户的 **UAS** (用户代理服务器)。用户代理的范例是 **SIP** 代理服务器和 **SIP** 电话。

SIP 请求方法

主要有六种类型的 SIP 请求，每种请求满足不同的目的。每种 SIP 请求都包含一个 *method* 字段，它表示请求的目的。以下列出了六种不同的方法。

INVITE – 用户发送 INVITE 请求，邀请其他用户参与会话。INVITE 请求的主体可能包含会话说明。

ACK – 发出 INVITE 的用户发送 ACK 请求，以确认是否接收到对 INVITE 的最终响应。如果初始 INVITE 请求不包含会话说明，则 ACK 请求必须包括。

OPTIONS – 用户向服务器发送 OPTIONS 请求，以获取有关其功能的信息。服务器以方法、会话说明协议及其支持的消息编码等信息回复。

BYE – 用户发送 BYE 请求以放弃会话。来自任一用户的 BYE 请求都将自动终止会话。

CANCEL – 用户可以发送 CANCEL 请求，以取消等待中的 INVITE 请求。如果处理 INVITE 的 SIP 服务器接收到 CANCEL 之前，已经发送 INVITE 请求的最终响应，则 CANCEL 请求不起作用。

REGISTER – 用户向 SIP *registrar* 服务器发送 REGISTER 请求，将自身当前的位置告知服务器。SIP *registrar* 服务器记录在 REGISTER 请求中接收到的所有信息，任何尝试查找用户的 SIP 服务器均可使用此信息。

SIP 响应的类别

SIP 响应指出事务的状态。它们包括分组为以下类别的代码：

100 到 199 – 信息性：已接收到请求，继续处理请求

200 到 299 – 成功：已成功接收、了解和接受操作

300 到 399 – 重新定向：为完成请求，需要采取进一步行动

400 到 499 – 客户端错误：请求包含错误语法或无法在此服务器上完成

500 到 599 – 服务器错误：服务器无法完成显然有效的请求

600 到 699 – 全局失败：在任何服务器上都无法完成请求

以下是当前 SIP 响应代码的完整列表。NetScreen 支持所有响应代码。

1xx	100 尝试中	180 呼叫中	181 呼叫已转移
	182 已排队	183 会话进程	
2xx	200 OK	202 已接受	
3xx	300 多重选择	301 永久移动	302 临时移动
	305 使用代理	380 可选服务	
4xx	400 请求错误	401 未授权	402 需要付款
	403 禁止	404 未找到	405 不允许的方法
	406 不可接受	407 需要代理认证	408 请求超时
	409 冲突	410 遗失	411 需要的长度
	413 请求实体太多	414 请求的 URL 太大	415 不支持的介质类型
	420 扩展名错误	480 暂时不可用	481 呼叫路线 / 事务不存在
	482 检测到回路	483 跳跃太多	484 地址不完整
	485 不明确	486 此处正忙	487 取消请求
	488 此处不可接受		
5xx	500 服务器内部错误	501 未执行	502 网关错误
	502 服务不可用	504 网关超时	505 不支持的 SIP 版本
6xx	600 全域忙碌中	603 谢绝	604 不存在于任何地方
	606 不可接受		

ALG – 应用程序层网关

有两种类型的 SIP 信息流，它们是信号发送和媒体流。SIP 信号发送信息流由客户端和服务端间的请求和响应组成，并使用传输协议，如 UDP 或 TCP。媒体流携带数据（例如，音频数据）并在 UDP 上使用应用程序层协议，如 RTP（实时传输协议）。

NetScreen 设备支持端口 5060 上的 SIP 信号发送消息。只需创建允许 SIP 服务的策略，NetScreen 设备即会过滤 SIP 信号信息流（像其它任何类型的信息流一样），允许或拒绝信息流。但是，媒体流使用动态分配的端口号，在呼叫过程期间可以进行数次更改。由于没有固定的端口，所以创建静态策略来控制媒体信息流是不可能的。在这种情况下，NetScreen 设备就会调用 SIP ALG。SIP ALG 读取 SIP 消息及其 SDP 内容，然后提取需要的端口号信息来动态打开针孔⁶，并让媒体流通过 NetScreen 设备。

SIP ALG 监控 SIP 事务，根据从这些事务中提取的信息动态创建并管理针孔。NetScreen SIP ALG 支持所有 SIP 方法和响应（请参阅第 173 页上的“SIP 请求方法”和第 173 页上的“SIP 响应的类别”）。通过创建允许 SIP 服务的静态策略，可以允许 SIP 事务通过 NetScreen 防火墙。该策略使得 NetScreen 设备截取 SIP 信息流，并执行下列操作之一：允许或拒绝信息流或启用 SIP ALG 打开针孔，以便通过媒体流。仅仅为了 SIP 请求和包含媒体信息（SDP）的响应，SIP ALG 需要打开针孔。对于不包含 SDP 的 SIP 消息，NetScreen 设备就会让它们通过。

SIP ALG 截取包含 SDP 的 SIP 消息，并且使用剖析器提取创建针孔需要的信息。SIP ALG 检查封包的 SDP 部分，剖析器提取 SIP ALG 在针孔表中记录的信息，如 IP 地址和端口号。SIP ALG 使用针孔表中记录的 IP 地址和端口号，打开针孔并允许媒体流通过 NetScreen 设备。

注意：NetScreen 设备不支持加密的 SDP。如果 NetScreen 设备接收到其中 SDP 加密的 SIP 消息，则 SIP ALG 允许该消息通过防火墙，但生成日志消息通知用户无法处理该封包。如果 SDP 加密，则 SIP ALG 不能从 SDP 提取打开针孔需要的信息。结果，SDP 描述的媒体内容不能通过 NetScreen 设备。

6. 我们将针孔称为端口的有限开口，允许唯一信息流通过。

SDP

SDP 会话说明是基于文本的，并且由一组行构成。可能包含会话级和媒体级信息。会话级信息应用于整个会话，而媒体级信息应用于特定的媒体流。SDP 会话说明始终包含会话级信息，在说明的开始部分出现，并且可能包含随后出现的媒体级信息⁷。

在 SDP 说明的许多字段中，其中有两个字段对 SIP ALG 特别有用，因为他们包含传输层信息。这两个字段如下所示：

- **c=** 表示连接信息

此字段可能出现在会话级或媒体级。其显示格式为：

c=< 网络类型 >< 地址类型 >< 连接地址 >

当前，NetScreen 设备仅支持将 “IN” (表示互联网) 作为网络类型、将 “IP4” 作为地址类型、将单点传送的 IP 地址⁸ 或域名作为目标 (连接) IP 地址。

如果目标 IP 地址是单点传送的 IP 地址，则 SIP ALG 使用媒体说明字段 **m=** 中指定的 IP 地址和端口号创建针孔。

- **m=** 表示媒体声明

此字段出现在媒体级，并且包含媒体说明。其显示格式为：

m=< 媒体 >< 端口 >< 传输 ><fmt 列表 >

当前，NetScreen 设备仅支持将 “audio” 作为媒体，并将 “RTP” 作为应用程序层协议 (传输)。端口号指出媒体流的目标 (而不是媒体流的来源)。格式列表 (fmt 列表) 提供了有关媒体使用的应用程序层协议的信息。

在 ScreenOS 的此版本中，NetScreen 设备仅为 RTP 和 RTCP 打开端口。每个 RTP 会话都有一个相应的 RTCP⁹ (实时传输控制协议) 会话。因此，每当媒体流使用 RTP 时，SIP ALG 必须为 RTP 和 RTCP 信息流保留端口 (创建针孔)。在缺省情况下，RTCP 的端口号比 RTP 的端口号高一个号码。

7. 在 SDP 会话说明中，媒体级信息以 **m=** 字段开始。

8. 通常，目标 IP 地址还可以是多点传送的 IP 地址，但 NetScreen 当前并不支持带有 SIP 的多点传送。

9. RTCP 提供媒体同步和有关会话成员及通信质量的信息。

针孔创建

RTP 和 RTCP 信息流的针孔共享同一个目标 IP 地址。该 IP 地址来源于 SDP 会话说明中的 **c=** 字段。由于 **c=** 字段可能会出现在 SDP 会话说明的会话级或媒体级部分，所以剖析器根据下列规则 (与 SDP 约定一致) 确定该 IP 地址：

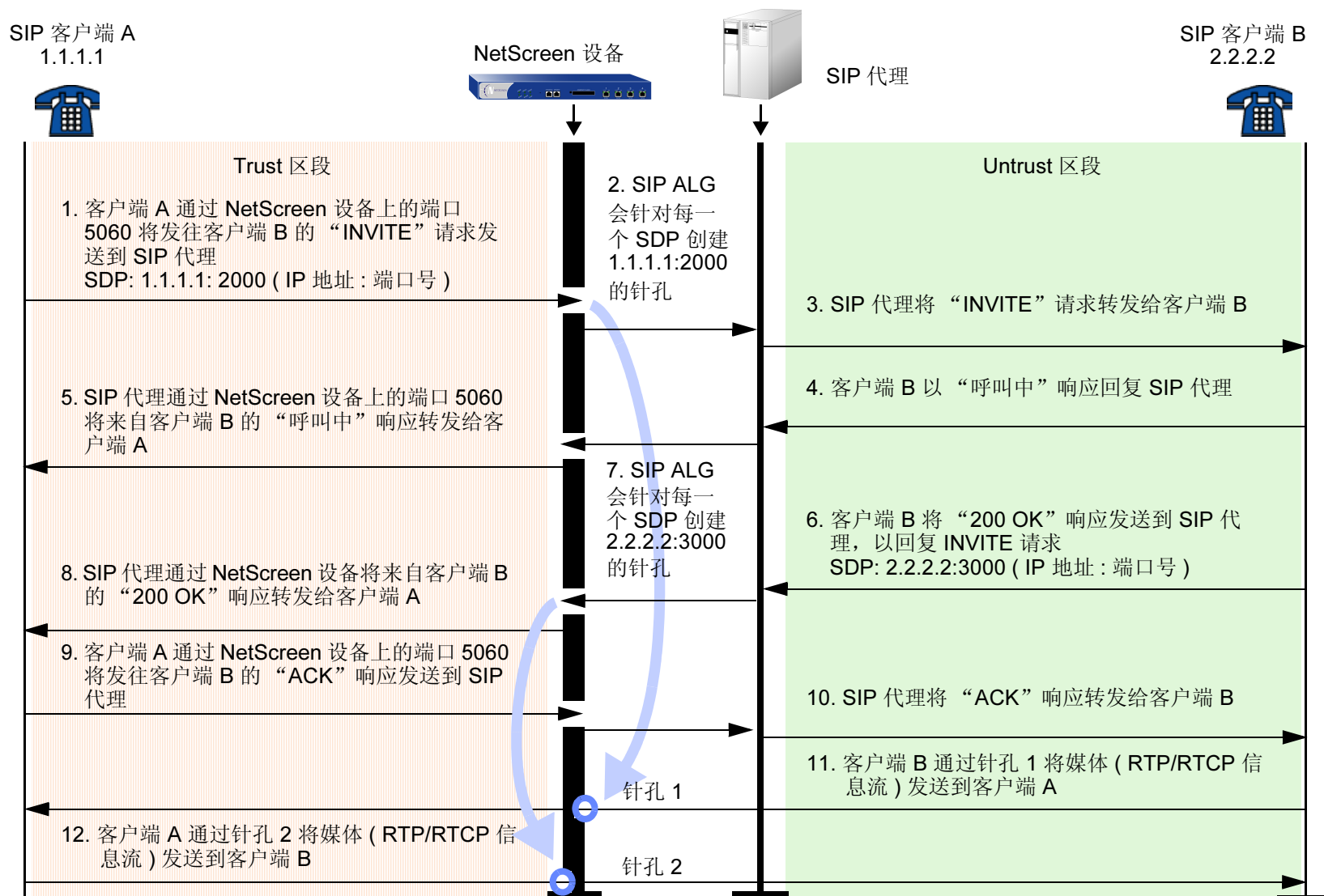
- 首先，SIP ALG 剖析器验证媒体级中是否有包含 IP 地址的 **c=** 字段。如果有，则剖析器提取该 IP 地址，然后 SIP ALG 使用该地址为媒体创建针孔。
- 如果媒体级中没有 **c=** 字段，则 SIP ALG 剖析器从会话级的 **c=** 字段中提取 IP 地址，然后 SIP ALG 使用该地址为媒体创建针孔。如果会话说明的两个级中均不包含 **c=** 字段，这表明协议栈中存在错误，NetScreen 设备将丢弃封包并记录事件。

以下列出了 SIP ALG 创建针孔需要的信息。此信息来源于 NetScreen 设备上的 SDP 会话说明和参数。

- **Protocol:** UDP
- **Source IP:** 未知
- **Source port:** 未知
- **Destination IP:** 剖析器会从媒体级或会话级的 **c=** 字段中提取目标 IP 地址。
- **Destination port:** 剖析器会从媒体级的 **m=** 字段中提取 RTP 的目标端口号，然后使用下列公式计算 RTCP 的目标端口号： $RTP \text{ 端口号} + 1$ 。
- **Lifetime:** 此值指出针孔打开期间允许封包通过的时间长度 (以秒计)。封包必须在生存期到期之前通过针孔。生存期到期时，SIP ALG 即移除针孔。

一旦封包在生存期之内通过针孔，SIP ALG 就立即移除封包来源方向的针孔。

下图说明了两个 SIP 客户端之间的呼叫设置，以及 SIP ALG 如何创建针孔以允许 RTP 和 RTCP 信息流通过。本图假定 NetScreen 设备具有允许 SIP 的策略，因此打开端口 5060 以便 SIP 发出消息。



注意：如果目标 IP 地址为 0.0.0.0 (表示会话暂停中)，则 SIP ALG 不会为 RTP 和 RTCP 信息流创建针孔。例如，要想在电话通信期间暂停会话，用户 (用户 A) 可以将 SIP 消息 (目标 IP 地址为 0.0.0.0) 发送到其他用户 (用户 B)。执行上述操作以指示用户 B 在另行通知前不要再发送任何媒体。如果用户 B 仍然发送媒体，则 NetScreen 设备即会丢弃封包。

会话静止超时

通常，如果一方客户端发送 BYE 或 CANCEL 请求，呼叫随即终止。SIP ALG 会截取 BYE 或 CANCEL 请求，并移除该呼叫的所有媒体会话。如果呼叫中的客户端无法发送 BYE 或 CANCEL 请求，可能有特殊原因或问题，如电源故障。在这种情况下，呼叫可能会一直进行下去，并持续消耗 NetScreen 设备上的资源。静止超时功能有助于 NetScreen 设备监控呼叫的活动状况，如果在某特定时期内没有活动即终止呼叫。

一个呼叫可具有一个或多个语音通道。每个语音通道具有两个会话 (或两个媒体流)，分别用于 RTP 和 RTCP。NetScreen 设备在管理会话时，会将各语音通道中的会话视为一个组。诸如静止超时这样的设置适用于各会话的相对组。

有两种静止超时类型可决定组的生存期：

- 信号发送静止超时：该参数指出呼叫可以维持活动的最大时间长度 (以秒为单位)，而不进行任何 SIP 信号发送信息流。每次呼叫中进行 SIP 发信号消息时，即重设超时。缺省设置为 43200 秒 (12 小时)。
- 媒体静止超时：该参数指出呼叫可以维持活动的最大时间长度 (以秒为单位)，而组中不进行任何媒体 (RTP 或 RTCP) 信息流。每次呼叫中出现 RTP 或 RTCP 封包时，即重设超时。缺省值为 120 秒。

如果这两种超时有任一种到期，则 NetScreen 设备会将该呼叫的所有会话从其表格中移除，然后终止呼叫。

范例：创建策略以允许 SIP

在本例中，将创建两个策略以允许双向信息流。一个策略允许 SIP 信息流从 Untrust 区段中的 SIP 客户端 B 流向 Trust 区段中的 SIP 客户端 A。另一个策略允许 SIP 信息流从 Trust 区段中的 SIP 客户端 A 流向 Untrust 区段中的 SIP 客户端 B。



WebUI

1. 地址

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

Address Name: Client-A

IP Address/Domain Name: IP/Netmask: 1.1.1.1/32

Zone: Trust

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

Address Name: Client-B

IP Address/Domain Name: IP/Netmask: 2.2.2.2/32

Zone: Untrust

2. 策略

Policies > (From: Untrust, To: Trust) > New: 输入以下内容，然后单击 **OK**:

Source Address:

New Address: 2.2.2.2/32

Destination Address:

New Address: 1.1.1.1/32

Service: SIP

Action: Permit

Policies > (From: Trust, To: Untrust) > New: 输入以下内容，然后单击 **OK**:

Source Address:

New Address: 1.1.1.1/32

Destination Address:

New Address: 2.2.2.2/32

Service: SIP

Action: Permit

CLI

1. 地址

```
set address trust client-a 1.1.1.1/32
set address untrust client-b 2.2.2.2/32
```

2. 策略

```
set policy from untrust to trust 2.2.2.2 1.1.1.1 sip permit
set policy from trust to untrust 1.1.1.1 2.2.2.2 sip permit
save
```

范例：信号发送与媒体静止超时

在本例中，将信号发送静止超时配置为 30,000 秒，将媒体静止超时配置为 90 秒。

WebUI

注意：不能使用 WebUI 配置此功能。

CLI

```
set sip signaling-inactivity-timeout 30000
set sip media-inactivity-timeout 90
save
```

服务组

服务组是一组集合在一个名称下的服务。在创建包含几个服务的组后，就可以在组级将服务应用到策略，从而简化了管理。

NetScreen 服务组选项具有下列功能：

- 每个服务簿条目都可以被一个或多个服务组引用。
- 每个服务组都可包含预定义的和用户定义的服务簿条目。

服务组受到以下限制：

- 服务组不能与服务的名称相同；因此，如果有一项服务的名称为“FTP”，则不能将服务组命名为“FTP”。
- 如果某服务组被策略引用，则可以编辑但不能移除该组，除非先在策略中移除对它的引用。
- 从服务簿中删除定制服务簿条目时，也将该条目从所有引用它的组中移除。
- 一个服务组不能将其它服务组当作成员包含在内。
- 全包含式服务术语“ANY”不能添加到组中。
- 一个服务一次仅能作为一个组的一部分。

范例：创建服务组

在本范例中，您创建名为 **grp1** 的服务组，其中包括 **IKE**、**FTP** 和 **LDAP** 服务。

WebUI

Objects > Services > Groups > New: 输入以下组名称，移动以下服务，然后单击 **OK**:

Group Name: grp1

选择 **IKE**，并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **FTP**，并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **LDAP**，并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

CLI

```
set group service grp1
set group service grp1 add ike
set group service grp1 add ftp
set group service grp1 add ldap
save
```

注意：如果尝试将服务添加到不存在的服务组中，**NetScreen** 设备将创建该组。同样，应确保引用其它组的组不能将其自身包括在引用列表中。

范例：修改服务组

在本范例中，更改名称为 **grp1** 的服务组中的成员，此组是您在第 184 页上的“范例：创建服务组”中创建的。移除 **IKE**、**FTP** 和 **LDAP** 服务，并添加 **HTTP**、**FINGER** 和 **IMAP**。

WebUI

Objects > Services > Groups > Edit (对于 **grp1**): 移动以下服务，然后单击 **OK**:

选择 **IKE**，并使用 **>>** 按钮将服务从 Group Members 栏移动到 Available Members 栏中。

选择 **FTP**，并使用 **>>** 按钮将服务从 Group Members 栏移动到 Available Members 栏中。

选择 **LDAP**，并使用 **>>** 按钮将服务从 Group Members 栏移动到 Available Members 栏中。

选择 **HTTP**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **Finger**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **IMAP**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

CLI

```
unset group service grp1 clear
set group service grp1 add http
set group service grp1 add finger
set group service grp1 add imap
save
```

范例：移除服务组

在本例中，将删除名为 “grp1” 的服务组。

WebUI

Objects > Services > Groups: 单击 **Remove** (对于 grp1)。

CLI

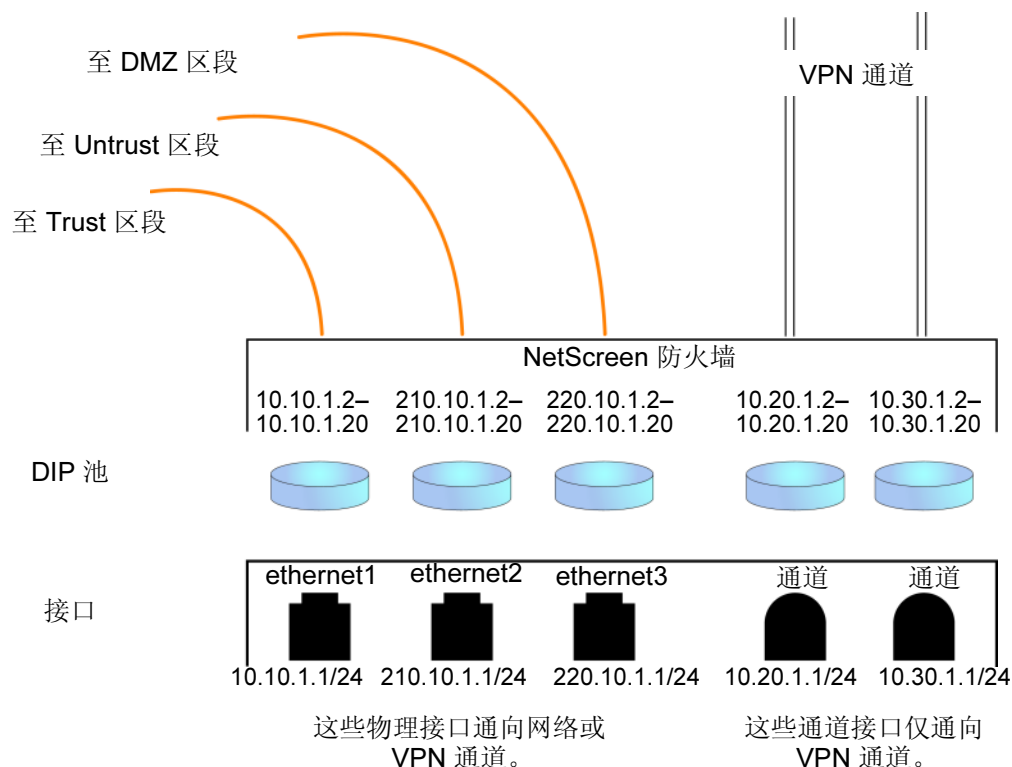
```
unset group service grp1  
save
```

注意：NetScreen 设备不会自动删除已经移除其中所有成员的组。

DIP 池

动态 IP (DIP) 池包含一个范围内的 IP 地址，NetScreen 设备在对 IP 封包包头中的源 IP 地址执行网络地址转换时，可从中动态地或定态地提取地址。[有关确定源地址转换的信息，请参阅第 283 页上的“来自 DIP 池 (带有地址变换) 的 NAT-Src”]。如果 DIP 池的地址范围与接口 IP 地址在相同的子网中，那么该池必须排除也可能在该子网中的接口 IP 地址、路由器 IP 地址及任何映射 IP (MIP) 或虚拟 IP (VIP) 地址。如果地址范围在扩展接口的子网中，那么该池必须排除扩展接口的 IP 地址。

可将三种接口链接到“动态 IP”(DIP) 池：网络和 VPN 信息流的物理接口和子接口，以及仅用于 VPN 通道的通道接口。



端口地址转换

使用“端口地址转换”(PAT)，多台主机可共享同一 IP 地址，NetScreen 设备维护一个已分配端口号的列表，以识别哪个会话属于哪个主机。启用 PAT 后，最多 64,500 台主机即可共享单个 IP 地址。

一些应用，如“NetBIOS 扩展用户接口”(NetBEUI)和“Windows 互联网命名服务”(WINS)，需要具体的端口号，如果将 PAT 应用于它们，它们将无法正常运行。对于这种应用，应用 DIP 时，可指定不执行 PAT (即，使用固定端口)。对于固定端口 DIP，NetScreen 设备散列原始的主机 IP 地址，并将它保存在其主机散列表中，从而允许 NetScreen 设备将正确的会话与每个主机相关联。

范例：创建带有 PAT 的 DIP 池

在本例中，将为本地网站的用户创建 VPN 通道，以到达远程网站的 FTP 服务器。但是，这两个网站的内部网络使用相同的私有地址空间 (10.1.1.0/24)。为了解决重叠地址的问题，在本地 NetScreen 设备的 Untrust 区段中创建通道接口，给它分配 IP 地址 10.10.1.1/24，然后将它与地址范围为 10.10.1.2 –10.10.1.2 (来自中性地址空间 10.10.1.0/24) 的 DIP 池相关联。

在远程网站的 admin，也必须创建 IP 地址在中性地址空间的通道接口，如 10.20.2.1/24，然后设置到其 FTP 服务器的“映射 IP”(MIP) 地址，如到主机 10.1.1.5 的 10.20.2.5。

注意：本例仅包括通道接口配置及其伴随的 DIP 池。有关此方案所有必要配置步骤的完整范例，请参阅第 5-168 页上的“具有重叠地址的 VPN 站点”。

WebUI

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.10.1.1/24

Network > Interfaces > Edit (对于 tunnel.1) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5¹⁰

IP Address Range: 10.10.1.2 ~ 10.20.1.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

CLI

```
set interface tunnel.1 zone untrust-tun
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 dip 5 10.10.1.2 10.20.1.2
save
```

注意: 在缺省情况下, 启用 **PAT**, 因此没有启用它的参数。要创建与上述相同的 **DIP** 池但无 **PAT** (即, 使用固定端口号), 请执行以下操作:

- **(WebUI)** Network > Interfaces > Edit (对于 tunnel.1) > DIP > New: 清除 **Port Translation** 复选框, 然后单击 **OK**。
- **(CLI)** `set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2 fix-port`

10. 可使用显示出的 ID 号, 它是依顺序的下一可用号码, 或键入不同的号。

范例：修改 DIP 池

在本例中，将更改一个现有 DIP 池 (ID 5) 的地址范围，从 10.20.1.2 – 10.20.1.2 到 10.20.1.2 – 10.20.1.10。此 DIP 池与 tunnel.1 相关联。请注意，要通过 CLI 更改 DIP 池范围，必须首先移除 (或撤消) 现有 dip 池，然后创建新池。

注意：没有使用此特定 DIP 池的策略。如果策略使用 DIP 池，必须先删除策略或将它修改为不使用 DIP 池，然后才能修改 DIP 池。

WebUI

Network > Interfaces > Edit (对于 tunnel.1) > DIP > Edit (对于 ID 5): 输入以下内容，然后单击 **OK**:

IP Address Range: 10.20.1.2 ~ 10.20.1.10

CLI

```
unset interface tunnel.1 dip 5
set interface tunnel.1 dip 5 10.20.1.2 10.20.1.10
save
```

附着 DIP 地址

主机发起与要求网络地址转换 (NAT) 的策略相匹配的几个会话，并且获得了来自 DIP 池 (已启用端口转换) 的分配地址时¹¹，NetScreen 设备为每个会话分配不同的源 IP 地址。对于创建多个会话 (每个会话都需要同一源 IP 地址) 的服务，这种随机地址分配可能会产生问题。

例如，使用“**AOL 即时消息 (AIM)**”客户端时，多个会话具有相同的 IP 地址非常重要。登录时将创建一个会话，并且将创建另一个用于每个聊天的会话。对于验证新聊天属于认证用户的 AIM 服务器，必须使登录会话的源 IP 地址与聊天会话的源 IP 地址相匹配。如果它们不同 — 可能因为是在 NAT 过程期间从 DIP 池随机分配的 — AIM 服务器将拒绝聊天会话。

要确保 NetScreen 设备从 DIP 池将相同的 IP 地址分配给主机的多个同时会话，可输入 CLI 命令 **set dip sticky**，启用“附着”DIP 地址功能。

11. 如果 DIP 池未执行端口转换，NetScreen 设备将会从相同的主机为所有并发会话分配一个 IP 地址。

扩展接口和 DIP

根据情况，如果需要将出站防火墙信息流中的源 IP 地址，从出口接口的地址转换成不同子网中的地址，可使用扩展接口选项。此选项允许将第二个 IP 地址和一个伴随 DIP 池连接到一个在不同子网中的接口。然后，可基于每个策略启用 NAT，并且指定 DIP 池，该池在用于转换的扩展接口上创建。

范例：在不同子网中使用 DIP

在本例中，有两个分支机构租借了到总部的线路。总部要求他们仅使用总部分配给他们的授权 IP 地址。然而，这两个分支机构从其 ISP 处收到了不同的用于互联网信息流的 IP 地址。为了与总部进行通讯，使用扩展接口选项配置每个分支机构的 NetScreen 设备，将其发送至总部的封包的源 IP 地址转换为授权地址。分支机构 A 和 B 的授权和分配的 IP 地址如下：

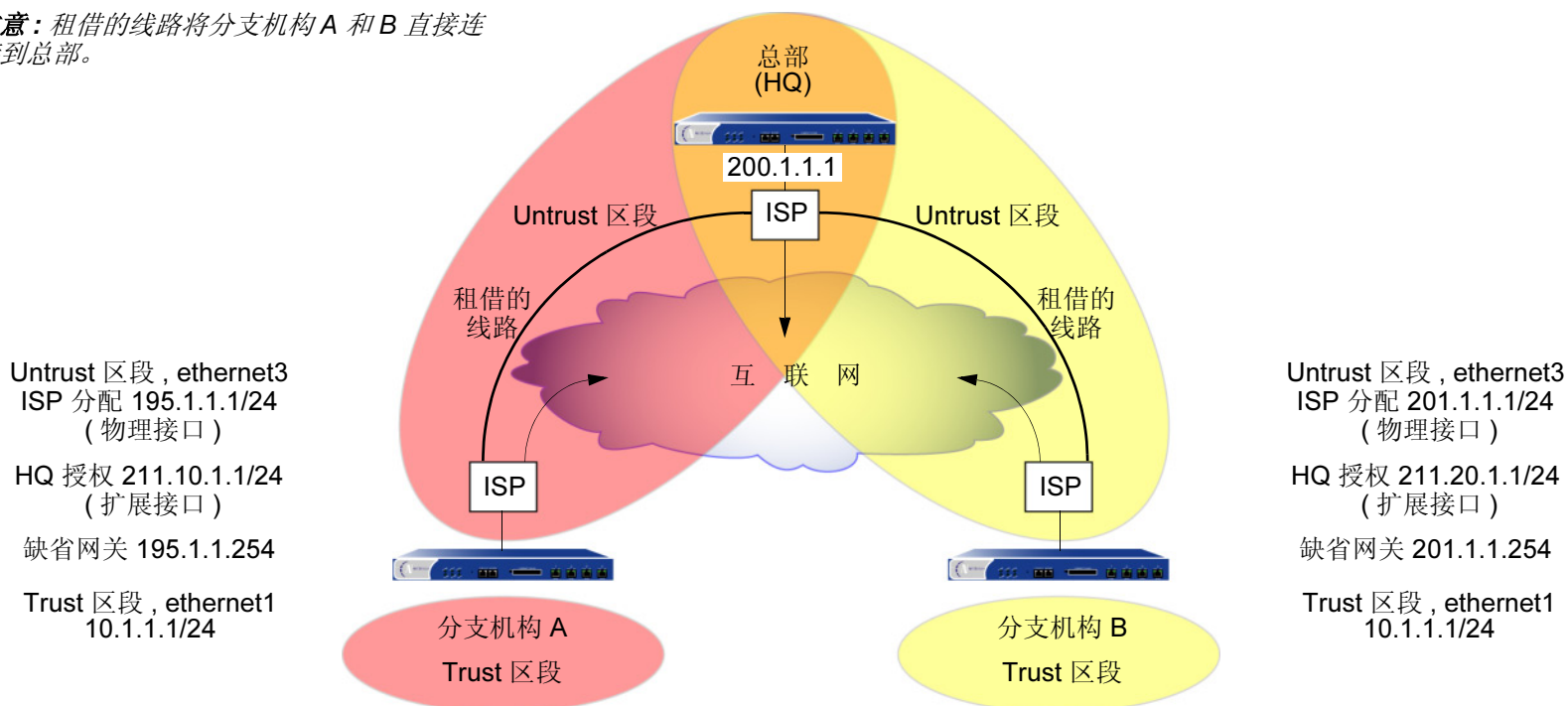
	分配的 IP 地址 (从 ISP) 用于 Untrust 区段物理接口	授权的 IP 地址 (从总部) 用于 Untrust 区段扩展接口 DIP
分支机构 A	195.1.1.1/24	211.10.1.1/24
分支机构 B	201.1.1.1/24	211.20.1.1/24

两个站点的 NetScreen 设备都有 Trust 区段和 Untrust 区段。所有安全区域都在 trust-vr 路由域中。将 ethernet1 绑定到 Trust 区段并分配 IP 地址 10.1.1.1/24。将 ethernet3 绑定到 Untrust 区段并给定由 ISP 分配的 IP 地址：“分支机构 A”为 195.1.1.1/24，“分支机构 B”为 201.1.1.1/24。然后在 ethernet3 上创建具有 DIP 池的扩展接口，该池包含授权 IP 地址：

- 分支机构 A: 扩展接口 IP 211.10.1.10/24; DIP 池 211.10.1.1 – 211.10.1.1; PAT 已启用
- 分支机构 B: 扩展接口 IP 211.20.1.10/24; DIP 池 211.20.1.1 – 211.20.1.1; PAT 已启用

设置 Trust 区段接口模式为 NAT。它使用 Untrust 区段接口 IP 地址充当其所有出站信息流的源地址 (发送至总部的信息流除外)。配置一个到达总部的策略, 将源地址转换为扩展接口 DIP 池中的地址。(DIP 池的 ID 号是 5。它包含一个 IP 地址, 使用端口地址转换后, 它可为 64,500 台主机处理会话。) 总部用于入站信息流的 MIP 地址是 200.1.1.1, 它是您在每个 NetScreen 设备的 Untrust 区段通讯簿中输入的 “HQ”。

注意: 租借的线路将分支机构 A 和 B 直接连接到总部。



注意: 为了使用该租借线路, 每个 ISP 都必须为流向租借线路端点网站的信息流设置路由。ISP 将他们从本地 NetScreen 设备接收到的任何其它信息流发送到互联网。

WebUI (分支机构 A)

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **OK**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 195.1.1.1/24

Interface Mode: 路由

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5

IP Address Range: 211.10.1.1 ~ 211.10.1.1

Port Translation: (选择)

Extended IP/Netmask: 211.10.1.10/255.255.255.0

2. 地址

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

Address Name: HQ

IP Address/Domain Name:

IP/Netmask: (选择), 200.1.1.1/32

Zone: Untrust

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 195.1.1.254

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), HQ

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

(DIP on): 5 (211.10.1.1-211.10.1.1)/X-late

WebUI (分支机构 B)

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **OK**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 201.1.1.1/24

Interface Mode: 路由

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容，然后单击 **OK**:

ID: 5

IP Address Range: 211.20.1.1 ~ 211.20.1.1

Port Translation: (选择)

Extended IP/Netmask: 211.20.1.10/255.255.255.0

2. 地址

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

Address Name: HQ

IP Address/Domain Name:

IP/Netmask: (选择), 200.1.1.1/32

Zone: Untrust

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 201.1.1.254

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), HQ

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

DIP On: (选择), 5 (211.20.1.1-211.20.1.1)/X-late

CLI (分支机构 A)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 195.1.1.1/24
set interface ethernet3 rout
set interface ethernet3 ext ip 211.10.1.10 255.255.255.0 dip 5 211.10.1.1
```

2. 地址

```
set address untrust hq 200.1.1.1/32
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 195.1.1.254
```

4. 策略

```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

CLI (分支机构 B)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 201.1.1.1/24
set interface ethernet3 route
set interface ethernet3 ext ip 211.20.1.10 255.255.255.0 dip 5 211.20.1.1
```

2. 地址

```
set address untrust hq 200.1.1.1/32
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.1.1.254
```

4. 策略

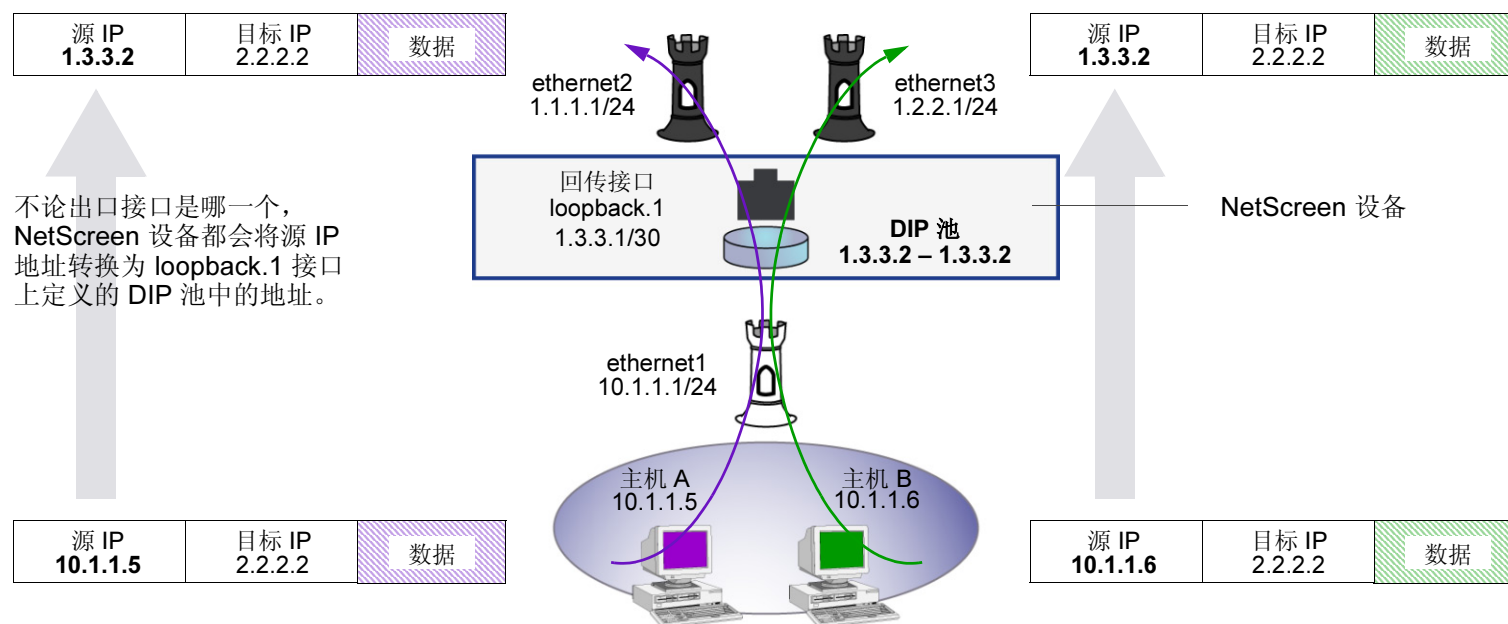
```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

回传接口和 DIP

回传接口是一个逻辑接口，只要其所在的设备开启，该接口始终处于工作中的状态¹²。可以在回传接口上创建动态 IP (DIP) 地址池，这样在执行源地址转换时，属于其相关回传接口组的接口组即可访问该池。**NetScreen** 设备从这类 DIP 池中提取的地址与回传接口 IP 地址处于相同的子网中，而不是在任何成员接口的子网中。(请注意，DIP 池中的地址不能与接口 IP 地址或任何已在回传接口定义的 MIP 地址重叠。)

将 DIP 池放置在回传接口上的主要应用是将源地址转换为相同地址或地址范围，尽管不同的封包可能会使用不同的出口接口。

使用回传接口上的 DIP 池转换源地址



12. 有关回传接口的信息，请参阅第 103 页上的“回传接口”。

范例：回传接口上的 DIP

在本例中，NetScreen 设备从不同的互联网服务提供商 (ISP) 接收到两个 Untrust 区段接口的 IP 地址：ISP-1 和 ISP-2:

- ethernet2, 1.1.1.1/24, ISP-1
- ethernet3, 1.2.2.1/24, ISP-2

将这些接口绑定到 Untrust 区段，然后为其分配上述 IP 地址。还要将 ethernet1 绑定到 Trust 区段并为其分配 IP 地址 10.1.1.11/24。

您希望 NetScreen 设备将 Trust 区段中的出站信息流中的源地址转换为 Untrust 区段中的远程办公室。转换的地址必须是相同的 IP 地址 (1.3.3.2)，因为远程办公室的策略仅允许来自该 IP 地址的进站信息流。您先前已经获得公开 IP 地址 1.3.3.1 和 1.3.3.2，并且已经通知两个 ISP，您除了使用他们分配给设备的地址外，也使用这些地址。

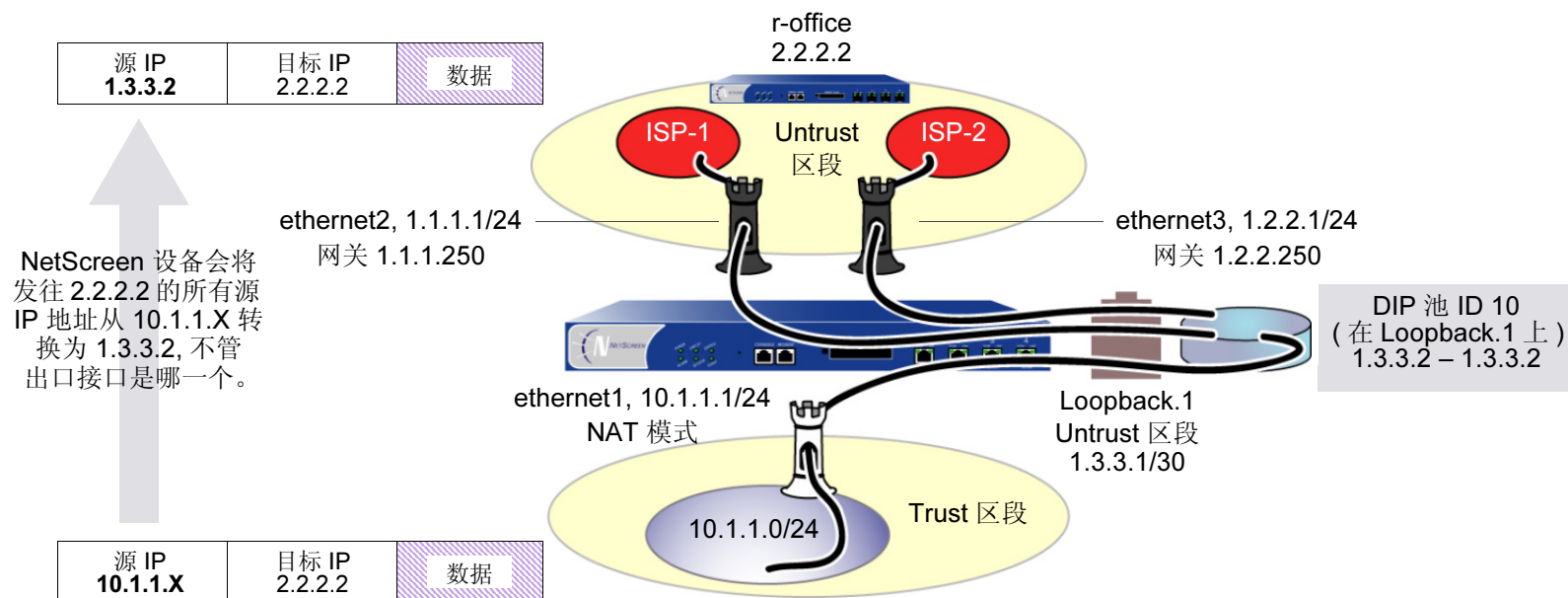
用 IP 地址 1.3.3.1/30 配置回传接口 loopback.1，用 1.3.3.2 – 1.3.3.2 配置该接口上的 DIP 池。DIP 池的 ID 号为 10。然后，将 ethernet1 和 ethernet2 加入 loopback.1 回传组，使其成为该组成员。

为名为 “r-office” 的远程办公室定义地址 (IP 地址为 2.2.2.2/32)，并为分别指向 ISP-1 和 ISP-2 路由器的 ethernet1 和 ethernet2 接口定义缺省路由。

为出站信息流定义要使用的两个网关路由。由于您对这两个路由并没有优先选择，因此不将度量加入路由中。出站信息流可能会流向任一个路由¹³。

最后，创建一个策略，该策略应用的源网络地址转换 (NAT-src) 是：将出站信息流转换为远程办公室。策略引用 DIP 池 ID 10。

13. 要指出路由优先级 (即将度量加入两个路由中)，请给首选路由较高的度量 — 即较接近于 1 的值。



WebUI

1. 接口

Network > Interfaces > New Loopback IF: 输入以下内容, 然后单击 **OK**:

Interface Name: loopback.1

Zone: Untrust (trust-vr)

IP Address/Netmask: 1.3.3.1/30

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **OK**:

As member of loopback group: loopback.1

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

As member of loopback group: loopback.1

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Interface Mode: 路由

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Interface Mode: 路由

2. DIP 池

Network > Interfaces > Edit (对于 loopback.1) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5

IP Address Range: 1.3.3.2 ~ 1.3.3.2

Port Translation: (选择)

3. 地址

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

Address Name: r-office

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.2/32

Zone: Untrust

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet2

Gateway IP address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 1.2.2.250

5. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), r-office

Service: ANY

Action: Permit

> Advanced: 输入以下内容, 然后单击 **Return**, 设置高级选项并返回基本配置页:

NAT:

Source Translation: (选择)

DIP On: (选择), 10 (1.3.3.2-1.3.3.2)/port-xlate

CLI

1. 接口

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.3.3.1/30

set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
set interface ethernet2 loopback-group loopback.1

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.2.2.1/24
set interface ethernet3 loopback-group loopback.1
```

2. DIP 池

```
set interface loopback.1 dip 10 1.3.3.2 1.3.3.2
```

3. 地址

```
set address untrust r-office 2.2.2.2/32
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet2 gateway 1.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.2.2.250
```

5. 策略

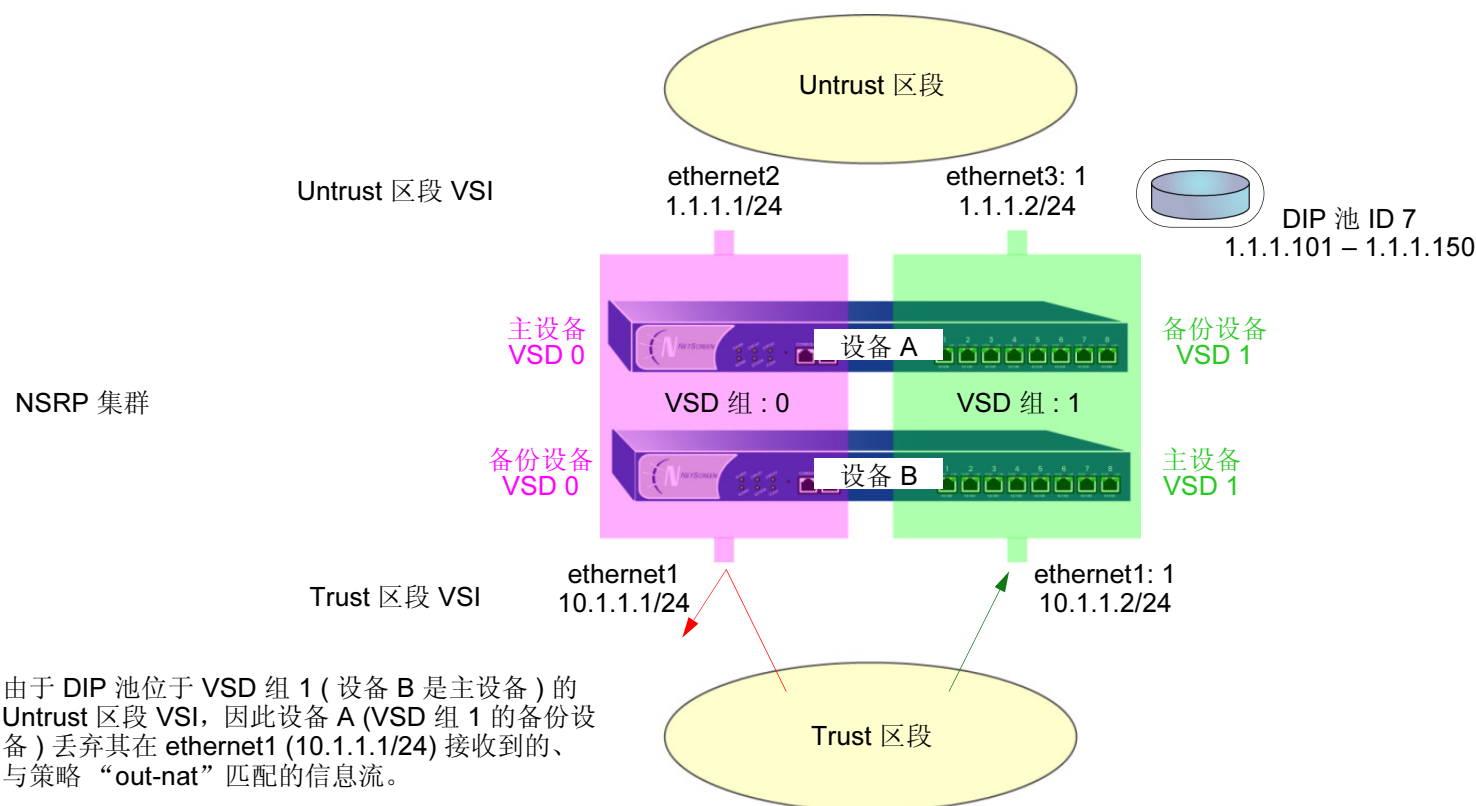
```
set policy from trust to untrust any r-office any nat src dip-id 10 permit
save
```

DIP 组

当您将两个 NetScreen 设备组成一个冗余集群，以提供双主动配置的高可用性 (HA) 时，两个设备都共享同一配置并且同时处理信息流。定义使用 DIP 池 (位于一个 VSI 上) 执行网络地址转换 (NAT) 的策略时，可能会出现这个问题。因为仅在 NetScreen 设备充当绑定 VSI 的 VSD 组的主设备时，该 VSI 才活动，因此任何发送到其它 NetScreen 设备 (充当该 VSD 组的备份设备) 的信息流无法使用该 DIP 池并被丢弃。

在 NSRP 集群中时，不当使用 DIP 池的策略：

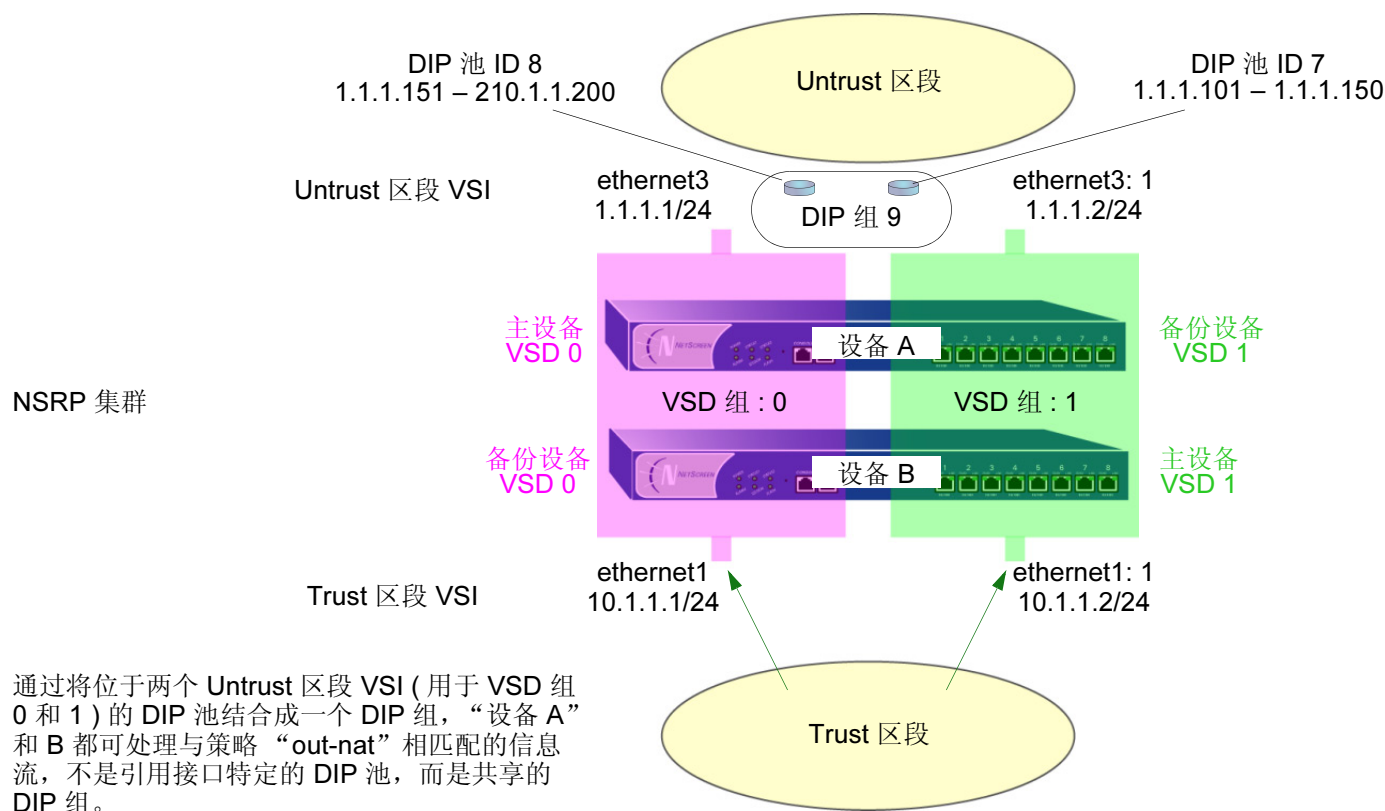
set policy name out-nat from trust to untrust any any nat src dip-id 7 permit



为了解决此问题，创建两个 DIP 池（一个在每个 VSD 组的 Untrust 区段 VSI 上），并将两个 DIP 池结合成一个 DIP 组，以在策略中引用。即使策略指定 DIP 组，每个 VSI 仍使用其自己的 VSD 池。

在 NSRP 集群中时，策略中 DIP 组的推荐用法：

set policy name out-nat from trust to untrust any any nat dip-id 9 permit



注意：有关为 HA 设置 NetScreen 设备的详细信息，请参阅第 8 卷，“高可用性”。

范例 : DIP 组

在本例中, 在双活动 HA 对的两个 NetScreen 设备 (设备 A 和 B) 上提供 NAT 服务。

创建两个 DIP 池 — ethernet3 上的 DIP 5 (1.1.1.20 – 1.1.1.29), ethernet3: 1 上的 DIP 6 (1.1.1.30 – 1.1.1.39)。然后将它们组合成一个 DIP 组并标识为 DIP 7, 在策略中引用。

VSD 组 0 和 1 的 VSI 如下 :

- Untrust 区段 VSI ethernet3 1.1.1.1/24 (VSD 组 0)
- Untrust 区段 VSI ethernet3: 1 1.1.1.1/24 (VSD 组 1)
- Trust 区段 VSI ethernet1 10.1.1.1/24 (VSD 组 0)
- Trust 区段 VSI ethernet1: 1 10.1.1.1/24 (VSD 组 1)

本例假设已设置 NSRP 集群中的设备 A 和 B, 创建 VSD 组 1 (将设备置入 NSRP 集群时, NetScreen 自动创建 VSD 组 0), 并配置上述接口。(有关为 NSRP 配置 NetScreen 设备的信息, 请参阅第 8 卷, “高可用性”。)

WebUI

1. DIP 池

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5

IP Address Range: 1.1.1.20 – 1.1.1.29

Port Translation: (选择)

Network > Interfaces > Edit (对于 ethernet3:1) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 6

IP Address Range: 1.1.1.30 – 1.1.1.39

Port Translation: (选择)

注意: 本版发行时, 只能通过 CLI 定义 DIP 组。

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

DIP On: (选择), 7

CLI

1. DIP 池

```
set interface ethernet3 dip 5 1.1.1.20 1.1.1.29
set interface ethernet3: 1 dip 6 1.1.1.30 1.1.1.39
```

2. DIP 组

```
set dip group 7 member 5
set dip group 7 member 6
```

3. 策略

```
set policy from trust to untrust any any any nat src dip-id 7 permit
save
```

时间表

时间表是一个可配置的对象，可将其与一个或多个策略相关联以定义策略生效的时间。通过应用时间表，可以控制网络信息流并确保网络安全。

定义时间表时，请输入下列参数的值：

Schedule Name: 出现在 **Policy Configuration** 对话框的 **Schedule** 下拉列表中的名称。请选择描述性的名称以帮助识别时间表。名称必须是唯一的，并且限制在 19 个字符以内。

Comment: 要添加的任何额外信息。

Recurring: 在希望时间表每周重复时启用此项。

Start and End Times: 必须配置开始和结束时间。同一天内最多可指定两个时间段。

Once: 希望时间表只开始和结束一次时启用此项。

mm/dd/yyyy hh:mm: 必须输入开始和停止的日期和时间。

范例：循环时间表

在本例中，有一个名为 **Tom** 的短期职员，他在下班后使用公司的互联网进行私人访问。创建非上班时间的时间表，然后关联策略，以拒绝发自该职员计算机 (10.1.1.5/32) 的、正常上班时间以外的出站 **TCP/IP** 信息流。

WebUI

1. 时间表

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

Schedule Name: After Hours

Comment: For non-business hours

Recurring: (选择)

周期 1:

Week Day	Start Time	End Time
Sunday	00:00	23:59
Monday	00:00	06:00
Tuesday	00:00	06:00
Wednesday	00:00	06:00
Thursday	00:00	06:00
Friday	00:00	06:00
Saturday	00:00	23:59

周期 2:

Week Day	Start Time	End Time
Sunday	17:00	23:59
Monday	17:00	23:59
Tuesday	17:00	23:59
Wednesday	17:00	23:59
Thursday	17:00	23:59
Friday	17:00	23:59
Saturday	17:00	23:59

2. 地址

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

Address Name: Tom

Comment: Temp

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: No Net

Source Address:

Address Book Entry: (选择), Tom

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Deny

Schedule: After Hours

CLI

1. 时间表

```
set schedule "after hours" recurrent sunday start 00:00 stop 23:59
set schedule "after hours" recurrent monday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule "after hours" recurrent tuesday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule "after hours" recurrent wednesday start 00:00 stop 06:00 start
    17:00 stop 23:59
set schedule "after hours" recurrent thursday start 00:00 stop 06:00 start
    17:00 stop 23:59
set schedule "after hours" recurrent friday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule "after hours" recurrent saturday start 00:00 stop 23:59 comment
    "for non-business hours"
```

2. 地址

```
set address trust tom 10.1.1.5/32 "temp"
```

3. 策略

```
set policy from trust to untrust tom any http deny schedule "after hours"
save
```

策略

NetScreen 设备的缺省行为是拒绝安全区内部的所有信息流 (区段内部信息流)¹ (Untrust 区段内的信息流除外), 并允许绑定到同一区段的接口间的所有信息流 (区段内部信息流)。为了允许选定的区段内部信息流通过 NetScreen 设备, 必须创建覆盖缺省行为的区段内部策略。同样, 为了防止选定的区段内部信息流通过 NetScreen 设备, 必须创建区段内部策略。

本章介绍各种策略的功能以及组成策略的不同元素是如何关联的。本章分为以下几个部分:

- 第 215 页上的 “基本元素”
- 第 216 页上的 “三种类型的策略”
 - 第 216 页上的 “区段内部策略”
 - 第 217 页上的 “区段内部策略”
 - 第 217 页上的 “全局策略”
- 第 218 页上的 “策略组列表”
- 第 219 页上的 “策略定义”
 - 第 219 页上的 “策略和规则”
 - 第 220 页上的 “策略的结构”
- 第 231 页上的 “策略应用”
 - 第 231 页上的 “查看策略”
 - 第 232 页上的 “创建策略”
 - 第 250 页上的 “输入策略环境”

1. 在缺省情况下, NetScreen-5XP 和 NetScreen-5XT 允许从 Trust 区段到 Untrust 区段的信息流。

- 第 251 页上的 “每个策略组件含多个条目”
- 第 252 页上的 “地址排除”
- 第 256 页上的 “修改和禁用策略”
- 第 257 页上的 “策略验证”
- 第 258 页上的 “重新排序策略”
- 第 259 页上的 “移除策略”

基本元素

允许、拒绝或设置² 两点间指定类型单向信息流的策略。信息流 (或 “服务”) 的类型、两端点的位置以及调用的动作构成了策略的基本元素。尽管可以有其它组件，但是共同构成策略核心部分的必要元素如下：

- **Direction** – 两个安全区 (从源区段到目的区段) 间信息流的方向
- **Source address** – 信息流发起的地址
- **Destination address** – 信息流发送到的地址
- **Service** – 信息流传输的类型
- **Action** – NetScreen 设备接收到满足头四个标准的信息流时执行的动作，这些标准为 : **permit**、**deny** 或 **tunnel**

例如，在下列 CLI 命令中声明的策略允许 FTP 信息流从 Trust 区段中的任何地址流向 DMZ 区段中名为 “server1” 的 FTP 服务器：

set policy from trust to untrust any server1 ftp permit

- **Direction: from trust to untrust** (即从 Trust 区段到 Untrust 区段)
- **Source Address: any** (即 Trust 区段中的任何地址。术语 “any” 代表应用到区段中任何地址的预定义地址)
- **Destination Address: server1** (Untrust 区段通讯簿中用户定义的地址)
- **Service: ftp** (文件传输协议)
- **Action: permit** (NetScreen 设备允许此信息流通过其防火墙)

2. “tunnel” 动作 (VPN 或 L2TP 通道)，隐含 permit (允许) 的概念。

三种类型的策略

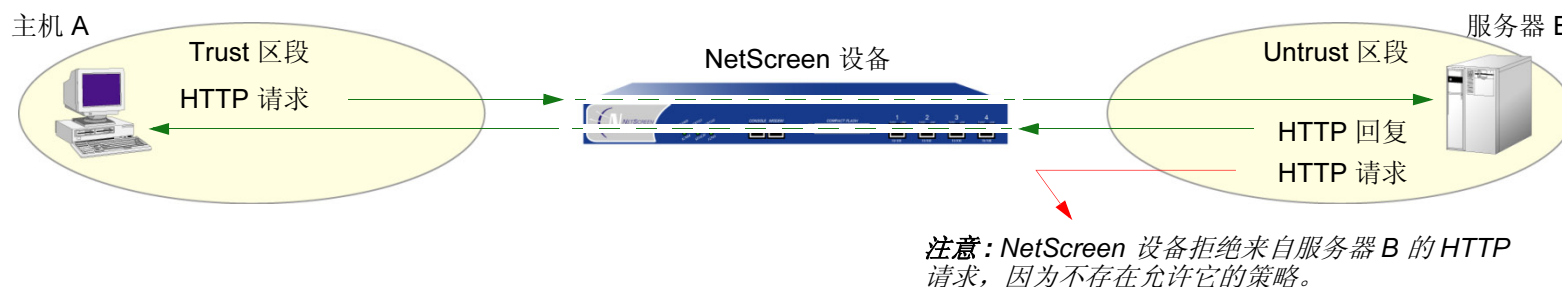
可通过以下三种策略控制信息流的流动：

- 通过创建区段内部策略，可以管理允许从一个安全区到另一个安全区的信息流的种类。
- 通过创建区段内部策略，也可以控制允许通过绑定到同一区段的接口间的信息流的类型。
- 通过创建全局策略，可以管理地址间的信息流，而不考虑它们的安全区。

区段内部策略

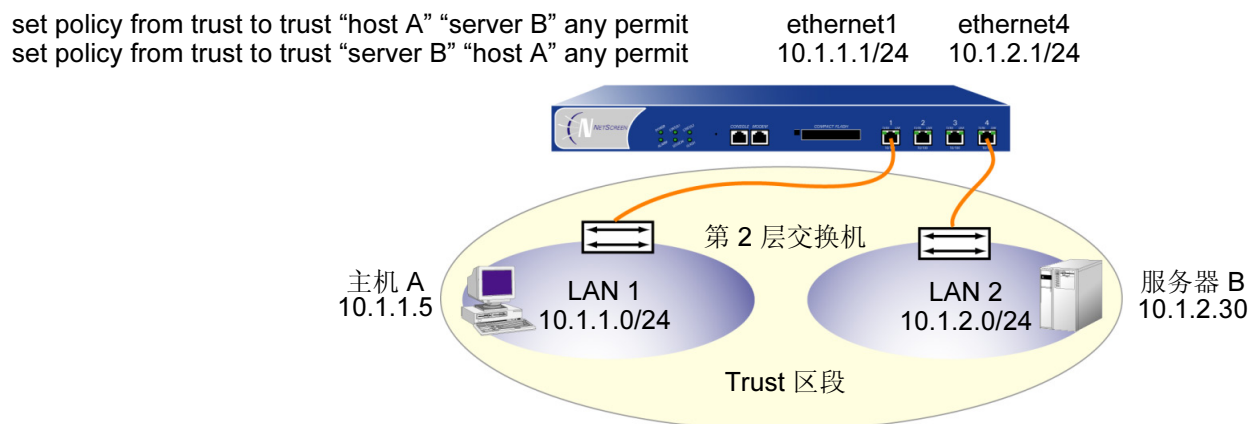
区段内部策略提供对安全区内部信息流的控制。可以设置区段内部策略来允许、拒绝或设置从一个区段到另一个区段的信息流。使用状态式检查技术，**NetScreen** 设备保持活动 TCP 会话表和活动 UDP “pseudo” 会话表，以便允许它能回应服务请求。例如，如果有一个策略允许从 **Trust** 区段中的主机 A 到 **Untrust** 区段中的服务器 B 的 HTTP 请求，则当 **NetScreen** 设备接收到从服务器 B 到主机 A 的 HTTP 回应时，**NetScreen** 设备将接收到的封包与它的表进行对照检查。当找到回应批准 HTTP 请求的封包时，**NetScreen** 设备允许来自 **Untrust** 区段中服务器 B 的封包穿越防火墙到达 **Trust** 区段中的主机 A。要允许由服务器 B 发起的流向主机 A 的信息流（不只是回应由主机 A 发起的信息流），必须创建从 **Untrust** 区段中服务器 B 到 **Trust** 区段中主机 A 的第二个策略。

```
set policy from trust to untrust "host A" "server B" http permit
```



区段内部策略

区段内部策略提供对绑定到同一安全区的接口间信息流的控制。源地址和目的地址都在同一安全区中，但是通过 **NetScreen** 设备上的不同接口到达。与区段内部策略一样，区段内部策略也控制信息流单向流动。要允许从数据路径任一端发起的信息流，必须创建两个策略，每个方向一个策略。



在接口级设置时 (**set interface interface nat**)，区段内部策略不支持 VPN 通道或源网络地址转换 (NAT-src)。但是，区段内部策略支持基于策略的 NAT-src 和 NAT-dst。当策略将映射 IP (MIP) 引用为目的地址时，它们还支持目的地地址转换。(有关 NAT-src、NAT-dst 和 MIP 的信息，请参阅第 261 页上的“地址转换”。)

全局策略

与区段内部和区段内部策略不同，全局策略不引用特定的源和目的区段。全局策略引用用户定义的 **Global** 区段地址或预定义的 **Global** 区段地址 “any”。这些地址可以跨越多个安全区。例如，如果要提供对多个区段的访问或从多个区段进行访问，则可以创建具有 **Global** 区段地址 “any” 的全局策略，它包含所有区段中的所有地址。

注意：本版本发行时，全局策略不支持源网络地址转换 (NAT-src)、VPN 通道或“透明”模式。不过，可以将 MIP 或 VIP 指定为全局策略中的目的地地址。

策略组列表

NetScreen 设备维护三种不同的策略组列表，每种策略组列表对应于以下三种策略之一：

- 区段内部策略
- 区段内部策略
- 全局策略

NetScreen 设备接收到发起新会话的封包时，会记录入口接口，从而获知接口所绑定的源区段。然后 NetScreen 设备执行路由查询以确定出口接口，从而确定该接口所绑定的目的区段。使用源区段和目的区段，NetScreen 设备可以执行策略查找，按以下顺序查阅策略组列表：

1. 如果源区段和目的区段不同，则 NetScreen 设备在区段内部策略组列表中执行策略查找。

(或)

如果源区段和目的区段相同，则 NetScreen 设备在区段内部策略组列表中执行策略查找。

2. 如果 NetScreen 设备执行区段内部或区段内部策略查找，但是没有找到匹配策略，则 NetScreen 设备会检查全局策略组列表以查找匹配策略。
3. 如果 NetScreen 设备执行区段内部和全局策略查找，但是没有找到匹配项，NetScreen 设备会将缺省的允许 / 拒绝策略应用到封包：**unset/set policy default-permit-all**。

(或)

如果 NetScreen 设备执行区段内部和全局策略查找，但是没有找到匹配策略，NetScreen 设备会将该区段的区段内部阻塞设置应用到封包：**unset/set zone zone block**。

NetScreen 设备从上至下搜索每个策略组列表。因此，必须在列表中将较为特殊的策略定位在不太特殊的策略上面。(有关策略顺序的信息，请参阅第 258 页上的“重新排序策略”。)

策略定义

防火墙提供具有单个进入和退出点的网络边界。由于所有信息流都必须通过此点，因此可以筛选并引导通过执行策略组列表（区段内部策略、内部区段策略和全局策略）产生的信息流。

策略能允许、拒绝、加密和解密、认证、排定优先次序、调度、过滤以及监控尝试从一个安全区流到另一个安全区的信息流。可以决定哪些用户和数据能进出，以及它们进出的时间和地点。

注意：对于支持虚拟系统的 **NetScreen** 设备，根系统中的策略组不影响虚拟系统中的策略组。

策略和规则

单个用户定义的策略内部生成一个或多个逻辑规则，而每个逻辑规则都由一组组件（源地址、目的地址和服务）组成。组件占用内存资源。引用组件的逻辑规则不占用内存资源。

根据源地址组、目的地址组和策略中服务组件的多个条目或组的使用，逻辑规则的数量可比创建单个策略时明显可见的大得多。例如，以下策略产生 125 个逻辑规则：

1 个策略 : 5 个源地址 x 5 个目的地址 x 5 个服务 = 125 个逻辑规则

但是，**NetScreen** 设备不为每个逻辑规则复制组件。规则以不同的组合使用同一组组件。例如，产生 125 个逻辑规则的上述策略只生成 15 个组件：

5 个源地址 + 5 个目的地址 + 5 个服务 = 15 个组件

这 15 个组件以不同方式组合，生成由单个策略产生的 125 个逻辑规则。允许多个逻辑规则以不同组合使用同一组组件，与每个逻辑规则与其组件具有一对一关系相比，**NetScreen** 设备占用的资源少得多。

由于新策略的安装时间与 **NetScreen** 设备添加、删除或修改的组件数量成比例，因此组件较少策略的安装更快。同样，与每个规则都需要专用组件相比，通过允许大量的逻辑规则共享一小组组件，**NetScreen** 使用户能创建更多的策略，**NetScreen** 设备能创建更多的规则。

策略的结构

策略必须包含下列元素：

- ID (自动生成的，但可能是 CLI 中用户定义的)
- 区段 (源区段和目的区段)
- 地址 (源地址和目的地址)
- 服务
- 动作 (permit、deny、tunnel)

策略也可包含下列元素：

- 应用
- 名称
- VPN 通道确定
- L2TP 通道确定
- 深层检测
- 策略列表顶部位置
- 源地址转换
- 目的地址转换
- 用户认证
- HA 会话备份
- URL 过滤
- 记录
- 计数
- 信息流报警临界值
- 时间表
- 防病毒扫描
- 信息流整形

本节的余下部分将依次分析上述每一元素。

ID

不管是您定义还是 NetScreen 设备自动分配，每个策略都具有一个 ID 号。您只能为策略定义一个 ID 号，方法是通过 CLI 中的设置策略命令：**set policy id number ...** 知道 ID 号之后，即可输入策略环境以发出修改策略的其他命令。(有关策略环境的详细信息，请参阅第 250 页上的“输入策略环境”。)

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)、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)。策略允许信息流在两个安全区内部流动 (区段内部策略)，或在两个绑定到同一区段的接口间流动 (区段内部策略)。(有关详细信息，请参阅第 45 页上的“区段”、第 216 页上的“区段内部策略”和第 217 页上的“区段内部策略”。)

地址

地址是通过相对于防火墙 (在一个安全区中) 的位置，识别网络设备 (如主机和网络) 的对象。单个主机使用掩码 255.255.255.255 指定，表示所有 32 位地址都有意义。网络使用其子网掩码指定，指示有意义的位数。要为特定地址创建策略，必须首先在通讯簿中创建相关主机和网络的条目。

也可创建地址组，并将策略应用到地址组，就象应用到其它通讯簿条目一样。将地址组用作策略的元素时，应注意由于 NetScreen 设备将策略应用到组中的每个地址，可用的内部逻辑规则数和组成这些规则的组件数将会比预期更快耗尽。当源和目的地址都使用地址组时尤其危险。(有关详细信息，请参阅第 219 页上的“策略和规则”。)

服务

服务是使用第 4 层信息 (如应用程序服务 Telnet、FTP、SMTP 和 HTTP 的标准和公认的 TCP 和 UDP 端口号) 识别应用程序协议的对象。ScreenOS 包括预定义的核心互联网服务。另外，还可以定义定制服务。

可以定义策略，指定允许、拒绝、加密、认证、记录或统计哪些服务。

动作

动作是描述防火墙如何处理接收到的信息流的对象。

- **Permit** 允许封包通过防火墙。
- **Deny** 阻塞封包，使之不能通过防火墙。
- **Tunnel** 封装外向 IP 封包和解除内向 IP 封包的封装。对于 IPSec VPN 通道，指定要使用哪个 VPN 通道。对于 L2TP 通道，指定要使用哪个 L2TP 通道。对于 IPSec 上的 L2TP，指定一个 IPSec VPN 通道和一个 L2TP 通道³。

NetScreen 设备将指定动作应用到与预先提供的标准匹配的信息流，这些标准为：区段（源区段和目的区段）、地址（源地址和目的地址）以及服务。

应用

应用选项指定映射到策略中引用的第 4 层服务的第 7 层应用。预定义服务已经有到第 7 层应用的映射。不过，对于定制服务，必须将服务明确链接到应用程序，尤其是希望策略将应用层网关 (ALG⁴) 或“深层检测”应用于定制服务时。

将 ALG 应用于定制服务包括以下两个步骤：

- 使用名称、超时值、传输协议和源端口及目的端口定义定制服务
- 配置策略时，引用该服务和希望应用的 ALG 的应用类型

有关将“深层检测”应用于定制服务的信息，请参阅第 4-156 页上的“将定制服务映射到应用程序”。

3. 对于 IPSec 上的 L2TP，IPSec VPN 通道的源地址和目的地址必须与 L2TP 通道的源地址和目的地址相同。

4. NetScreen 支持多个服务的 ALG，包括 DNS、FTP、H.323、HTTP、RSH、SIP、telnet 和 TFTP。

名称

可以给策略一个描述性的名称，便于识别该策略。

注意：有关 ScreenOS 命名约定的信息—适用于为策略创建的名称—请参阅第 xiv 页上的“命名约定和字符类型”。

VPN 通道确定

可以将单个或多个策略应用到已配置的任何 VPN 通道。在 WebUI 中，VPN Tunnel 选项提供所有这些通道的下拉列表。在 CLI 中，可以用 **get vpn** 命令查看所有可用的通道。(有关详细信息，请参阅第 5-69 页上的“站点到站点 VPN”和第 5-199 页上的“拨号 VPN”。)

当 VPN 通道两端的 VPN 配置都使用基于策略的 NAT 时，两个网关设备的管理员都需要创建入站和出站策略 (总共四个策略)。当 VPN 策略构成匹配对 (即，除源地址和目的地址反向外，入站和出站策略配置中的任何内容都相同) 时，可以配置一个策略，然后选择 **Modify matching bidirectional VPN policy** 复选框，自动为相反方向创建第二个策略。对于新策略的配置，**matching VPN policy** 复选框在缺省情况下是清除的。对于是匹配对成员的现有策略的修改，在缺省情况下，复选框被选中，并且对一个策略所作的更改会传播到另一个策略。

注意：此选项只能通过 WebUI 获得。以下任一策略组件的有多个条目时不可用：源地址、目的地址或服务。

L2TP 通道确定

可以将单个或多个策略应用到已配置的任何“第 2 层通道协议 (L2TP)”通道。在 WebUI 中，L2TP 选项提供所有这些通道的下拉列表。在 CLI 中，可以用 **get l2tp all** 命令查看所有可用的通道。也可以将 VPN 通道和 L2TP 通道组合在一起 (如果两者都具有相同的端点)，创建结合每个通道特征的通道。这称为 IPSec 上的 L2TP。

注意：处于透明模式的 NetScreen 设备不支持 L2TP。

深层检测

“深层检测”是过滤网络和“传输层”允许的信息流的机制，不仅检查这些层，而且检查“应用层”的内容和协议特征⁵。“深层检测”的目的是检测和防护任何攻击或异常行为，它们可能存在于 NetScreen 防火墙允许的信息流中。有关详细信息，请参阅第 4-127 页上的“深层检测”。

要为攻击保护配置策略，必须进行两项选择：如果检测到攻击，要使用的攻击组和要采取的攻击行动。(有关“深层检测”的详细信息，请参阅第 4-127 页上的“深层检测”。)

策略列表顶部位置

在缺省情况下，NetScreen 将最近创建的策略定位在策略组列表的底部。如果需要重新定位策略，可以使用在第 258 页上的“重新排序策略”中说明的任一策略重新排序方法。在将最近创建的策略重新定位到策略列表的顶部时，为避免额外的步骤，可以在 WebUI 中选择 **Position at Top** 选项，或在 CLI 中的 **set policy** 命令中使用关键字 **top** (**set policy top ...**)。

5. 在“开放式系统互连”(OSI)模式中，“网络层”是第 3 层，“传输层”是第 4 层，“应用层”是第 7 层。OSI 模式是网络业在网络协议体系结构方面的标准模式。OSI 模式由七层组成。

源地址转换

可以在策略级应用源地址转换 (NAT-src)。使用 NAT-src，可以转换内向或外向网络和 VPN 信息流中的源地址。新的源地址可以来自动态 IP (DIP) 池或出口接口。NAT-src 还支持源端口地址转换 (PAT)。要了解所有可用的 NAT-src 选项，请参阅第 275 页上的“源网络地址转换”。

注意：还可在接口级执行源地址转换，称为网络地址转换 (NAT)。有关接口级 NAT-src 或只是 NAT 的信息，请参阅第 126 页上的“NAT 模式”。

目的地址转换

可以在策略级应用目的地址转换 (NAT-dst)。使用 NAT-dst，可以转换内向或外向网络和 VPN 信息流中的目的地址。NAT-dst 还支持目的地端口映射。要了解所有可用的 NAT-dst 选项，请参阅第 292 页上的“目的网络地址转换”。

用户认证

选择此选项要求源地址的 auth 用户，在允许信息流穿越防火墙或进入 VPN 通道前，通过提供用户名和密码，以认证他 / 她的身份。NetScreen 设备可使用本地数据库或外部 RADIUS、SecurID 或 LDAP auth 服务器，执行认证检查。

注意：如果要将需要认证的策略应用到 IP 地址的子网，则该子网中的每个 IP 地址都需要认证。

如果主机支持多个 auth 用户帐户 (如运行 Telnet 的 Unix 主机)，则在 NetScreen 设备对第一个用户进行认证后，该主机的所有其它用户都可以继承第一个用户的权限，让信息流通过 NetScreen 设备而不必经过认证。

NetScreen 提供两种认证方案：

- 运行时认证，在收到与启用认证的策略相匹配的 HTTP、FTP 或 Telnet 信息流时，NetScreen 设备提示 auth 用户登录
- WebAuth，通过 NetScreen 设备发送信息流前，用户必须认证自己

运行时认证

运行时认证的过程如下：

1. 当 auth 用户发送 HTTP、FTP 或 Telnet 连接请求到目的地址时，NetScreen 设备截取封包并对其进行缓冲。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备认证 auth 用户的登录信息。

如果认证成功，则在 auth 用户和目的地址间建立连接。

对于初始的连接请求，策略必须包括下列三个服务中的一项或所有服务：Telnet、HTTP 或 FTP。只有具有这些服务中的一个或所有服务的策略才能启动认证过程。可以在涉及用户认证的策略中使用以下任一服务：

- Any (因为 “any” 包括所有三项必需的服务)
- Telnet、HTTP 或 FTP。
- 包括所希望的服务或多个服务的服务组，加上启动认证过程必需的三个服务中的一个或多个 (Telnet、FTP 或 HTTP)。例如，可以创建名为 “Login” 的定制服务组，支持 FTP、网络会议系统和 H.323 服务。然后，在创建策略时，指定服务为 “Login”。

对于成功认证后的任何连接，策略中指定的所有服务都有效。

注意：启用了认证的策略不支持将 DNS (端口为 53) 作为服务。

策略前检查认证 (WebAuth)

WebAuth 认证的过程如下：

1. auth 用户为 WebAuth 服务器建立到 IP 地址的 HTTP 连接。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备或外部 auth 服务器认证 auth 用户的登录信息。

如果认证尝试成功，则 NetScreen 设备允许 auth 用户启动信息流，使其流向在强制通过 WebAuth 方法执行认证的策略中指定的目的位置。

注意：有关这两种用户认证方法的详细信息，请参阅第 414 页上的“Auth 用户和用户组”。

通过选择特定的用户组、本地或外部用户或组表达式，可以限制或扩展应用策略的 auth 用户的范围。(有关组表达式的信息，请参阅第 484 页上的“组表达式”。) 如果在策略中没有引用 auth 用户或用户组 (在 WebUI 中，选择 **Allow Any** 选项)，则策略应用到指定 auth 服务器中的所有 auth 用户。

注意：NetScreen 用 auth 用户登录的主机的 IP 地址链接认证权限。如果 NetScreen 设备认证来自某 NAT 设备后主机的用户，且该 NAT 设备对所有 NAT 指派都使用同一个 IP 地址，则该 NAT 设备后其它主机的用户自动具有相同的权限。


HA 会话备份

当两台 NetScreen 设备都在高可用性 (HA) 的 NSRP 集群中时，可以指定哪个会话要备份，哪个会话不要备份。对于不想备份的会话的信息流，应用 HA 会话备份选项禁用的策略。在 WebUI 中，清除 **HA Session Backup** 复选框。在 CLI 中，在 **set policy** 命令中使用 **no-session-backup** 参数。在缺省情况下，NSRP 集群中的 NetScreen 设备备份会话。

URL 过滤

NetScreen 利用 Websense Enterprise Engine 支持 URL 过滤，根据站点的 URL、域名和 IP 地址，Websense Enterprise Engine 可以阻止或允许访问不同的站点。启用策略上的 URL 过滤时，NetScreen 设备缓冲所有 HTTP GET 请求（在应用此策略的信息流中），并将 URL 发送到 Websense 服务器。Websense 服务器将 URL 与其数据库进行比较。如果 URL 与受限制的 URL 匹配，则 Websense 服务器通知 NetScreen 设备，该设备向源地址和目的地址发送 TCP RST 以关闭 TCP 连接。NetScreen 设备也向源地址发送“blocked URL”消息。如果 URL 与受限制的 URL 不匹配，则 Websense 服务器将“permit”消息返回到 NetScreen 设备，然后设备将缓冲的 HTTP 封包转发到其预定目的地。

记录

在策略中启用记录时，NetScreen 设备记录应用特定策略的所有连接。可通过 WebUI 或 CLI 查看日志。在 WebUI 中，单击 **Reports > Policies** > （对于要查看其日志的策略）。在 CLI 中，使用 **get log traffic policy id_num** 命令。

注意：有关查看日志和图表的详细信息，请参阅第 3-65 页上的“监控 NetScreen 设备”。

计数

在策略中启用计数时，NetScreen 设备计算应用此策略的信息流的总字节数，并将信息记录在历史记录图表中。要在 WebUI 中查看策略的历史记录图表，请单击 **Reports > Policies** > （对于要查看其信息流计数的策略）。

信息流报警临界值

可以设置当策略允许的信息流超过指定的每秒字节数、每分钟字节数（或两者）时，触发警报的临界值。由于信息流报警要求 NetScreen 设备监控字节总数，因此也必须启用计数功能。

注意：有关信息流报警的详细信息，请参阅第 3-82 页上的“信息流报警”。

时间表

通过将时间表与策略相关联，可以确定策略生效的时间。可以将时间表配置为循环生效，也可配置为单次事件。时间表为控制网络信息流的流动以及确保网络安全提供了强有力的工具。在稍后的一个范例中，如果您担心职员向公司外传输重要数据，则可设置一个策略，阻塞正常上班时间以外的出站 **FTP-Put** 和 **MAIL** 信息流。

在 **WebUI** 中，在 **Objects > Schedules** 部分中定义时间表。在 **CLI** 中，使用 **set schedule** 命令。

注意：在 WebUI 中，已排定进度的策略如有灰色背景，表示当前时间不在定义的时间表内。已排定进度的策略活动时，背景为白色。

防病毒扫描

使用 Trend Micro InterScan VirusWall 扫描器 (版本 3.6)，某些 NetScreen 设备可以支持在 **SMTP** 和 **HTTP** 信息流中进行防病毒 (AV) 扫描。NetScreen 设备收到应用防病毒阻塞策略的信息流时，将信息流发送到 VirusWall 防病毒扫描器。扫描器收到 **SMTP** 或 **HTTP** 封包的全部内容后，通过与其病毒模式数据库进行比较来检查病毒的数据。如果扫描器发现问题，VirusWall 将隔离受感染的数据以供进一步研究，并将 **SMTP** 或 **HTTP** 文件 (不含受感染的数据) 返回到 NetScreen 设备。然后 NetScreen 设备将该文件转发到预定接收者。

某些 NetScreen 设备支持内部 AV 扫描器，可以配置此扫描器以过滤 **POP3**、**SMTP** 和 **HTTP** 信息流。如果嵌入的 AV 扫描器检测到病毒，将丢弃封包，并向发起信息流的客户端发送消息，报告病毒。

(有关防病毒扫描的详细信息，请参阅第 4-80 页上的“防病毒扫描”。有关 VirusWall 扫描器的详细信息，请参阅 Trend Micro 文档。)

信息流整形

可以为每个策略设置控制和整形信息流的参数。信息流整形参数包括：

Guaranteed Bandwidth: 以千比特每秒 (kbps) 表示的保障吞吐量。低于此临界值的信息流以最高优先级通过，不受任何信息流管理或整形机制的限制。

Maximum Bandwidth: 以千比特每秒 (kbps) 表示的连接类型可用的安全带宽。超过此临界值的信息流被抑制并丢弃。

注意：建议不要使用低于 10 kbps 的额定值。低于此临界值的额定值会导致封包被丢弃以及过多的重试，从而使信息流的管理目的失败。

Traffic Priority: 当信息流带宽在保障带宽和最大带宽设置之间时，NetScreen 设备首先让较高优先级的信息流通过，并且只有在没有其它更高优先级的信息流时，才让较低优先级的信息流通过。有八个优先级。

DiffServ Codepoint Marking: 差异服务 (DiffServ) 是标记信息流在优先级层次结构中位置的系统。可以将八个 NetScreen 优先级映射到 DiffServ 系统中。在缺省情况下，NetScreen 系统中的最高优先级 (优先级 0) 映射到 DiffServ 字段 (请参阅 RFC 2474) 中的头三位 (0111)，或映射到 IP 封包包头的 ToS 字节 (请参阅 RFC 1349) 的 IP 前字段中。NetScreen 系统中的最低优先级 (优先级 7) 映射到 ToS DiffServ 系统中的 (0000)。

注意：有关信息流管理和整形的更详细讨论，请参阅第 493 页上的“信息流整形”。

要更改 NetScreen 优先级和 DiffServ 系统间的映射，请使用以下 CLI 命令：

```
set traffic-shaping ip_precedence number0 number1 number2 number3 number4 number5  
number6 number7
```

其中 *number0* 是优先级 0 (TOS DiffServ 系统中的最高优先级) 的映射，*number1* 是优先级 1 的映射，依次类推。

策略应用

本节说明策略的管理：查看、创建、修改、排序和重新排序以及移除策略。








查看策略

要通过 WebUI 查看策略，请单击 **Policies**。通过从 **From** 和 **To** 下拉列表中选择区段名称，然后单击 **Go**，可以按源区段和目的区段分类显示策略。在 CLI 中，使用 **get policy [all | from zone to zone | global | id number]** 命令。

策略图标

查看策略列表时，WebUI 使用图标提供策略组件的图形化汇总。下表解释了策略页中使用的不同图标。

图标	功能	说明
	允许	NetScreen 设备通过应用该策略的所有信息流。
	拒绝	NetScreen 设备阻止应用该策略的所有信息流。
	策略级 NAT	NetScreen 设备对应用该策略的所有信息流都执行基于策略的源或目的网络地址转换 (NAT-src 或 NAT-dst)。
	封装和解封	NetScreen 设备封装所有出站 VPN 信息流并解封应用该策略的所有入站 VPN 信息流。
	双向 VPN 策略	存在相反方向的匹配 VPN 策略。

图标	功能	说明
	认证	用户在启动连接时必须认证自己。
	防病毒	NetScreen 设备将应用该策略的所有信息流发送到 Trend Micro 防病毒 (AV) 扫描器。
	深层检测	NetScreen 设备对应用该策略的所有信息流执行 “深层检测” (DI)。
	深层检测与防病毒	NetScreen 设备对应用该策略的所有信息流执行 “深层检测” 和防病毒保护。
	记录	如果启用，则记录所有信息流，并使其可用于系统日志和电子邮件。
	计数	NetScreen 设备计算 (以字节为单位) 应用该策略的信息流的量。
	信息流报警	指示已经设置信息流报警临界值。

创建策略

要允许信息流在两个区段内部流动，应在这些区段内部创建允许、拒绝或设置信息流的策略。如果 NetScreen 设备唯一能够设置 (在策略中引用的) 源和目的地址间区段内部信息流的路由的网络设备，则也可创建策略，控制同一区段内的信息流。也可创建全局策略，使用 Global 区段通讯簿中的源和目的地址。

要允许两个区段内部 (例如，Trust 和 Untrust 区段) 的双向信息流，需要创建从 Trust 到 Untrust 的策略，然后创建从 Untrust 到 Trust 的第二个策略。根据需要，两个策略可以使用相同或不同的 IP 地址，只是源地址和目的地址需反向。

策略位置

可以在同一系统（根或虚拟系统）中的任何区段内部定义策略。要在根系统和虚拟系统间定义策略，其中一个区段必须为共享区段。（有关与虚拟系统有关的共享区段的信息，请参阅第 7 卷，“虚拟系统”。）

范例：区段内部策略邮件服务

在本例中，将创建三个策略以控制电子邮件信息流。

第一个策略允许 **Trust** 区段中的内部用户发送并检索来自 **DMZ** 区段中本地邮件服务器的电子邮件。此策略允许来自内部用户的服务 **MAIL**（即 **SMTP**）和 **POP3** 穿越 **NetScreen** 防火墙到达本地邮件服务器。

第二个和第三个策略允许服务 **MAIL** 穿越 **DMZ** 区段中本地邮件服务器和 **Untrust** 区段中远程邮件服务器之间的防火墙。

不过，在创建策略控制不同安全区内部的信息流之前，必须首先设计应用那些策略的环境。第一，首先将接口绑定到区段并分配接口 IP 地址：

- 将 **ethernet1** 绑定到 **Trust** 区段并将其 IP 地址指派为 **10.1.1.1/24**。
- 将 **ethernet2** 绑定到 **DMZ** 区段并将其 IP 地址指派为 **1.2.2.1/24**。
- 将 **ethernet3** 绑定到 **Untrust** 区段并将其 IP 地址指派为 **1.1.1.1/24**。

所有安全区都在 **trust-vr** 路由选择域中。

第二，创建在策略中使用的地址：

- 在 **Trust** 区段中定义名为 “**corp_net**” 的地址并将其 IP 地址指派为 **10.1.1.0/24**。
- 在 **DMZ** 区段中定义名为 “**mail_svr**” 的地址并将其 IP 地址指派为 **1.2.2.5/32**。
- 在 **Untrust** 区段中定义名为 “**r-mail_svr**” 的地址并将其 IP 地址指派为 **2.2.2.5/32**。

第三，创建名为 “**MAIL-POP3**” 的服务组，包含两个预定义服务 **MAIL** 和 **POP3**。

第四，在 **trust-vr** 路由选择域中配置缺省路由，通过 **ethernet3**，指向 **1.1.1.250** 处的外部路由器。

完成步骤 1 – 4 之后，即可创建必需的策略，使受保护的网内外可传输、检索和发送电子邮件。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: corp_net

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

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

Address Name: mail_svr

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

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

Address Name: r-mail_svr

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 服务组

Objects > Services > Groups: 输入以下组名称，移动以下服务，然后单击 **OK**:

Group Name: MAIL-POP3

选择 **MAIL**，并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **POP3**，并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

Policies > (From: Trust, To: Untrust) > New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), corp_net

Destination Address:

Address Book Entry: (选择), mail_svr

Service: Mail-POP3

Action: Permit

Policies > (From: DMZ, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), mail_svr

Destination Address:

Address Book Entry: (选择), r-mail_svr

Service: MAIL

Action: Permit

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), r-mail_svr

Destination Address:

Address Book Entry: (选择), mail_svr

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address trust corp_net 10.1.1.0/24
set address dmz mail_svr 1.2.2.5/32
set address untrust r-mail_svr 2.2.2.5/32
```

3. 服务组

```
set group service MAIL-POP3
set group service MAIL-POP3 add mail
set group service MAIL-POP3 add pop3
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. 策略

```
set policy from trust to dmz corp_net mail_svr MAIL-POP3 permit
set policy from dmz to untrust mail_svr r-mail_svr MAIL permit
set policy from untrust to dmz r-mail_svr mail_svr MAIL permit
save
```

范例：区段内部策略设置

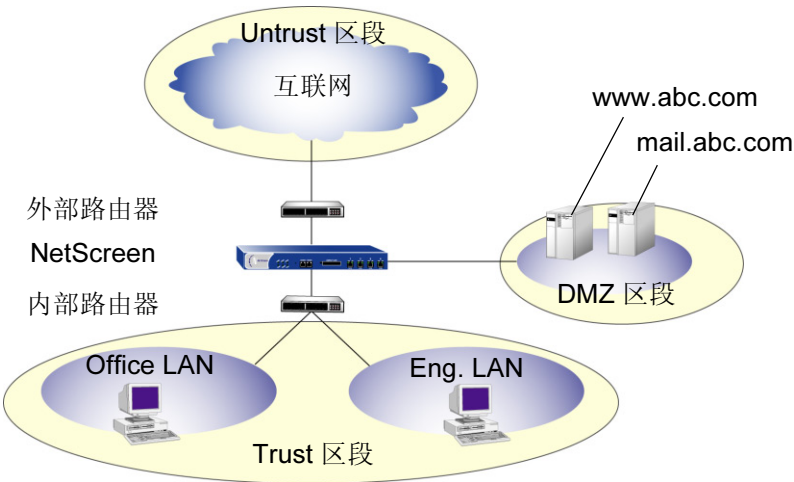
一个小的软件公司 (ABC Design) 已将其内部网络分成两个子网，这两个子网都在 **Trust** 区段中。这两个子网为：

- 工程 (定义地址为 “Eng”)
- 公司的其余部分 (定义地址为 “Office”)。

其 **Web** 和邮件服务器也有一个 **DMZ** 区段。

下例介绍了对以下用户的一组典型策略：

- “Eng” 可使用用于出站信息流的所有服务，FTP-Put、IMAP、MAIL 和 POP3 除外。
- “Office” 可使用电子邮件和访问 “互联网”，只要它们通过 WebAuth 认证自己。(有关 WebAuth 用户认证的信息，请参阅第 414 页上的 “Auth 用户和用户组”。)
- **Trust** 区段中的任何用户都可访问 **DMZ** 区段中的 **Web** 和邮件服务器。
- **Untrust** 区段中的远程邮件服务器可访问 **DMZ** 区段中的本地邮件服务器。
- 也有一组系统管理员 (定义地址为 “sys-admins”)，对 **DMZ** 区段中的服务器具有全部用户和管理访问权限。



本例仅重点介绍策略，并假定已经配置了的接口、地址、服务组和必需到位的路由。有关配置这些内容的详细信息，请参阅第 67 页上的“接口”、第 142 页上的“地址”、第 183 页上的“服务组”和第 29 页上的“路由表和静态路由”。

从区段 (源地址)	到区段 (目的地址)	服务	动作
Trust - Any	Untrust - Any	Com (服务组 : FTP-Put、IMAP、MAIL、POP3)	Deny
Trust - Eng	Untrust - Any	Any	Permit
Trust - Office	Untrust - Any	Internet (服务组 : FTP-Get、HTTP、HTTPS)	Permit (+ WebAuth)

从区段 (源地址)	到区段 (目的地址)	服务	动作
Untrust - Any	DMZ - mail.abc.com	MAIL	Permit
Untrust - Any	DMZ - www.abc.com	Web (服务组 : HTTP、HTTPS)	Permit

从区段 (源地址)	到区段 (目的地址)	服务	动作
Trust - Any	DMZ - mail.abc.com	e-mail (服务组 : IMAP、MAIL、POP3)	Permit
Trust - Any	DMZ - www.abc.com	Internet (服务组 : FTP-Get、HTTP、HTTPS)	Permit
Trust - sys-admins	DMZ - Any	Any	Permit

从区段 (源地址)	到区段 (目的地址)	服务	动作
DMZ - mail.abc.com	Untrust - Any	MAIL	Permit

注意：缺省策略为全部拒绝。

WebUI

1. 从 Trust，到 Untrust

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Eng

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Office

Destination Address:

Address Book Entry: (选择), Any

Service: Internet⁶

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

WebAuth: (选择)

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Com⁷

Action: Deny

Position at Top: (选择)

注意：对于从 *Untrust* 区段到 *Trust* 区段的信息流，缺省的拒绝策略拒绝所有信息流。

6. “Internet” 是具有以下成员的服务组：FTP-Get、HTTP 和 HTTPS。

7. “Com” 是具有以下成员的服务组：FTP-Put、MAIL、IMAP 和 POP3。

2. 从 Untrust, 到 DMZ

Policies > (From: Untrust, To: DMZ) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mail.abc.com

Service: MAIL

Action: Permit

Policies > (From: Untrust, To: DMZ) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), www.abc.com

Service: Web⁸

Action: Permit

8. “Web” 是具有以下成员的服务组: HTTP 和 HTTPS。

3. 从 Trust, 到 DMZ

Policies > (From: Trust, To: DMZ) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mail.abc.com

Service: e-mail⁹

Action: Permit

Policies > (From: Trust, To: DMZ) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), www.abc.com

Service: Internet

Action: Permit

9. “e-mail” 是具有以下成员的服务组: MAIL、IMAP 和 POP3。

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), sys-admins

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

4. 从 DMZ, 到 Untrust

Policies > (From: DMZ, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), mail.abc.com

Destination Address:

Address Book Entry: (选择), Any

Service: MAIL

Action: Permit

CLI

1. 从 Trust, 到 Untrust

```
set policy from trust to untrust eng any any permit
set policy from trust to untrust office any Internet10 permit webauth
set policy top from trust to untrust any any Com11 deny
```

2. 从 Untrust, 到 DMZ

```
set policy from untrust to dmz any mail.abc.com mail permit
set policy from untrust to dmz any www.abc.com Web12 permit
```

3. 从 Trust, 到 DMZ

```
set policy from trust to dmz any mail.abc.com e-mail13 permit
set policy from trust to dmz any www.abc.com Internet10 permit
set policy from trust to dmz sys-admins any any permit
```

4. 从 DMZ, 到 Untrust

```
set policy from dmz to untrust mail.abc.com any mail permit
save
```

10. “Internet” 是具有以下成员的服务组：FTP-Get、HTTP 和 HTTPS。

11. “Com” 是具有以下成员的服务组：FTP-Put、MAIL、IMAP 和 POP3。

12. “Web” 是具有以下成员的服务组：HTTP 和 HTTPS。

13. “e-mail” 是具有以下成员的服务组：MAIL、IMAP 和 POP3。

范例：区段内部策略

在本例中，创建内部区段策略，允许一组帐户访问 **Trust** 区段中企业 LAN 上的机密服务器。首先将 **ethernet1** 绑定到 **Trust** 区段，并给定 IP 地址为 10.1.1.1/24。然后将 **ethernet2** 绑定到 **Trust** 区段，并指派 IP 地址为 10.1.5.1/24。启用 **Trust** 区段中的区段内部阻塞。接着，定义两个地址，一个作为公司存储财务记录的服务器地址 (10.1.1.100/32)，另一个作为会计部门主机所在位置的子网地址 (10.1.5.0/24)。然后创建区段内部策略，允许从这些主机访问服务器。

WebUI

1. Trust 区段 – 接口和阻塞

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.5.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Zones > Edit (对于 Trust): 输入以下内容，然后单击 **OK**:

Block Intra-Zone Traffic: (选择)

2. 地址

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

Address Name: Hamilton

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.100/32

Zone: Trust

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

Address Name: accounting

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.5.0/24

Zone: Trust

3. 策略

Policies > (From: Trust, To: Trust) > New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), accounting

Destination Address:

Address Book Entry: (选择), Hamilton

Service: ANY

Action: Permit

CLI

1. Trust 区段 – 接口和阻塞

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.5.1/24
set interface ethernet2 nat
```

```
set zone trust block
```

2. 地址

```
set address trust Hamilton 10.1.1.100/32
set address trust accounting 10.1.5.0/24
```

3. 策略

```
set policy from trust to trust accounting Hamilton any permit
save
```

范例：全局策略

在本例中，将创建一个全局策略，使每个区段中的每台主机都可以访问公司的 Web 网站，网址为 www.netscreen.com¹⁴。在存在许多安全区时，使用全局策略是一种便捷方式。在本例中，一个全局策略即可实现 n 个区段内部策略所实现的任务（其中 n = 区段数）。

WebUI

1. 全局地址

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

Address Name: server1

IP Address/Domain Name:

Domain Name: (选择), www.netscreen.com

Zone: Global

2. 策略

Policies > (From: Global, To: Global) > New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), server1

Service: HTTP

Action: Permit

14. 要用域名而非 IP 地址，应确保在 NetScreen 设备上配置 DNS 服务。

CLI

1. 全局地址

```
set address global server1 www.netscreen.com
```

2. 策略

```
set policy global any server1 http permit
save
```

输入策略环境

通过 CLI 配置策略时，首先创建策略，然后输入策略环境进行添加和修改。例如，可能首先创建以下策略：

```
set policy id 1 from trust to untrust host1 server1 HTTP permit attack
HIGH:HTTP:SIGS action close
```

如果想对策略进行某些修改，如添加其它源或目的地址、其它服务或其它攻击组，则可输入策略 1 的环境，然后输入有关的命令：

```
set policy id 1
ns(policy:1)-> set src-address host2
ns(policy:1)-> set dst-address server2
ns(policy:1)-> set service FTP
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS
```

也可移除单个策略组件的多个条目，只要不将它们全部移除。例如，可从上述配置移除 **server2**，但不能同时移除 **server2** 和 **server1**，因为同时移除之后就不再有目的地址。

可移除 **server2**,

✓ `ns(policy:1)-> unset dst-address server2`

或移除 **server1**,

✓ `ns(policy:1)-> unset dst-address server1`

但不能同时将它们移除。

✗ `ns(policy:1)-> unset dst-address server2`
`ns(policy:1)-> unset dst-address server1`

每个策略组件含多个条目

利用 ScreenOS 可将多个条目添加到策略的下列组件：

- 源地址
- 目的地址
- 服务
- 攻击组

在 ScreenOS 5.0.0 之前的版本中，具有多个源和目的地址或服务的唯一方法是首先创建具有多个成员的地址或服务组，然后在策略中引用该组。ScreenOS 5.0.0 版本中策略的地址和服务组仍可使用。此外，也可以直接添加新条目到策略组件。

注意：如果策略中引用的第一个地址或服务是 “Any”，则逻辑上不能向策略组件添加其它条目。NetScreen 防止此类错误配置，如果出现，会显示错误消息。

要向策略组件添加多个条目，请执行下列操作：

WebUI

要添加多个地址和服务，请单击要添加条目的组件旁的 **Multiple** 按钮。要添加多个攻击组，请单击 **Attack Protection** 按钮。在 “Available Members” 栏中选择一个条目，然后使用 << 键将该条目移动到 “Active Members” 栏中。对于其它条目，可重复此操作。完成后，单击 **OK** 返回策略配置页。

CLI

使用以下命令输入策略环境：

```
set policy id number
```

然后使用下列命令中可适用的命令：

```
ns(policy:number)-> set src-address string
ns(policy:number)-> set dst-address string
ns(policy:number)-> set service string
ns(policy:number)-> set attack string
```

地址排除

可以配置策略，使其应用到除指定为源或目的地址之外的其它所有地址。例如，可创建允许互联网访问除“P-T_contractors”地址组之外的其它所有地址的策略。要实现此目的，可使用地址排除选项。

在 WebUI 中，单击策略配置页上源地址或目的地址旁的 **Multiple** 按钮时，此选项会出现在弹出菜单中。

在 CLI 中，在源地址或目的地址前直接插入感叹号 (!)。

注意：地址排除出现在策略组件级，应用于排除组件的所有条目。

范例：目的地址排除

在本例中，将创建一个内部区段策略，允许 Trust 区段中的所有地址访问除名为“vulcan”的 FTP 服务器之外的所有 FTP 服务器，工程部门用此服务器发送功能规格给其他使用者。

不过，在创建策略之前，必须首先设计应用策略的环境。第一，启用 Trust 区段的内部区段阻塞。在 NetScreen 设备通过两个接口（绑定到同一区段）间的信息流之前，内部区段阻塞要求进行策略查找。

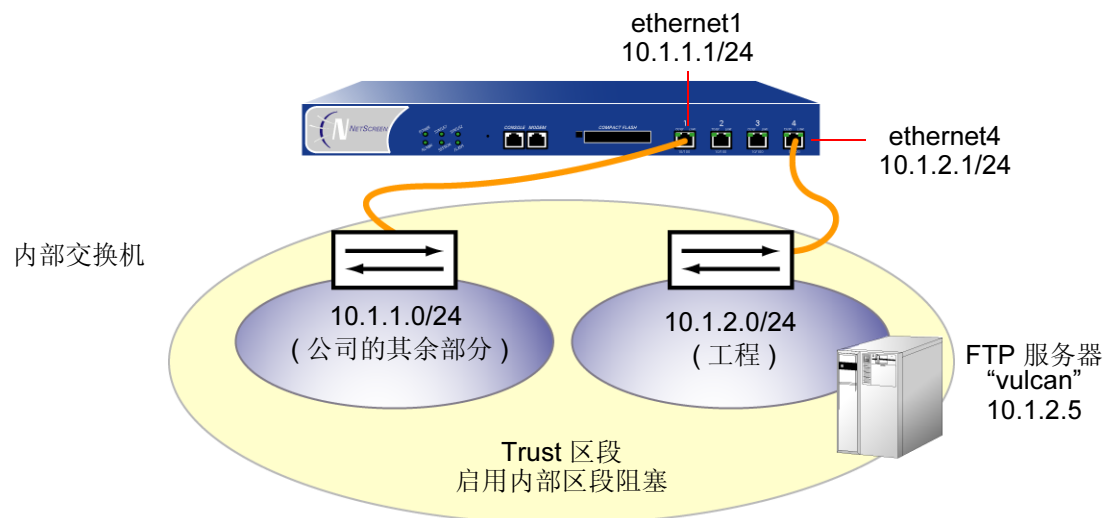
第二，将两个接口绑定到 Trust 区段并为其分配 IP 地址：

- 将 ethernet1 绑定到 Trust 区段并将其 IP 地址指派为 10.1.1.1/24。
- 将 ethernet4 绑定到 Trust 区段并将其 IP 地址指派为 10.1.2.1/24。

第三，在 Trust 区段中为名为“vulcan”的 FTP 服务器创建地址 (10.1.2.5/32)。

完成这两个步骤之后，即可创建内部区段策略。

注意：不必为工程部门创建到达其 FTP 服务器的策略，因为工程师也在 10.1.2.0/24 子网中，并且不必穿越 NetScreen 防火墙到达他们自己的服务器。



WebUI

1. 内部区段阻塞

Network > Zones > Edit (对于 Trust): 输入以下内容, 然后单击 **OK**:

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (选择)

2. Trust 区段接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet4): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.2.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

3. 地址

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

Address Name: vulcan

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.2.5/32

Zone: Trust

4. 策略

Policies > (From: Trust, To: Trust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), vulcan

> 单击 **Multiple**, 选择 **Negate Following** 复选框, 然后单击 **OK** 返回基本策略配置页。

Service: FTP

Action: Permit

CLI

1. 内部区段阻塞

```
set zone trust block
```

2. Trust 区段接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet4 zone trust
set interface ethernet4 ip 10.1.2.1/24
set interface ethernet1 nat
```

3. 地址

```
set address trust vulcan 10.1.2.5/32
```

4. 策略

```
set policy from trust to trust any !vulcan ftp permit
save
```

修改和禁用策略

创建策略后，始终都可以返回到该策略进行修改。在 WebUI 中，单击要更改的策略 **Configure** 栏中的 **Edit** 链接。在该策略出现的 **Policy** 配置页面中进行更改，然后单击 **OK**。在 CLI 中，使用 **set policy** 命令。

ScreenOS 也提供启用和禁用策略的方法。在缺省情况下，策略被启用。要禁用策略，请执行以下操作：

WebUI

Policies: 在要禁用的策略的 **Configure** 栏中，清除 **Enable** 复选框。

被禁用策略的文本行以灰色显示。

CLI

```
set policy id id_num disable  
save
```

注意：要再次启用策略，请在要启用的策略 **Configure** 栏中选择 **Enable** (WebUI)，或键入 **unset policy id id_num disable** (CLI)。

策略验证

ScreenOS 提供一种工具，用于验证策略列表中策略的顺序是否有效。可能会出现一种策略掩蔽或“遮盖”另一种策略的现象。考虑以下示例：

```
set policy id 1 from trust to untrust any any HTTP permit
set policy id 2 from trust to untrust any dst-A HTTP deny
```

因为 NetScreen 设备从列表顶部开始查找策略，所以找到所接收信息流的匹配策略后，就不再向下查找策略列表中的其它策略。在上例中，NetScreen 设备从未到达策略 2，因为策略 1 中的目的地址“any”包括策略 2 中更具体的“dst-A”地址。某 HTTP 封包从 Trust 区段（为 Untrust 区段中的 dst-A 绑定）中的一个地址到达 NetScreen 设备时，NetScreen 设备始终首先找到与之匹配的策略 1。

要纠正上述范例，只需颠倒策略顺序，将较为具体的策略放在第一位：

```
set policy id 2 from trust to untrust any dst-A HTTP deny
set policy id 1 from trust to untrust any any HTTP permit
```

当然，本例的目的只是为了说明基本概念。在有很多策略的情况下，一个策略对另一个策略的掩蔽可能就不会这么容易发现。要检查¹⁵策略列表中是否有策略遮盖，可使用下列 CLI 命令：

```
exec policy verify
```

此命令报告遮盖策略和被遮盖的策略。然后，则由管理员负责纠正此情形。

策略验证工具无法检测出一个策略组合遮盖另一个策略的情况。在下例中，没有任何单一策略遮盖策略 3，但是，策略 1 和策略 2 的组合遮盖了策略 3：

```
set group address trust grp1 add host1
set group address trust grp1 add host2
set policy id 1 from trust to untrust host1 server1 HTTP permit
set policy id 2 from trust to untrust host2 server1 HTTP permit
set policy id 3 from trust to untrust grp1 server1 HTTP deny
```

15. 策略“遮盖”的概念是指策略列表中位置较高的策略始终在之后策略前生效的情况。因为策略查找始终使用找到的第一个策略（与源和目的区段、源和目的地址及服务类型 5 部分元组相匹配），所以，如果另一个策略应用于同一元组（或元组子网），则策略查找使用列表中第一个策略，且决不会到达第二个策略。

重新排序策略

NetScreen 设备将所有穿越防火墙的尝试与策略进行对照检查，从列在相应列表（请参阅第 218 页上的“策略组列表”）的策略组中的第一个开始，并检查整个列表。由于 NetScreen 设备将策略中指定的动作应用到列表中第一个匹配的策略，因此，必须按照从最特殊到最一般的顺序安排策略。（特殊策略不排除位于列表下部的更一般性策略的应用，但位于特殊策略前的一般性策略会产生此排除效应。）

在缺省情况下，最近创建的策略出现在策略组列表的底部。有一个选项允许将策略定位在列表的顶部。在 WebUI 的 Policy 配置页面中，选择 **Position at Top** 复选框。在 CLI 中，将关键字 **top** 添加到 **set policy** 命令中：
set policy top ...

要将策略移动到列表中的不同位置，请执行以下操作之一：

WebUI

在 WebUI 中有两种方法重新排序策略：在要移动的策略的 **Configure** 栏中，单击圆形箭头或单击单箭头。

如果单击圆形箭头：

出现 **User Prompt** 对话框。

要将策略移到列表的最底端，请输入 **<-1>**。要将策略向上移动，输入要移动到其前的策略的 ID 号。

单击 **OK**，执行移动。

如果单击单箭头：

出现 **Policy Move** 页面，显示要移动的策略以及显示其它策略的表格。

在显示其它策略的表格中，第一栏 (**Move Location**) 包含指向不同位置的箭头，可将策略移动这些位置。单击指向策略要移动到的列表中位置的箭头。

出现 **Policy List** 页面，移动的策略出现在新位置。

CLI

```
set policy move id_num { before | after } number  
save
```

移除策略

除修改和重新排序策略外，还可以删除策略。在 WebUI 中，在要移除的策略的 **Configure** 栏中单击 **Remove**。当系统消息提示是否继续删除时，单击 **Yes**。在 CLI 中，使用 **unset policy *id_num*** 命令。

地址转换

NetScreen 提供了许多方法执行源与目的 IP 地址、源与目的端口地址的转换。本章介绍几种可用的地址转换方法，分为以下几个部分：

- 第 262 页上的 “地址转换简介”
 - 第 269 页上的 “基于策略的转换选项”
 - 第 273 页上的 “NAT-Src 和 NAT-Dst 的方向特性”
- 第 275 页上的 “源网络地址转换”
 - 第 276 页上的 “来自 DIP 池 (启用 PAT) 的 NAT-Src”
 - 第 280 页上的 “来自 DIP 池 (禁用 PAT) 的 NAT-Src”
 - 第 283 页上的 “来自 DIP 池 (带有地址变换) 的 NAT-Src”
 - 第 289 页上的 “来自出口接口 IP 地址的 NAT-Src”
- 第 292 页上的 “目的网络地址转换”
 - 第 294 页上的 “目的地址转换的封包流”
 - 第 298 页上的 “目的地址转换的路由”
 - 第 302 页上的 “NAT-Dst: 一对一映射”
 - 第 311 页上的 “NAT-Dst: 多对一映射”
 - 第 316 页上的 “NAT-Dst: 多对多映射”
 - 第 321 页上的 “带有端口映射的 NAT-Dst”
 - 第 326 页上的 “同一策略中的 NAT-Src 和 NAT-Dst”
- 第 347 页上的 “映射 IP 地址”
 - 第 348 页上的 “MIP 和 Global 区段”
 - 第 358 页上的 “MIP-Same-as-Untrust”
 - 第 362 页上的 “MIP 和回传接口”
- 第 372 页上的 “虚拟 IP 地址”
 - 第 375 页上的 “VIP 和 Global 区段”

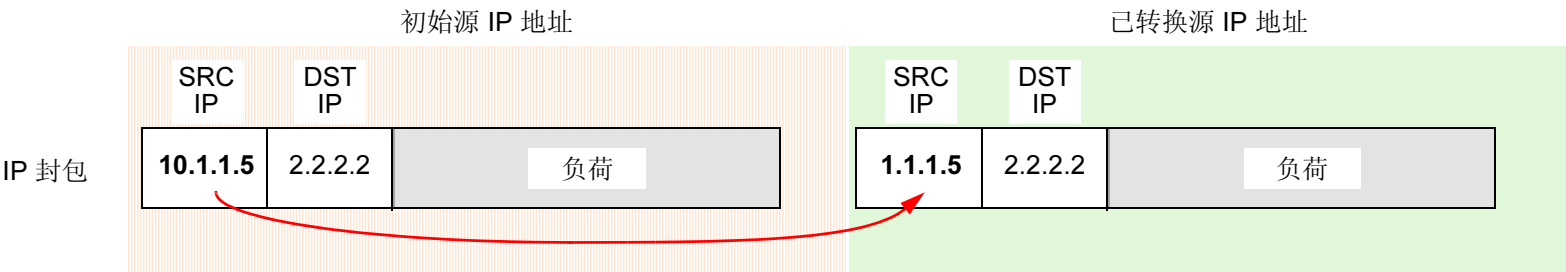
地址转换简介

NetScreen 提供了应用网络地址转换 (NAT) 的几种机制。NAT 的概念包括 IP 封包包头中的 IP 地址转换, 此外, 还可以包括 TCP 片段或 UDP 数据报报头中的端口号转换。转换中包含源地址 (以及可选的源端口号)、目的地址 (以及可选的目的端口号) 或已转换元素的组合。

源网络地址转换

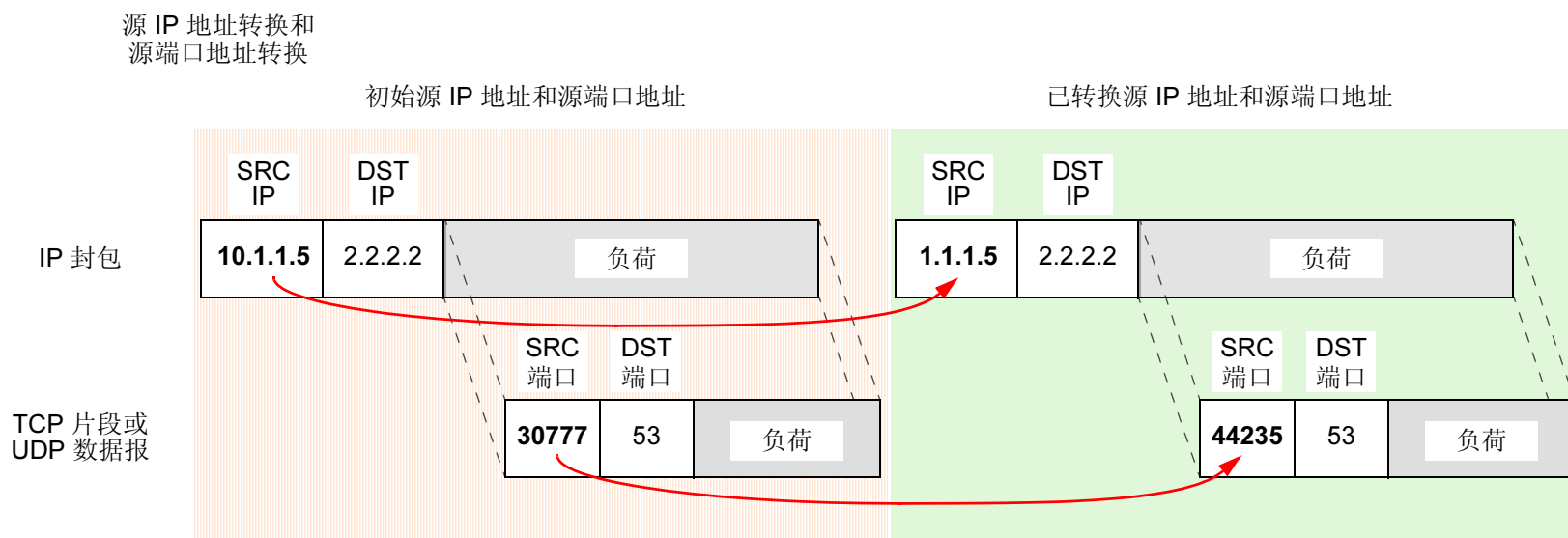
执行源网络地址转换 (NAT-src) 时, NetScreen 设备将初始源 IP 地址转换成不同的地址。已转换地址可以来自动态 IP (DIP) 池或 NetScreen 设备的出口接口。如果从 DIP 池中提取已转换的地址, NetScreen 设备可以随机提取或提取明确的地址, 也就是说, 既可以从 DIP 池中随机提取地址, 也可以持续提取与初始源 IP 地址有关的特定地址¹。如果已转换地址来自出口接口, NetScreen 设备会将所有封包中的源 IP 地址转换成该接口的 IP 地址。您可以配置 NetScreen 设备, 在接口级或策略级应用 NAT-src。如果配置策略以应用 NAT-src, 且入口接口处于 NAT 模式, 则基于策略的 NAT-src 设置会覆盖基于接口的 NAT²。(本章重点介绍基于策略的 NAT-src。有关基于接口的 NAT-src 或 “NAT” 的详细信息, 请参阅第 126 页上的 “NAT 模式”。有关 DIP 池的详细信息, 请参阅第 187 页上的 “DIP 池”。)

源 IP 地址转换



- 1. 明确的地址转换使用了一种称作地址变换的技术, 稍后将在本章中加以解释。有关应用于 NAT-src 的地址变换信息, 请参阅第 283 页上的 “来自 DIP 池 (带有地址变换) 的 NAT-Src”。有关应用于 NAT-dst 的地址变换信息, 请参阅第 326 页上的 “同一策略中的 NAT-Src 和 NAT-Dst”。
- 2. 入口接口处于 “路由” 或 NAT 模式时, 可以使用基于策略的 NAT-src。如果处于 NAT 模式, 策略级的 NAT-src 参数将取代接口级的 NAT 参数。

使用基于策略的 NAT-src 时，可以选择让 NetScreen 设备在初始源端口号上执行端口地址转换 (PAT)。启用 PAT 后，NetScreen 设备可以使用多个不同的端口号³ (最多 64,500 个) 将多个不同的 IP 地址 (最多 64,500 个) 转换成单个 IP 地址。NetScreen 设备使用唯一的已转换端口号维护会话状态信息，以便信息流入、流出同一个 IP 地址。对于基于接口的 NAT-src 或 “NAT”，设备会自动启用端口地址转换。由于 NetScreen 设备将所有的初始 IP 地址转化成同一个已转换 IP 地址 (来自出口接口)，因此 NetScreen 设备使用已转换端口号标识封包所属的每个会话。同样，如果 DIP 池只含有一个 IP 地址，且您希望 NetScreen 设备使用该地址将 NAT-src 应用于多个主机，则需要用到 PAT。



如果自定义的应用程序需要特定的源端口号才能正常运行，则执行 PAT 将导致这类应用程序出错。针对上述情况，可以禁用 PAT。

注意：有关 NAT-src 的详细信息，请参阅第 275 页上的“源网络地址转换”。

3. 启用 PAT 后，NetScreen 设备负责维护空闲端口号池，将这些端口号连同 DIP 池中的地址一起分配。用最大端口数 65,535 减去 1023 后，即可得到数字 64,500。设备给众所周知的端口保留了 1023 个端口号。因此，如果 NetScreen 设备使用只含单个 IP 地址的 DIP 池执行 NAT-src，且启用了 PAT，NetScreen 设备会将多个 (最多 64,500 个) 主机的初始 IP 地址转换成单个 IP 地址，并将每个初始端口号转换成唯一的端口号。

目的网络地址转换

NetScreen 提供以下三种机制执行目的网络地址转换 (NAT-dst):

- 基于策略的 NAT-dst
- 映射 IP (MIP)
- 虚拟 IP (VIP)

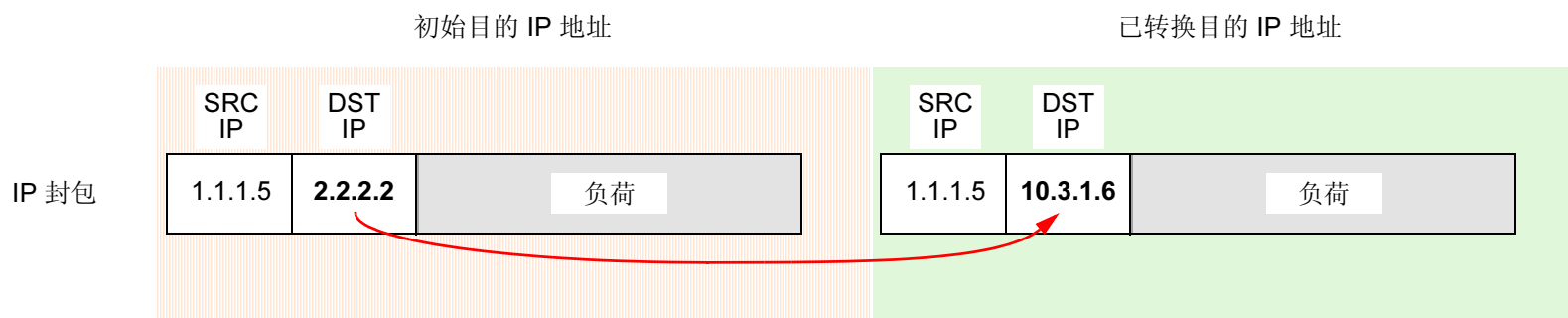
这三个选项都会将 IP 封包包头中的初始目的 IP 地址转换成不同的地址。使用基于策略的 NAT-dst 和 VIP 时，还可以启用端口映射⁴。

注意：NetScreen 不支持同时将基于策略的 NAT-dst 与 MIP、VIP 配合使用。如果您配置了 MIP 或 VIP，NetScreen 设备会在应用了基于策略的 NAT-dst 的任何信息流上应用 MIP 或 VIP。换言之，如果 NetScreen 设备偶然将 MIP 和 VIP 应用于同一信息流，则 MIP 和 VIP 将禁用基于策略的 NAT-dst。

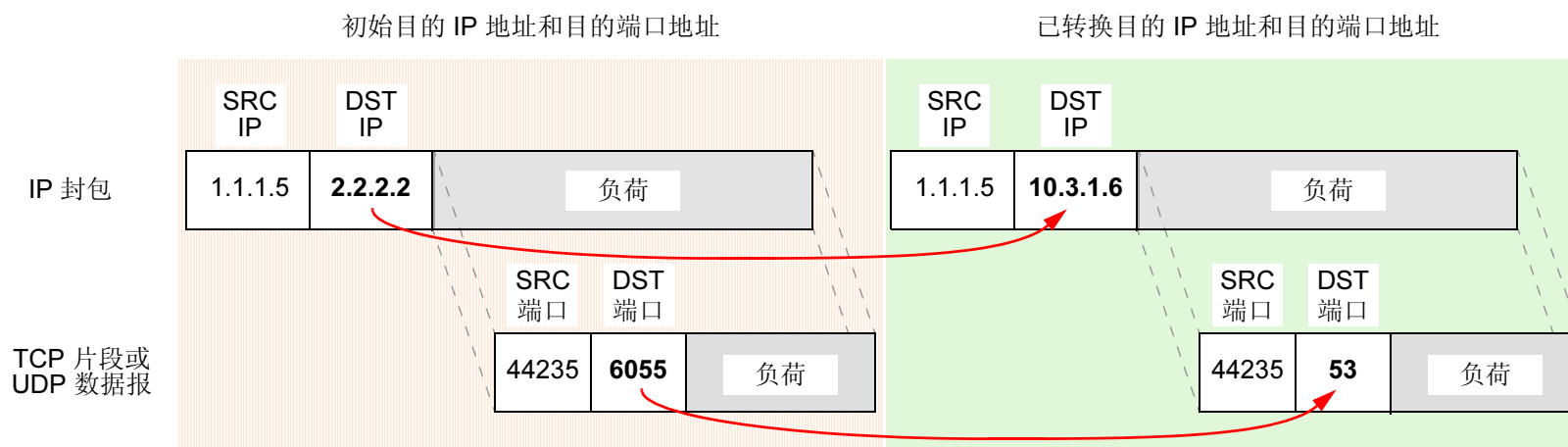
4. 有关端口映射的信息，请参阅下一页上的“基于策略的 NAT-Dst”以及第 292 页上的“目的网络地址转换”。

基于策略的 NAT-Dst: 您可以配置策略，将一个目的 IP 地址转换成另一个地址，将一个 IP 地址范围转换成单个 IP 地址，或将一个 IP 地址范围转换成另一个 IP 地址范围。将单个目的 IP 地址转换成另一个 IP 地址或将 IP 地址范围转换成单个 IP 地址时，NetScreen 均支持 NAT-dst，无论是否使用端口映射。端口映射是明确的转换，即将一个初始目的端口号转换成另一个特定端口号。它与 PAT 不同，后者将任一源端口号（由启动的主机随机分配）转换成另一个端口号（由 NetScreen 设备随机分配）。

不使用目的端口映射的目的 IP 地址转换

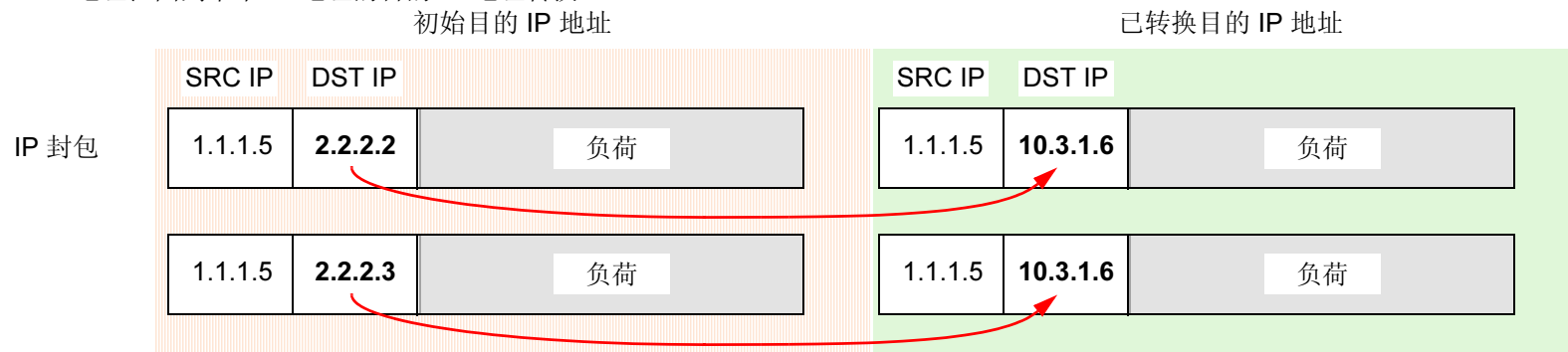


使用目的端口映射的目的 IP 地址转换

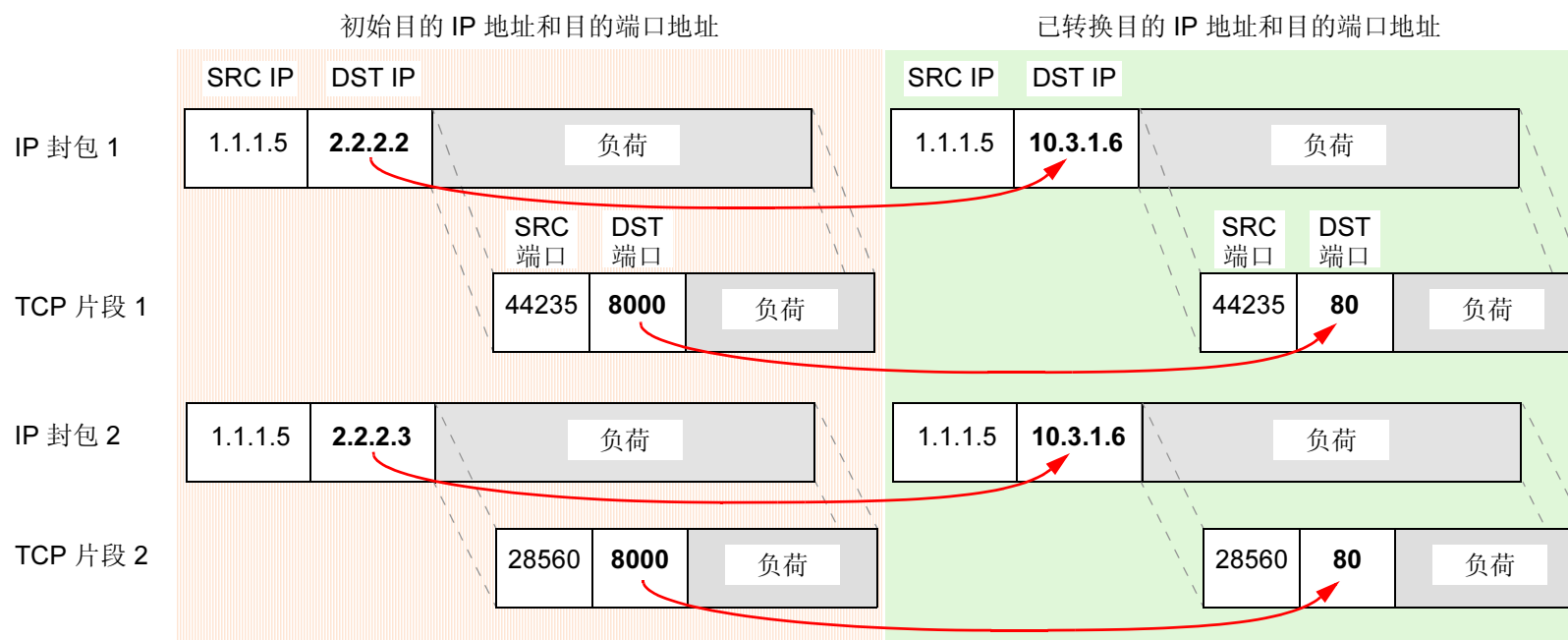


如果配置策略以执行 **NAT-dst**，将地址范围转换成单个地址，则 **NetScreen** 设备会将用户定义的初始目的地址范围内的所有目的 IP 地址转换成单个地址。还可以启用端口映射。

IP 地址范围到单个 IP 地址的目的 IP 地址转换

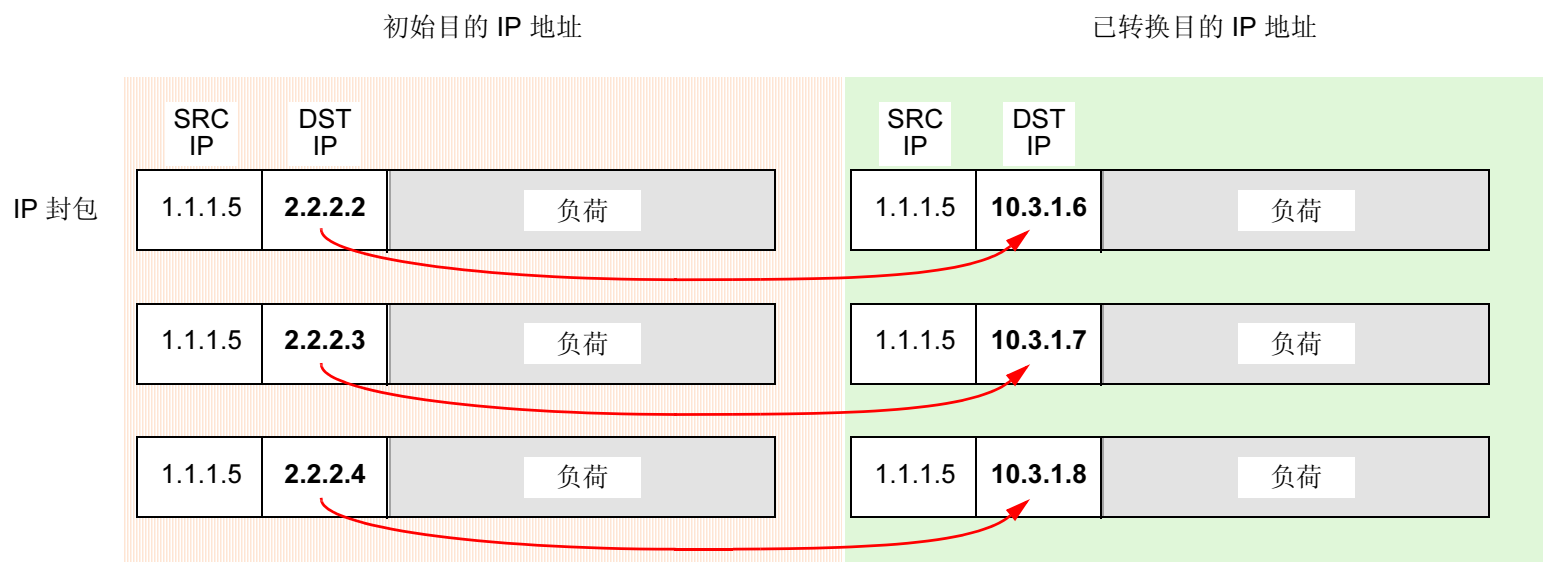


使用目的端口映射的从 IP 地址范围到单个 IP 地址的目的 IP 地址转换



配置策略以执行地址范围的 NAT-dst 时，NetScreen 设备会使用地址变换将初始目的地址范围内的目的 IP 地址转换成另一地址范围内的已知地址。

使用地址变换的目的 IP 地址转换



执行 IP 地址范围的 NAT-dst 时，NetScreen 设备会维护从一个地址范围内的每个 IP 地址到另一地址范围内的对应 IP 地址的映射。

注意：可以在同一策略中结合使用 NAT-src 和 NAT-dst。每个转换机制均独立执行，且只能单向执行。也就是说，如果在从 zone1 到 zone2 的信息流上启用 NAT-dst，NetScreen 设备就不会在从 zone2 到 zone1 的信息流上执行 NAT-src，除非您明确配置策略让设备这样执行。有关详细信息，请参阅第 273 页上的“NAT-Src 和 NAT-Dst 的方向特性”。有关 NAT-dst 的详细信息，请参阅第 292 页上的“目的网络地址转换”。

MIP: MIP 是从一个 IP 地址到另一个 IP 地址的映射。将同一子网中的一个地址定义为接口 IP 地址。另一个地址则属于信息流要流入的主机。MIP 的地址转换双向执行，因此 NetScreen 设备可以将到达 MIP 地址的所有信息流中的目的 IP 地址转换成主机 IP 地址，并将主机 IP 地址发出的所有信息流中的源 IP 地址转换成 MIP 地址。MIP 不支持端口映射。有关 MIP 的详细信息，请参阅第 347 页上的“映射 IP 地址”。

VIP: VIP 是从一个 IP 地址到基于目的端口号的另一个 IP 地址的映射。在同一子网中定义为接口的单个 IP 地址可以托管从若干服务（使用不同的目的端口号标识）到同样多主机⁵的映射。VIP 还支持端口映射。与 MIP 类似，VIP 的地址转换也是双向执行。NetScreen 设备可以将到达 VIP 地址的所有信息流中的目的 IP 地址转换成主机 IP 地址，并将主机 IP 地址发出的所有信息流中的源 IP 地址转换成 VIP 地址。有关 VIP 的详细信息，请参阅第 372 页上的“虚拟 IP 地址”。

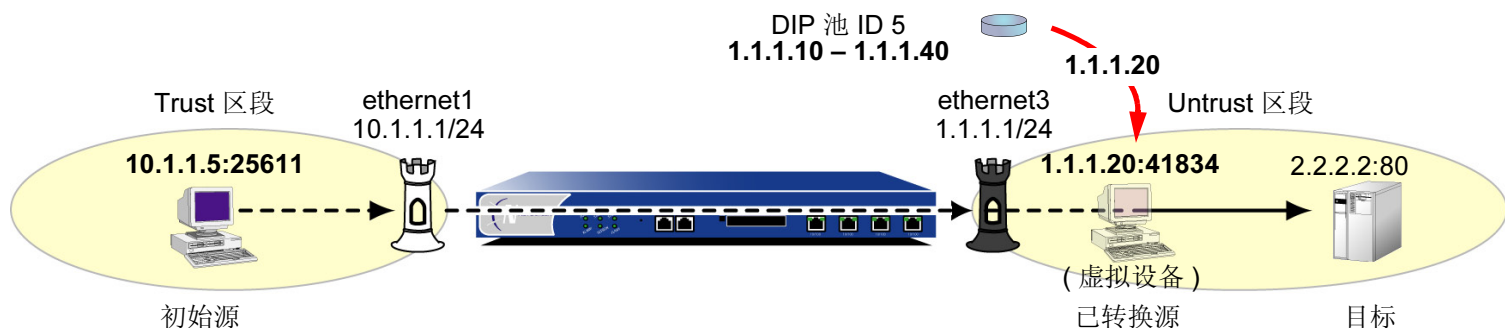
虽然 MIP 和 VIP 的地址转换机制是双向的，但基于策略的 NAT-src 和 NAT-dst 能够将入站和出站信息流的地址转换分开，以提供较好的控制与安全性能。例如，如果在 Web 服务器上使用 MIP，则每当服务器发起出站信息流以获取更新或补丁程序时，其活动都会被公开，这样就将信息提供给警觉的攻击者，供其进行攻击。利用基于策略的地址转换方法，可以在 Web 服务器（使用 NAT-dst）接收信息流而不是（使用 NAT-src）发起信息流时定义不同的地址映射。这样可以使服务器的活动处于隐藏状态，防止他人收集信息趁机攻击，从而更好地保护服务器。在此版 ScreenOS 中，基于策略的 NAT-src 和 NAT-dst 各提供一种单一方法，加起来可以取代基于接口的 MIP 和 VIP 功能，而且超过了后者。

5. 在某些 NetScreen 设备上，可以像定义接口 IP 地址那样定义 VIP 地址。如果 NetScreen 设备只有一个分配的 IP 地址，且该 IP 地址是动态分配的，则使用此功能很方便。

基于策略的转换选项

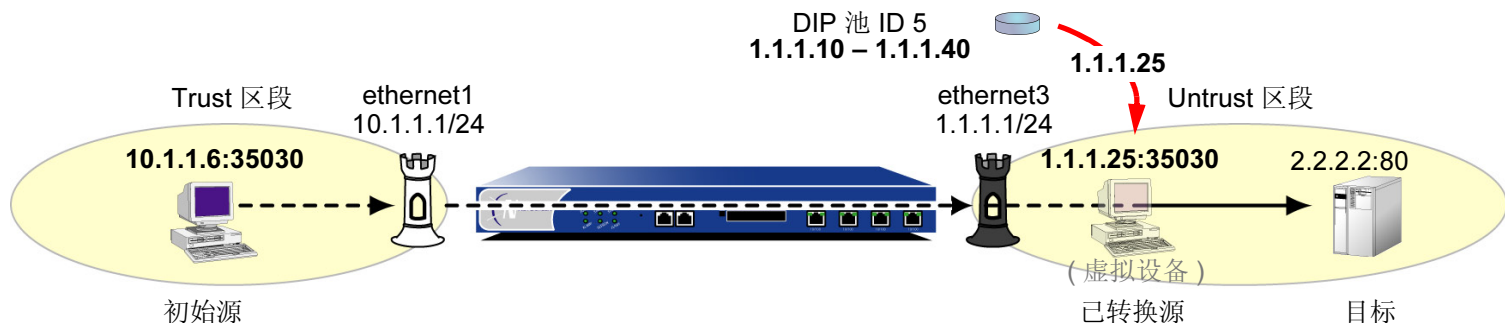
NetScreen 提供以下几种方法应用源网络地址转换 (NAT-src) 和目的网络地址转换 (NAT-dst)。注意, 始终可以在同一策略中结合使用 NAT-src 和 NAT-dst。

来自 **DIP 池 (带有 PAT)** 的 **NAT-Src** – NetScreen 设备将初始源 IP 地址转换成从动态 IP (DIP) 池中提取的地址。NetScreen 设备还会应用源端口地址转换 (PAT)。有关详细信息, 请参阅第 276 页上的“来自 DIP 池 (启用 PAT) 的 NAT-Src”。

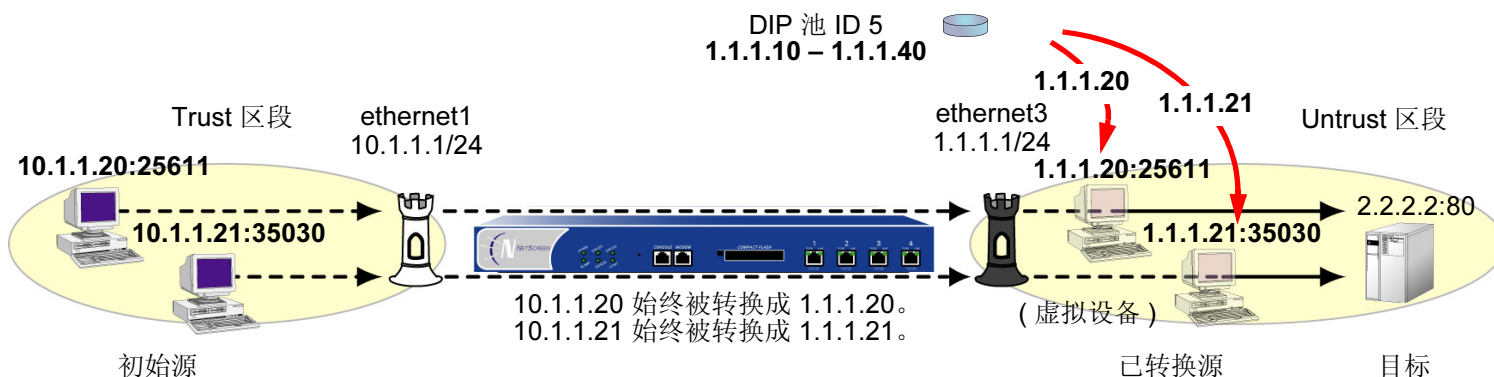


注意: 在本图和后续示意图中, “虚拟设备”代表已转换的源地址或目的地址 (如果该地址不属于实际设备)。

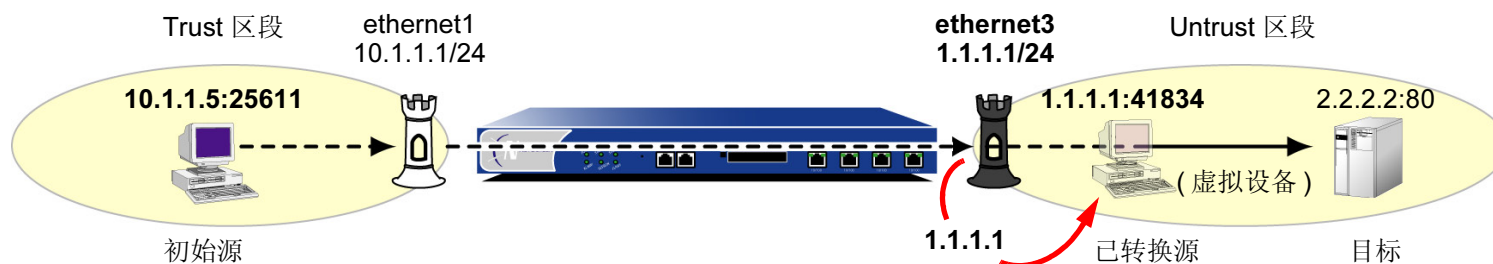
来自 **DIP 池 (无 PAT)** 的 **NAT-Src** – NetScreen 设备将初始源 IP 地址转换成从 DIP 池中提取的地址。NetScreen 设备不应用源 PAT。有关详细信息, 请参阅第 280 页上的“来自 DIP 池 (禁用 PAT) 的 NAT-Src”。



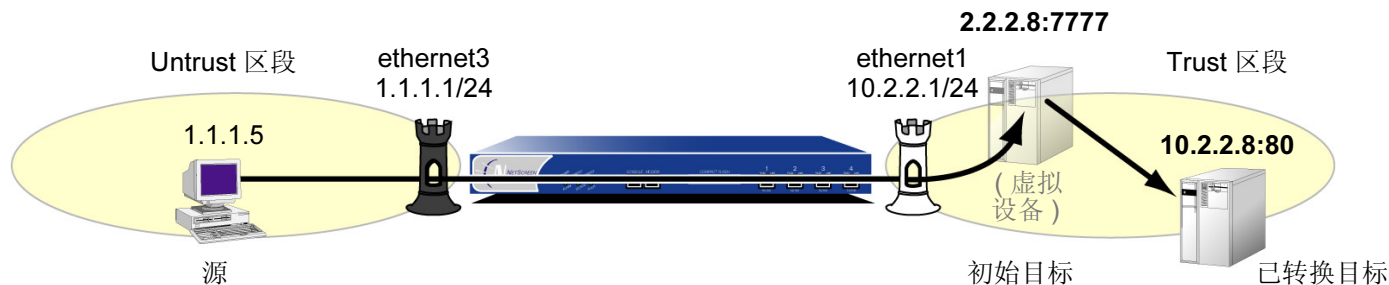
来自 **DIP 池 (带有地址变换)** 的 **NAT-Src – NetScreen** 设备将初始源 IP 地址转换成从动态 IP (DIP) 池中提取的地址, 并持续将每个初始地址映射成特定的已转换地址。**NetScreen** 设备不应用源端口地址转换 (PAT)。有关详细信息, 请参阅第 283 页上的“来自 DIP 池 (带有地址变换) 的 NAT-Src”。



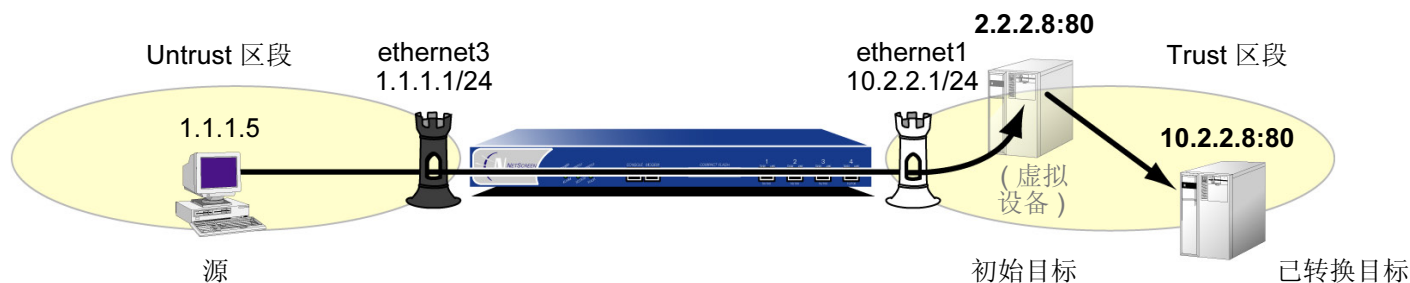
来自出口接口 IP 地址的 **NAT-Src – NetScreen** 设备将初始源 IP 地址转换成出口接口的地址。**NetScreen** 设备还会应用源 PAT。有关详细信息, 请参阅第 289 页上的“来自出口接口 IP 地址的 NAT-Src”。



转换成单个 IP 地址 (带有端口映射) 的 **NAT-Dst** – NetScreen 设备执行目的网络地址转换 (NAT-dst) 和目的端口映射。有关详细信息, 请参阅第 321 页上的 “带有端口映射的 **NAT-Dst**”。



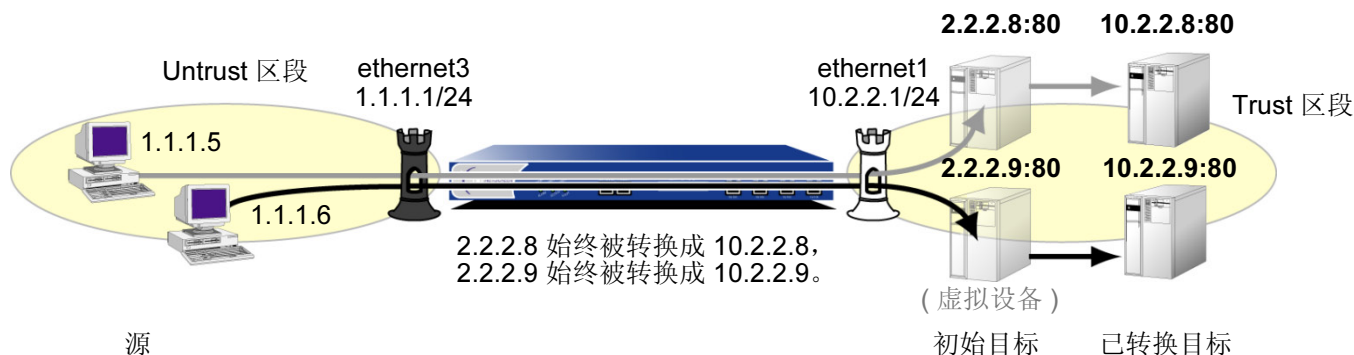
转换成单个 IP 地址 (无端口映射) 的 **NAT-Dst** – NetScreen 设备执行 NAT-dst, 但不更改初始目的端口号。有关详细信息, 请参阅第 292 页上的 “目的网络地址转换”。



从 IP 地址范围到单个 IP 地址的 **NAT-Dst** – NetScreen 设备执行 NAT-dst, 将 IP 地址范围转换成单个 IP 地址。如果还启用了端口映射, NetScreen 设备会将初始目的端口号转换成其它端口号。有关详细信息, 请参阅第 311 页上的“**NAT-Dst: 多对一映射**”。



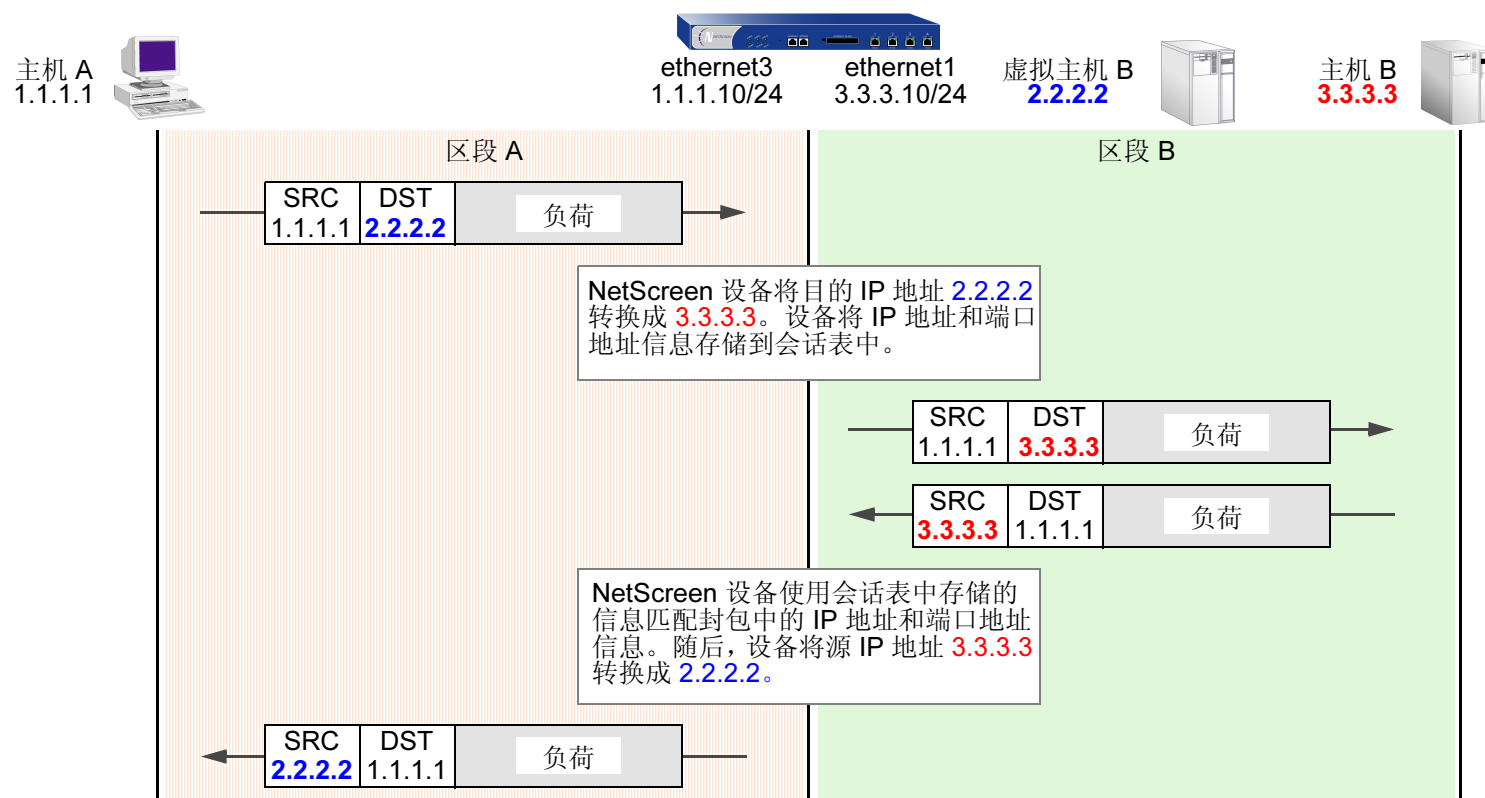
IP 地址范围之间的 NAT-Dst – 为 IP 地址范围应用 NAT-dst 时, NetScreen 设备会使用一种称作地址变换的技术, 将初始目的地址始终映射成特定范围内的已转换地址。注意, 地址变换不支持端口映射。有关详细信息, 请参阅第 316 页上的“**NAT-Dst: 多对多映射**”。



NAT-Src 和 NAT-Dst 的方向特性

NAT-src 和 NAT-dst 的应用各自独立。通过策略中指示的方向，可以确定二者在信息流上的应用方式。例如，如果 NetScreen 设备应用一个策略，对从主机 A 发送到虚拟主机 B 的信息流执行 NAT-dst，则 NetScreen 设备会将初始目的 IP 地址 2.2.2.2 转换成 3.3.3.3。（此外，设备还会将响应信息流中的源 IP 地址 3.3.3.3 转换成 2.2.2.2。）

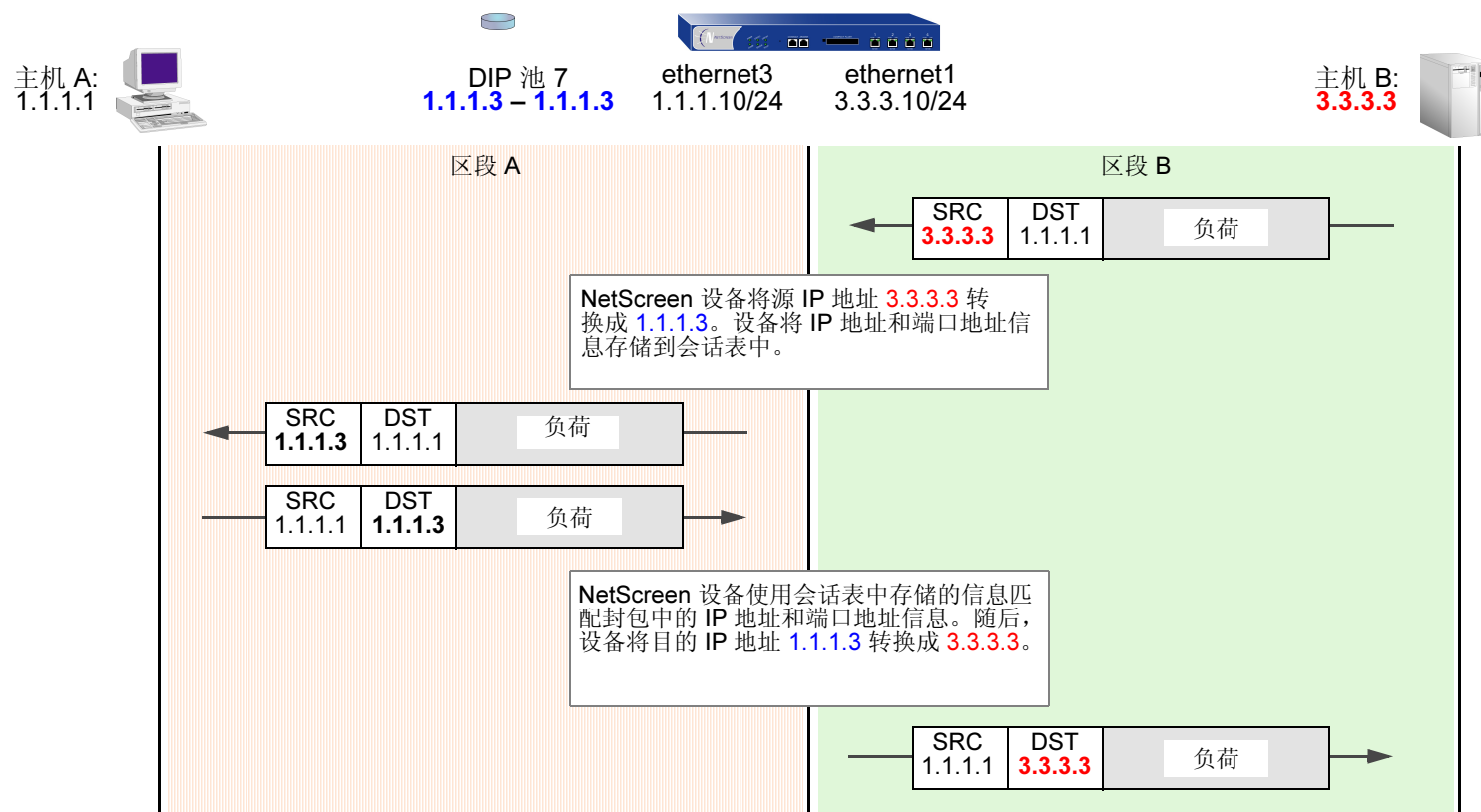
```
set policy from "zone A" to "zone B" "host A" "virtual host B" any nat dst ip 3.3.3.3 permit
set vrtrout trust-vr route 2.2.2.2/32 interface ethernet1
```



注意：您必须设置指向 2.2.2.2/32 (虚拟主机 B) 的路由，这样 NetScreen 设备才能执行路由查询确定目的区段。有关 NAT-dst 路由问题的详细信息，请参阅第 298 页上的“目的地址转换的路由”。

但是，如果只创建上述策略指定从主机 A 到主机 B 的 NAT-dst，当主机 B 发起流向主机 A 的信息流（而非响应主机 A 的信息流）时，NetScreen 设备不会转换主机 B 的初始源 IP 地址。为保证在主机 B 发起流向主机 A 的信息流时，NetScreen 设备能转换主机 B 的源 IP 地址，必须配置第二个从主机 B 到指定 NAT-src 的主机 A 的策略⁶。（此行为与 MIP 和 VIP 不同。请参阅第 347 页上的“映射 IP 地址”和第 372 页上的“虚拟 IP 地址”。）

```
set interface ethernet1 dip-id 7 1.1.1.3 1.1.1.3
set policy from "zone B" to "zone A" "host B" "host A" any nat src dip-id 7 permit
```



6. 为继续围绕 IP 地址转换机制这一重点，上图没有显示端口地址转换 (PAT)。如果为只含单个 IP 地址的 DIP 池指定固定端口号，则同一时间内只能有一个主机使用该池。上述策略只将“主机 B”指定为源地址。如果“主机 B”是唯一一台使用 DIP 池 7 的主机，就没必要启用 PAT。

源网络地址转换

有时，NetScreen 设备需要将 IP 封包包头中的初始源 IP 地址转换成另一个地址。例如，当私有 IP 地址上的主机发起流向公共地址空间的信息流时，NetScreen 设备必须将私有源 IP 地址转换成公共地址⁷。同理，如果将一个私有地址空间的信息流通过 VPN 通道发送到使用相同地址的站点，则通道两端的 NetScreen 设备必须将源 IP 地址和目的 IP 地址转换成相互中立的地址。

动态 IP (DIP) 地址池提供了大量可用地址，供 NetScreen 设备在执行源网络地址转换 (NAT-src) 时从中提取地址。如果策略要求执行 NAT-src，且引用了特定的 DIP 池，则 NetScreen 设备将在执行转换时从该池中提取地址。

注意：DIP 池使用的地址必须与策略引用的目的区段的缺省接口位于同一子网中。如果要使用的 DIP 池的地址不在目的区段接口所在的子网中，则必须在扩展接口上定义 DIP 池。有关详细信息，请参阅第 191 页上的“扩展接口和 DIP”。

最小的 DIP 池只包含单个 IP 地址，但如果启用了端口地址转换 (PAT)，则 DIP 池最多能同时支持 64,500 台主机⁸。尽管所有封包从 DIP 池接收的源 IP 地址完全相同，但它们获得的端口号各不相同。通过维护初始地址和端口号与已转换地址和端口号相匹配的会话表条目，NetScreen 设备可以跟踪哪些封包属于哪个会话以及哪些会话属于哪台主机。

如果只在策略中使用 NAT-src，却没有指定 DIP 池，NetScreen 设备会将源地址转换成目的区段中的出口接口地址。上述情况需要用到 PAT，设备会自动启用它。

对于需要将特定源端口号保持固定的应用程序，必须禁用 PAT，并定义一个 IP 地址范围足够大的 DIP 池，以确保每台并行活动主机收到的不同的已转换地址。对于固定端口的 DIP，NetScreen 设备将一个已转换源地址分配给所有并行会话所在的同一台主机。反之，如果 DIP 池启用了 PAT，NetScreen 设备可能会给单台主机分配不同地址，以进行不同会话 — 除非将 DIP 池定义为“附着”（请参阅第 190 页上的“附着 DIP 地址”）。

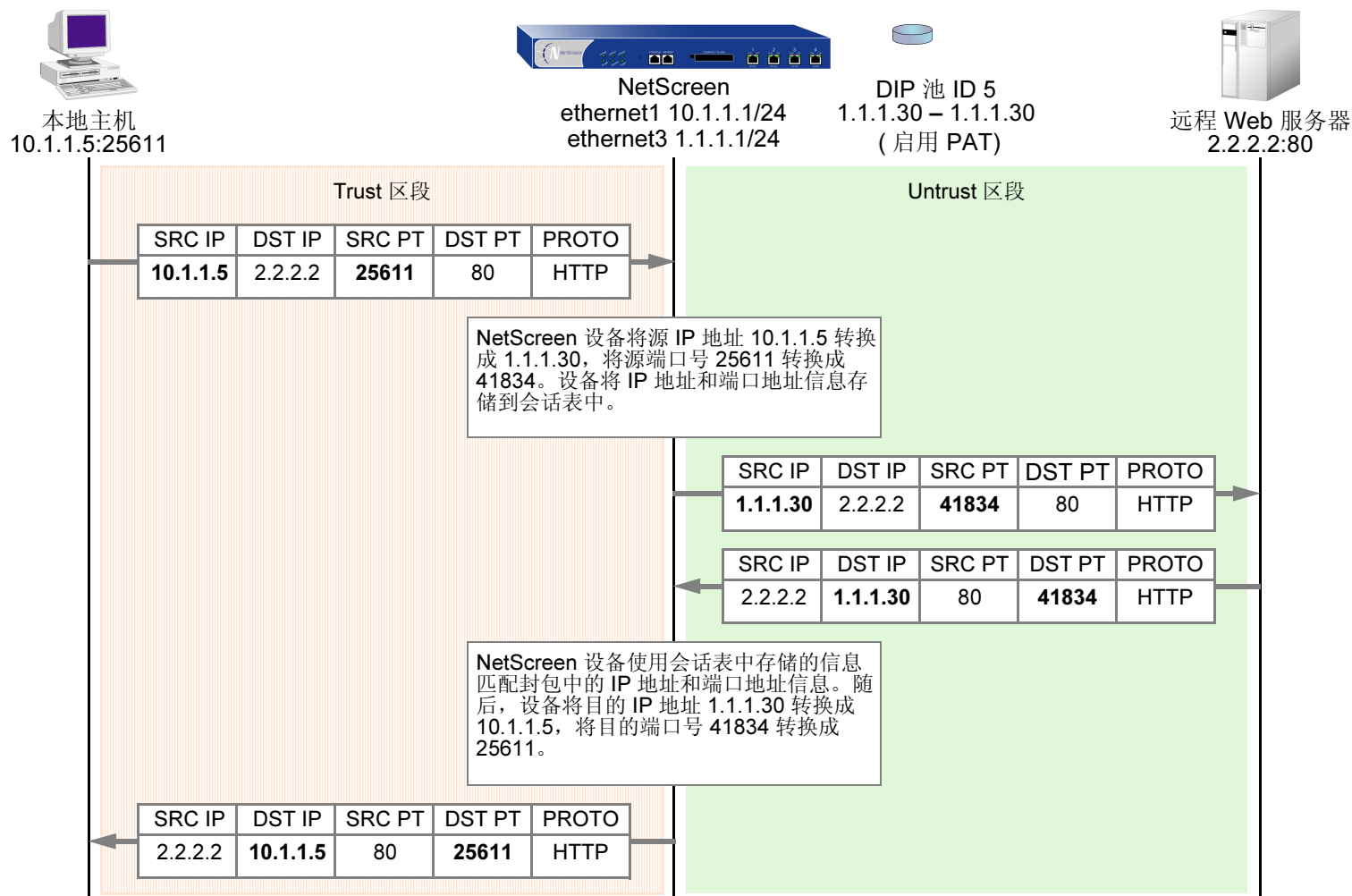
7. 有关公共和私有 IP 地址的信息，请参阅第 79 页上的“公开 IP 地址”和第 80 页上的“私有 IP 地址”。

8. 启用 PAT 后，NetScreen 设备还要维护空闲端口号池，将这些端口号连同 DIP 池中的地址一起分配。用最大端口数 65,535 减去 1023 后，即可得到数字 64,500。设备给众所周知的端口保留了 1023 个端口号。

来自 DIP 池 (启用 PAT) 的 NAT-Src

在与端口地址转换 (PAT) 一起应用源网络地址转换 (NAT-src) 时, NetScreen 设备转换 IP 地址和端口号, 如下图所示执行状态检查 (注意, 只显示 IP 封包包头和 TCP 片段包头中与 NAT-src 有关的元素):

```
set policy from trust to untrust any any http nat src dip-id 5 permit
```

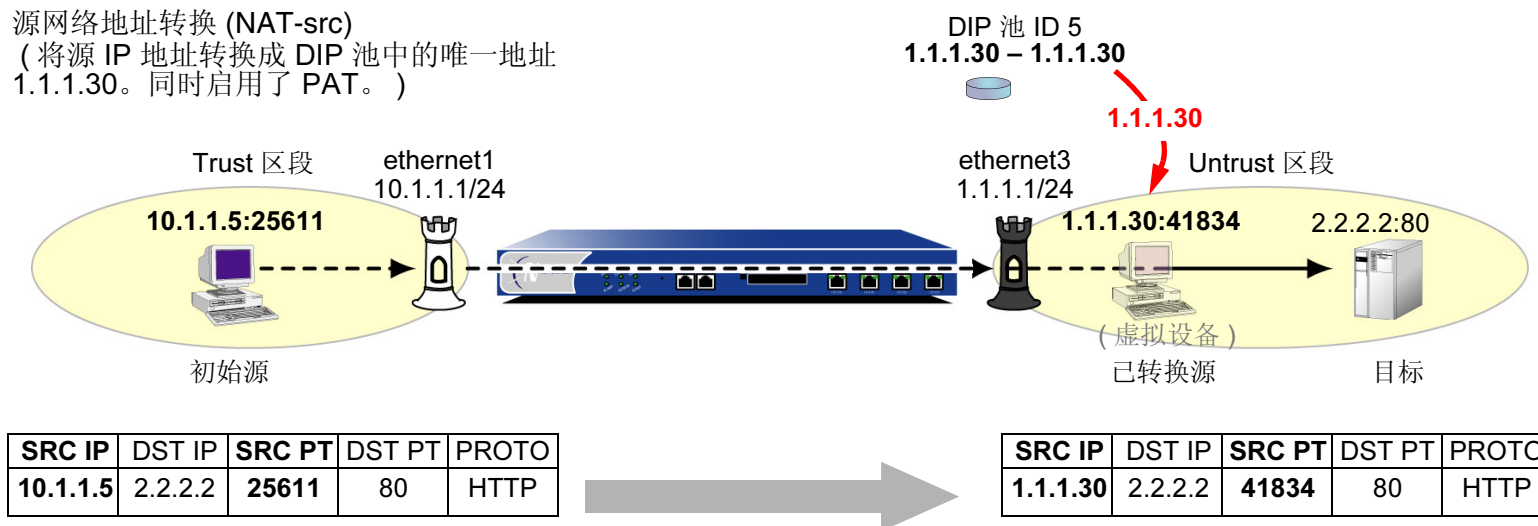


范例：带有 PAT 的 NAT-Src

在本例中，在绑定到 Untrust 区段的 ethernet3 接口上定义 DIP 池 5。DIP 池只包含单个 IP 地址 1.1.1.30，且启用了 PAT (缺省情况下启用 PAT)⁹。随后，可以设置一个策略，指示 NetScreen 设备执行以下任务：

- 允许 Trust 区段中任意地址发出的 HTTP 信息流流向 Untrust 区段中的任意地址
- 将 IP 封包包头中的源 IP 地址转换成 1.1.1.30，该地址是 DIP 池 5 中的唯一条目
- 将 TCP 片段包头或 UDP 数据报报头的初始源端口号转换成唯一的新端口号
- 将带有已转换源 IP 地址和端口号的 HTTP 信息流通过 ethernet3 发送到 Untrust 区段

源网络地址转换 (NAT-src)
(将源 IP 地址转换成 DIP 池中的唯一地址 1.1.1.30。同时启用了 PAT。)



9. 定义 DIP 池时，缺省情况下 NetScreen 设备启用 PAT。要禁用 PAT，必须向 CLI 命令结尾添加关键字固定端口，或清除 WebUI 中 DIP 配置页的 Port Translation 选项。例如，**set interface ethernet3 dip 5 1.1.1.30 1.1.1.30 fix-port** 或 Network > Interfaces > Edit (对于 ethernet3) > DIP: ID: 5; Start: 1.1.1.30; End: 1.1.1.30; Port Translation: (清除)。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5

IP Address Range: (选择), 1.1.1.30 ~ 1.1.1.30

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**：

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

(DIP on): 5 (1.1.1.30 - 1.1.1.30)/X-late

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 5 1.1.1.30 1.1.1.30
```

3. 策略

```
set policy from trust to untrust any any http nat src dip-id 5 permit
save
```

来自 DIP 池 (禁用 PAT) 的 NAT-Src

如果只要执行 IP 地址的源网络地址转换 (NAT-src), 而不执行源端口号的端口地址转换 (PAT), 则会出现这种情况。自定义应用程序可能需要特定的源端口地址, 也就是源端口地址可能为特定数字。目标主机可能要求源 IP 地址和端口地址为特定数字, 以唯一标识主机。在上述情况下, 可以定义一个策略, 指示 NetScreen 设备只执行无 PAT 的 NAT-src。

范例 : 禁用 PAT 的 NAT-Src

在本例中, 在绑定到 Untrust 区段的 ethernet3 接口上定义 DIP 池 6。该 DIP 池包含从 1.1.1.50 到 1.1.1.150 的 IP 地址范围。首先要禁用 PAT。随后, 可以设置一个策略, 指示 NetScreen 设备执行以下任务:

- 允许 Trust 区段任意地址发出的名为 “e-stock” 的用户定义服务的信息流流向 Untrust 区段中的任意地址¹⁰
- 将 IP 封包包头中的源 IP 地址转换成 DIP 池 6 中的任意可用地址
- 让 TCP 片段包头或 UDP 数据报报头的初始源端口号保持不变
- 将带有已转换源 IP 地址和初始端口号的 e-stock 信息流通过 ethernet3 发送到 Untrust 区段

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

10. 假设先前定义了用户定义服务 “e-stock”。此虚构服务要求所有 e-stock 交易始发自特定源端口号。基于上述原因, 必须禁用 DIP 池 6 的 PAT。

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 6

IP Address Range: (选择), 1.1.1.50 ~ 1.1.1.150

Port Translation: (清除)

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: e-stock

Action: Permit

> Advanced: 输入以下内容, 然后单击 **Return**, 设置高级选项并返回基本配置页:

NAT:

Source Translation: (选择)

DIP on: (选择), 6 (1.1.1.50 - 1.1.1.150)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 6 1.1.1.50 1.1.1.150 fix-port
```

3. 策略

```
set policy from trust to untrust any any e-stock nat src dip-id 6 permit
save
```


来自 DIP 池 (带有地址变换) 的 NAT-Src

可以定义一对一映射, 将 IP 地址范围内的初始源 IP 地址映射成已转换源 IP 地址。上述映射可以确保 NetScreen 设备始终将该范围内的特定源 IP 地址转换成 DIP 池内的同一已转换地址。该范围内的地址可以为任意数字。甚至还可以将一个子网映射到另一子网, 但需要使用一致的一对一映射 (将一个子网中的每个初始地址映射成另一子网中相应的已转换地址)。

执行带有地址变换的 NAT-src 可能有一个用途: 为接收来自第一个 NetScreen 设备的信息流的另一个 NetScreen 设备提供较大的策略精细度。例如, 站台 A 的 NetScreen-A 管理员的政策定义如下: 通过站台对站台 VPN 通道与站台 B 的 NetScreen 进行通信时, 转换其主机的源地址。如果 NetScreen-A 使用无地址变换的 DIP 池的地址应用 NAT-src, 则 NetScreen-B 的管理员只能为站点 A 发出的信息流配置通用策略。除非知道特定的已转换 IP 地址, 否则 NetScreen-B 的管理员只能为从 NetScreen-A DIP 池提取的源地址范围设置入站策略。另一方面, 如果 NetScreen-B 的管理员 (通过地址变换) 得知已转换源地址, 则会针对来自站点 A 的入站信息流设置的策略, 做出选择性及限制性的处理。

注意, 可以在策略中应用启用地址变换的 DIP 池 (该策略应用于超出池中指定的范围之外的源地址)。在上述情况下, NetScreen 设备传递策略允许的所有源地址发出的信息流, 将带有地址变换的 NAT-src 应用于 DIP 池范围内的地址, 但让源地址超出了 DIP 池范围之外的地址保持不变。如果希望 NetScreen 设备对所有源地址应用 NAT-src, 请确保源地址范围小于或等于 DIP 池的范围。

注意: NetScreen 设备不支持带有地址变换的源端口地址转换 (PAT)。

范例：带有地址变换的 NAT-Src

在本例中，在绑定到 **Untrust** 区段的 **ethernet3** 上定义 **DIP** 池 10。假设需要将 10.1.1.11 - 10.1.1.15 之间的五个地址转换成 1.1.1.101 - 1.1.1.105 之间的五个地址，且希望每对初始地址与已转换地址之间的关系保持一致：

初始源 IP 地址	已转换源 IP 地址
10.1.1.11	1.1.1.101
10.1.1.12	1.1.1.102
10.1.1.13	1.1.1.103
10.1.1.14	1.1.1.104
10.1.1.15	1.1.1.105

为 **Trust** 区段中的五台主机定义地址，并将它们添加到名为 “**group1**” 的地址组。这些主机的地址分别为 10.1.1.11、10.1.1.12、10.1.1.13、10.1.1.14 和 10.1.1.15。可以配置从 **Trust** 到 **Untrust** 区段的策略，该策略中引用了上述地址组（在使用 **DIP** 池 10 应用 **NAT-src** 的策略中也转换过该地址组）。该策略指示 **NetScreen** 设备每当 **group1** 的成员发起到 **Untrust** 区段地址的 **HTTP** 信息流时都执行 **NAT-src**。此外，**NetScreen** 设备始终执行 **NAT-src**，将特定 IP 地址（例如 10.1.1.13）转换成同一已转换 IP 地址 1.1.1.103。

随后，可以设置一个策略，指示 **NetScreen** 设备执行以下任务：

- 允许 **Trust** 区段中 **group1** 发出的 **HTTP** 信息流流向 **Untrust** 区段的任意地址
- 将 IP 封包包头中的源 IP 地址转换成 **DIP** 池 10 中的相应地址
- 将带有已转换源 IP 地址和端口号的 **HTTP** 信息流通过 **ethernet3** 发送到 **Untrust** 区段

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. DIP

Network > Interfaces > Edit (对于 ethernet3) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 10

IP Shift: (选择)

From: 10.1.1.11

To: 1.1.1.101 ~ 1.1.1.105

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 地址

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: host1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.11/32

Zone: Trust

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: host2

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.12/32

Zone: Trust

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: host3

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.13/32

Zone: Trust

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: host4

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.14/32

Zone: Trust

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: host5

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.15/32

Zone: Trust

Objects > Addresses > Groups > (对于 Zone: Trust) New: 输入以下组名称，移动以下地址，然后单击 **OK**:

Group Name: group1

选择 **host1**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **host2**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **host3**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **host4**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **host5**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), group1

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

(DIP on): 10 (1.1.1.101 - 1.1.1.105)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. DIP

```
set interface ethernet3 dip 10 shift-from 10.1.1.11 to 1.1.1.101 1.1.1.105
```

3. 地址

```
set address trust host1 10.1.1.11/32
set address trust host2 10.1.1.12/32
set address trust host3 10.1.1.13/32
set address trust host4 10.1.1.14/32
set address trust host5 10.1.1.15/32
```

```
set group address trust group1 add host1
set group address trust group1 add host2
set group address trust group1 add host3
set group address trust group1 add host4
set group address trust group1 add host5
```

4. 策略

```
set policy from trust to untrust group1 any http nat src dip-id 10 permit
save
```

来自出口接口 IP 地址的 NAT-Src

如果只在策略中应用 NAT-src 而不指定 DIP 池，NetScreen 设备会将源 IP 地址转换成出口接口的地址。在上述情况下，NetScreen 设备始终应用 PAT。

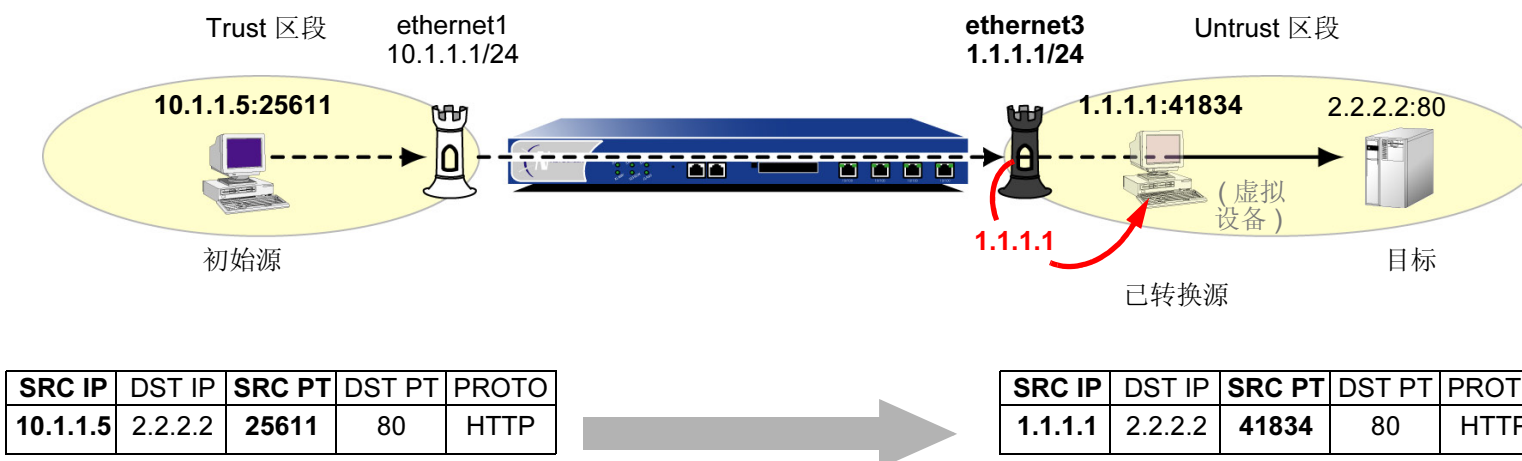
范例：无 DIP 的 NAT-Src

在本例中，将定义一个策略指示 NetScreen 设备执行以下任务：

- 允许 Trust 区段中任意地址发出的 HTTP 信息流流向 Untrust 区段中的任意地址
- 将 IP 封包包头中的源 IP 地址转换成 ethernet3 接口 (被绑定到 Untrust 区段) 的 IP 地址 1.1.1.1，从而可通过出口接口将信息流发送到 Untrust 区段的任意地址
- 将 TCP 片段包头或 UDP 数据报报头的初始源端口号转换成唯一的新端口号
- 将带有已转换源 IP 地址和端口号的信息流通过 ethernet3 发送到 Untrust 区段

源网络地址转换 (NAT-src)

(将源 IP 地址转换成目的区段出口接口的 IP 地址 1.1.1.1。
同时启用了 PAT。)



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Source Translation: (选择)

(DIP on): None (使用出口接口 IP)

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

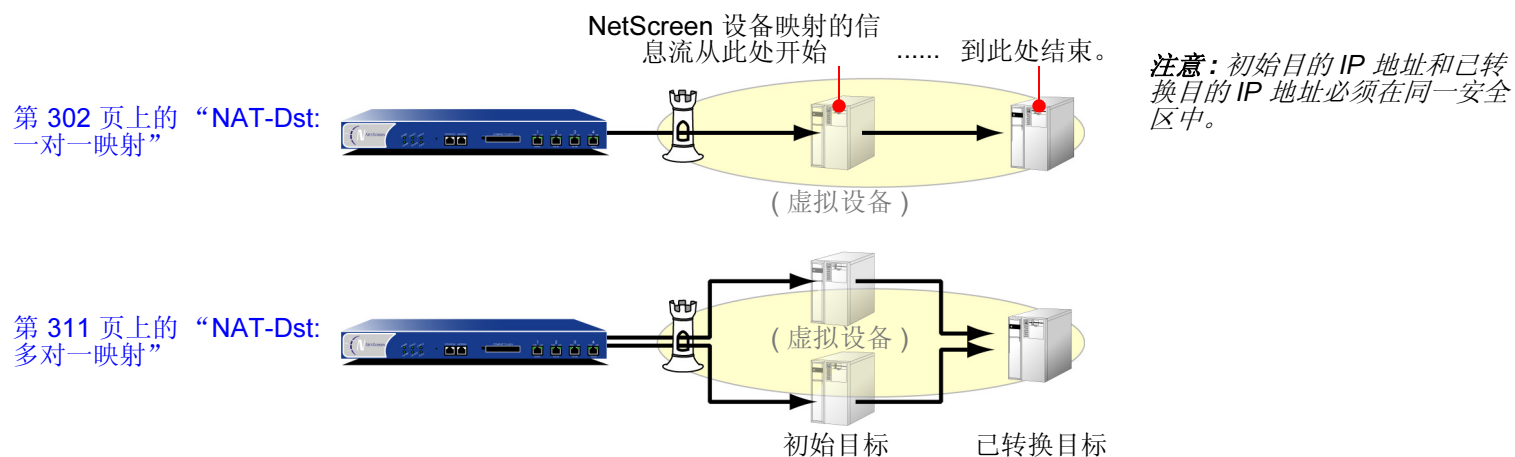
```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 策略

```
set policy from trust to untrust any any http nat src permit
save
```

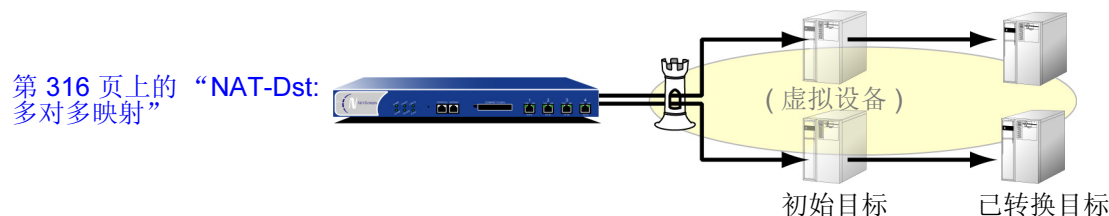
目的网络地址转换

可以定义策略将一个目的 IP 地址转换成另一个地址。可能需要 NetScreen 设备将一个或多个公共 IP 地址转换成一个或多个私有 IP 地址。初始目的地址与已转换目的地址之间的关系可能是一对一、多对一或多对多关系。以图说明了一对一和多对一 NAT-dst 关系的概念。



上述两种配置均支持目的端口映射。端口映射就是将一个初始目的端口号明确转换成另一个特定端口号。在端口映射中，初始端口号与已转换端口号之间的关系不同于端口地址映射 (PAT)。使用端口映射时，NetScreen 设备将一个预定义的初始端口号转换成另一个预定义的端口号。使用 PAT 时，NetScreen 设备将一个随机分配的初始源端口号转换成另一个随机分配的端口号。

可使用地址变换将一个目的地址范围转换成另一个地址范围 (如, 将一个子网转换成另一个子网), 这样 NetScreen 设备就可以将每个初始目的地址始终转换成特定的已转换目的地址。注意, NetScreen 不支持带有地址变换的端口映射。下图说明了多对多 NAT-dst 关系的概念。

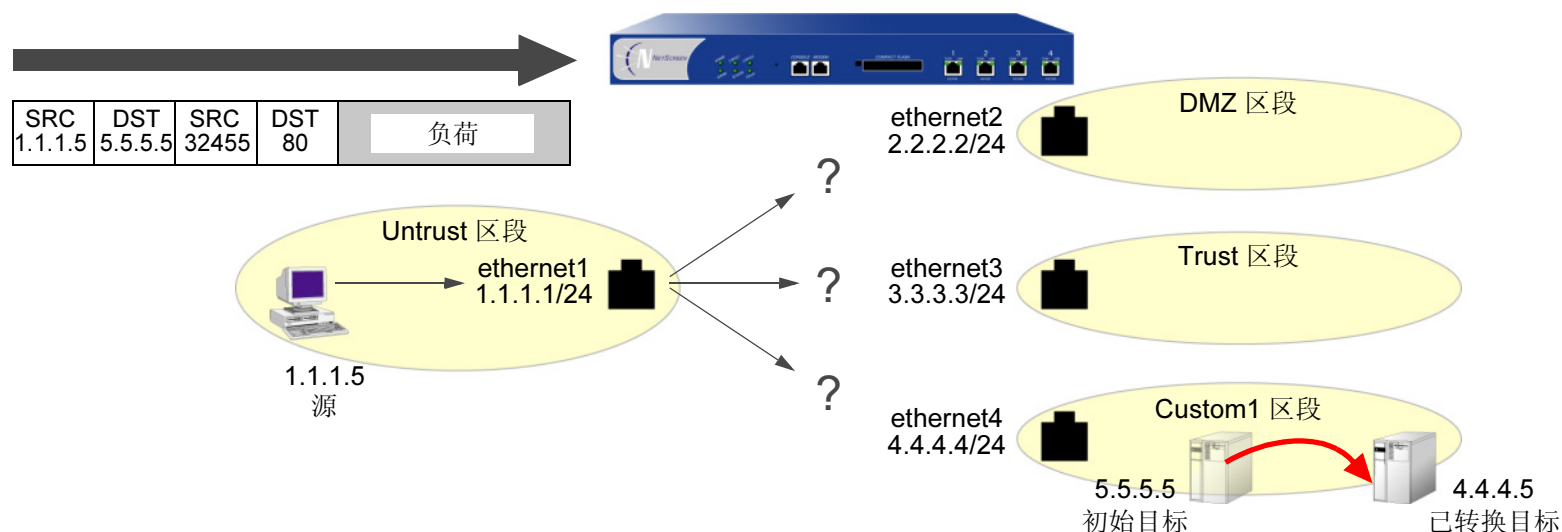


路由表中一定同时存在初始目的 IP 地址和已转换目的 IP 地址的条目。NetScreen 设备先使用初始目的 IP 地址执行路由查询, 确定后续策略查询的目的区段。然后使用已转换地址执行第二次路由查询, 确定发送封包的位置。为确保由路由确定的结果与策略相符, 初始目的 IP 地址和已转换目的 IP 地址必须在同一安全区中。(有关目的 IP 地址、路由查询及策略查询之间的关系, 请参阅第 294 页上的 “目的地址转换的封包流”。)

目的地址转换的封包流

以下步骤介绍封包流经 **NetScreen** 设备的路径以及设备应用目的网络地址转换时执行的各种操作。

1. 源 IP 地址：端口号为 1.1.1.5:32455 和目的 IP 地址：端口号为 5.5.5.5:80 的 HTTP 封包到达绑定到 **Untrust** 区段 **ethernet1**。



NetScreen 设备尚未执行相应步骤，来确定转发封包必须使用的接口。示意图中用三个问号标出了可能使用的接口。

2. 如果启用了 **Untrust** 区段的 **SCREEN** 选项，**NetScreen** 设备会在此时激活 **SCREEN** 模块。**SCREEN** 选项可能产生以下三种结果：
 - 如果 **SCREEN** 机制检测到封锁封包的异常行为，**NetScreen** 设备将丢弃封包，并在事件日志中生成一个条目。
 - 如果 **SCREEN** 机制检测到异常行为，该行为只记录事件却不封锁封包，则 **NetScreen** 设备将在入口接口的 **SCREEN** 计数器列表中记录该事件，然后继续进行下一步。
 - 如果 **SCREEN** 机制没有检测到异常行为，**NetScreen** 设备将继续进行下一步。

如果未启用 Untrust 区段的 SCREEN 选项，NetScreen 设备将立即进行下一步。

3. 会话模块执行会话查询，尝试用现有会话与封包匹配。

如果该封包与现有会话不匹配，NetScreen 设备会执行“首包处理”，该过程包括余下的步骤。

如果该封包与现有会话匹配，NetScreen 设备会执行“快速处理”，用现有会话条目中可用的信息来处理该封包。“快速处理”将直接跳到最后一步，因为之前各步生成的信息已在会话的首包处理期间获得。

4. 地址映射模块检查是否有映射 IP (MIP) 或虚拟 IP (VIP) 配置使用了目的 IP 地址 5.5.5.5。

如果存在这样的配置，NetScreen 设备会将 MIP 或 VIP 转变成已转换目的 IP 地址，并将后者作为路由查询的依据。随后，设备将在 Untrust 和 Global 区段之间执行策略查询。如果找到了允许信息流的策略，NetScreen 设备会将封包转发到在路由查询中确定的出口接口。

如果在 MIP 或 VIP 配置未使用 IP 地址 5.5.5.5，NetScreen 设备将继续进行下一步。

5. 为确定目的区段，路由模块将查询初始目的 IP 地址的路由，也就是说，该模块将使用到达 **ethernet1** 的封包头中出现的目的 IP 地址。(路由模块使用入口接口来确定路由查询使用的虚拟路由)。设备随即发现，可通过绑定到 **Custom1** 区段的 **ethernet 4** 访问 **5.5.5.5/32**。

trust-vr 路由表

到达：	使用接口：	所在区段：	使用网关：
0.0.0.0/0	ethernet1	Untrust	1.1.1.250
1.1.1.0/24	ethernet1	Untrust	0.0.0.0
2.2.2.0/24	ethernet2	DMZ	0.0.0.0
3.3.3.0/24	ethernet3	Trust	0.0.0.0
4.4.4.0/24	ethernet4	Custom1	0.0.0.0
5.5.5.5/32	ethernet4	Custom1	0.0.0.0

6. 策略引擎在 **Untrust** 和 **Custom1** 区段之间执行策略查询 (由相应的入口和出口接口确定)。源 IP 地址、目的 IP 地址和服务符合将 HTTP 信息流从 **5.5.5.5** 重新定向到 **4.4.4.5** 的策略。

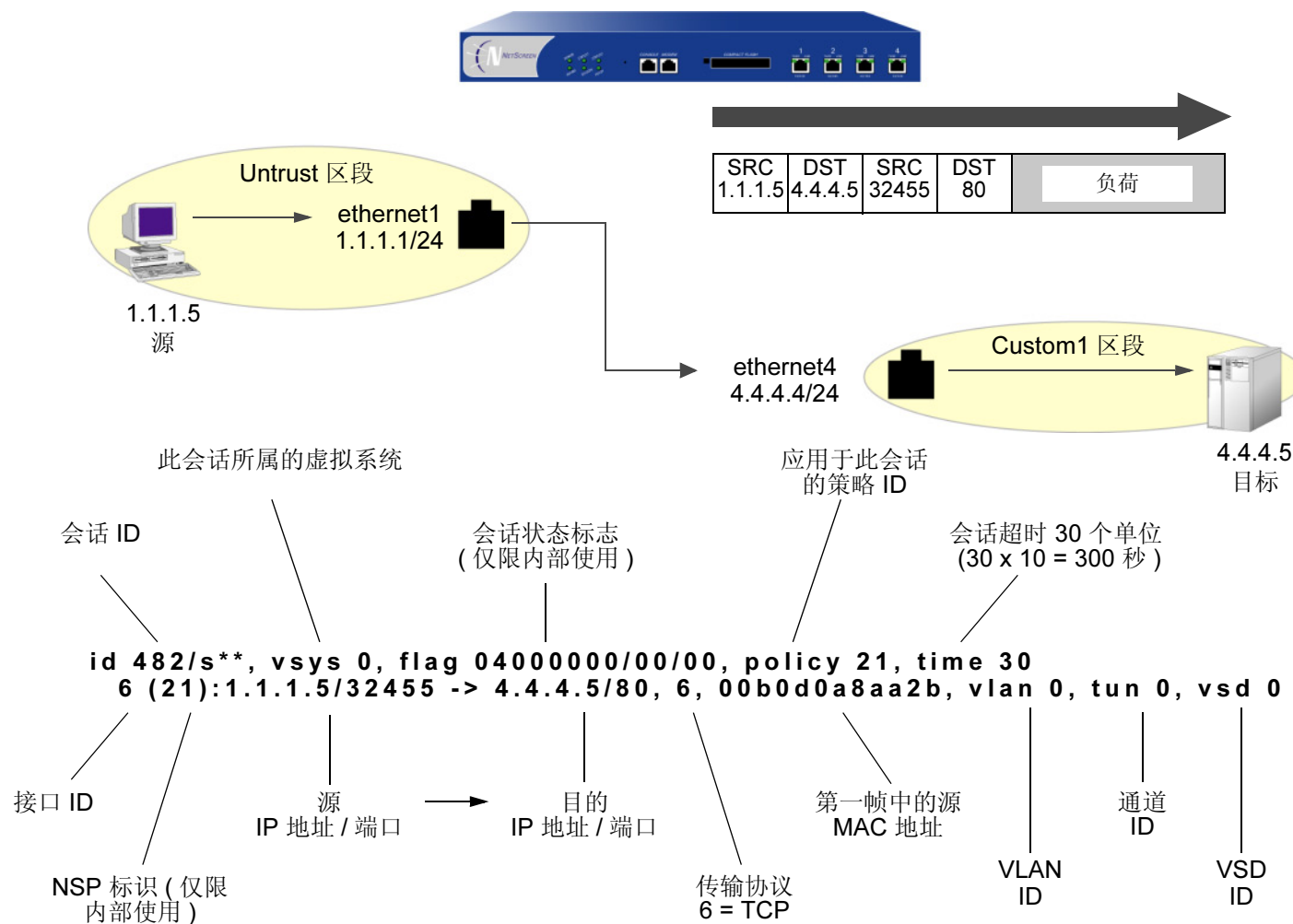
set policy from untrust to custom1 any v-server1 http nat dst ip 4.4.4.5 permit

(先前已将 IP 地址 **5.5.5.5/32** 定义为 “v-server1”，该地址在 **Custom1** 区段中。)

NetScreen 设备将目的 IP 地址 **5.5.5.5** 转换成 **4.4.4.5**。策略指出，不需要源网络地址转换和目的端口地址转换。

7. 接着，**NetScreen** 设备使用已转换 IP 地址执行第二次路由查询，发现可通过 **ethernet4** 访问地址 **4.4.4.5/32**。

8. 地址映射模块将封包包头中的目的 IP 地址转换成 4.4.4.5。随后，NetScreen 设备将该封包从 ethernet4 转发出去，并在会话表中生成一个条目（除非此封包是现有会话的一部分且记录条目已存在）。



注意：由于此会话不包含虚拟系统、VLAN、VPN 通道或虚拟安全设备 (VSD)，因此所有 ID number 均设为零。

目的地址转换的路由

配置 NAT-dst 地址时，NetScreen 设备的路由表中必须同时存在指向封包包头中的初始目的地址和已转换目的地址 (即 NetScreen 设备将封包包头重新定向到的地址) 的路由。如第 294 页上的“目的地址转换的封包流”中所述，NetScreen 设备使用初始目的地址执行路由查询，以此来确定出口接口。反过来，出口接口给出目的区段 (接口绑定到的区段)，以便 NetScreen 设备执行策略查询。NetScreen 设备找到符合要求的策略时，该策略定义从初始目的地址到已转换目的地址的映射。随后，NetScreen 设备执行第二次路由查询，确定转发封包的接口，封包必须通过该接口才能到达新的目的地址。总之，指向初始目的地址的路由提供了执行策略查询的方法，指向已转换目的地址的路由则指定了 NetScreen 转发封包使用的出口接口。

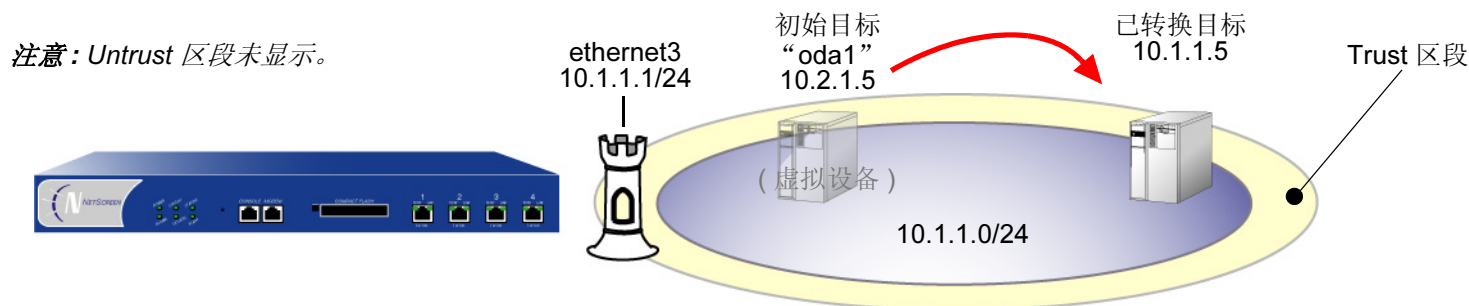
在以下三种情况中，根据策略中引用的目的地址周围的网络拓扑，输入静态路由的需求将有所不同：

set policy from untrust to trust any oda1 http nat dst ip 10.1.1.5 permit

其中 “oda1” 是初始目的地址 10.2.1.5，已转换目的地址为 10.1.1.5。

连接到一个接口的地址

在此情况中，连接初始目的地址和已转换目的地址的路由引导信息流通过同一接口 **ethernet3**。将 **ethernet3** 接口的 IP 地址配置为 **10.1.1.1/24** 时，**NetScreen** 设备会自动添加通过 **ethernet3**、指向 **10.1.1.0/24** 的路由。要完成该路由要求，必须添加一个通过 **ethernet3**、指向 **10.2.1.5/32** 的附加路由。



注意：由于指向 **10.2.1.5** 的路由未指定网关，因此 **10.2.1.5** 不在 **10.1.1.0/24** 子网中。但在图中看来，**10.2.1.5** 与 **10.1.1.0/24** 地址空间似乎在同一个已连接的子网中。

WebUI

Network > Routing > Routing Entries > (trust-vr) New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 10.2.1.5/32

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 0.0.0.0

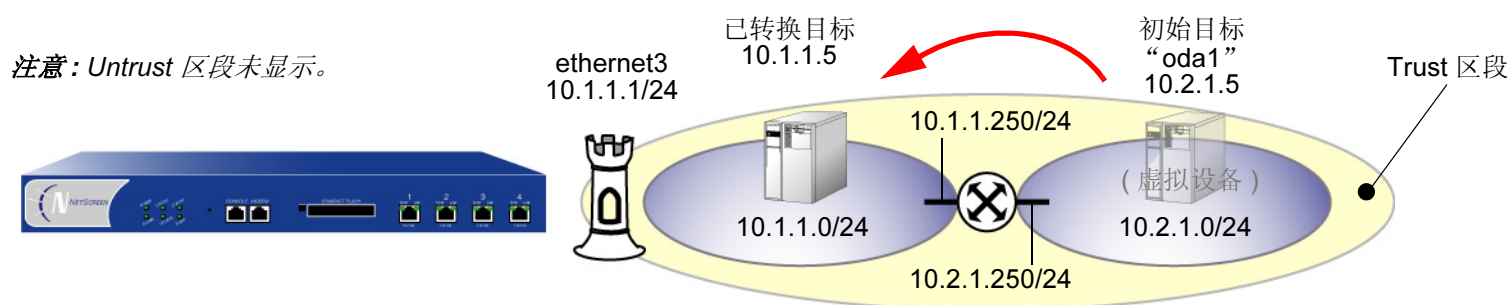
CLI

```
set vrouter trust-vr route 10.2.1.5/32 interface ethernet3
save
```

连接到一个接口但被路由器分隔的地址

在此情况中，连接初始目的地址和已转换目的地址的路由引导信息流通过 **ethernet3**。将 **ethernet3** 接口的 IP 地址配置为 **10.1.1.1/24** 时，**NetScreen** 设备会自动添加通过 **ethernet3**、指向 **10.1.1.0/24** 的路由。要完成该路由要求，必须添加一个通过 **ethernet3**、指向 **10.2.1.0/24** 的路由以及连接 **10.1.1.0/24** 和 **10.2.1.0/24** 子网的网关。

注意：由于需要此路由才能到达 **10.2.1.0/24** 子网中的任意一个地址，因此可能已经配置了该路由。如果已配置该路由，则不必为了让策略将 **NAT-dst** 应用到 **10.2.1.5** 而添加其它路由。



WebUI

Network > Routing > Routing Entries > (trust-vr) New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 10.2.1.0/24

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 10.1.1.250

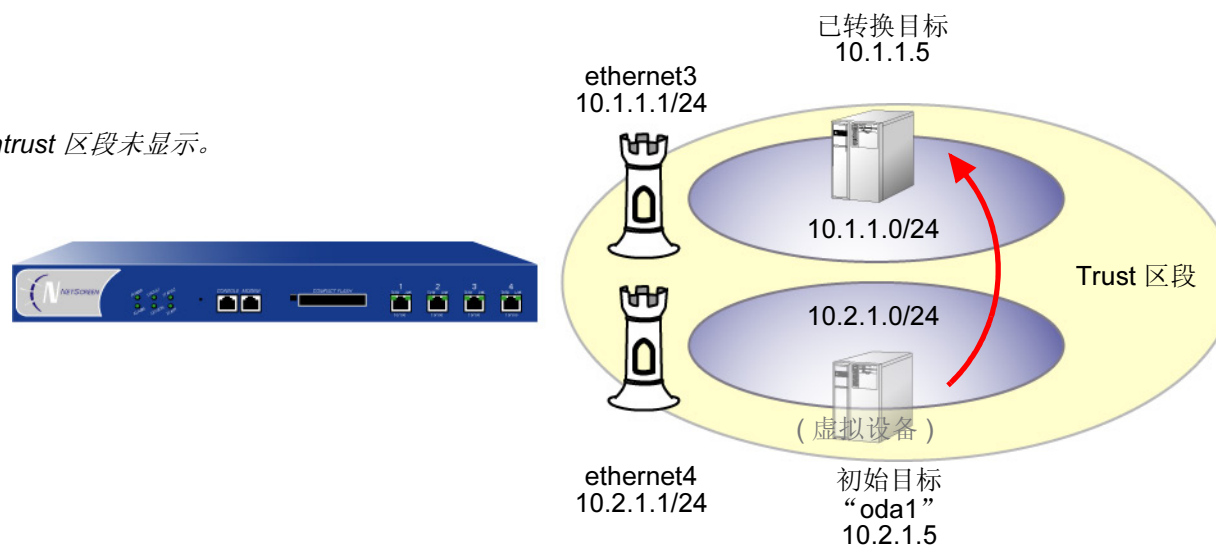
CLI

```
set vrtr trust-vr route 10.2.1.0/24 interface ethernet3 gateway 10.1.1.250
save
```

由接口分隔的地址

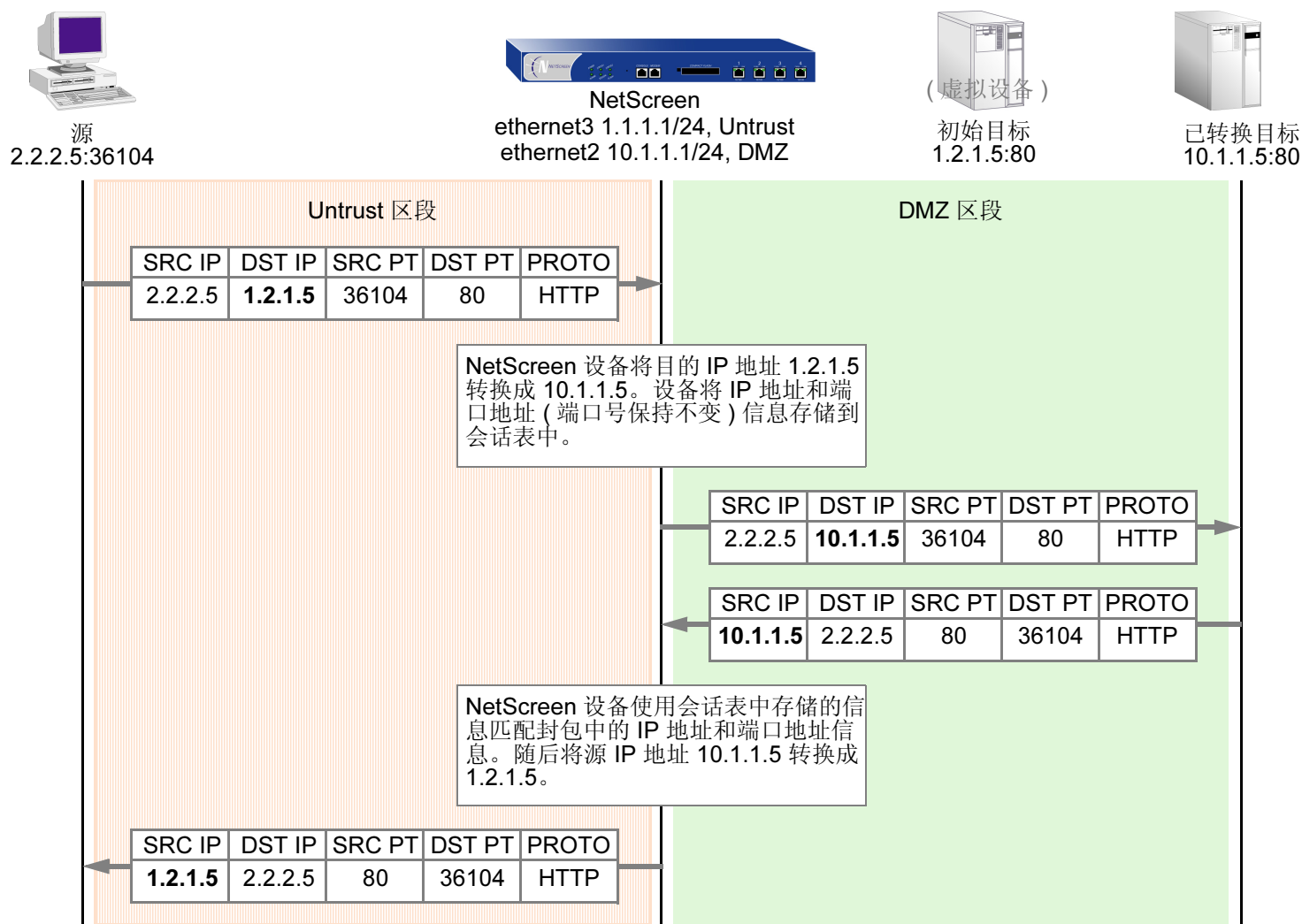
在此情况中，有两个接口绑定到 Trust 区段：IP 地址为 10.1.1.1/24 的 ethernet3 和 IP 地址为 10.2.1.1/24 的 ethernet4。配置这些接口的 IP 地址时，NetScreen 设备会自动添加通过 ethernet3、指向 10.1.1.0/24 的路由和通过 ethernet4、指向 10.2.1.0/24 的路由。将初始目的地址放入 10.2.1.0/24 子网，并将已转换目的地址放入 10.1.1.0/24 子网，就不必为了让设置 NetScreen 设备将 NAT-dst 应用从 10.1.1.5 到 10.2.1.5 而添加其它路由。

注意：Untrust 区段未显示。



NAT-Dst: 一对一映射

应用目的网络地址转换 (NAT-dst) 而不应用端口地址转换时, NetScreen 设备转换目的 IP 地址, 如下图所示执行状态检查 (注意, 只显示 IP 封包包头和 TCP 片段包头中与 NAT-dst 有关的元素):

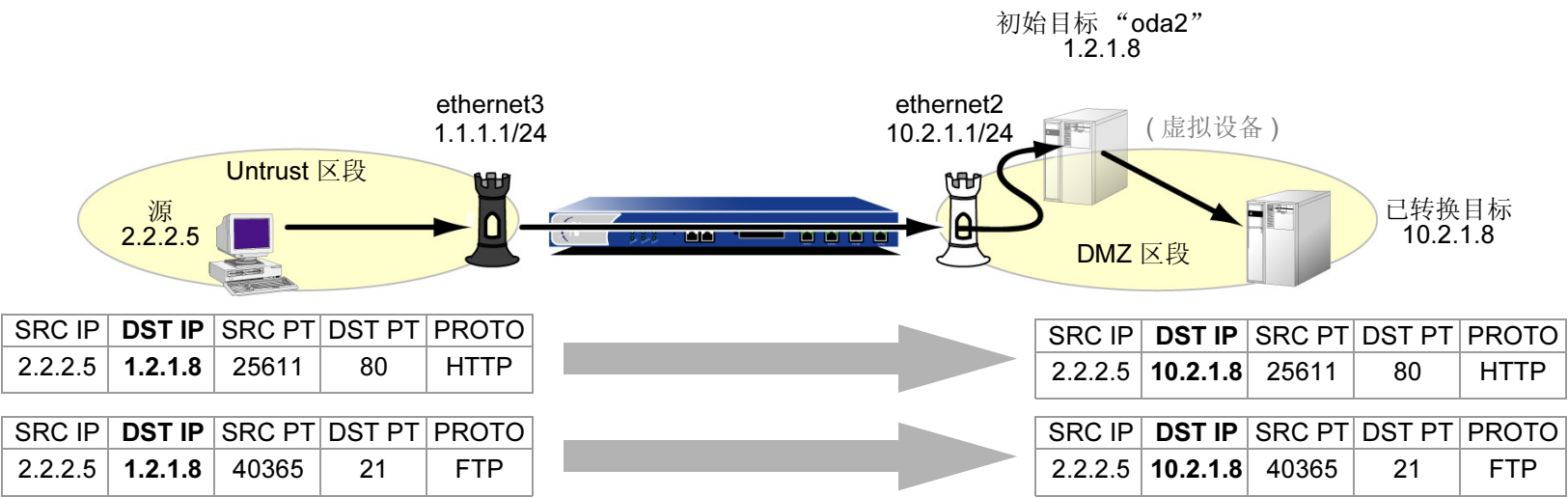


范例：一对一目的地址转换

在本例中，将设置策略，在不更改目的端口地址的情况下，提供一对一的目的网络地址转换 (NAT-dst)。策略指示 NetScreen 设备执行以下任务：

- 允许从 Untrust 区段中任意地址发出的 FTP 和 HTTP 信息流 (定义为服务组 “http-ftp”) 流向 DMZ 区段中名为 “oda2” 的初始目的地址 1.2.1.8。
- 将 IP 封包包头中的目的 IP 地址 1.2.1.8 转换成 10.2.1.8
- 让 TCP 片段包头的初始目的端口号保持不变 (HTTP 为 80、FTP 为 21)
- 将 HTTP 和 FTP 信息流转发到 DMZ 区段中的地址 10.2.1.8

先将 ethernet3 绑定到 Untrust 区段，为其分配 IP 地址 1.1.1.1/24。再将 ethernet2 绑定到 DMZ 区段，为其分配 IP 地址 10.2.1.1/24。还要定义一个通过 ethernet2、指向初始目的地址 1.2.1.8 的路由。Untrust 和 DMZ 区段都在 trust-vr 路由域中。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下信息, 然后单击 **OK**:

Address Name: oda2

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.1.8/32

Zone: DMZ

3. 服务组

Objects > Services > Groups: 输入以下组名称, 移动以下服务, 然后单击 **OK**:

Group Name: HTTP-FTP

选择 **HTTP**, 并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **FTP**, 并使用 << 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 1.2.1.8/32

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

5. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda2

Service: HTTP-FTP

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.8

Map to Port: (清除)

CLI

1. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. 地址

```
set address dmz oda2 1.2.1.8/32
```

3. 服务组

```
set group service http-ftp
set group service http-ftp add http
set group service http-ftp add ftp
```

4. 路由

```
set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
```

5. 策略

```
set policy from untrust to dmz any oda2 http-ftp nat dst ip 10.2.1.8 permit
save
```

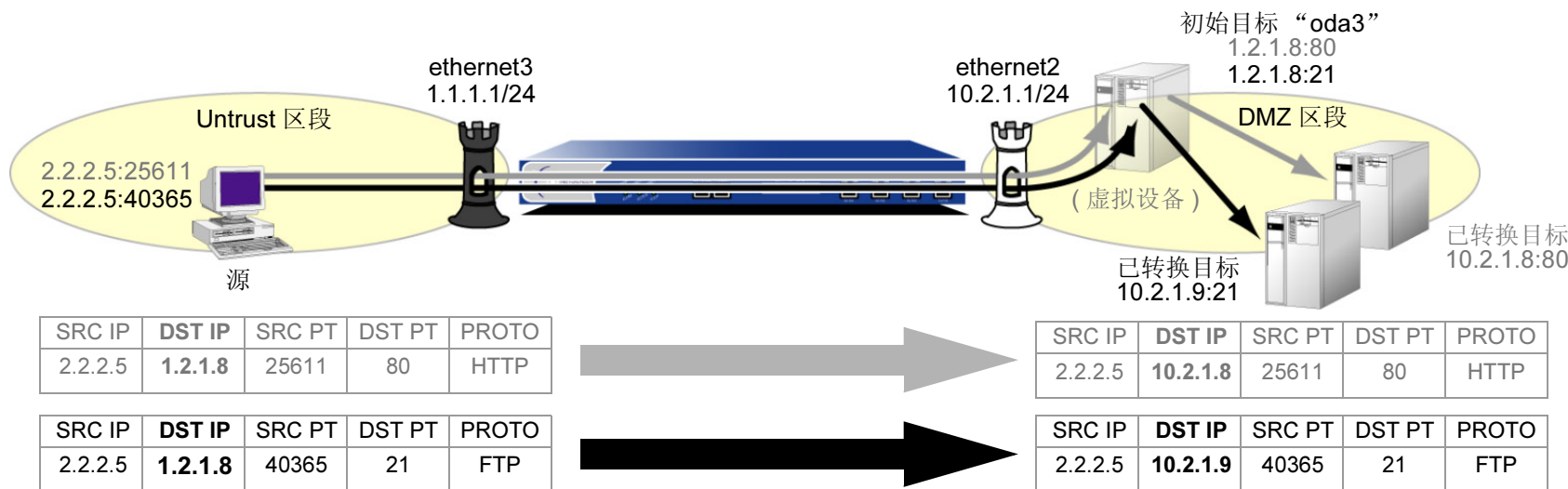

从一个地址到多个地址的转换

根据每个策略中指定的服务或源地址的类型，NetScreen 设备可以将同一初始目的地址转换成不同策略中指定的多个已转换目的地址。您可能希望 NetScreen 设备将 HTTP 信息流从 1.2.1.8 重新定向到 10.2.1.8，将 FTP 信息流从 1.2.1.8 重新定向到 10.2.1.9 (参见上例)。还可能希望 NetScreen 设备将从 host1 发送到 1.2.1.8 的 HTTP 信息流重新定向到 10.2.1.8，将从 host2 发送到 1.2.1.8 的 HTTP 信息流重新定向到 10.2.1.37。在上述两种情况中，NetScreen 设备均将发送到同一初始目的地址的信息流重新定向到多个已转换地址。

范例：一对多目的地址转换

在本例中，将创建两个策略，它们使用相同的初始目的地址 (1.2.1.8)，并根据服务的类型，分别引导信息流发送到两个不同的已转换目的地址。这两个策略指示 NetScreen 设备执行以下任务：

- 将 Untrust 区段中任意地址发出的 FTP 和 HTTP 信息流发送到 DMZ 区段中名为 “oda3” 的用户定义地址
- 对于 HTTP 信息流，将 IP 封包包头中的目的 IP 地址 1.2.1.8 转换成 10.2.1.8
- 对于 FTP 信息流，将目的 IP 地址 1.2.1.8 转换成 10.2.1.9
- 让 TCP 片段包头的初始目的端口号保持不变 (HTTP 为 80，FTP 为 21)
- 将 HTTP 信息流转发到 DMZ 区段中的地址 10.2.1.8，将 FTP 信息流转发到 DMZ 区段中的地址 10.2.1.9



先将 **ethernet3** 绑定到 **Untrust** 区段，为其分配 IP 地址 **1.1.1.1/24**。再将 **ethernet2** 绑定到 **DMZ** 区段，为其分配 IP 地址 **10.2.1.1/24**。还要定义一个通过 **ethernet2**、指向初始目的地址 **1.2.1.8** 的路由。**Untrust** 和 **DMZ** 区段都在 **trust-vr** 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 **ethernet3**): 输入以下内容，然后单击 **OK**:

Zone Name: **Untrust**

Static IP: (出现时选择此选项)

IP Address/Netmask: **1.1.1.1/24**

Network > Interfaces > Edit (对于 **ethernet2**): 输入以下内容，然后单击 **OK**:

Zone Name: **DMZ**

Static IP: (出现时选择此选项)

IP Address/Netmask: **10.2.1.1/24**

2. 地址

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: **oda3**

IP Address/Domain Name:

IP/Netmask: (选择), **1.2.1.8/32**

Zone: **DMZ**

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 1.2.1.8/32

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

4. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda3

Service: HTTP

Action: Permit

> **Advanced**: 输入以下内容, 然后单击 **Return**, 设置高级选项并返回基本配置页:

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.8

Map to Port: (清除)

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda3

Service: FTP

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.9

Map to Port: (清除)

CLI

1. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. 地址

```
set address dmz oda3 1.2.1.8/32
```

3. 路由

```
set vrouter trust-vr route 1.2.1.8/32 interface ethernet2
```

4. 策略

```
set policy from untrust to dmz any oda3 http nat dst ip 10.2.1.8 permit
set policy from untrust to dmz any oda3 ftp nat dst ip 10.2.1.9 permit
save
```

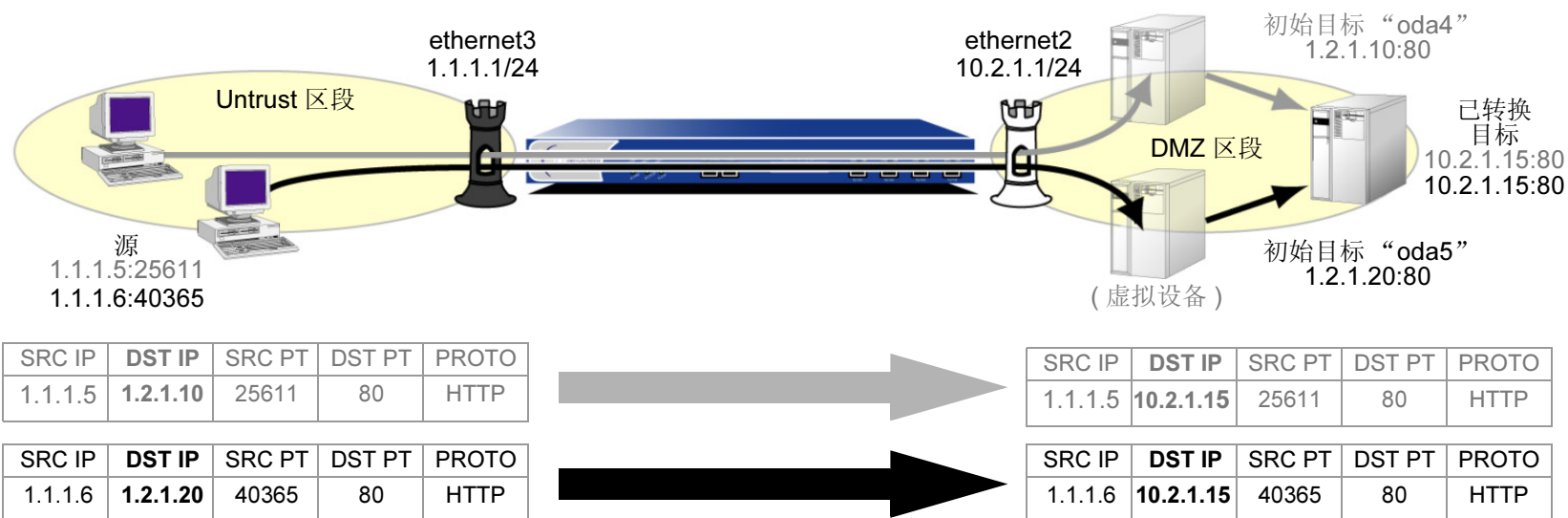
NAT-Dst: 多对一映射

初始目的地址和已转换目的地址之间也可能是多对一关系。在上述情况下，NetScreen 设备将发送到多个初始目的地址的信息流转发到单个已转换目的地址。此外，还可以指定目的端口映射。

范例：多对一目的地址转换

在本例中，创建一个策略，将发送到不同初始目的地址 (1.2.1.10 和 1.2.1.20) 的信息流重新定向到同一个已转换目的地址。本策略指示 NetScreen 设备执行以下任务：

- 允许将 Untrust 区段中任意地址发出的 HTTP 信息流重新定向到名为 “oda45” 的用户定义地址组，其中包括 DMZ 区段中的地址 “oda4” (1.2.1.10) 和 “oda5” (1.2.1.20)。
- 将 IP 封包包头中的目的 IP 地址 1.2.1.10 和 1.2.1.20 转换成 10.2.1.15
- 让 TCP 片段包头的初始目的端口号保持不变 (HTTP 为 80)
- 将 HTTP 信息流转发到 DMZ 区段中的 10.2.1.15



先将 ethernet3 绑定到 Untrust 区段，为其分配 IP 地址 1.1.1.1/24。再将 ethernet2 绑定到 DMZ 区段，为其分配 IP 地址 10.2.1.1/24。还要定义一个通过 ethernet2、指向初始目的地址 1.2.1.10 和 1.2.1.20 的路由。Untrust 和 DMZ 区段都在 trust-vr 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: oda4

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.1.10/32

Zone: DMZ

Objects > Addresses > List > New: 输入以下信息，然后单击 **OK**:

Address Name: oda5

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.1.20/32

Zone: DMZ

Objects > Addresses > Groups > (对于 Zone: DMZ) New: 输入以下组名称，移动以下地址，然后单击 **OK**:

Group Name: oda45

选择 **oda4**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

选择 **oda5**，并使用 << 按钮将地址从 Available Members 栏移动到 Group Members 栏中。

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 1.2.1.10/32

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 1.2.1.20/32

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

4. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda45

Service: HTTP

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.15

Map to Port: (清除)

CLI

1. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. 地址

```
set address dmz oda4 1.2.1.10/32
set address dmz oda5 1.2.1.20/32
set group address dmz oda45 add oda4
set group address dmz oda45 add oda5
```

3. 路由

```
set vrouter trust-vr route 1.2.1.10/32 interface ethernet2
set vrouter trust-vr route 1.2.1.20/32 interface ethernet2
```

4. 策略

```
set policy from untrust to dmz any oda45 http nat dst ip 10.2.1.15 permit
save
```

NAT-Dst: 多对多映射

可以使用目的网络地址转换 (NAT-dst) 将一个 IP 地址范围转换成另一个地址范围。该地址范围可以是子网或更小的子网内地址集合。NetScreen 使用地址变换机制维护初始目的地址范围与转换后新地址范围之间的关系。例如，如果初始地址范围为 10.1.1.1 – 10.1.1.50，而已转换地址范围的起始地址为 10.100.3.101，NetScreen 设备将进行如下地址转换：

- 10.1.1.1 – 10.100.3.101
- 10.1.1.2 – 10.100.3.102
- 10.1.1.3 – 10.100.3.103
- ...
- 10.1.1.48 – 10.100.3.148
- 10.1.1.49 – 10.100.3.149
- 10.1.1.50 – 10.100.3.150

例如，如果希望创建一个策略对 HTTP 信息流应用上述转换，该信息流从 zoneA 中的任意地址流向名为“addr1-50”的地址组，且地址组中包含 zoneB 中从 10.1.1.1 到 10.1.1.50 的所有地址，则可输入以下 CLI 命令：

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
10.100.3.150 permit
```

如果 zoneA 中的主机发起到 zoneB 定义范围内任意地址 (如 10.1.1.37) 的 HTTP 信息流，NetScreen 设备会应用此策略将目的地址转换成 10.100.3.137。

如果策略中指定的源地址、目的地址及服务与封包中的对应部分完全匹配，则 NetScreen 设备只执行 NAT-dst。例如，您可能创建另一个策略，允许 zoneA 中任意主机发出的信息流流向 zoneB 中的任意主机，然后在策略列表中将策略置于策略 1 之后：

```
set policy id 1 from zoneA to zoneB any addr1-50 http nat dst ip 10.100.3.101
10.100.3.150 permit
set policy id 2 from zoneA to zoneB any any any permit
```

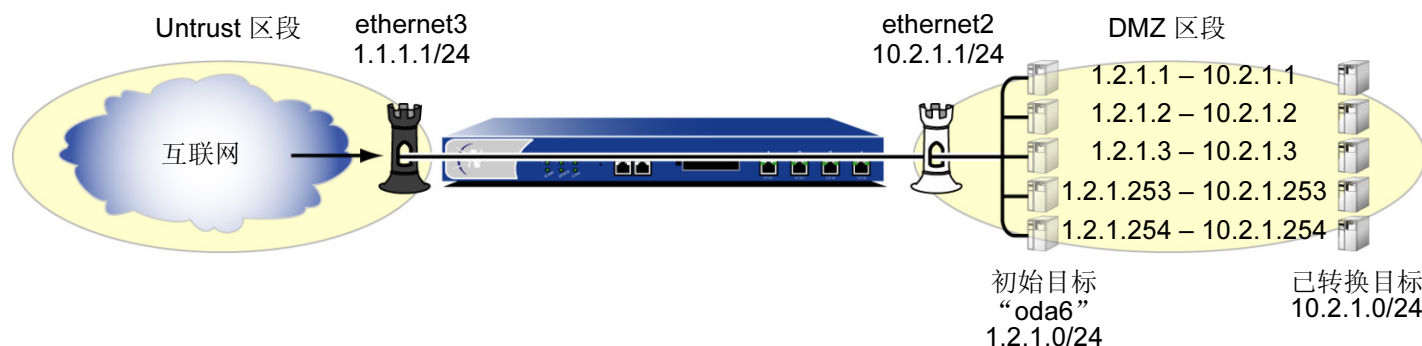
如果已配置这两个策略，设备将避开 NAT-dst 机制将以下类型的信息流从 zoneA 中的主机发送到 zoneB 中的主机：

- ZoneA 中的主机发起到 zoneB 中 10.1.1.37 的非 HTTP 信息流。由于信息流的服务类型不是 HTTP，因此 NetScreen 设备会应用策略 2，只传递信息流而不转换目的地址。
- ZoneA 中的主机发起到 zoneB 中 10.1.1.51 的 HTTP 信息流。由于目的地址不在 addr1-50 地址组中，因此 NetScreen 设备仍会应用策略 2，只传递信息流而不转换目的地址。

范例：多对多目的地址转换

在本例中，将配置一个策略，当任意类型的信息流发送到子网中的任意主机时应用 NAT-dst，并指示 NetScreen 设备执行以下任务：

- 允许 Untrust 区段中任意地址发出的所有类型的信息流流向 DMZ 区段中的任意地址
- 将 1.2.1.0/24 子网中名为 “oda6” 的初始目的地址转换成 10.2.1.0/24 子网中的相应地址
- 让 TCP 片段包头的初始目的端口号保持不变
- 将 HTTP 信息流转发到 DMZ 区段中的已转换地址



先将 ethernet3 绑定到 Untrust 区段，为其分配 IP 地址 1.1.1.1/24。再将 ethernet2 绑定到 DMZ 区段，为其分配 IP 地址 10.2.1.1/24。还要定义一个通过 ethernet2、指向初始目的地址子网 (1.2.1.0/24) 的路由。Untrust 和 DMZ 区段都在 trust-vr 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下信息, 然后单击 **OK**:

Address Name: oda6

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.1.0/24

Zone: DMZ

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 1.2.1.0/24

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

4. 策略

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda6

Service: Any

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.2.1.0 – 10.2.1.254

CLI

1. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

2. 地址

```
set address dmz oda6 1.2.1.0/24
```

3. 路由

```
set vrouter trust-vr route 1.2.1.0/24 interface ethernet2
```

4. 策略

```
set policy from untrust to dmz any oda6 any nat dst ip 10.2.1.1 10.2.1.254
    permit
save
```

带有端口映射的 NAT-Dst

配置 NetScreen 设备执行目的网络地址转换 (NAT-dst) 时, 也可启用端口映射。启用端口映射的原因之一是为了在一台主机上支持单个服务的多个服务器进程。例如, 一台主机可以运行两个 Web 服务器 (一个在端口 80 上, 另一个在端口 8081 上)。对于 HTTP 服务 1, NetScreen 设备执行 NAT-dst 而不执行端口映射 (dst 端口 80 -> 80)。对于 HTTP 服务 2, NetScreen 设备在相同目的 IP 地址上执行 NAT-dst, 并执行端口映射 (dst 端口 80 -> 8081)。通过两个不同的目的端口号, 主机能将 HTTP 信息流划分给两个 Web 服务器。

注意: NetScreen 设备不支持带有地址变换的 NAT-dst 的端口映射。请参阅第 316 页上的 “NAT-Dst: 多对多映射”。

范例: 带有端口映射的 NAT-Dst

在本例中, 将创建两个策略, 在从 Trust、Untrust 区段到 DMZ 区段 Telnet 服务器的 Telnet 信息流上执行 NAT-dst 和端口映射。这两个策略指示 NetScreen 设备执行以下任务:

- 允许 Untrust、Trust 区段中任意地址发出的 Telnet 信息流流向 DMZ 区段中的地址 1.2.1.15
- 将名为 “oda7” 的初始目的 IP 地址 1.2.1.15 转换成 10.2.1.15
- 将 TCP 片段包头的初始目的端口号 23 转换成 2200
- 将 Telnet 信息流转发到 DMZ 区段中的已转换地址

配置以下 “接口到区段” 的绑定信息和地址分配:

- ethernet1: Trust 区段, 10.1.1.1/24
- ethernet2: DMZ 区段, 10.2.1.1/24
- ethernet3: Untrust 区段, 1.1.1.1/24

在 DMZ 区段定义一个 IP 地址为 1.2.1.15/32 的地址条目 “oda7”。再定义一个通过 ethernet2、指向初始目的地址 1.2.1.15 的路由。Trust、Untrust 和 DMZ 区段都在 trust-vr 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.1.1/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

Objects > Addresses > List > New: 输入以下信息, 然后单击 **OK**:

Address Name: oda7

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.1.15/32

Zone: DMZ

3. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 1.2.1.15/32

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 0.0.0.0

4. 策略

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda7

Service: Telnet

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.15

Map to Port: (选择), 2200

Policies > (From: Untrust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), oda7

Service: Telnet

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.2.1.15

Map to Port: (选择), 2200

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 10.2.1.1/24
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address dmz oda7 1.2.1.15/32
```

3. 路由

```
set vrouter trust-vr route 1.2.1.15/32 interface ethernet2
```

4. 策略

```
set policy from trust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200
    permit
set policy from untrust to dmz any oda7 telnet nat dst ip 10.2.1.15 port 2200
    permit
save
```

同一策略中的 NAT-Src 和 NAT-Dst

可以在同一策略中结合使用源网络地址转换 (NAT-src) 和目的网络地址转换 (NAT-dst)。二者的结合为您带来了一种方法，即在数据路径的单一点上同时更改源 IP 地址和目的 IP 地址。

范例：结合 NAT-Src 和 NAT-Dst

在本例中，在服务提供商的客户与服务器群组之间配置 NetScreen 设备 (NetScreen-1)。客户通过 ethernet1 (IP 地址为 10.1.1.1/24，且绑定到 Trust 区段) 连接 NetScreen-1。随后，NetScreen-1 将通过基于路由的两个 VPN 通道之一将信息流转发到目标服务器¹¹。绑定到这两个通道的接口处于 Untrust 区段中。Trust 和 Untrust 区段都在 trust-vr 路由域中。

由于客户拥有的地址可能与要连接服务器的地址相同，因此 NetScreen-1 必须同时执行源地址转换 (NAT-src) 和目的地址转换 (NAT-dst)。为确保地址转换的独立性与灵活性，NetScreen 设备通过执行 NAT-dst 保护服务器群组 NetScreen-A 和 NetScreen-B。出于上述目的，服务提供商会指示客户和服务器群组的管理员保留以下地址：10.173.10.1–10.173.10.7、10.173.20.0/24、10.173.30.0/24 和 10.173.40.0/24。这些地址的用途如下：

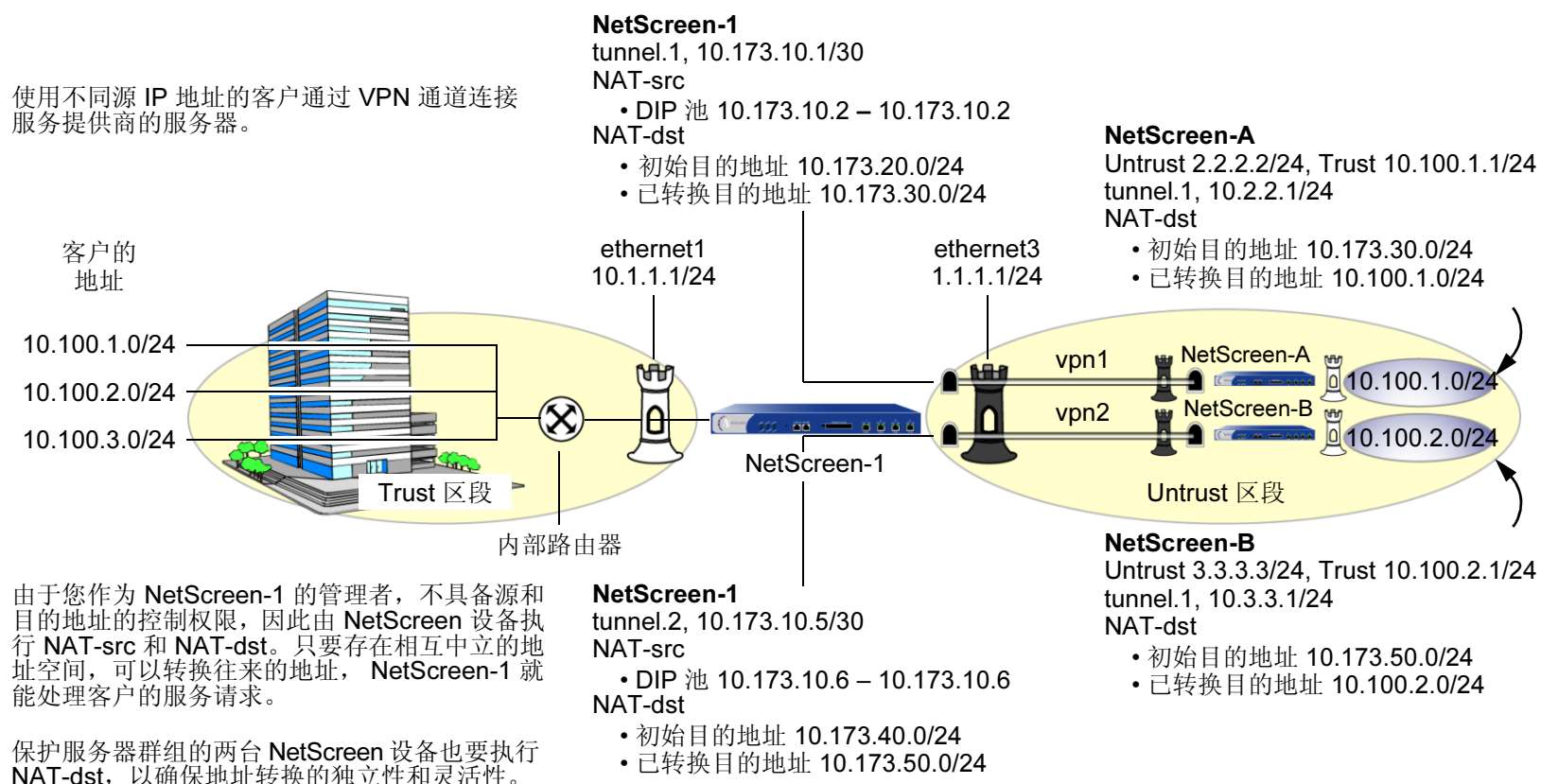
- 两个通道接口分配到下列地址：
 - tunnel.1, 10.173.10.1/30
 - tunnel.2, 10.173.10.5/30
- 每个通道接口都支持以下 DIP 池 (启用 PAT)：
 - tunnel.1, DIP ID 5: 10.173.10.2–10.173.10.2
 - tunnel.2, DIP ID 6: 10.173.10.6–10.173.10.6
- NetScreen-1 执行 NAT-dst 时，使用地址变换转换初始目的地址，如下所示¹²：
 - 10.173.20.0/24 到 10.173.30.0/24
 - 10.173.40.0/24 到 10.173.50.0/24

11. 基于策略的 VPN 不支持 NAT-dst。必须将基于路由的 VPN 配置与 NAT-dst 一起使用。

12. 有关执行 NAT-dst 时使用的地址变换信息，请参阅第 316 页上的“NAT-Dst: 多对多映射”。

配置 vpn1 和 vpn2 这两个通道时将用到以下参数：AutoKey IKE、预共享密钥 (vpn1 为 “netscreen1”，vpn2 为 “netscreen2”) 以及为 “阶段 1” 和 “阶段 2” 提议预定义的安全级别 “Compatible (兼容)”。(有关上述提议的详细信息，请参阅第 5-11 页上的 “通道协商”)。vpn1 和 vpn2 的代理 ID 均为 0.0.0.0/0 - 0.0.0.0/0 - any。

注意：先给出 NetScreen-1 的配置。接着是 NetScreen-A 和 NetScreen-B 的 VPN 配置，合起来即得到完整的配置信息。



WebUI (NetScreen-1)

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.173.10.1/30

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.173.10.5/30

2. DIP 池

Network > Interfaces > Edit (对于 tunnel.1) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 5

IP Address Range: (选择), 10.173.10.2 ~ 10.173.10.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

Network > Interfaces > Edit (对于 tunnel.2) > DIP > New: 输入以下内容, 然后单击 **OK**:

ID: 6

IP Address Range: (选择), 10.173.10.6 ~ 10.173.10.6

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 地址

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

Address Name: serverfarm-A

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.20.0/24

Zone: Untrust

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

Address Name: serverfarm-B

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.40.0/24

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**：

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw-A

Type: Static IP: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3¹³

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

13. 外向接口不一定位于通道接口绑定到的区段中，但在本例中二者位于同一区段。

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**：

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw-B

Type: Static IP: (选择), Address/Hostname: 3.3.3.3

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.2

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

5. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.173.20.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.173.30.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.173.40.0/24

Gateway: (选择)

Interface: tunnel.2

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.173.50.0/24

Gateway: (选择)

Interface: tunnel.2

Gateway IP Address: 0.0.0.0

6. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), serverfarm-A

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：

NAT:

Source Translation: (选择)

(DIP on): 5 (10.173.10.2–10.173.10.2)/X-late

Destination Translation: (选择)

Translate to IP Range: (选择), 10.173.30.0 – 10.173.30.255

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), serverfarm-B

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：

NAT:

Source Translation: (选择)

(DIP on): 6 (10.173.10.6–10.173.10.6)/X-late

Destination Translation: (选择)

Translate to IP Range: (选择), 10.173.50.0 – 10.173.50.255

CLI (NetScreen-1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.173.10.1/30

set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.173.10.5/30
```

2. DIP 池

```
set interface tunnel.1 dip-id 5 10.173.10.2 10.173.10.2
set interface tunnel.2 dip-id 6 10.173.10.6 10.173.10.6
```

3. 地址

```
set address untrust serverfarm-A 10.173.20.0/24
set address untrust serverfarm-B 10.173.40.0/24
```

4. VPN

```
set ike gateway gw-A ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway gw-A sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

```
set ike gateway gw-B ip 3.3.3.3 main outgoing-interface ethernet3 preshare
netscreen2 sec-level compatible
set vpn vpn2 gateway gw-B sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.173.20.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface tunnel.1
set vrouter trust-vr route 10.173.40.0/24 interface tunnel.2
set vrouter trust-vr route 10.173.50.0/24 interface tunnel.2
```

6. 策略

```
set policy top from trust to untrust any serverfarm-A any nat src dip-id 5 dst
ip 10.173.30.0 10.173.30.255 permit
set policy top from trust to untrust any serverfarm-B any nat src dip-id 6 dst
ip 10.173.50.0 10.173.50.255 permit
save
```

WebUI (NetScreen-A)

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.100.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.2.2.1/24

2. 地址

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

Address Name: serverfarm-A

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.30.0/24

Zone: Trust

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

Address Name: customer1

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.10.2/32

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw-1

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 10.173.10.2/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 10.173.30.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**：

Source Address:

Address Book Entry: (选择), customer1

Destination Address:

Address Book Entry: (选择), serverfarm-A

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.100.1.0 – 10.100.1.255

CLI (NetScreen-A)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.2.2.1/24
```

2. 地址

```
set address trust serverfarm-A 10.173.30.0/24
set address untrust customer1 10.173.10.2/32
```

3. VPN

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway gw-1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.173.10.2/32 interface tunnel.1
set vrouter trust-vr route 10.173.30.0/24 interface ethernet1
```

5. 策略

```
set policy top from untrust to trust customer1 serverfarm-A any nat dst ip
    10.100.1.0 10.100.1.255 permit
save
```

WebUI (NetScreen-B)

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.100.2.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **OK**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.3.3.1/24

2. 地址

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

Address Name: serverfarm-B

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.50.0/24

Zone: Trust

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

Address Name: customer1

IP Address/Domain Name:

IP/Netmask: (选择), 10.173.10.6/32

Zone: Untrust

3. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw-1

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 10.173.10.6/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 10.173.50.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), customer1

Destination Address:

Address Book Entry: (选择), serverfarm-B

Service: ANY

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.100.2.0 – 10.100.2.255

CLI (NetScreen-B)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.100.2.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
```

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.3.3.1/24
```

2. 地址

```
set address trust serverfarm-B 10.173.50.0/24
set address untrust customer1 10.173.10.6/32
```

3. VPN

```
set ike gateway gw-1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare
  netscreen2 sec-level compatible
set vpn vpn2 gateway gw-1 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
set vrouter trust-vr route 10.173.10.6/32 interface tunnel.1
set vrouter trust-vr route 10.173.50.0/24 interface ethernet1
```

5. 策略

```
set policy top from untrust to trust customer1 serverfarm-B any nat dst ip
  10.100.2.0 10.100.2.255 permit
save
```

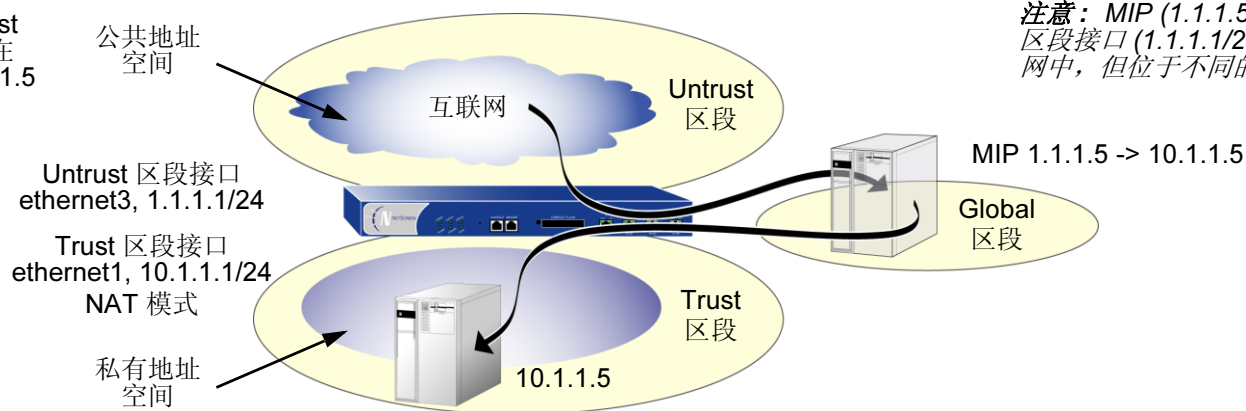

映射 IP 地址

映射 IP (MIP) 是从一个 IP 地址到另一个 IP 地址的直接一对一映射。NetScreen 设备将目的地为 MIP 的内向信息流转发至地址为 MIP 指向地址的主机。实际上，MIP 是一个静态目的地址转换，将 IP 封包包头中的目的 IP 地址映射成另一个静态 IP 地址。MIP 主机发起出站信息流时，NetScreen 设备将该主机的源 IP 地址转换成 MIP 地址的源 IP 地址。这一对称的双向转换不同于源和目的地址转换的行为 (请参阅第 273 页上的“NAT-Src 和 NAT-Dst 的方向特性”)。

MIP 允许入站信息流到达接口模式为 NAT 的区段中的私有地址。MIP 还部分解决通过 VPN 通道连接的两个站点之间地址空间重叠的¹⁴问题。(有关此问题完整的解决方案，请参阅第 5-168 页上的“具有重叠地址的 VPN 站点”。)

可在以下接口所在的子网中创建 MIP: 带有 IP 地址 / 网络掩码的通道接口或绑定到第 3 层 (L3) 安全区且带有 IP 地址 / 网络掩码的接口¹⁵。虽然 MIP 是为绑定到通道区段和安全区的接口配置的，但是定义的 MIP 存储在 Global 区段。

映射 IP: 来自 Untrust 区段的入站信息流在 Trust 区段从 210.1.1.5 映射到 10.1.1.5。



14. 重叠地址空间就是当两个网络中 IP 地址范围部分或全部相同时的空间。

15. 为 Untrust 区段中接口定义的 MIP 例外。该 MIP 可以在不同于 Untrust 区段接口 IP 地址的子网中。但是，如果真是这样，就必须在外置路由器上添加一条路由，指向 Untrust 区段接口，以便内向信息流能到达 MIP。此外，必须在与 MIP 相关的 NetScreen 设备上定义一个静态路由，该设备还具备能执行 MIP 的接口。

注意：在一些 NetScreen 设备上，MIP 可使用与接口相同的地址，但是 MIP 地址不能在 DIP 池中。

可映射“地址到地址”或“子网到子网”关系。定义“子网到子网”映射 IP 配置后，映射 IP 子网和原始 IP 子网都将应用网络掩码。

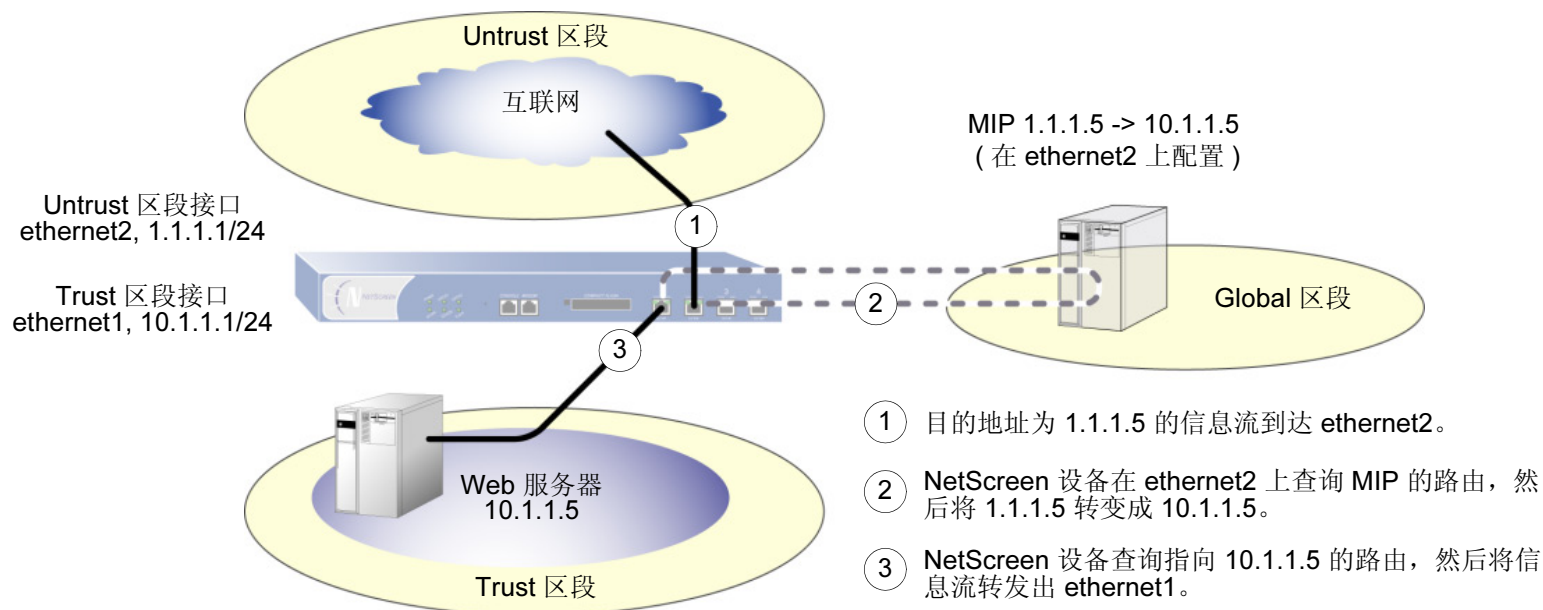
MIP 和 Global 区段

无论设置哪个区段接口的 MIP，都会在 Global 区段的通讯簿中生成该 MIP 的条目。Global 区段通讯簿存储所有 MIP 地址，不管其接口属于哪一个区段。可以将这些 MIP 地址用作两个区段间策略的目的地址，还可以用作定义全局策略时的目的地址。(有关全局策略的信息，请参阅第 217 页上的“全局策略”)。尽管 NetScreen 设备将 MIP 地址存储在 Global 区段中，但在策略中引用 MIP 时，既可以使用 Global 区段，也可以使用 MIP 指向的目的区段(以地址形式表示)。

范例 : Untrust 区段接口上的 MIP

在本例中，将 **ethernet1** 绑定到 **Trust** 区段并为其分配 IP 地址 **10.1.1.1/24**。将 **ethernet2** 绑定到 **Untrust** 区段并为其分配 IP 地址 **1.1.1.1/24**。然后配置 **MIP**，将目的地址为 **Untrust** 区段中 **1.1.1.5** 的内向 HTTP 信息流发送到 **Trust** 区段地址为 **10.1.1.5** 的 Web 服务器。最后，要创建一个策略，允许 HTTP 信息流从 **Untrust** 区段的任意地址流向 **Trust** 区段的 MIP 地址（始终流向 MIP 指向的地址上的主机）。所有安全区域都在 **trust-vr** 路由域中。

注意：映射 IP 或 MIP 指向的主机不需要通讯簿条目。



WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. MIP

Network > Interfaces > Edit (对于 ethernet2) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

3. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.5)

Service: HTTP

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
```

2. MIP

```
set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.25516
vrouter trust-vr17
```

3. 策略

```
set policy from untrust to trust any mip(1.1.1.5) http permit
save
```

16. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，将地址映射到单个主机。还可为某个范围内的地址定义 MIP。例如，要通过 CLI 将 1.1.1.5 定义为 C 类子网中地址 10.1.10.129 - 10.1.10.254 的 MIP，请使用以下语法：**set interface interface mip 1.1.1.5 host 10.1.10.128 netmask 255.255.255.128**。小心切勿使用包括接口或路由器地址的地址范围。

17. 缺省的虚拟路由器为 trust-vr。不必指定虚拟路由器为 trust-vr 或 MIP 有 32 位网络掩码。此命令中包含这些参数，以便和 WebUI 配置对称。

范例：从不同区段到达 MIP

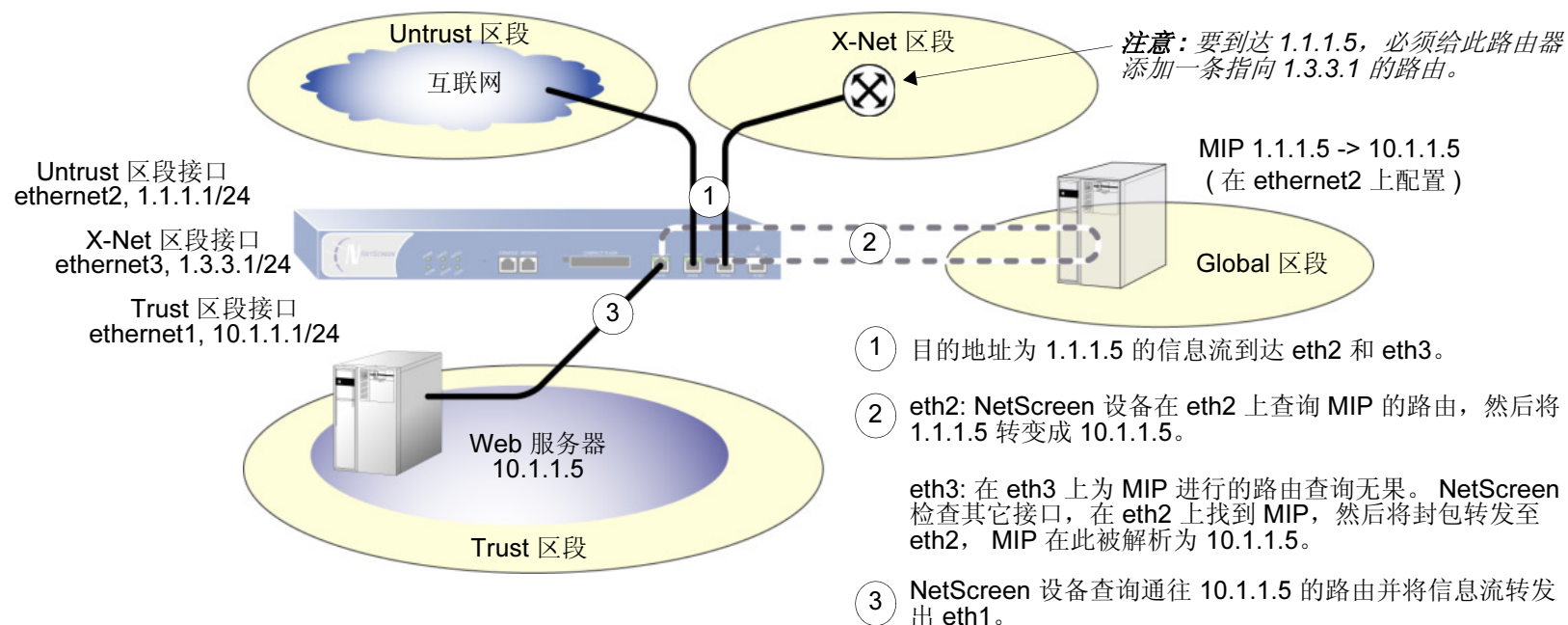
来自不同区段的信息流仍可通过其它接口 (而非您在其上配置 MIP 的接口) 到达 MIP。要完成上述操作, 必须在其它各个区段的路由器上设置路由, 将入站信息流指向它们各自接口的 IP 地址, 以到达 MIP¹⁸。

在本例中, 将在 Untrust 区段 (ethernet2, 1.1.1.1/24) 的接口上配置 MIP (1.1.1.5), 以映射到 Trust 区段 (10.1.1.5) 中的 Web 服务器。绑定到 Trust 区段的接口是 IP 地址为 10.1.1.1/24 的 ethernet1。

创建名为 X-Net 的安全区, 将 ethernet3 绑定到该区段, 然后给接口分配 IP 地址 1.3.3.1/24。定义地址 1.1.1.5, 以便在策略中使用, 该策略允许 HTTP 信息流从 X-Net 区段的任意地址流向 Untrust 区段的 MIP。还将配置一个策略, 允许 HTTP 信息流从 Untrust 区段流向 Trust 区段。所有安全区域都在 trust-vr 路由域中。

注意：必须在 X-Net 区段的路由器上输入一条路由, 引导目的地址为 1.1.1.5 (MIP) 的信息流流向 1.3.3.1 (ethernet3 的 IP 地址)。

18. 如果 MIP 与接口 (在该接口上配置 MIP) 在相同的子网中, 则不必为了使信息流通过不同的接口到达 MIP, 而添加到 NetScreen 设备的路由。但是, 如果 MIP 在与其接口的 IP 地址不同的子网中 (仅对于 Untrust 区段中接口上的 MIP 才可能出现这种情况), 则必须将一条静态路由添加至 NetScreen 路由选择表。使用 `set vrouter name_str route ip_addr interface interface` 命令 (或 WebUI 中的等同命令), 其中, `name_str` 是指定接口所属的虚拟路由器, `interface` 是在其上配置 MIP 的接口。



WebUI

1. 接口和区段

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **OK**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet2): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Zones > New: 输入以下内容, 然后单击 **OK**:

Zone Name: X-Net

Virtual Router Name: untrust-vr

Zone Type: Layer 3

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: X-Net

IP Address/Netmask: 1.3.3.1/24

2. 地址

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

Address Name: 1.1.1.5

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/32

Zone: Untrust

3. MIP

Network > Interfaces > Edit (对于 ethernet2) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

4. 策略

Policies > (From: X-Net, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), 1.1.1.5

Service: HTTP

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.5)

Service: HTTP

Action: Permit

CLI

1. 接口和区段

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
```

```
set zone name X-Net
set interface ethernet3 zone X-Net
set interface ethernet3 ip 1.3.3.1/24
```

2. 地址

```
set address untrust "1.1.1.5" 1.1.1.5/32
```

3. MIP

```
set interface ethernet2 mip 1.1.1.5 host 10.1.1.5 netmask 255.255.255.255
vrouter trust-vr19
```

4. 策略

```
set policy from X-Net to untrust any "1.1.1.5" http permit
set policy from untrust to trust any mip(1.1.1.5) http permit
save
```

19. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

范例：将 MIP 添加到 Tunnel 接口

在本例中，Trust 区段中网络的 IP 地址空间为 10.1.1.0/24，通道接口 “tunnel.8” 的 IP 地址为 10.20.3.1。Trust 区段中网络上服务器的物理 IP 地址为 10.1.1.25。为了允许一个远程网站（其网络在 Trust 区段中）使用重叠地址空间，通过 VPN 通道访问本地服务器，在 tunnel.8 接口所在的相同子网中创建 MIP。MIP 地址为 10.20.3.25/32。（有关带有 Tunnel 接口的 MIP 的完整范例，请参阅第 5-168 页上的“具有重叠地址的 VPN 站点”。）

WebUI

Network > Interfaces > Edit (对于 tunnel.8) > MIP > New: 输入以下内容，然后单击 **OK**:

Mapped IP: 10.20.3.25

Netmask: 255.255.255.255

Host IP Address: 10.1.1.25

Host Virtual Router Name: trust-vr

CLI

```
set interface tunnel.8 mip 10.20.3.25 host 10.1.1.25 netmask 255.255.255.255
vrouter trust-vr20
save
```

注意：远程管理员将服务器地址添加到他的 Untrust 区段通讯簿时，必须输入 MIP (10.20.3.25)，而不是服务器的物理 IP 地址 (10.1.1.25)。

远程管理员还需要对通过 VPN 发往服务器的外向封包应用基于策略的 NAT (使用 DIP)，以便本地管理员可添加与本地 Trust 区段地址不冲突的 Untrust 区段地址。否则，内向策略中的源地址会看似在 Trust 区段中。

20. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

MIP-Same-as-Untrust

由于 IPv4 地址越来越少，ISP 越来越不愿意分配给客户多于一个或两个 IP 地址。如果绑定到 Untrust 区段的接口只有一个 IP 地址 (绑定到 Trust 区段的接口处于 “网络地址转换” (NAT) 模式)，则可将 Untrust 区段接口的 IP 地址用作映射 IP (MIP)，以提供对内部服务器、主机、VPN 或 L2TP 通道端点的入站访问。

MIP 将到达一个地址的信息流映射到另一个地址，因此，通过使用 Untrust 区段接口的 IP 地址作为 MIP，NetScreen 设备将使用 Untrust 区段接口的所有入站信息流映射到指定内部地址。如果 Untrust 接口上的 MIP 被映射到 VPN 或 L2TP 通道端点，只要 Untrust 接口上没有配置 VPN 或 L2TP 通道，设备会自动将收到的 IKE 或 L2TP 封包转发到通道端点。

如果创建一个策略，在该策略中，目的地地址是使用 Untrust 区段接口 IP 地址的 MIP，并且指定 HTTP 充当该策略中的服务，那么您就失去经由该接口对 NetScreen 设备进行 Web 管理的能力 (因为流向该地址的所有入站 HTTP 信息流都被映射到内部服务器或主机)。通过更改 Web 管理的端口号，仍然可以使用 WebUI 通过 Untrust 区段接口管理该设备。要更改 Web 管理端口号，请执行以下操作：

1. Admin > Web: 在 “HTTP Port” 字段输入注册的端口号 (从 1024 到 65,535)。然后单击 **Apply**。
2. 下一次连接到 Untrust 区段接口管理该设备时，请将此端口号附加到 IP 地址 — 例如，
`http://209.157.66.170:5000`。

范例 : Untrust 接口上的 MIP

在本例中, 将选择 Untrust 区段接口 (ethernet3, 1.1.1.1/24) 的 IP 地址作为 Web 服务器的 MIP, 该 Web 服务器的实际 IP 地址为 Trust 区段中的 10.1.1.5。由于希望保持对 ethernet3 接口的 Web 管理访问, 因此将 Web 管理的端口号更改为 8080。随后, 将创建一个策略, 允许 HTTP 服务 (在 HTTP 缺省端口 80 上) 从 Untrust 区段流向 Trust 区段的 MIP 地址 (始终流向 MIP 指向地址上的主机)。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容, 然后单击 **OK**:

NAT:²¹ (选择)

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. HTTP Port

Configuration > Admin > Management: 在 “HTTP Port” 字段键入 **8080**, 然后单击 **Apply**。

(失去 HTTP 连接。)

21. 缺省情况下, 绑定到 Trust 区段的任意接口都处于 NAT 模式。因此, 对于绑定到 Trust 区段的接口, 此选项已经启用。

3. 重新连接

重新连接到 NetScreen 设备，将 8080 附加到 web 浏览器 URL 地址字段的 IP 地址。(如果您当前正通过 Untrust 接口管理设备，请键入 **http://1.1.1.1:8080**。)

4. MIP

Network > Interface > Edit (对于 ethernet3) > MIP > New: 输入以下内容，然后单击 **OK**:

Mapped IP: 1.1.1.1

Netmask: 255.255.255.255²²

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

5. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.1)

Service: HTTP

Action: Permit

22. 使用 Untrust 区段接口 IP 地址的 MIP 的网络掩码必须为 32 位。

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. HTTP 端口

```
set admin port 8080
```

3. MIP

```
set interface ethernet3 mip 1.1.1.1 host 10.1.1.5 netmask 255.255.255.255
vrouter trust-vr23
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

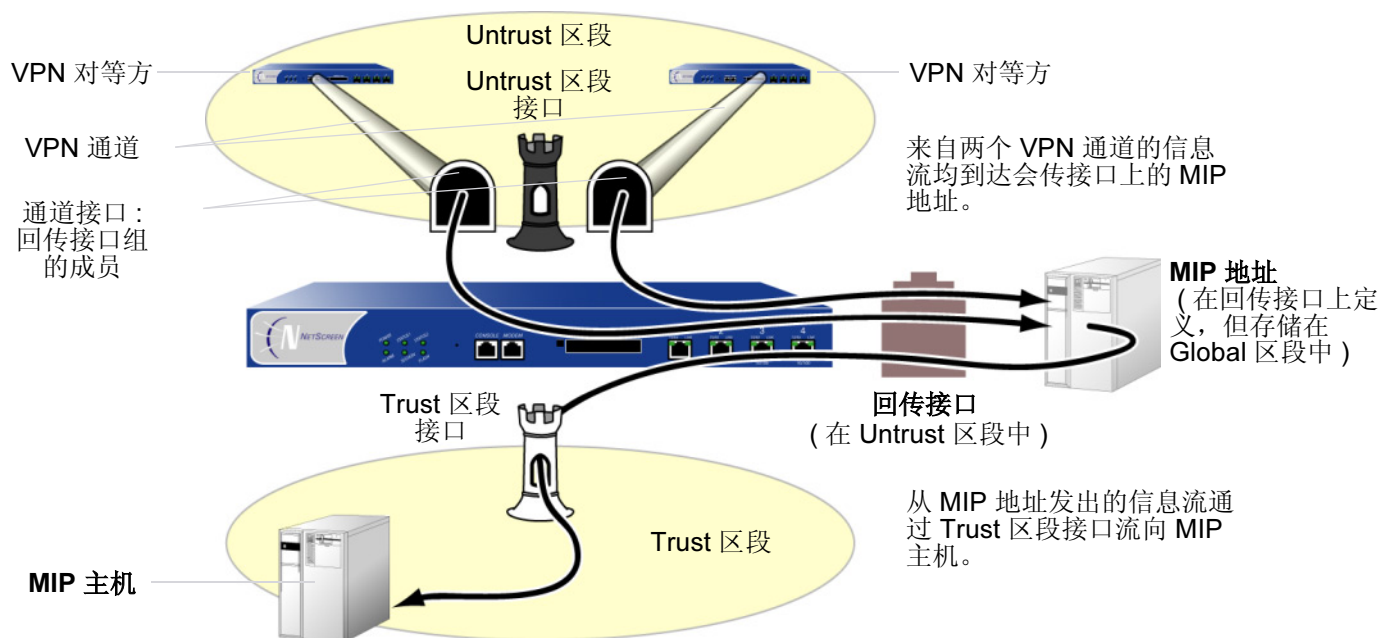
5. 策略

```
set policy from untrust to trust any mip(1.1.1.1) http permit
save
```

23. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

MIP 和回传接口

在回传接口上定义 MIP 后，可以让一组接口访问 MIP。这样做的主要目的是为了使用同一个 MIP 地址通过多个 VPN 通道之一访问主机。MIP 主机还可以发起信息流通过相应通道发往远程站点。



您可以将回传接口想象成包含 MIP 地址的资源容器。可使用名称 `loopback.id_num` 配置回传接口 (其中 `id_num` 是唯一标识设备接口的索引号)，并给接口分配一个 IP 地址 (请参阅第 103 页上的“回传接口”)。为准许其它接口使用回传接口上的 MIP，可将该接口添加为回传组中的一员。

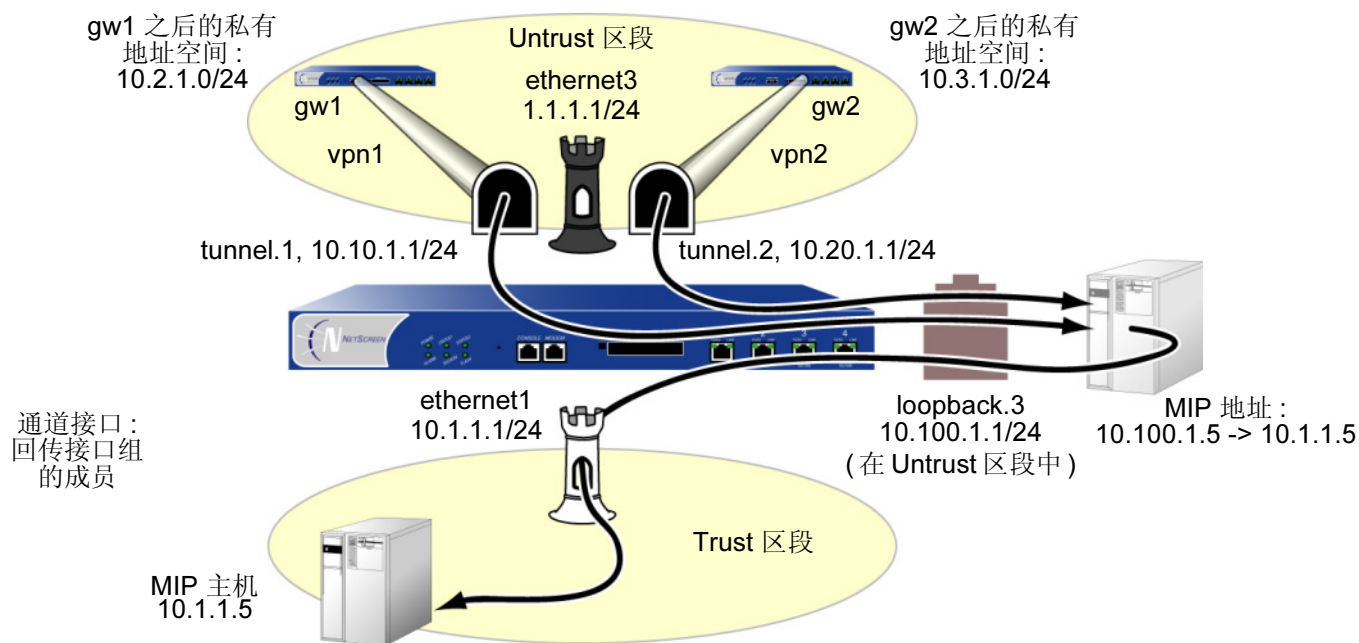
回传接口及其成员接口必须位于同一区段的不同 IP 子网中。任何一个有 IP 地址的接口都可以成为回传组的成员。如果要在回传接口和一个成员接口上配置 MIP，请优先配置回传接口。回传接口不能是其它回传组的成员。

范例：两个通道接口的 MIP

在本例中，将配置以下接口：

- ethernet1, Trust 区段, 10.1.1.1/24
- ethernet3, Untrust 区段, 1.1.1.1/24
- tunnel.1, Untrust 区段, 10.10.1.1/24, 绑定到 vpn1
- tunnel.2, Untrust 区段, 10.20.1.1/24, 绑定到 vpn2
- loopback.3, Untrust 区段, 10.100.1.1/24

通道接口是 loopback.3 接口组的成员。Loopback.3 接口包含 MIP 地址 10.100.1.5，该地址映射到 Trust 区段中地址为 10.1.1.5 的主机。



当目的地址为 10.100.1.5 的封包通过 VPN 通道到达 tunnel.1 时，NetScreen 设备将在回传接口 loopback.3 上搜索 MIP。在 loopback.3 上找到匹配项后，NetScreen 设备会将初始目的 IP 地址 (10.100.1.5) 转换成主机 IP 地址

(10.1.1.5)，然后通过 **ethernet1** 将封包转发到 MIP 主机。目的地址为 10.100.1.5 的信息流也可以通过绑定到 **tunnel.2** 的 VPN 通道到达。同样，NetScreen 设备先在 **loopback.3** 上找到匹配项，再将初始目的 IP 地址 10.100.1.5 转换成 10.1.1.5，然后将封包转发到 MIP 主机。

为完成配置，仍需要定义地址、VPN 通道、路由及策略。所有安全区域都在 **trust-vr** 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 **ethernet1**): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

NAT: ²⁴ (选择)

Network > Interfaces > Edit (对于 **ethernet3**): 输入以下内容，然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Network > Interfaces > New Loopback IF: 输入以下内容，然后单击 **OK**:

Interface Name: loopback.3

Zone: Untrust (trust-vr)

IP Address/Netmask: 10.100.1.1/24

24. 缺省情况下，绑定到 Trust 区段的任意接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **Apply**:

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.10.1.1/24

在 Member of Loopback Group 下拉列表中选择 **loopback.3**, 然后单击 **OK**。

Network > Interfaces > New Tunnel IF: 输入以下内容, 然后单击 **Apply**:

Tunnel Interface Name: tunnel.2

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address/Netmask: 10.20.1.1/24

在 Member of Loopback Group 下拉列表中选择 **loopback.3**, 然后单击 **OK**。

2. MIP

Network > Interfaces > Edit (对于 loopback.3) > MIP > New: 输入以下内容, 然后单击 **OK**:

Mapped IP: 10.100.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

3. 地址

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

Address Name: local_lan

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

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

Address Name: peer-1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.1.0/24

Zone: Untrust

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

Address Name: peer-2

IP Address/Domain Name:

IP/Netmask: (选择), 10.3.1.0/24

Zone: Untrust

4. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**：

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw1

Type: Static IP: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**：

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw2

Type: Static IP: (选择), Address/Hostname: 3.3.3.3

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

> **Advanced:** 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Bind to Tunnel Interface: (选择), tunnel.2

Proxy-ID: (选择)

Local IP/Netmask: 0.0.0.0/0

Remote IP/Netmask: 0.0.0.0/0

Service: ANY

5. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 10.2.1.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 10.3.1.0/24

Gateway: (选择)

Interface: tunnel.2

Gateway IP Address: 0.0.0.0

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**：

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), peer-1

Destination Address:

Address Book Entry: (选择), MIP(10.100.1.5)

Service: ANY

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), peer-2

Destination Address:

Address Book Entry: (选择), MIP(10.100.1.5)

Service: ANY

Action: Permit

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), local_lan

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24

set interface loopback.3 zone trust
set interface loopback.3 ip 10.100.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.1.1/24
set interface tunnel.1 loopback-group loopback.3

set interface tunnel.2 zone untrust
set interface tunnel.2 ip 10.20.1.1/24
set interface tunnel.2 loopback-group loopback.3
```

2. MIP

```
set interface loopback.3 mip 10.100.1.5 host 10.1.1.5 netmask 255.255.255.255
vrouter trust-vr25
```

3. 地址

```
set address trust local_lan 10.1.1.0/24
set address untrust peer-1 10.2.1.0/24
set address untrust peer-2 10.3.1.0/24
```

25. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

4. VPN

```
set ike gateway gw1 address 2.2.2.2 outgoing-interface ethernet3 preshare
netscreen1 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

set ike gateway gw2 address 3.3.3.3 outgoing-interface ethernet3 preshare
netscreen2 sec-level compatible
set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. 路由

```
set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.3.1.0/24 interface tunnel.2
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. 策略

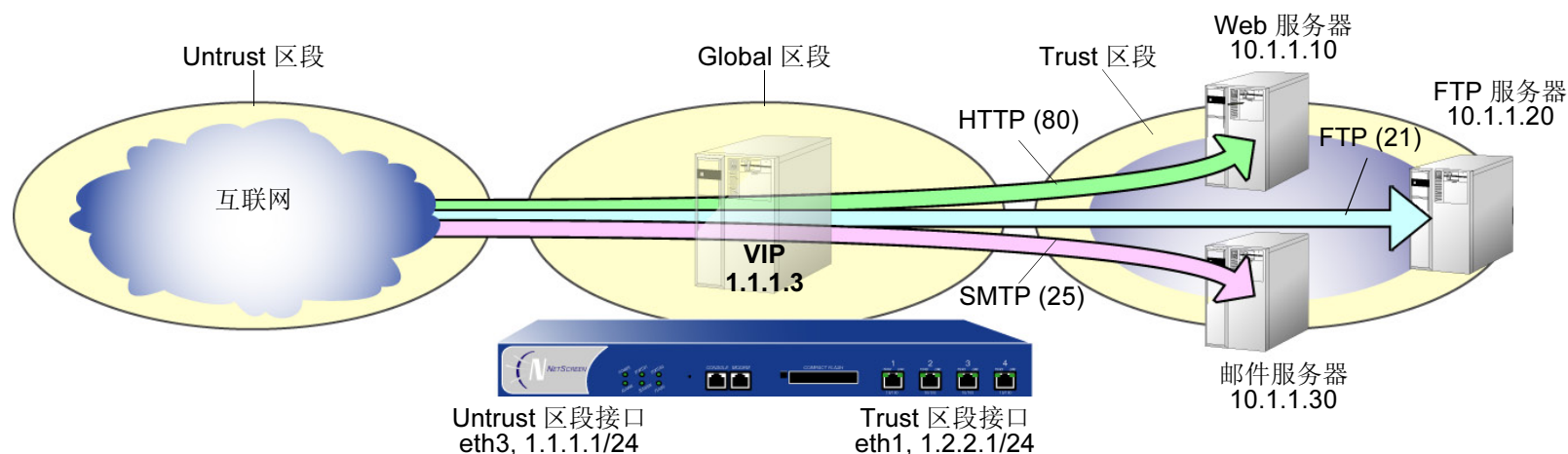
```
set policy top from untrust to trust peer-1 mip(10.100.1.5) any permit
set policy top from untrust to trust peer-2 mip(10.100.1.5) any permit
set policy from trust to untrust local_lan any any permit
save
```

虚拟 IP 地址

根据 TCP 或 UDP 片段包头的目的地端口号，虚拟 IP (VIP) 地址将在一个 IP 地址处接收到的信息流映射到另一个地址。例如，

- 目的地址为 1.1.1.3:80 (也就是 IP 地址为 1.1.1.3，端口号为 80) 的 HTTP 封包可能映射到地址为 10.1.1.10 的 Web 服务器。
- 目的地址为 1.1.1.3:21 的 FTP 封包可能映射到地址为 10.1.1.20 的 FTP 服务器。
- 目的地址为 1.1.1.3:25 的 SMTP 封包可能映射到地址为 10.1.1.30 的邮件服务器。

目的地 IP 地址相同。目的地端口号确定 NetScreen 设备将信息流转发到的主机。



虚拟 IP 转发表

区段中的接口 IP	Global 区段 中的 VIP	端口	转发至	Trust 区段 中的主机 IP
1.1.1.1/24	1.1.1.3	80 (HTTP)	→	10.1.1.10
1.1.1.1/24	1.1.1.3	21 (FTP)	→	10.1.1.20
1.1.1.1/24	1.1.1.3	25 (SMTP)	→	10.1.1.30

NetScreen 设备将去往 VIP 的内向信息流转发到 VIP 指向地址上的主机。VIP 主机发起出站信息流时，NetScreen 设备将该主机的源 IP 地址转换成 VIP 地址的源 IP 地址。这一对称的双向转换不同于源和目的地址的转换 (请参阅第 273 页上的 “NAT-Src 和 NAT-Dst 的方向特性”)。

需要以下信息来定义 “虚拟 IP”：

- VIP 的 IP 地址必须与 Untrust 区段中的接口 (或某些 NetScreen 设备上的接口) 在同一子网中，甚至可以是该接口使用的地址²⁶
- 处理请求的服务器的 IP 地址
- 希望 NetScreen 设备从 VIP 转发到主机 IP 地址的服务类型

注意：只能在 Untrust 区段接口上设置 VIP。

以下为一些有关 NetScreen VIP 的注释：

- 在一台机器上运行多个服务器进程时，可以让用户熟悉的服务使用虚拟端口号。例如，如果在同一台机器上运行两个 FTP 服务器，可以在端口 21 上运行一个服务器，在端口 2121 上运行另一个服务器。用户若要访问第二个 FTP 服务器，必须预先知道虚拟端口号并将其附加到封包包头的 IP 地址后。
- 可映射预先定义的服务和用户定义的服务。
- 单个 VIP 可识别具有相同源及目的地端口号但传输方式不同的定制服务。
- 定制服务可使用任何目的地端口号或端口号范围，从 1 到 65,535，而不仅是从 1024 到 65,535。

26. 在某些 NetScreen 设备上，Untrust 区段中的接口可以通过 DHCP 或 PPPoE 动态接收 IP 地址。如果希望在上述情况中使用 VIP，请执行以下操作之一：在 WebUI 中 (Network > Interfaces > Edit (对于 Untrust 区段中的接口) > VIP:) 设置 VIP 时，选择 **Same as the untrusted interface IP address** 选项。在 CLI 中，请使用 **set interface name vip untrust-ip** 命令。

如果配置 VIP，将同一 IP 地址用作支持多个 VIP 的 NetScreen 设备的 Untrust 区段接口，其它 “常规” VIP 将不可用。如果配置了常规 VIP，除非先删除常规 VIP，否则无法使用 Untrust 区段接口创建 VIP。

- 通过在单个 VIP 下创建多个服务条目，单个 VIP 可支持具有多个端口条目的定制服务 (服务中的每个端口条目在 VIP 中对应有一个服务条目)。缺省情况下，可在 VIP 中使用单端口服务。要在 VIP 中使用多端口服务，必须首先发出 CLI 命令 **set vip multi-port**，然后重新设置 NetScreen 设备。(请参阅第 379 页上的“范例：具有定制和多端口服务的 VIP”)。
- 必须可从 **trust-vr** 到达 NetScreen 设备将 VIP 信息流映射到的主机。如果该主机不在 **trust-vr** 的路由选择域中，则必须定义到达它的路由。
- 自定义服务可使用任意目的端口号或从 1 到 32,767 之间的任意端口号范围，而不仅仅是从 1024 到 32,767。

VIP 和 Global 区段

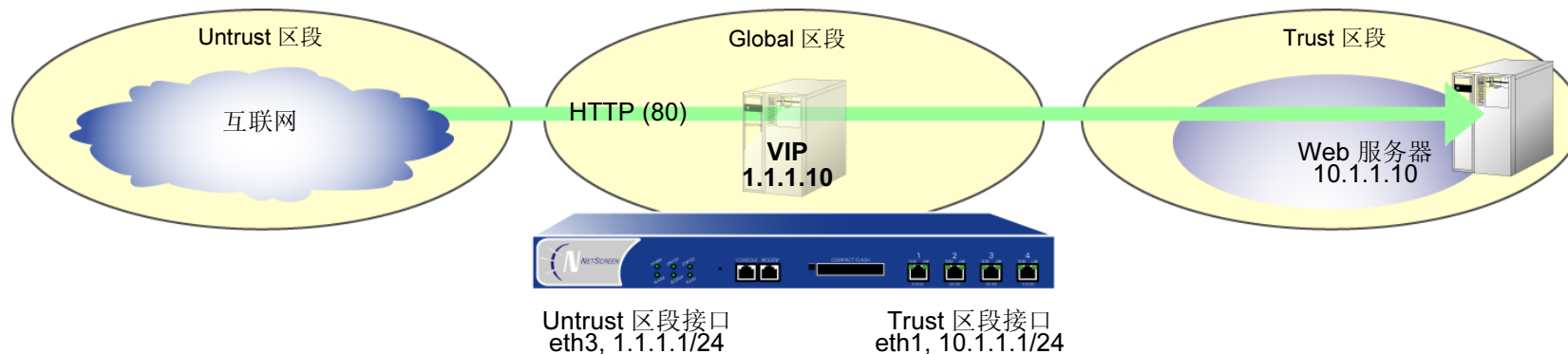
为 Untrust 区段中的接口设置 VIP 将在 Global 区段通讯簿中生成一条条目。不管接口属于哪个区段，Global 区段通讯簿保留所有接口的全部 VIP。可以将这些 VIP 地址用作任意两个区段间策略的目的地址，还可以用作 Global 策略中的目的地址。

范例：配置虚拟 IP 服务器

在本例中，将接口 ethernet1 绑定到 Trust 区段，并为其分配 IP 地址 10.1.1.1/24。将接口 ethernet3 绑定到 Untrust 区段，并为其分配 IP 地址 1.1.1.1/24。

然后，在 1.1.1.10 配置 VIP，以便将入站 HTTP 信息转发到地址为 10.1.1.10 的 Web 服务器，并创建一个策略，允许 Untrust 区段的信息流到达 Trust 区段中的 VIP（始终到达 VIP 指向地址上的主机）。

由于 VIP 与 Untrust 区段接口 (1.1.1.0/24) 在同一子网中，因此无需定义路由，以便 Untrust 区段的信息流到达 VIP²⁷。此外，VIP 将信息转发到的主机不需要通讯簿条目。所有安全区域都在 trust-vr 路由域中。



27. 如果希望安全区（而非 Untrust 区段）的 HTTP 信息流到达 VIP，则必须在安全区的路由器上设置到达 1.1.1.10 的路由，从而指向绑定到该区段的接口。例如，假设 ethernet2 被绑定到用户定义区段上，且配置了该区段的路由器，将目的地址为 1.1.1.10 的信息流发送到 ethernet2。路由器将信息流发送到 ethernet2 后，NetScreen 设备中的转发机制将 VIP 定位在 ethernet3，它将信息流映射到 10.1.1.10 并发送出 ethernet1，到达 Trust 区段。此过程与第 352 页上的“范例：从不同区段到达 VIP”中描述的类似。此外，还必须设置一个策略，允许 HTTP 信息流从源区段流向 Trust 区段中的 VIP。

WebUI

1. 接口

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容, 然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. VIP

Network > Interfaces > Edit (对于 ethernet3) > VIP: 输入以下地址, 然后单击 **Add**:

Virtual IP Address: 1.1.1.10

Network > Interfaces > Edit (对于 ethernet3) > VIP > New VIP Service: 输入以下内容, 然后单击 **OK**:

Virtual IP: 1.1.1.10

Virtual Port: 80

Map to Service: HTTP (80)

Map to IP: 10.1.1.10

3. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), ANY

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.10)

Service: HTTP

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet2 ip 1.1.1.1/24
```

2. VIP

```
set interface ethernet3 vip 1.1.1.10 80 http 10.1.1.10
```

3. 策略

```
set policy from untrust to trust any vip(1.1.1.10) http permit
save
```

范例：编辑 VIP 配置

在本例中，将修改在上一范例中创建的“虚拟 IP”服务器配置。为了限制对 Web 服务器的访问，将 HTTP 信息流的虚拟端口号从 80 (缺省值) 更改为 2211。现在，只有那些连接 Web 服务器时知道使用端口号 2211 的人员才能访问它。

WebUI

Network > Interfaces > Edit (对于 ethernet3) > VIP > Edit (在 1.1.1.10 的 VIP Services Configure 部分中): 输入以下内容，然后单击 **OK**:

Virtual Port: 2211

CLI

```
unset interface ethernet3 vip 1.1.1.10 port 80
set interface ethernet3 vip 1.1.1.10 2211 http 10.1.1.10
save
```

范例：移除 VIP 配置

在本例中，将删除以前创建并修改的 VIP 配置。必须首先移除与其有关的任何现有策略，才能移除 VIP。在[第 375 页上的“范例：配置虚拟 IP 服务器”](#)中创建的策略 ID number 为 5。

WebUI

Policies > (From: Untrust, To: Trust) > Go: 为策略 ID 5，单击 **Remove**。

Network > Interfaces > Edit (对于 ethernet3) > VIP: 在 1.1.1.10 的 VIP Configure 部分中，单击 **Remove**。

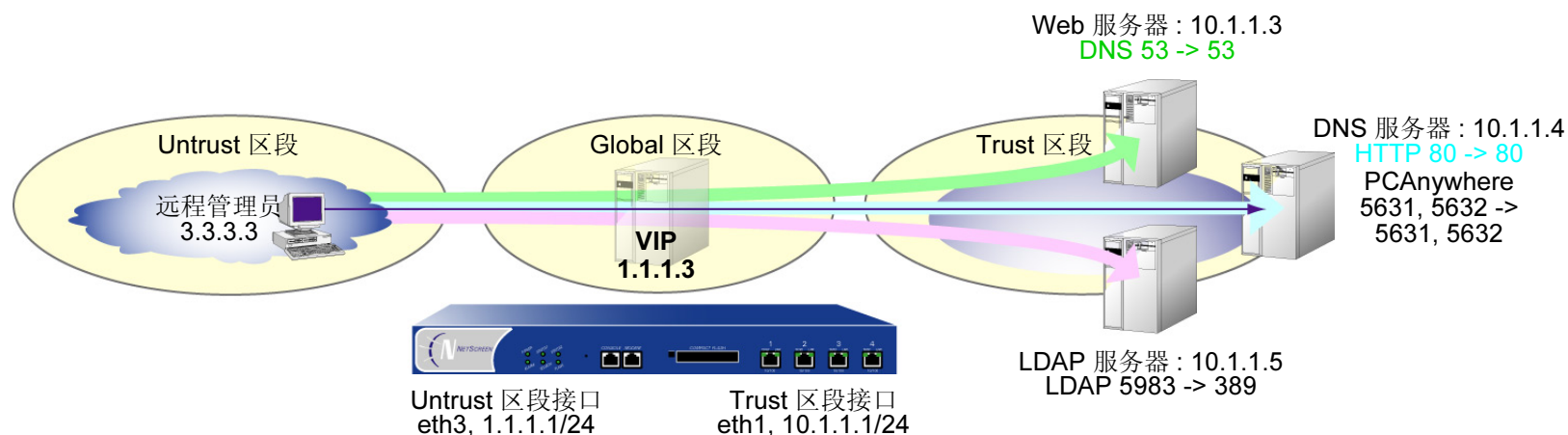
CLI

```
unset policy id 5
unset interface ethernet3 vip 1.1.1.10
save
```


范例：具有定制和多端口服务的 VIP

在以下范例中，将在 1.1.1.3 上配置 VIP，将以下服务发送到下列内部地址：

服务	Transport	虚拟端口号	实际端口号	主机 IP 地址
DNS	TCP, UDP	53	53	10.1.1.3
HTTP	TCP	80	80	10.1.1.4
PCAnywhere	TCP, UDP	5631, 5632	5631, 5632	10.1.1.4
LDAP	TCP, UDP	5983	389	10.1.1.5



VIP 将 DNS 查询发送到 10.1.1.3 上的 DNS 服务器，将 HTTP 信息流发送到 10.1.1.4 上的 Web 服务器，并将认证检查发送到 10.1.1.5 上的 LDAP 服务器上的数据库。对于 HTTP、DNS 和 PCAnywhere，虚拟端口号与实际端口号保持一致。对于 LDAP，虚拟端口号 (5983) 用于将额外的安全级别添加到 LDAP 认证信息流。

为了远程管理 HTTP 服务器，定义一个定制服务并且命名为 PCAnywhere。PCAnywhere 是一项多端口服务，它发送并监听 TCP 端口 5631 上的数据以及 UDP 端口 5632 上的状态检查。

还要在 **Untrust** 区段的通讯簿中输入远程管理员的地址 **3.3.3.3**，并为所有要使用 **VIP** 的信息流配置从 **Untrust** 到 **Trust** 区段的策略。所有安全区域都在 **trust-vr** 路由域中。

WebUI

1. 接口

Network > Interfaces > Edit (对于 **ethernet1**): 输入以下内容，然后单击 **Apply**:

Zone Name: **Trust**

Static IP: (出现时选择此选项)

IP Address/Netmask: **10.1.1.1/24**

选择以下内容，然后单击 **OK**:

Interface Mode: **NAT**

Network > Interfaces > Edit (对于 **ethernet3**): 输入以下内容，然后单击 **OK**:

Zone Name: **Untrust**

Static IP: (出现时选择此选项)

IP Address/Netmask: **1.1.1.1/24**

2. 地址

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

Address Name: **Remote Admin**

IP Address/Domain Name:

IP/Netmask: (选择), **3.3.3.3/32**

Zone: **Untrust**

3. 定制服务

Object > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: PCAnywhere

No 1:

Transport protocol: TCP

Source Port Low: 0

Source Port High: 65535

Destination Port Low: 5631

Destination Port High: 5631

No 2:

Transport protocol: UDP

Source Port Low: 0

Source Port High: 65535

Destination Port Low: 5632

Destination Port High: 5632

4. VIP 地址和服务²⁸

Network > Interfaces > Edit (对于 ethernet3) > VIP: 单击此处进行配置：在 “Virtual IP Address” 字段中键入 **1.1.1.3**，然后单击 **Add**。

> New VIP Service: 输入以下内容，然后单击 **OK**:

Virtual IP: 1.1.1.3

Virtual Port: 53

Map to Service: DNS

Map to IP: 10.1.1.3

28. 要启用 VIP 支持多端口服务，就必须输入 CLI 命令 **set vip multi-port**，保存配置，然后重新启动设备。

- > New VIP Service: 输入以下内容，然后单击 **OK**:
 - Virtual IP: 1.1.1.3
 - Virtual Port: 80
 - Map to Service: HTTP
 - Map to IP: 10.1.1.4
- > New VIP Service: 输入以下内容，然后单击 **OK**:
 - Virtual IP: 1.1.1.3
 - Virtual Port: 5631²⁹
 - Map to Service: PCAnywhere
 - Map to IP: 10.1.1.4
- > New VIP Service: 输入以下内容，然后单击 **OK**:
 - Virtual IP: 1.1.1.3
 - Virtual Port: 5983³⁰
 - Map to Service: LDAP
 - Map to IP: 10.1.1.5

29. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

30. 使用非标准端口号可添加另一安全层，以阻挡对使用标准端口号的服务的常见攻击。

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.3)

Service: DNS

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.3)

Service: HTTP

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.3)

Service: LDAP

Action: Permit

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Remote Admin

Destination Address:

Address Book Entry: (选择), VIP(1.1.1.3)

Service: PCAnywhere

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address untrust "Remote Admin" 3.3.3.3/32
```

3. 定制服务

```
set service pcanywhere protocol udp src-port 0-65535 dst-port 5631-5631
set service pcanywhere + tcp src-port 0-65535 dst-port 5632-5632
```

4. VIP 地址和服务

```
set vip multi-port
save
reset
System reset, are you sure? y/[n] y
```

```
set interface ethernet3 vip 1.1.1.3 53 dns 10.1.1.3
set vip 1.1.1.3 + 80 http 10.1.1.4
set vip 1.1.1.3 + 5631 pcanywhere 10.1.1.431
set vip 1.1.1.3 + 5983 ldap 10.1.1.5
```

5. 策略

```
set policy from untrust to trust any vip(1.1.1.3) dns permit
set policy from untrust to trust any vip(1.1.1.3) http permit
set policy from untrust to trust any vip(1.1.1.3) ldap permit
set policy from untrust to trust "Remote Admin" vip(1.1.1.3) pcanywhere permit
save
```

31. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

用户认证

本章重点介绍进行用户认证的几种方法。首先研究不同类型的认证服务器 — 内置于各 **NetScreen** 设备中的本地数据库以及外部 **RADIUS**、**SecurID** 和 **LDAP** 认证服务器。然后，介绍如何定义不同的用户帐户 (或 “配置文件”)，如何创建用户组，如何在策略、“自动密钥 **IKE**” 网关和 **L2TP** 通道中引用用户和用户组。本章最后一节介绍如何自定义 **HTTP**、**FTP**、**L2TP**、**Telnet** 和 **XAuth** 登录提示中出现的标题。本章包括以下部分：

- 第 388 页上的 “认证服务器”
- 第 390 页上的 “本地数据库”
- 第 392 页上的 “外部 **Auth** 服务器”
 - 第 395 页上的 “**Auth** 服务器类型”
 - 第 404 页上的 “定义 **Auth** 服务器对象”
 - 第 411 页上的 “定义缺省 **Auth** 服务器”
- 第 413 页上的 “认证类型及应用”
 - 第 414 页上的 “**Auth** 用户和用户组”
 - 第 447 页上的 “**IKE** 用户和用户组”
 - 第 452 页上的 “**XAuth** 用户和用户组”
 - 第 476 页上的 “**L2TP** 用户和用户组”
 - 第 481 页上的 “**Admin** 用户”
- 第 483 页上的 “多类型用户”
- 第 484 页上的 “组表达式”
- 第 492 页上的 “标题自定义”

认证服务器

可对 NetScreen 设备进行配置，以便使用本地数据库或者一个或多个外部认证服务器验证以下类型用户的身份：

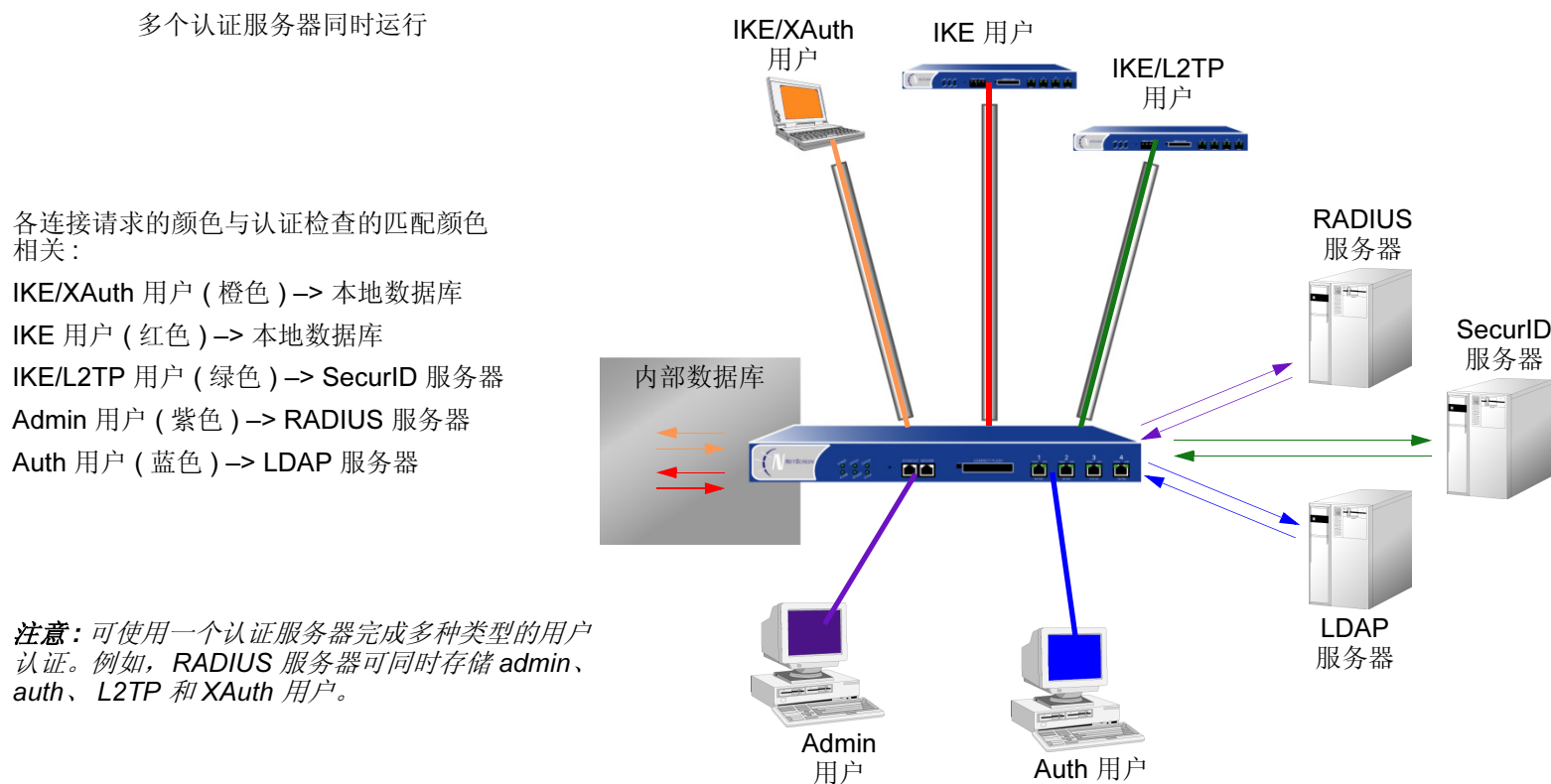
- Auth 用户
- IKE 用户
- L2TP 用户
- XAuth 用户
- Admin 用户

注意：IKE 用户帐户必须存储在本地数据库上。RADIUS 是唯一支持 L2TP 和 XAuth 远程设置指派和管理权限指派的外部服务器。

除其本地数据库外，NetScreen 设备还支持外部 RADIUS、SecurID 和 LDAP 服务器。可使用各种类型的认证服务器对 auth 用户、L2TP 用户、XAuth 用户和 admin 用户进行认证。此外，NetScreen 还支持 WebAuth，这是面向 auth 用户的一种可选认证方案。(有关 WebAuth 的范例，请参阅第 443 页上的“范例：WebAuth + SSL (外部用户组)”。)所有包含 auth 用户帐户类型的 auth 服务器都可以作为缺省的 WebAuth auth 服务器。下表对服务器与用户类型及认证功能之间的对应支持关系加以总结：

服务器类型	支持的用户类型和功能									
	Auth 用户	IKE 用户	L2TP 用户		XAuth 用户		Admin 用户		用户组	组表达式
			Auth	远程设置	Auth	远程设置	Auth	权限		
Local	b	b	b	b	b	b	b	b	b	
RADIUS	b		b	b	b	b	b	b	b	b
SecurID	b		b		b		b			
LDAP	b		b		b		b			

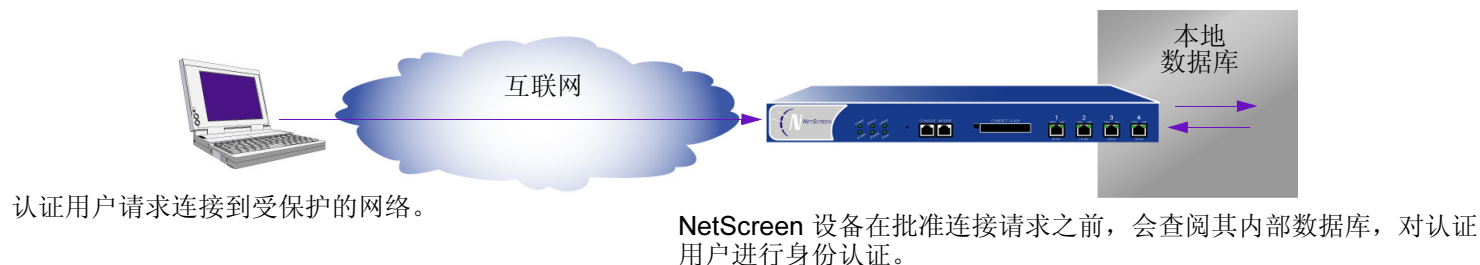
在大多数 **NetScreen** 设备上，可对每个系统 — 根系统和虚拟系统 — 以任意组合形式使用最多 10 个主认证服务器。这一数字包括本地数据库，但不包括备份认证服务器。一个 **RADIUS** 或 **LDAP** 服务器支持两个备份服务器，一个 **SecurID** 服务器支持一个备份服务器；例如，您可使用本数据库和 9 个不同的主 **RADIUS** 服务器，每个 **RADIUS** 服务器分配有两个备份服务器。



以下部分进一步详细研究本地数据库以及各种认证服务器。

本地数据库

所有 NetScreen 设备都支持使用内置用户数据库进行认证。在 NetScreen 设备上定义用户时，NetScreen 设备将用户名和密码输入到其本地数据库中。



支持的用户类型和功能

本地数据库支持以下类型的用户和认证功能：

- Auth 用户
- IKE 用户
- L2TP 用户
- XAuth 用户
- Admin 用户
- Admin 权限
- WebAuth
- 用户组
- 组表达式*

* 在 NetScreen 设备上定义组表达式，但用户和用户组必须存储在外部的 RADIUS auth 服务器上。有关组表达式的详细信息，请参阅第 484 页上的“组表达式”。

对于所有类型的认证而言，本地数据库是缺省的认证服务器 (auth 服务器)。有关如何通过 WebUI 和 CLI 向本地数据库添加用户和用户组的说明，请参阅第 413 页上的“认证类型及应用”。

范例：本地数据库超时

在缺省情况下，**admin** 和 **auth** 用户的本地数据库认证超时时限为 10 分钟。在本例中，将 **admin** 用户的此项设置更改为永不超时，而将 **auth** 用户的此项设置更改为 30 分钟后超时。

WebUI

Configuration > Admin > Management: 清除 Enable Web Management Idle Timeout 复选框，然后单击 **Apply**。

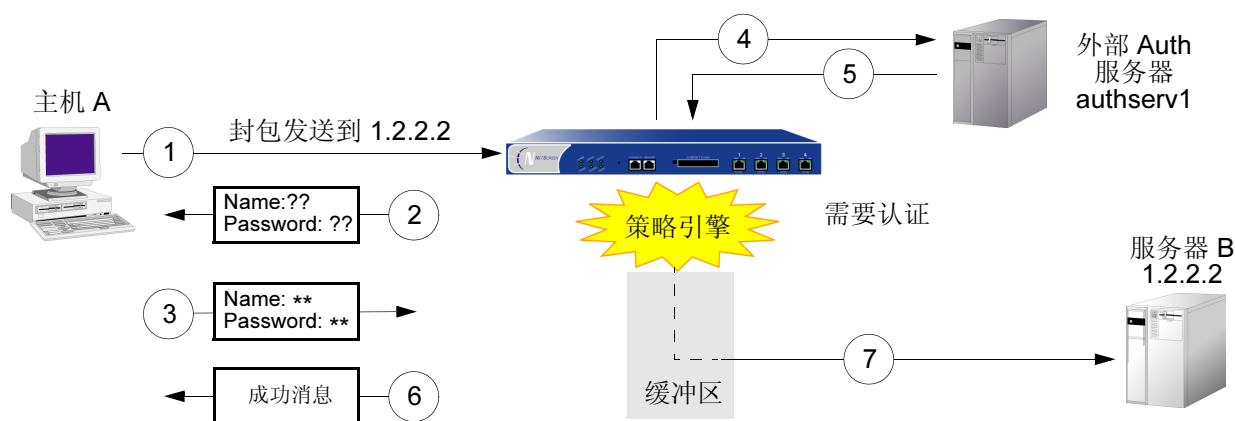
Configuration > Auth > Servers > Edit (对于 Local): 在 Timeout 字段中输入 **30**，然后单击 **Apply**。

CLI

```
set admin auth timeout 0
set auth-server Local timeout 30
save
```

外部 AUTH 服务器

NetScreen 设备可与存储用户帐户的一个或多个外部认证服务器或“auth 服务器”相连。NetScreen 设备在接收到要求进行认证验证的连接请求后，会请求策略、L2TP 通道配置或 IKE 网关配置中所指定的 auth 外部服务器进行认证检查。然后，NetScreen 充当用户请求认证与 auth 服务器批准认证之间的中继器。成功的外部 auth 服务器认证检查的过程如下：

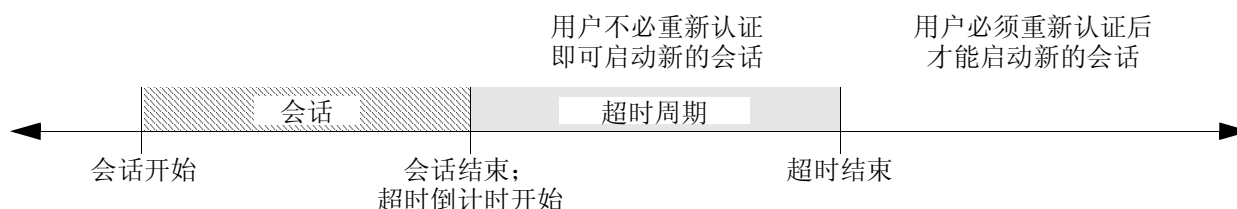


1. 主机 A 将 FTP、HTTP 或 Telnet TCP SYN 封包发送到 1.2.2.2。
2. NetScreen 设备截取封包、记录其相应策略要求从 authserv1 获得认证、将封包放入缓冲区，并提示用户输入用户名和密码。
3. 用户以用户名和密码回复。
4. NetScreen 设备将登录信息转发到 authserv1。
5. Authserv1 将成功通知发送回 NetScreen 设备。
6. NetScreen 设备通知 auth 用户登录成功。
7. 然后，NetScreen 设备将封包从其缓冲区转发到其目的地 1.2.2.2。

Auth 服务器对象属性

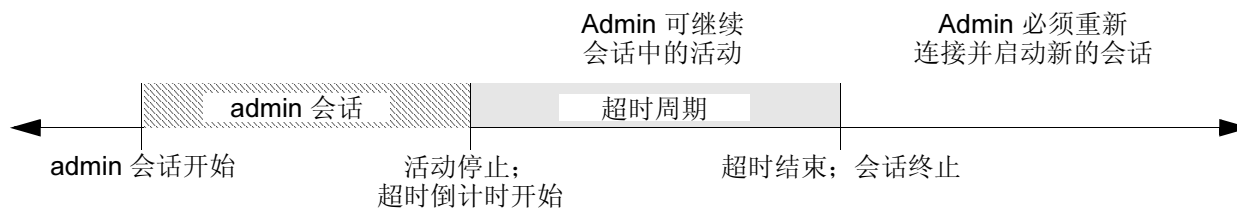
NetScreen 设备将每个 auth 服务器视为可在策略、IKE 网关和 L2TP 通道中引用的一个对象。以下属性定义并唯一标识 auth 服务器对象：

- 对象名：名称字符串，如 “authserv1”（唯一的预定义 auth 服务器为 “Local”。）
- ID 号：可手动设置 ID 号，也可让 NetScreen 设备自动对其进行设置。如果设置 ID 号，则必须选择未使用的号码。
- 类型：RADIUS、SecurID、LDAP。
- 服务器名称：服务器的 IP 地址或域名
- 备份服务器 1：主备份服务器的 IP 地址或域名
- 备份服务器 2：(RADIUS 和 LDAP) 辅助备份服务器的 IP 地址或域名
- 帐户类型：以下一种或多种用户类型：Auth、L2TP、Xauth；或仅 Admin。
- 超时值：对于不同的用户（auth 用户或 admin 用户），超时值具有不同的意义。
 - Auth 用户：第一个认证会话完成后开始超时倒计时。如果用户在倒计时达到超时临界值前发起新的会话，则不必重新认证，超时倒计时功能会自动重置。缺省超时值为 10 分钟，最大值为 255 分钟。也可将超时值设置为 0，此时认证周期将永远不会超时。



注意：用户认证超时与会话空闲超时不同。如果在预定的时间长度内，某会话中未发生任何活动，NetScreen 设备会自动将该会话从其会话表中移除。

- **Admin 用户**：如果空闲时间长度达到超时临界值，**NetScreen** 设备将终止 **admin** 会话。要继续管理 **NetScreen** 设备，**admin** 必须重新连接到该设备并重新认证。缺省超时值为 10 分钟，最大值为 1000 分钟。也可将超时值设置为 0，此时 **admin** 会话将永远不会超时。



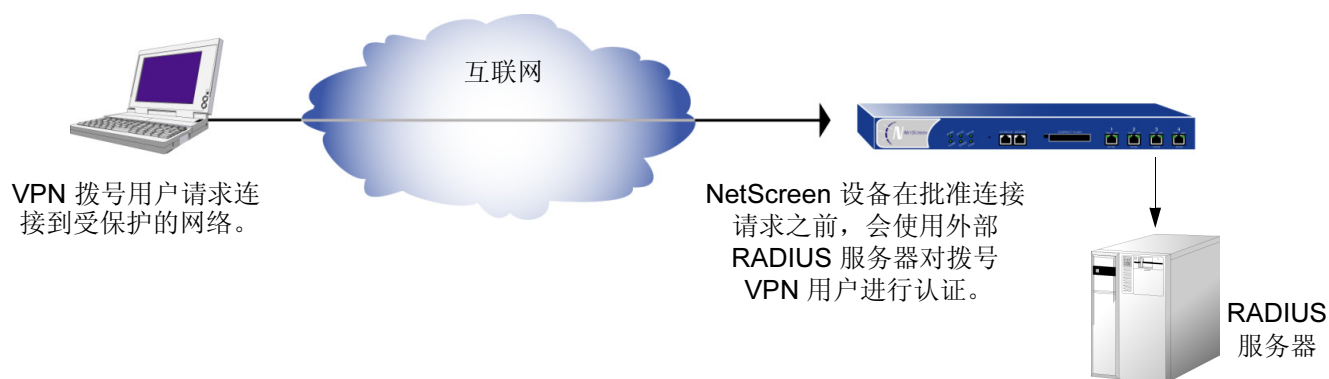
除上述适用于所有 **auth** 服务器对象的属性外，每个服务器还具有一些自己专有的属性。这些内容将在后续的 **RADIUS**、**SecurID** 和 **LDAP auth** 服务器属性部分中加以说明。

Auth 服务器类型

除内部数据库外，NetScreen 还支持三种类型的外部 auth 服务器：RADIUS、SecurID 和 LDAP。

RADIUS

远程认证拨号的用户服务 (RADIUS) 是一个用于认证服务器的协议，它最多可支持几万个用户。



RADIUS 客户端 (即 NetScreen 设备) 通过客户端与服务器之间的一系列通信对用户进行认证。通常，RADIUS 会要求登录人员输入其用户名和密码。然后，它将这些值与其数据库中的对应值比较，用户通过认证后，客户端即允许其访问相应的网络服务。

要针对 RADIUS 配置 NetScreen 设备，必须指定 RADIUS 服务器的 IP 地址并定义共享机密 — 与 RADIUS 服务器上的定义相同。共享机密是一个密码，RADIUS 服务器用它来生成密钥，以便对 NetScreen 和 RADIUS 设备之间的信息流进行加密。

RADIUS Auth 服务器对象属性

除第 393 页上的“Auth 服务器对象属性”中列出的通用 auth 服务器属性外，RADIUS 服务器还使用以下属性：

- **Shared Secret:** NetScreen 设备与 RADIUS 服务器之间共享的机密 (密码)。设备利用此机密将其向 RADIUS 服务器发送的用户密码进行加密。
- **RADIUS Port:** RADIUS 服务器上的端口号，NetScreen 设备向此处发送认证请求。缺省端口号为 1645。
- **RADIUS Retry Timeout:** 先前的请求未引发响应时，向 RADIUS 服务器发送另外的认证请求之前，NetScreen 设备等待的时间间隔 (单位为秒)。缺省值为三秒。

支持的用户类型和功能

RADIUS 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 (认证和远程设置)
- XAuth 用户 (认证和远程设置)
- Admin 用户 (认证和权限指派)
- 用户组

RADIUS 服务器可支持本地数据库所支持的所有用户类型和功能 (除 IKE 用户之外)。在三种类型的外部 auth 服务器中，RADIUS 是目前唯一能支持如此众多对象的服务器。为了使 RADIUS 服务器能够支持管理权限、用户组及远程 L2TP 和 XAuth IP 地址¹、DNS 和 WINS 服务器地址分配等 NetScreen 专用属性，必须在 RADIUS 服务器上加载定义上述属性的 NetScreen 词典文件。

1. NetScreen 使用标准 RADIUS 属性进行 IP 地址分配。如果只想用 RADIUS 进行 IP 地址分配，则不必加载 NetScreen 供应商专用属性 (VSA)。

NetScreen 词典文件

词典文件用于定义可加载到 RADIUS 服务器上的供应商专用属性 (VSA)。定义上述 VSA 的值后, NetScreen 可以在用户登录 NetScreen 设备时查询这些属性。NetScreen VSA 包括管理权限、用户组及远程 L2TP 和 XAuth IP 地址、DNS 和 WINS 服务器地址分配。NetScreen 词典文件共有两个, 一个用于 Cisco RADIUS 服务器, 另一个用于 Funk Software RADIUS 服务器。如果使用 Microsoft RADIUS 服务器, 则不会有任何词典文件。必须以可从 www.netscreen.com/resources/application_notes/technical.jsp 下载的 *Using a Windows NT Domain / Active Directory for User Authentication NetScreen Devices* 中所述的方式对其进行配置。

每个 NetScreen 词典文件都包含以下具体信息:

- **Vendor ID:** NetScreen 供应商 ID (VID; 也称“IETF 编号”) 为 3224。VID 用于识别特殊属性的具体供应商。某些类型的 RADIUS 服务器要求为每个属性条目输入 VID, 而其它类型则只要求输入一次, 然后即可全局应用。有关详细信息, 请参阅 RADIUS 服务器文档。
- **Attribute Name:** 属性名用于描述各 NetScreen 专用属性, 例如 NS-Admin-Privilege、NS-User-Group、NS-Primary-DNS-Server 等等。
- **Attribute Number:** 属性编号用于识别各供应商专用属性。NetScreen 专用属性编号分为两个范围:
 - NetScreen ScreenOS: 1 – 199
 - NetScreen-Global PRO: 200 以上

例如, 用户组的 ScreenOS 属性编号为 3。用户组的 NetScreen-Global PRO 属性编号为 200。

- **Attribute Type:** 属性类型用于确定属性数据 (或“值”) 的显示形式 — 字符串、IP 地址或整数。

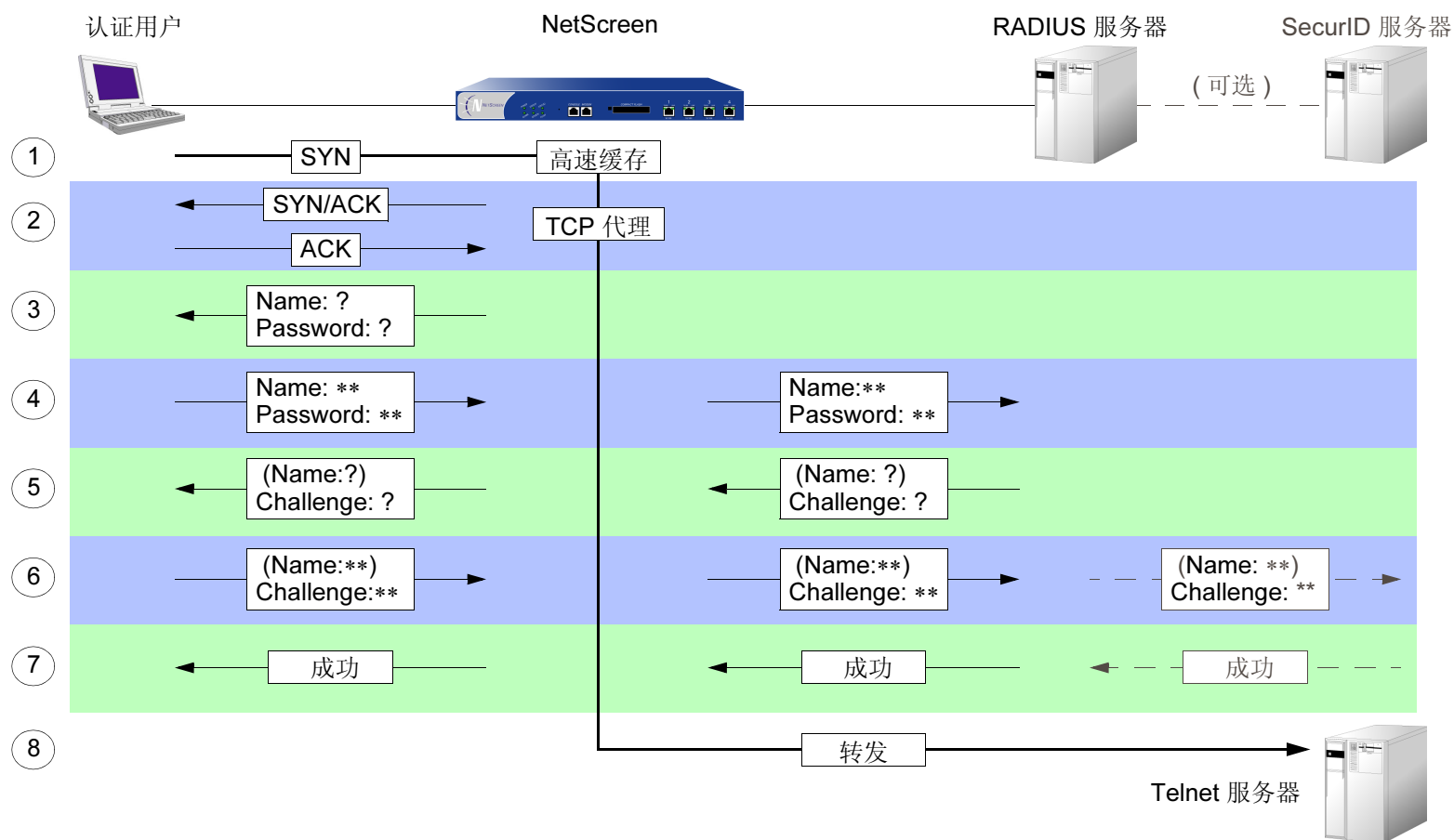
向 RADIUS 服务器加载 NetScreen 词典文件时, 服务器会自动接收上述信息。要输入新数据, 必须以属性类型所指定的形式手动输入所需值。例如, 为读写 admin 输入如下条目:

VID	属性名	属性编号	属性类型	值
3224	NS-Admin-Privileges	1	data=int4 (即整数)	2 (2 = 全部权限)

要下载词典文件, 请访问 www.netscreen.com/services/tac_online/index.jsp, 选择 NetScreen 产品, 然后选择 RADIUS 词典文件。

RADIUS 访问质询

现在，当认证用户尝试通过 Telnet 登录时，NetScreen 设备可以处理外部 RADIUS 服务器的“访问质询”封包。批准用户名和密码后，“访问质询”向登录过程提供附加条件。在认证用户响应登录提示、输入正确的用户名和密码后，RADIUS 服务器向 NetScreen 设备发送“访问质询”，然后 NetScreen 设备转发将其给用户。用户回应后，NetScreen 设备向 RADIUS 服务器发送含有用户响应的新的“访问请求”。如果用户响应正确，则认证过程成功结束。请考虑认证用户希望 telnet 到服务器的下列方案：



1. 认证用户发送 SYN 封包，以启动 Telnet 会话与 Telnet 服务器的 TCP 连接。
2. NetScreen 设备截取该封包、检查其策略列表、确定该会话是否需要用户认证。NetScreen 设备缓存 SYN 封包并代理与该用户的 TCP 三方握手。
3. NetScreen 设备提示用户输入用户名和密码进行登录。
4. 认证用户输入用户名和密码并发送给 NetScreen 设备。然后，NetScreen 设备将含有登录信息的“访问请求”发送到 RADIUS 服务器。
5. 如果信息正确，则 RADIUS 服务器向 NetScreen 设备发送具有“回复消息”属性的“访问质询”，提示用户对质询提供响应。（“访问质询”可以有选择地提示认证用户再次提供用户名。第二个用户名可以与第一个相同，也可以不同。）然后，NetScreen 设备向该用户发送另一条包括“回复消息”属性的登录提示。
6. 认证用户输入质询响应（或者用户名）并发送给 NetScreen 设备。然后，NetScreen 设备将含有用户“访问响应”的第二个“访问请求”发送到 RADIUS 服务器。

如果 RADIUS 服务器需要通过另一台 auth 服务器对“访问响应”进行认证（例如，如果 SecurID 服务器必须对令牌代码进行认证），则 RADIUS 服务器向其它 auth 服务器发送“访问请求”。
7. 如果 RADIUS 服务器将“访问响应”转发给另一台 auth 服务器，并且该服务器发送“访问接受”，或者如果 RADIUS 服务器本身批准“访问响应”，则 RADIUS 服务器向 NetScreen 设备发送“访问接受”消息。然后，NetScreen 设备通知认证用户登录成功。
8. NetScreen 设备将初始 SYN 封包转发到其初始目的地：Telnet 服务器。

注意：在本版发行时，NetScreen 并不支持具有 L2TP 的“访问质询”。

SecurID

SecurID 结合两种因素来创建动态变化的密码，而不使用固定密码。SecurID 具有一个信用卡大小的设备，称为认证器，它拥有一个用于显示随机生成的数字字符串的 LCD 窗口，这种数字字符串称为令牌代码，每分钟变化一次。用户还拥有个人识别号码 (PIN)。用户登录时，需要输入用户名、其 PIN 以及当前令牌代码。

SecurID 认证设备
(认证器)



令牌代码每 60 秒就
变成另一伪随机号码。

认证器执行只有 RSA 了解的算法，创建 LCD 窗口中出现的值。被认证的用户输入其 PIN 及卡上的号码时，执行相同算法的 ACE 服务器将接收到的值与其数据库中的值进行比较。如果它们匹配，则认证成功。

NetScreen 设备和 RSA SecurID ACE 服务器之间的关系与 NetScreen 设备和 RADIUS 服务器之间的关系相似。即，NetScreen 设备充当客户端，将认证请求转发到外部服务器申请批准，并在用户和服务器之间传递登录信息。SecurID 与 RADIUS 的不同之处在于用户“密码”中包括不断变化的令牌代码。

SecurID Auth 服务器对象属性

除第 393 页上的“Auth 服务器对象属性”中列出的通用 auth 服务器属性外，SecurID 服务器还使用以下属性：

- **Authentication Port:** SecurID ACE 服务器上的端口号，NetScreen 设备向此处发送认证请求。缺省端口号为 5500。
- **Encryption Type:** 用于对 NetScreen 设备与 SecurID ACE 服务器之间的通信进行加密的算法 - SDI 或 DES。
- **Client Retries:** 放弃尝试之前，SecurID 客户端 (即 NetScreen 设备) 尝试建立与 SecurID ACE 服务器的通信的次数。
- **Client Timeout:** 两次认证重试操作之间 NetScreen 设备等待的时间长度 (秒)。
- **Use Duress :** 禁止或允许使用不同 PIN 号码的选项。如果启用此选项，用户输入先前确定的强迫 PIN 号码时，NetScreen 设备会向 SecurID ACE 服务器发送一个信号，指示用户正在违背自己的意愿进行登录；即处于强迫之下。SecurID ACE 服务器会允许访问一次，之后，它会拒绝该用户的所有进一步登录尝试，直至他 / 她与 SecurID 管理员联系。只有 SecurID ACE 服务器支持此选项时，才可使用强迫模式。

支持的用户类型和功能

SecurID ACE 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 (用户认证； L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置)
- XAuth 用户 (用户认证；不支持远程设置指派)
- Admin 用户 (用户认证； admin 用户接收只读的缺省权限指派)

目前，尽管可使用 SecurID 服务器存储 L2TP、XAuth 和 admin 用户帐户进行认证，但 SecurID ACE 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 SecurID 配套使用时，NetScreen 不支持用户组。

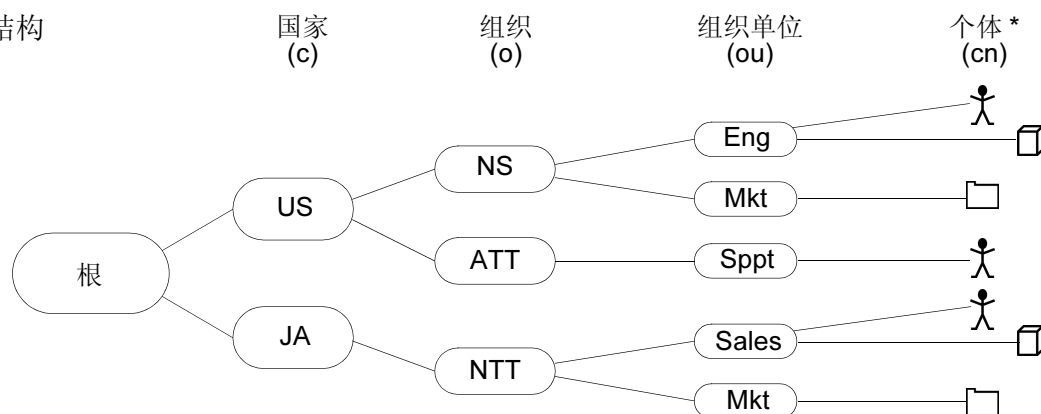
LDAP

轻量目录访问协议 (LDAP) 是密歇根大学在 1996 年开发出来的目录服务器标准。LDAP 是一个用于以类似分支树的层次结构组织并访问信息的协议。其用途包括两部分：

- 确定资源位置，如网络上的组织、个体和文件等
- 帮助认证用户尝试连接由目录服务器控制的网络

LDAP 的基本结构分支至上而下依次为国家、组织、组织单位、个体。其中间还可包含其它分支层，如“州”和“县”等。下图为 LDAP 分支组织结构的一个范例。

LDAP 层次结构



* 个体可以是人、设备、文件等。(cn = 通用名称)

注意：有关 LDAP 的信息，请参阅 RFC-1777 “Lightweight Directory Access Protocol”。

可对 NetScreen 设备进行配置，以便链接到“轻量目录访问协议”(LDAP) 服务器。此服务器使用 LDAP 分层式语法来唯一识别每位用户。

LDAP Auth 服务器对象属性

除第 393 页上的“Auth 服务器对象属性”中列出的通用 auth 服务器属性外，LDAP 服务器还使用以下属性：

- **LDAP (LDAP) Server Port (服务器端口):** LDAP 服务器上的端口号，NetScreen 设备向此处发送认证请求。缺省端口号为 389。

注意：如果更改 NetScreen 设备上的 LDAP 端口号，同时也应在 LDAP 服务器上进行更改。

- **Common Name Identifier (通用名称标识符):** LDAP 服务器用来识别在 LDAP 服务器中输入的个体的标识符。例如，“uid”表示“用户 ID”，“cn”表示“通用名称”。
- **Distinguished Name (识别名称) (dn) :** LDAP 服务器在使用通用名称标识符搜索具体条目前使用的路径。(例如 c=us;o=netScreen，其中“c”代表“县”，“o”代表“组织”。)

支持的用户类型和功能

LDAP 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 (用户认证；L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置)
- XAuth 用户 (用户认证；不支持远程设置指派)
- Admin 用户 (用户认证；admin 用户接收只读的缺省权限指派)

目前，尽管可使用 LDAP 服务器存储 L2TP、XAuth 和 admin 用户帐户进行认证，但 LDAP 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 LDAP 配套使用时，NetScreen 不支持用户组。

定义 Auth 服务器对象

要在策略、IKE 网关和 L2TP 通道中引用外部认证服务器 (auth 服务器), 必须首先定义 auth 服务器对象。以下示例说明如何为 RADIUS 服务器、SecurID 服务器和 LDAP 服务器定义 auth 服务器对象。

范例 : RADIUS Auth 服务器

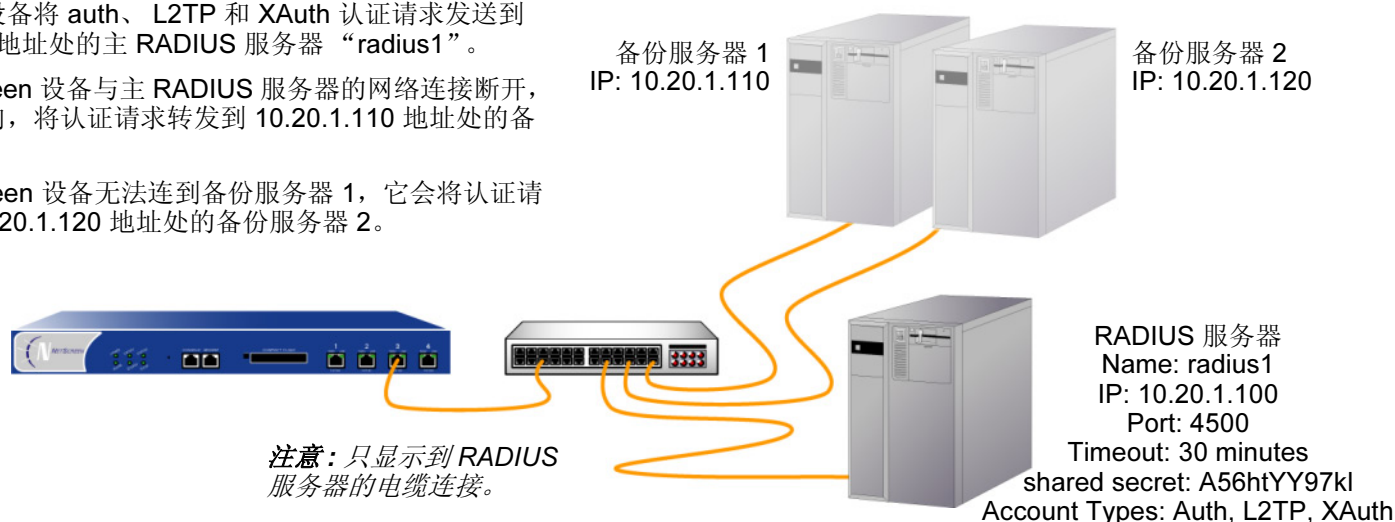
在下例中, 将为 RADIUS 服务器定义 auth 服务器对象。将其用户帐户类型指定为 auth、L2TP 和 XAuth。将 RADIUS 服务器命名为 “radius1”, 并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.1.100 ; 将其端口号由缺省值 (1645) 更改为 4500。将其共享机密定义为 “A56htYY97kl”。将认证超时值由缺省值 (10 分钟) 更改为 30 分钟, 并将 RADIUS 重试超时值由 3 秒更改为 4 秒。同时将两个备份服务器的 IP 地址分别指定为 10.20.1.110 和 10.20.1.120。

此外, 还要将 NetScreen 词典文件加载到 RADIUS 服务器上, 使其能支持下列供应商专用属性 (VSA) 的查询 : 用户组、管理权限、远程 L2TP 和 XAuth 设置。

NetScreen 设备将 auth、L2TP 和 XAuth 认证请求发送到 10.20.1.100 地址处的主 RADIUS 服务器 “radius1”。

如果 NetScreen 设备与主 RADIUS 服务器的网络连接断开, 它会重新定向, 将认证请求转发到 10.20.1.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1, 它会将认证请求转发到 10.20.1.120 地址处的备份服务器 2。



WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth, L2TP, XAuth

RADIUS: (选择)

RADIUS Port: 4500

Retry Timeout: 4 (秒)

Shared Secret: A56htYY97kl

将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的详细信息，请参阅第 397 页上的“NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。

CLI

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth l2tp xauth2
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 45003
set auth-server radius1 radius timeout 4
set auth-server radius1 radius secret A56htYY97kl
save
```

将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的详细信息，请参阅第 397 页上的“NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。

-
2. 帐户类型的输入顺序非常重要。例如，如果首先键入 **set auth-server radius1 account-type l2tp**，则随后只能选择 **xauth**；不能在 **l2tp** 后键入 **auth**。正确顺序非常容易记住，因为它是按字母顺序排列的。
 3. 更改端口号有助于防止可能有针对缺省 RADIUS 端口号 (1645) 展开的攻击。

范例 : SecurID Auth 服务器

在下例中, 将为 SecurID ACE 服务器配置 auth 服务器对象。将其用户帐户类型指定为 admin。将服务器命名为 “securid1”, 并接受 NetScreen 设备自动指派的 ID 号。输入主服务器的 IP 地址 10.20.2.100, 及备份服务器的 IP 地址 : 10.20.2.110。将其端口号由缺省值 (5500) 更改为 15000。NetScreen 设备和 SecurID ACE 服务器使用 DES 加密法保护认证信息。允许重试三次, 客户端超时值为 10 秒⁴。将空闲超时值由缺省值 (10 分钟) 更改为 60 分钟⁵。禁用 **Use Duress** 设置。

NetScreen 设备将 admin 认证请求发送到 10.20.2.100 地址处的主 SecurID 服务器 “securid1”。

如果 NetScreen 设备与主 SecurID 服务器的网络连接断开, 它会重新定向, 将认证请求转发到 10.20.2.110 地址处的备份服务器 1。

注意: NetScreen 针对 SecurID 只支持一个备份服务器。



4. 客户端超时值是指两次认证重试操作之间 SecurID 客户端 (即 NetScreen 设备) 等待的时间长度 (秒)。
5. 空闲超时值是指 NetScreen 设备在自动终止非活动 admin 会话前等待的空闲时间长度 (分钟)。(有关应用于 admin 用户和其它用户类型的超时值比较信息, 请参阅第 393 页上的 “Auth 服务器对象属性”。)

WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: securid1

IP/Domain Name: 10.20.2.100

Backup1: 10.20.2.110

Timeout: 60

Account Type: Admin

SecurID: (选择)

Client Retries: 3

Client Timeout: 10 seconds

Authentication Port: 15000

Encryption Type: DES

User Duress: No

CLI

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type admin
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
save
```

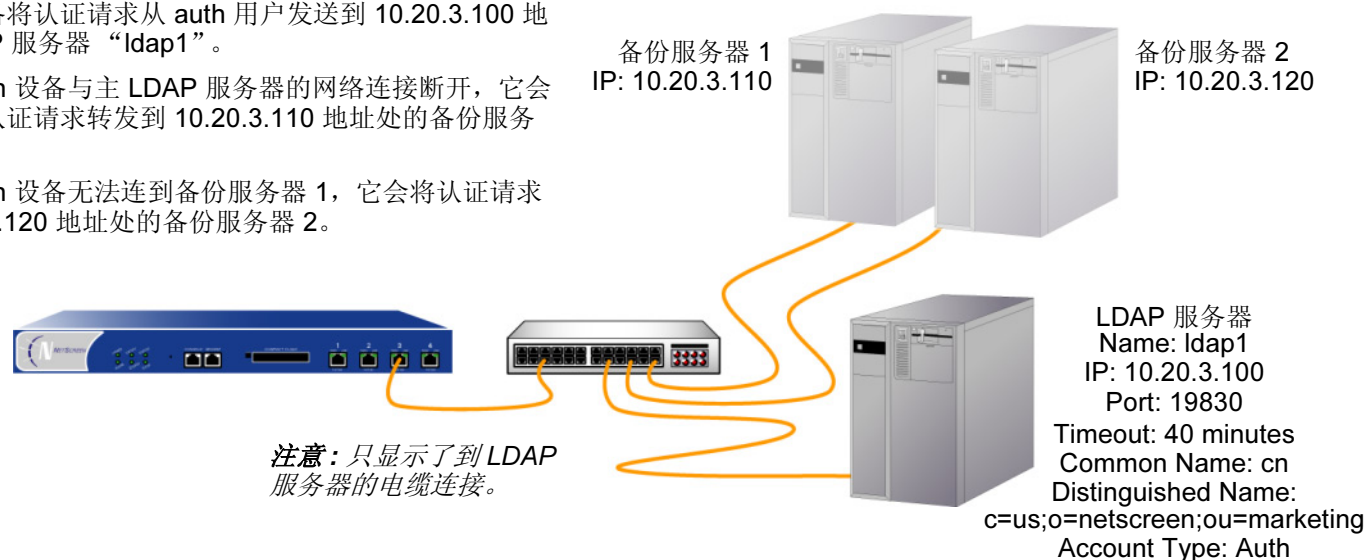
范例 : LDAP Auth 服务器

在下例中, 将为 LDAP 服务器配置 auth 服务器对象。将用户帐户类型指定为 auth。将 LDAP 服务器命名为“ldap1”, 并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.3.100; 将其端口号由缺省值 (389) 更改为 19830。将超时值由缺省值 (10 分钟) 更改为 40 分钟。同时将两个备份服务器的 IP 地址分别指定为 10.20.3.110 和 10.20.3.120。LDAP 通用名称标识符为 cn, Distinguished Name (识别名称) 为 c=us;o=netscreen;ou=marketing。

NetScreen 设备将认证请求从 auth 用户发送到 10.20.3.100 地址处的主 LDAP 服务器 “ldap1”。

如果 NetScreen 设备与主 LDAP 服务器的网络连接断开, 它会重新定向, 将认证请求转发到 10.20.3.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1, 它会将认证请求转发到 10.20.3.120 地址处的备份服务器 2。



WebUI

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: ldap1

IP/Domain Name: 10.20.3.100

Backup1: 10.20.3.110

Backup2: 10.20.3.120

Timeout: 40

Account Type: Auth

LDAP: (选择)

LDAP Port: 4500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=netScreen;ou=marketing

CLI

```
set auth-server ldap1 type ldap
set auth-server ldap1 account-type auth
set auth-server ldap1 server-name 10.20.3.100
set auth-server ldap1 backup1 10.20.3.110
set auth-server ldap1 backup2 10.20.3.120
set auth-server ldap1 timeout 40
set auth-server ldap1 ldap port 15000
set auth-server ldap1 ldap cn cn
set auth-server ldap1 ldap dn c=us;o=netScreen;ou=marketing
save
```


定义缺省 Auth 服务器

在缺省情况下，本地数据库是所有用户类型的缺省 **auth** 服务器。您可针对下列一种或多种用户类型，指定外部 **auth** 服务器作为缺省 **auth** 服务器：

- Admin
- Auth
- L2TP
- XAuth

这样，在策略、L2TP 通道、或 IKE 网关中配置认证时，如果希望对具体用户类型使用缺省 **auth** 服务器，则不必在每个配置中都指定 **auth** 服务器。NetScreen 设备会引用先前已指定为缺省服务器的相应 **auth** 服务器。

范例：更改缺省 Auth 服务器

在本例中，将使用先前范例中创建的 RADIUS、SecurID 和 LDAP **auth** 服务器对象：

- radius1 (第 404 页上的“范例：RADIUS Auth 服务器”)
- securid1 (第 407 页上的“范例：SecurID Auth 服务器”)
- ldap1 (第 409 页上的“范例：LDAP Auth 服务器”)

然后，指定本地数据库、radius1、securid1 和 ldap1 作为下列用户类型的缺省服务器：

- radius1: admin 用户的缺省 **auth** 服务器
- securid1: L2TP 用户的缺省 **auth** 服务器
- ldap1: auth 用户的缺省 **auth** 服务器
- Local: XAuth 用户的缺省 **auth** 服务器⁶

6. 在缺省情况下，本地数据库是所有用户类型的缺省 **auth** 服务器。因此，除非先前已为 XAuth 用户指定外部 **auth** 服务器作为缺省服务器，否则不必进行此配置。

WebUI

Configuration > Admin > Administrators: 从 Admin Auth Server 下拉列表中选择 **Local/radius1**，然后单击 **Apply**。

VPNs > AutoKey Advanced > XAuth Settings: 从 Default Authentication Server 下拉列表中选择 **Local**，然后单击 **Apply**⁷。

注意：对于策略中的 **auth** 用户认证或 **IKE** 网关中的 **XAuth** 用户认证，不能在 **WebUI** 中设置和引用缺省 **auth** 服务器。必须在要应用用户认证的每个策略和每个 **IKE** 网关配置中，从下拉列表选择一个 **auth** 服务器。

CLI

```
set admin auth server radius1
set auth default auth server ldap1
set l2tp default auth server securid1
set xauth default auth server Local7
save
```

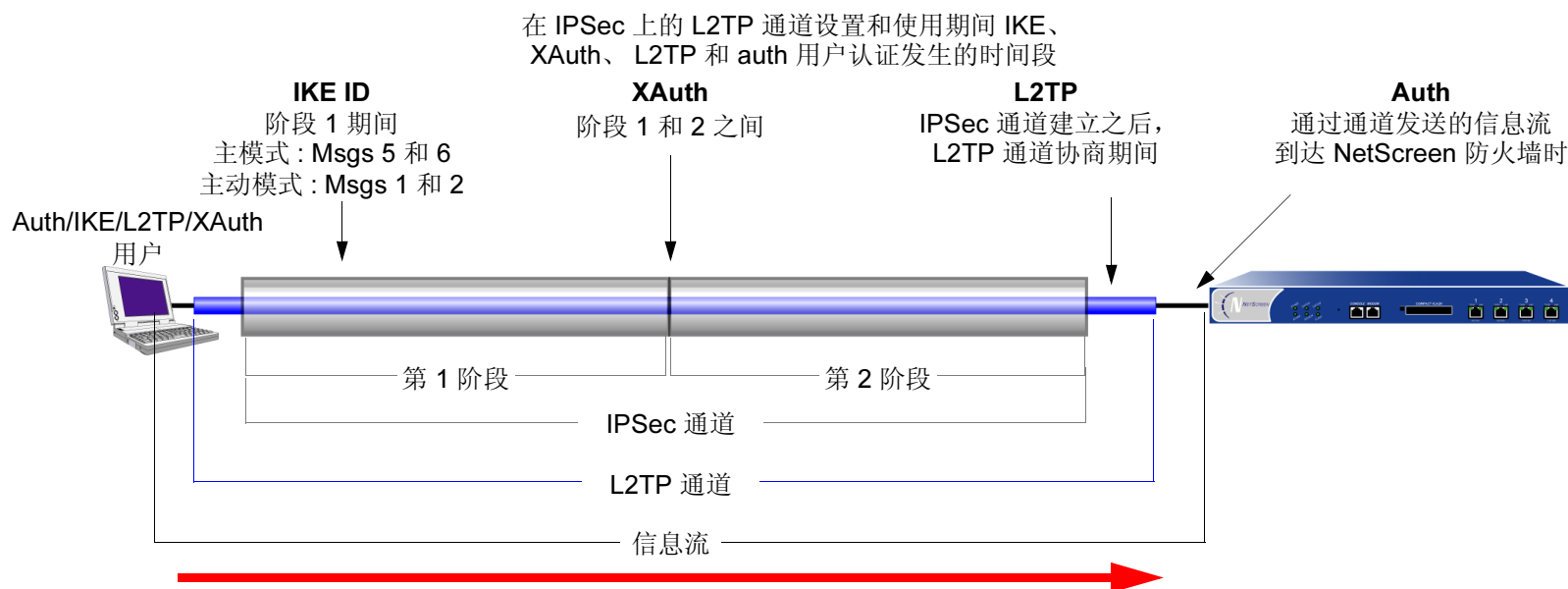
7. 在缺省情况下，本地数据库是所有用户类型的缺省 **auth** 服务器。因此，除非先前已为 **XAuth** 用户指定外部 **auth** 服务器作为缺省服务器，否则不必进行此配置。

认证类型及应用

以下部分介绍可以创建的不同类型用户组 and 用户，以及在配置策略、IKE 网关和 L2TP 通道时如何使用它们：

- 第 414 页上的 “Auth 用户和用户组”
- 第 447 页上的 “IKE 用户和用户组”
- 第 452 页上的 “XAuth 用户和用户组”
- 第 476 页上的 “L2TP 用户和用户组”
- 第 481 页上的 “Admin 用户”

NetScreen 设备在连接过程的不同阶段对不同类型的用户进行认证。有关在创建 IPsec 上的 L2TP VPN 通道期间 IKE、XAuth、L2TP 和 auth 认证技术运行的时间，请参阅下图：



注意：因为 XAuth 和 L2TP 都提供用户认证和地址分配，故通常它们不同时使用。此处将两者同时显示，只是为了说明 VPN 通道创建期间各种认证类型发生的时间。

Auth 用户和用户组

auth 用户是一个网络用户，启动通过防火墙的连接时，他 / 她必须提供用户名和密码进行认证。可将 **auth** 用户帐户存储在本地数据库或外部 **RADIUS**、**SecurID** 或 **LDAP** 服务器上。

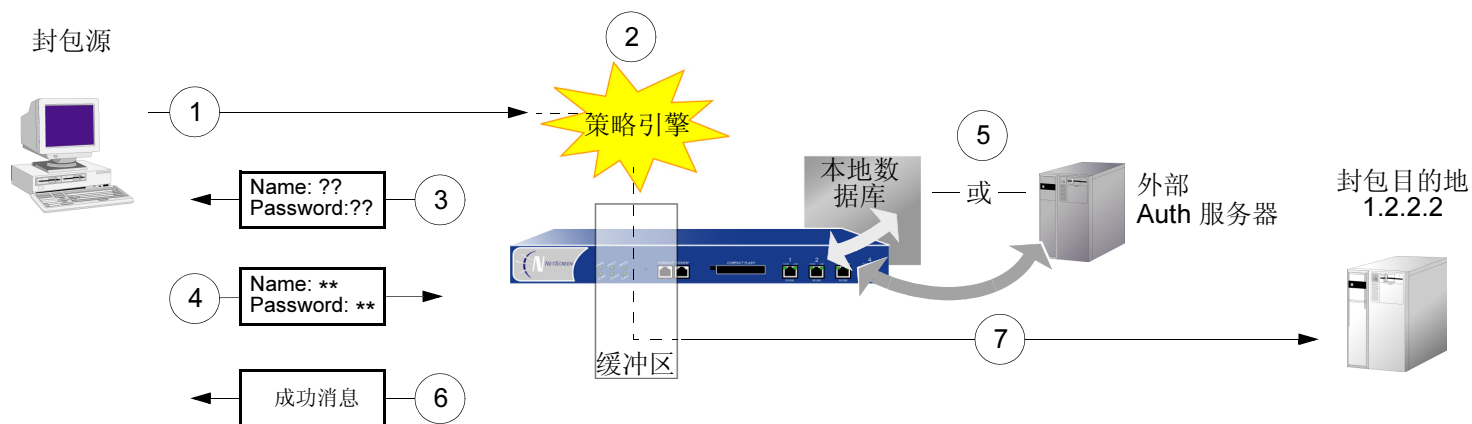
可将多个 **auth** 用户帐户集合到一起组成 **auth** 用户组，用户组可以存储在本地数据库或 **RADIUS** 服务器上。单个 **auth** 用户帐户最多可以存在于本地数据库或 **RADIUS** 服务器上的四个用户组中。如果在 **RADIUS** 服务器上创建外部用户组，也必须在 **NetScreen** 设备上创建一个相同 (但空白) 的用户组。例如，如果在名为 “**rs1**” 的 **RADIUS** 服务器上定义一个名为 “**au_grp1**” 的 **auth** 用户组，并在组中添加 10 个成员，则在 **NetScreen** 设备上必须也定义一个名为 “**au_grp1**” 的 **auth** 用户组，将其标识为外部用户组，但不能在其中添加成员。如果在策略中引用外部 **auth** 用户组 “**au_grp1**” 和 **auth** 服务器 “**rs1**”，则当与该策略匹配的信息流引发认证检查时，**NetScreen** 设备可以正确查询指定的 **RADIUS** 服务器。

在策略中引用 Auth 用户

定义 **auth** 用户后，可创建一个要求用户通过两种认证方案之一进行认证的策略。第一种方案在与要求认证的策略匹配的 **FTP**、**HTTP** 或 **Telnet** 信息流到达 **NetScreen** 设备时，对用户进行认证。在第二种方案中，用户在发送应用要求用户认证的策略的信息流 (任何类型，不局限于 **FTP**、**HTTP** 或 **Telnet**) 之前进行认证。

运行时认证

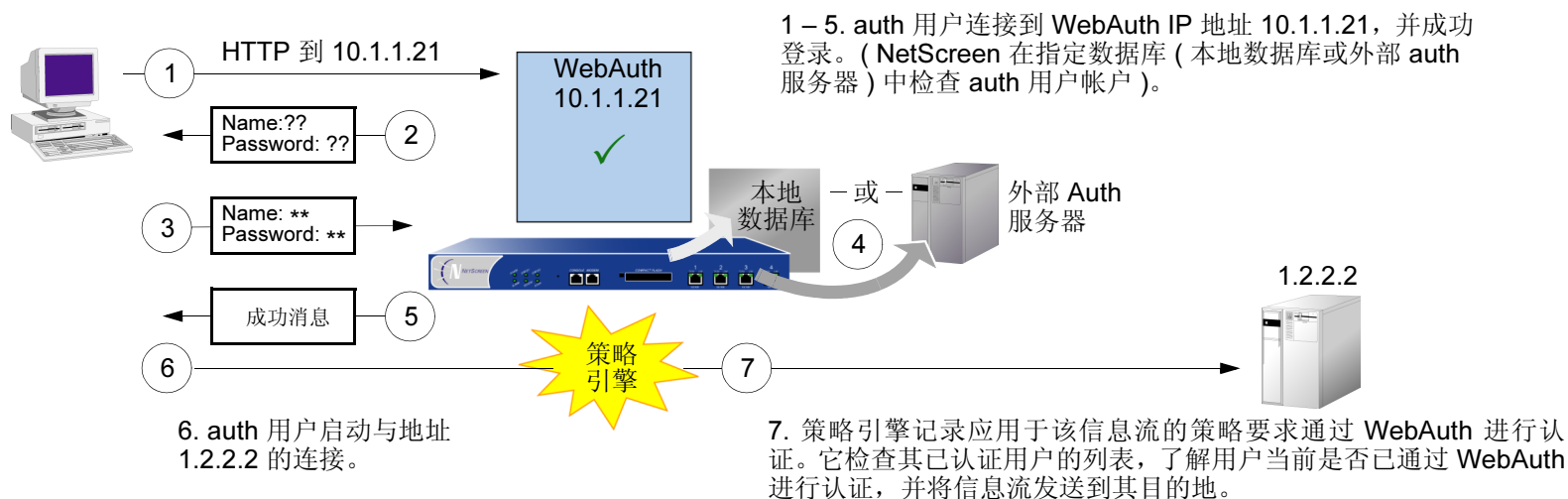
用户尝试启动 (应用要求进行认证的策略的) HTTP、FTP 或 Telnet 连接请求时, NetScreen 设备会截取该请求, 并提示用户输入名称和密码 (请参阅第 225 页上的 “用户认证”)。在批准请求之前, NetScreen 设备会将用户名和密码与本地数据库或外部 auth 服务器上的用户名和密码进行比较, 以确认其有效性。



1. auth 用户将 FTP、HTTP 或 Telnet 封包发送到 1.2.2.2。
2. NetScreen 设备截取封包, 记录其策略要求从本地数据库或 auth 服务器获得认证, 并将封包放入缓冲区。
3. NetScreen 设备提示用户通过 FTP、HTTP 或 Telnet 输入登录信息。
4. 用户以用户名和密码回复。
5. NetScreen 设备在其本地数据库上检查 auth 用户帐户, 或将登录信息发送到策略中指定的外部 auth 服务器。
6. 找到有效匹配项 (或从外部 auth 服务器接收到有效匹配的通告) 后, NetScreen 设备会通知用户登录成功。
7. NetScreen 设备将封包从其缓冲区转发到其目的地 1.2.2.2。

策略前检查认证 (WebAuth)

将信息流发送到预定目的地之前，auth 用户启动面向此 IP 地址的 HTTP 会话 (将 WebAuth 功能交由 NetScreen 设备托管)，并对自己进行认证。NetScreen 设备对用户进行认证后，用户可根据要求通过 WebAuth 进行认证的策略的许可，将信息流发送至目的地。(有关详细信息，请参阅第 414 页上的“Auth 用户和用户组”。)



有关 WebAuth 的一些详细说明：

- 可保留本地数据库作为缺省 WebAuth auth 服务器，也可为之选择外部 auth 服务器。WebAuth auth 服务器的主要要求是：auth 服务器必须具有 auth 用户帐户类型。
- WebAuth 地址必须与要用来托管该地址的接口处于相同的子网内。例如，如果希望 auth 用户通过 ethernet3 (IP 地址为 1.1.1.1/24) 与 WebAuth 相连，则可将 WebAuth 的 IP 地址指定在 1.1.1.0/24 子网内。
- 可将 WebAuth 地址设置在与任意物理接口、子接口或虚拟安全接口 (VSI) 相同的子网内。(有关不同类型接口的信息，请参阅第 67 页上的“接口”。)

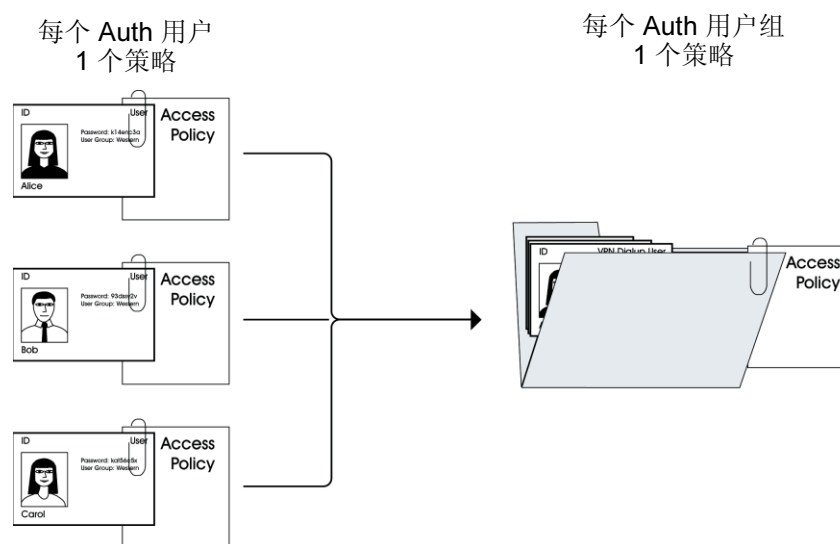
- 如果要在“透明”模式中使用 WebAuth，可将 WebAuth 地址设置在与 VLAN1 IP 地址相同的子网内。
- 可将 WebAuth 地址设置于多个接口上。
- 如果在同一安全区绑定多个接口，则可将 WebAuth 地址设置于某个接口的子网中，来自同一区段但使用不同接口的信息流仍可到达该处。
- 注意：NetScreen 设备对特定源 IP 地址的用户进行认证，随后允许来自同一地址其他任何用户的信息流（在需要通过 WebAuthit 进行认证的策略中指定）。如果用户从 NAT 设备（可将所有初始源地址更改为单个转换后的地址）后面发出信息流，则实际情况可能就是这样。

在策略中引用 Auth 用户组

要管理多个 **auth** 用户，可创建 **auth** 用户组，并将其存储在本地 **NetScreen** 设备或外部 **RADIUS** 服务器上。

注意：如果将用户存储到 **RADIUS** 服务器上的组中，则必须在 **NetScreen** 设备上创建空白的外部用户组，其名称与在 **RADIUS** 服务器上创建的用户组名称一致。

您可将用户集合成组，使对此组实施的任何更改应用于组的所有成员，而不必分别管理每个用户。一个 **auth** 用户最多可以成为本地数据库或 **RADIUS** 服务器上的四个用户组的成员。要求属于多个组的 **auth** 用户只提供一次用户名和密码，即可准予访问为该用户所属的每个组定义的资源。



范例：运行时认证（本地用户）

在本例中，将定义一个名为 **louis** 的本地 **auth** 用户，其密码为 **iDa84rNk**，在 **Trust** 区段通讯簿中的地址名为 **“host1”**。然后配置两个外向策略：一个拒绝所有出站信息流，另一个来自 **host1**，要求 **louis** 进行认证。（**Louis** 必须启动所有来自 **host1** 的出站信息流。）**NetScreen** 设备会拒绝来自其它所有地址的出站访问请求以及来自 **“host1”** 的未经认证信息流。

WebUI

1. 本地 Auth 用户和地址

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: louis

Status: Enable

Authentication User: (选择)

User Password: iDa84rNk

Confirm Password: iDa84rNk

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

Address Name: host1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.4/32

Zone: Trust

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Deny

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), host1

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User: (选择), Local Auth User - louis

CLI

1. 本地用户和地址

```
set user louis password iDa84rNk8  
set address trust host1 10.1.1.4/32
```

2. 策略

```
set policy from trust to untrust any any any deny  
set policy top from trust to untrust host1 any any permit auth user louis  
save
```

8. 在缺省情况下，要为之指定密码的用户被归类为 **auth** 用户。

范例：运行时认证（本地用户组）

在本例中，将定义一个名为 **auth_grp1** 的本地用户组。将先前创建的 **auth** 用户 **louis** 和 **lara** 添加到该组中⁹。然后配置一个引用 **auth_grp1** 的策略。此策略为 **auth_grp1** 提供 **FTP-GET** 和 **FTP-PUT** 权限，令其以区段中“**auth_grp1**”地址名 (IP 地址 10.1.8.0/24) 访问 DMZ 区段中名为“**ftp1**” (IP 地址 1.2.2.3/32) 的 FTP 服务器。

WebUI

1. 本地用户组和成员

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **auth_grp1**，执行以下操作，然后单击 **OK**：

选择 **louis**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **lara**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. 地址

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

Address Name: **auth_grp1**

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.8.0/24

Zone: Trust

9. 在本地数据库中创建用户组时，在向组中添加用户之前，用户组的用户类型不会定义。而添加用户后，用户组将获得与添加于其中的用户相同的类型。通过添加 **auth**、**IKE**、**L2TP** 和 **XAuth** 用户类型可创建多类型用户组。不能将 **Admin** 用户与其它任意用户类型组合。

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

Address Name: ftp1

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.3/32

Zone: DMZ

3. 策略

Policies > (From: Trust; To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), auth_grp1

Destination Address:

Address Book Entry: (选择), ftp1

Service: FTP

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - auth_grp1

CLI

1. 本地用户组和成员

```
set user-group auth_grp1 location local
set user-group auth_grp1 user louis
set user-group auth_grp1 user lara
```

2. 地址

```
set address trust auth_grp1 10.1.8.0/24
set address dmz ftp1 1.2.2.3/32
```

3. 策略

```
set policy top from trust to dmz auth_grp1 ftp1 ftp permit auth user-group
    auth_grp1
save
```

范例：运行时认证（外部用户）

在本例中，将定义名为“x_srv1”的外部 LDAP auth 服务器，其属性如下：

- Account type: auth
- IP address: 10.1.1.100
- Backup1 IP address: 10.1.1.110
- Backup2 IP address: 10.1.1.120
- Authentication timeout: 60 minutes
- LDAP port number: 14500
- Common name identifier: cn
- Distinguished name: c=us;o=netscreen

以密码 eTcS114u 将 auth 用户“euclid”加载到外部 auth 服务器上。然后，为外部用户 euclid 配置要求在 auth 服务器 x_srv1 上进行认证的外向策略。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: x_srv1

IP/Domain Name: 10.1.1.100

Backup1: 10.1.1.110

Backup2: 10.1.1.120

Timeout: 60

Account Type: Auth

LDAP: (选择)

LDAP Port: 14500

Common Name Identifier: cn

Distinguished Name (dn): c=us;o=netscreen

2. 外部用户

在外部 LDAP auth 服务器 x_serv1 上定义 auth 用户 “euclid”，密码为 eTcS114u。

3. 地址

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

Address Name: euc_host

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.20/32

Zone: Trust

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: x_srv1

User: (选择), External User

External User: euclid

CLI

1. Auth 服务器

```
set auth-server x_srv1
set auth-server x_srv1 type ldap
set auth-server x_srv1 account-type auth
set auth-server x_srv1 server-name 10.1.1.100
set auth-server x_srv1 backup1 10.1.1.110
set auth-server x_srv1 backup2 10.1.1.120
set auth-server x_srv1 timeout 60
set auth-server x_srv1 ldap port 14500
set auth-server x_srv1 ldap cn cn
set auth-server x_srv1 ldap dn c=us;o=netscreen
```

2. 外部用户

在外部 LDAP auth 服务器 **x_serv1** 上定义 auth 用户 “euclid”，密码为 eTcS114u。

3. 地址

```
set address trust euc_host 10.1.1.20/32
```

4. 策略

```
set policy top from trust to untrust euc_host any any auth server x_srv1 user
    euclid
save
```

范例：运行时认证（外部用户组）

在本例中，将配置名为“radius1”的外部 RADIUS auth 服务器¹⁰，定义名为“auth_grp2”的外部 auth 用户组。在下列两个位置定义外部 auth 用户组 auth_grp2：

1. 外部 RADIUS auth 服务器 “radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 auth 用户装入 auth 用户组“auth_grp2”中，而将 NetScreen 设备上的组保留为空白。此组中的成员是要求独占访问 IP 地址 10.1.1.80 处服务器的帐户用户。为该服务器创建一个通讯簿条目，并将地址命名为“midas”。然后配置一个内部区段策略，只允许已经认证的信息流从 auth_grp2 流向 midas，这两者均位于 Trust 区段中。（有关内部区段策略的详细信息，请参阅第 7 章，“策略”。）

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上¹¹。

注意：有关 NetScreen 词典文件的信息，请参阅第 397 页上的“NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。

2. 在 RADIUS 服务器上定义 auth 用户帐户后，使用 NetScreen 用户组 VSA 创建用户组“auth_grp2”，并将其应用于要添加到该组中的 auth 用户帐户。

10. RADIUS auth 服务器的配置与第 404 页上的“范例：RADIUS Auth 服务器”中大致相同，但本例中仅指定“auth”作为用户帐户类型。

11. 如果使用 Microsoft IAS RADIUS 服务器，则不会有要加载的任何词典文件。相反，应在服务器上定义正确的供应商专用属性 (VSA)。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth

RADIUS: (选择)

RADIUS Port: 4500

Shared Secret: A56htYY97kl

2. 外部用户组

Objects > Users > External Groups > New: 输入以下内容，然后单击 **OK**:

Group Name: auth_grp2

Group Type: Auth

3. 地址

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

Address Name: midas

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.80/32

Zone: Trust

4. 策略

Policies > (From: Trust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), midas

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

User Group: (选择), External Auth Group - auth_grp2

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. 外部用户组

```
set user-group auth_grp2 location external
set user-group auth_grp2 type auth
```

3. 地址

```
set address trust midas 10.1.1.80/32
```

4. 策略

```
set policy top from trust to trust any midas any permit auth server radius1
    user-group auth_grp2
save
```

范例：多个组中的本地 Auth 用户

在本例中，将定义一个名为 **Mary** 的本地 **auth** 用户。**Mary** 是一名销售经理，需要访问下列两台服务器：用于销售人员 (**sales_reps** 组) 的服务器 **A** 和用于经理 (**sales_mgrs** 组) 的服务器 **B**。要提供对这两台服务器的访问权限，需要将 **Mary** 添加到两个用户组中。然后创建两个策略——一组一个策略。

注意：本例并不说明其他组成员的配置。

WebUI

1. 本地用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: mary

Status: Enable

Authentication User: (选择)

User Password: iFa8rBd

Confirm Password: iFa8rBd

2. 本地用户组和成员

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **sales_mgrs**，执行以下操作，然后单击 **OK**:

选择 **mary**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **sales_reps**，执行以下操作，然后单击 **OK**:

选择 **mary**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

3. 地址

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

Address Name: sales

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.8.0/24

Zone: Trust

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

Address Name: server_a

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/32

Zone: Untrust

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

Address Name: server_b

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.6/32

Zone: Untrust

4. 策略

Policies > (From: Trust; To: Untrust) > New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), sales

Destination Address:

Address Book Entry: (选择), server_a

Service: FTP

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - sales_reps

Policies > (From: Trust; To: Untrust) > New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), sales

Destination Address:

Address Book Entry: (选择), server_b

Service: FTP

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

User Group: (选择), Local Auth Group - sales_mgrs

CLI

1. 本地用户

```
set user mary password iFa8rBd
```

2. 本地用户组和成员

```
set user-group sales_mgrs location local
set user-group sales_mgrs user mary
set user-group sales_reps location local
set user-group sales_reps user mary
```

3. 地址

```
set address trust sales 10.1.8.0/24
set address untrust server_a 1.1.1.5/32
set address untrust server_b 1.1.1.6/32
```

4. 策略

```
set policy top from trust to untrust sales server_a ftp permit auth user-group
    sales_reps
set policy top from trust to untrust sales server_b ftp permit auth user-group
    sales_mgrs
save
```

范例 : WebAuth (本地用户组)

本例中，在启动流向互联网的出站信息流之前，要求用户通过 **WebAuth** 方式进行预认证。在 **NetScreen** 设备上的本地数据库中创建名为 “**auth_grp3**” 的用户组。然后，为 **Trust** 区段中的每个对象创建 **auth** 用户帐户，并将其添加到 “**auth_grp3**” 中。

Trust 区段接口使用 **ethernet1**，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 **WebAuth** IP 地址，并保留本地数据库作为缺省的 **WebAuth** 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 **HTTP** 方式连接到 10.1.1.50，并以用户名和密码登录。然后，**NetScreen** 设备将该用户名和密码与其数据库中的内容进行比较，以批准或拒绝认证请求。如果它批准该请求，被认证的用户将有 30 分钟的时间启动流向互联网的信息流。终止该启动会话后，在 **NetScreen** 设备要求用户重新认证之前，用户又有 30 分钟的时间启动另一会话。

WebUI

1. WebAuth

Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **Local**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet1): 选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.1.1.50**。

Configuration > Auth > Servers > Edit (对于 Local): 在 Timeout 字段中输入 **30**，然后单击 **Apply**。

2. 用户组

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **auth_grp3**，执行以下操作，然后单击 **OK**:

选择 **user name**，并使用 << 按钮将该用户从 Available Members 栏移动到 Group Members 栏中。

重复选择过程，添加 **auth** 用户，直到该组完成为止。

3. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), Local Auth Group - auth_grp3

CLI

1. WebAuth

```
set webauth server Local
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
set auth-server Local timeout 30
```

2. 用户组

```
set user-group auth_grp3 location local
```

注意：NetScreen 设备根据添加于本地用户组中的成员类型来确定组的类型。要使 `auth_grp3` 成为 `auth` 用户组，应在组中添加一个 `auth` 用户。

使用以下命令将 `auth` 用户添加到刚刚创建的用户组中：

```
set user-group auth_grp3 user name_str
```

3. 策略

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp3
save
```

范例 : WebAuth (外部用户组)

WebAuth 是一种用于在用户启动通过防火墙的信息流之前进行预认证的方法。在本例中，将创建一个要求对所有外向信息流通过 WebAuth 方法进行认证的策略。

在 RADIUS 服务器 “radius1” 和 NetScreen 设备上创建名为 “auth_grp4” 的 auth 用户组。在 RADIUS 服务器上，为 Trust 区段中的每个对象创建用户帐户，并将其添加到 “auth_grp4” 中。

注意：此处使用的 RADIUS 服务器设置与第 404 页上的 “范例: RADIUS Auth 服务器” 中大致相同，但本例中仅指定 “auth” 作为用户帐户类型。

Trust 区段接口使用 ethernet1，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 WebAuth IP 地址，并使用外部 RADIUS auth 服务器 “radius1” 作为缺省的 WebAuth 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 10.1.1.50，并以用户名和密码登录。然后，NetScreen 设备在 “radius1” 和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的信息，请参阅第 397 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。

2. 在 auth 服务器 “radius1” 上输入用户组 “auth_grp4”，然后在其中装入 auth 用户帐户。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth

RADIUS: (选择)

RADIUS Port: 4500

Shared Secret: A56htYY97k

2. WebAuth

Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet1): 选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.10.1.50**，然后单击 **OK**。

3. 用户组

Objects > Users > External Groups > New: 输入以下内容，然后单击 **OK**:

Group Name: auth_grp4

Group Type: Auth

4. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), External Auth Group - auth_grp4

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. WebAuth

```
set webauth server radius1
set interface ethernet1 webauth-ip 10.1.1.50
set interface ethernet1 webauth
```

3. 用户组

```
set user-group auth_grp4 location external
set user-group auth_grp4 type auth
```

4. 策略

```
set policy top from trust to untrust any any any permit webauth user-group
    auth_grp4
save
```


范例 : WebAuth + SSL (外部用户组)

在本例中, 将 WebAuth 与 “安全套接字层” (SSL) 技术组合, 来保护用户登录时发送的用户名和密码。WebAuth 利用相同的证书来保护流向 NetScreen 设备的管理信息流 (以通过 WebUI 进行管理)。(有关 SSL 的详细信息, 请参阅第 3-7 页上的 “安全套接字层”。)

使用外部 auth 服务器的 WebAuth 加 SSL 的配置包括以下步骤:

- 定义外部 RADIUS auth 服务器 “radius1”, 在 RADIUS 服务器和 NetScreen 设备上创建名为 “auth_grp5” 的 auth 用户组。在 RADIUS 服务器上, 为 Untrust 区段中的所有 auth 用户创建用户帐户, 并将其添加到 “auth_grp5” 中。

注意: 此处使用的 RADIUS 服务器设置与第 404 页上的 “范例: RADIUS Auth 服务器” 中大致相同, 但本例中仅指定 “auth” 作为用户帐户类型。

- 区段接口使用 ethernet3, 其 IP 地址为 1.1.1.1/24。指定 1.1.1.50 作为 WebAuth IP 地址, 并使用外部 RADIUS auth 服务器 “radius1” 作为缺省的 WebAuth 服务器。
- 指定以下 SSL 设置:
 - 先前加载到 NetScreen 设备上的证书的 IDX 号 (本例中为 1)¹²
 - DES_SHA-1 密码
 - SSL 端口号 2020
- 在 ethernet3 上启用 SSL 可管理性, 这样 ethernet3 不会拒绝与该接口的 SSL 连接尝试。
- 然后, 配置一个要求对从 Untrust 区段到 Trust 区段的所有信息流通过 WebAuth + SSL 方法进行认证的内向策略。

因此, 用户在启动流向互联网的信息流之前, 必须首先以 HTTP 方式连接到 https://1.1.1.50: 2020, 并以用户名和密码登录。然后, NetScreen 设备在 “radius1” 和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

12. 有关如何获取数字证书并将其加载到 NetScreen 设备的信息, 请参阅第 5-15 页上的 “公开密钥密码术”。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的信息，请参阅第 397 页上的“NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。

2. 在 auth 服务器 “radius1” 上输入用户组 “auth_grp5”，然后在其中装入 auth 用户帐户。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1

IP/Domain Name: 10.20.1.100

Backup1: 10.20.1.110

Backup2: 10.20.1.120

Timeout: 30

Account Type: Auth

RADIUS: (选择)

RADIUS Port: 4500

Shared Secret: A56htYY97k

2. WebAuth

Configuration > Auth > WebAuth: 从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet3): 选择 **WebAuth**，在 WebAuth IP 字段中输入 **1.1.1.50**，然后单击 **OK**。

3. SSL

Configuration > Admin > Management: 输入以下内容，然后单击 **OK**:

HTTPS (SSL) Port: 2020

Certificate: (选择先前加载的证书)

Cipher: DES_SHA-1

Network > Interfaces > Edit (对于 ethernet3): 在 Management Services 区域中选择 **SSL**，然后单击 **OK**。

4. 用户组

Objects > Users > External Groups> New: 输入以下内容，然后单击 **OK**:

Group Name: auth_grp5

Group Type: Auth

5. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

WebAuth: (选择)

User Group: (选择), External Auth Group - auth_grp5

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type auth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的信息，请参阅第 397 页上的“NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。

2. WebAuth

```
set webauth server radius1
set interface ethernet3 webauth-ip 1.1.1.50
set interface ethernet3 webauth
```

3. SSL

```
set ssl port 2020
set ssl cert 1
set ssl encrypt des sha-1
set ssl enable
```

4. 用户组

```
set user-group auth_grp5 location external
set user-group auth_grp5 type auth
```

5. 策略

```
set policy top from untrust to trust any any any permit webauth user-group
    auth_grp5
save
```

IKE 用户和用户组

IKE 用户是具有动态分配 IP 地址的远程 VPN 用户。用户 (实际上是用户的设备) 在 “阶段 1” 与 NetScreen 设备协商期间, 通过发送 IKE ID 及证书或预共享密钥, 来对自身进行认证。

IKE ID 可以是电子邮件地址、IP 地址、域名或 ASN1-DN 字符串¹³。如果某 IKE 用户发送以下内容, NetScreen 设备将认证此 IKE 用户:

- **证书**, 其中 Distinguished name (DN) (识别名称) 字段或 SubAltName 字段中的一个或多个值与 NetScreen 设备上配置的用户 IKE ID 相同。
- **预共享密钥**和 **IKE ID**, NetScreen 设备可从接收的 IKE ID 及其上存储的预共享密钥种子值成功生成相同的预共享密钥

在 “自动密钥” IKE 网关配置中引用 IKE 用户或用户组。将需要相同网关和通道配置的 IKE 用户集合到一个组中后, 只需定义一个引用该组的网关 (和一个引用该网关的 VPN 通道), 而不必为每个 IKE 用户定义一个网关和通道。

通常, 为每个主机创建独立的用户帐户是不可能的。在这种情况下, 可创建只具有一个成员的 IKE 用户组, 作为一个组 IKE ID 用户。该用户的 IKE ID 包含一组必须出现在拨号 IKE 用户的 IKE ID 定义中的值。如果远程拨号 IKE 用户的 IKE ID 与组 IKE ID 用户的 IKE ID 相匹配, NetScreen 将认证该远程用户。有关详细信息, 请参阅第 5-237 页上的 “组 IKE ID”。

注意: IKE 用户和 IKE 用户组帐户只能存储在本地数据库上。

13. 使用 “抽象语法表示法” 版本 1 的一个 IKE ID 示例, 识别名称 (ASN1-DN) 格式为: CN=joe,OU=it,O=netscreen,L=sunnyvale,ST=ca,C=us,E=joe@ns.com。

范例：定义 IKE 用户

在本例中，将定义四个 IKE 用户，Amy、Basil、Clara 和 Desmond，每个用户具有不同的 IKE ID 类型。

- Amy – 电子邮件地址 (用户完全合格的域名或 U-FQDN): amy@ns.com
- Basil – IP 地址 : 3.3.1.1
- Clara – 完全合格的域名 (FQDN): www.netscreen.com
- Desmond – ASN1-DN 字符串 : CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com

WebUI

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Amy

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: amy@ns.com

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Basil

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: 3.3.1.1

Objects > Users > Local > New: 输入以下内容, 然后单击 **OK**:

User Name: Clara

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: www.netscreen.com

Objects > Users > Local > New: 输入以下内容, 然后单击 **OK**:

User Name: Desmond

Status: Enable

IKE User: (选择)

Use Distinguished Name for ID: (选择)

CN: des

OU: art

Organization: netscreen

Location: sunnyvale

State: ca

Country: us

E-mail: des@ns.com

CLI

```
set user Amy ike-id u-fqdn amy@ns.com
set user Basil ike-id ip 3.3.1.1
set user Clara ike-id fqdn www.netscreen.com
set user Desmond ike-id wildcard
    CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com
save
```

范例：创建 IKE 用户组

在本例中，将创建一个名为 `ike_grp1` 的用户组。向其中添加 IKE 用户 **Amy** 时，它即成为 IKE 用户组。然后添加上例第 448 页上的“范例：定义 IKE 用户”中定义的其它三个 IKE 用户。

WebUI

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **ike_grp1**，执行以下操作，然后单击 **OK**:

选择 **Amy**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Basil**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Clara**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Desmond**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

CLI

```
set user-group ike_grp1 location local
set user-group ike_grp1 user amy
set user-group ike_grp1 user basil
set user-group ike_grp1 user clara
set user-group ike_grp1 user desmond
save
```


在网关中引用 IKE 用户

定义 IKE 用户或 IKE 用户组后，当远程 IKE 网关是一个拨号用户或拨号用户组时，可在 IKE 网关配置中引用它。

以下为在网关配置中引用 IKE 用户的范例：

- 第 5-201 页上的“范例：基于策略的拨号 VPN，自动密钥 IKE”
- 第 5-243 页上的“范例：组 IKE ID (证书)”
- 第 5-252 页上的“范例：组 IKE ID (预共享密钥)”

XAuth 用户和用户组

XAuth 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¹⁴、DNS 服务器与 WINS 服务器分配）。NetScreen 支持其中一项或两项同时应用。

XAuth 用户或用户组是通过“自动密钥 IKE”VPN 通道连接到 NetScreen 设备时对自身进行认证的一个或多个远程用户，也可接受来自 NetScreen 设备的 TCP/IP 设置。IKE 用户认证实际是对 VPN 网关或客户端的认证，而 XAuth 用户的认证则是对个体自身的认证。XAuth 用户必须输入只有自己应该知道的信息——用户名和密码。

NetScreen-Remote 客户端可使用接收的 TCP/IP 设置创建一个虚拟适配器¹⁵，发送 VPN 信息流时可使用此虚拟适配器，而对于非 VPN 信息流则使用 ISP 或网络管理员提供的 TCP/IP 网络适配器设置。通过为远程用户分配已知的 IP 地址，可在 NetScreen 设备上定义通过特定通道接口到达此地址的路由。然后，NetScreen 设备可以确保返回路由通过 VPN 通道而非缺省网关，到达远程用户的 IP 地址。地址分配还允许下游防火墙在创建策略时引用这些地址。您可控制 IP 地址与具有 XAuth 生存期设置的单个 XAuth 用户相关联的时间长度。

14. 分配的网络掩码始终为 255.255.255.255，并且不能修改。

15. 虚拟适配器是 TCP/IP 设置（IP 地址、DNS 服务器地址、WINS 服务器地址），它由 NetScreen 设备分配给远程用户，以在 VPN 通道连接期间使用。只有 NetScreen-Remote 客户端才支持虚拟适配器功能。NetScreen 平台不支持此功能。

ScreenOS 支持 XAuth 的以下方面：

- 本地 XAuth 用户和外部 XAuth 用户的认证
- 本地 XAuth 用户组和外部 XAuth 用户组的认证 (如果存储在 RADIUS auth 服务器上)
- 从 IP 地址池为本地 XAuth 用户和 RADIUS auth 服务器上存储的外部 XAuth 用户分配 IP、DNS 服务器和 WINS 服务器地址

要配置 NetScreen 设备，使之使用外部 RADIUS 服务器上存储的缺省 XAuth 设置，请执行以下任一操作：

- WebUI: 在 VPNs > AutoKey Advanced > XAuth Settings 页面上，选择 **Query Client Settings on Default Server**。
- CLI: 输入 **set xauth default auth server name_str query-config** 命令。

NetScreen 设备还可使用外部 RADIUS 服务器上存储的网关专用 XAuth 设置。配置具体的 IKE 网关时，请执行以下操作之一：

- WebUI: 在 VPNs > AutoKey Advanced > Gateway > New > Advanced 页面上，从 External Authentication 下拉列表中选择 RADIUS 服务器的名称，然后选择 **Query Remote Setting**。
- CLI: 输入 **set ike gateway name_str xauth server name_str query-config** 命令。

IKE 协商中的 XAuth 用户

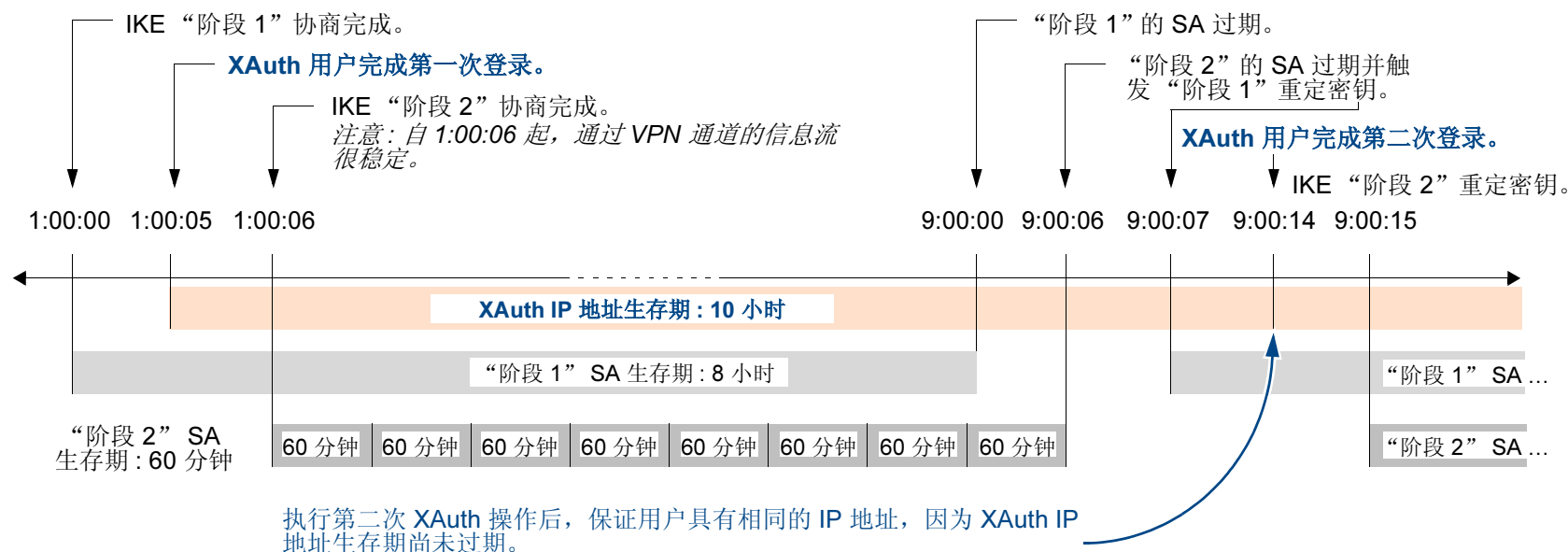
NetScreen 支持 XAuth 版本 6 (v6)。为确保“阶段 1”IKE 协商中的双方都支持 XAuth v6，它们在前两个“阶段 1”消息中都向对方发送以下供应商 ID: 0x09002689DFD6B712。此供应商 ID 号在 XAuth 互联网草案 draft-beaulieu-ike-xauth-02.txt 中指定。

“阶段 1”协商完成后，NetScreen 设备向远程站点的 XAuth 用户发送登录提示。如果 XAuth 用户使用正确的用户名和密码成功登录，则 NetScreen 设备将为该用户分配 IP 地址、32 位网络掩码、DNS 服务器地址和 WINS 服务器地址，双方继续进行“阶段 2”协商。

XAuth 用户有 60 秒时间完成登录过程。如果第一次登录尝试失败，则 XAuth 用户还可进行四次尝试，每次尝试都有 60 秒时间。如果用户连续 5 次尝试均失败，则 NetScreen 设备停止提供登录提示，并切断会话。

至少, XAuth 分配的 IP 地址在指定的 XAuth 地址生存期期间属于某用户。IP 地址属于 XAuth 用户的时间可能更长, 具体取决于“阶段 1”和“阶段 2”安全联盟 (SA) 重定密钥。下例说明“阶段 1”和“阶段 2”重定密钥操作与 XAuth IP 地址生存期的关系。

XAuth IP 地址生存期



1. “阶段 1” SA 生存期设置为 8 小时, 第一个 8 小时后过期。
2. “阶段 2” SA 生存期设置为 60 分钟。由于当 XAuth 用户输入用户名和密码时, 在初始 IKE 协商期间有 5 秒的延迟, 所以“阶段 1”协商完成后, 第 8 个“阶段 2” SA 过期 8 小时 6 秒 (XAuth 登录 5 秒 + “阶段 2”协商 1 秒)。
3. 由于有活动的 VPN 信息流, 所以第 8 个“阶段 2” SA 的到期引起 6 秒前到期的“阶段 1” SA 重定密钥, 即“阶段 1” IKE 协商 (或“重新协商”) 发生。

4. “阶段 1” IKE 重新协商完成后，NetScreen 设备提示 XAuth 用户再次登录。

注意：要避免初始登录后重复进一步登录，请用 CLI 命令为 VPN 通道配置除 0 之外的任何空闲时间：**set vpn name gateway name idletime number** (单位为分钟)。如果“阶段 1”IKE 重新协商完成时有 VPN 活动，则 NetScreen 设备不会提示 XAuth 用户再次登录。利用此选项，用户可以毫无中断地下载大文件、传输或接收流动媒体、参与网络会议。

5. 由于 XAuth 地址生存期 (10 小时) 超过了“阶段 1”SA 生存期，所以用户保持相同的 IP 地址 — 尽管下一个“阶段 1”重定密钥发生后，用户可能得到一个不同的地址。

如果 XAuth 地址生存期比“阶段 1”SA 生存期短，则 NetScreen 设备会为用户分配另一个 IP 地址，它可能与先前分配的地址¹⁶相同，也可能不同。

注意：要更改地址生存期，请执行以下操作之一：

- (WebUI) VPNs > AutoKey Advanced > XAuth Settings: 在 Reserve Private IP for XAuth User 字段中输入数值 (分钟)，然后单击 **Apply**。
- (CLI) **set xauth lifetime number**

要有效禁用地址生存期功能，请输入允许的最小值 1。

16. 如果必须为某个用户始终分配相同的 IP 地址，则可在用户配置中指定地址。然后，NetScreen 设备会分配此地址，而不是从 IP 池中随机分配一个地址。请注意，这样的地址不能在 IP 池中，否则，它可能会被分配给其它用户，而在需要时无法使用。

范例 : XAuth 认证 (本地用户)

在本例中，将在本地数据库上定义名为 **x1**、密码为 **aGgb80L0ws** 的 XAuth 用户。

然后，在远程 IKE 网关配置中对 IP 2.2.2.2 处的对等方引用该用户。将远程网关命名为 “**gw1**”，为 “阶段 1” 协商指定 “主” 模式和方案 **pre-g2-3des-sha**，并使用预共享密钥 “**netscreen1**”。将 VPN 通道命名为 “**vpn1**”，为 “阶段 2” 协商指定 “**Compatible (兼容)**” 组的方案。选择 **Untrust** 区段接口 **ethernet3** 作为外向接口。

WebUI

1. XAuth 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: x1

Status: Enable

XAuth User: (选择)

User Password: iDa84rNk

Confirm Password: iDa84rNk

2. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw1

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Outgoing Interface: ethernet3

> **Advanced:** 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页：

Security Level: Custom: (选择)
 Phase 1 Proposal: pre-g2-3des-sha
 Mode (Initiator): Main (ID Protection)
 XAuth Server: (选择)
 Local Authentication: (选择)
 User: (选择), x1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1
 Security Level: Compatible
 Remote Gateway Tunnel: gw1

CLI

1. XAuth 用户

```
set user x1 password aGgb80L0ws
set user x1 type xauth
unset user x1 type auth17
```

2. VPN

```
set ike gate gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
netscreen1 proposal pre-g2-3des-sha
set ike gateway gw1 xauth server Local user x1
set vpn vpn1 gateway gw1 sec-level compatible
save
```

17. CLI 命令 **set user name_str password pswd_str** 将创建一个 **auth** 用户。要创建仅为 XAuth 类型的用户，必须将该用户定义为 XAuth 用户 (**set user name_str type xauth**)，然后删除 **auth** 用户定义 (**unset user name_str type auth**)。

范例 : XAuth 认证 (本地用户组)

本例中，将在本地数据库上创建一个名为 **xa-grp1** 的用户组，并添加上例第 456 页上的“范例 : XAuth 认证 (本地用户)”中创建的 XAuth 用户 “**x1**”。将该用户添加到组中时，它自动成为 XAuth 用户组。

然后，在远程 IKE 网关配置中对 IP 2.2.2.2 处的对等方引用该组。将远程网关命名为 “**gw2**”，为 “阶段 1” 协商指定 Main mode (主模式) 和方案 **pre-g2-3des-sha**，并使用预共享密钥 “**netscreen2**”。将 VPN 通道命名为 “**vpn2**”，为 “阶段 2” 协商指定 “Compatible” 组的方案。选择 Untrust 区段接口 **ethernet3** 作为外向接口。

WebUI

1. XAuth 用户组

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **xa-grp1**，执行以下操作，然后单击 **OK**:

选择 **x1**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw2

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen2

Outgoing Interface: ethernet3

> **Advanced**: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页：

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

Local Authentication: (选择)

User Group: (选择), xa-grp1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn2

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (选择), gw2

CLI

1. XAuth 用户组

```
set user-group xa-grp1 location local
set user-group xa-grp1 user x1
```

2. VPN

```
set ike gate gw2 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
netscreen2 proposal pre-g2-3des-sha
set ike gateway gw2 xauth server Local user-group xa-grp1
set vpn vpn2 gateway gw2 sec-level compatible
save
```

范例 : XAuth 认证 (外部用户)

在本例中，将引用先前加载到外部 SecurID auth 服务器上的 XAuth 用户，用户名为“xa-1”，密码为 iNWw10bd01。本例使用的 SecurID auth 服务器配置与第 407 页上的“范例 : SecurID Auth 服务器”中定义的大致相同，但此处将帐户类型定义为 XAuth。

在远程 IKE 网关配置中对 IP 2.2.2.2 处的对等方引用 XAuth 用户 xa-1。将远程网关命名为“gw3”，为“阶段 1”协商指定 Main mode (主模式) 和方案 pre-g2-3des-sha，并使用预共享密钥“netscreen3”。将 VPN 通道命名为“vpn3”，为“阶段 2”协商指定方案 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为外向接口。

WebUI

1. 外部 SecurID Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: securid1

IP/Domain Name: 10.20.2.100

Backup1: 10.20.2.110

Timeout: 60

Account Type: XAuth

SecurID: (选择)

Client Retries: 3

Client Timeout: 10 seconds

Authentication Port: 15000

Encryption Type: DES

User Duress: No

2. XAuth 用户

在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户 “xa-1”。

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw3

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen3

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页：

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

External Authentication: (选择), securid1

User: (选择)

Name: xa-1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn3

Security Level: Compatible

Remote Gateway Tunnel:

Predefined: (选择), gw3

CLI

1. 外部 SecurID Auth 服务器

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type xauth
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. XAuth 用户

在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户 “xa-1”。

3. VPN

```
set ike gate gw3 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
  netscreen3 proposal pre-g2-3des-sha
set ike gateway gw3 xauth server securid1 user xa-1
set vpn vpn3 gateway gw3 sec-level compatible
save
```

范例 : XAuth 认证 (外部用户组)

在本例中，将配置名为 “radius1”¹⁸ 的外部 RADIUS auth 服务器，定义名为 “xa-grp2” 的外部 auth 用户组。在下列两个位置定义外部 XAuth 用户组 xa-grp2:

1. 外部 RADIUS auth 服务器 “radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 XAuth 用户装入 XAuth 用户组 “xa-grp2” 中，而将 NetScreen 设备上的组保留为空白。该组中的成员为远程站点处的分销商，需要在企业 LAN 中访问 FTP 服务器。在 区段通讯簿中，为具有 IP 地址 10.2.2.0/24、名为 “reseller1” 的远程站点添加一个条目。也可在 Trust 区段通讯簿中，为 IP 地址 10.1.1.5/32 的 FTP 服务器 “rsl-srv1” 输入一个地址。

将 VPN 通道配置为 2.2.2.2，以便对用户组 xa-grp2 中的 XAuth 用户进行认证。将远程网关命名为 “gw4”，为 “阶段 1” 协商指定 Main mode (主模式) 和方案 pre-g2-3des-sha，并使用预共享密钥 “netscreen4”。将 VPN 通道命名为 “vpn4”，为 “阶段 2” 协商指定 “Compatible” 组的方案。选择 Untrust 区段接口 ethernet3 作为外向接口。

最后，设置并创建一个策略，允许 FTP 信息流从 区段中的 reseller1 通过 vpn4 流向 Trust 区段中的 rsl-srv1。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：有关 NetScreen 词典文件的信息，请参阅第 397 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。

2. 在外部 auth 服务器 “radius1” 上输入 auth 用户组 “xa-grp2”，然后在其中装入 XAuth 用户帐户。

18. RADIUS auth 服务器的配置与第 404 页上的 “范例 : RADIUS Auth 服务器” 中大致相同，但本例中仅指定 “xauth” 作为用户帐户类型。

WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: radius1
IP/Domain Name: 10.20.1.100
Backup1: 10.20.1.110
Backup2: 10.20.1.120
Timeout: 30
Account Type: XAuth
RADIUS: (选择)
RADIUS Port: 4500
Shared Secret: A56htYY97kl

2. 外部用户组

Objects > Users > External Groups > New: 输入以下内容，然后单击 **OK**:

Group Name: xa-grp2
Group Type: XAuth

3. 地址

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

Address Name: reseller1
IP Address/Domain Name:
IP/Netmask: (选择), 10.2.2.0/24
Zone: Untrust

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

Address Name: rsl-svr1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

4. XAuth 用户

在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户 “xa-1”。

5. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: gw4

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen4

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页：

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

XAuth Server: (选择)

External Authentication: (选择), securid1

User Group: (选择)

Name: xa-grp2

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn4

Security Level: Compatible

Remote Gateway:

Predefined: (选择), gw4

6. 策略

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), reseller1

Destination Address:

Address Book Entry: (选择), rsl-svr1

Service: FTP-Get

Action: Tunnel

Tunnel VPN: vpn4

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. Auth 服务器

```
set auth-server radius1 type radius
set auth-server radius1 account-type xauth
set auth-server radius1 server-name 10.20.1.100
set auth-server radius1 backup1 10.20.1.110
set auth-server radius1 backup2 10.20.1.120
set auth-server radius1 timeout 30
set auth-server radius1 radius port 4500
set auth-server radius1 radius secret A56htYY97kl
```

2. 外部用户组

```
set user-group xa-grp2 location external
set user-group xa-grp2 type xauth
```

3. 地址

```
set address untrust reseller1 10.2.2.0/24
set address trust rsl-svr1 10.1.1.5/32
```

4. VPN

```
set ike gate gw4 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
netscreen4 proposal pre-g2-3des-sha
set ike gateway gw4 xauth server radius1 user-group xa-grp2
set vpn vpn4 gateway gw4 sec-level compatible
```

5. 策略

```
set policy top from untrust to trust reseller1 rsl-svr1 ftp-get tunnel vpn vpn4
save
```

范例 : XAuth 认证和地址分配 (本地用户组)

在本例中，为本地数据库上存储的 IKE/XAuth 用户组建立认证和 IP、DNS 服务器及 WINS 服务器 IP 地址分配¹⁹。IKE/XAuth 用户以拨号 VPN 连接方式尝试连接 NetScreen 设备时，NetScreen 设备会在“阶段 1”协商期间使用 IKE ID 和 RSA 证书对用户 (即客户端设备) 进行认证。然后，NetScreen 设备使用用户名和密码对 XAuth 用户 (即使用设备的个体) 进行认证，并在“阶段 1”和“阶段 2”协商之间分配 IP、DNS 服务器和 WINS 服务器 IP 地址。

创建本地用户组 `ixa-grp1`。然后定义两个名称分别为“`ixa-u1`” (密码 : `ccF1m84s`) 和“`ixa-u2`” (密码 : `C113g1tw`) 的 IKE/XAuth 用户，将它们添加到组中，从而将组类型定义为 IKE/XAuth。(本例中将不向组中另外添加其它 IKE/XAuth 用户。)

创建名为 `xa-pool1` 的 DIP 池，地址范围从 10.2.2.1 到 10.2.2.100。NetScreen 设备为 XAuth 用户分配 IP 地址时，即从此地址池中提取地址。

注意：DIP 池与 XAuth 用户发送信息流的目标区段必须具有不同的地址空间，以避免出现路由选择问题和地址分配重复。

¹⁹ 也可使用外部 RADIUS auth 服务器对 XAuth 用户进行认证和地址分配。但外部 SecurID 或 LDAP auth 服务器只能用于 XAuth 认证 (不能进行地址分配)。对于 IKE 用户认证，只能使用本地数据库。

配置以下 XAuth 缺省设置：

- 将 XAUTH 地址超时设置为 480 分钟。
- 选择本地数据库作为缺省 auth 服务器。
- 启用 CHAP (质询握手认证协议)， NetScreen 设备根据此协议向远程客户端发送一个质询 (加密密钥)，该客户端用户使用此密钥对其登录名和密码进行加密。
- 选择 xa-pool1 作为缺省 DIP 池。
- 将主、辅 DNS 服务器 IP 地址分别定义为 10.1.1.150 和 10.1.1.151。
- 将主、辅 WINS 服务器 IP 地址分别定义为 10.1.1.160 和 10.1.1.161。

引用用户组 **ixa-grp1** 并使用缺省 XAuth auth 服务器设置，配置名为 “**ixa-gw1**” 的 IKE 网关。然后，配置名为 “**ixa-tun1**” 的 VPN 通道和允许信息流通过 VPN 通道 **ixa-tun1** 从 **ixa-grp1** 流向 Trust 区段 (IP 地址为 10.1.1.0/24) 的策略。

WebUI

1. IKE/XAuth 用户和用户组

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: **ixa-u1**

Status: **Enable**

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: **AUTO**

IKE Identity: **u1@ns.com**

XAuth User: (选择)

User Password: **ccF1m84s**

Confirm Password: **ccF1m84s**

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: ixa-u2

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE ID Type: AUTO

IKE Identity: u2@ns.com

XAuth User: (选择)

User Password: C113g1tw

Confirm Password: C113g1tw

Objects > Users > Local Groups > New: 在 Group Name 字段中输入 **ixa-grp1**，执行以下操作，然后单击 **OK**:

选择 **ixa-u1**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **ixa-u2**，并使用 << 按钮将其从 Available Members 栏移动到 Group Members 栏中。

2. IP 池

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: xa-pool1

Start IP: 10.2.2.1

End IP: 10.2.2.100

3. 缺省 XAuth Auth 服务器

VPNs > AutoKey Advanced > XAuth Settings: 输入以下内容, 然后单击 **Apply**:

Reserve Private IP for XAuth User: 480 Minutes

Default Authentication Server: Local

Query Client Settings on Default Server: (清除)

CHAP: (选择)

IP Pool Name: xa-pool1

DNS Primary Server IP: 10.1.1.150

DNS Secondary Server IP: 10.1.1.151

WINS Primary Server IP: 10.1.1.160

WINS Secondary Server IP: 10.1.1.161

4. 地址

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

Address Name: Trust_zone

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

5. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容, 然后单击 **OK**:

Gateway Name: ixa-gw1

Security Level: Custom

Remote Gateway Type:

Dialup User Group: (选择)

Group: ixa-grp1

> **Advanced**: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页：

Phase 1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Aggressive

Outgoing Interface: ethernet3

XAuth Server: (选择)

Use Default: (选择)

User Group: (选择), ixa-grp1

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: ixa-vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (选择), ixa-gw1

6. 策略

Policies > (From: Untrust; To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), Trust_zone

Service: ANY

Action: Tunnel

Tunnel VPN: ixa-vpn1

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. IKE/XAuth 用户和用户组

```
set user-group ixa-grp1 location local
set user ixa-u1 type ike xauth
set user ixa-u1 ike-id u-fqdn u1@ns.com
set user ixa-u1 password ccF1m84s
unset user ixa-u1 type auth
set user ixa-u2 type ike xauth
set user ixa-u2 ike-id u-fqdn u2@ns.com
set user ixa-u2 password C113g1tw
unset user ixa-u2 type auth
```

2. IP 池

```
set ippool xa-pool1 10.2.2.1 10.2.2.100
```

3. 缺省 XAuth Auth 服务器

```
set xauth lifetime 480
set xauth default auth server Local chap
set xauth default ippool xa-pool1
set xauth default dns1 10.1.1.150
set xauth default dns2 10.1.1.151
set xauth default wins1 10.1.1.160
set xauth default wins2 10.1.1.161
```

4. 地址

```
set address trust Trust_zone 10.1.1.0/24
```

5. VPN

```
set ike gateway ixa-gw1 dialup ixa-grp1 aggressive outgoing-interface ethernet3
proposal rsa-g2-3des-sha
set ike gateway ixa-gw1 xauth server Local user-group ixa-grp1
set vpn ixa-vpn1 gateway ixa-gw1 sec-level compatible
```

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" Trust_zone any tunnel vpn
ixa-vpn1
save
```

XAuth 客户端

XAuth 客户端是一个远程用户或设备，它通过“自动密钥 IKE”VPN 通道与 NetScreen 服务器相连。NetScreen 设备可以作为 XAuth 客户端，响应远程 XAuth 服务器的认证请求。“阶段 1”协商完成后，远程 XAuth 服务器向 NetScreen 设备发送登录提示。如果作为 XAuth 客户端的 NetScreen 设备使用正确的用户名和密码成功登录，则“阶段 2”协商开始。

要将 NetScreen 设备配置为 XAuth 客户端，必须指定下列内容：

- IKE 网关名
- XAuth 用户名和密码

可以配置以下类型的 XAuth 认证：

- Any — 允许“质询握手认证协议”(CHAP)或“密码认证协议”(PAP)
- CHAP — 仅允许 CHAP

范例 : NetScreen 设备作为 XAuth 客户端

在本例中, 首先配置 IP 地址为 2.2.2.2 的远程 IKE 网关 *gw1*。指定标准安全级别, 并使用预共享密钥 *netscreen1*。然后, 为用户名为 *beluga9*、密码为 *1234567* 的 IKE 网关配置 XAuth 客户端。还需要对该客户端进行 CHAP 认证。

WebUI

VPN > AutoKey Advanced > Gateway > New: 输入以下内容, 然后单击 **OK**:

Gateway Name: gw1

Security Level: Standard (选择)

Remote Gateway Type:

Static IP Address: (选择), Address/Hostname: 2.2.2.2

Preshared Key: netscreen1

Outgoing Interface: Untrust

> Advanced: 输入以下高级设置, 然后单击 **Return**, 返回基本 Gateway 配置页:

XAuth Client: (选择)

User Name: beluga9

Password: 1234567

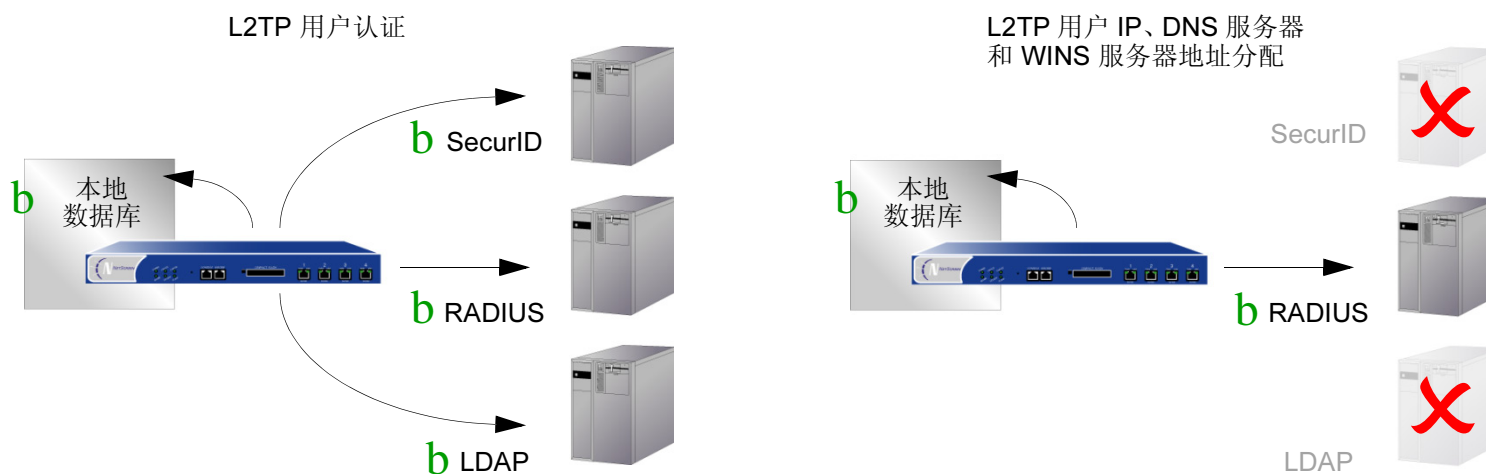
Allowed Authentication Type: (选择), CHAP Only

CLI

```
set ike gateway gw1 ip 2.2.2.2 Main outgoing-interface untrust preshare
netscreen1 sec-level standard
set ike gateway gw1 xauth client chap username beluga1 password 1234567
save
```

L2TP 用户和用户组

“第 2 层通道协议” (L2TP) 提供一种认证远程用户和分配 IP、DNS 服务器与 WINS 服务器地址的方法。可对 NetScreen 设备进行配置，以便使用本地数据库或外部 auth 服务器认证 L2TP 用户。要对 IP、DNS 服务器及 WINS 服务器地址进行分配，可相应配置 NetScreen 设备，以使用本地数据库或 RADIUS 服务器 (加载有 NetScreen 词典文件 — 请参阅第 397 页上的“NetScreen 词典文件”)。



甚至可使用 auth 服务器的组合，不同服务器分别对应 L2TP 两个方面之一。例如，可使用 SecurID 服务器对 L2TP 用户进行认证，但从本地数据库进行地址分配。下例说明如何应用两个 auth 服务器分别处理 L2TP 的两方面需求。有关其它范例以及 L2TP 的详细解释，请参阅第 5-269 页上的“L2TP”。

范例：本地和外部 L2TP Auth 服务器

在本例中，将设置外部 SecurID auth 服务器对 L2TP 用户进行认证，并使用本地数据库为 L2TP 用户分配 IP、DNS 服务器和 WINS 服务器地址。

外部 SecurID auth 服务器为 securid1。Auth 服务器的配置与第 407 页上的“范例：SecurID Auth 服务器”中基本相同，只是此处帐户类型为 L2TP。SecurID auth 服务器参数如下：

- Name: securid1
- IP Address: 10.20.2.100
- Backup1 IP Address: 10.20.2.110
- Port: 15000
- Encryption: DES
- Client Retries: 3
- Client Timeout: 10 seconds
- Idle Timeout: 60 minutes
- Account Type: L2TP

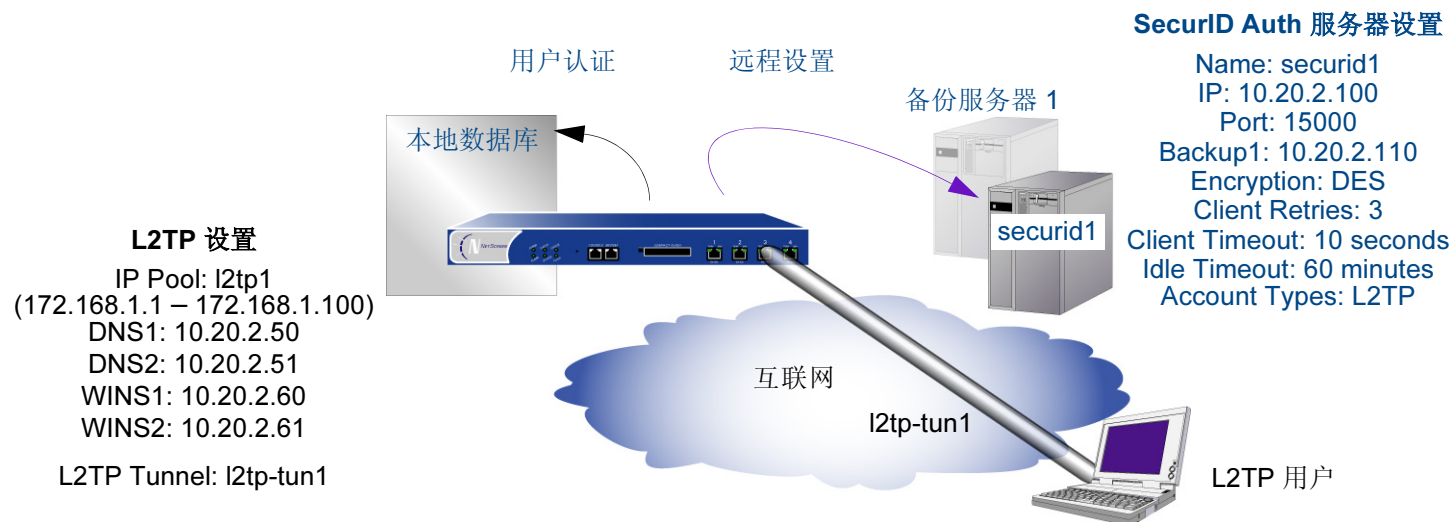
L2TP 缺省设置如下：

- IP Pool: l2tp1 (172.168.1.1 – 172.168.1.100)
- DNS Primary Server IP: 10.20.2.50
- DNS Secondary Server IP: 10.20.2.51
- PPP Authentication: CHAP
- WINS Primary Server IP: 10.20.2.60
- WINS Primary Server IP: 10.20.2.61

以上述设置对 NetScreen 设备进行配置后，创建名为 “l2tp-tun1” 的 L2TP 通道，它引用 securid1 进行认证，并使用缺省设置进行地址分配。

此外，还必须如上所示设置 SecurID 服务器，并在其中装入 L2TP 用户。

注意：一个只有 L2TP 的配置并不安全。为了对 L2TP 通道进行保护，建议将其与 IPsec 通道（必须处于 Transport 模式）结合使用，如第 5-286 页上的“范例：配置 IPsec 上的 L2TP”中所示。



WebUI

1. Auth 服务器

Configuration > Auth > Servers > New: 输入以下内容，然后单击 **OK**:

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: L2TP
SecurID: (选择)
Client Retries: 3
Client Timeout: 10 seconds
Authentication Port: 15000
Encryption Type: DES
Use Duress: No

2. IP 池

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: l2tp1

Start IP: 172.168.1.1

End IP: 172.168.1.100

3. L2TP 缺省设置

VPNs > L2TP > Default Settings: 输入以下内容，然后单击 **Apply**:

Default Authentication Server: Local

IP Pool Name: l2tp1

PPP Authentication: CHAP

DNS Primary Server IP: 10.20.2.50

DNS Secondary Server IP: 10.20.2.51

WINS Primary Server IP: 10.20.2.60

WINS Secondary Server IP: 10.20.2.61

4. L2TP 通道

VPNs > L2TP > Tunnel > New: 输入以下内容，然后单击 **OK**:

Name: l2tp-tun1

Use Custom Settings: (选择)

Authentication Server: securid1

Query Remote Settings: (清除)

Dialup User: (选择), Allow Any

CLI

1. Auth 服务器

```
set auth-server securid1 type securid
set auth-server securid1 server-name 10.20.2.100
set auth-server securid1 backup1 10.20.2.110
set auth-server securid1 timeout 60
set auth-server securid1 account-type l2tp
set auth-server securid1 securid retries 3
set auth-server securid1 securid timeout 10
set auth-server securid1 securid auth-port 15000
set auth-server securid1 securid encr 1
set auth-server securid1 securid duress 0
```

2. IP 池

```
set ippool l2tp1 172.168.1.1 172.168.1.100
```

3. L2TP 缺省设置

```
set l2tp default auth server Local
set l2tp default ippool l2tp1
set l2tp default ppp-auth chap
set l2tp dns1 10.20.2.50
set l2tp dns1 10.20.2.51
set l2tp wins1 10.20.2.60
set l2tp wins2 10.20.2.61
```

4. L2TP 通道

```
set l2tp l2tp-tun1
set l2tp l2tp-tun1 auth server securid1
save
```

Admin 用户

Admin 用户是 NetScreen 设备的管理员。共有五种 admin 用户：

- 根 admin
- 根级读 / 写 admin
- 根级只读 admin
- Vsys admin
- Vsys 只读 admin

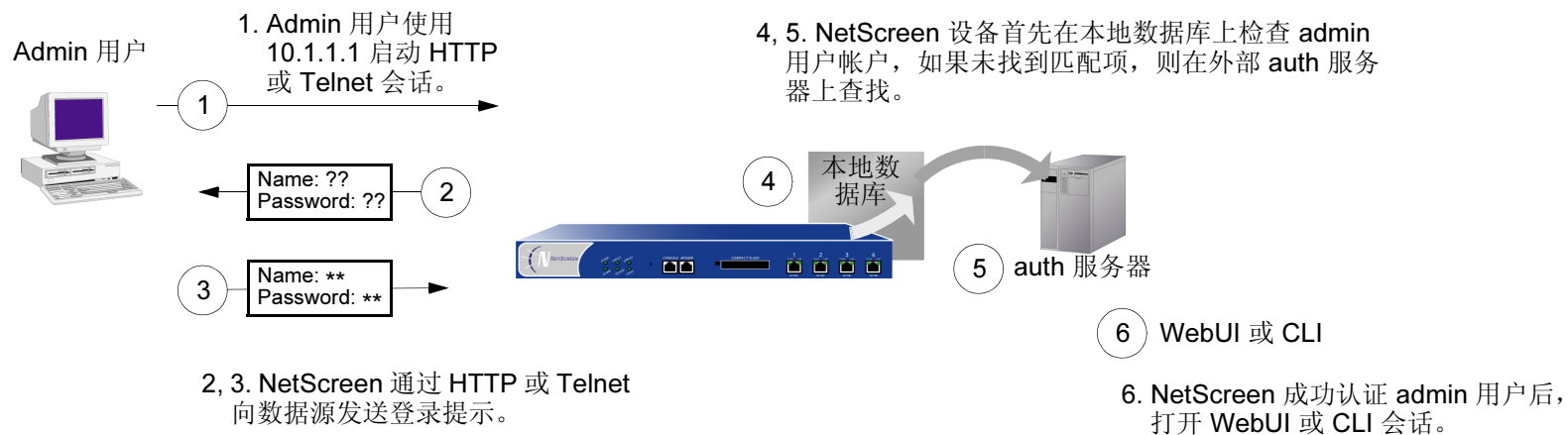
注意：有关各类型 admin 用户权限的信息，以及创建、修改和删除 admin 用户的范例，请参阅第 3-1 页上的“管理”。

尽管 NetScreen 设备根用户的配置文件必须存储在本地数据库中，但可将具有读 / 写和只读权限的 vsys 用户和根级 admin 用户存储在本地数据库或外部 auth 服务器中。

如果将 admin 用户帐户存储在外部 RADIUS auth 服务器上，并在 auth 服务器上加载 NetScreen 词典文件 (请参阅第 397 页上的“NetScreen 词典文件”)，则可选择查询服务器上定义的 admin 权限。此外，您也可以指定某权限级别，以全局方式应用于该 auth 服务器上存储的所有 admin 用户。可指定读 / 写或只读权限。如果将 admin 用户存储在外部 SecurID 或 LDAP auth 服务器或者未加载 NetScreen 词典文件的 RADIUS 服务器上，则不能在 auth 服务器上定义它们的权限属性。因此，必须在 NetScreen 设备上为它们指定权限级别。

如果在 NetScreen 设备上设置：	且 RADIUS 服务器已加载 NetScreen 词典文件，则：	且 SecurID、LDAP 或 RADIUS 服务器未加载 NetScreen 词典文件，则：
从 RADIUS 服务器获取权限	指定适当权限	根级或 vsys 级 admin 登录失败
为外部 admin 指定读 / 写权限	指定根级或 vsys 级读 / 写权限	指定根级读 / 写权限 Vsys admin 登录失败
为外部 admin 指定只读权限	指定根级或 vsys 级只读权限	指定根级只读权限 Vsys admin 登录失败

admin 认证过程如下图所示：



多类型用户

可将 **auth**、**IKE**、**L2TP**、**XAuth** 用户组合在一起，创建下列组合对象并存储在本地数据库上：

- **Auth/IKE** 用户
- **Auth/L2TP** 用户
- **Auth/IKE/L2TP** 用户
- **IKE/L2TP** 用户
- **Auth/XAuth** 用户
- **Auth/IKE/XAuth** 用户
- **IKE/XAuth** 用户
- **L2TP/XAuth** 用户
- **IKE/L2TP/XAuth** 用户
- **Auth/IKE/L2TP/XAuth** 用户

尽管在本地数据库上定义多类型用户帐户时，可以创建上述所有组合形式，但在创建之前仍须考虑以下事项：

- 将 **IKE** 用户类型与其它任何用户类型组合后，会限制其扩展的潜在能力。必须将 **IKE** 用户帐户存储在本地数据库上。如果创建 **auth/IKE**、**IKE/L2TP** 和 **IKE/XAuth** 用户帐户，而之后用户数超出本地数据库容量时，您就无法将这些帐户重新置于外部 **auth** 服务器中。如果将 **IKE** 用户帐户与其它类型帐户分离，则在必要时，您可以灵活地将非 **IKE** 用户帐户移动到外部 **auth** 服务器中。
- **L2TP** 和 **XAuth** 提供相同的服务：远程用户认证以及 **IP**、**DNS** 服务器与 **WINS** 服务器地址分配。建议不要对 **IPSec** 上的 **L2TP** 通道同时使用 **L2TP** 和 **XAuth**。不仅因为这两种协议的作用相同，而且在“阶段 2”**IKE** 协商完成、**L2TP** 协商开始后，**L2TP** 地址分配将会覆盖 **XAuth** 地址分配。
- 如果将 **auth/L2TP** 或 **auth/XAuth** 组合在一起，在本地数据库上创建多类型用户帐户，则两种类型用户登录时必须使用相同的用户名和密码。

尽管创建一个多类型用户帐户较之将用户类型分为两个单独帐户操作起来更为方便，但后者却可以为您带来更高的安全性。例如，可将 **auth** 用户帐户存储在外部 **auth** 服务器上，将 **XAuth** 用户帐户存储在本地数据库上。然后，可以为每个帐户指定不同的登录用户名和密码，并在 **IKE** 网关配置中引用 **XAuth** 用户，而在策略配置中引用 **auth** 用户。拨号 **VPN** 用户必须经过两次认证，认证时可以使用两个完全不同的用户名和密码。

组表达式

组表达式是可以在策略中用来使认证要求实现条件化的语句。组表达式可以将用户、用户组或其它组表达式作为认证的可选条件 (“a” OR “b”) 或者作为认证的必需条件 (“a” AND “b”) 组合起来, 也可以将某个用户、用户组或另一组表达式排除在外 (NOT “c”)。

注意: 虽然您在 NetScreen 设备上定义组表达式 (并存储在本地数据库上), 但组表达式中引用的用户和用户组必须存储在外部 RADIUS 服务器上。RADIUS 服务器允许一个用户属于多个用户组。但本地数据库不允许这样。

组表达式使用三个运算符 OR、AND 和 NOT。表达式中用 OR、AND 和 NOT 关联起来的对象可以是一个 auth 用户、auth 用户组或先前定义的组表达式。

用户

OR – 如果策略的认证情况指定用户为 “a” OR “b”, 则当该用户为其中一个时, NetScreen 设备会认证他 / 她。

AND – 组表达式中使用 AND 运算符时, 要求两个表达式对象中至少有一个是用户组或组表达式。(要求某个用户为用户 “a” AND 用户 “b” 是不符合逻辑的)。如果策略的认证情况要求用户为 “a” AND 组 “b” 中的成员, 则只有当满足这两个条件时, NetScreen 设备才会认证该用户。

NOT – 如果策略的认证情况指定用户为除用户 “c” 外的任何其它用户 (NOT “c”), 则只要用户不是 “c”, NetScreen 设备就会认证他 / 她。

用户组

OR – 如果策略的认证情况指定用户属于组 “a” OR 组 “b”, 则当该用户属于任一组时, NetScreen 设备会认证他 / 她。

AND – 如果策略的认证情况要求用户属于组 “a” AND 组 “b”, 则只有当用户同时属于两组时, NetScreen 设备才会认证他 / 她。

NOT – 如果策略的认证情况指定用户属于除组 “c” 外的任意组 (NOT “c”), 则当用户不属于此组时, NetScreen 设备认证他 / 她。

组表达式

OR – 如果策略的认证情况指定用户符合组表达式 “a” OR 组表达式 “b” 的描述，则只有当其中某一组表达式适用于该用户时， **NetScreen** 设备才会认证他 / 她。

AND – 如果策略的认证情况指定用户应符合组表达式 “a” AND 组表达式 “b” 的描述，则只有当两个表达式都适用于该用户时， **NetScreen** 设备才会认证他 / 她。

NOT – 如果策略的认证情况指定用户应不符合组表达式 “c” 的描述 (NOT “c”)，则只有当该用户不符合此组表达式时， **NetScreen** 设备才会认证他 / 她。

范例：组表达式 (AND)

在本例中，将创建一个表述为 “sales AND marketing” 的组表达式 “s+m”。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建了 auth 用户组 “sales” 和 “marketing”，并在其中留置了用户。(有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 404 页上的“范例：RADIUS Auth 服务器”。) 然后，在内部区段策略²⁰中使用该组表达式，策略中的认证部分要求用户必须是这两个用户组的成员，才能访问名为 “project1” 的服务器 (10.1.1.70) 上的机密内容。

WebUI

1. 地址

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

Address Name: project1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.70/32

Zone: Trust

2. 组表达式

Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

Group Expression: s+m

AND: (选择), sales AND marketing

20. 要使内部区段策略正常工作，源地址和目标地址必须位于不同的子网中，这些子网通过绑定到同一区段的接口连接到 NetScreen 设备。除 NetScreen 设备外，其它任何路由设备都不能在两个地址间转发信息流。有关内部区段策略的详细信息，请参阅第 213 页上的“策略”。

3. 策略

Policies > (From: Trust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Source Address

Address Book Entry: (选择), Any

Destination Address

Address Book Entry: (选择), project1

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

Group Expression: (选择), External Group Expression - s+m

CLI

1. 地址

```
set address trust project1 10.1.1.70/32
```

2. 组表达式

```
set group-expression s+m sales and marketing
```

3. 策略

```
set policy top from trust to trust any project1 any permit auth server radius1
  group-expression s+m
save
```

范例：组表达式 (OR)

在本例中，将创建一个表述为“amy OR basil”的组表达式“a/b”。您先前已在名为“radius1”的外部 RADIUS auth 服务器上创建了 auth 用户帐户“amy”和“basil”。(有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 404 页上的“范例：RADIUS Auth 服务器”。)然后在从 Trust 区段到 DMZ 的策略中使用该组表达式。策略的认证部分要求用户必须为 amy 或 basil，才能访问 210.1.1.70 处名为“web1”的 Web 服务器。

WebUI

1. 地址

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

Address Name: web1

IP Address/Domain Name

IP/Netmask: (选择), 210.1.1.70/32

Zone: DMZ

2. 组表达式

Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

Group Expression: a/b

OR: (选择), amy OR basil

3. 策略

Policies > (From: Trust, To: DMZ) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), web1

Service: ANY

Action: Permit

Position at Top: (选择)

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: radius1

Group Expression: (选择), External Group Expression - a/b

CLI

1. 地址

```
set address trust project1 210.1.1.70/32
```

2. 组表达式

```
set group-expression a/b any or basil
```

3. 策略

```
set policy top from trust to dmz any web1 any permit auth server radius1
  group-expression a/b
save
```

范例 : 组表达式 (NOT)

在本例中，将创建一个表述为 “NOT temp” 的组表达式 “-temp”。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建本地 auth 用户组 “temp”。(有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 404 页上的 “范例 : RADIUS Auth 服务器”。) 然后，在从 Trust 区段到 Untrust 区段的策略中使用该组表达式，该策略允许除临时合同工以外的所有专职雇员访问互联网。策略的认证部分要求使 Trust 区段中除 “temp” 中的用户而外的所有人员通过认证，拒绝 “temp” 中的用户访问 Untrust 区段。

WebUI

1. 组表达式

Objects > Group Expressions > New: 输入以下内容，然后单击 **OK**:

Group Expression: -temp

OR: (选择), NOT temp

2. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Authentication: (选择)

Auth Server: (选择)

Use: Local

Group Expression: (选择), External Group Expression - -temp

CLI

1. 组表达式

```
set group-expression -temp not temp
```

2. 策略

```
set policy top from trust to untrust any any any permit auth server radius1  
    group-expression -temp  
save
```

标题自定义

标题是指在以下类型登录期间在屏幕的下列位置出现的消息：

- **Admin** 用户连接登录到 **NetScreen** 设备时，在 **Telnet** 或控制台显示器的顶部显示
- **Auth** 用户成功登录到 **WebAuth** 地址后，在 **Web** 浏览器屏幕的顶部显示
- 对于 **auth** 用户，在 **Telnet**、**FTP** 或 **HTTP** 的登录提示、成功消息和失败消息上显示

除控制台登录标题外，所有标题都具有缺省消息。您可以自定义出现在标题上的消息，使其更适合使用 **NetScreen** 设备的网络环境。

范例：自定义 WebAuth 标题

在本例中，将更改通过 **WebAuth** 成功登录后出现在 **Web** 浏览器中的消息，用以指示 **auth** 用户已成功通过认证。新消息为 “**Authentication approved**”。

WebUI

Configuration > Banners > WebAuth: 在 **Success Banner** 字段中，键入 **Authentication approved**，然后单击 **Apply**。

CLI

```
set webauth banner success "Authentication approved"  
save
```

信息流整形

本章论述在不牺牲所有用户的网络连接质量及可用性的情况下，使用 **NetScreen** 设备来管理有限带宽的各种方法。

讨论的主题包括：

- 第 494 页上的 “应用信息流整形”
 - 第 494 页上的 “在策略级管理带宽”
- 第 501 页上的 “设置服务优先级”

应用信息流整形

信息流整形是指为接口上的每一位用户和应用程序分配适当的网络带宽数量。适当的带宽数量指在保证服务质量 (QoS) 的前提下具成本效益的载流容量。通过创建策略并将适当的速率控制应用到流经 NetScreen 设备的每一种信息流类别，您可使用 NetScreen 设备对信息流进行整形。

注意：只有那些目的区段有单个物理接口绑定到其中的策略才可以应用信息流整形。如果目的区段含有一个 (或多个) 子接口或者多个物理接口，则 NetScreen 不支持信息流整形。

在策略级管理带宽

要将信息流分类，可创建一个指定每类信息流的保障带宽数量、最大带宽及优先级等内容的策略。每一接口的物理带宽都分配给所有策略的保障带宽参数。如果有带宽剩余，可由其它信息流共享。换句话说，每个策略可得到其保障带宽并基于其优先级共享剩余的带宽 (直至达到其最大带宽规格的限制)。

信息流整形功能适用于所有策略的信息流。如果您关闭特定策略的信息流整形但其它策略的信息流整形仍然开启，则系统将对特定策略应用缺省信息流整形策略，使用的参数如下：

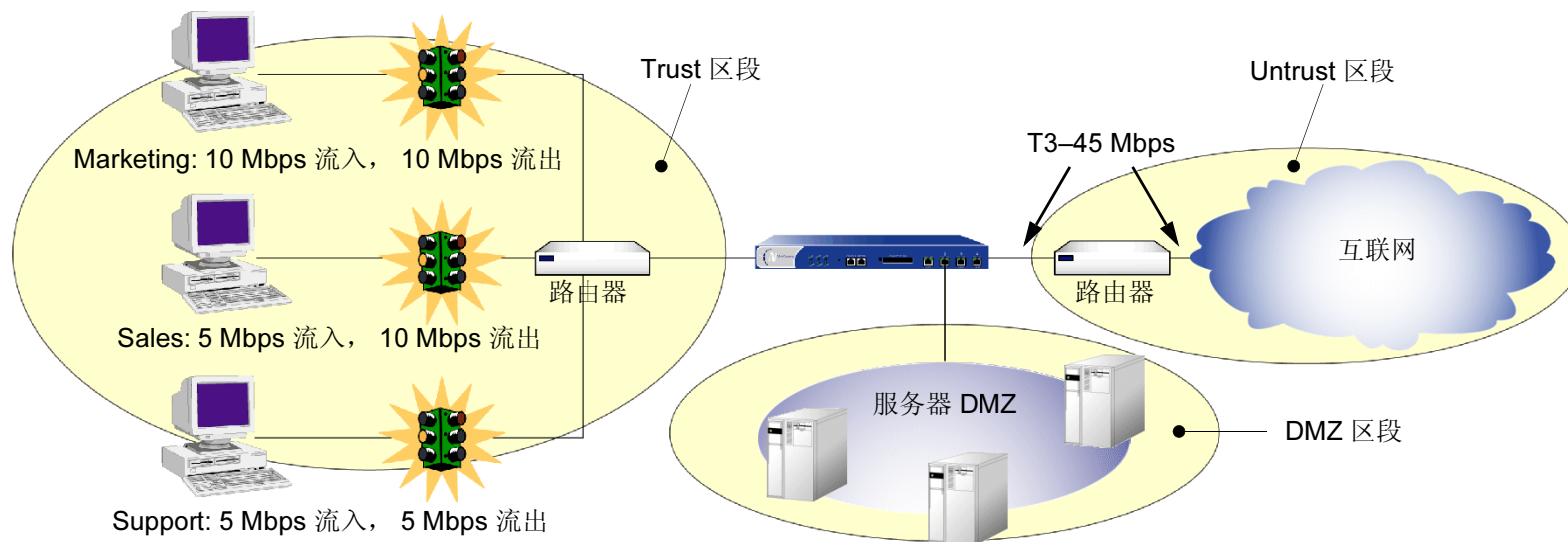
- 保障带宽为 0
- 最大带宽无限制
- 优先级为 7 (最低的优先级设置)¹

如果您不希望系统将此缺省信息流整形策略指派给已关闭其信息流整形的策略，则可通过 CLI 命令 **set traffic-shaping mode off** 关闭整个系统的信息流整形。可将信息流整形设置为自动：**set traffic-shaping mode auto**。这允许系统在策略需要时开启信息流整形，在策略不需要时将其关闭。

1. 您可启用 NetScreen 优先级到 DiffServ 码点标记系统的映射。有关“DS 码点标记”的详细信息，请参阅第 230 页上的“信息流整形”。

范例：信息流整形

在本例中，您需要在 T3 接口上划分 45Mbps 的带宽，其中该接口处于同一子网的三个部门之间。ethernet1 接口被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。



WebUI

1. 接口带宽

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **OK**:

Traffic Bandwidth: 45000²

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Traffic Bandwidth: 45000

2. 如果您未指定接口的带宽设置，NetScreen 将使用所有可用的物理带宽。

2. 策略带宽

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: Marketing Traffic Shaping

Source Address:

Address Book Entry: (选择), Marketing

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

VPN Tunnel: None³

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 15000

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: Sales Traffic Shaping Policy

Source Address:

Address Book Entry: (选择), Sales

Destination Address:

Address Book Entry: (选择), Any

Service: Any

3. 您也可在参考 VPN 通道的策略中启用信息流整形。

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 10000

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: Support Traffic Shaping Policy

Source Address:

Address Book Entry: (选择), Support

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Allow Incoming Access to Marketing

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Marketing

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Allow Incoming Access to Sales

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Sales

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 10000

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Allow Incoming Access to Support

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Support

Service: Any

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 5000

CLI

要通过策略启用信息流整形，请执行以下操作：

1. 接口带宽

```
set interface ethernet1 bandwidth 450004  
set interface ethernet3 bandwidth 45000
```

2. 策略带宽

```
set policy name "Marketing Traffic Shaping" from trust to untrust marketing any  
any permit traffic gbw 10000 priority 0 mbw 15000  
set policy name "Sales Traffic Shaping Policy" from trust to untrust sales any  
any permit traffic gbw 10000 priority 0 mbw 10000  
set policy name "Support Traffic Shaping Policy" from trust to untrust support  
any any permit traffic gbw 5000 priority 0 mbw 10000  
set policy name "Allow Incoming Access to Marketing" from untrust to trust any  
marketing any permit traffic gbw 10000 priority 0 mbw 10000  
set policy name "Allow Incoming Access to Sales" from untrust to trust any  
sales any permit traffic gbw 5000 priority 0 mbw 10000  
set policy name "Allow Incoming Access to Support" from untrust to trust any  
support any permit traffic gbw 5000 priority 0 mbw 5000  
save
```

4. 如果您未指定接口的带宽设置，NetScreen 将使用所有可用的物理带宽。

设置服务优先级

通过 NetScreen 设备上的信息流整形功能，可对未分配给保障带宽的或未使用的保障带宽执行优先级排列。优先级排列功能允许所有用户和应用程序在需要时都能够访问可用带宽，同时又确保重要的信息流可以通过，必要时可以能够以牺牲次要信息流的带宽为代价。通过排列功能，NetScreen 能够以八种不同的优先级排列对信息流进行缓冲。这八种排列为：

- High priority
- 2nd priority
- 3rd priority
- 4th priority
- 5th priority
- 6th priority
- 7th priority
- Low priority (缺省)

策略的优先级设置意味着未分配给其它策略的带宽基于高优先级在前和低优先级在后的原则进行了排列。具有相同优先级设置的策略将以轮询方式竞争带宽。NetScreen 设备首先处理具有较高优先级策略的所有信息流，然后再处理具有次优先级设置策略的信息流，依此类推，直至处理完所有的信息流请求。如果信息流请求超过可用带宽，则将丢弃优先级最低的信息流。

注意：应注意不要分配给接口超过其支持能力的带宽。策略配置过程本身不能避免创建不支持的策略配置。如果竞争策略的保障带宽超过接口上设置的信息流带宽，将有可能丢失数据。

如果您未分配任何保障带宽，则可使用优先级排列来管理网络的所有信息流。也就是说，必须在发送完全部高优先级信息流之后，才能发送 2nd priority 信息流，依此类推。只有在处理完其它所有信息流之后，NetScreen 设备才处理低优先级信息流。

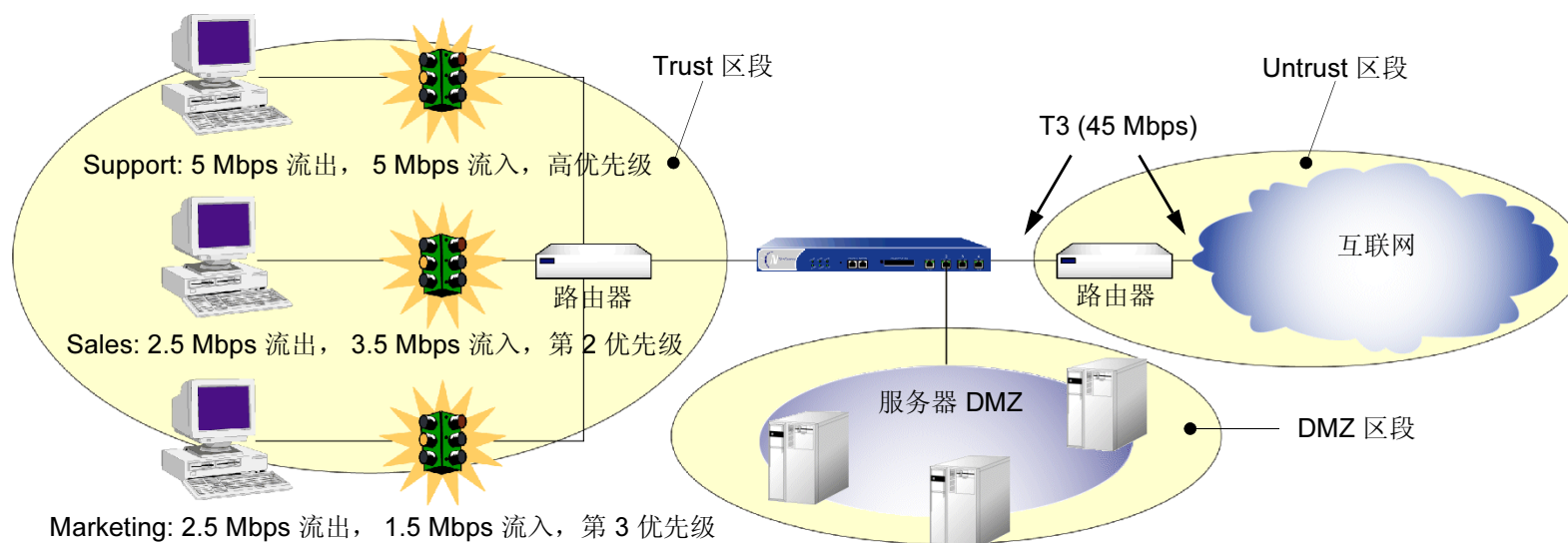
范例：优先级排列

在本例中，您需要为三个部门 (Support、Sales 和 Marketing) 配置保障带宽和最大带宽，如下所示：

	出站保证	入站保证	组合保证	优先级
Support	5*	5	10	高
Sales	2.5	3.5	6	2
Marketing	2.5	1.5	4	3
总计	10	10	20	

* 兆位每秒 (Mbps)

如果三个部门同时通过 NetScreen 防火墙发送和接收信息流，那么 NetScreen 设备必须分配 20 Mbps 的带宽以满足保证的策略要求。ethernet1 接口被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。



WebUI

1. 接口带宽

Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **OK**:

Traffic Bandwidth: 40000

Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Traffic Bandwidth: 40000

2. 策略带宽

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Name: Sup-out

Source Address:

Address Book Entry: (选择), Support

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

> **Advanced**: 输入以下内容, 然后单击 **Return**, 设置高级选项并返回基本配置页:

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 40000

Traffic Priority: High priority

DiffServ Codepoint Marking⁵: (选择)

5. 差异服务 (DS) 是在优先级层次结构中的某一位置标记 (或 “做记号”) 信息流的系统。DS 码点标记将 NetScreen 的策略优先级映射到 IP 封包包头 DS 字段中码点的前三位。有关 “DS 码点标记” 的详细信息, 请参阅第 230 页上的 “信息流整形”。

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: Sal-out

Source Address:

Address Book Entry: (选择), Sales

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 2500

Maximum Bandwidth: 40000

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: Enable

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:

Name: Mar-out

Source Address:

Address Book Entry: (选择), Marketing

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 2500

Maximum Bandwidth: 40000

Traffic Priority: 3rd priority

DiffServ Codepoint Marking: (选择)

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Sup-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Support

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 40000

Traffic Priority: High priority

DiffServ Codepoint Marking: (选择)

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Sal-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Sales

Service: Any

Action: Permit

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 3500

Maximum Bandwidth: 40000

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: (选择)

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:

Name: Mar-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Marketing

Service: Any

Action: Permit

> **Advanced:** 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Traffic Shaping: (选择)

Guaranteed Bandwidth: 1500

Maximum Bandwidth: 40000

Traffic Priority: 3rd priority

DiffServ Codepoint Marking: (选择)

CLI

1. 接口带宽

```
set interface ethernet1 bandwidth 40000
set interface ethernet3 bandwidth 40000
```

2. 策略带宽

```
set policy name sup-out from trust to untrust support any any permit traffic
  gbw 5000 priority 0 mbw 40000 dscp enable
set policy name sal-out from trust to untrust sales any any permit traffic gbw
  2500 priority 2 mbw 40000 dscp enable
set policy name mar-out from trust to untrust marketing any any permit traffic
  gbw 2500 priority 3 mbw 40000 dscp enable
set policy name sup-in from untrust to trust any support any permit traffic gbw
  5000 priority 0 mbw 40000 dscp enable
set policy name sal-in from untrust to trust any sales any permit traffic gbw
  3500 priority 2 mbw 40000 dscp enable
set policy name mar-in from untrust to trust any marketing any permit traffic
  gbw 1500 priority 3 mbw 40000 dscp enable
save
```


系统参数

本章重点介绍与建立系统参数有关的概念，这些参数会影响 NetScreen 安全设备的下列方面：

- 第 511 页上的“域名系统支持”
 - 第 512 页上的“DNS 查找”
 - 第 513 页上的“DNS 状态表”
- 第 516 页上的“DHCP”
 - 第 518 页上的“DHCP 服务器”
 - 第 526 页上的“DHCP 中继代理”
 - 第 532 页上的“DHCP 客户端”
 - 第 534 页上的“TCP/IP 设置传播”
- 第 537 页上的“PPPoE”
- 第 544 页上的“下载/上传设置和固件”
 - 第 544 页上的“保存和导入设置”
 - 第 546 页上的“上传和下载固件”
 - 第 547 页上的“配置回滚”
 - 第 550 页上的“锁定配置文件”
 - 第 551 页上的“向配置文件添加注释”
- 第 552 页上的“许可密钥”
- 第 554 页上的“签名服务的注册与激活”
 - 第 554 页上的“临时服务”
 - 第 554 页上的“在新设备上捆绑 AV 和 DI 服务”

- 第 555 页上的 “与 DI 一起更新 AV 服务”
 - 第 556 页上的 “只更新 DI 服务”
- 第 557 页上的 “系统时钟”
 - 第 557 页上的 “日期和时间”
 - 第 557 页上的 “时区”
 - 第 558 页上的 “NTP”

域名系统支持

NetScreen 设备集成了“域名系统”(DNS)支持,允许您既可使用 IP 地址也可使用域名来识别位置。DNS 服务器保留有与域名相关联的 IP 地址表。除了使用可路由的 IP 地址(域名 www.netscreen.com 对应的 IP 地址是 209.125.148.13)来引用位置以外,还可以通过 DNS 用域名(如 www.netscreen.com)来引用位置。下列所有程序均支持 DNS 转换:

- 地址簿
- 系统日志
- 电子邮件
- WebTrends
- Websense
- LDAP
- SecurID
- RADIUS
- NetScreen-Security Manager

在将 DNS 用于域名 / 地址解析之前,必须在 NetScreen 设备中输入 DNS 服务器(主 DNS 服务器和辅 DNS 服务器)的地址。

注意: 在启用 NetScreen 设备作为“动态主机配置协议”(DHCP)服务器(请参阅[第 516 页上的“DHCP”](#))时,还必须得在 WebUI 的 DHCP 页中输入 DNS 服务器的 IP 地址,也可以使用 CLI 中的 **set interface interface dhcp** 命令。

DNS 查找

出现以下情况时，NetScreen 设备会使用特定的 DNS 服务器检查 DNS 表中的所有条目，从而将这些条目全部刷新：

- 发生 HA 故障切换后
- 到达每天固定的预定时间及一天中固定的预定时间间隔
- 手动命令设备执行 DNS 查找时
 - WebUI: Network > DNS: 单击 Refresh DNS cache。
 - CLI: `exec dns refresh`

除使用现有方法设置每天自动刷新 DNS 表的时间外，还可以自行定义刷新的时间间隔（4 到 24 小时之间）。

注意：如果通过 WebUI 来添加诸如地址或 IKE 网关等完全合格的域名 (FQDN)，点击 **Apply** 或 **OK** 后，NetScreen 设备会解析该域名。键入引用 FQDN 的 CLI 命令后，NetScreen 设备将在输入后尝试对其进行解析。

当 NetScreen 设备与 DNS 服务器连接以解析域名 / 地址映射时，会将该条目存储在其 DNS 状态表中。下面的列表包含 DNS 查找涉及到的一些具体内容：

- 当 DNS 查找返回多个条目时，通讯簿会接受所有条目。511 页列出的其它程序只接受第一个条目。
- 当使用 WebUI 中的 **Refresh** 按钮或输入 `exec dns refresh` CLI 命令刷新查找时，如果 NetScreen 设备发现域名表中有内容发生了变化，将重新安装所有策略。
- 如果 DNS 服务器发生故障，NetScreen 设备会重新查找所有内容。
- 如果查找失败，NetScreen 设备将从高速缓存表中将其删除。
- 如果在向通讯簿添加地址时域名查找失败，NetScreen 设备会显示一条错误信息，声明已成功添加地址，但是 DNS 名查找失败。

NetScreen 设备必须每天进行一次新的查找，您可以安排 NetScreen 设备在指定时间进行查找：

WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:
DNS refresh every day at: 选中复选框而后输入时间 <hh:mm>

CLI

```
set dns host schedule time_str  
save
```

DNS 状态表

DNS 状态表会报告查找到的所有域名、相应的 IP 地址、查找是否成功以及每个域名 /IP 地址上次解析的时间。报告格式如下面的例子所示：

名称	IP 地址	状态	上一次查询
www.yahoo.com	204.71.200.74	Success	8/13/2000 16:45:33
	204.71.200.75		
	204.71.200.67		
	204.71.200.68		
www.hotbot.com	209.185.151.28	Success	8/13/2000 16:45:38
	209.185.151.210		
	216.32.228.18		

要查看 DNS 状态表，请按下列任一方法进行操作：

WebUI

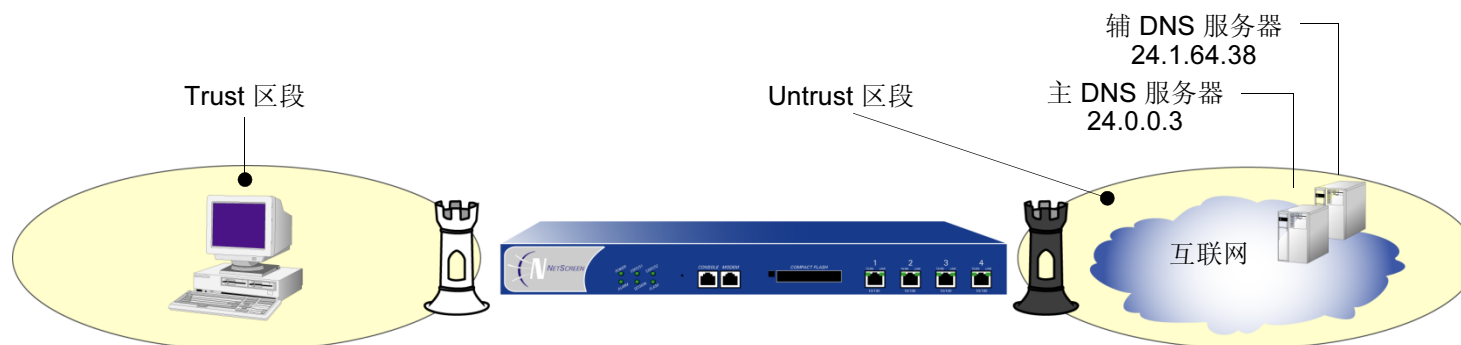
Network > DNS > Show DNS Table

CLI

```
get dns host report
```

范例：DNS 服务器和刷新进度

要实现 DNS 功能，在 NetScreen 设备中为 24.1.64.38 和 24.0.0.3 上的 DNS 服务器输入 IP 地址，保护总公司仅有的一台主机。将 NetScreen 设备安排为在每天晚上 11:00 时刷新存储在 DNS 状态表中的 DNS 设置。



WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:

Primary DNS Server: 24.0.0.3

Secondary DNS Server: 24.1.64.38

DNS Refresh: (选择)

Every Day at: 23:00

CLI

```
set dns host dns1 24.0.0.3
set dns host dns2 24.1.64.38
set dns host schedule 23:00
save
```

范例：设置 DNS 刷新时间间隔

在本例中，将配置 NetScreen 设备自每天凌晨 00:01 起，每隔 4 小时刷新一次 DNS 表。

WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:

DNS Refresh: (选择)

Every Day at: 00:01

Interval: 4

CLI

```
set dns host schedule 00:01 interval 4
save
```

DHCP

“动态主机配置协议” (DHCP) 的设计目的是通过自动为网络中的主机分配 TCP/IP 设置，来减少对网络管理员的需求。DHCP 会代替管理员自动为网络中的每台机器分配、配置、跟踪和更改 (必要时) 所有 TCP/IP 设置。此外，DHCP 还可以确保不使用重复地址、重新分配未使用的地址，并且可以自动为主机连接的子网分配适当的 IP 地址。

不同的 NetScreen 设备支持不同的 DHCP 角色：

- **DHCP 客户端**：某些 NetScreen 设备可以充当 DHCP 客户端，接收为任意区段中的任意物理接口动态分配的 IP 地址。
- **DHCP 服务器**：另一些 NetScreen 设备可以充当 DHCP 服务器，为任意区段内的任意物理接口或 VLAN 接口上的主机 (充当 DHCP 客户端) 动态分配 IP 地址。

注意：使用 DHCP 服务器模块为区段内的工作站等主机分配地址时，仍然可以让其它机器 (如邮件服务器和 WINS 服务器) 使用固定 IP 地址。

- **DHCP 转接代理**：还有一些 NetScreen 设备可以充当 DHCP 中继代理，接收来自 DHCP 服务器的 DHCP 信息，然后将这些信息转交给任意区段内的任意物理接口或 VLAN 接口上的主机。
- **DHCP 客户端 / 服务器 / 中继代理**：某些 NetScreen 设备可以同时充当 DHCP 客户端、服务器和中继代理。注意，一个接口上只能配置一个 DHCP 角色。例如，不能在同一接口上同时配置 DHCP 客户端和服务器。根据需要，可以配置 DHCP 客户端模块，将其收到的 TCP/IP 设置转发给 DHCP 服务器模块，以便服务器模块将 TCP 设置提供给 Trust 区段内充当 DHCP 客户端的主机。

DHCP 由两部分组成：用于传送与主机有关的 TCP/IP 配置设置的协议和用于分配 IP 地址的机制。当 NetScreen 设备充当 DHCP 服务器时，它会在每一主机启动时为其提供下面的 TCP/IP 设置：

- 缺省网关的 IP 地址和网络掩码。如果将这些设置保留为 0.0.0.0/0，DHCP 服务器模块会自动使用缺省 Trust 区段接口¹的 IP 地址和网络掩码。
- 下列服务器的 IP 地址：
 - WINS 服务器 (2):² “Windows 互联网命名服务” (WINS) 服务器将 Windows NT 网络环境使用的 NetBIOS 名称映射为基于 IP 的网络中使用的 IP 地址。
 - NetInfo 服务器 (2): NetInfo 是一种 Apple 网络服务，用于在 LAN 内分发管理数据。
 - NetInfo 标记 (1): Apple NetInfo 数据库使用的识别标记。
 - DNS 服务器 (3): “域名系统” (DNS) 服务器可将统一资源定位器 (URL) 映射为 IP 地址。
 - SMTP 服务器 (1): “简单邮件传输协议” (SMTP) 服务器可向存储收到邮件的邮件服务器 (如 POP3 服务器) 传送 SMTP 消息。
 - POP3 服务器 (1): “邮局协议版本 3” (POP3) 服务器可存储收到的邮件。POP3 服务器必须与 SMTP 服务器联合使用。
 - 新闻服务器 (1): 新闻服务器接收并存储新闻组寄来的信息。

注意：当 NetScreen 设备向某一 DHCP 客户端传递上述参数时，如果该客户端有指定的 IP 地址，该地址将忽略从 DHCP 服务器接收到的所有动态信息。

1. 在可以于 Trust 区段绑定多个接口的设备上，缺省接口是第一个绑定到该区段并指定 IP 地址的接口。
2. 括号中的数字表示支持的服务器数量。

DHCP 服务器

一台 NetScreen 设备，最多支持八个 DHCP 服务器，这些服务器可以位于任意区段内的任一物理接口或 VLAN 接口上。充当 DHCP 服务器时，NetScreen 设备以两种模式分配 IP 地址和子网掩码：

- 在“动态”模式下，充当 DHCP 服务器的 NetScreen 设备会将地址池³中的 IP 地址分配（或“租借”）给 DHCP 客户端主机。可在一定时间内租用该 IP 地址，也可无限期租用，直到客户端放弃该 IP 地址为止。（要定义无限租用期，请输入 0。）
- 在“保留”模式下，特定客户端每次联机时，NetScreen 设备都会从地址池中专门为其分配一个指定的 IP 地址。

注意：NetScreen 设备在快速存储器中保存通过 DHCP 分配的每个 IP 地址。因此，重新启动 NetScreen 设备不影响地址分配。

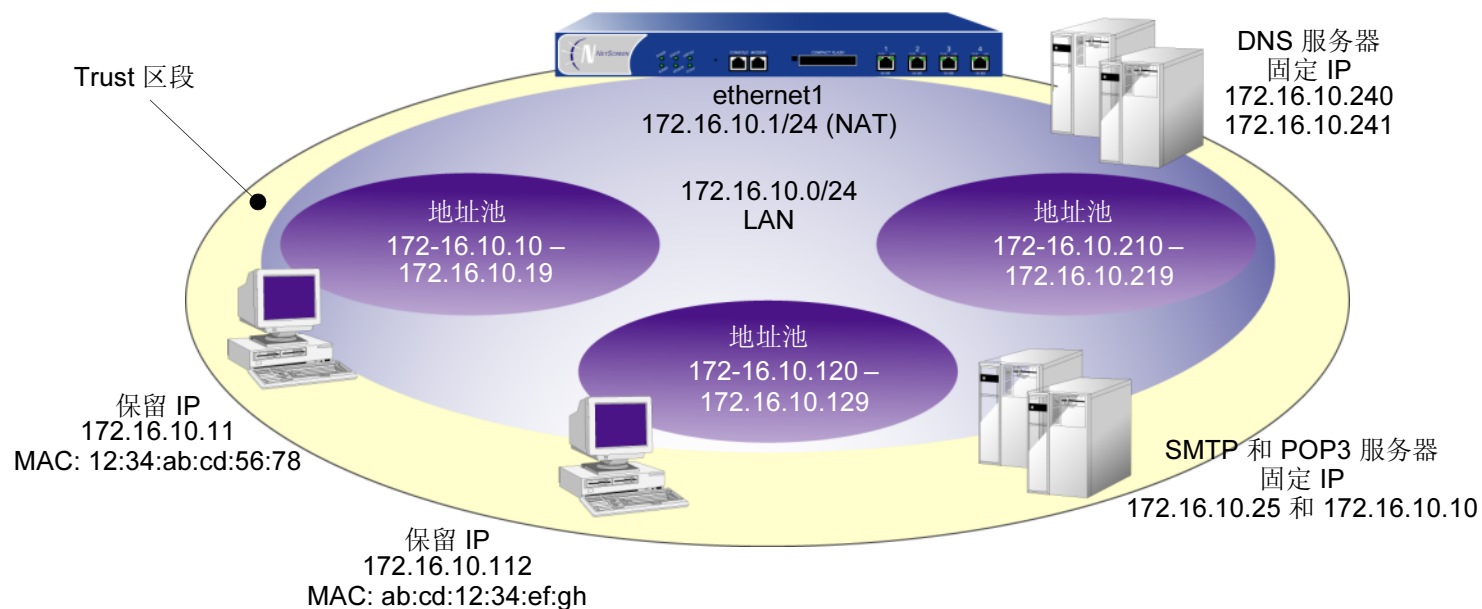
范例：NetScreen 设备作为 DHCP 服务器

用 DHCP 将 Trust 区段内的 172.16.10.0/24 网络分成三个 IP 地址池。

- 172.16.10.10 直达 172.16.10.19
- 172.16.10.120 直达 172.16.10.129
- 172.16.10.210 直达 172.16.10.219

DHCP 服务器将动态分配所有 IP 地址，只有使用预留 IP 地址的两个工作站和使用静态 IP 地址的四个服务器除外。接口 ethernet1 绑定到 Trust 区段，其 IP 地址为 172.16.10.1/24，并且处于 NAT 模式。域名是 dynamic.com。

3. 地址池是指同一子网内的 IP 地址的定义范围，NetScreen 设备可以从中提取 DHCP 地址进行分配。最多可以编组 255 个 IP 地址。



WebUI

1. 地址

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

Address Name: DNS#1

Comment: Primary DNS Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.240/32

Zone: Trust

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

Address Name: DNS#2

Comment: Secondary DNS Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.241/32

Zone: Trust

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

Address Name: SMTP

Comment: SMTP Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.25/32

Zone: Trust

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

Address Name: POP3

Comment: POP3 Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.110/32

Zone: Trust

2. DHCP 服务器

Network > DHCP > Edit (对于 ethernet1) > DHCP Server: 输入以下内容, 然后单击 **Apply**:⁴

Lease: Unlimited (选择)

WINS#1: 0.0.0.0

DNS#1: 172.16.10.240

> Advanced Options: 输入以下内容, 然后单击 **Return**, 设置高级选项并返回基本配置页:

WINS#2: 0.0.0.0

DNS#2: 172.16.10.241

DNS#3: 0.0.0.0

SMTP: 172.16.10.25

POP3: 172.16.10.110

NEWS: 0.0.0.0

NetInfo Server #1: 0.0.0.0

NetInfo Server #2: 0.0.0.0

NetInfo Tag: (保留字段为空)

Domain Name: dynamic.com

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

Dynamic: (选择)

IP Address Start: 172.16.10.10

IP Address End: 172.16.10.19

4. 如果将 Gateway 和 Netmask 字段保留为 0.0.0.0, DHCP 服务器模块会将设置给 ethernet1 的 IP 地址和网络掩码发送到客户端 (本例中为 172.16.10.1 和 255.255.255.0)。但是, 如果启用 DHCP 客户端模块将 TCP/IP 设置转发到 DHCP 服务器模块 (请参阅第 534 页上的 “TCP/IP 设置传播”), 则必须在 Gateway 和 Netmask 字段中手动输入 172.16.10.1 和 255.255.255.0。

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

Dynamic: (选择)

IP Address Start: 172.16.10.120

IP Address End: 172.16.10.129

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

Dynamic: (选择)

IP Address Start: 172.16.10.210

IP Address End: 172.16.10.219

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

Reserved: (选择)

IP Address: 172.16.10.11

Ethernet Address: 1234 abcd 5678

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

Reserved: (选择)

IP Address: 172.16.10.112

Ethernet Address: abcd 1234 efgh

CLI

1. 地址

```
set address trust dns1 172.16.10.240/32 "primary dns server"  
set address trust dns2 172.16.10.241/32 "secondary dns server"  
set address trust snmp 172.16.10.25/32 "snmp server"  
set address trust pop3 172.16.10.110/32 "pop3 server"
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server option domainname dynamic.com5  
set interface ethernet1 dhcp server option lease 0  
set interface ethernet1 dhcp server option dns1 172.16.10.240  
set interface ethernet1 dhcp server option dns2 172.16.10.241  
set interface ethernet1 dhcp server option smtp 172.16.10.25  
set interface ethernet1 dhcp server option pop3 172.16.10.110  
set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19  
set interface ethernet1 dhcp server ip 172.16.10.120 to 172.16.10.129  
set interface ethernet1 dhcp server ip 172.16.10.210 to 172.16.10.219  
set interface ethernet1 dhcp server ip 172.16.10.11 mac 1234abcd5678  
set interface ethernet1 dhcp server ip 172.16.10.112 mac abcd1234efgh  
set interface ethernet1 dhcp server service  
save
```

5. 如果不设置网关或网络掩码的 IP 地址，DHCP 服务器模块会向客户端发送 ethernet1 的 IP 地址和网络掩码（本例中为 172.16.10.1 和 255.255.255.0）。但是，如果启用 DHCP 客户端模块将 TCP/IP 设置转发到 DHCP 服务器模块（请参阅第 534 页上的“TCP/IP 设置传播”），则必须手动设置这些选项：
set interface ethernet1 dhcp server option gateway 172.16.10.1 和 **set interface ethernet1 dhcp server option netmask 255.255.255.0**。

NSRP 集群中的 DHCP 服务器

当冗余 NSRP 集群中的主单元行使 DHCP 服务器的功能时，集群中的所有成员都会保留全部的 DHCP 配置以及 IP 地址分配信息。一旦发生故障切换，新的主单元将负责维护所有 DHCP 分配。但是，HA 通信的终止破坏了集群成员之间现有 DHCP 分配的同步。恢复 HA 通信后，通过在集群的两个单元上使用以下 CLI 命令，可以再次同步 DHCP 分配：**set nsrp rto-mirror sync**。

DHCP 服务器检测

在 NetScreen 设备上启动 DHCP 服务器时，系统首先要检查该接口上是否已存在 DHCP 服务器。如果检测到网络上存在其它 DHCP 服务器，ScreenOS 会自动终止本地 DHCP 服务器进程的启动。为检测其它 DHCP 服务器，设备每隔两秒自动发送一次 DHCP 启动请求。如果发出启动请求后没有收到任何响应，设备随即会启动本地的 DHCP 服务器进程。

如果 NetScreen 设备收到其它 DHCP 服务器发出的响应，系统会生成一条消息，指出已在 NetScreen 设备上启用该 DHCP 服务器，但由于网络上存在另一个 DHCP 服务器，因此没有启动该服务器。日志消息中还包括现有 DHCP 服务器的 IP 地址。

可以设置以下三种可选模式，检测接口上的 DHCP 服务器：Auto、Enable 或 Disable⁶。在 Auto 模式下，NetScreen 设备始终在启动服务器时检测现有的 DHCP 服务器。通过将 NetScreen DHCP 服务器设置为 Enable 或 Disable 模式，可以配置设备不尝试检测接口上的其它 DHCP 服务器。在 Enable 模式下，DHCP 服务器始终开启，设备不检测网络上是否存在现有 DHCP 服务器。在 Disable 模式下，DHCP 服务器始终关闭。

6. 对于 NetScreen-5XP 和 NetScreen-5XT 设备，Auto 模式是缺省的 DHCP 服务器检测模式。对于支持 DHCP 服务器的其它 NetScreen 设备，Enable 模式是缺省的 DHCP 服务器检测模式。

范例：打开 DHCP 服务器检测

在本例中，将设置 **ethernet1** 接口上的 DHCP 服务器，在其启动前先检测该接口上是否存在 DHCP 服务器。

WebUI

Network > DHCP > Edit (对于 ethernet1) > DHCP Server: 输入以下内容，然后单击 **OK**:
Server Mode: Auto (选择)

CLI

```
set interface ethernet1 dhcp server auto
save
```

范例：关闭 DHCP 服务器检测

在本例中，将设置 **ethernet1** 接口上的 DHCP 服务器，在其启动时不检测网络上是否存在 DHCP 服务器。

WebUI

Network > DHCP > Edit (对于 ethernet1) > DHCP Server: 输入以下内容，然后单击 **OK**:
Server Mode: Enable (选择)

CLI

```
set interface ethernet1 dhcp server enable
save
```

注意：发出 CLI 命令 **set interface interface dhcp server service** 后，DHCP 服务器将被激活。如果将接口的 DHCP 服务器检测模式设置为 Auto，仅当 NetScreen 设备在网络上找不到现有服务器时，才启动 DHCP 服务器。发出 **unset interface interface dhcp server service** 命令后，将禁用 NetScreen 设备上的 DHCP 服务器，并删除任何现有的 DHCP 配置。

DHCP 中继代理

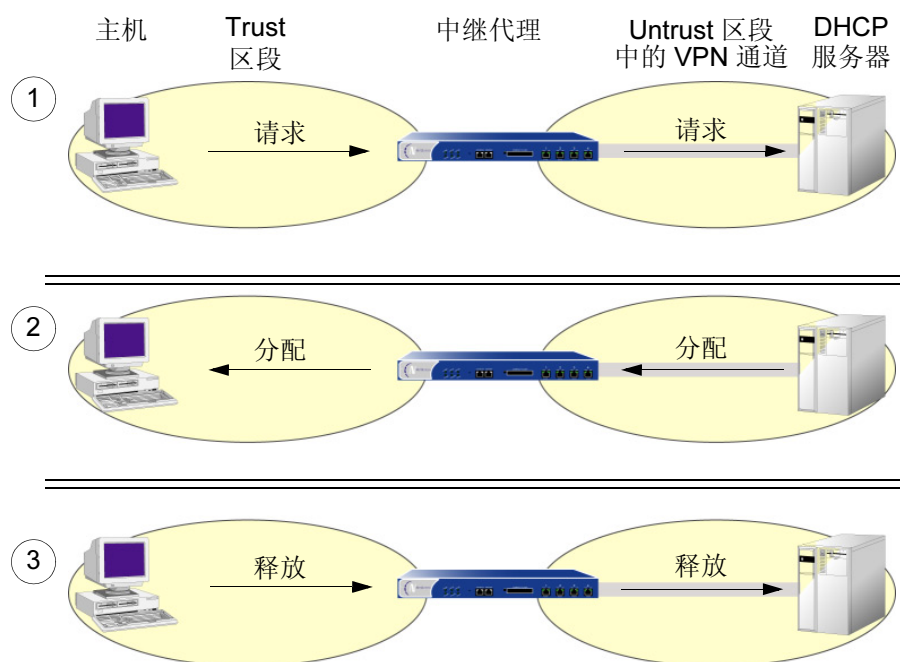
充当 DHCP 中继代理时，NetScreen 设备负责在一个区段内的主机与另一个区段内的 DHCP 服务器之间转发 DHCP 请求和分配信息。DHCP 消息可以在 NetScreen 设备与 DHCP 服务器之间公开传送，或通过 VPN 通道进行传送。

虽然不能在同一接口上配置 DHCP 中继代理、DHCP 服务器或客户端功能，但是可以在 NetScreen 设备上的一个或多个物理或 VLAN 接口上配置 DHCP 中继代理。当 NetScreen 设备用作 DHCP 中继代理时，其接口必须处于“路由”模式或“透明”模式。对于“路由”模式的接口，必须为预定义的 DHCP 中继服务配置从一个区段到另一个区段的策略。对于“透明”模式的接口，DHCP 客户端必须在 V1-Trust 区段中，而 DHCP 服务器既可以在 V1-Untrust 区段中，也可以在 V1-DMZ 区段中。不必为“透明”模式的接口配置策略。

一个 DHCP 中继代理最多可以配置三个 DHCP 服务器。中继代理将 DHCP 客户端的地址请求单点广播到所有已配置的 DHCP 服务器上。随后，中继代理将收到的第一个服务器响应转发给客户端。

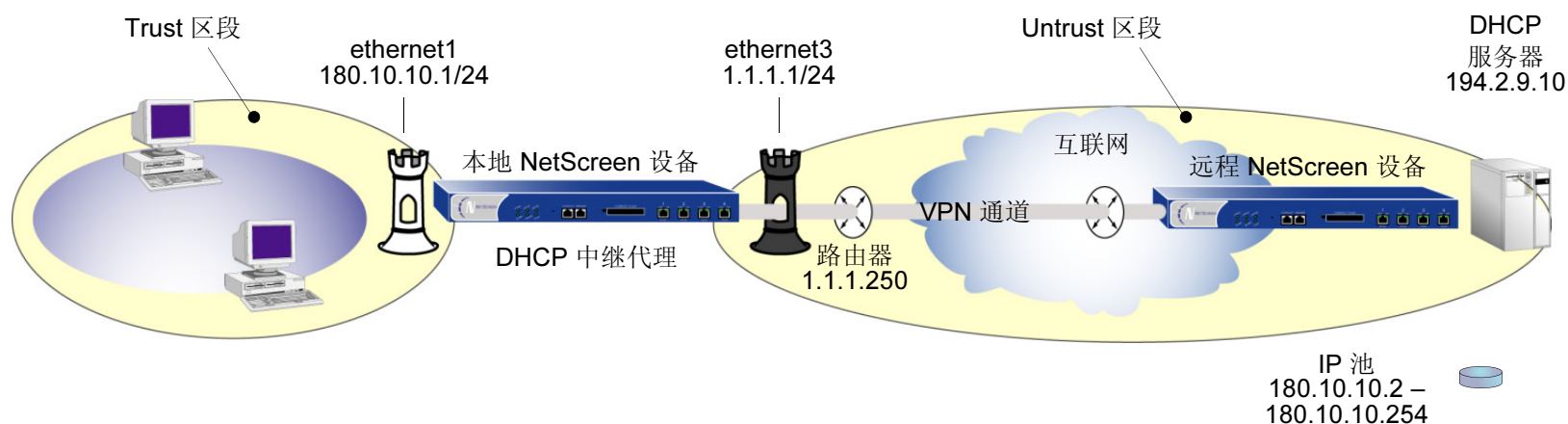
注意：当 NetScreen 设备充当 DHCP 中继代理时，由于远程 DHCP 服务器控制着所有 IP 地址分配，所以 NetScreen 设备不会生成 DHCP 分配状态报告。

下面的简化示意图展示了使用 NetScreen 设备作为 DHCP 中继代理时的有关过程。请注意，当 DHCP 消息在不可信网络中传送时，为确保安全，这些消息将通过 VPN 通道进行传递。



范例 : NetScreen 设备作为 DHCP 中继代理

在本例中，NetScreen 设备从 IP 地址为 194.2.9.10 的 DHCP 服务器中接收 DHCP 信息，而后将其转递给 Trust 区段中的主机。主机从 DHCP 服务器上定义的 IP 池中接收 IP 地址。地址范围是 180.10.10.2—180.10.10.254。DHCP 消息流经本地 NetScreen 设备和 DHCP 服务器之间的 VPN 通道，该 DHCP 服务器位于 Untrust 区段接口 IP 地址为 2.2.2.2/24 的远程 NetScreen 设备之后。接口 ethernet1 被绑定到 Trust 区段，IP 地址为 180.10.10.1/24，且处于“路由”模式。接口 ethernet3 被绑定到 Untrust 区段中，IP 地址为 1.1.1.1/24。所有安全区都在 trust-vr 路由域中。



WebUI

1. 接口

Interfaces > Edit (对于 ethernet1): 输入以下内容, 然后单击 **Apply**:

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 180.10.10.1/24

输入以下内容, 然后单击 **OK**:

Interface Mode: Route

Interfaces > Edit (对于 ethernet3): 输入以下内容, 然后单击 **OK**:

Zone: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: DHCP 服务器

IP Address/Domain Name:

IP/Netmask: (选择), 194.2.9.10/32

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: dhcp server

Security Level: Custom

Remote Gateway Type:

Static IP: (选择), Address/Hostname: 2.2.2.2

Outgoing Interface: ethernet3

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Security Level:

User Defined: Custom (选择)

Phase1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: to_dhcp

Security Level: Compatible

Remote Gateway:

Predefined: (选择), to_dhcp

> **Advanced**: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Bind To: None

4. DHCP 中继代理

Network > DHCP > Edit (对于 ethernet1) > DHCP Relay Agent: 输入以下内容, 然后单击 **Apply**:

Relay Agent Server IP or Domain Name: 194.2.9.10

Use Trust Zone Interface as Source IP for VPN: (选择)

5. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容, 然后单击 **OK**:

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250⁷

6. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容, 然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), DHCP Server

Service: DHCP-Relay

Action: Tunnel

Tunnel VPN: to_dhcp

Modify matching outgoing VPN policy: (选择)

7. 对于出站 VPN 和网络信息流, 设置到指定为缺省网关的外部路由器的路由至关重要。在本例中, NetScreen 设备将向这个路由器发送经过封装的 VPN 信息流, 因为该路由器是路由上到远程 NetScreen 设备的首个跳跃。在本范例的图解中, 通过对经过该路由器的通道的描述介绍此概念。

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 180.10.10.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address untrust dhcp_server 194.2.9.10/32
```

3. VPN

```
set ike gateway "dhcp server" ip 2.2.2.2 main outgoing-interface ethernet3
  proposal rsa-g2-3des-sha
set vpn to_dhcp gateway "dhcp server" proposal g2-esp-3des-sha
```

4. DHCP 中继代理

```
set interface ethernet1 dhcp relay server-name 194.2.9.10
set interface ethernet1 dhcp relay vpn
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. 策略

```
set policy from trust to untrust any dhcp_server dhcp-relay tunnel vpn to_dhcp
set policy from untrust to trust dhcp_server any dhcp-relay tunnel vpn to_dhcp
save
```

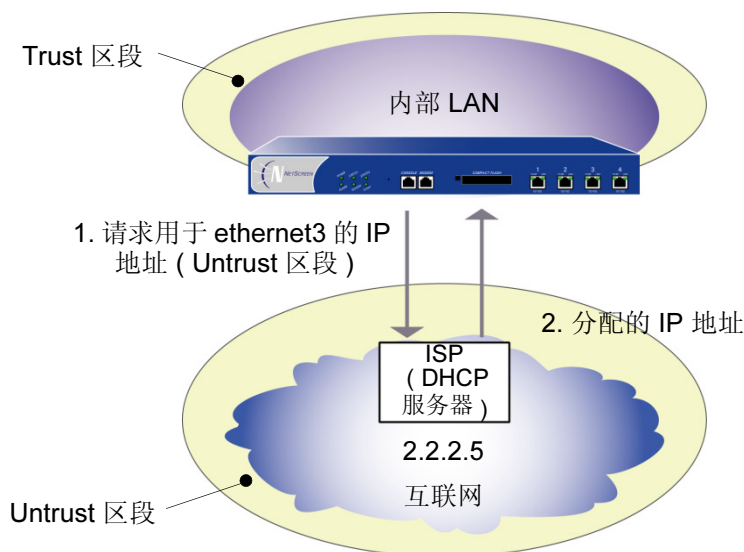
DHCP 客户端

充当 DHCP 客户端时，NetScreen 设备接收服务器为任意安全区内的任意物理接口动态分配的 IP 地址。如果有多个接口绑定到同一安全区，则可为所有接口配置一个 DHCP 客户端，前提是任意两个接口都没有连接到同一网络区段。如果为连接到同一网络区段的两个接口配置了一个 DHCP 客户端，则只使用 DHCP 服务器分配的第一个地址。(如果 DHCP 客户端收到同一 IP 地址的地址更新，则不必重新指定 IKE 密钥。)

注意：由于某些 NetScreen 设备可以同时充当 DHCP 服务器、DHCP 中继代理或 DHCP 客户端，因此不能在同一个接口上配置多个 DHCP 角色。

范例：NetScreen 设备作为 DHCP 客户端

在本例中，绑定到 Untrust 区段的接口有一个动态分配的 IP 地址。当 NetScreen 设备向其 ISP 请求 IP 地址时，它会接收到 IP 地址、子网掩码、网关 IP 地址以及租用该地址的期限。DHCP 服务器的 IP 地址为 2.2.2.5。



注意：在设立 DHCP 服务站点之前，您必须拥有下列设备：

- 数字用户线 (DSL) 调制解调器和线缆
- ISP 帐户

WebUI

Network > Interfaces > Edit (对于 ethernet3): 选择 **Obtain IP using DHCP**⁸，然后单击 **OK**。

CLI

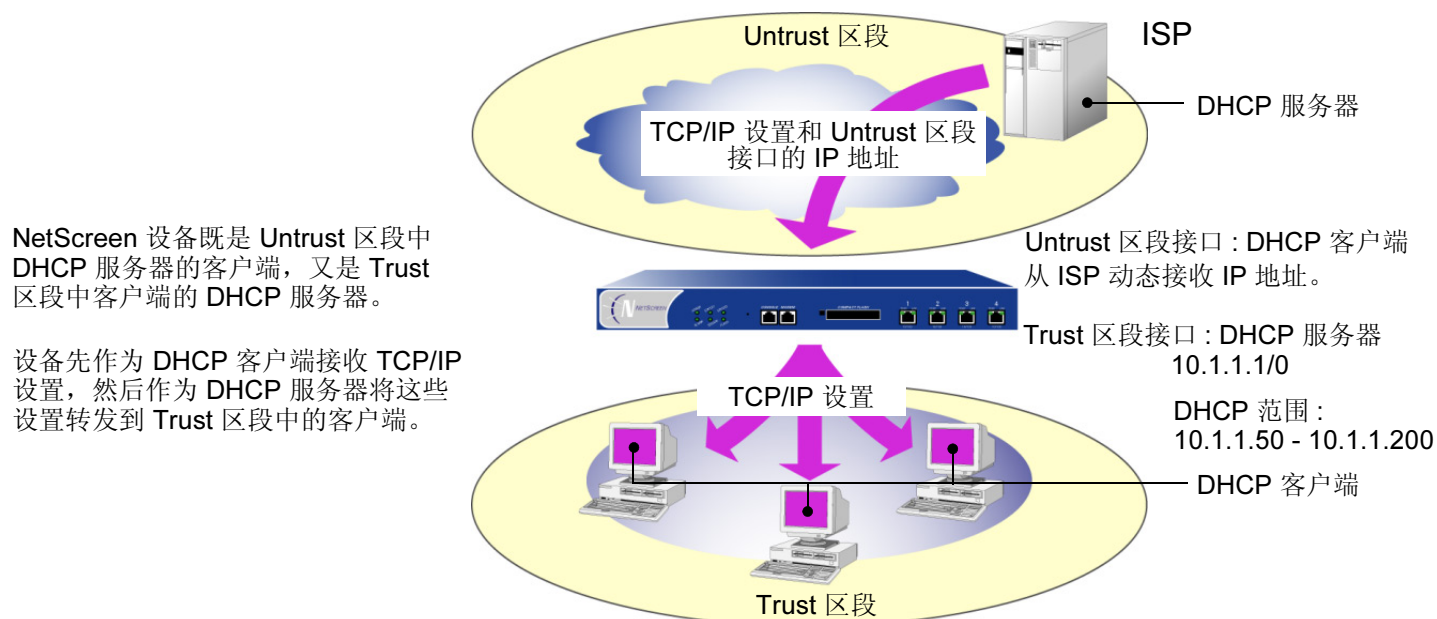
```
set interface ethernet3 dhcp client
set interface ethernet3 dhcp settings server 2.2.2.5
save
```

8. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址，但通过 CLI 则可以。

TCP/IP 设置传播

某些 NetScreen 设备可以充当“动态主机控制协议”(DHCP)客户端，从外部 DHCP 服务器接收任意安全区内的任意物理接口的 TCP/IP 设置和 IP 地址。某些 NetScreen 设备可以充当 DHCP 服务器，为任意区段内的客户端提供 TCP/IP 设置和 IP 地址。当 NetScreen 设备同时充当 DHCP 客户端和 DHCP 服务器时，可将通过 DHCP 客户端模块获知的 TCP/IP 设置传送给缺省的 DHCP 服务器模块⁹。TCP/IP 设置包括缺省网关的 IP 地址和子网掩码，以及下列服务器的全部或部分 IP 地址：

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)



9. 尽管某个物理接口或 VLAN 接口上最多可以配置八个 DHCP 服务器，但设备的缺省 DHCP 服务器只能位于每个平台的特定接口上。在 NetScreen-5XP 上，缺省 DHCP 服务器在 Trust 接口上。在 NetScreen-5XT 上，缺省 DHCP 服务器可以位于以下特定接口上：Trust-Untrust 端口模式的 Trust 接口、Dual-Untrust 端口模式的 ethernet1 接口、Home-Work 和 Combined 端口模式的 ethernet2 接口。对于其它设备，缺省 DHCP 服务器在 ethernet1 接口上。

使用 **set interface interface dhcp-client settings update-dhcpserver** 命令，可以配置 DHCP 服务器模块传播从 DHCP 客户端模块接收的所有 TCP/IP 设置。还可以使用其它设置覆盖某个设置。

范例：转发 TCP/IP 设置

在本例中，将配置 NetScreen 设备同时充当 ethernet3 接口上的 DHCP 客户端和 ethernet1 接口上的 DHCP 服务器。(缺省 DHCP 服务器位于 ethernet1 接口上。)

NetScreen 设备先作为 DHCP 客户端，从外部 DHCP 服务器 (地址为 211.3.1.6) 上接收 ethernet3 接口的 IP 地址和 TCP/IP 设置。随后，您需要启用 NetScreen 设备的 DHCP 客户端模块，将收到的 TCP/IP 设置传送到 DHCP 服务器模块。

您配置 NetScreen 设备 DHCP 服务器模块对其从 DHCP 客户端模块接收到的 TCP/IP 设置进行下列工作：

- 转发 DNS IP 地址到其在 Trust 区段中的 DHCP 客户端。
- 请用下列信息覆盖缺省网关¹⁰、网络掩码、SMTP 服务器和 POP3 服务器的 IP 地址：
 - 10.1.1.1 (这是 ethernet1 接口的 IP 地址)
 - 255.255.255.0 (这是 ethernet1 接口的网络掩码)
 - SMTP: 211.1.8.150
 - POP3: 211.1.8.172

您也会配置 DHCP 服务器模块以发送下列未从 DHCP 客户端模块接收到的 TCP/IP 设置：

- Primary WINS server: 10.1.2.42
- Secondary WINS server: 10.1.5.90

最后，需要配置 DHCP 服务器模块，将以下 IP 池中的 IP 地址分配给 Trust 区段内充当 DHCP 客户端的主机：10.1.1.50 – 10.1.1.200.

10. 如果 DHCP 服务器已在 Trust 接口上启用并有已定义的 IP 地址池 (这是有些 NetScreen 设备上的缺省行为)，您必须先删除 IP 地址池，然后才能更改缺省网关和网络掩码。

WebUI

注意：只能通过 **CLI** 设置此功能。

CLI

1. DHCP 客户端

```
set interface ethernet3 dhcp-client settings server 211.3.1.6
set interface ethernet3 dhcp-client settings update-dhcpserver
set interface ethernet3 dhcp-client settings autoconfig
set interface ethernet3 dhcp-client enable
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server option gateway 10.1.1.1
set interface ethernet1 dhcp server option netmask 255.255.255.0
set interface ethernet1 dhcp server option wins1 10.1.2.42
set interface ethernet1 dhcp server option wins2 10.1.5.90
set interface ethernet1 dhcp server option pop3 211.1.8.172
set interface ethernet1 dhcp server option smtp 211.1.8.150
set interface ethernet1 dhcp server ip 10.1.1.50 to 10.1.1.200
set interface ethernet1 dhcp server service
save
```

PPPoE

“以太网点对点协议”(PPPoE)结合了“点对点协议”(PPP)和以太网协议,前者(PPP)通常用于拨号连接,后者用于将一个站点上的多个用户连接到同一用户端设备。虽然多个用户可以共享同一物理连接,但访问控制、计费以及服务类型等仍按单个用户处理。某些 NetScreen 设备支持 PPPoE 客户端,允许使用 PPPoE 访问其客户端互联网,以兼容方式在 ISP 管理的 DSL、Ethernet Direct 和电缆网络上运行。

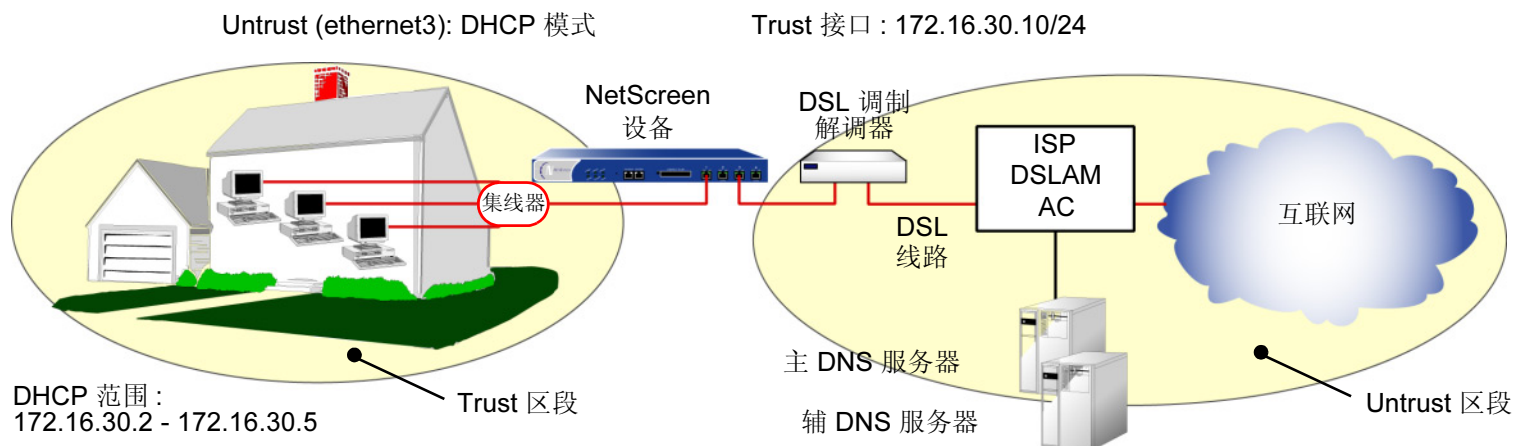
在支持 PPPoE 的设备上,可以在部分或全部接口上配置 PPPoE 客户端实例。可以使用用户名、密码和其它参数配置特定的 PPPoE 实例,然后将该实例绑定到接口上。当存在两个 Ethernet 接口(主接口和备份接口)绑定到 Untrust 区段时,可以只配置一个接口,也可以在两个接口上全部配置 PPPoE。例如,处于 Dual Untrust 端口模式时,¹¹可以在主接口(ethernet3)上配置 DHCP,在备份接口(ethernet2)上配置 PPPoE。也可以为主接口和备份接口全部配置 PPPoE。

范例：设置 PPPoE

下例讲解如何为 PPPoE 连接定义 NetScreen 设备的不可信接口,以及如何开始 PPPoE 服务。

在本例中, NetScreen 设备先从 ISP 那里接收为 Untrust 区段接口(ethernet3)动态分配的 IP 地址,再为 Trust 区段内的三台主机动态分配 IP 地址。在本例中, NetScreen 设备既充当 PPPoE 客户端又充当 DHCP 服务器。Trust 区段接口必须处于 NAT 模式或“路由”模式。在本例中,它处于 NAT 模式。

11. 某些 NetScreen 设备支持端口模式,例如 NetScreen-5XT。



在为 PPPoE 服务设立本例中的站点之前，您必须得有以下设备：

- 数字用户线 (DSL) 调制解调器和线缆
- ISP 帐户
- 用户名及密码 (ISP 提供)

WebUI

1. Interfaces and PPPoE

Network > Interfaces > Edit (对于 ethernet1): 输入以下内容，然后单击 **OK**:

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 172.16.30.10/24

Network > Interfaces > Edit (对于 ethernet3): 输入以下内容，然后单击 **OK**:

Zone: Untrust

Obtain IP using PPPoE: (选择)

User Name/Password: < 名称 >/< 密码 >

Network > Interfaces > Edit (对于 ethernet3): 要测试 PPPoE 连接, 请单击 **Connect**。

*注意: 建立 PPPoE 连接后, ISP 会自动为 Untrust 区段接口和“域名服务”(DNS) 服务器提供 IP 地址。如果 NetScreen 设备通过 PPPoE 接收 DNS 地址, 则缺省时新的 DNS 设置会覆盖本地设置。如果不希望新的 DNS 设置取代本地设置, 可使用 CLI 命令 **unset pppoe dhcp-updateserver** 禁止此行为。*

如果配置 Untrust 区段接口使用静态 IP 地址, 必须先获得 DNS 服务器的 IP 地址, 然后在 NetScreen 设备和 Trust 区段的主机上手动输入这些地址。

2. DHCP 服务器

Network > Interfaces > Edit (对于 ethernet1) > DHCP: 选择 **DHCP Server**, 然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet1) > DHCP: 输入以下内容, 然后单击 **Apply**:

Lease: 1 hour

Gateway: 0.0.0.0

Netmask: 0.0.0.0

DNS#1: 0.0.0.0

> Advanced: 输入以下内容, 然后单击 **Return**:

DNS#2: 0.0.0.0

Domain Name: (保留空白)

Network > Interfaces > DHCP (对于 ethernet1) > New Address: 输入以下内容, 然后单击 **OK**:

Dynamic: (选择)

IP Address Start: 172.16.30.2

IP Address End: 172.16.30.5

3. 激活 NetScreen 设备上的 PPPoE

关闭 DSL 调制解调器、NetScreen 设备和三台工作站的电源。

打开 DSL 调制解调器。

打开 NetScreen 设备。

NetScreen 设备与 ISP 建立 PPPoE 连接，并通过 ISP 获得 DNS 服务器的 IP 地址。

4. 激活内部网络上的 DHCP

打开工作站。

工作站自动接收 DNS 服务器的 IP 地址。在它们尝试进行 TCP/IP 连接时，它们会获得自己的 IP 地址。

注意：使用 DHCP 为 Trust 区段的主机分配 IP 地址时，NetScreen 设备会自动将从 ISP 接收的 DNS 服务器的 IP 地址转发给该主机。

如果不通过 DHCP 动态分配主机 IP 地址，必须在每台主机中手动输入 DNS 服务器的 IP 地址。

区段中的主机与 Untrust 区段建立的每个 TCP/IP 连接都要自动经过 PPPoE 封装处理。

CLI

1. 接口和 PPPoE

```
set interface ethernet1 zone trust
set interface ethernet1 ip 172.16.30.10/24
set interface ethernet3 zone untrust
set pppoe interface ethernet3
set pppoe username name_str password pswd_str
```

要测试 PPPoE 连接：

```
exec pppoe connect
get pppoe
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 172.16.30.2 to 172.16.30.5
set interface ethernet1 dhcp server option lease 60
save
```

3. 激活 NetScreen 设备上的 PPPoE

关闭 DSL 调制解调器、NetScreen 设备和三台工作站的电源。

打开 DSL 调制解调器。

打开 NetScreen 设备。

4. 激活内部网络上的 DHCP

打开工作站。

工作站自动接收 DNS 服务器的 IP 地址。在它们尝试进行 TCP/IP 连接时，它们会获得自己的 IP 地址。

Trust 区段中的主机与 Untrust 区段建立的每个 TCP/IP 连接都要自动经过 PPPoE 封装处理。

范例：在主 Untrust 接口和备份 Untrust 接口上配置 PPPoE

在本例中，NetScreen-5XT 处于 Dual Untrust 模式。在下例中，将为 Untrust 区段的主接口 (ethernet3) 和备份接口 (ethernet2) 配置 PPPoE。

WebUI

ethernet3 接口的 PPPoE 配置

Network > PPPoE > New: 输入以下内容，然后单击 **OK**:

PPPoE instance: eth3-pppoe
Bound to interface: ethernet3 (选择)
Username: user1
Password: 123456
Authentication: Any (选择)
Access Concentrator: ac-11

ethernet2 接口的 PPPoE 配置

Network > PPPoE > New: 输入以下内容，然后单击 **OK**:

PPPoE instance: eth2-pppoe
Bound to interface: ethernet2 (选择)
Username: user2
Password: 654321
Authentication: Any (选择)
Access Concentrator: ac-22

CLI

1. ethernet3 接口的 PPPoE 配置

```
set pppoe name eth3-pppoe username user1 password 123456
set pppoe name eth3-pppoe ac ac-11
set pppoe name eth3-pppoe authentication any
set pppoe name eth3-pppoe interface ethernet3
```

2. ethernet2 接口的 PPPoE 配置

```
set pppoe name eth2-pppoe username user2 password 654321
set pppoe name eth2-pppoe ac ac-22
set pppoe name eth2-pppoe authentication any
set pppoe name eth2-pppoe interface ethernet2
save
```

下载 / 上传设置和固件

可以向 NetScreen 设备上传和从中下载配置设置和固件。上传和下载的位置种类取决于您是使用 WebUI 还是使用 CLI 来执行该操作。如果使用 WebUI 和 Web 浏览器支持，您可以从任何本地目录上传或下载配置设置以及上传 ScreenOS 固件。如果是通过 CLI，您可以向 TFTP 服务器或 PC 卡上传和从中下载设置及固件。

保存和导入设置

在每次做出重要改动后备份设置是一种很好的习惯。通过 WebUI，您可以将配置下载至任何本地目录，做为预防备份。对于某些 NetScreen 设备，可以使用 CLI 将配置下载至 TFTP 服务器或闪存卡中。如果需要保存的备份配置，只需将其上传到 NetScreen 设备。

上传和下载配置的功能还提供了大量分发配置模板的方法。

要下载配置：

WebUI

1. Configuration > Update > Config File: 单击 **Save to File**。
会出现一条系统消息，提示您打开该文件或将其保存到计算机上。
2. 单击 **Save**。
3. 找到要保存配置文件的位置，然后单击 **Save**。

CLI

```
save config from flash to { tftp ip_addr | slot } filename [ from interface ]
```

注意：在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。

要上传配置：

WebUI

Configuration > Update > Config File: 输入以下内容，然后单击 **Apply**:

如果要将新配置和当前配置合并在一起，请选择 **Merge to Current Configuration**；如果要用新配置覆盖当前配置，请选择 **Replace Current Configuration**。

> New Configuration File: 输入配置文件位置或单击 **Browse** 找到文件位置，选择该文件，然后单击 **Open**。

CLI

```
save config from { tftp ip_addr | slot } filename to flash [ merge [ from  
interface ] ]
```

注意：在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。

上传和下载固件

一旦新的 NetScreen ScreenOS 版本变得可用，即可购买该版本，并从 NetScreen 下载站点下载。然后可使用 **save** 命令上传新固件，或使用 WebUI 从本地目录上传固件。通过 CLI，可以从 TFTP 服务器或 PC 卡上传固件，并且可以将固件下载至 TFTP 服务器。

注意：软件升级后，请重新启动 NetScreen 设备。此过程需要几分钟时间。

WebUI

Configuration > Update > ScreenOS/Keys: 输入以下内容，然后单击 **Apply**:

Select what you want to update: Firmware、Image Key 或 License Key。

> Load File: 输入要更新的文件的位置或单击 **Browse** 找到文件位置，选择该文件，然后单击 **Open**。

CLI

```
save software from { flash | slot1 filename | tftp ip_addr filename } to flash
```

注意：在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。

您还可以通过 CLI 将固件下载至 TFTP 服务器，使用以下 **save** 命令：

```
save software from flash to tftp ip_addr filename [ from interface ]
```


配置回滚

如果加载配置文件时出现问题，例如 **NetScreen** 设备发生故障或远程用户失去了管理设备的能力，则可执行配置回滚，恢复到先前在闪存中保存的上次已知正确的配置文件。我们将恢复后的配置文件称为 **LKG** (上次已知正确) 配置文件。

***注意：**并非所有的 **NetScreen** 设备都支持配置回滚。要查看您的 **NetScreen** 设备是否支持此功能，请参阅与平台相关的数据表。*

上次已知正确的配置

执行配置回滚之前，请确保闪存中已保存 **LKG** 配置文件，以供 **NetScreen** 设备恢复使用。要进行此操作，请使用 **get config rollback** CLI 命令。**LKG** 配置文件的名称是 *\$lkg\$.cfg*。如果看不到此文件，说明该文件不存在，必须手动创建它。

将配置文件保存成闪存中的上次已知正确文件：

1. 确保 **NetScreen** 设备当前的配置文件正确。
2. 使用 **save config to last-known-good** CLI 命令将当前配置文件保存到闪存中。执行此命令后，当前配置文件会覆盖闪存中现有的 **LKG** 配置文件。

如果既要备份最近的配置更改，又要维护最新的配置副本，则定期将 **NetScreen** 设备上的配置文件保存成 **LKG** 配置文件不失为一个两全其美的好办法。

自动与手动配置回滚

您既可以启用 **NetScreen** 设备自动恢复到上次已知正确 (**LKG**) 的配置文件，也可以手动执行回滚。一旦最新加载的配置文件出错，可使用自动配置回滚功能将 **NetScreen** 设备回滚到 **LKG** 配置文件。

在缺省情况下禁用自动配置回滚功能。此外，无论设备启动前该功能处于禁用还是启用状态，每次启动后都会禁用它。要启用自动配置回滚，请使用 **exec config rollback enable** 命令。要禁用该功能，请使用 **exec config rollback disable** 命令。

要执行手动配置回滚，请使用 **exec config rollback** 命令。

注意：WebUI 不支持配置回滚功能。

启用配置回滚功能后，命令提示符会相应改变，以指示其状态：

```
ns-> exec config rollback enable
```

```
ns(rollback enabled)->
```

禁用配置回滚功能后，命令提示符将改回设备主机名：

```
ns(rollback enabled)-> exec config rollback disable
```

```
ns->
```

要验证已启用自动回滚功能，请使用 **get config rollback** 命令。如果已启用该功能，**get config rollback** 的第一行输出为：

```
config rollback is enabled
```

否则，输出的第一行信息为：

```
config rollback is disabled
```

如果存在 LKG 配置文件，**get config rollback** 的第二行输出为：

```
Last-known-good config file flash:/$lkg$.cfg exists in the flash.
```

该行下显示文件的大小和内容。

如果 LKG 配置文件不存在，第二行（即最后一行）输出为：

```
Last-known-good config file flash:/$lkg$.cfg does not exist.
```

启用配置回滚功能后，可通过以下操作触发回滚操作：

- 重新启动 NetScreen 设备（先关闭电源，再打开）
- 重置 NetScreen 设备（输入 **reset** 命令）
- 输入 **exec config rollback** 命令

加载新的配置文件

以下内容介绍如何加载新的配置文件、启用配置回滚功能以及新配置文件的紧急故障排除。

1. 使用 **Save config to last-known-good CLI** 命令，将当前配置文件保存为 LKG。
2. 使用 **exec config rollback enable CLI** 命令，可以在 NetScreen 设备上启用自动配置回滚功能。启用此功能的同时请锁定 LKG 文件，以防止其它用户覆盖该文件，从而破坏正在进行的配置回滚。
3. 可使用 WebUI 或 CLI 加载新的配置文件。有关详细信息，请参阅第 546 页上的“上传和下载固件”。
4. 发出命令测试新的配置文件。可能出现以下几种情况：
 - 新配置文件运行正确。
 - 新配置文件有问题，无法再访问及管理 NetScreen 设备。遇到上述情况，只能关闭设备。NetScreen 设备打开后，先读取闪存文件，这些文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。
 - 您可能注意到新配置文件存在某些问题或错误。此时，需要使用 **reset CLI** 命令重置 NetScreen 设备。设备重启后，先读取闪存文件，该文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。
 - 新配置文件有问题，导致 NetScreen 设备无法操作。此时，NetScreen 设备会自动重启。设备重启后，先读取闪存文件，该文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。

注意：NSRP—在主动/主动设置中，如果加载新的配置文件失败，两台 NetScreen 设备都会恢复到 LKG 文件。在主动/被动设置中，如果加载新的配置文件失败，只有主设备恢复到 LKG 文件。只有将配置保存到文件后，主设备才能与备份设备同步。

锁定配置文件

为防止闪存中的配置文件被其它管理员覆盖，可将其锁定；导入新的配置文件之前通常也要锁定原文件。锁定配置文件时，设备会启动一个加锁计时器。如果设备在先前指定的锁定期限内没有收到 **CLI** 命令，则会使用闪存中锁定的配置文件自动重启。请养成良好的习惯，在开始导入配置文件之前锁定设备当前的配置文件。这样可以有效防止因导入过程出错而导致设备进入无限期的死机状态。

一旦锁定配置文件，您和其它连接到设备 (例如通过 **Telnet** 或 **WebUI**) 的管理员就无法保存配置文件。必须先解除配置文件的锁定，然后才能使用 **save** 命令保存新的配置命令。

注意：您只能通过 **CLI** 锁定 / 解锁配置文件。不能在 **WebUI** 上使用此功能。

CLI

锁定配置文件：

exec config lock start

解除文件锁定：

exec config lock end

终止锁定并立即用之前在闪存中锁定的配置文件重启设备：

exec config lock abort

更改缺省锁定期限 (5 分钟):

set config lock timeout <number>

向配置文件添加注释

可以为外部配置文件添加注释。注释可能是一行单独的文本，也可能在一行的结尾处。注释必须以 **#** (井号) 开头，后面接一个空格。注释位于一行的结尾时，还需要在井号前加一个空格。可采用两种方法将文件保存到 **NetScreen** 设备：合并新配置文件与现有配置文件；用新配置文件完全取代现有配置文件。设备分析配置文件时，会查找以井号开头的行，并删除找到的所有注释。

注意：如果井号出现在引号内，**NetScreen** 设备不会将其看作特殊标记，而是当作对象名的一部分，因此不会删除井号。例如，**NetScreen** 设备不会删除命令 **set address trust “#5 server” 10.1.1.5/32** 中的 **“#5 server”**，因为此处的井号出现在引号内。

NetScreen 设备不会将以井号开头的注释保存到闪存的任一 **RAM** 中。例如，假设外部配置文件包含以下各行：

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24 # change IP address
# add new MIP addresses
set interface ethernet3 mip 1.1.1.10 host 10.1.1.10 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.11 host 10.1.1.11 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.12 host 10.1.1.12 netmask 255.255.255.255
# all MIPs use the trust-vr routing domain by default
```

加载文件后，再次查看配置文件时，您会看到以下各行 (注释已不在)：

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 mip 1.1.1.10 host 10.1.1.10 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.11 host 10.1.1.11 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.12 host 10.1.1.12 netmask 255.255.255.255
```

此外，如果粘贴了大段注释 (包括加入控制台会话或 **Telnet** 会话中的注释)，运行命令时，**NetScreen** 设备会立即忽略所有注释。

许可密钥

利用许可密钥功能，无需将 **NetScreen** 设备升级为不同的设备或系统映像，即可对其能力进行扩展。您可以购买一个密钥来解锁固件中已加载的指定功能，比如下面的这些功能：

- 用户容量
- 虚拟系统、区段和虚拟路由器
- HA

每台 **NetScreen** 设备出厂时都已启用了标准功能集，而且可能会支持激活可选功能或提高现有功能的能力。要了解当前都有哪些功能可以进行升级，请参阅 **NetScreen** 的最新市场文献。

获得并应用许可密钥的过程如下：

1. 与向您销售 **NetScreen** 设备的增值转售商 (VAR) 联系，或者直接与 **NetScreen Technologies** 联系。
2. 提供您设备的序列号并说明您想要的功能选项。
生成许可密钥，而后通过电子邮件将其发送给您。
3. 通过 **WebUI** 或 **CLI** 输入该密钥。(参见以下示例。)

范例：扩大用户容量

某家小公司使用了单台 NetScreen 设备，该设备只具有数量为 10 位用户的许可，随着公司的发展，它现在需要一种用户数不受限制的许可。此时，NetScreen 管理员只要获得一个不限制用户数目的固件密钥，即可扩展设备的能力。许可密钥号码为 6a48e726ca050192，该号码在 C:\netscreen\keys 目录下的名为“A2010002.txt”的文本文件中。

WebUI

Configuration > Update > ScreenOS/Keys: 执行下列操作，然后单击 **Apply**:

License Key Update: (选择)

Load File: C:\netscreen\keys\A2010002.txt

或者

单击 **Browse** 找到 C:\netscreen\keys，选择 A2010002.txt，
然后单击 **Open**。

CLI

```
exec license-key capacity 6a48e726ca050192  
reset
```

签名服务的注册与激活

为了让 NetScreen 设备定期收到 AV (防病毒) 模式的签名服务或 DI (深层检测) 签名, 必须先订购服务, 再注册服务, 然后才能收到预订服务。收到预定服务后, 设备上的服务会被激活。服务的激活过程取决于购买服务的方式和服务的具体内容。

临时服务

为确保用户有足够时间订购 AV 或 DI 服务, NetScreen 设备提供了一段临时宽限期。在此期限内, 设备可以获得临时服务。

- 出厂后的 NetScreen 设备一律没有启用 DI 服务。要获得临时 DI 服务, 必须先启动 WebUI 会话, 然后在 Configuration > Update > ScreenOS/Keys 页面上单击 Retrieve Subscriptions Now。随后即可获得期限为一天的一次性 DI 密钥。
- 如果购买设备时捆绑了 AV 服务, 则该设备已预先安装临时服务。

警告: 为避免服务中断, 必须在订购后尽早注册服务。通过注册, 可以确保连续收到订购的服务。

在新设备上捆绑 AV 和 DI 服务

如果新买的 NetScreen 设备自带 AV 和 DI 服务, 请执行以下步骤激活这些服务。

1. 配置设备连接到互联网。(有关说明, 请参阅 NetScreen 设备的 *Getting Started* 手册页和用户指南。)
2. 请在以下站点上注册设备:

www.netscreen.com/cso

绑定了 AV 服务的设备带有一个预先安装的临时预订服务, 从而可以免去安装, 立即使用该服务。但是, 必须先注册设备接收全面付款的预订服务。

3. 恢复设备上的预订服务。可以采取以下两种方法之一：
 - 在 WebUI 中，单击 **Configuration > Update > ScreenOS/Keys** 页面上的 **Retrieve Subscriptions Now**。
 - 使用 CLI 时，请运行以下命令：

```
exec license-key update
```

现在即可配置设备自动恢复或手动恢复签名服务。有关配置 NetScreen 设备执行这些服务的说明，请参阅第 128 页上的“深层检测概述”和第 80 页上的“防病毒扫描”。

与 DI 一起更新 AV 服务

如果在 NetScreen 设备之外单独购买 AV 和 DI 服务，请执行以下步骤激活服务。

1. 订购服务后，您将从 NetScreen 或 NetScreen 授权转销商那里收到支持证书。此证书是一份简单易懂的文档，包含注册设备所需的信息。
2. 请确保设备已注册。如果目前尚未注册，请转到以下站点：
www.netscreen.com/cso
3. 在设备上注册支持证书。
4. 如果只准备订购并注册 DI 服务，请立即进入步骤 5。
如果正准备订购并注册 AV 服务，必须先等待四小时，让系统处理注册，然后再进入步骤 5。
5. 确认设备已连接到互联网。
6. 恢复设备上的预订服务。可以采取以下两种方法之一：
 - 在 WebUI 中，单击 **Configuration > Update > ScreenOS/Keys** 页面上的 **Retrieve Subscriptions Now**。
 - 使用 CLI 时，请运行以下命令：

```
exec license-key update
```

现在即可配置设备自动恢复或手动恢复签名服务。有关配置 NetScreen 设备执行这些服务的说明，请参阅第 128 页上的“深层检测概述”和第 80 页上的“防病毒扫描”。

只更新 DI 服务

如果只购买了 DI 服务，且 NetScreen 设备与 DI 服务分开购买，请执行以下步骤激活服务。

1. 订购服务后，您将从 NetScreen 或 NetScreen 授权转销商那里收到支持证书。此证书是一份简单易懂的文档，包含注册设备所需的信息。
2. 请确保设备已注册。如果目前尚未注册，请转到以下站点：
www.netscreen.com/cso
3. 在设备上注册支持证书。进行下一步之前，可能需要先等待四小时，让系统处理注册。
4. 确认设备已连接到互联网。
5. 恢复设备上的预订服务。可以采取以下两种方法之一：
 - 在 WebUI 中，单击 **Configuration > Update > ScreenOS/Keys** 页面上的 **Retrieve Subscriptions Now**。
 - 使用 CLI 时，请运行以下命令：
`exec license-key update`

现在即可配置设备自动检索或手动检索 DI 签名服务。有关配置 NetScreen 设备执行此服务的说明，请参阅第 128 页上的“深层检测概述”和第 80 页上的“防病毒扫描”。

系统时钟

NetScreen 设备应始终设置成正确的时间，这一点极为重要。在众多因素中，NetScreen 设备上的时间会直接影响 VPN 通道的设置和计划进度的定时。可采取多种方法确保 NetScreen 设备始终保持精确的时间。首先，必须将系统时钟设置成当前时间。接着，可以启用夏令时选项，并配置不超过三个 NTP 服务器（一台主服务器和两台备份服务器），NetScreen 设备将通过这些服务器定期更新系统时钟。

日期和时间

可以使用 WebUI 或 CLI，将时钟设置成当前时间与日期。使用 WebUI 时，会根据计算机时钟同步系统时钟，从而将系统时钟设置成当前时间。

1. Configuration > Date/Time: 单击 **Sync Clock with Client** 按钮。
会弹出一条消息，提示您指定是否已在计算机时钟上启用了夏令时选项。
2. 单击 **Yes** 将同步系统时钟，并根据夏令时调整系统时钟；单击 **No** 只同步系统时钟，不根据夏令时对其进行调整。

使用 CLI 设置时钟时，可以使用命令 “**set clock mm/dd/yyyy hh:mm:ss**” 手动输入日期与时间。

时区

设置时区时，要指定 NetScreen 设备当地时间早于或晚于 GMT（格林威治标准时间）的小时数。例如，如果 NetScreen 设备的当地时区是“太平洋标准时间”，则它要比 GMT 时间晚 8 小时。因此必须将时钟设置为 **-8**。

如果使用 WebUI 设置时区：

Configuration > Date/Time > Set Time Zone_hours_minutes from GMT

如果使用 CLI 设置时区：

```
ns -> set clock timezone number ( -12 到 12 之间的数字 )
```

或

```
ns-> set ntp timezone number ( -12 到 12 之间的数字 )
```

NTP

为确保 NetScreen 设备始终保持正确时间，可以使用 NTP (网络时间协议) 通过互联网来同步系统时钟与 NTP 服务器的时钟。您可以手动同步，也可以配置 NetScreen 设备在指定的时间间隔自动执行同步。

多个 NTP 服务器

一台 NetScreen 设备上最多可以配置三台 NTP 服务器：一台主服务器和两台备份服务器。如果配置 NetScreen 设备自动同步系统时钟，设备会按顺序查询配置的 NTP 服务器。设备总是最先查询主 NTP 服务器。如果查询失败，设备会继续查询第一台备份 NTP 服务器，依此类推，直到从 NetScreen 设备上配置的某台 NTP 服务器那里得到有效回复。对于每台 NTP 服务器，设备最多尝试四次查询。如果仍得不到有效回复，设备将终止更新，并在日志中留下失败记录。

手动同步系统时钟时，只能使用 CLI，可以指定特定的 NTP 服务器，也可以一个都不指定。如果指定了 NTP 服务器，NetScreen 设备会只查询该服务器。如果不指定 NTP 服务器，NetScreen 设备将按顺序查询设备上配置的每台 NTP 服务器。可以使用服务器的 IP 地址或域名指定 NTP 服务器。

最大时间调整

对于自动同步，可以指定最大时间差值 (单位为秒)。最大时间差值是指 NetScreen 设备系统时钟与收到的 NTP 服务器时间之间允许的时间差。仅当设备时钟与 NTP 服务器时间的时间差小于设置的最大时间差值时，NetScreen 设备才会按照 NTP 服务器的时间调整时钟。例如，假设最大时间差值为 3 秒，设备系统时钟的时间为 4:00:00，NTP 服务器发送的时间为 4:00:02，由于两者之间的时间差在允许范围内，因此 NetScreen 设备会更新其时钟。如果时间差大于设定值，NetScreen 设备不会同步时钟，而是继续试着查询设备上配置的第一个 NTP 服务器。如果尝试查询所有配置的 NTP 服务器之后，NetScreen 设备仍未收到有效回复，设备会在事件日志中生成一条错误消息。

此功能的缺省值为 3 秒，取值范围从 0 (无限制) 到 3600 (一小时)。

手动同步系统时钟时，只能使用 CLI，此时 NetScreen 设备不验证最大时间调整值。反之，NetScreen 设备收到有效值后，会显示一条消息，通知您访问的 NTP 服务器、时间差以及使用的验证方法类型。该消息还会要求您确认或取消对系统时钟的更新。

如果 NetScreen 设备收不到回复，则会显示超时消息。仅当 NetScreen 设备尝试访问设备上配置所有的 NTP 服务器失败后，才会出现此消息。

注意：使用 CLI 发出请求时，在键盘上按下 Ctrl-C 后，可以取消当前请求。

NTP 与 NSRP

“NetScreen 冗余协议” (NSRP) 中包含一种机制，用于同步 NSRP 集群成员的系统时钟。尽管同步操作以秒为单位，但 NTP 服务器却采用次秒级的定时机制。由于处理延迟，可能导致每个集群成员的时间相差几秒。当两个集群成员同时启用 NTP 时，NetScreen 设备会建议您禁用 NSRP 时间同步，因为这两个成员要通过 NTP 服务器更新各自的系统时钟。要禁用 NSRP 时间同步功能，请输入以下命令：

```
set ntp no-ha-sync
```

范例：配置 NTP 服务器和最大时间差值

在下例中，将配置 NetScreen 设备通过 NTP 服务器每隔五分钟更新一次时钟，NTP 服务器的 IP 地址为 1.1.1.1、1.1.1.2 和 1.1.1.3。还需将最大时间差值设置为 2 秒。

WebUI

Configuration > Date/Time: 输入以下内容，然后单击 **Apply**:

Automatically synchronize with an Internet Time Server (NTP): (选择)

Update system clock every minutes: 5

Maximum time adjustment seconds: 2

Primary Server IP/Name: 1.1.1.1

Backup Server1 IP/Name: 1.1.1.2

Backup Server2 IP/Name: 1.1.1.3

CLI

```
set clock ntp
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp interval 5
set ntp max-adjustment 2
save
```

保护 NTP 服务器

可以使用基于 MD5 的校验和算法验证 NTP 封包，以此来保护 NTP 信息流。同时不需要创建 IPSec 通道。这种验证方法能确保 NTP 信息流的完整性。该方法不能阻止外来者查看数据，但可以防止任何人篡改数据。

要启用 NTP 信息流的验证机制，必须为 NetScreen 设备上配置的每个 NTP 服务器分配唯一的密钥 ID 和预共享密钥。密钥 ID 和预共享密钥用于生成校验和，NetScreen 设备和 NTP 服务器通过校验和来验证数据。

验证类型

NTP 信息流有两种验证方法：必需验证和首选验证。

选择 **Required** 验证后，NetScreen 设备必须在发送给 NTP 服务器的所有封包中加入验证信息 (密钥 ID 和校验和)，还必须验证从 NTP 服务器接收的所有 NTP 封包。NetScreen 设备和 NTP 服务器的管理员必须先交换密钥 ID 和预共享密钥，然后才能验证 NetScreen 设备与 NTP 服务器之间往来的信息流。必须手动交换验证信息，例如采取电子邮件、电话等不同方法。

选择 **Preferred** 验证后，NetScreen 设备必须先以 Required 模式运行，然后才能尝试验证所有 NTP 信息流。如果所有验证尝试都失败，NetScreen 设备将返回正常模式运行。同时向 NTP 服务器发送一个不含密钥 ID 和校验和的封包。实际上，尽管 NetScreen 设备会优先执行验证，但即使验证失败，设备仍允许 NTP 信息流的往来流通。

索引

A

- admin 用户 481–482
 - auth 过程 482
 - 超时 394
 - 服务器支持 388
 - 来自 RADIUS 的权限 481
- ALG 175
 - 对于定制服务 223
- ARP 111
 - 入口 IP 地址 114
- auth 服务器 388
 - 备份服务器 393
 - 策略中 412
 - 超时 393
 - 地址 393
 - 定义 404–412
 - 对象名 393
 - 对象属性 393
 - 多种用户类型 389
 - 功能支持 388
 - ID 号 393
 - IKE 网关中 412
 - LDAP 402–403
 - LDAP, 定义 409
 - 类型 393
 - 缺省 411
 - RADIUS 395–397
 - RADIUS, 定义 404
 - RADIUS, 用户类型支持 396
 - 认证过程 392
 - SecurID 400–401
 - SecurID, 定义 407
 - 外部 392
 - XAuth 查询 453
 - 用户类型支持 388
 - 最大数量 389
- auth 用户 414–446
 - 策略前认证 228, 416
 - 策略中 414
 - 超时 393
 - 服务器支持 388

- 认证点 413
- WebAuth 228, 416
- WebAuth + SSL (外部用户组) 443
- WebAuth (本地用户组) 436
- WebAuth (外部用户组) 439
- 运行时认证 227, 415
- 运行时认证过程 227, 415
- 运行时 (本地用户组) 422
- 运行时 (本地用户) 419
- 运行时 (外部用户) 425
- 执行时 (外部用户组) 428
- 组 414, 418
- 安全区 2
 - global 2
 - 接口 3, 68
 - 目的区段确定 13
 - 物理接口 68
 - 预定义的 2
 - 源区段确定 12
 - 子接口 68

B

- 报警
 - 临界值 229
- 被遮盖的策略 258
- 本地数据库 390–391
 - 超时 391
 - IKE 用户 447
 - 支持的用户类型 390
- 编辑
 - 策略 257
 - 地址组 148
 - 区段 52
- 标题, 定制 492

C

- CHAP 469
- CLI
 - set arp always-on-dest 85, 91
 - set vip multi-port 374

- 约定 x
- 策略 3
 - 安全区 222
 - 报警 229
 - 必要元素 215
 - 策略环境 251
 - 策略验证 258
 - 策略组列表 218
 - 查询顺序 218
 - DIP 组 206
 - 地址 222
 - 地址排除 253
 - 地址组 222
 - 定位在顶部 225, 259
 - 动作 223
 - 防病毒扫描 230
 - 服务 222
 - 服务簿 150
 - 服务于 150, 222
 - 服务组 183
 - 根系统 219
 - 更改 257
 - 功能 213
 - 管理 232
 - 管理带宽 494
 - HA 会话备份 228
 - ID 222
 - 计数 229
 - 禁用 257
 - 拒绝 223
 - L2TP 225
 - L2TP 通道 225
 - 类型 216–217
 - 每个组件含多个条目 252
 - 名称 224
 - NAT-dst 226
 - NAT-src 226
 - 内部规则 219
 - 启用 257
 - 区段内部 216, 217, 233, 234, 239, 247
 - 全局 217, 233, 250
 - 认证 226

- 深层检测 225
- 时间表 230
- 双向 VPN 224, 232
- 顺序 259
- 通道 223
- 图标 232
- VPN 224
- VPN 拨号用户组 222
- URL 过滤 229
- 位置 234
- 信息流记录 229
- 信息流整形 231
- 虚拟系统 219
- 移除 260
- 应用 223
- 允许 223
- 遮盖 258
- 重新排序 259
- 最大限制 146
- 插图
 - 约定 xiii
- 差异服务 231
- 超时
 - admin 用户 394
 - auth 用户 393
- 创建
 - 地址组 147
 - 服务组 184
 - MIP 地址 349
 - 区段 51
- 词典文件 481
- 存取策略
 - 请参阅策略

D

- DHCP 131, 137, 537
 - 服务器 516
 - HA 524
 - 客户端 516
 - 中继代理 516
- DiffServ
 - 请参阅DS 码点标记
- DIP 135, 187–190
 - 池 226
 - 固定端口 189

- PAT 188
 - 修改 DIP 池 190
 - 组 205–208
- DIP 池
 - 大小 275
 - 地址注意事项 275
 - NAT-src 262
- DNS 511
 - 查找 512
 - 服务器 539
 - 状态表 513
- DS 码点标记 494, 503, 504
- DSL 533, 538
- 带宽
 - 保证的 494, 502
 - 管理 494
 - 缺省优先级 501
 - 未限定最大值 494
 - 优先级 501
 - 优先级排列 501
 - 最大 231, 502
 - 最大规格 494
- 地址
 - 策略中 222
 - 公开 79
 - 私有 80
 - 通讯簿条目 143
 - 已定义 222
- 地址排除 253
- 地址转换
 - 请参阅NAT、NAT-dst 和 NAT-src
- 地址组 145, 222
 - 编辑 148
 - 创建 147
 - 选项 146
 - 移除条目 149
- 订购
 - 临时服务 554
 - 注册与激活 554–556
- 定义
 - 区段 51
- 动态 IP 池
 - 请参阅DIP 池
- 动态路由 30
- 端口
 - 端口号 382

- 端口地址转换
 - 请参阅PAT
- 端口模式 55–65
- 端口映射 265, 292
- 多类型用户 483
- 多媒体会话, SIP 172

E

- 二级 IP 地址 101

F

- 防病毒扫描
 - 策略 230
- 封包流 11–13
 - NAT-dst 294–297
- 服务 150
 - 策略中 222
 - 超时临界值 151
 - 定制 ALG 223
 - ICMP 155
 - 下拉式列表 150
 - 修改超时 152
 - 已定义 222
- 服务簿
 - 定制服务 150
 - 定制服务 (CLI) 152
 - 服务组 (Web 用户界面) 183
 - 添加服务 152
 - 修改条目 (CLI) 154
 - 修改条目 (Web 用户界面) 185
 - 移除条目 (CLI) 154
 - 预配置服务 150
- 服务组 183–186
 - 创建 184
 - 删除 186
 - 修改 185

G

- global 区段 375
- 高可用性
 - 请参阅HA
- 公开地址 79
- 功能区段接口 70

- 管理接口 70
- HA 接口 70
- 供应商专用属性
 - 请参阅 VSA
- 固件
 - 上传和下载 546
- 管理接口
 - 请参阅 MGT 接口
- 关守设备 157
- 规则，源自策略 219

H

- H.323 协议 157
- HA
 - DHCP 524
 - 虚拟 HA 接口 70
 - 另请参阅 NSRP
- Home 区段 62
- 回滚，配置 547–548
- 会话超时
 - 空闲超时 393
- 会话启动协议
 - 请参阅 SIP
- 回传接口 103

I

- ICMP 服务 155
 - 消息代码 155
 - 消息类型 155
- IKE
 - IKE ID 447, 468
 - 用户 447–451
 - 用户组，定义 450
 - 用户，定义 448
 - 用户，组 447
- IKE 用户
 - 服务器支持 388
 - IKE ID 413, 447
 - 与其它用户类型 483
- IP
 - 跟踪地址 84
- IP 池
 - 请参阅 DIP 池
- IP 地址

- 第 3 层安全区 79–80
- 定义每一个端口 143
- 二级 101
- 公开 79
- 接口上的跟踪 84
- 私有 79
- 私有地址范围 80
- 网络 ID 80
- 虚拟 372
- 主机 ID 80
- IP 跟踪
 - 出口接口上的失败 86–88
 - 入口接口上的失败 89–92
 - 重新路由信息流 84–92
- IP 语音通信 157

J

- 记录 229
- 计数 229
- 基于策略的 NAT
 - 请参阅 NAT-dst 和 NAT-src
- 通道接口 71
- 接口
 - 绑定到区段 78
 - 编址 79
 - 查看接口表 76
 - 从区段解除绑定 82
 - DIP 187
 - 第 3 层安全区 79
 - 二级 IP 地址 101
 - 跟踪 IP 地址 84
 - HA 70
 - 回传 103
 - IP 跟踪 84
 - 聚合 69
 - MGT 70
 - MIP 347
 - 缺省 81
 - 冗余 69
 - 通道 49, 71, 71–75
 - VIP 372
 - VSI 69
 - 物理 3
 - 修改 83
 - 虚拟 HA 70

- 静态路由 30, 33–44
 - 配置 38
 - 使用 36
- 聚合接口 69

K

- 空闲会话超时 393

L

- L2TP
 - 本地数据库 477
 - 策略 225
 - 地址分配 476
 - 外部 auth 服务器 477
 - 用户认证 476
 - L2TP 用户 476–480
 - 服务器支持 388
 - 认证点 413
 - 与 XAuth 483
- LDAP 402–403
 - auth 服务器对象 409
 - 服务器端口 403
 - 结构 402
 - 通用名称标识符 403
 - 识别名称 403
 - 支持的用户类型 403
- LKG 配置 547
- LKG（上次已知正确） 547
- 历史记录图表 229
- 令牌代码 400
- 路由 30
- 路由表 31
- 路由模式 134–139
 - 接口设置 135
- 路由选择
 - 二级 IP 地址之间 101

M

- MGT 接口 70
- MIP 12, 347
 - 创建地址 349
 - 从其它区段可到达 352
 - 地址范围 351

- 定义 268
- global 区段 348
- 流向带有基于接口的 NAT 的区段 128
- 缺省网络掩码 351
- 缺省虚拟路由器 351
- same-as-untrust 接口 358–361
- 双向转换 268
- 在区段接口上创建 349
- 在通道接口上创建 357

名称

- 约定 xiv

N

NAT

- 定义 262
- NAT-src 与 NAT-dst 326–346

NAT 模式 126–133

- 接口设置 129
- 流向 Untrust 区段的信息流 107, 128

NAT-dst 292–346

- 带有端口映射的单个 IP 地址 271
- 单个 IP, 无端口映射 271
- 单向转换 268, 273
- 地址变换 267, 293, 316
- 地址范围 266
- 地址范围到单个 IP 地址 272, 311
- 地址范围到地址范围 272, 316
- 端口映射 265, 292, 321
- 封包流 294–297
- 路由注意事项 293, 298–301
- 一对多转换 307
- 一对一转换 302
- 与 MIP 或 VIP 一起 264

NAT-src 262, 275–291

- 出口接口 270, 289–291
- DIP 池 262
- DIP 池, 固定端口 269
- 带有 PAT 的 DIP 池 269, 276–279
- 带有地址变换的 DIP 池 270
- 单向转换 268, 273
- 地址变换 283–288
- 地址变换, 范围注意事项 283
- 端口地址转换 263
- 固定端口 275, 280–282
- 基于接口 263

- 路由模式路由模式
- NAT-src 134

NetInfo 517

NetScreen 词典文件 397

NSRP

- DHCP 524
- DIP 组 205–208
- HA 会话备份 228
- NTP 同步 559
- 配置回滚 549
- 冗余接口 69
- VSI 69

NTP 558–561

- 保护服务器 561
- 多台服务器 558
- 服务器 558
- 服务器配置 560
- NSRP 同步 559
- 验证类型 561
- 最大时间调整 558

P

PAT 188, 275

PC 卡 546

排除, 地址 253

配置

- 回滚 547–548, 549
- 加载 549
- LKG 547
- 锁定 550
- 添加注释 551

Q

QoS 494

轻量目录访问协议

请参阅 LDAP

区段 45–54

- 安全 48
- 第 2 层 109
- global 375
- 功能 54
- 全局 48
- 通道 49
- VLAN 54, 109

R

RADIUS 395–397

- auth 服务器对象 404
- 端口 396
- 对象属性 396
- 共享机密 396
- NetScreen 词典文件 481
- 重试超时 396

RFC

- 1349, “Type of Service in the Internet Protocol Suite” 231
- 1777, “Lightweight Directory Access Protocol” 402
- 1918, “Address Allocation for Private Internets” 80
- 2474, “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers” 231

RSH ALG 156

认证

- Allow Any 228
- 策略 226
- WebAuth 416
- 用户 226, 387–492

认证, 用户 387–492

- admin 481
- auth 服务器 388
- auth 用户 414
- 本地数据库 390–391
- 多类型 483
- IKE 用户 388, 447
- L2TP 用户 476
- 类型和应用 413–483
- 配置文件 387
- 认证点 413
- 使用不同登录 483
- 手动密钥用户 388
- WebAuth 388
- XAuth 用户 452
- 用户类型 388
- 帐户 387

软件

- 更新 546
- 上传和下载 546

S

SCREEN

MGT 区段 48

ScreenOS

安全区 2, 48

安全区接口 3

安全区, 全域 2

安全区, 预定义 2

策略 3

端口模式 55

封包流 11–13

global 区段 48

概述 1–27

更新 546

功能区段 54

Home-Work 区段 62

区段 45–54

通道区段 49

物理接口 3

虚拟系统 10

子接口 4

SDP 175–176

SecurID 400–401

ACE 服务器 400

auth 服务器对象 407

加密类型 401

客户端超时 401

客户端重试次数 401

令牌代码 400

强迫 401

认证端口 401

认证器 400

用户类型支持 401

SIP 172–182

ALG 175, 179

多媒体会话 172

会话静止超时 179

静止超时 179

连接信息 176

媒体静止超时 179, 182

媒体声明 176

请求方法 173

请求方法的类型 173

RTCP 176

RTP 176

SDP 175–176

响应 173

响应代码 174

响应类型 173

消息 172

信号发送 175

信号发送静止超时 179, 182

已定义 172

针孔 175

SSL

与 WebAuth 443

上次已知正确的配置

请参阅 LKG 配置

上次已知正确的配置文件

请参阅 LKG 配置文件

设置

保存 544

导入 544

识别名称 403

时间表 209, 230

时区 557

时钟, 系统 557–561

请参阅 系统时钟

私有地址 80

T

TFTP 服务器 546

trace-route 114, 117

通道接口 71

定义 71

基于策略的 NAT 71

通讯簿

编辑组的条目 148

另请参阅地址

添加地址 143

条目 143

修改地址 144

移除地址 149

组 145

通用名称 403

透明模式 108–125

ARP/trace-route 112

泛滥 112

广播信息流 110

路由 110

unicast 选项 112

阻止非 ARP 信息流 110

阻止非 IP 信息流 110

图标

策略 232

已定义 232

图表, 历史记录 229

U

URL 过滤 229

V

VIP 12

必需的信息 373

编辑 378

从其它区段可到达 375

定义 268

定制服务, 低端口号 373

定制和多端口服务 379–385

global 区段 375

流向带有基于接口的 NAT 的区段 128

配置 375

双向转换 268

移除 378

VLAN

标记 4

VLAN 区段 109

VLAN1

接口 109, 118

区段 109

VPN

策略 224

空闲时间 455

流向带有基于接口的 NAT 的区段 128

通道区段 49

VR 35

简介 5

转发信息流的范围 5

VSA 397

供应商 ID 397

属性编号 397

属性类型 397

属性名 397

W

WebAuth 388

- 本地用户组 436
- 策略前认证进程 228, 416
- 外部用户组 439
- 与 SSL（外部用户组） 443

WebUI

- 约定 xi

Work 区段 62

网络掩码 222

- 用途 80

网络, 带宽 494

未知 Unicast 选项 111–117

- ARP 114–117
- 泛滥 112–113
- trace-route 114, 117

X

XAuth

- auth 和地址 468
- 本地用户 auth 456
- 本地用户组 auth 458
- 查询远程设置 453
- 地址超时 454
- 地址分配 452, 454
- IP 地址生存期 454–455
- 客户端认证 474
- ScreenOS 作为客户端 474
- 生存期 455
- TCP/IP 分配 453
- VPN 空闲时间 455
- 外部 auth 服务器查询 453
- 外部用户 auth 460
- 外部用户组 auth 463
- 虚拟适配器 452
- 已定义 452
- 用户认证 452

XAuth 用户 452–474

- 服务器支持 388
- 认证点 413
- 与 L2TP 483
- 系统时钟 557–561
- 日期和时间 557
- 时区 557
- 与客户端同步 557

系统, 参数 509–560

信息流

- 记录 229
- 计数 229
- 整形 494
- 信息流整形 493–507
- 服务优先级 501
- 接口要求 494
- 自动 494

许可密钥 552–553

虚拟 HA 接口 70

虚拟 IP

请参阅 VIP

虚拟路由器

请参阅 VR

虚拟适配器 452

虚拟系统 10

Y

映射 IP

请参阅 MIP

应用, 策略中 223

用户

IKE 447–451

IKE, 组 450

组, 服务器支持 388

用户认证

请参阅 认证, 用户

用户, admin 481–482

auth 过程 482

超时 394

用户, IKE

定义 448

IKE ID 447

组 447

用户, L2TP 476–480

用户, XAuth 452–474

优先级排列 501

域名系统

请参阅 DNS

远程认证拨号的用户服务

请参阅 RADIUS

约定

CLI x

插图 xiii

名称 xiv

WebUI xi

运行时认证 227, 415

Z

针孔 177

支持证书 555, 556

字符类型, ScreenOS 支持的 xiv

子接口 4

创建（根系统） 99

删除 100

组

地址 145

服务 183

组表达式 484–491

服务器支持 388

其它组表达式 485

用户 484

用户组 484

运算符 484