NetScreen 概念与范例

ScreenOS 参考指南

第 7 卷：地址转换

ScreenOS 5.1.0

编号 093-1372-000-SC

修订本 B

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

第 7 卷，“地址转换”重点介绍 ScreenOS 中可用于执行地址转换的各种方法。本卷包含以下章节，介绍如何配置 NetScreen 设备以执行以下类型的转换：

- 第 1 章，地址转换 – 概述各种转换选项，在随后的章节中将详细介绍这些选项。
- 第 2 章，源网络地址转换 – (NAT-src) 数据包包头中的源 IP 地址的转换 [包括和不包括端口地址转换 (PAT)]。
- 第 3 章，目标网络地址转换 – (NAT-dst) 数据包包头中的目标 IP 地址转换 (包括和不包括目标端口地址映射)。本节还将介绍有关执行 NAT-src、路由选择注意事项及地址变换时的数据包流的信息。
- 第 4 章，映射和虚拟 IP 地址 – 仅基于 IP 地址 (映射 IP) 或基于目标 IP 地址及目标端口号 (虚拟 IP) 将一个目标 IP 地址映射到另一个地址。

注意：*有关基于接口的网络源地址转换 (简称 NAT) 的内容，请参阅第* ***2*** *-122 页上的 “NAT 模式”。*

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

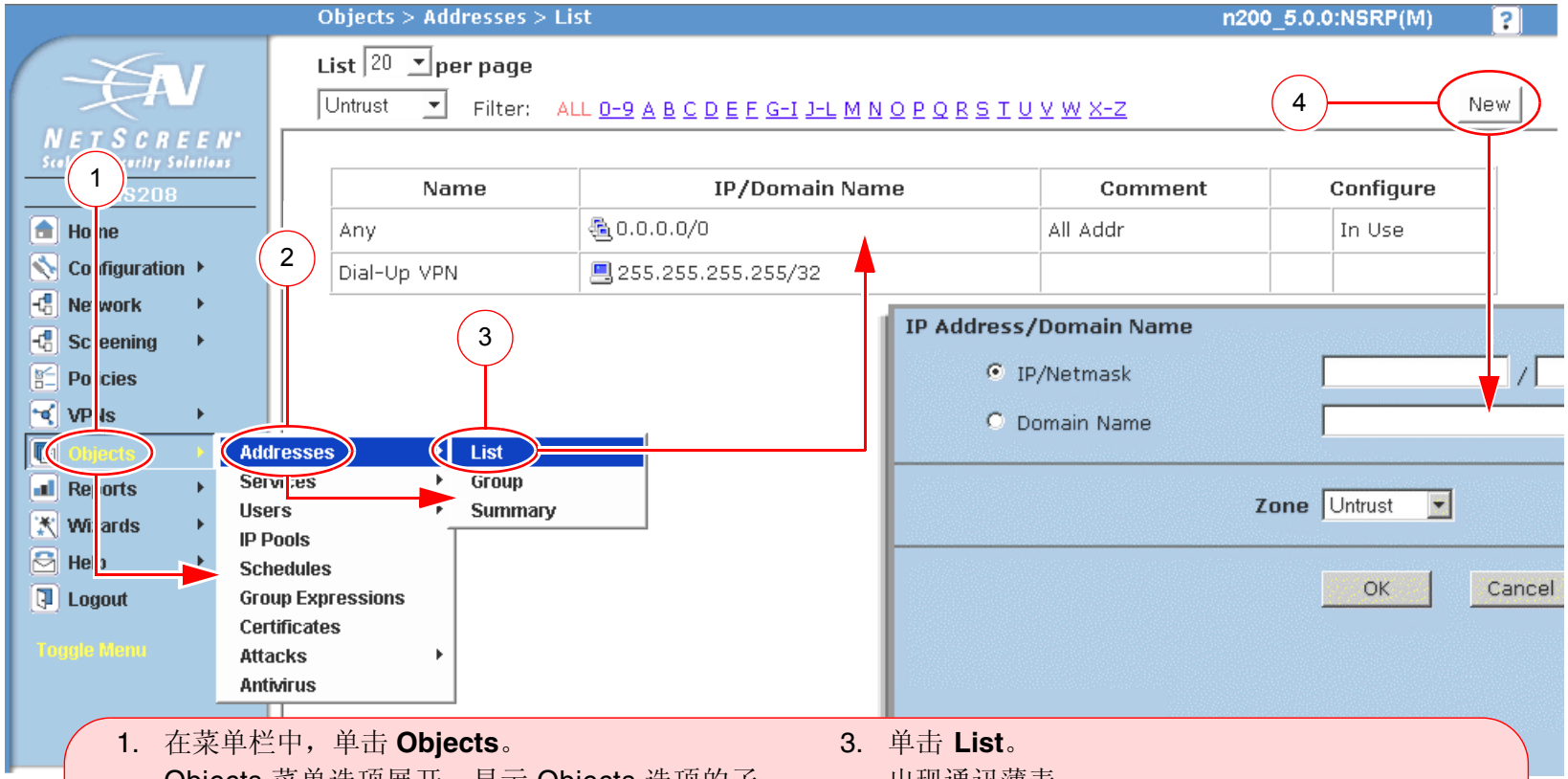
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

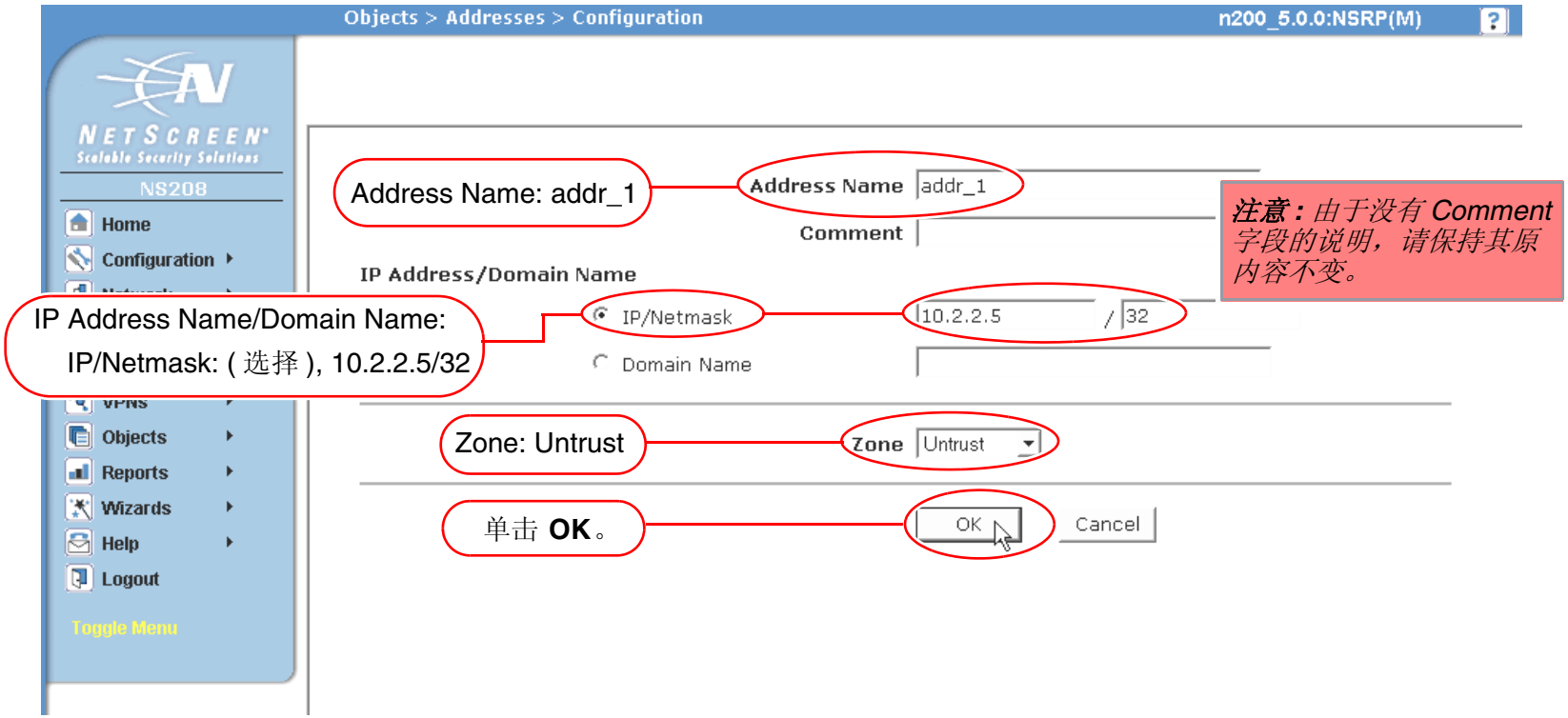
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

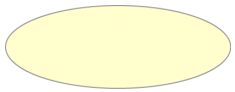


插图约定

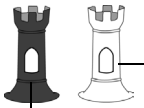
下列图形构成了贯穿本书的插图所用的基本图像集：

通用 NetScreen 设备

虚拟路由选择域



安全区段



安全区段接口

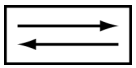
白色 = 受保护区段接口
（例如：Trust 区段）

黑色 = 区段外接口
（例如：Untrust 区段）

通道接口

VPN 通道

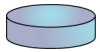
路由器图标



交换机图标

包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）

互联网



动态 IP (DIP) 池

台式计算机

便携式计算机

通用网络设备
（例如：NAT 服务器，
接入集中器）

服务器

命名约定和字符类型

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

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

ScreenOS 支持以下字符类型 :

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

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

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

JUNIPER NETWORKS NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

地址转换

NetScreen 提供了许多执行源与目标 IP 地址、源与目标端口地址转换的方法。本章介绍几种可用的地址转换方法，分为以下几个部分：

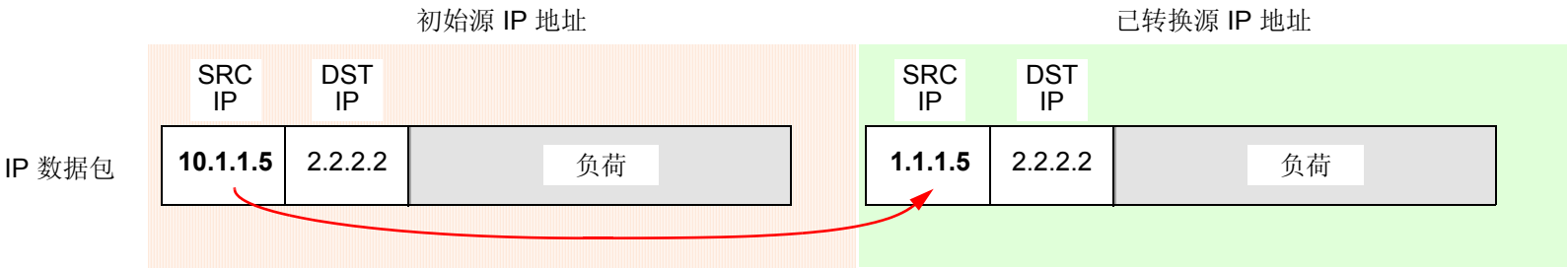
地址转换简介

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 数据包包头中的 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)、目标地址 (以及可选的目标端口号) 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 设备会将所有数据包中的源 IP 地址转换成该接口的 IP 地址。您可以配置 NetScreen 设备，以便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 NAT[2]。(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 **2**-122 页上的 “NAT 模式” 。有关 DIP 池的详细信息，请参阅第 **2**-267 页上的 “DIP 池”。)

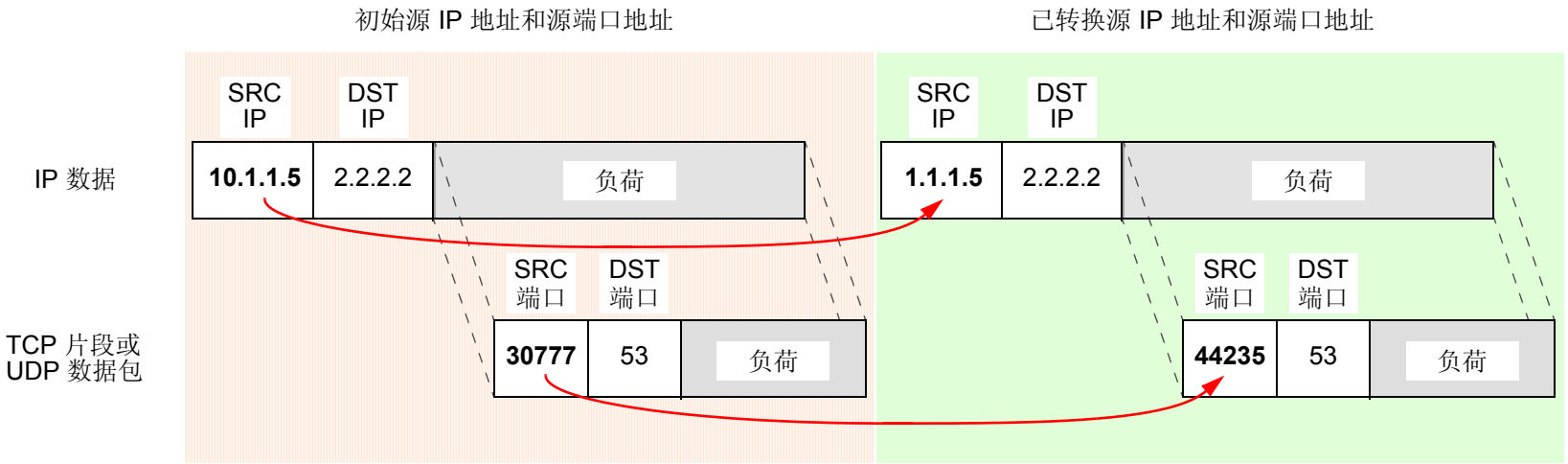
源 IP 地址转换



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 24 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 68 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信息流流入、流出同一个 IP 地址的会话状态信息。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 地址转换成同一个已转换 IP 地址 (来自出口接口)，因此 NetScreen 设备使用已转换端口号标识数据包所属的每个会话。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，则需要使用 PAT。

源 IP 地址转换和源端口地址转换



3. 启用 PAT 后， NetScreen 设备会维护空闲端口号池，将这些端口号与 DIP 池中的地址一起分配。用最大端口数 65,535 减去 1023 (这些端口号保留用于众所周知的端口)，可得到数字 64,500。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 设备会将多达 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。

如果定制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 15 页上的 “源网络地址转换”。*

目标网络地址转换

NetScreen 提供以下三种机制执行目标网络地址转换 (NAT-dst):

- 基于策略的 NAT-dst
- 映射 IP (MIP)
- 虚拟 IP (VIP)

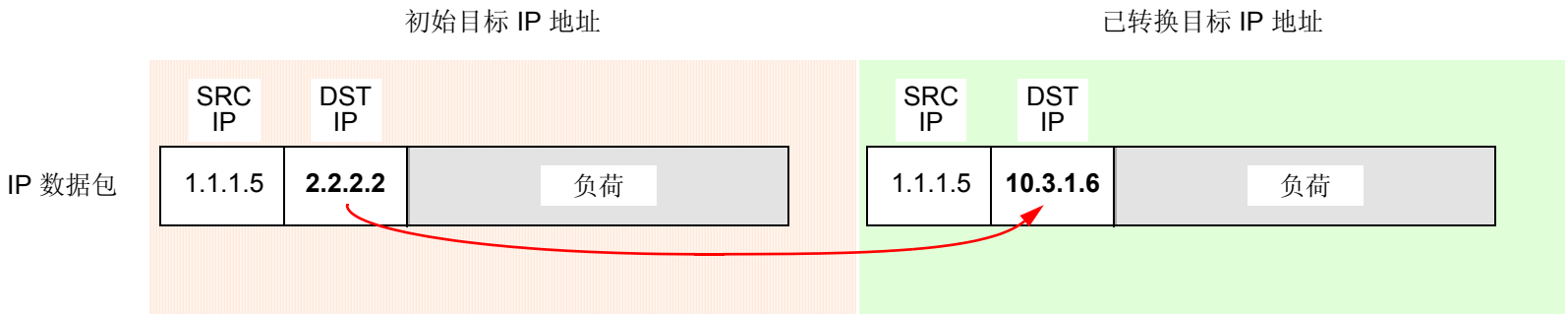
这三个选项都会将 IP 数据包包头中的初始目标 IP 地址转换成不同的地址。使用基于策略的 NAT-dst 和 VIP 时，还可以启用端口映射[4]。

***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 设备偶然被配置为将 MIP 和 VIP 及基于策略的 NAT-dst 应用于同一信息流，则 MIP 和 VIP 将禁用基于策略的 NAT-dst。*

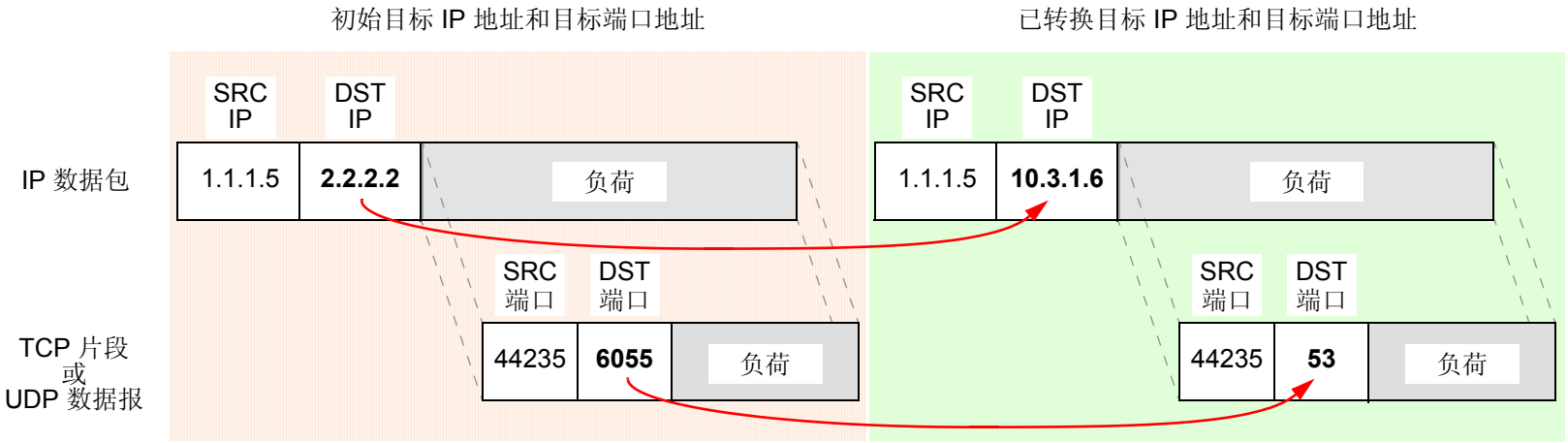
4. 有关端口映射的信息，请参阅下一页上的 “基于策略的 NAT-Dst”以及第 33 页上的 “目标网络地址转换”。

基于策略的 NAT-Dst: 您可以配置策略，将一个目标 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。将单个目标 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，无论是否使用端口映射， NetScreen 均支持 NAT-dst。端口映射是明确的转换，即将一个初始目标端口号转换成另一个特定端口号。它与 PAT 不同，后者将任意初始源端口号 (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)。

不使用目标端口映射的目标 IP 地址转换

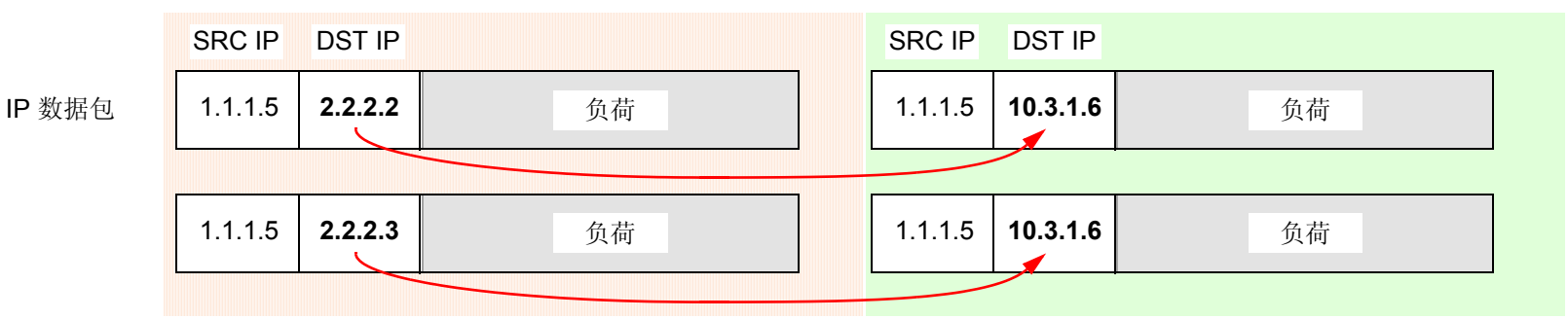


使用目标端口映射的目标 IP 地址转换

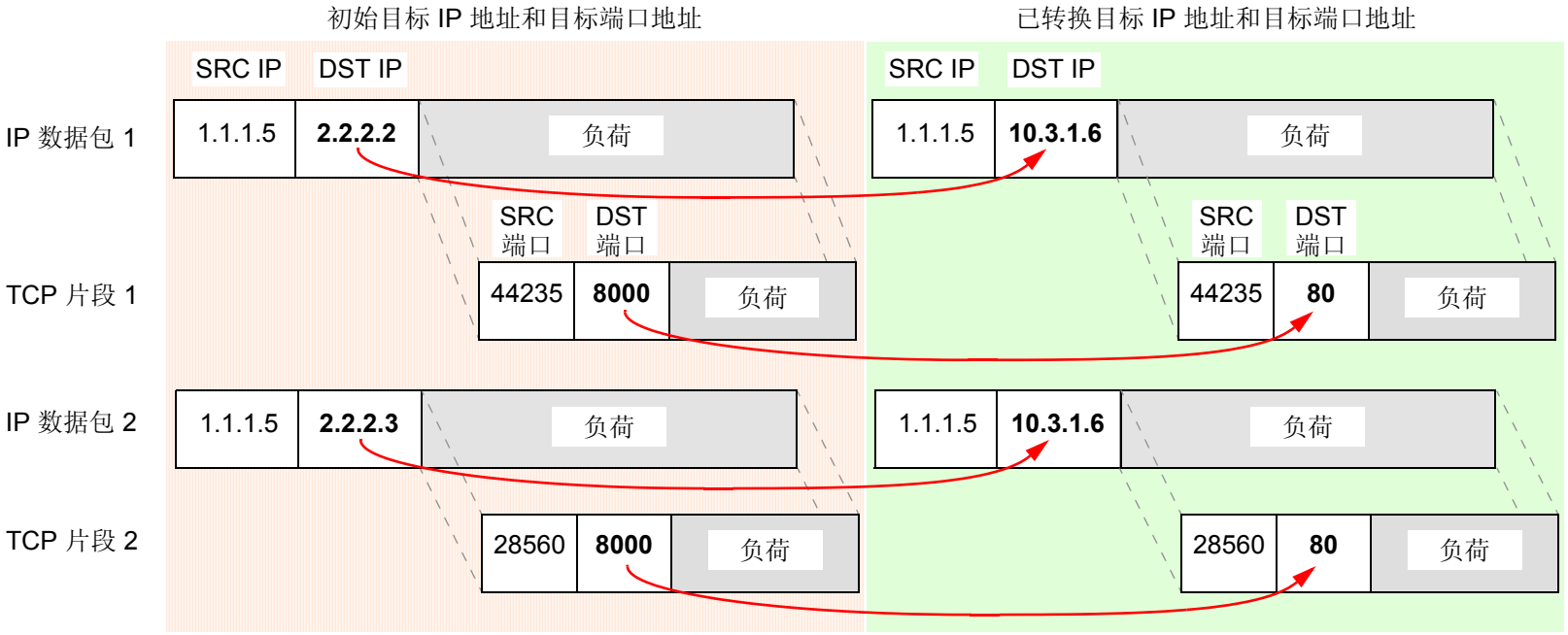


如果将策略配置为执行 NAT-dst 以将地址范围转换成单个地址，则 NetScreen 设备会将用户定义的初始目标地址范围内的所有目标 IP 地址转换成单个地址。还可以启用端口映射。

从 IP 地址范围到单个 IP 地址的目标 IP 地址转换

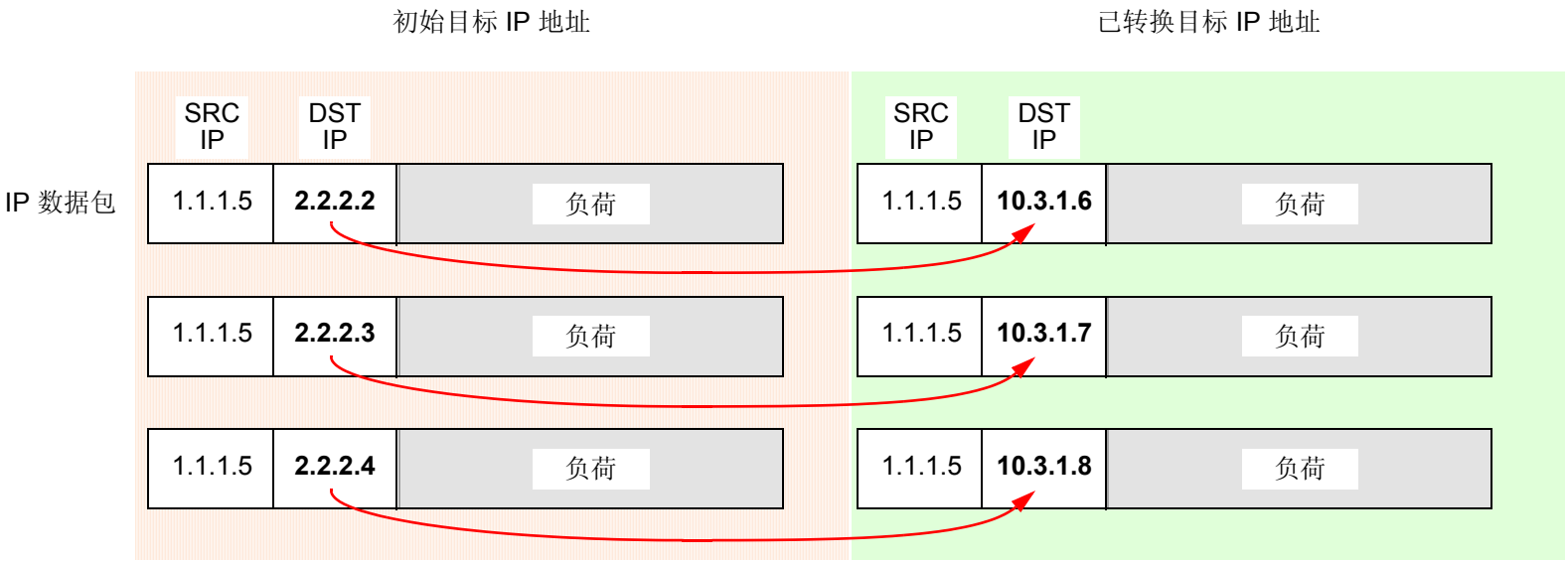


使用目标端口映射从 IP 地址范围到单个 IP 地址的目标 IP 地址转换



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标地址范围内的目标 IP 地址转换成另一地址范围内的已知地址。

使用地址变换的目标 IP 地址转换



执行 IP 地址范围的 NAT-dst 时，NetScreen 设备会始终将一个地址范围内的每个 IP 地址映射到另一地址范围内的对应 IP 地址。

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 zone 1 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 13 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 33 页上的 “目标网络地址转换”。*

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 90 页上的 “映射 IP 地址”。

VIP: VIP 是从一个 IP 地址到基于目标端口号的另一个 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 (使用不同的目标端口号标识) 到同样多主机[5]的映射。VIP 还支持端口映射。与 MIP 不同，VIP 的地址转换将单向执行。 NetScreen 设备可以将到达 VIP 地址的所有信息流中的目标 IP 地址转换成主机 IP 地址。(NetScreen 设备将仅检查目标 IP 地址是否被绑定至 VIP，该 VIP 位于到达已绑定到 Untrust 区段的接口的数据包上。) NetScreen 设备不会将 VIP 主机的出站信息流中的初始源 IP 地址转换成 VIP 地址的初始源 IP 地址。相反，如果先前进行了配置，则 NetScreen 设备将应用基于接口或基于策略的 NAT-src。否则， NetScreen 设备将不会对 VIP 主机发出的信息流执行任何 NAT-src。有关 VIP 的详细信息，请参阅第 115 页上的 “虚拟 IP 地址”。

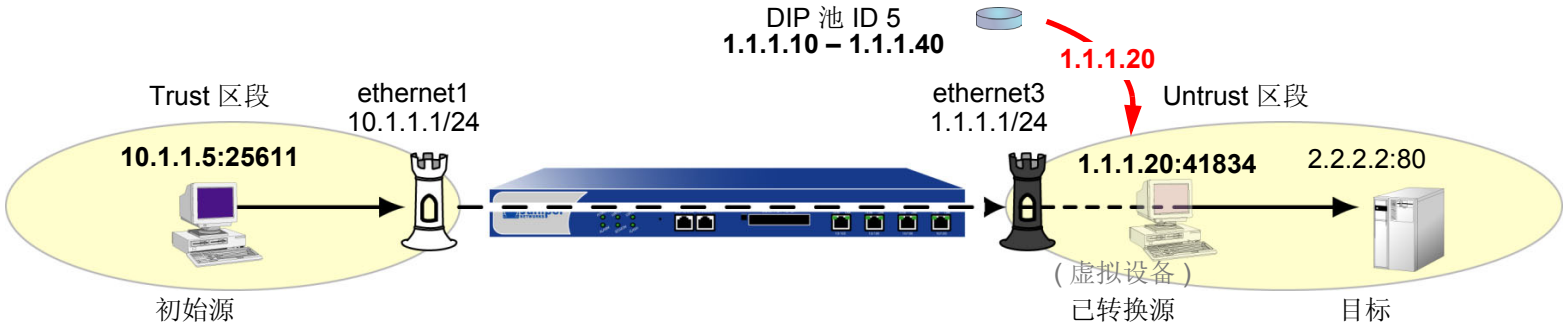
虽然 MIP 和 VIP 的地址转换机制是双向的，但基于策略的 NAT-src 和 NAT-dst 能够将入站和出站信息流的地址转换分开，以提供较好的控制与安全性。例如，如果在 Web 服务器上使用 MIP，则每当服务器发起出站信息流以获取更新或补丁程序时，其活动都会被公开，这样就将信息提供给警觉的攻击者，供其进行攻击。利用基于策略的地址转换方法，可以在 Web 服务器 (使用 NAT-dst) 接收信息流而不是 (使用 NAT-src) 发出信息流时定义不同的地址映射。这样可以使服务器的活动处于隐藏状态，防止他人收集信息趁机攻击，从而更好地保护服务器。在此版 ScreenOS 中，基于策略的 NAT-src 和 NAT-dst 各提供一种方法，可结合使用并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。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

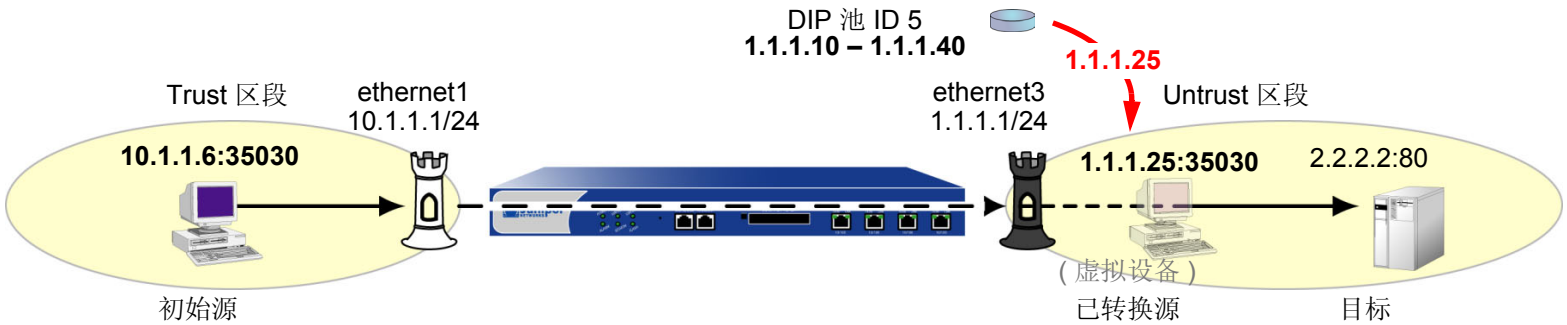
NetScreen 提供以下几种应用源网络地址转换 (NAT-src) 和目标网络地址转换 (NAT-dst) 的方法。注意，始终可以在同一策略中结合使用 NAT-src 和 NAT-dst。

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 17 页上的 “来自 DIP 池 (启用 PAT) 的 NAT-Src”。

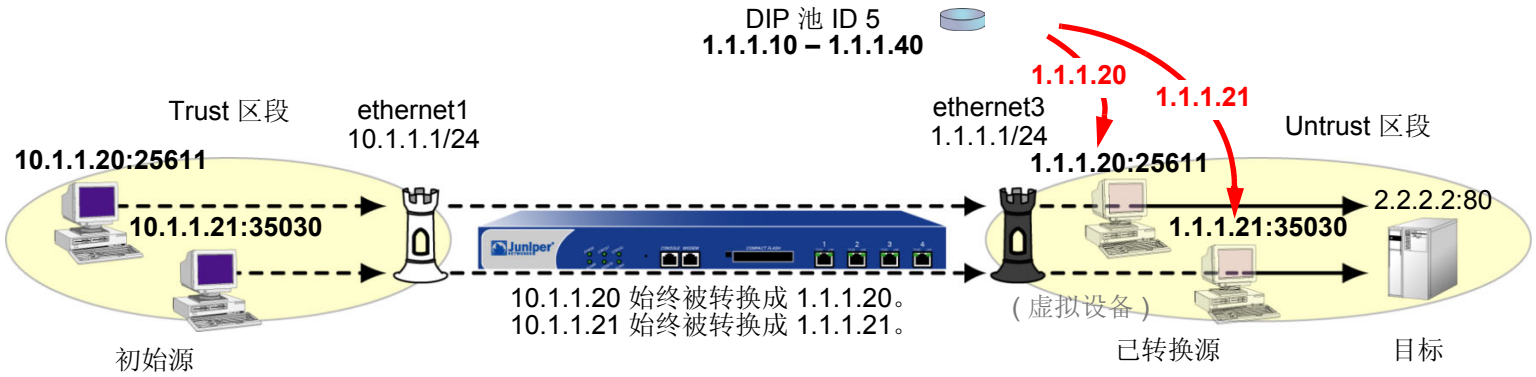


***注意：**在本图和后续示意图中，“虚拟设备”代表已转换的源地址或目标地址 (如果该地址不属于实际设备)。*

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 21 页上的 “来自 DIP 池 (禁用 PAT) 的 NAT-Src”。

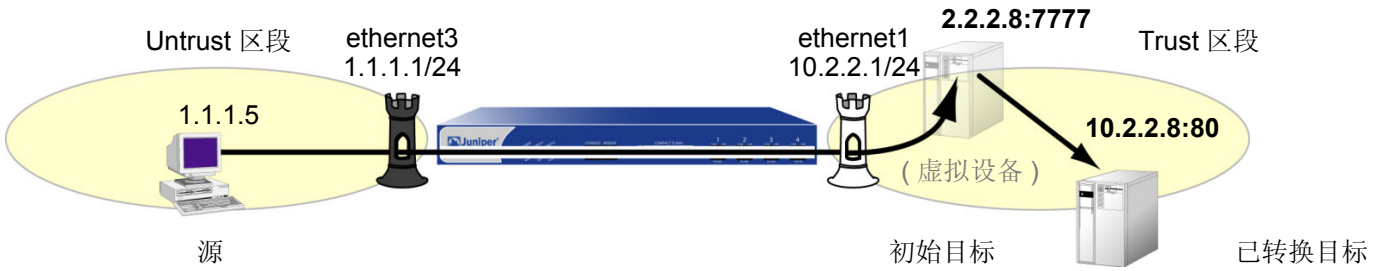


来自 DIP 池 (带有地址变换) 的 NAT-Src – NetScreen 设备将初始源 IP 地址转换成从动态 IP (DIP) 池中提取的地址，并持续将每个初始地址映射到特定的已转换地址。 NetScreen 设备不应用源端口地址转换 (PAT)。有关详细信息，请参阅第 24 页上的 “来自 DIP 池 (带有地址变换) 的 NAT-Src”。

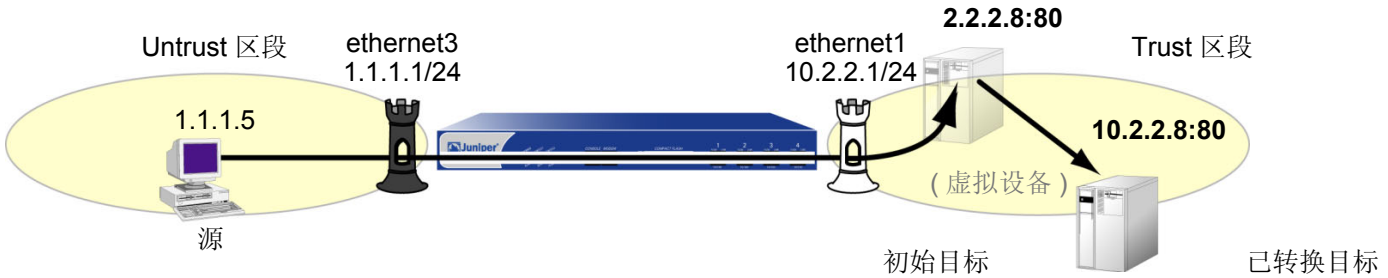


来自出口接口 IP 地址的 NAT-Src – NetScreen 设备将初始源 IP 地址转换成出口接口的地址。 NetScreen 设备还会应用源 PAT。有关详细信息，请参阅第 30 页上的 “来自出口接口 IP 地址的 NAT-Src”。

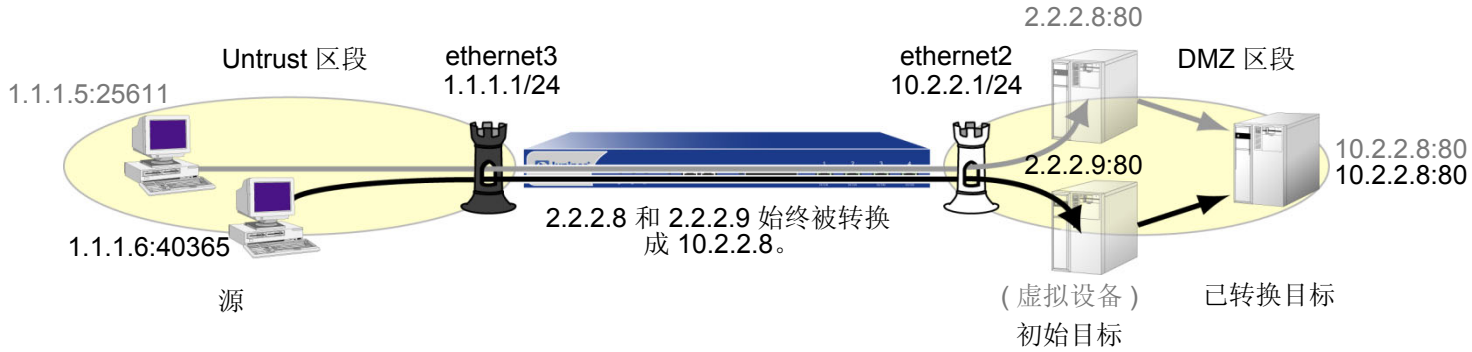
转换成单个 IP 地址 (带有端口映射) 的 NAT-Dst – NetScreen 设备执行目标网络地址转换 (NAT-dst) 和目标端口映射。有关详细信息，请参阅第 63 页上的 “带有端口映射的 NAT-Dst”。



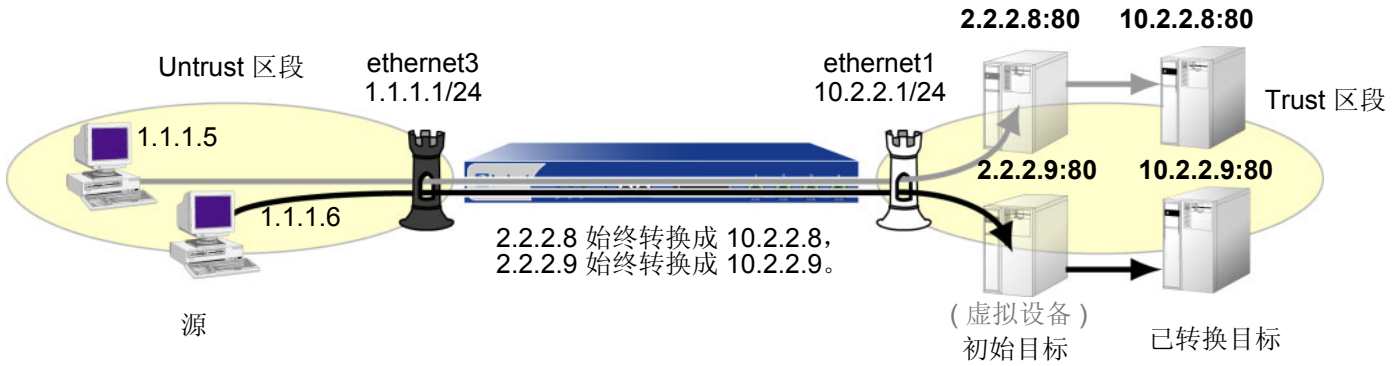
转换成单个 IP 地址 (无端口映射) 的 NAT-Dst – NetScreen 设备执行 NAT-dst，但不更改初始目标端口号。有关详细信息，请参阅第 33 页上的 “目标网络地址转换”。



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 设备会将初始目标端口号转换成其它端口号。有关详细信息，请参阅第 53 页上的“NAT-Dst: 多对一映射”。

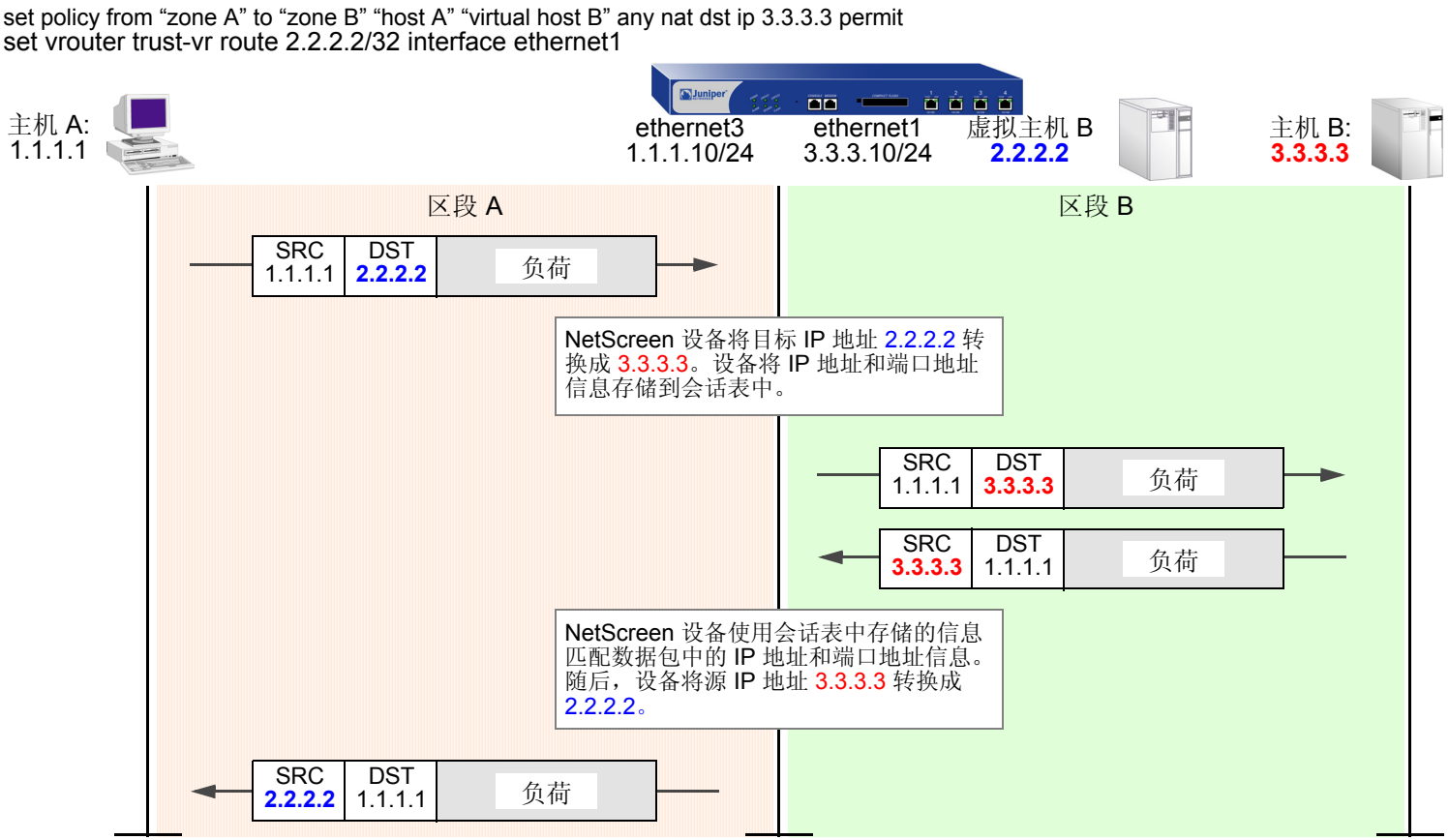


IP 地址范围之间的 NAT-Dst – 为 IP 地址范围应用 NAT-dst 时， NetScreen 设备会使用一种称作地址变换的技术，将初始目标地址始终映射成特定范围内的已转换地址。注意，地址变换不支持端口映射。有关详细信息，请参阅第 58 页上的 “NAT-Dst: 多对多映射”。



NAT-Src 和 NAT-Dst 的方向特性

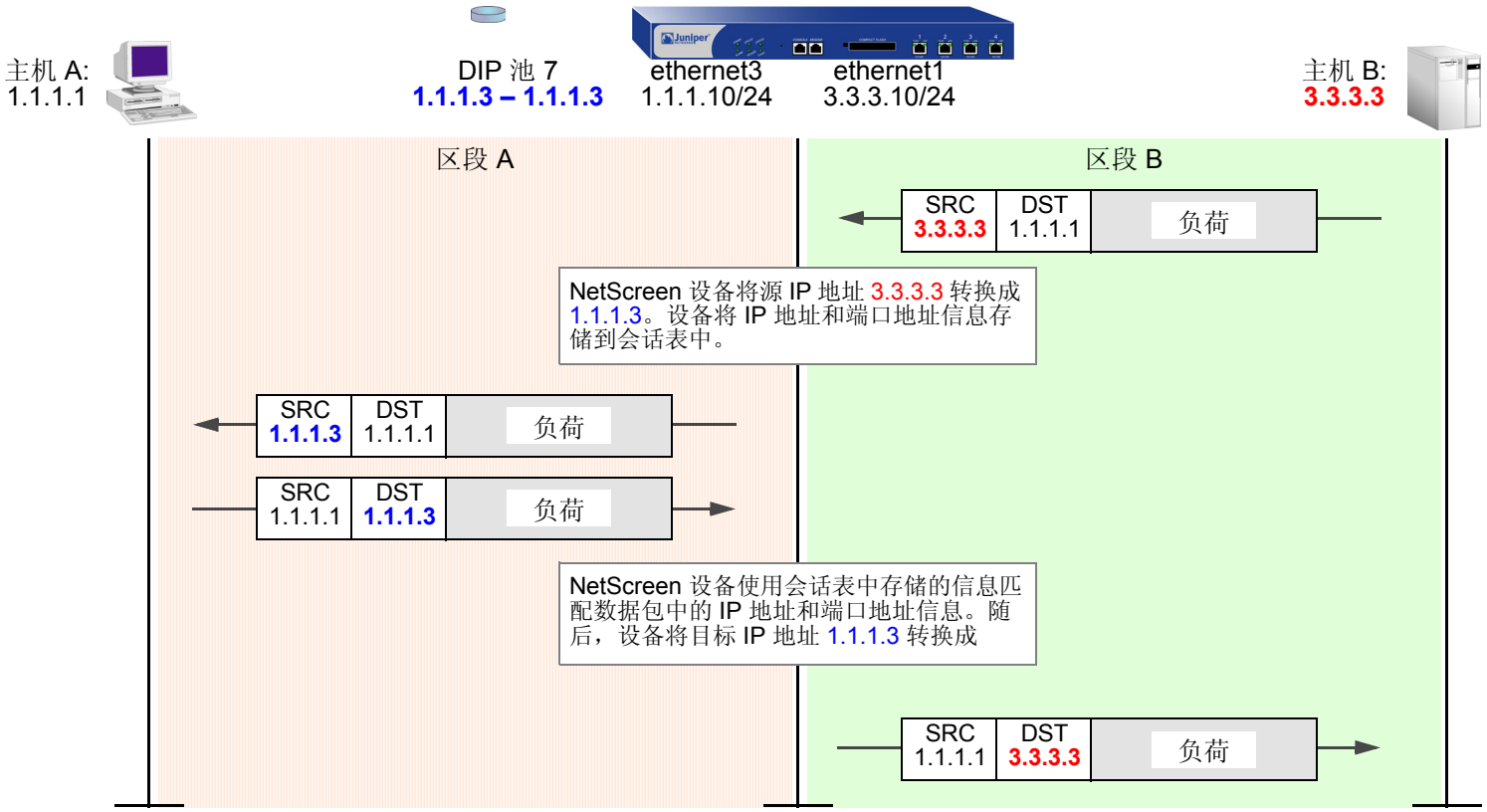
NAT-src 和 NAT-dst 的应用各自独立。通过策略中所指示的方向，可以确定二者在信息流上的应用方式。例如，如果 NetScreen 设备应用一个策略，对从主机 A 发送到虚拟主机 B 的信息流执行 NAT-dst，则 NetScreen 设备会将初始目标 IP 地址 2.2.2.2 转换成 3.3.3.3。（此外，设备还会将响应信息流中的源 IP 地址 3.3.3.3 转换成 2.2.2.2。）



***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找确定目标区段。有关 NAT-dst 路由选择问题的详细信息，请参阅第 40 页上的 “NAT-Dst 的路由选择”。*

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 不同。请参阅第 90 页上的 “映射 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。

2

源网络地址转换

NetScreen 提供了许多执行源网络地址转换 (NAT-src) 和源端口地址转换 (PAT) 的方法。本章介绍几种可用的地址转换方法，分为以下几个部分：

NAT-Src 简介

有时， NetScreen 设备需要将 IP 数据包包头中的初始源 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[1]。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 地址和目标 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标区段的缺省接口位于同一子网中。如果要使用的 DIP 池的地址不在目标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 **2**-271 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[2]。尽管所有数据包从 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 设备可以跟踪哪些数据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标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。

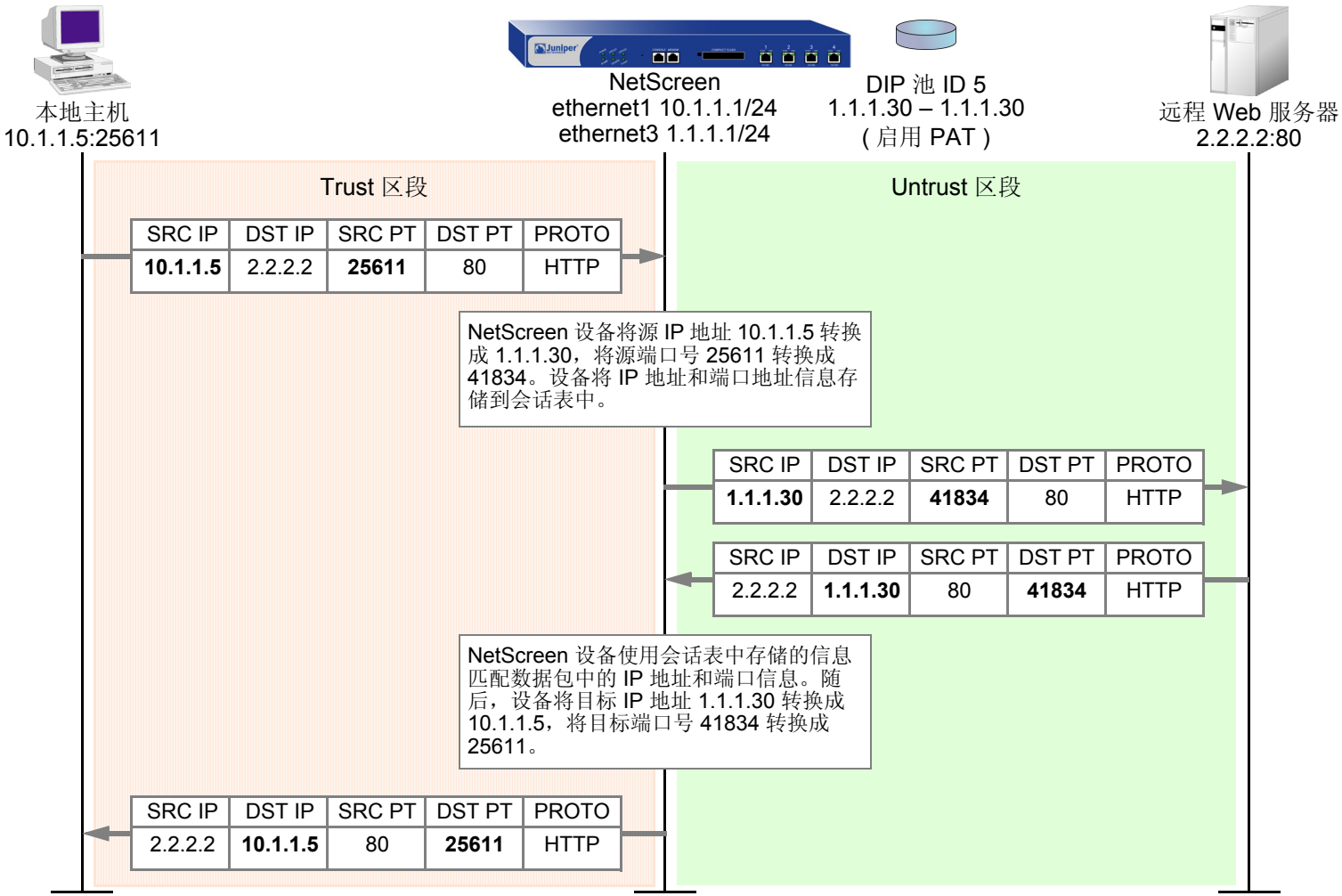
对于需要将特定源端口号保持固定的应用程序，必须禁用 PAT，并定义一个 IP 地址范围足够大的 DIP 池，以确保每台并行活动的主机收到不同的已转换地址。对于固定端口的 DIP， NetScreen 设备将一个已转换源地址分配给所有并行会话所在的同一台主机。反之，如果 DIP 池启用了 PAT， NetScreen 设备可能会给单台主机分配不同地址，以进行不同会话 — 除非将 DIP 定义为 “附着” (第 **2**-270 页上的 “附着 DIP 地址”)。

1. 有关公共和私有 IP 地址的信息，请参阅第 **2**-64 页上的 “公共 IP 地址”和第 **2**-65 页上的 “私有 IP 地址”。
2. 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 数据包包头和 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
```

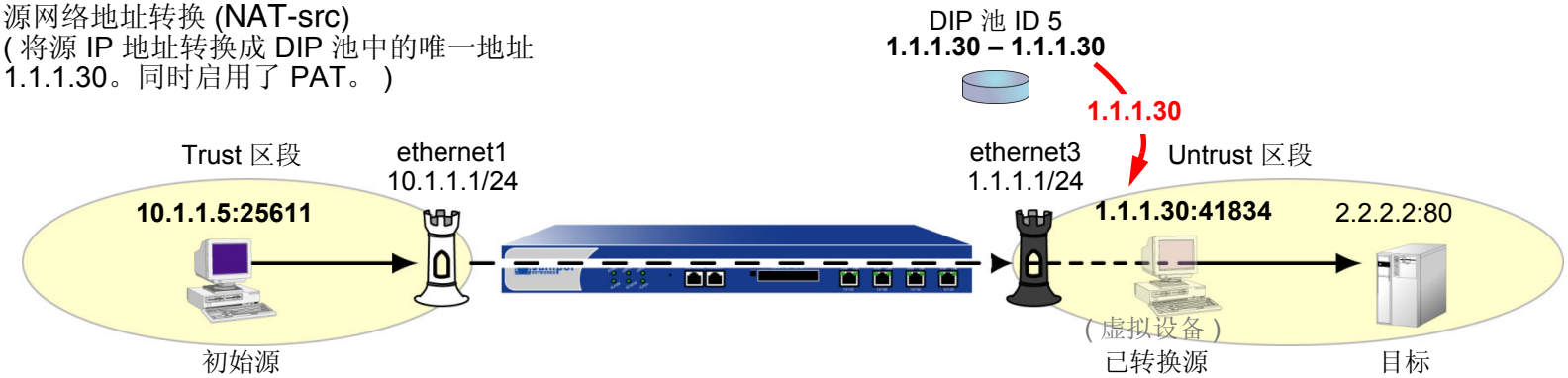


范例 : 已启用 PAT 的 NAT-Src

在本例中，在绑定到 Untrust 区段的 ethernet3 接口上定义 DIP 池 5。DIP 池只包含单个 IP 地址 1.1.1.30，且启用了 PAT (在缺省情况下启用 PAT)[3]。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 数据包包头中的源 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。)



SRC IP	DST IP	SRC PT	DST PT	PROTO
10.1.1.5	2.2.2.2	**25611**	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.30	2.2.2.2	**41834**	80	HTTP

3. 定义 DIP 池时，在缺省情况下 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。定制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[4]
- 将 IP 数据包包头中的源 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

4. 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 事务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确度。例如，站点 A 的 NetScreen-A 管理员的策略定义如下 : 通过站点对站点 VPN 通道与站点 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 池中的地址来应用 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，可以在策略中应用已启用地址变换的 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 接口上定义 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，在该策略中引用了上述地址组 (使用 DIP 池 10 将 NAT-src 应用到该策略)。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) 转换成同一已转换的 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 数据包包头中的源 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 数据包包头中的源 IP 地址转换成绑定到 Untrust 区段的 ethernet3 接口的 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 地址转换成目标区段出口接口的 IP 地址 1.1.1.1。同时启用了 PAT。)

SRC IP	DST IP	SRC PT	DST PT	PROTO
10.1.1.5	2.2.2.2	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.1	2.2.2.2	41834	80	HTTP

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 (Use Egress Interface 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
```

3

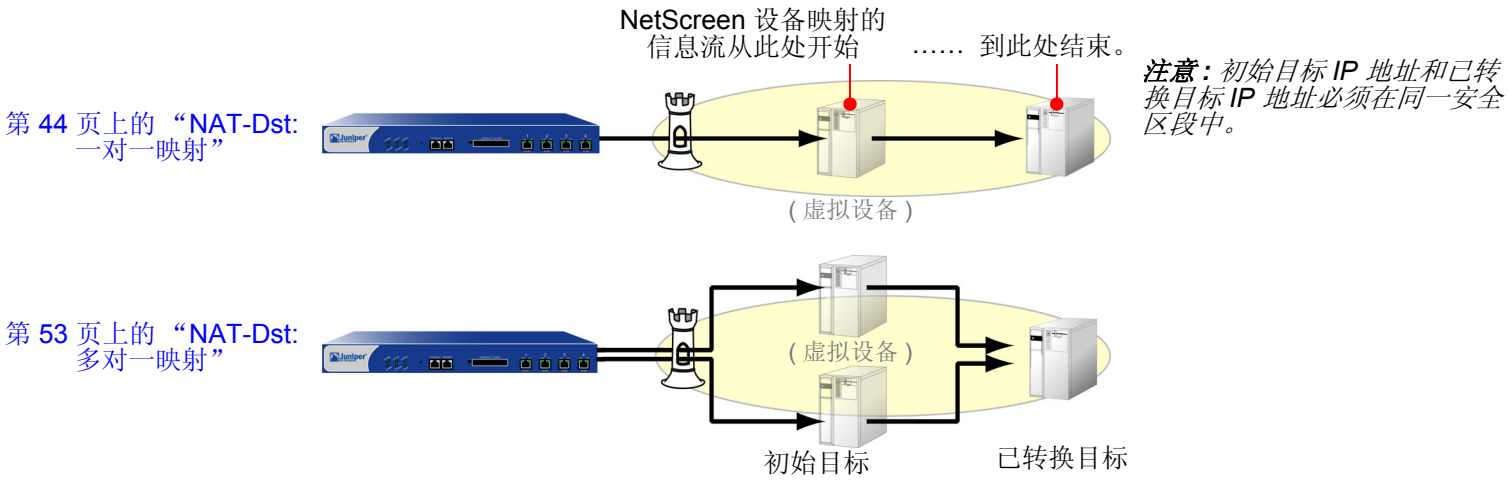
目标网络地址转换

NetScreen 提供了许多执行目标网络地址 (NAT-dst) 转换和目标端口地址映射的方法。本章介绍几种可用的地址转换方法，分为以下几个部分：

***注意：**有关使用映射 IP (MIP) 或虚拟 IP (VIP) 地址进行目标地址转换的信息，请参阅第 89 页上的 “映射和虚拟 IP 地址”。*

NAT-Dst 简介

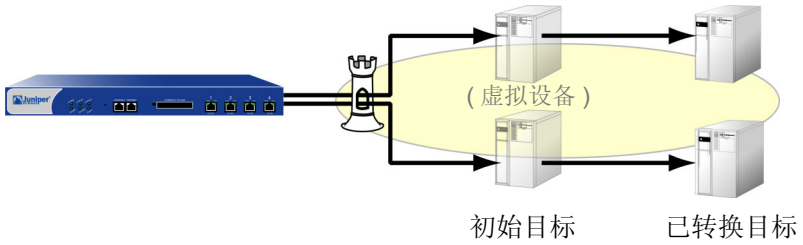
可以定义策略将一个目标 IP 地址转换成另一个地址。可能需要 NetScreen 设备以便将一个或多个公共 IP 地址转换成一个或多个私有地址。初始目标地址与已转换目标地址之间的关系可能是一对一、多对一或多对多关系。下图说明了一对一和多对一 NAT-dst 关系的概念。



上述两种配置均支持目标端口映射。端口映射就是将一个初始目标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标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标地址始终转换成特定的已转换目标地址。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。

第 58 页上的 “NAT-Dst: 多对多映射”

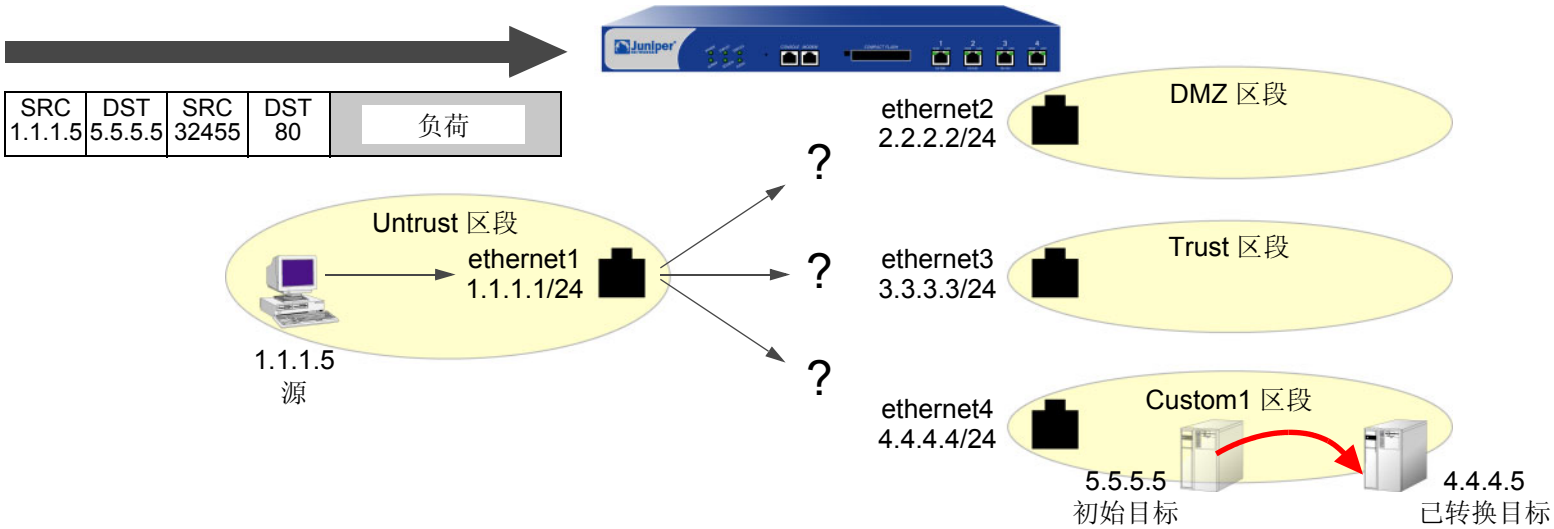


路由表中必须同时存在初始目标 IP 地址和已转换目标 IP 地址的条目。 NetScreen 设备使用初始目标 IP 地址执行路由查找，确定后续策略查找的目标区段。然后使用已转换地址执行第二次路由查找，确定发送数据包的位置。为确保由路由确定的结果与策略相符，初始目标 IP 地址和已转换目标 IP 地址必须在同一安全区段中。 (有关目标 IP 地址、路由查找及策略查找之间的关系，请参阅第 36 页上的 “NAT-Dst 的数据包流”。)

NAT-Dst 的数据包流

以下步骤介绍数据包流经 NetScreen 设备的路径以及设备应用目标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 和目标 IP 地址 : 端口号为 5.5.5.5:80 的 HTTP 数据包到达绑定到 Untrust 区段的 ethernet1。



NetScreen 设备尚未执行确定转发数据包必须使用的接口所需的步骤。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 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 设备封锁该数据包)，则 NetScreen 设备会丢弃该数据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，设备被配置为对该行为只记录事件却不封锁数据包，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，则 NetScreen 设备继续下一步骤。

   如果未启用 Untrust 区段的 SCREEN 选项， NetScreen 设备将立即进行下一步。

3. 会话模块将执行会话查找，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，则 NetScreen 设备将执行 “首包处理”，该过程包括其余的步骤。

   如果该数据包与现有会话匹配，则 NetScreen 设备将执行 “快速处理”，用现有会话条目中可用的信息来处理该数据包。“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)[1] 配置使用了目标 IP 地址 5.5.5.5。

   如果存在这样的配置， NetScreen 设备会将 MIP 或 VIP 转变成已转换目标 IP 地址，并将后者作为路由查找的依据。随后，设备将在 Untrust 和 Global 区段之间执行策略查找。如果找到了允许信息流的策略匹配项，NetScreen 设备会将数据包转发到在路由查找中确定的出口接口。

   如果未在 MIP 或 VIP 配置中使用 IP 地址 5.5.5.5， NetScreen 设备将继续进行下一步。

5. 为确定目标区段，路由模块将查找初始目标 IP 地址的路由，也就是说，该模块将使用到达 ethernet1 的数据包包头中出现的目标 IP 地址。 (路由模块使用入口接口来确定路由查找使用的虚拟路由。) 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**

1. 仅当数据包到达绑定到 Untrust 区段的接口时， NetScreen 设备才检查是否在 VIP 配置中使用了目标 IP 地址。

6. 策略引擎在 Untrust 和 Custom1 区段之间执行策略查找 (由相应的入口和出口接口确定)。源 IP 地址、目标 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。

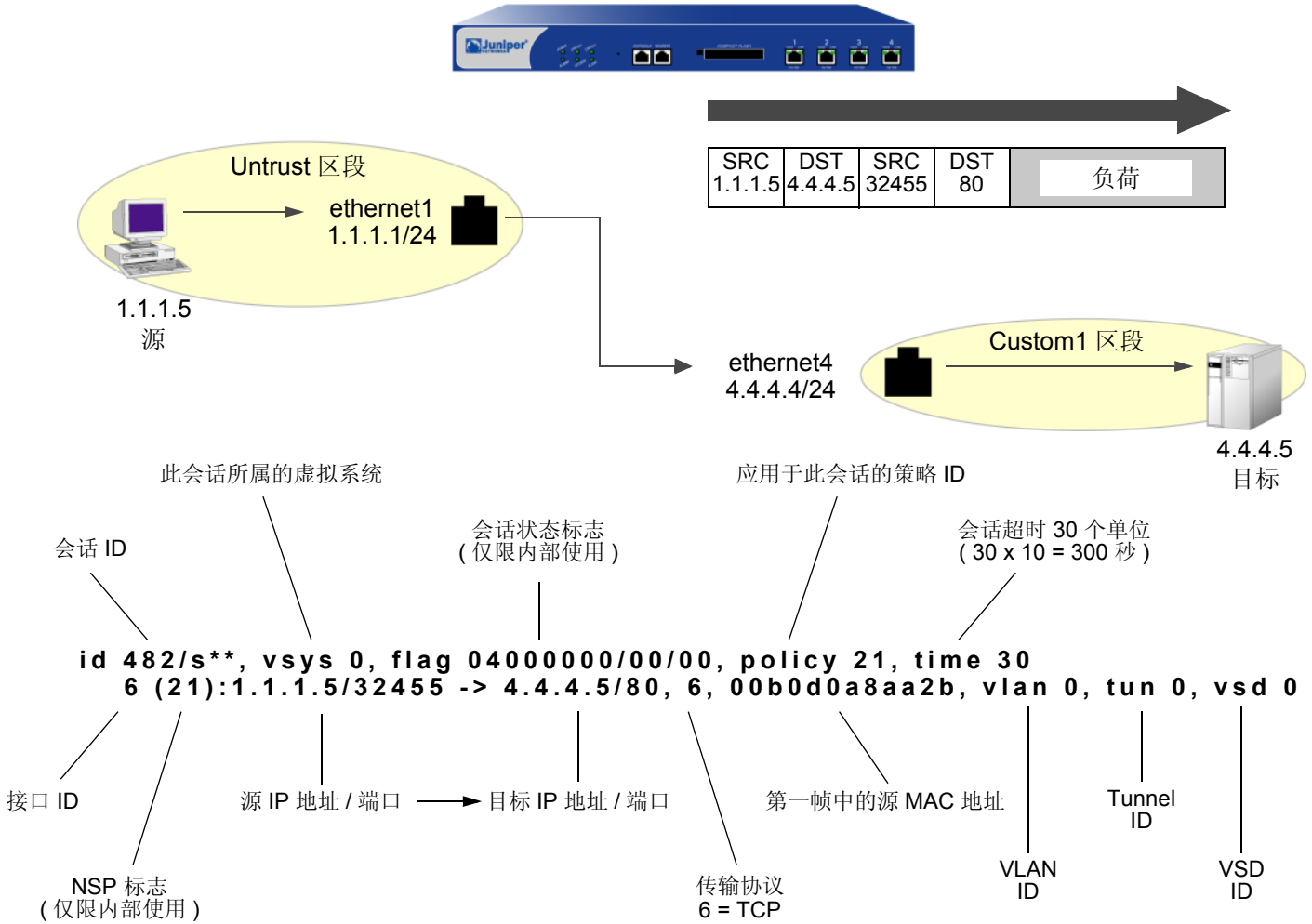
   set policy from untrust to custom1 any v-server1 http nat dst ip 4.4.4.5 permit

   (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 设备将目标 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标端口地址转换。

7. 接着， NetScreen 设备使用已转换 IP 地址执行第二次路由查找，发现可通过 ethernet4 访问地址 4.4.4.5/32。

8. 地址映射模块将数据包包头中的目标 IP 地址转换成 4.4.4.5。随后，NetScreen 设备将该数据包从 ethernet4 转发出去，并在会话表中生成一个条目 (除非此数据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 号均设为零。*

NAT-Dst 的路由选择

配置 NAT-dst 地址时， NetScreen 设备的路由表中必须同时存在指向数据包包头中出现的的初始目标地址和已转换目标地址 (即 NetScreen 设备将数据包重新定向到的地址) 的路由。如第 36 页上的 “NAT-Dst 的数据包流”中所述， NetScreen 设备使用初始目标地址执行路由查找，以此来确定出口接口。反过来，出口接口给出目标区段 (接口绑定到的区段)，以便 NetScreen 设备执行策略查找。 NetScreen 设备找到符合要求的策略时，该策略会定义从初始目标地址到已转换目标地址的映射。随后， NetScreen 设备执行第二次路由查找，确定转发数据包的接口，数据包必须通过该接口才能到达新的目标地址。总之，指向初始目标地址的路由提供了执行策略查找的方法，指向已转换目标地址的路由则指定了 NetScreen 设备转发数据包所使用的出口接口。

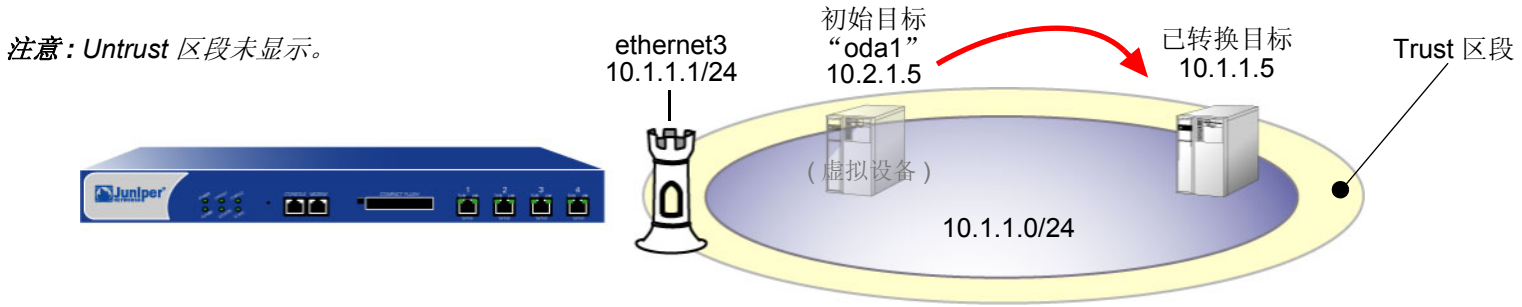
在以下三种情况中，根据策略中引用的目标地址周围的网络拓扑，输入静态路由的需求将有所不同 :

set policy from untrust to trust any oda1 http nat dst ip 10.1.1.5 permit

其中 “oda1”是初始目标地址 10.2.1.5，已转换目标地址为 10.1.1.5。

连接到一个接口的地址

在此情况中，连接初始目标地址和已转换目标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。要完成该路由选择要求，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

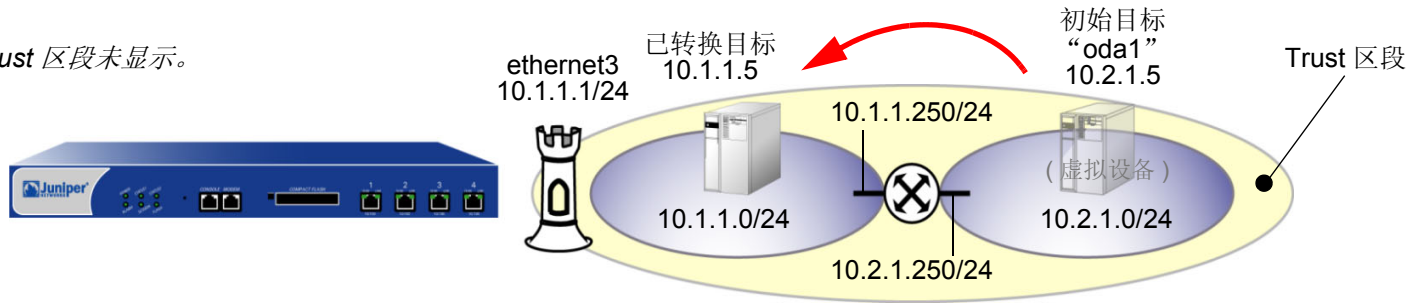
```
set vrouter trust-vr route 10.2.1.5/32 interface ethernet3
save
```

连接到一个接口但被路由器分隔的地址

在此情况中，连接初始目标地址和已转换目标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。要完成该路由选择要求，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，则不必为了将 NAT-dst 应用到 10.2.1.5 而向策略添加其它路由。*

注意：*Untrust 区段未显示。*



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

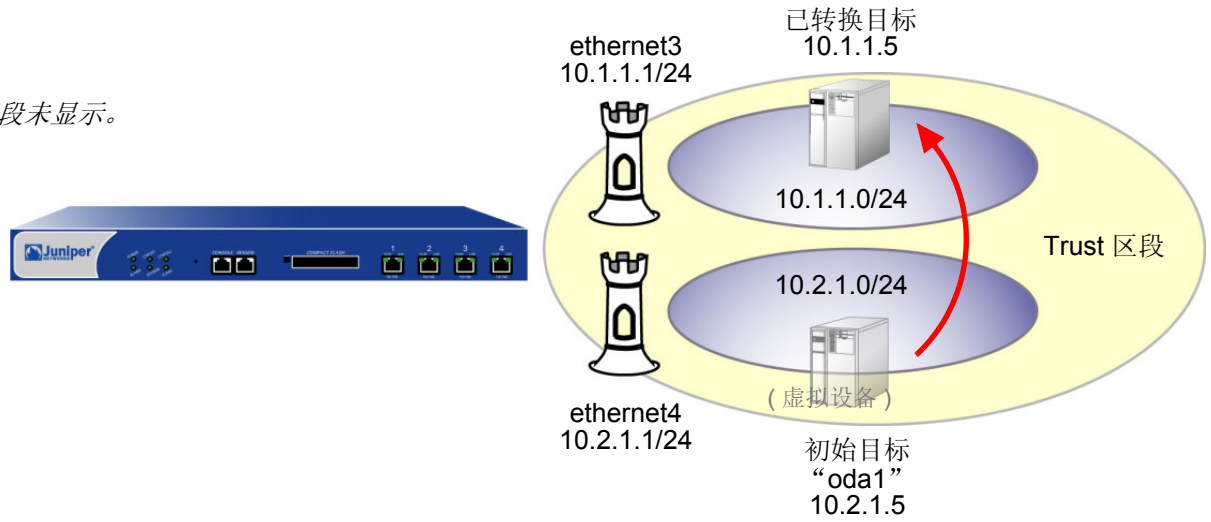
CLI

```
set vrouter trust-vr route 10.2.1.0/24 interface ethernet3 gateway 10.1.1.250
save
```

由接口分隔的地址

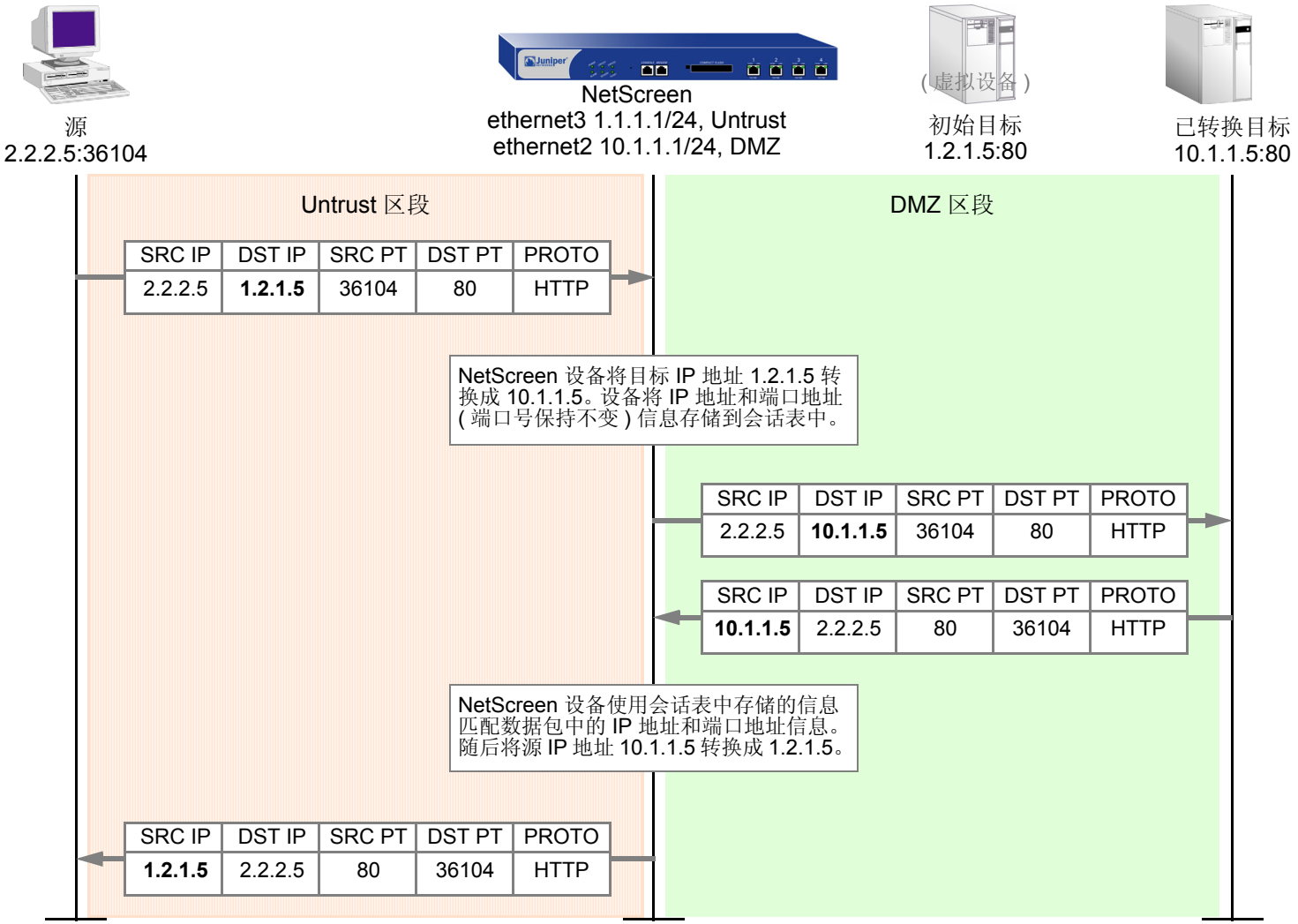
在此情况中，有两个接口绑定到 Trust 区段 : IP 地址为 10.1.1.1/24 的 ethernet3 和 IP 地址为 10.2.1.1/24 的 ethernet4。配置这些接口的 IP 地址时， NetScreen 设备会自动添加通过 ethernet3 指向 10.1.1.0/24 的路由和通过 ethernet4 指向 10.2.1.0/24 的路由。将初始目标地址放入 10.2.1.0/24 子网，并将已转换目标地址放入 10.1.1.0/24 子网，不必为将 NAT-dst 应用于从 10.1.1.5 到 10.2.1.5 而向 NetScreen 设备添加其它路由。

注意 : Untrust 区段未显示。



NAT-Dst: 一对一映射

在应用目标网络地址转换 (NAT-dst) 而不应用端口地址转换时， NetScreen 设备转换目标 IP 地址，并如下图所示执行状态检查 (注意，只显示 IP 数据包包头和 TCP 片段包头中与 NAT-dst 有关的元素):

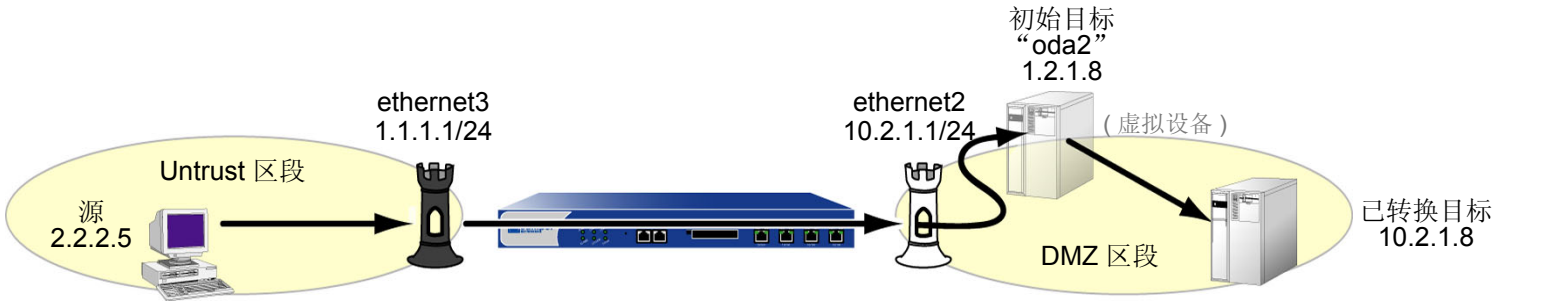


范例：一对一目标地址转换

在本例中，将设置一个提供一对一的目标网络地址转换 (NAT-dst) 但不更改目标端口地址的策略。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” 的初始目标地址 1.2.1.8
- 将 IP 数据包包头中的目标 IP 地址 1.2.1.8 转换成 10.2.1.8
- 让 TCP 片段包头的初始目标端口号保持不变 (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 指向初始目标地址 1.2.1.8 的路由。 Untrust 和 DMZ 区段都在 trust-vr 路由选择域中。



SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**1.2.1.8**	25611	80	HTTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**10.2.1.8**	25611	80	HTTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**1.2.1.8**	40365	21	FTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**10.2.1.8**	40365	21	FTP

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标地址转换成不同策略中指定的多个已转换目标地址。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标地址的信息流重新定向到多个已转换地址。

范例：一对多目标地址转换

在本例中，将创建两个策略，它们使用相同的初始目标地址 (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标地址。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”的用户定义的地址
- 对于 HTTP 信息流，将 IP 数据包包头中的目标 IP 地址 1.2.1.8 转换成 10.2.1.8
- 对于 FTP 信息流，将目标 IP 地址 1.2.1.8 转换成 10.2.1.9
- 让 TCP 片段包头的初始目标端口号保持不变 (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

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**1.2.1.8**	25611	80	HTTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**10.2.1.8**	25611	80	HTTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**1.2.1.8**	40365	21	FTP

SRC IP	**DST IP**	SRC PT	DST PT	PROTO
2.2.2.5	**10.2.1.9**	40365	21	FTP

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 指向初始目标地址 1.2.1.8 的路由。 Untrust 和 DMZ 区段都在 trust-vr 路由选择域中。

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

初始目标地址和已转换目标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标地址的信息流转发到单个已转换目标地址。此外，还可以指定目标端口映射。

范例：多对一目标地址转换

在本例中，创建一个策略，将发送到不同初始目标地址 (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标地址。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 数据包包头中的目标 IP 地址 1.2.1.10 和 1.2.1.20 转换成 10.2.1.15
- 让 TCP 片段包头的初始目标端口号保持不变 (HTTP 为 80)
- 将 HTTP 信息流转发到 DMZ 区段中的 10.2.1.15

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.5	**1.2.1.10**	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.5	**10.2.1.15**	25611	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.6	**1.2.1.20**	40365	80	HTTP

SRC IP	DST IP	SRC PT	DST PT	PROTO
1.1.1.6	**10.2.1.15**	40365	80	HTTP

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 指向初始目标地址 1.2.1.10 和 1.2.1.20 的路由。 Untrust 和 DMZ 区段都在 trust-vr 路由选择域中。

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

可以使用目标网络地址转换 (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标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，如果希望创建一个对 HTTP 信息流应用上述转换的策略，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标地址转换成 10.100.3.137。

如果策略中指定的源和目标区段、源和目标地址及服务与数据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该策略置于策略 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
```

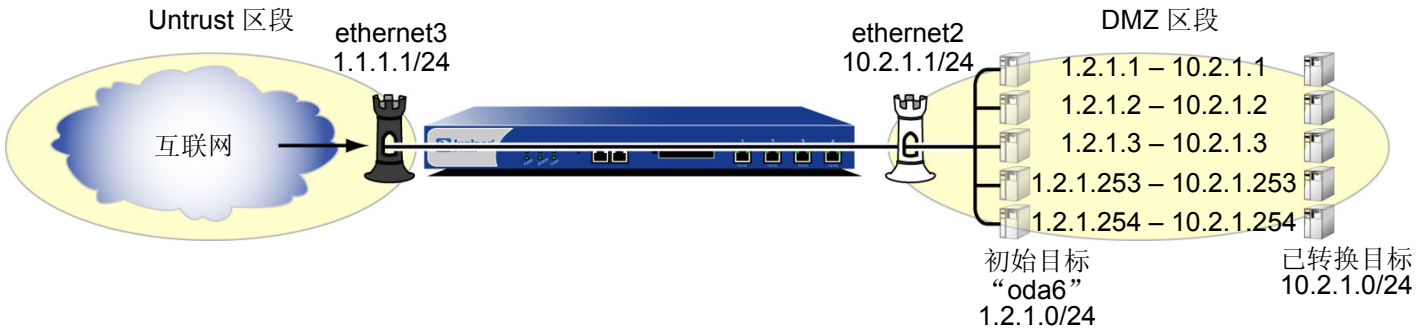
如果已配置这两个策略，设备将避开 NAT-dst 机制将以下类型的信息流从 zoneA 中的主机发送到 zoneB 中的主机：

- 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标地址。
- ZoneA 中的主机发起到 zoneB 中 10.1.1.51 的 HTTP 信息流。由于目标地址不在 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标地址。

范例：多对多目标地址转换

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” 的初始目标地址转换成 10.2.1.0/24 子网中的相应地址
- 让 TCP 片段包头的初始目标端口号保持不变
- 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 指向初始目标地址子网 (1.2.1.0/24) 的路由。Untrust 和 DMZ 区段都在 trust-vr 路由选择域中。

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 设备执行目标网络地址转换 (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 设备在相同目标 IP 地址上执行 NAT-dst，并执行端口映射 (dst 端口 80 -> 8081)。通过两个不同的目标端口号，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 58 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 区段中 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” 的初始目标 IP 地址 1.2.1.15 转换成 10.2.1.15
- 将 TCP 片段包头的初始目标端口号 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 指向初始目标地址 1.2.1.15 的路由。 Trust、 Untrust 和 DMZ 区段都在 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

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) 和目标网络地址转换 (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 地址和目标 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[2]。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 路由选择域中。

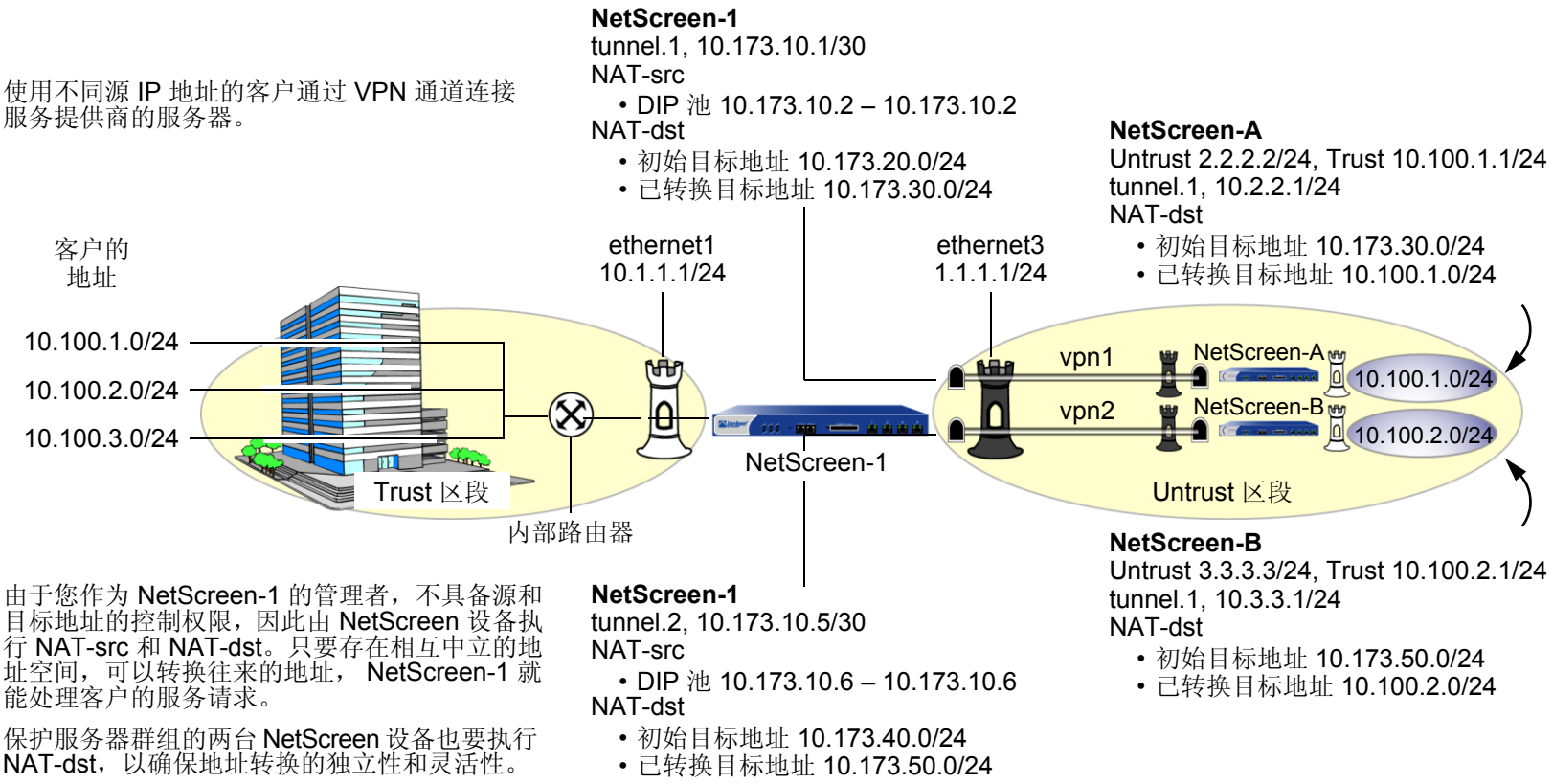
由于客户拥有的地址可能与要连接服务器的地址相同，因此 NetScreen-1 必须同时执行源地址转换 (NAT-src) 和目标地址转换 (NAT-src)。为确保地址转换的独立性与灵活性， NetScreen 设备通过执行 NAT-dst 保护服务器群组 NetScreen-A 和 NetScreen-B。出于上述目的，服务提供商会指示客户和服务器群组的管理员保留以下地址：10.173.10.1–10.173.10.7、 10.173.20.0/24、 10.173.30.0/24、 10.173.40.0/24 和 10.173.50.0/24。这些地址的用途如下：

- 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标地址，如下所示[3]：
  - 10.173.20.0/24 到 10.173.30.0/24
  - 10.173.40.0/24 到 10.173.50.0/24

2. 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。
3. 有关执行 NAT-dst 时使用的地址变换信息，请参阅第 58 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”。 (有关这些提议的详细信息，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: ethernet3[4]

> 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. 出接口不一定非要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
```

4

映射和虚拟 IP 地址

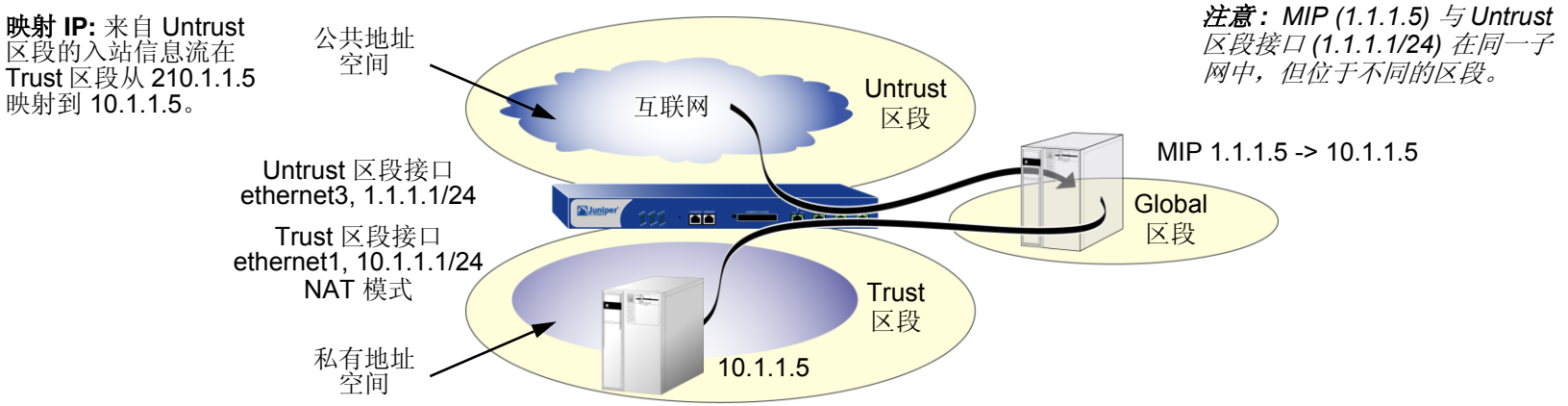
NetScreen 提供了许多执行目标 IP 地址和目标端口地址转换的方法。本章介绍如何使用映射 IP (MIP) 和虚拟 IP (VIP) 地址，并分为以下部分：

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 是一个静态目标地址转换，将 IP 数据包包头中的目标 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标地址的转换 (请参阅第 13 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[1] 问题。(有关此问题完整的解决方案，请参阅第 **5** -199 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) 安全区段且带有 IP 地址/网络掩码的接口[2]。虽然 MIP 是为绑定到通道区段和安全区段的接口配置的，但是定义的 MIP 存储在 Global 区段。



1. 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。
2. 为 Untrust 区段中接口定义的 MIP 例外。该 MIP 可以在不同 Untrust 区段接口 IP 地址的子网中。但是，如果真是这样，就必须在外部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。

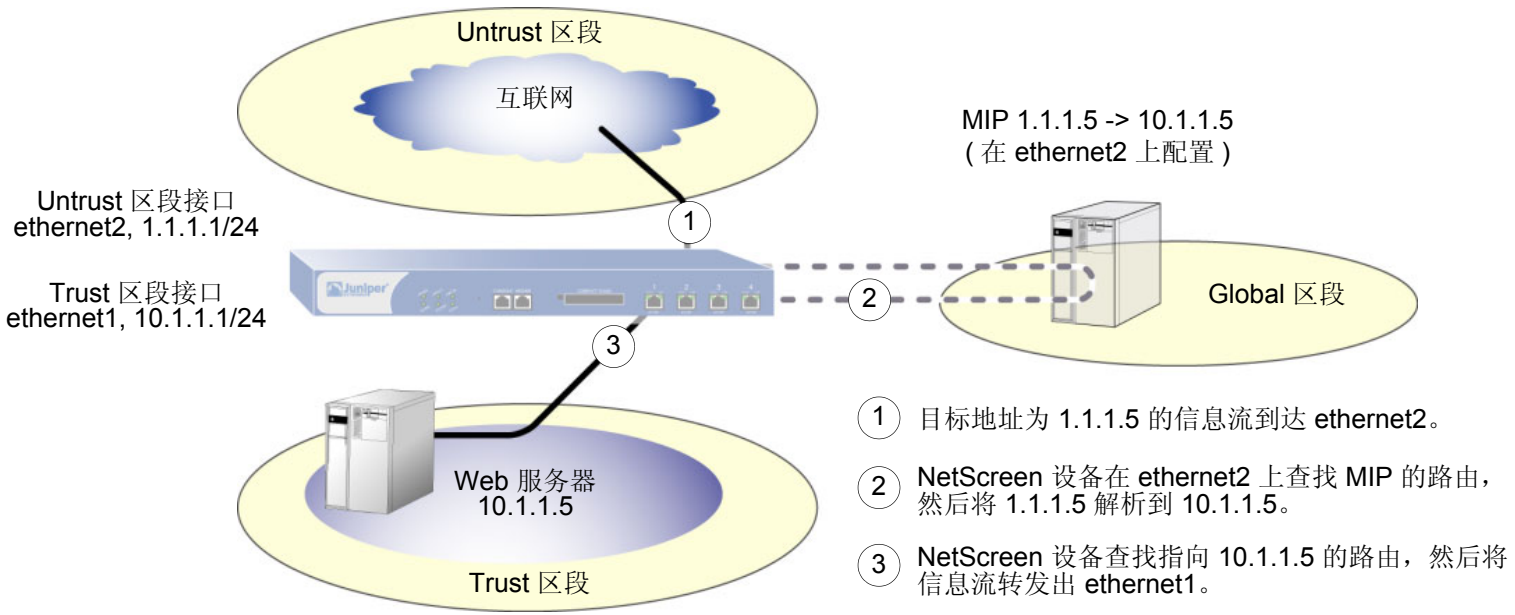
MIP 和 Global 区段

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标地址，还可以在定义全局策略时用作目标地址。(有关全局策略的信息，请参阅第 **2**-297 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 指向的目标区段 (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，将目标地址为 Untrust 区段中 1.1.1.5 的内向 HTTP 信息流发送到 Trust 区段中地址为 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 路由选择域中。

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 255.255.255.255[3]
    vrouter trust-vr[4]
```

3. 策略

```
set policy from untrust to trust any mip(1.1.1.5) http permit
save
```

---

3. 在缺省情况下， 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。

4. 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

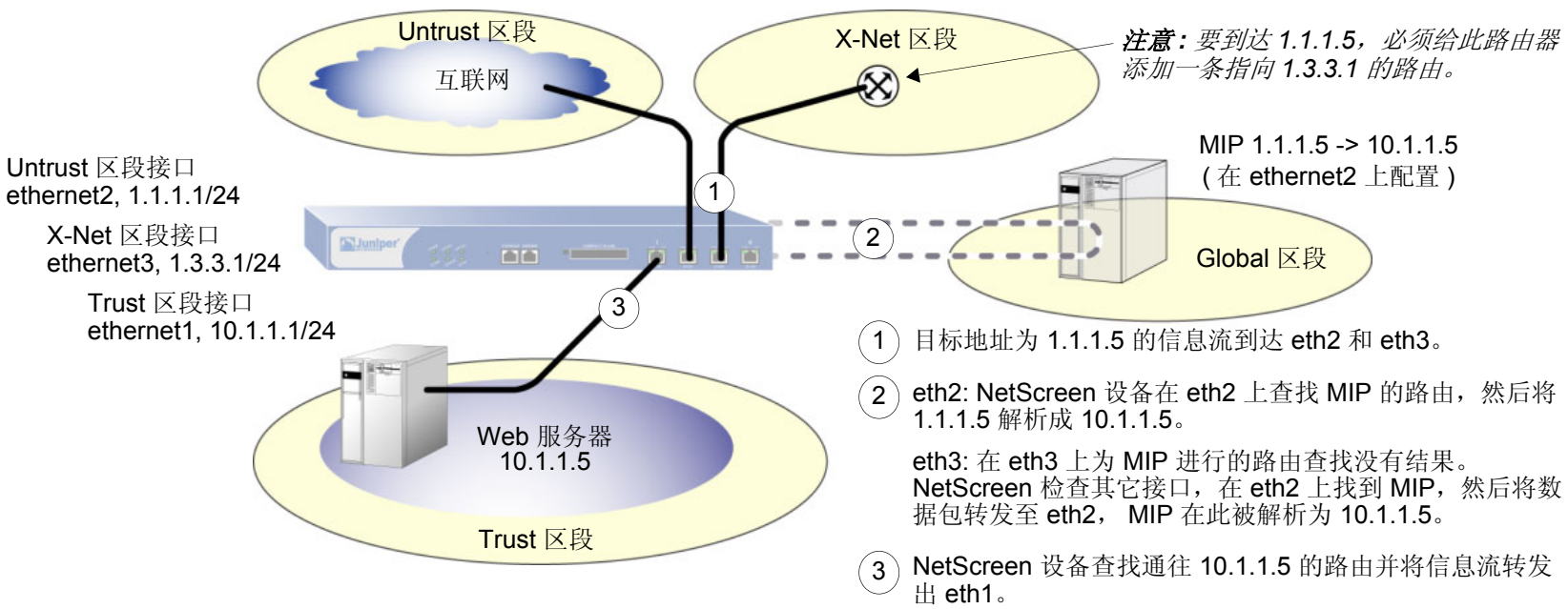
来自不同区段的信息流仍可通过其它接口 (而非您在其上配置 MIP 的接口) 到达 MIP。要完成上述操作，必须在其它各个区段的路由器上设置路由，将入站信息流指向它们各自接口的 IP 地址，以到达 MIP[5]。

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 的安全区段，将 ethernet3 绑定到该区段，然后给接口分配 IP 地址 1.3.3.1/24。定义要在策略中使用的地址 1.1.1.5，以允许 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。所有安全区段都在 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，引导目标地址为 1.1.1.5 (MIP) 的信息流流向 1.3.3.1 (ethernet3 的 IP 地址)。*

5. 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-vr[6]
```

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
```

6. 在缺省情况下，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 添加到通道接口

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。为了允许一个网络在 Trust 区段中的远程网站使用重叠地址空间，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。(有关带有通道接口的 MIP 的完整范例，请参阅第 **5**-199 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-vr[7]
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 发往服务器的外向数据包应用基于策略的 NAT-src (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。

7. 在缺省情况下， 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 数据包转发到通道端点。

如果创建一个策略，在该策略中目标地地址是使用 Untrust 区段接口 IP 地址的 MIP，并且指定 HTTP 充当该策略中的服务，那么您就失去通过该接口对 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: [8] (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 端口

Configuration > Admin > Management: 在 “HTTP Port” 字段键入 **8080**，然后单击 **Apply**。

(失去 HTTP 连接。)

8. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 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 地址字段中的 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: 255.255.255.255[9]

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

9. 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-vr[10]
```

4. 路由

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

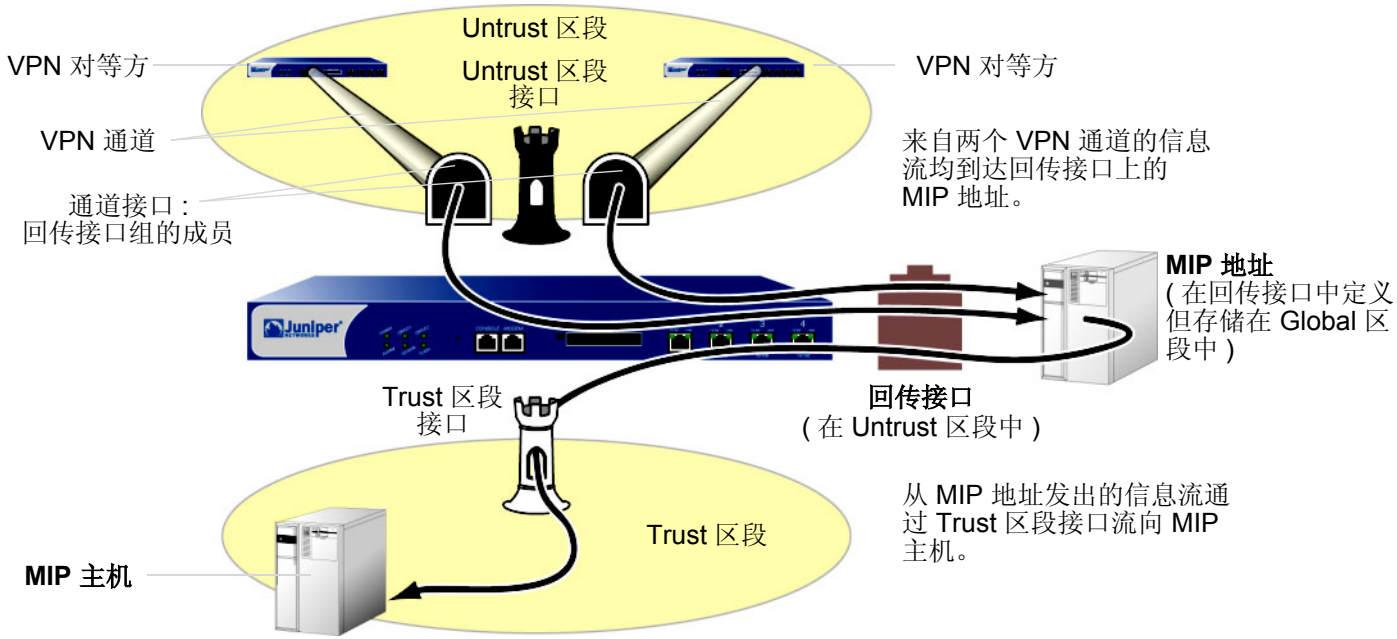
5. 策略

```
set policy from untrust to trust any mip(1.1.1.1) http permit
save
```

10. 在缺省情况下，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 **2**-74 页上的 “回传接口”)。为允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成员。

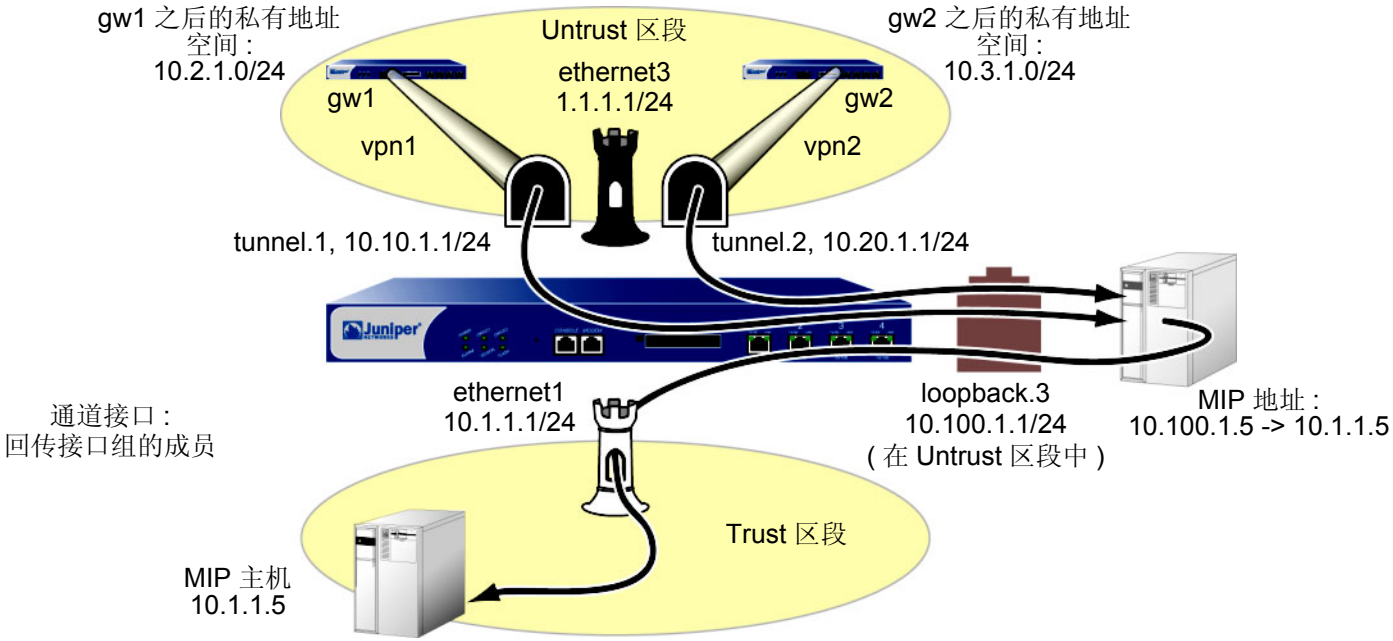
回传接口及其成员接口必须位于同一区段的不同 IP 子网中。任何一个有 IP 地址的接口都可以成为回传组的成员。如果要在回传接口和一个成员接口上配置 MIP，请优先配置回传接口。回传接口不能是其它回传组的成员。

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。



当目标地址为 10.100.1.5 的数据包通过 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 设备会将初始目标 IP 地址 (10.100.1.5) 转换成主机 IP 地址

(10.1.1.5)，然后通过 ethernet1 将数据包转发到 MIP 主机。目标地址为 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，再将初始目标 IP 地址 10.100.1.5 转换成 10.1.1.5，然后将数据包转发到 MIP 主机。

为完成配置，仍需要定义地址、 VPN 通道、路由及策略。所有安全区段都在 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**:

NAT: [11] (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

11. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 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 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 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-vr[12]
```

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
```

12. 在缺省情况下， 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

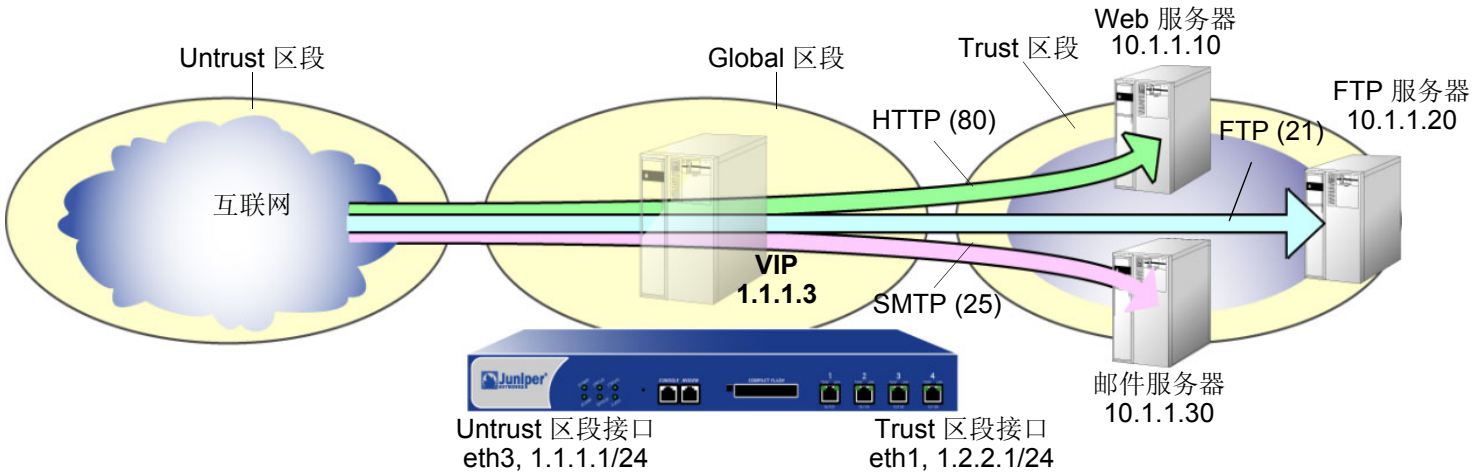
```
set policy top from untrust to trust peer-1 mip(10.100.1.5) any permit
set policy top from untrust to trust peer-2 mip(10.100.1.5) any permit
set policy from trust to untrust local_lan any any permit
save
```

虚拟 IP 地址

根据 TCP 或 UDP 片段包头的目标端口号，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，

- 目标地址为 1.1.1.3:80 (也就是 IP 地址为 1.1.1.3，端口号为 80) 的 HTTP 数据包可能映射到地址为 10.1.1.10 的 Web 服务器。
- 目标地址为 1.1.1.3:21 的 FTP 数据包可能映射到地址为 10.1.1.20 的 FTP 服务器。
- 目标地址为 1.1.1.3:25 的 SMTP 数据包可能映射到地址为 10.1.1.30 的邮件服务器。

目标 IP 地址相同。目标端口号确定 NetScreen 设备将信息流转发到的主机。



虚拟 IP 转发表

Untrust 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 设备将流向 VIP 的内向信息流转发到 VIP 指向地址上的主机。但是，当 VIP 主机发起出站信息流时，如果先前在入口接口或应用到来自该主机信息流的策略中的 NAT-src 上配置了 NAT，则 NetScreen 设备会仅将初始源 IP 地址转换为其它地址。否则， NetScreen 设备不会对来自 VIP 主机的信息流进行源 IP 地址转换。

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[13]
- 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数据包包头的 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标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标端口号或从 1 到 65,535 的端口号范围，而不仅是从 1024 到 65,535。
- 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 中也有一个对应服务条目)。在缺省情况下，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**，然后重置 NetScreen 设备。 (请参阅第 121 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。

13. 在某些 NetScreen 设备上，Untrust 区段中的接口可以通过 DHCP 或 PPPoE 动态接收其 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:] 进行选择，如果将 VIP 配置为使用与支持多个 VIP 的 NetScreen 设备上 Untrust 区段接口相同的 IP 地址，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。

VIP 和 Global 区段

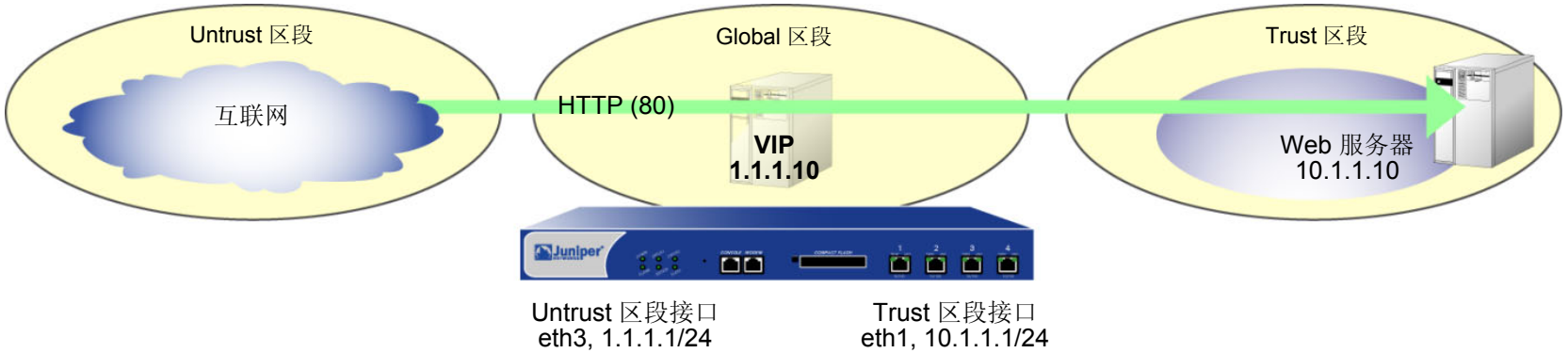
为 Untrust 区段中的接口设置 VIP 将在 Global 区段通讯簿中生成一条条目。不管接口属于哪个区段， Global 区段通讯簿会保留所有接口的全部 VIP。可以将这些 VIP 地址用作任意两个区段间策略的目标地址，还可以用作 Global 策略中的目标地址。

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 信息流转发到地址为 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 VIP[14]。此外， VIP 将信息流转发到的主机不需要通讯簿条目。所有安全区段都在 trust-vr 路由选择域中。



14. 如果希望安全区段 (而非 Untrust 区段) 的 HTTP 信息流到达 VIP，则必须在其它区段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，将目标地址为 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 95 页上的 “范例：从不同区段到达 MIP”中描述的过程类似。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 117 页上的 “范例：配置虚拟 IP 服务器” 中创建的策略 ID 号为 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**。

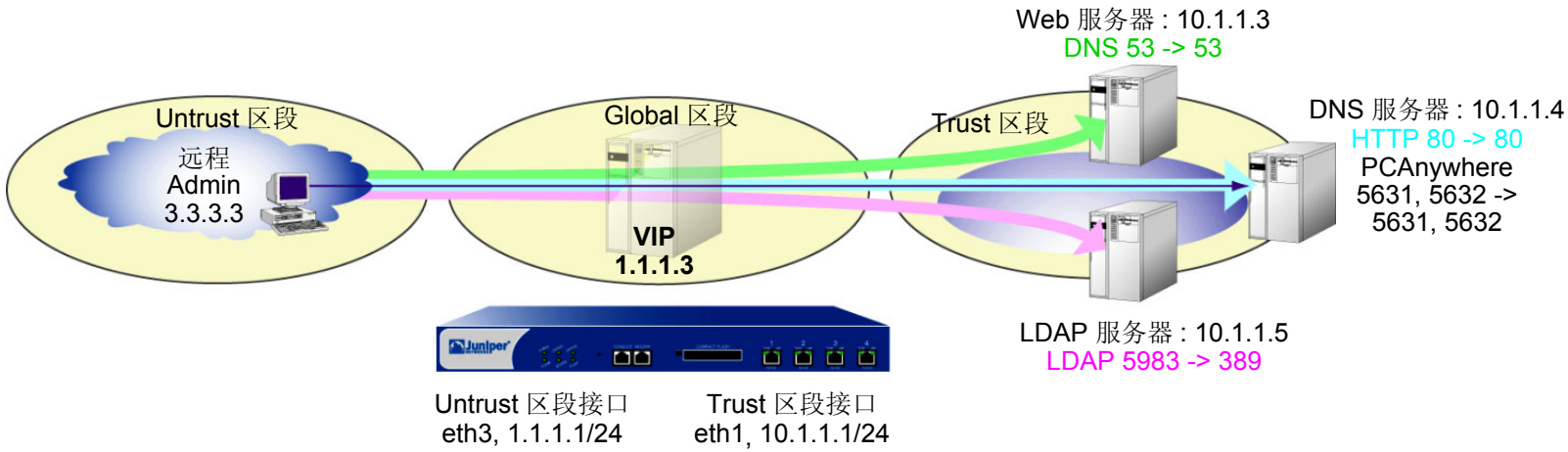
CLI

```
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	传输	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 查找发送到 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 Admin” 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。所有安全区段都在 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

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[15]

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

15. 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: 5631[16]

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: 5983[17]

Map to Service: LDAP

Map to IP: 10.1.1.5

16. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

17. 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 interface ethernet3 vip 1.1.1.3 + 80 http 10.1.1.4
set interface ethernet3 vip 1.1.1.3 + 5631 pcanywhere 10.1.1.4[18]
set interface ethernet3 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
```

18. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

索引

X

Y

Z