NetScreen 概念与范例

ScreenOS 参考指南

第 2 卷：基本原理

ScreenOS 5.1.0

编号 093-1367-000-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 2 卷，“基本原理”介绍了 ScreenOS 的体系结构及其组成元素，包括配置不同元素的范例。本卷介绍以下内容：

- ScreenOS 体系结构概述
- 安全性、通道和功能区段
- 各种接口类型，如物理接口、子接口、虚拟安全接口 (VSI)、冗余接口、聚合接口和 VPN 通道接口
- NetScreen 接口可以在其下运行的接口模式：网络地址转换 (NAT)、路由和透明
- 用来控制流过接口的信息流的策略，以及用来创建策略和虚拟专用网的元素，如地址、用户和服务
- 信息流管理方面的概念
- 下列功能的系统参数：
  - “域名系统” (DNS) 寻址
  - 用于分配或转递 TCP/IP 设置的 “动态主机配置协议” (DHCP)
  - URL 过滤
  - 向 NetScreen 设备上传以及从 NetScreen 设备下载配置设置和软件
  - 用来扩展 NetScreen 设备功能的许可密钥
  - 系统时钟配置

约定

本文档包含几种类型的约定，以下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：

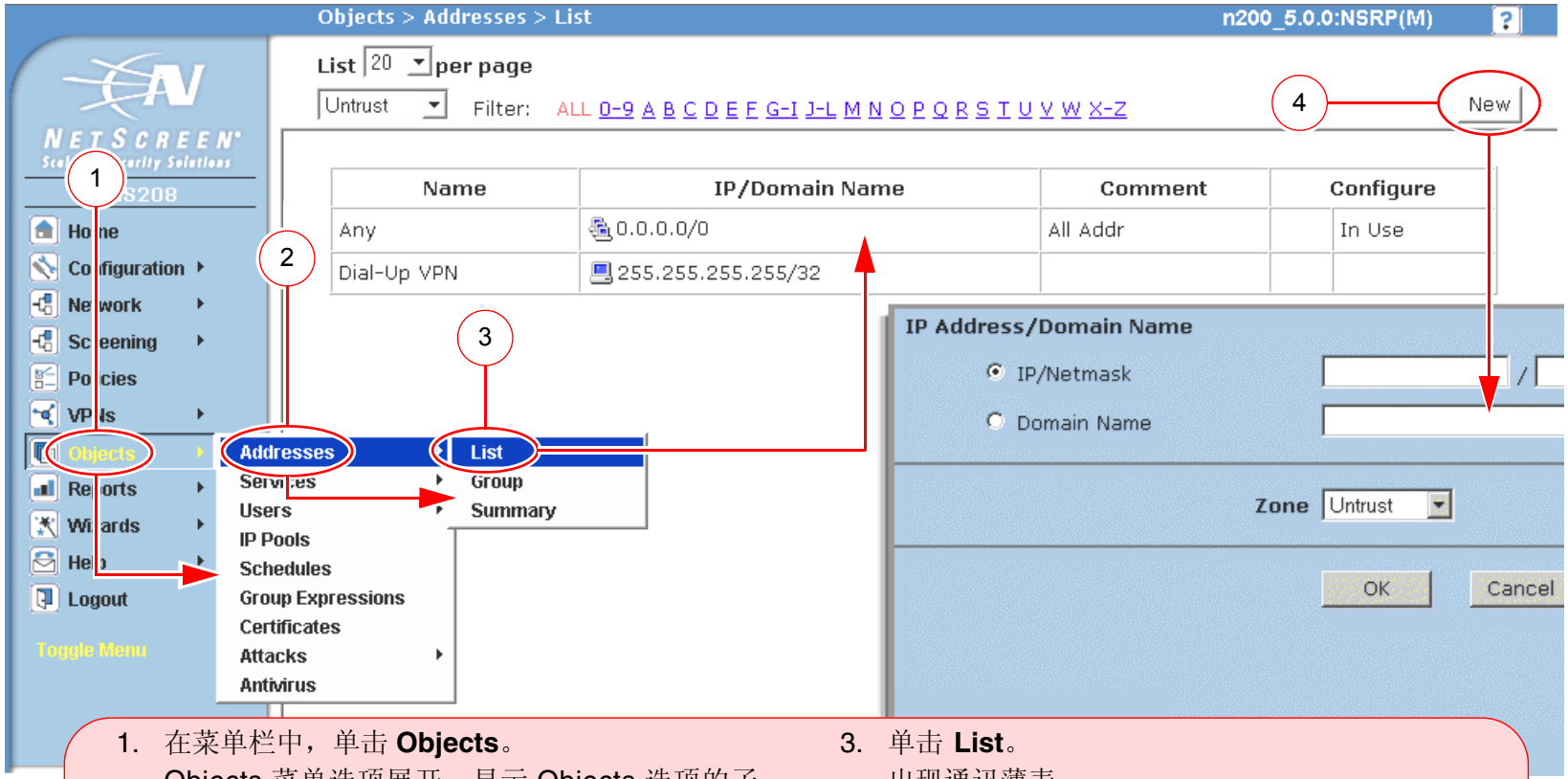
  ```
  set admin user name password
  ```

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

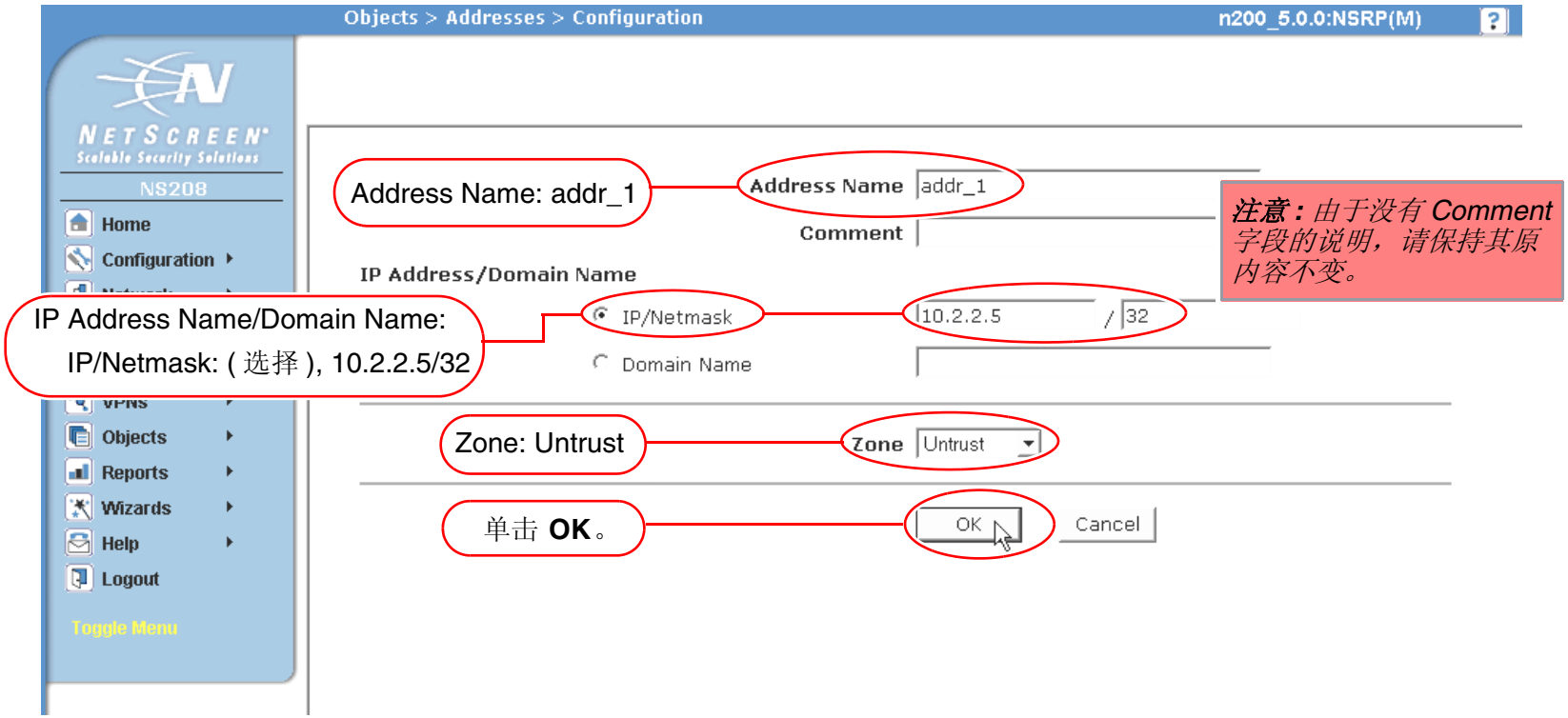
贯穿本书的全部篇章，用一个 V 形符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。例如，指向地址配置对话框的路径显示为 **Objects > Addresses > List > New**。此导航序列如下所示。



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

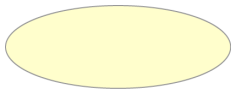


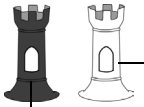
插图约定

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

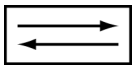

安全区段


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

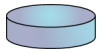

VPN 通道


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

ScreenOS 体系结构

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

本章将对 ScreenOS 进行简要介绍，其中包括以下几个主要内容：

此外，要更好地了解 ScreenOS 处理信息流的机制，请参阅第 12 页上的 “数据包流序列”中的内向数据包流序列。

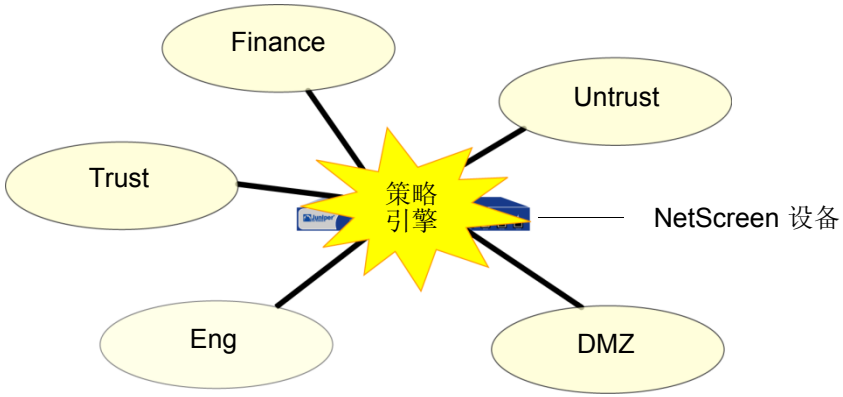
本章结束时将给出一个由四部分组成的范例，它例举了使用 ScreenOS 的 NetScreen 设备的基本配置：

安全区段

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

配置了 5 个安全区段的网络 — 3 个缺省区段 (Trust、Untrust、DMZ) 和 2 个用户定义区段 (Finance、 Eng)

信息流 (以黑线表示) 只有在策略允许时才能由一个安全区段传递到另一区段。



1. 无需任何网段的安全区段是 global 区段。 (有关详细信息，请参阅 Global 区段第 32 页上的 “Global 区段”。) 另外，任何区段，如果既没有与之绑定的接口也没有通讯簿条目，也可以认为它不包含任何网段。
2. 如果是从 ScreenOS 的早期版本进行升级，则这些区段的所有配置将保持不变。
3. 不能删除预定义安全区段。但是，可以删除用户定义的区段。删除安全区段时，也将自动删除为该区段配置的所有地址。

安全区段接口

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

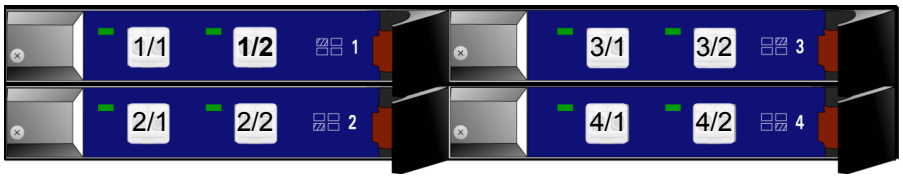
通过定义的策略，可使两个区段间的信息流实现单向或双向流动[4]。利用定义的路由，可指定信息流从一个区段到另一个区段必须使用的接口。由于可将多个接口绑定到一个区段上，所以制定的路由对于将信息流引向所选择的接口十分重要。

要允许信息流从一个区段流到另一个区段，需要将一个接口绑定到该区段，并且对于 “路由” 或 NAT 模式的接口 (参阅第 4 章，“接口模式”) 而言，还需要为该接口分配一个 IP 地址。两种常见的接口类型为物理接口和用于具有虚拟系统支持的设备的子接口 (即物理接口在第 2 层的具体体现)。有关详细信息，请参阅第 3 章，“接口”。

物理接口

物理接口与 NetScreen 设备上实际存在的组件有关。接口命名约定因设备的不同而变化。例如，对于 NetScreen-500，物理接口由接口模块的位置及该模块上的以太网端口标识。例如，接口 *ethernet1/2* 表示接口模块在**第一槽位** *(ethernet**1**/2)* 和**第二个端口** *(ethernet1/**2**)*。

物理接口分配



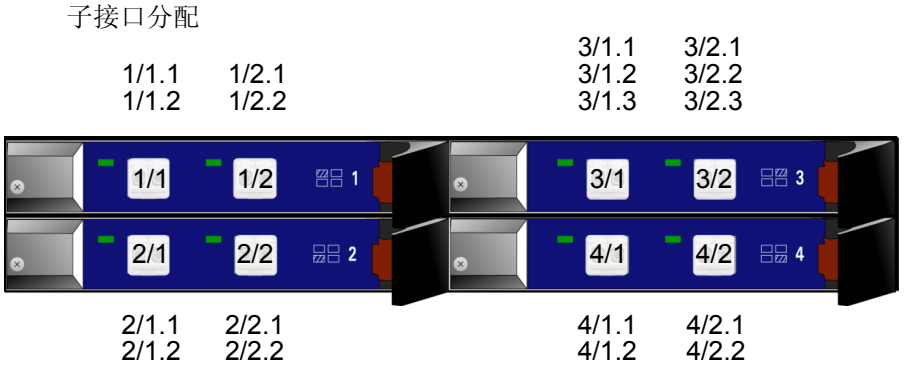
***注意：**要了解具体的 NetScreen 设备的命名约定，请参阅该设备的 “用户指南”。*

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

子接口

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

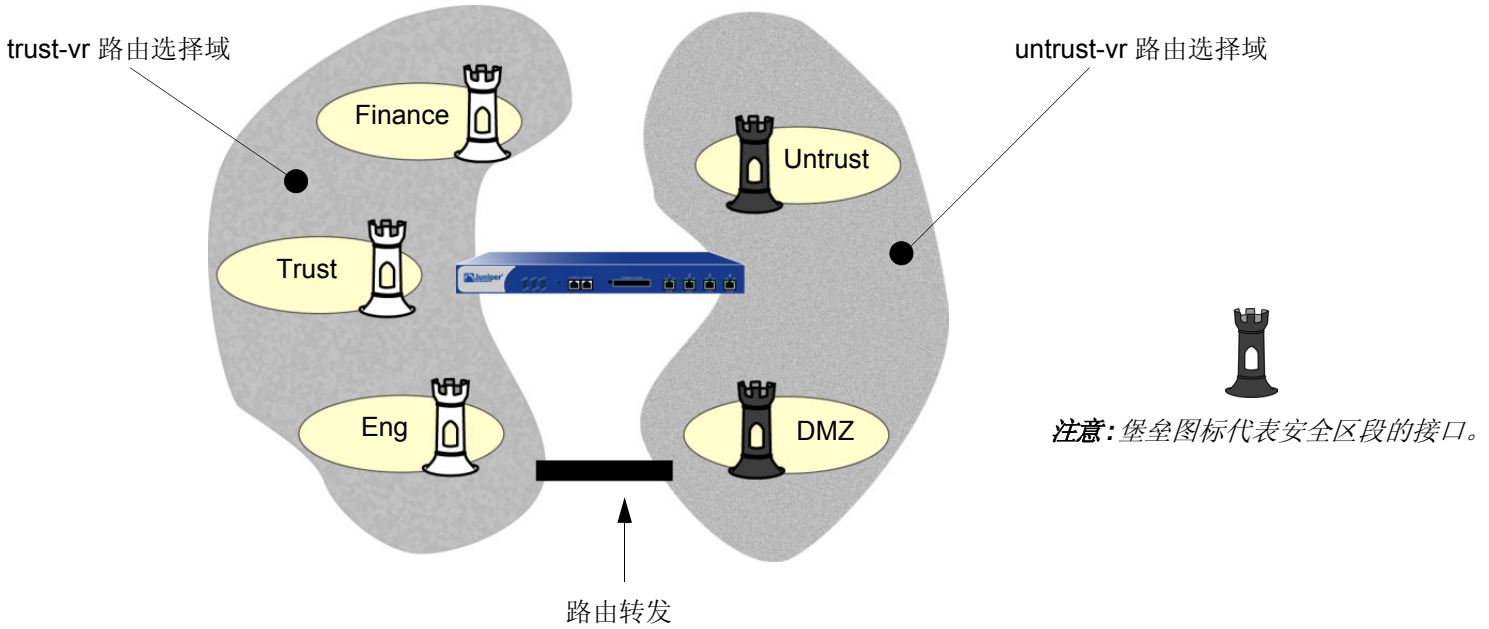
请注意，虽然子接口与物理接口共享部分标识，但是其绑定的区段并不依赖于物理接口绑定的区段。您可以将子接口 *ethernet1/2.3* 绑定到与物理接口 *ethernet1/2* 或 *ethernet1/2.2* 所绑定的不同区段上。同样， IP 地址的分配也没有限制。术语 *子接口*并不意味着其地址在物理接口地址空间的子网中。



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

虚拟路由器

虚拟路由器 (VR) 的功能与路由器相同。它拥有自己的接口及自己的单播和组播路由表。在 ScreenOS 中，NetScreen 设备支持两个预定义的虚拟路由器。这将允许 NetScreen 设备维护两个单独的单播和组播路由表，同时隐藏虚拟路由器彼此之间的路由信息。例如， untrust-vr 通常用来与不可信方进行通信，并且不包含保护区段的任何路由信息。保护区段的路由信息由 trust-vr 进行维护。因此，将无法通过从 untrust-vr 中秘密提取路由的方式来搜集任何内部网络信息。



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

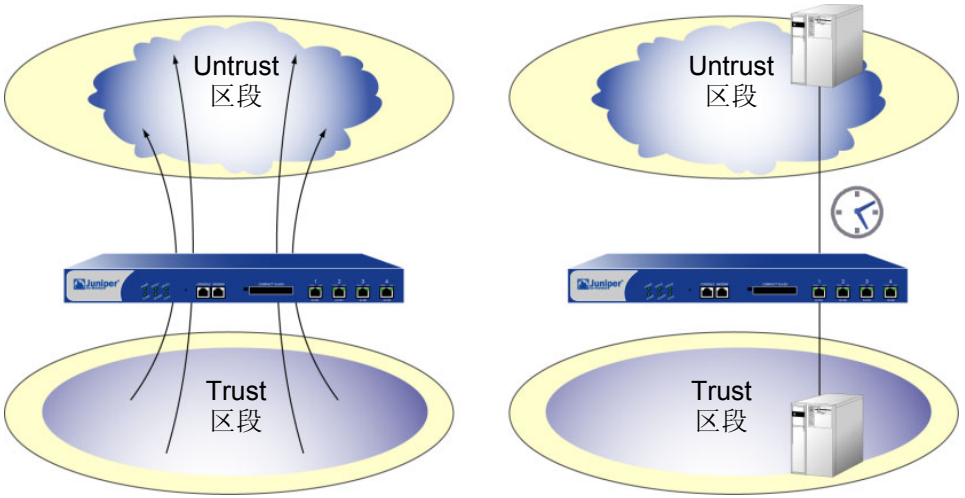
策略

NetScreen 设备用于保护网络的安全，它对所有要求穿过一个安全区段到另一区段的连接尝试都进行检查，然后予以通过或拒绝。

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

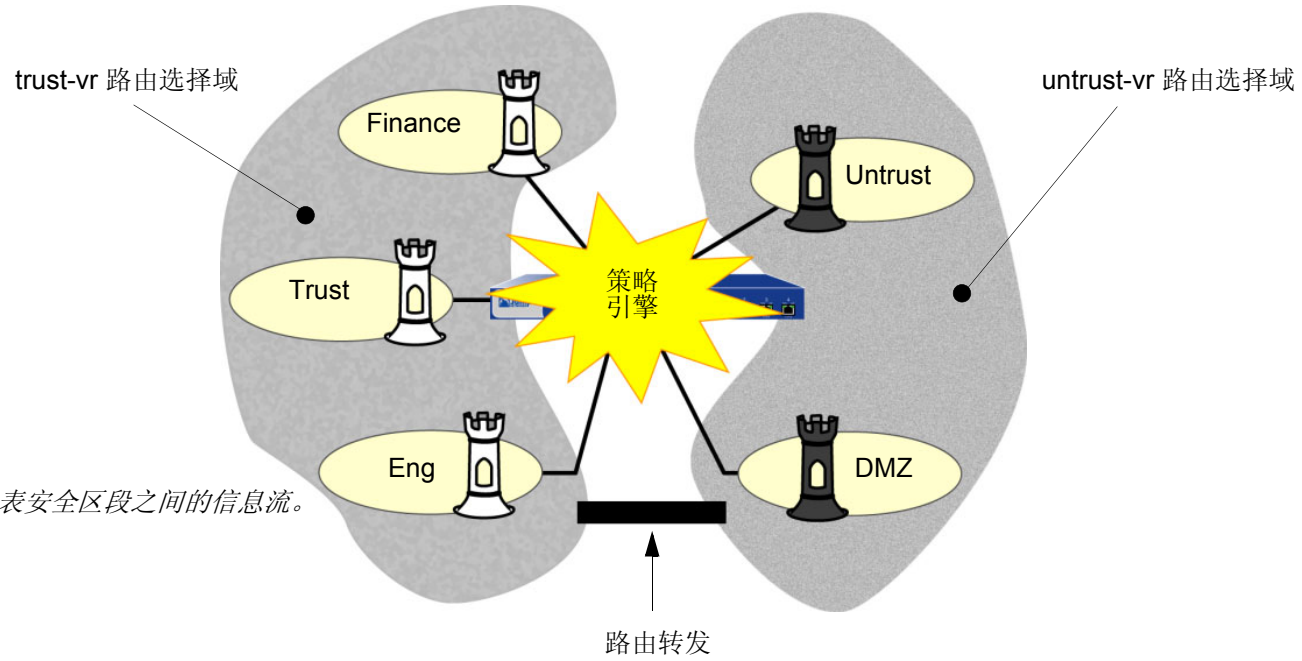
广义的互联网访问：任何服务可在任何时间从 Trust 区段的任何一点到 Untrust 区段的任何一点

狭义的互联网访问：SMTP 服务可在 5:00 AM 到 7:00 PM，从 Trust 区段的邮件服务器到 Untrust 区段的邮件服务器



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

每次当数据包尝试从一个区段向另一区段传递或在绑定到同一区段的两个接口间传递时，NetScreen 设备都会检查其策略组列表中是否有允许这种信息流的策略 (请参阅第 298 页上的 “策略组列表”)。要使信息流可以从一个安全区段传递到另一个区段 (例如，从区段 A 到区段 B)，必须配置一个允许区段 A 向区段 B 发送信息流的策略。要使信息流向另一方向流动，必须配置另一策略，允许信息流从区段 B 流向区段 A。对于从一个区段向另一区段传递的任何信息流，都必须有允许它的策略。同样，如果启用了内部区段阻塞，则必须要有允许信息流在该区段中从一个接口向另一个接口传递的策略。



注意：*黑线代表安全区段之间的信息流。*

注意：*有关策略方面的详细信息，请参阅第 6 章，“策略”。*

如果在 NetScreen 设备上配置组播路由，则可能必须配置组播策略。缺省情况下， NetScreen 设备不允许区段间的组播控制信息流。组播控制信息流是通过组播协议 (如 “协议无关组播” (PIM)) 传输的消息。组播策略仅控制组播控制信息流的流动。要允许数据信息流 (既包括单播也包括组播) 在区段间通过，必须配置防火墙策略。 (有关组播策略的信息，请参阅第 **6** -202 页上的 “组播策略”。)

VPN

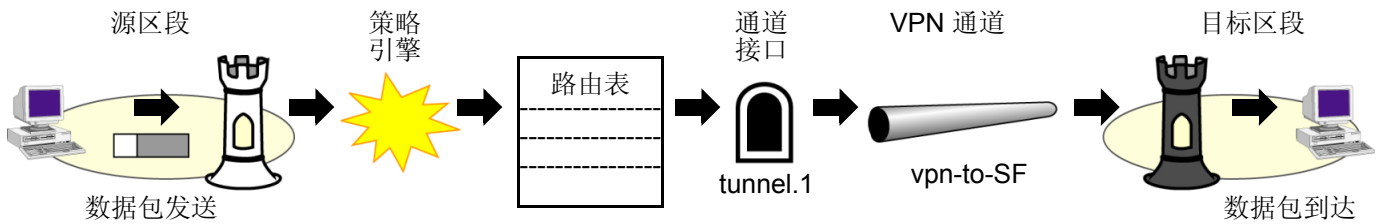
ScreenOS 支持多种虚拟专用网络 (VPN) 配置选项。两种主要类型如下所示：

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

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

以下步骤将介绍基于路由的 VPN 配置中涉及到的主要元素：

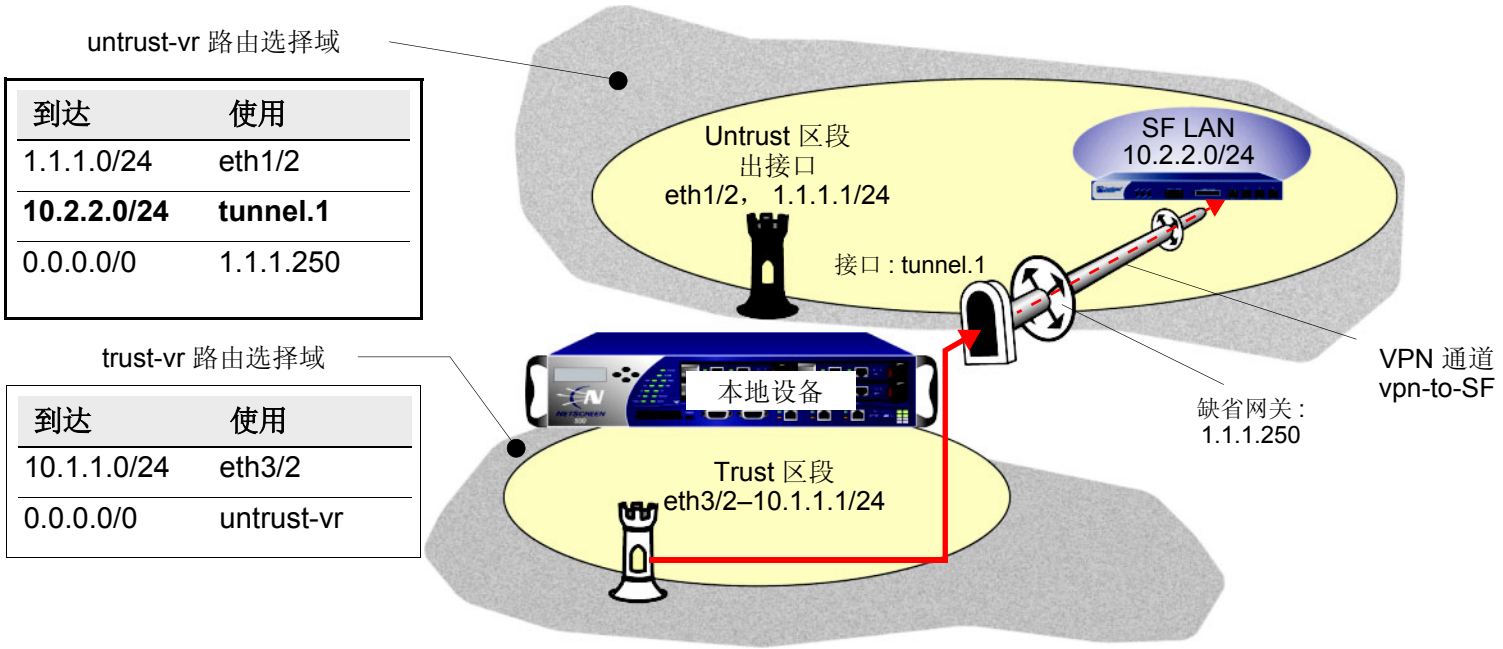
1. 配置 VPN 通道时 (例如， *vpn-to-SF*，其中 *SF* 为目标或端实体)，将本地设备上的一个物理接口或子接口指定为出接口。 (远程对等方配置其远程网关时，必须使用此接口的 IP 地址。)
2. 创建一个通道接口 (例如， *tunnel.1*)，将其绑定到一个安全区段[7]。
3. 将通道接口 *tunnel.1* 绑定到 VPN 通道 *vpn-to-SF* 上。
4. 要引导信息流通过此通道，请设置一个路由，指明到 *SF* 的信息流必须使用 *tunnel.1*。



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

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

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

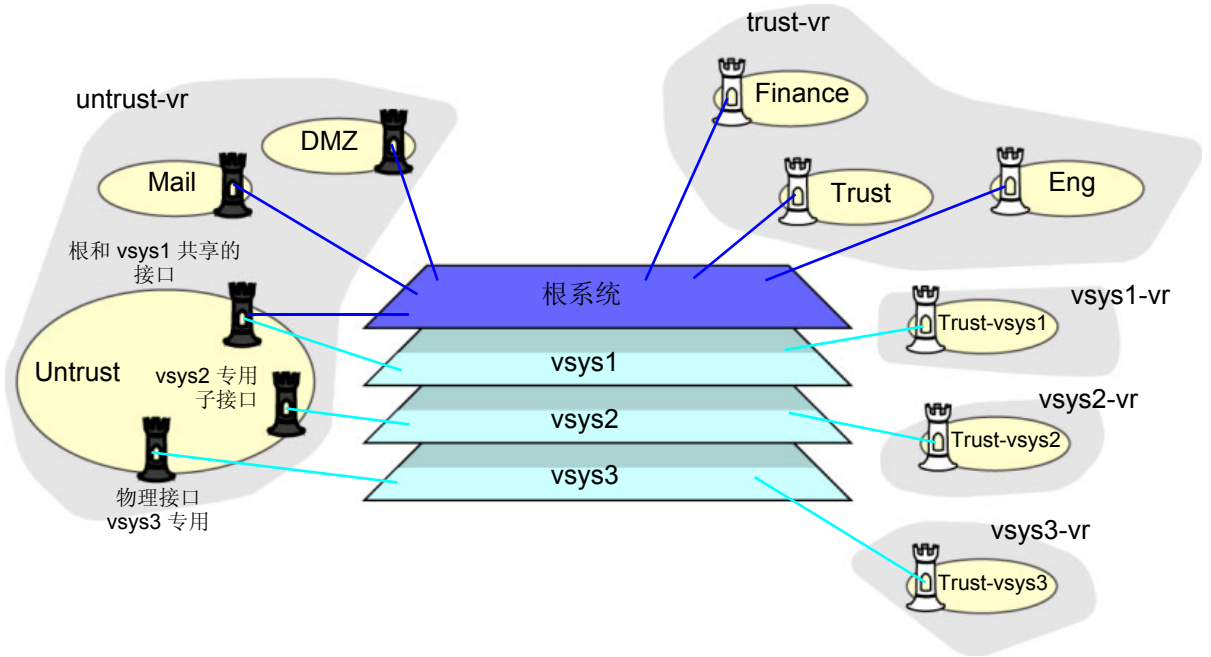


***注意：**有关 VPN 的详细信息，请参阅第 5 卷，“VPN”。*

虚拟系统

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

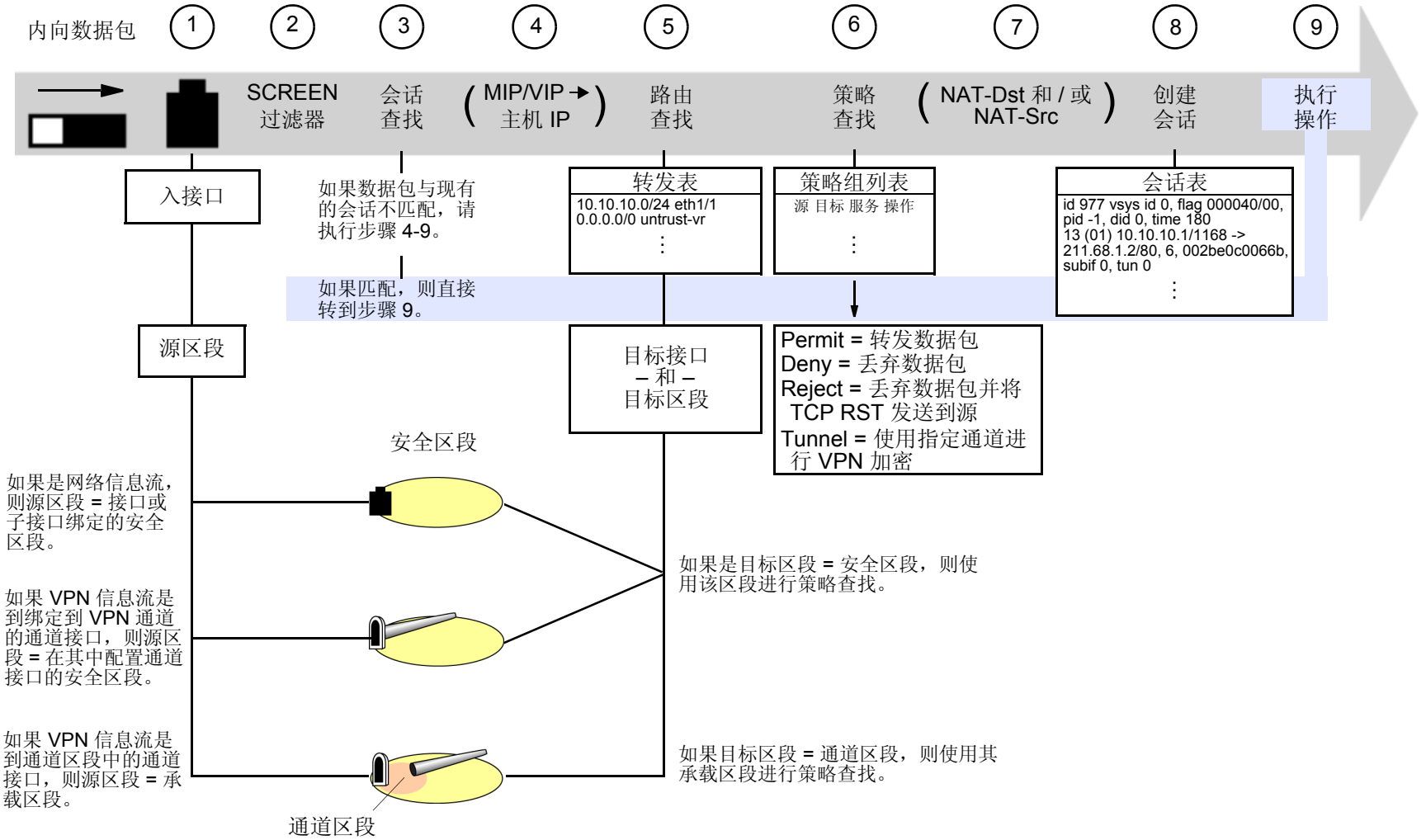
注意：*堡垒图标代表安全区段接口。*



注意：*有关虚拟系统以及在虚拟系统环境中应用区段、接口和虚拟路由器的详细信息，请参阅第 9 卷，“虚拟系统”。*

数据包流序列

在 ScreenOS 中，内向数据包的流序列按如下所示的方式进行。



1. 接口模块识别入接口，进而识别绑定到该接口的源区段。

   源区段根据以下判别条件进行确定：

   – 如果包没有封装，则源区段为入接口或子接口绑定的安全区段。
   – 如果包进行了封装并且通道接口绑定到 VPN 通道上，则源区段为在其中配置通道接口的安全区段。
   – 如果包进行了封装并且通道接口位于通道区段，则源区段为该通道区段相应的承载区段 (*携带* 通道区段的安全区段)。

2. 此时，如果启用了源区段的 SCREEN 选项，则 NetScreen 设备将激活 SCREEN 模块。 SCREEN 检查可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 (对此行为已配置 NetScreen 设备记录事件但不封锁数据包)，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。

3. 会话模块执行会话查找，尝试用现有会话与该数据包进行匹配。

   如果该数据包与现有会话不匹配， NetScreen 设备会执行 “首包处理”，该过程包括下面的步骤 4 到 9。

   如果该包与现有会话匹配， NetScreen 设备会执行 “快速处理”，用现有会话条目中可用的信息来处理该数据包。“快速处理”会跳过步骤 4 到 8，因为这些步骤产生的信息已经在会话的首包处理期间获得。

4. 如果使用映射 IP (MIP) 或虚拟 IP (VIP) 地址，地址映射模块会对 MIP 或 VIP 进行解析以便路由表能查找到实际的主机地址。

5. 路由表查找程序将寻找指向目标地址的接口。同时，接口模块识别该接口绑定的目标区段。

   目标区段根据以下判别条件进行确定：

   – 如果目标区段是安全区段，请使用该区段进行策略查找。
   – 如果目标区段是通道区段，请使用相应的承载区段进行策略查找。
   – 如果目标区段与源区段相同且禁用了该区段的内部区段阻塞，则 NetScreen 设备将跳过步骤 6 和 7 然后创建一个会话 (步骤 8)。如果启用内部区段阻塞，则 NetScreen 设备将丢弃数据包。

6. 策略引擎搜寻策略组列表，以便在识别出的源和目标区段中的地址之间查找策略。

   在策略中配置的操作决定了 NetScreen 防火墙将对包执行的动作：

   - 如果操作为 **Permit**， NetScreen 设备会决定将数据包转发到其目标地点。
   - 如果操作为 **Deny**， NetScreen 设备会决定将数据包丢弃。
   - 如果操作为 **Reject**， NetScreen 设备会决定将数据包丢弃并且如果协议为 TCP，它会将重置信号 (RST) 发送到源 IP 地址。
   - 如果操作为 **Tunnel**， NetScreen 设备会决定将数据包转发给 VPN 模块，该模块对数据包进行封装并用指定的 VPN 通道设置进行传送。

7. 如果策略中指定了目标地址转换 (NAT-dst)，则 NAT 模块会将 IP 数据包包头中的初始目标地址转换成一个不同的地址。

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

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

8. 会话模块将在会话表中创建一个新条目，其中包含步骤 1 到 7 的结果。

   随后， NetScreen 设备使用该会话条目中所含的信息来处理同一会话的后续数据包。

9. NetScreen 设备执行在会话中指定的操作。

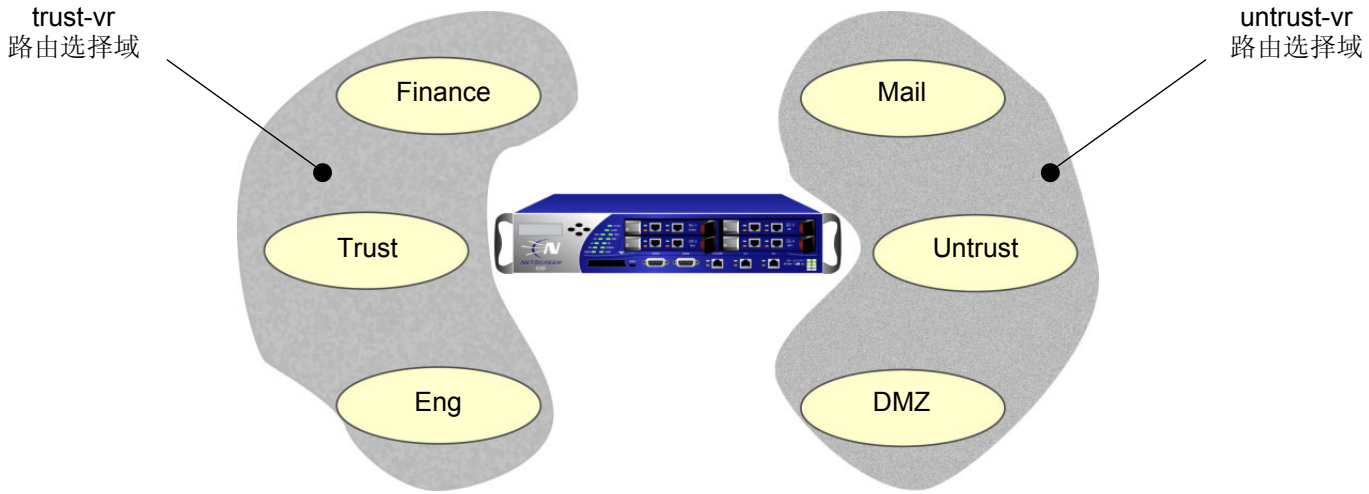
   典型的操作有源地址转换、 VPN 通道选择、加密、解密和包转发。

范例 (第 1 部分): 具有六个区段的企业

共有四部分范例，这是第一部分，其目的是为了说明前面几节介绍的部分概念。在第二部分中将设置每个区段的接口，请参阅第 17 页上的 “范例 (第 2 部分): 六个区段的接口”。在这里将为企业配置以下六个区段 :

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

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



8. 有关虚拟路由器及其路由选择域的详细信息，请参阅第 6 卷 “动态路由”。

WebUI

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

Zone Name: Finance

Virtual Router Name: trust-vr

Zone Type: Layer 3: (选择)

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

Zone Name: Eng

Virtual Router Name: trust-vr

Zone Type: Layer 3: (选择)

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

Zone Name: Mail

Virtual Router Name: untrust-vr

Zone Type: Layer 3: (选择)

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

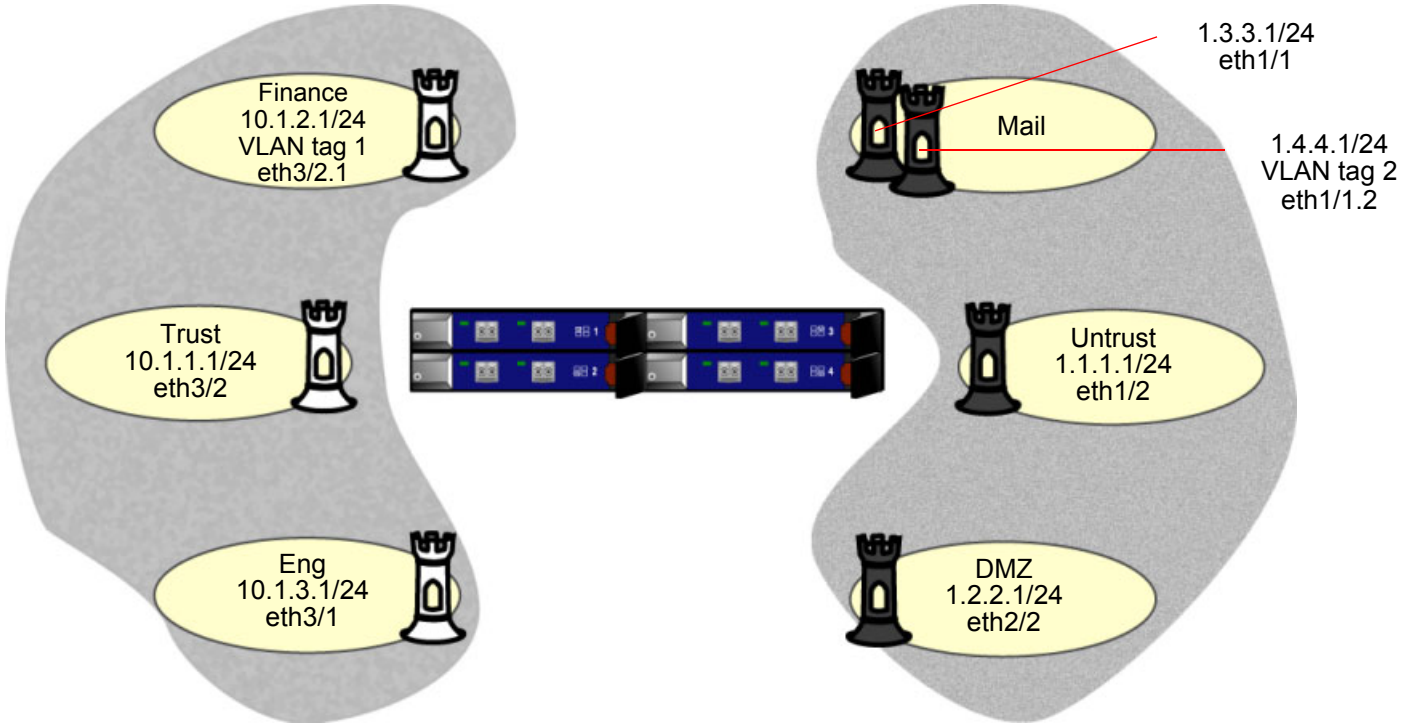
Network > Zones > Edit (对于 DMZ): 在 Virtual Router Name 下拉列表中选择 **untrust-vr**，然后单击 **OK**。

CLI

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

范例 (第 2 部分): 六个区段的接口

这是一个渐进式范例的第二部分。在第一部分中对区段进行了配置，请参阅第 15 页上的 “范例 (第 1 部分): 具有六个区段的企业”。在下一部分中，将对虚拟路由器进行配置，请参阅第 21 页上的 “范例 (第 3 部分): 两个路由选择域”。范例的这一部分将演示如何将接口绑定到区段上并为其配置 IP 地址和各种管理选项。



WebUI

1. 接口 ethernet3/2

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

   Zone Name: Trust

   Static IP: (出现时选择此选项)

   IP Address/Netmask: 10.1.1.1/24

   Manageable: (选择)

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

   Other Services: Ping (选择)

2. 接口 ethernet3/2.1

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

   Interface Name: ethernet3/2.1

   Zone Name: Finance

   Static IP: (出现时选择此选项)

   IP Address/Netmask: 10.1.2.1/24

   VLAN Tag: 1

   Other Services: Ping (选择)

3. 接口 ethernet3/1

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

   Zone Name: Eng

   Static IP: (出现时选择此选项)

   IP Address/Netmask: 10.1.3.1/24

   Other Services: Ping (选择)

4. 接口 ethernet1/1

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

Zone Name: Mail

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.3.3.1/24

5. 接口 ethernet1/1.2

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

Interface Name: ethernet1/1.2

Zone Name: Mail

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.4.4.1/24

VLAN Tag: 2

6. 接口 ethernet1/2

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Manageable: (选择)

Management Services: SNMP(选择)

7. 接口 ethernet2/2

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

Zone Name: DMZ

Static IP: (选择)

IP Address/Netmask: 1.2.2.1/24

CLI

1. 接口 ethernet3/2

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

2. 接口 ethernet3/2.1

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

3. 接口 ethernet3/1

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

4. 接口 ethernet1/1

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

5. 接口 ethernet1/1.2

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

6. 接口 ethernet1/2

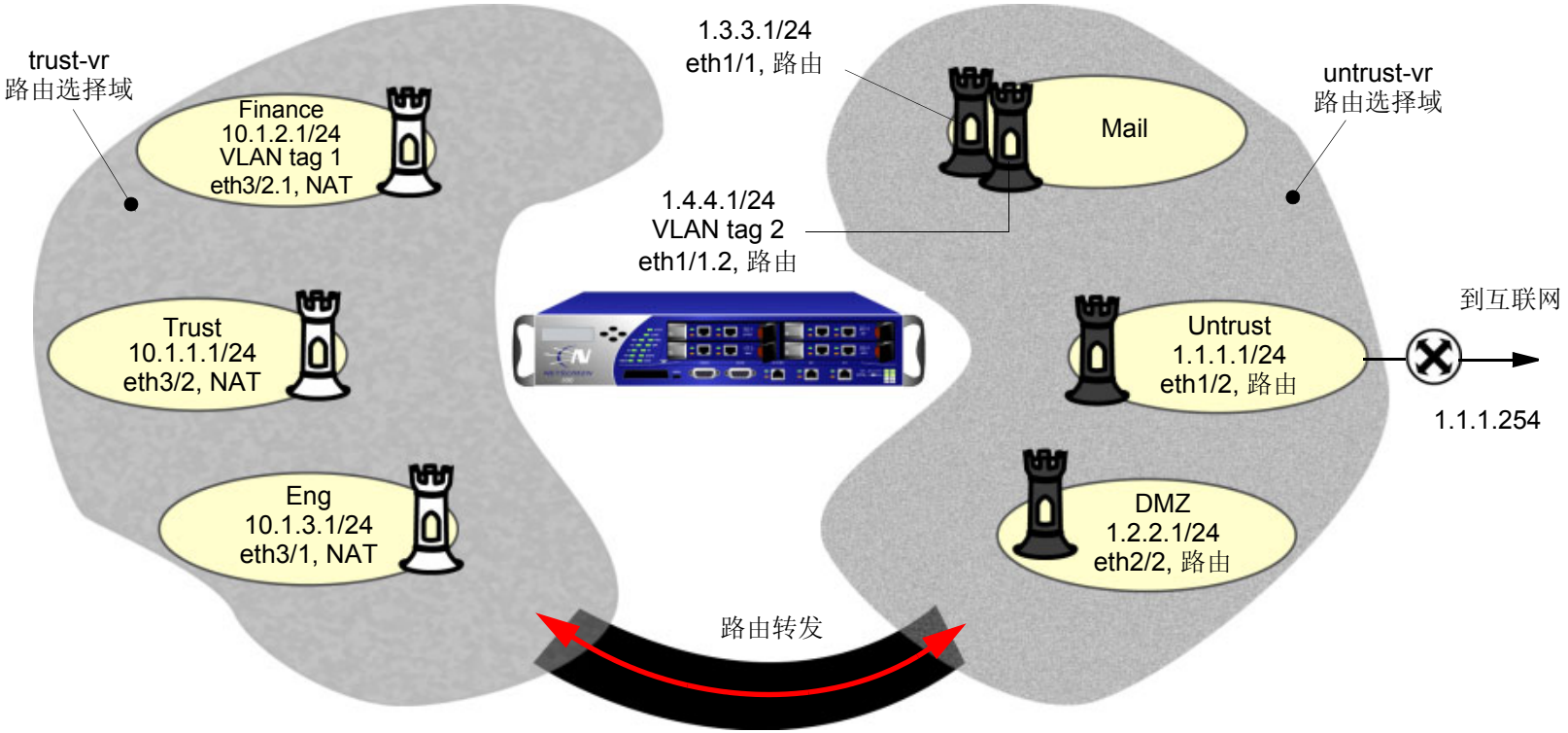
```
set interface ethernet1/2 zone untrust
set interface ethernet1/2 ip 1.1.1.1/24
set interface ethernet1/2 manage snmp
```

7. 接口 ethernet2/2

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

范例 (第 3 部分): 两个路由选择域

这是一个渐进式范例的第三部分。在上一部分中，对多个安全区段的接口进行了定义，请参阅第 17 页上的 “范例 (第 2 部分): 六个区段的接口”。在下一部分中，将对策略进行设置，请参阅第 23 页上的 “范例 (第 4 部分): 策略”。在本例中，您只需为连接到互联网的缺省网关配置路由。其它路由在您创建接口 IP 地址时由 NetScreen 设备自动创建。



WebUI

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

Network Address/Netmask: 0.0.0.0/0

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

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet1/2

Gateway IP Address: 1.1.1.254

CLI

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

NetScreen 设备自动创建以下路由 (黑色):

trust-vr

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

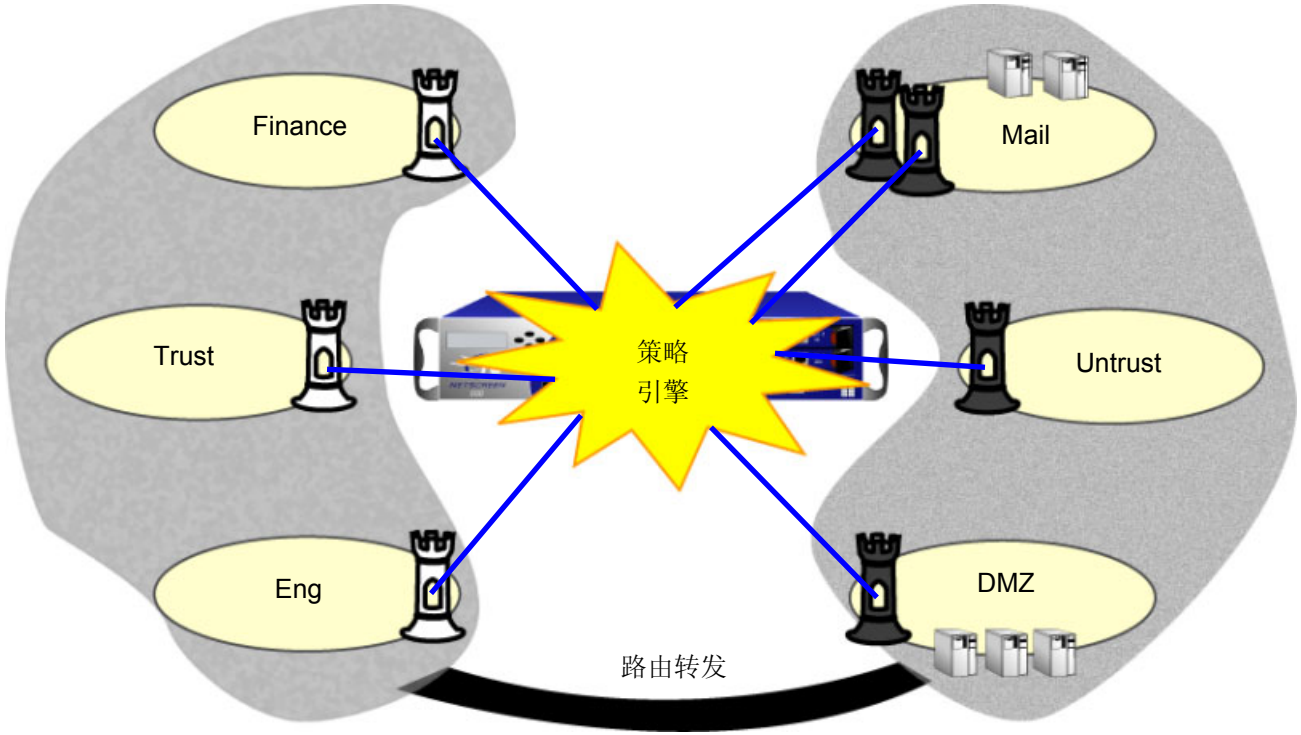
untrust-vr

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

注意 : 只有这些条目由用户配置。

范例 (第 4 部分): 策略

这是一个渐进式范例的最后一部分。上一部分为第 21 页上的 “范例 (第 3 部分): 两个路由选择域”。范例的这一部分演示如何配置新的策略。



为达到本例的目的，在开始配置新策略前，您需要创建新的服务组。

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

WebUI

1. 服务组

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

Group Name: Mail-Pop3

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

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

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

Group Name: HTTP-FTPGet

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

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

2. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail-Pop3

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Mail

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: FTP-Put

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP-FTPGet

Action: Permit

CLI

1. 服务组

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

2. 策略

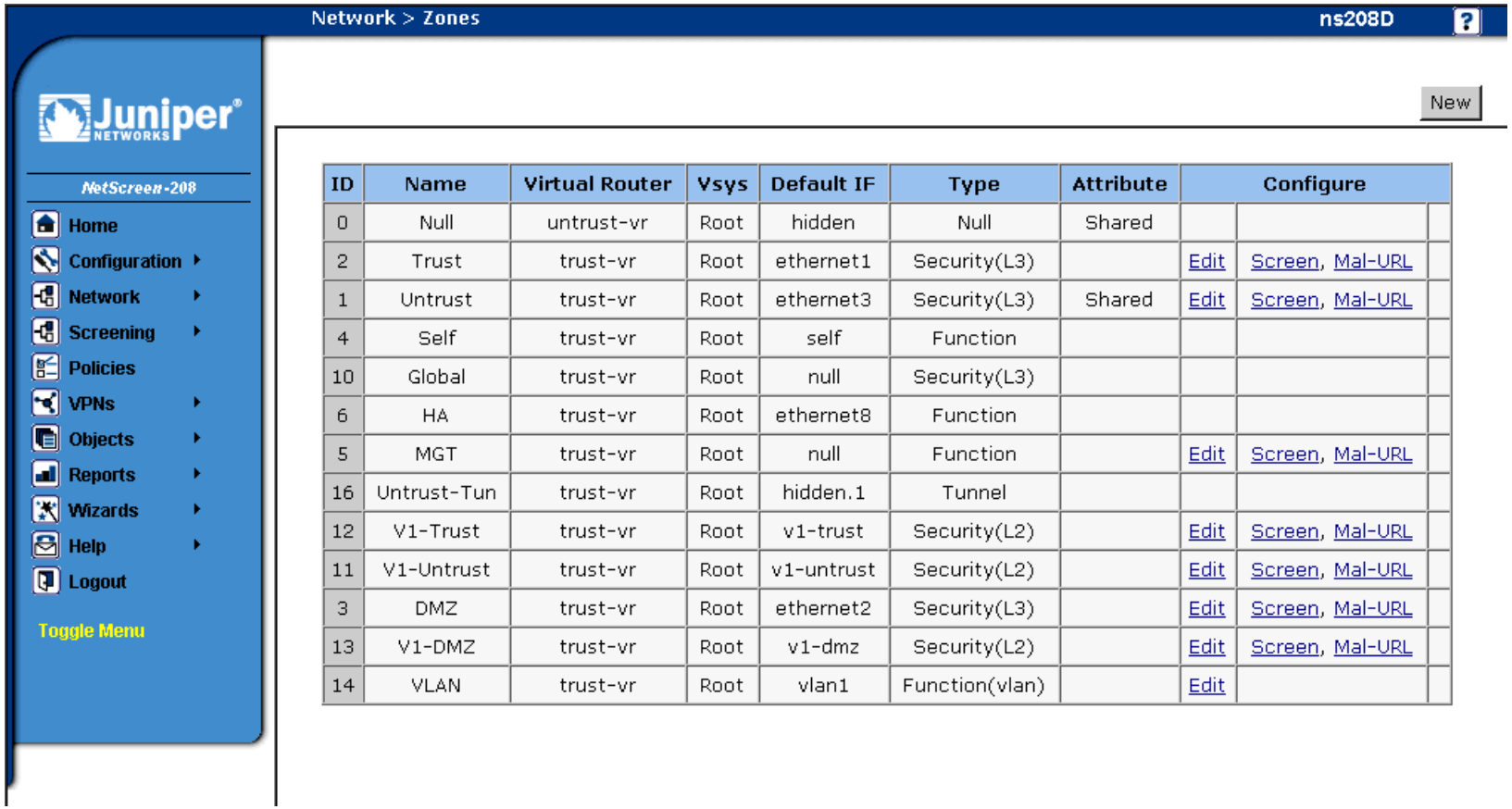
```
set policy from finance to mail any any mail-pop3 permit
set policy from trust to mail any any mail-pop3 permit
set policy from eng to mail any any mail-pop3 permit
set policy from untrust to mail any any mail permit
set policy from finance to untrust any any http-ftpget permit
set policy from finance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

2

区段

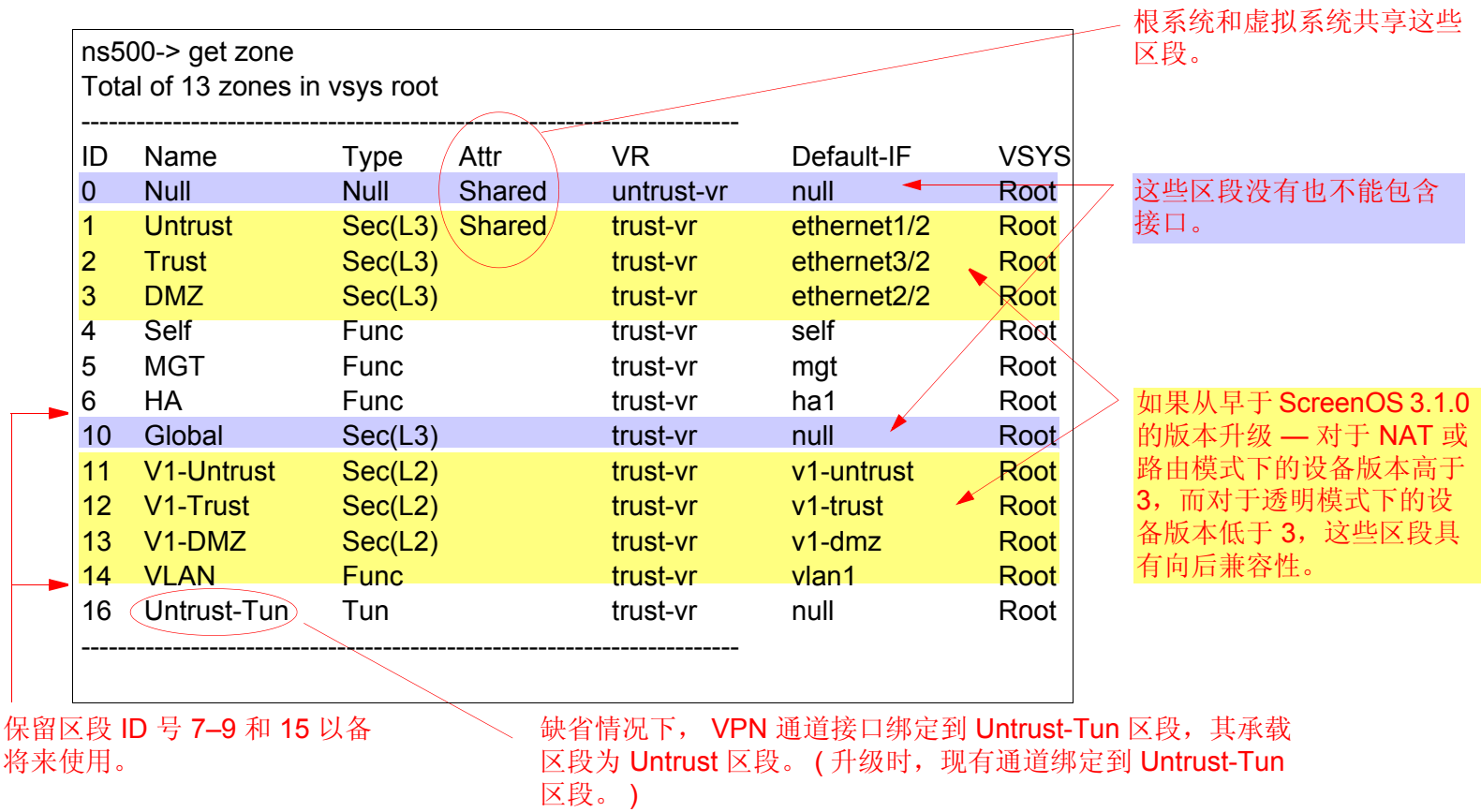
区段可以是网络空间中应用了安全措施的部分 (安全区段)、绑定了 VPN 通道接口的逻辑部分 (通道区段)，或者是执行特定功能的物理或逻辑实体 (功能区段)。本章将对每种类型的区段逐一进行介绍，特别将重点放在安全区段上。本章由以下几节组成：

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



ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure	
0	Null	untrust-vr	Root	hidden	Null	Shared		
2	Trust	trust-vr	Root	ethernet1	Security(L3)		Edit	Screen, Mal-URL
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	Edit	Screen, Mal-URL
4	Self	trust-vr	Root	self	Function			
10	Global	trust-vr	Root	null	Security(L3)			
6	HA	trust-vr	Root	ethernet8	Function			
5	MGT	trust-vr	Root	null	Function		Edit	Screen, Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel			
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)		Edit	Screen, Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)		Edit	Screen, Mal-URL
3	DMZ	trust-vr	Root	ethernet2	Security(L3)		Edit	Screen, Mal-URL
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)		Edit	Screen, Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)		Edit	

get zone 命令的输出为：



可将上图所示的预配置区段分为三种不同的类型：

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

通道区段 : Untrust-Tun

功能区段 : Null、 Self、 MGT、 HA、 VLAN

安全区段

在单个 NetScreen 设备上，可以配置多个安全区段，将网络分成多段，可对这些网段应用各种安全选项以满足各段的需要。至少需要定义两个安全区段，以便对其中的一个网络区段提供基本的保护，使其不受另一区段的影响。在某些 NetScreen 平台上，您可以定义多个安全区段，使网络安全设计具有更高的精确度 — 而且这样做无需配置多个安全设备。

Global 区段

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

Global 区段还包含全局策略中使用的地址。有关全局策略的详细信息，请参阅第 297 页上的 “全局策略”。

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

SCREEN 选项

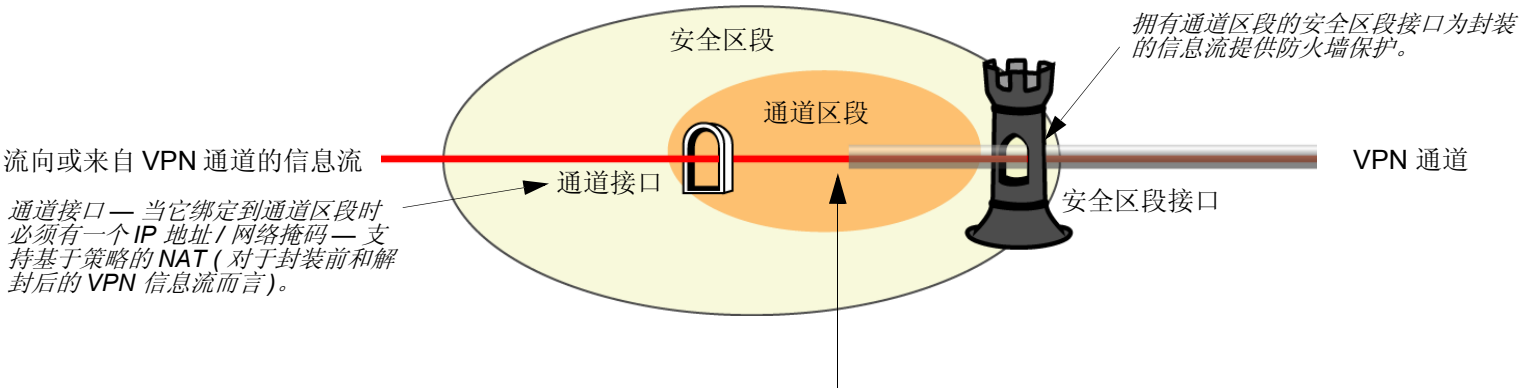
NetScreen 防火墙用于保护网络，具体做法是先检查要求从一个安全区段进入到另一安全区段的所有连接尝试，然后予以允许或拒绝。对于每个安全区段和 MGT 区段，可启用一组预定义的 SCREEN 选项，检测并阻塞 NetScreen 设备将其确定为具有潜在危害的各种信息流。有关多个可用 SCREEN 选项的详细信息，请参阅第 4 卷，“攻击检测和防御机制”。

通道区段

通道区段是一个或多个通道接口的宿主逻辑网段。通道区段在概念上以一种 “子父” 关系附属于安全区段。安全区段充当 “父”，您也可以将其视为承载区段，该区段对封装的信息流提供防火墙保护。通道区段提供数据包封装 / 解封，还提供基于策略的 NAT 服务 (通过支持具有可以拥有映射 IP (MIP) 地址和动态 IP (DIP) 池的 IP 地址和网络掩码的通道接口)。

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

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



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

1. 根系统与所有虚拟系统可以共享 Untrust 区段。但是，每个系统拥有各自单独的 Untrust-Tun 区段。

范例 : 将 Tunnel 接口绑定到 Tunnel 区段

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

WebUI

1. 通道接口

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

   Tunnel Interface Name: tunnel.3

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

   Fixed IP: (选择)

   IP Address / Netmask: 3.3.3.3/24

2. MIP

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

   Mapped IP: 3.3.3.5

   Netmask: 255.255.255.255

   Host IP Address: 10.1.1.5

   Host Virtual Router Name: trust-vr

CLI

1. 通道接口

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

2. MIP

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

配置安全区段和 TUNNEL 区段

第 3 层或第 2 层安全区段及通道区段的创建、修改和删除操作十分相似。

***注意：**您不能删除预定义的安全区段或预定义的通道区段，但是可以编辑它们。*

创建区段

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

WebUI

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

Zone Name: 键入区段名称[2]。

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

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

Block Intra-Zone Traffic: 选择此选项可阻塞同一安全区段中主机之间的信息流。在缺省情况下，禁用区段内部阻塞。

CLI

```
set zone name zone [ l2 vlan_id_num[3] | tunnel sec_zone ]
set zone zone block
set zone zone vrouter name_str
```

2. 第 2 层安全区段的名称必须以“L2-”开头；例如，“L2-Corp”或“L2-Xnet”。
3. 创建第 2 层安全区段时， VLAN ID 号必须为 1 (对于 VLAN1)。

修改区段

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

WebUI

1. 修改区段名称

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

当出现提示，请求对删除操作进行确认时，请单击 **Yes**。

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

2. 更改区段内部阻塞选项或虚拟路由器

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

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

Block Intra-Zone Traffic: 若要启用该功能，请选中此复选框。若要禁用该功能，请清除该复选框。

CLI

1. 修改区段名称

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

2. 更改区段内部阻塞选项或虚拟路由器

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

4. 删除区段前，必须先解除对所有绑定到该区段的接口的绑定。
5. 必须先删除绑定到区段的所有接口，然后再更改该区段的虚拟路由器。

删除区段

要删除安全区段或通道区段，请执行以下任一操作[6]：

WebUI

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

当出现提示，请求对删除操作进行确认时，请单击 **Yes**。

CLI

```
unset zone zone
```

6. 删除区段前，必须先解除对所有绑定到该区段的接口的绑定。要解除接口与区段间的绑定，请参阅第 63 页上的 “将接口绑定到安全区段”。

功能区段

共有五个功能区段，分别是 Null、 MGT、 HA、 Self 和 VLAN。正如以下内容所述，每个区段都有其专门的用途。

Null 区段

此区段用于临时存储没有绑定到任何其它区段的所有接口。

MGT 区段

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

HA 区段

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

Self 区段

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

VLAN 区段

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

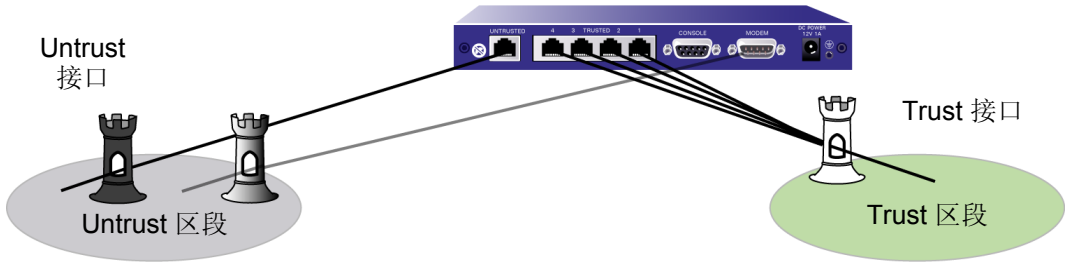
端口模式

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

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

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

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

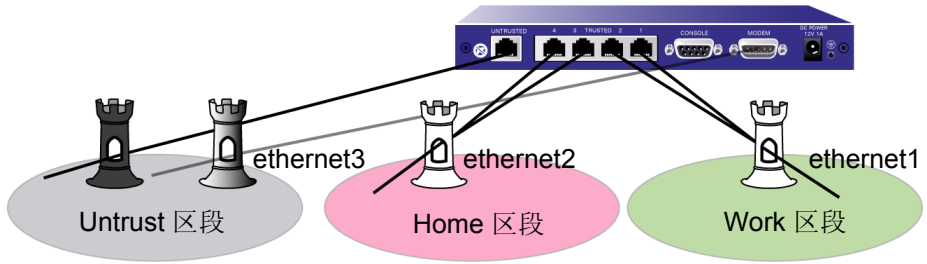


***注意：**对于 NetScreen-5GT 而言， Initial Configuration Wizard (初始配置向导) 稍有不同。*

7. 在端口模式上下文中，*端口*指的是 NetScreen 设备背面的物理接口。通过其标签对端口进行引用：Untrusted、1-4、Console 或 Modem。术语*接口*指的是可以通过 WebUI 或 CLI 配置的逻辑接口。每个端口只能绑定到一个接口，但是却可将多个端口绑定到一个接口。

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

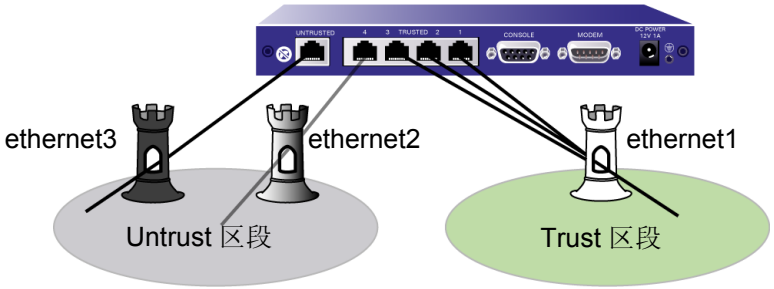
ethernet3 接口是 Untrust 区段的主接口。可以将串行接口 (以灰色显示) 作为备份接口绑定到 Untrust 区段。



有关配置和使用 Home-Work 模式的详细信息，请参阅第 47 页上的 “Home-Work 和 Combined 端口模式下的区段”。

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

ethernet3 接口是 Untrust 区段的主接口。ethernet2 接口 (以灰色显示) 是 Untrust 区段的备份接口。



注意：*串行接口在 Dual Untrust 端口模式下不可用。*

有关配置和使用 Dual Untrust 模式的详细信息，请参阅第 10 卷，“高可用性”。

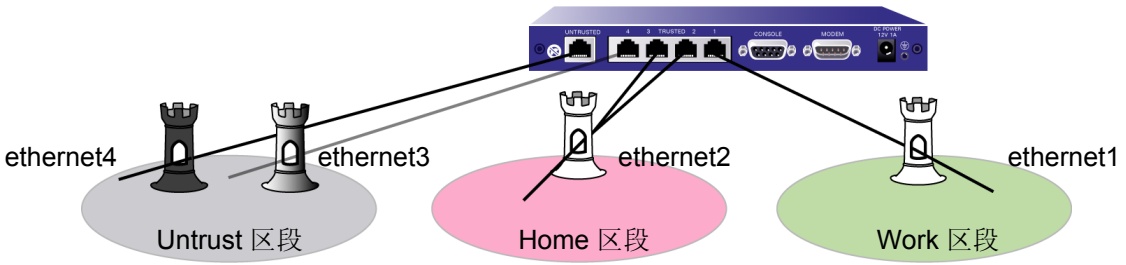
- Combined 模式允许互联网的主接口和备份接口及 Work 和 Home 区段中用户和资源的隔离。

***注意：**对于 NetScreen-5XT，只有 NetScreen-5XT Elite (不受限制的用户) 平台支持 Combined 端口模式。不能使用 Initial Configuration Wizard (初始配置向导) 配置 Combined 模式。只能使用 WebUI 或 CLI 命令配置此模式。*

此模式提供下列端口、接口和区段绑定：

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

ethernet4 接口是 Untrust 区段的主接口。
ethernet3 接口 (以灰色显示) 是 Untrust 区段的备份接口。



***注意：**串行接口在 Combined 端口模式下不可用。*

有关配置和使用 Combined 模式的详细信息，请参阅第 10 卷，“高可用性”和第 47 页上的 “Home-Work 和 Combined 端口模式下的区段”。

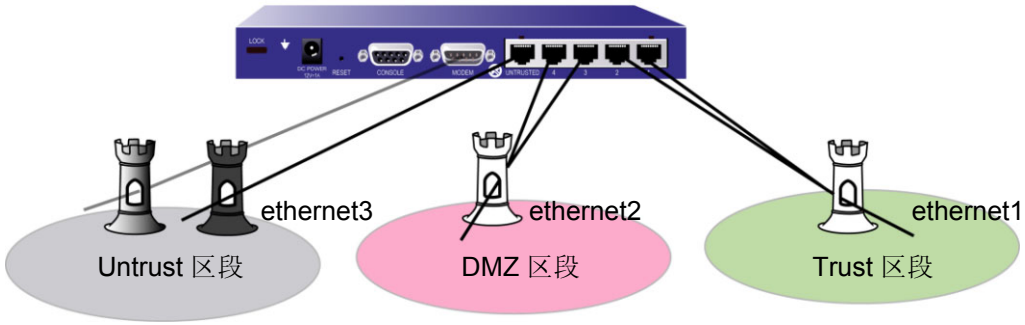
- Trust/Untrust/DMZ (扩展的) 模式将接口绑定到 Untrust、 Trust 和 DMZ 安全区段，允许将 web、电子邮件或其它应用程序服务器与内部网络分开。

  ***注意：**只有 NetScreen-5GT Extended 平台支持 Trust/Untrust/DMZ 端口模式。不能使用 Initial Configuration Wizard (初始配置向导) 配置 Combined 模式。只能使用 WebUI 或 CLI 命令配置此模式。*

  此模式提供下列端口、接口和区段绑定：

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

ethernet3 接口是 Untrust 区段的主接口。可以将串行接口作为备份接口绑定到 Untrust 区段。



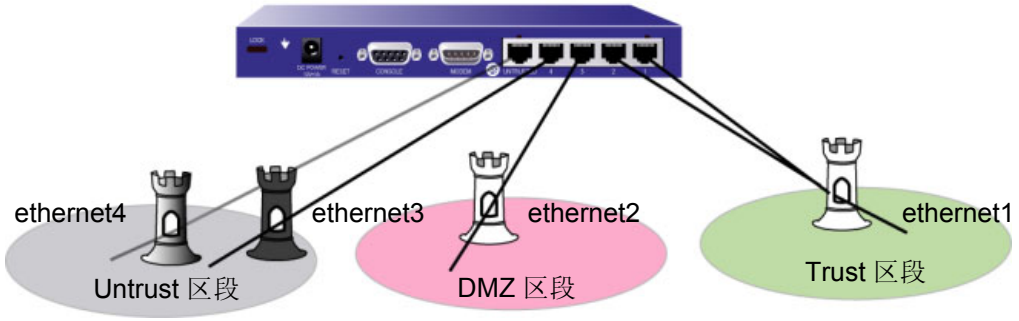
- DMZ/Dual Untrust 模式将接口绑定到 Untrust、 Trust 和 DMZ 安全区段，允许同时传送来自内部网络的信息流。

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

此模式提供下列端口、接口和区段绑定：

- 将以太网端口 1 和 2 绑定到 ethernet1 接口，该接口被绑定到 Trust 安全区段
- 将以太网端口 3 绑定到 ethernet2 接口，该接口被绑定到 DMZ 安全区段
- 将以太网端口 4 绑定到 ethernet3 接口，该接口被绑定到 Untrust 安全区段
- 将 Untrust 以太网端口绑定到 ethernet4 接口，该接口被绑定到 Untrust 安全区段

ethernet3 和 ethernet4 接口同时处于活动状态。在此图中，这两个接口被绑定到了 Untrust 区段以实现负载均衡。



注意：**串行接口在 DMZ/Dual Untrust 端口模式下不可用。要启用故障切换而不是同时传送信息流，请使用* ***set failover enable *命令。*

设置端口模式

下表对 NetScreen ScreenOS 端口模式提供的端口、接口和区段绑定加以汇总：

端口*	Trust-Untrust 模式†		Home-Work 模式		Dual Untrust 模式	
	接口	区段	接口	区段	接口	区段
Untrusted	Untrust	Untrust	ethernet3	Untrust	ethernet3	Untrust
1	Trust	Trust	ethernet1	Work	ethernet1	Trust
2	Trust	Trust	ethernet1	Work	ethernet1	Trust
3	Trust	Trust	ethernet2	Home	ethernet1	Trust
4	Trust	Trust	ethernet2	Home	ethernet2	Untrust
Modem	串行	Null	串行	Null	不适用	不适用

* 在 NetScreen 设备机箱上进行了标注。
† 缺省端口模式

端口*	Combined 模式		Trust/Untrust/DMZ 模式		DMZ/Dual Untrust 模式	
	接口	区段	接口	区段	接口	区段
Untrusted	ethernet4	Untrust	ethernet3	Untrust	ethernet4	Untrust
1	ethernet1	Work	ethernet1	Trust	ethernet1	Trust
2	ethernet2	Home	ethernet1	Trust	ethernet1	Trust
3	ethernet2	Home	ethernet2	DMZ	ethernet2	DMZ
4	ethernet3	Untrust	ethernet2	DMZ	ethernet3	Untrust
Modem	不适用	不适用	串行	Null	不适用	不适用

* 在 NetScreen 设备机箱上进行了标注。

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

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

范例：Home-Work 端口模式

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

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

WebUI

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

在下列提示下，单击 **OK**:

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

CLI

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

在下列提示下，输入 **y** (表示 “是”):

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

Are you sure y/[n] ?

查看 NetScreen 设备上的当前端口模式设置：

WebUI

Configuration > Port Mode

CLI

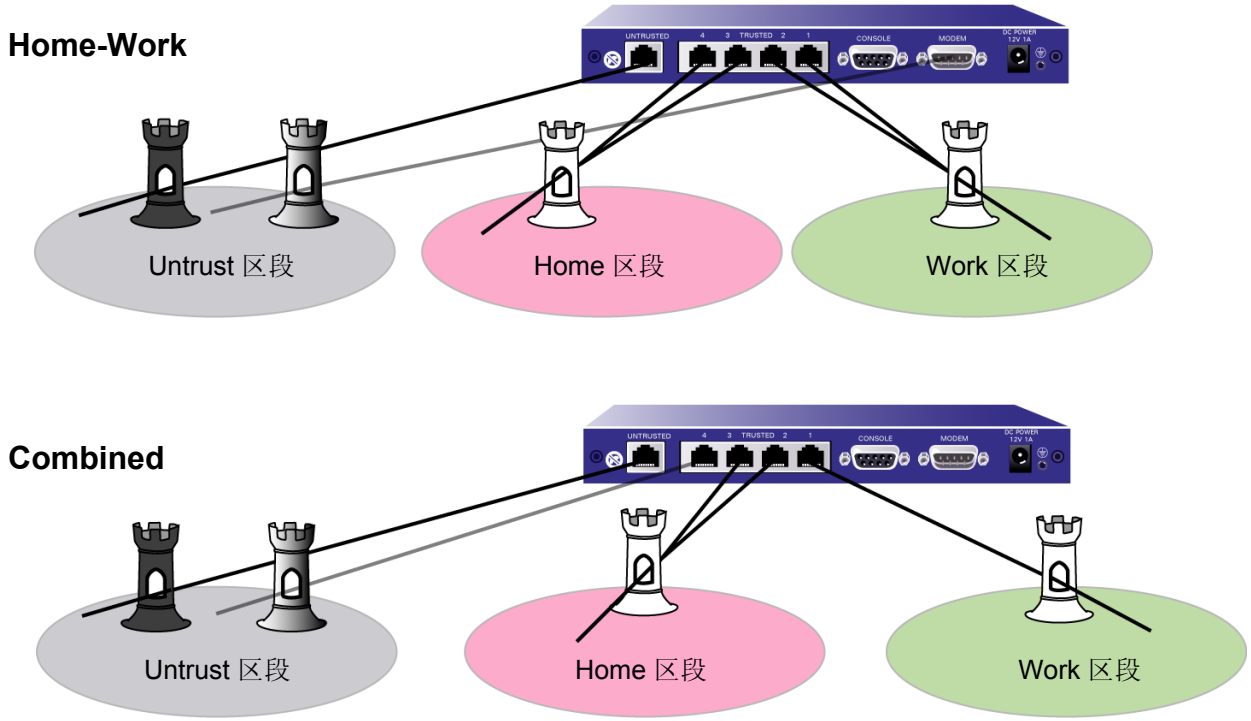
```
get system
```

Home-Work 和 Combined 端口模式下的区段

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

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

8. 可以仅在某些 NetScreen 设备上设置端口模式。请参阅第 39 页上的 “端口模式”。



Home-Work 端口模式也将调制解调器端口绑定到串行接口，可以将其作为备份接口绑定到 Untrust 安全区段。有关使用串行接口作为 Untrust 安全区段的备份接口的详细信息，请参阅第 10 卷，“高可用性”。

Combined 端口模式还将以太网端口 4 绑定到 Untrusted 区段以备份 Untrust 安全端口。仅当 Untrust 区段的主接口出现故障时，才使用备份接口。有关使用 ethernet3 接口作为 Untrust 安全区段的备份接口的详细信息，请参阅第 10 卷，“高可用性”。

在缺省情况下， NetScreen-5XT 充当 “动态主机配置协议” (DHCP) 服务器，为 Work 区段中的 DHCP 客户端分配动态 IP 地址。 (有关 DHCP 服务器的详细信息，请参阅第 372 页上的 “DHCP 服务器”。)

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

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

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

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

范例 : Home-Work 区段

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

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

WebUI

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

在下列提示下，单击 **OK**:

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

此时，系统将重新启动，首先进行登录，然后执行以下操作：

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: FTP

Action: Permit

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

CLI

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

在下列提示下，输入 **y** (表示 “是”):

```
    Change port mode from <trust-untrust> to <home-work> will erase system
         configuration and reboot box
    Are you sure y/[n] ?
```

```
set policy from home to untrust any any ftp permit
unset policy 2
save
```

3

接口

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

本章包括以下各节：

接口类型

本节将对安全区段、功能区段及通道接口逐一进行介绍。有关如何查看所有这些接口的表，请参阅第 61 页上的 “查看接口”。

安全区段接口

物理接口和子接口的作用是提供一个开口，网络信息流可通过它在区段之间流动。

物理接口

NetScreen 设备上的每个端口均表示一个物理接口，且该接口的名称是预定义的。物理接口的名称由媒体类型、插槽号 (对于某些 NetScreen 设备) 及端口号组成，例如， *ethernet3/2* 或 *ethernet2* (另请参阅第 3 页上的 “安全区段接口”)。可将物理接口绑定到可在其中将其充当入口的任何安全区段，信息流通过该入口进出区段。没有接口，信息流就无法访问或退出区段。

在支持对 “接口到区段” 绑定进行修改的 NetScreen 设备上，三个物理以太网接口被预先绑定到特定的第 2 层安全区段 — V1-Trust、 V1-Untrust 和 V1-DMZ。哪个接口绑定到哪个区段根据每个平台而定。 (有关安全区段的详细信息，请参阅第 2 页上的 “安全区段”。)

子接口

同物理接口一样，子接口也可充当信息流进出安全区段的入口。逻辑上，可将一个物理接口分成多个虚拟子接口。每个虚拟子接口都从自己来源的物理接口借用所需的带宽，因此其名称是物理接口名称的扩展，例如， *ethernet3/2.1* 或 *ethernet2.1*。 (另请参阅第 3 页上的 “安全区段接口”。)

可以将子接口绑定到任何区段。还可将子接口绑定到其物理接口所在的区段，也可将其绑定到其它区段。 (有关详细信息，请参阅第 63 页上的 “将接口绑定到安全区段”和第 **9**-23 页上的 “定义子接口和 VLAN 标记”。)

聚合接口

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

***注意：**有关聚合接口的详细信息，请参阅第 **10**-60 页上的 “冗余接口”。*

冗余接口

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

***注意：**有关冗余接口的详细信息，请参阅第 **10**-60 页上的 “冗余接口”。*

虚拟安全接口

虚拟安全接口 (VSI) 是指构成虚拟安全设备 (VSD) 的两个 NetScreen 设备在高可用性 (HA) 模式下运行时所共享的虚拟接口。网络和 VPN 信息流使用 VSI 的 IP 地址和虚拟 MAC 地址。然后， VSD 将信息流映像到之前已经将该 VSI 绑定到其上的物理接口、子接口或冗余接口。两个 NetScreen 设备在 HA 模式运行时，必须将要在设备发生故障切换时提供不间断服务的安全区段接口绑定到一个或多个虚拟安全设备 (VSD)。将接口绑定到 VSD 后，就会得到虚拟安全接口 (VSI)。

***注意：**有关 VSI 及其如何与 HA 集群中 VSD 一起使用的详细信息，请参阅第 10 卷，“高可用性”。*

功能区段接口

功能区段接口 (例如，“管理”和 HA) 都有专门的用途。

管理接口

在某些 NetScreen 设备上，可以通过单独的物理接口 [管理 (MGT) 接口] 管理设备，将管理信息流从常规网络用户信息流中分离出来。将管理信息流从网络用户信息流中分离出来，极大地提高了安全性，并确保了稳定的管理带宽。

***注意：** 有关配置管理设备的信息，请参阅第 **3**-1 页上的 “管理”。*

HA 接口

HA 接口是专用于 HA 功能的物理端口。使用具有专用“高可用性”(HA) 接口的 NetScreen 设备，可将两个设备链接在一起，组成冗余组或集群。在冗余组中，一个设备充当主设备，执行网络防火墙、 VPN 和信息流整形功能，而另一个设备充当备份设备，通常在主设备发生故障时接替防火墙功能。这是一种主动 / 被动配置。还可以将集群的两个成员都设置为彼此的主设备和备份设备。这是一种主动 / 主动配置。在第 10 卷，“高可用性”中对这两种配置做了详尽介绍。

虚拟 HA 接口

在没有专用 HA 接口的 NetScreen 设备上，虚拟高可用性 (HA) 接口提供相同的功能。由于没有 HA 信息流专用的独立物理端口，因此必须将 “虚拟 HA”接口绑定到其中的一个物理以太网端口。使用与将网络接口绑定到安全区段相同的方法，将网络接口绑定到 HA 区段 (请参阅第 63 页上的 “将接口绑定到安全区段”)。

***注意：** 有关 HA 接口的详细信息，请参阅第 **10**-39 页上的 “双 HA 接口”。*

通道接口

通道接口充当 VPN 通道的入口。信息流通过通道接口进出 VPN 通道。

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

可使用与通道接口处于同一子网中的动态 IP (DIP) 地址池对外向或内向信息流执行基于策略的 NAT。对通道接口使用基于策略的 NAT 的主要原因是为了避免在每个 VPN 通道末端各有的两个站点之间的 IP 地址发生冲突。

必须将基于路由的 VPN 通道绑定到通道接口，以便 NetScreen 设备可以将信息流发送到其中或从中向外发送信息流。可将基于路由的 VPN 通道绑定到一个有编号 (具有 IP 地址 / 网络掩码) 或没有编号 (没有 IP 地址 / 网络掩码) 的通道接口。如果通道接口没有编号，则必须指定它借用 IP 地址的接口。 NetScreen 设备自行启动通过通道的信息流 (如 OSPF 消息) 时， NetScreen 设备仅使用借用的 IP 地址作为源地址。通道接口可以从同一安全区段的接口或不同安全区段 (只要这两个区段位于同一个路由选择域中即可) 的接口借用 IP 地址。

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

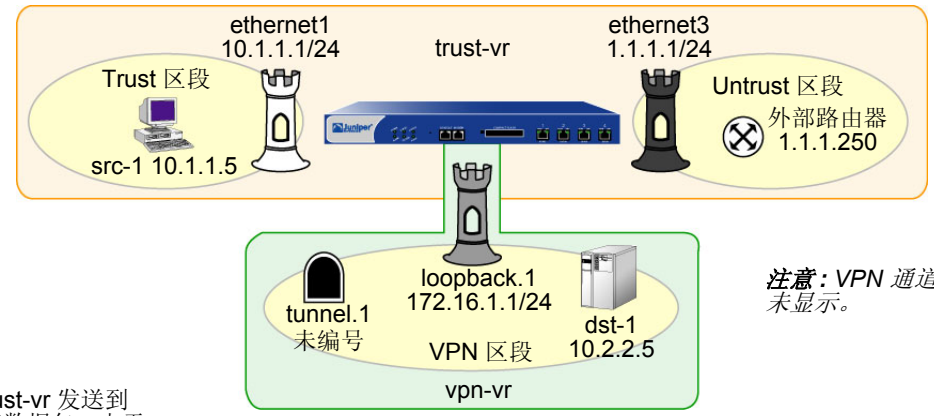
```
set vrouter name vpn-vr
set zone name vpn vrouter vpn-vr
set interface loopback.1 zone vpn
set interface loopback.1 ip 172.16.1.1/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip unnumbered loopback.1

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

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

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

NetScreen 设备将目的地为 10.2.2.5/32 的信息流从 trust-vr 发送到 vpn-vr。如果 tunnel.1 被禁用， NetScreen 设备将丢弃数据包。由于缺省路由 (到 0.0.0.0/0) 仅在 trust-vr 中，因此 NetScreen 设备不会尝试将以纯文本格式存在的数据包发送出 ethernet3。

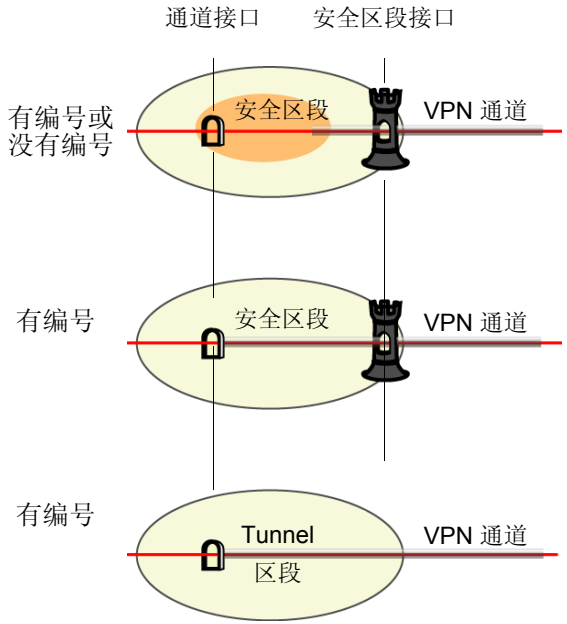


***注意：** VPN 通道本身未显示。*

将所有通道接口放置在这样的区段中非常安全，因为 VPN 不会由于出现故障 (这样会使通往相关通道接口的路由变成非活动状态) 而重新定向原本让通道使用非通道路由 (如缺省路由) 的信息流。 (有关如何避免出现类似问题的几点建议，请参阅第 **5** -90 页上的 “基于路由的 VPN 安全注意事项”。)

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

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



当通道接口在一个安全区段内时，必须将一个 VPN 通道绑定到该通道接口。这样就允许创建基于路由的 VPN 配置。

通道接口有无编号均可。如果通道接口没有编号，它将从创建该通道接口的安全区段的缺省接口借用 IP 地址。注意：只有具有 IP 地址和网络掩码的通道接口才能支持基于策略的 NAT。

当有编号的通道接口处于安全区段内并且是该区段内的唯一接口时，不需要创建安全区段接口。在此情况下，安全区段支持通过通道接口的 VPN 信息流，但不支持其它类型的信息流。

通道接口绑定到通道区段时，该通道接口必须具有 IP 地址和网络掩码。这样，就可在该接口上定义 DIP 池和 MIP 地址。如果已将某个 VPN 通道绑定到了通道区段，则无法再将其绑定到通道接口。在这种情况下，必须创建一个基于策略的 VPN 配置。

从概念上讲，可将 VPN 通道当作铺设的管道。它们从本地设备延伸到远程网关，而通道接口就是这些管道的开口。这些管道始终存在，当路由引擎将信息流引向其中的一个接口时即可使用这些管道。

通常，如果希望某个通道接口支持源地址转换 (NAT-src) 的一个或多个动态 IP (DIP) 池和目标地址转换 (NAT-dst) 的映射 IP (MIP) 地址，请为该通道接口分配一个 IP 地址。有关 VPN 和地址转换的详细信息，请参阅第 **5**-199 页上的“具有重叠地址的 VPN 站点”。可以在安全区段或通道区段创建具有 IP 地址和网络掩码的通道接口。

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

注意：*有关说明如何将通道接口绑定到通道的范例，请参阅第* ***5****-99 页上的“站点到站点 VPN”和第* ***5****-230 页上的“拨号 VPN”中基于路由的 VPN 范例。*

如果正在通过 VPN 通道传送组播数据包，可以在通道接口上启用“通用路由封装”(GRE) 以在单播数据包中封装组播数据包。 NetScreen 设备支持可在 IPv4 单播数据包中封装 IP 数据包的 GREv1。有关 GRE 的其它信息，请参阅第 **6**-199 页上的 “通用路由封装”。

删除通道接口

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

范例 : 删除通道接口

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

WebUI

1. 删除引用 DIP 池 8 的 策略 10

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

2. 删除链接到 tunnel.2 的 DIP 池 8

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

3. 解除 tunnel.2 到 vpn1 的绑定

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

4. 删除 tunnel.2

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

CLI

1. 删除引用 DIP 池 8 的 策略 10

   ```
   unset policy 10
   ```

2. 删除链接到 tunnel.2 的 DIP 池 8

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

3. 解除 tunnel.2 到 vpn1 的绑定

   ```
   unset vpn vpn1 bind interface
   ```

4. 删除 tunnel.2

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

查看接口

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

要在 WebUI 中查看接口表，请单击 **Network > Interfaces**。可指定要在 List Interfaces 下拉菜单中显示的接口的类型。

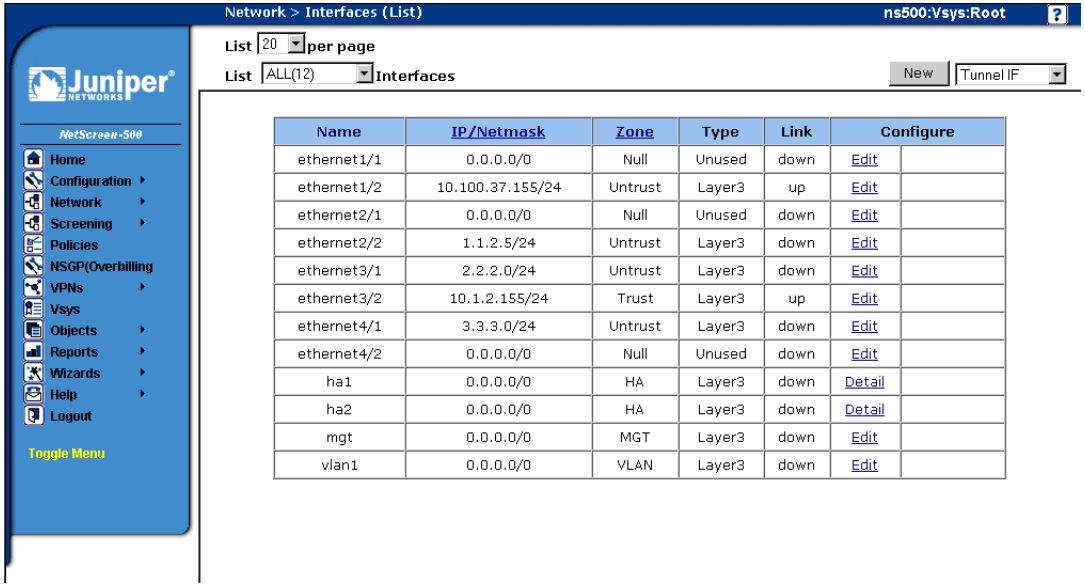
要在 CLI 中查看接口表，请使用 **get interface** 命令。

接口表

接口表显示每个接口的下列信息：

- **Name:** 此字段标识接口的名称。
- **IP/Netmask:** 此字段标识接口的 IP 地址和网络掩码地址。
- **Zone:** 此字段标识接口所绑定到的区段。
- **Type:** 此字段指出接口类型：Layer 2 (第 2 层)、 Layer 3 (第 3 层)、 tunnel (通道)、 redundant (冗余)、 aggregate (聚合)、 VSI。
- **Link:** 此字段标识接口是处于活动 (Up) 状态还是处于非活动 (Down) 状态。
- **Configure:** 此字段允许修改或移除接口。

WebUI 接口表



Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet1/2	10.100.37.155/24	Untrust	Layer3	up	Edit	
ethernet2/1	0.0.0.0/0	Null	Unused	down	Edit	
ethernet2/2	1.1.2.5/24	Untrust	Layer3	down	Edit	
ethernet3/1	2.2.2.0/24	Untrust	Layer3	down	Edit	
ethernet3/2	10.1.2.155/24	Trust	Layer3	up	Edit	
ethernet4/1	3.3.3.0/24	Untrust	Layer3	down	Edit	
ethernet4/2	0.0.0.0/0	Null	Unused	down	Edit	
ha1	0.0.0.0/0	HA	Layer3	down	Detail	
ha2	0.0.0.0/0	HA	Layer3	down	Detail	
mgt	0.0.0.0/0	MGT	Layer3	down	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	down	Edit	

CLI 接口表

```
ns500-> get interface

A - Active, I - Inactive, U - Up, D - Down, R - Ready

Interfaces in vsys Root:
Name           IP Address          Zone        MAC             VLAN State VSD Vsys
eth1/1         0.0.0.0/0           Null        0010.db0d.4ddc     -   D   -   Root
eth1/2         10.100.37.155/24    Untrust     0010.db0d.4dde     -   U   -   Root
eth2/1         0.0.0.0/0           Null        0010.db0d.4ddb     -   D   -   Root
eth2/2         1.1.2.5/24          Untrust     0010.db0d.4ddd     -   D   -   Root
eth3/1         2.2.2.0/24          Untrust     0010.db0d.4dd8     -   D   -   Root
eth3/2         10.1.2.155/24       Trust       0010.db0d.4dda     -   U   -   Root
eth4/1         3.3.3.0/24          Untrust     0010.db0d.4dd7     -   D   -   Root
eth4/2         0.0.0.0/0           Null        0010.db0d.4dd9     -   D   -   Root
mgt            0.0.0.0/0           MGT         0010.db0d.4dd0     -   D   -   Root
ha1            0.0.0.0/0           HA          0010.db0d.4dd5     -   D   -   Root
ha2            0.0.0.0/0           HA          0010.db0d.4dd6     -   D   -   Root
vlan1          0.0.0.0/0           VLAN        0010.db0d.4ddf     1   D   -   Root
null           0.0.0.0/0           Null        0010.dbff.0100     -   U   0   Root
ns500->
```

配置安全区段接口

本节将介绍如何配置安全区段接口的以下方面：

- 将接口绑定到安全区段及解除绑定
- 为第 3 层 (L3) 安全区段接口分配地址
- 修改物理接口和子接口
- 创建子接口
- 删除子接口

> ***注意：****有关为接口设置信息流带宽的信息，请参阅第 7 章，“信息流整形”。有关每种接口可用的管理及其它可用服务选项的详细信息，请参阅第* ***3****-36 页上的 “控制管理信息流”。*

将接口绑定到安全区段

可将任何物理接口绑定到 L2 (第 2 层) 或 L3 (第 3 层) 安全区段。由于子接口需要 IP 地址，因此只能将子接口绑定到 L3 (第 3 层) 安全区段。只有在将接口绑定到 L3 安全区段后，才能为该接口分配 IP 地址。

范例：绑定接口

在本例中，将 ethernet5 绑定到 Trust 区段。

WebUI

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

CLI

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

为 L3 安全区段接口编址

定义第 3 层 (L3) 安全区段接口或子接口时，必须为其分配 IP 地址和网络掩码。如果将接口绑定到 trust-vr 中的区段，则还可指定接口模式为 NAT 或 Route (路由)。 [如果接口所绑定到的区段位于 untrust-vr 中，则该接口的模式始终是 Route (路由)。]

***注意：** 有关 NAT 和 Route (路由) 模式配置的范例，请参阅第 4 章，第 103 页上的 “接口模式”。*

分配接口地址时，要了解以下两种基本类型的 IP 地址 :

- 公共地址，由互联网服务提供商 (ISP) 提供的地址，用于公用网络 (如互联网) 并且必须是唯一的
- 私有地址，由本地网络管理员分配，用于私有网络；其它管理员也可对其进行分配，用于其它私有网络

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

公共 IP 地址

连接到公用网络的接口必须具有公共 IP 地址。同样，如果 untrust-vr 中的 L3 (第 3 层) 安全区段连接到公用网络，并且 trust-vr 中区段的接口模式为 Route (路由)，那么 trust-vr 的区段中所有地址 (包括接口和主机的地址) 也必须为公共地址。公共 IP 地址分成三类， A、 B 和 C[2]，如下所示 :

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

2. 还有 D 和 E 类地址，留作特殊用途。

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

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

私有 IP 地址

如果将接口连接到私有网络，那么本地网络管理员可将任何地址分配给它，尽管通常使用专为私有地址预留范围中的地址 — 10.0.0.0/8, 172.16.0.0 – 172.31.255.255, 192.168.0.0/16 — RFC 1918, “Address Allocation for Private Internets” 中对其进行了定义。

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

3. 24 位掩码的十进制点格式等值为 255.255.255.0。

范例：编址接口

在本例中，将给 ethernet5 分配 IP 地址 210.1.1.1/24、管理 IP 地址 210.1.1.5。(请注意，管理 IP 地址必须与安全区段接口 IP 地址位于同一子网中。) 最后，将接口模式设置为 NAT，将所有内部 IP 地址转换为绑定到其它安全区段的缺省接口[4]。

WebUI

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

IP Address/Netmask: 210.1.1.1/24

Manage IP: 210.1.1.5

CLI

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

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

从安全区段解除接口绑定

如果接口未编号，那么可解除其到某个安全区段的绑定，然后再将其绑定到另一安全区段。如果接口已编号，则必须首先将其 IP 地址和网络掩码设置为 0.0.0.0。然后，可解除其到一个安全区段的绑定，然后再将其绑定到另一安全区段，并 (可选) 重新为其分配 IP 地址 / 网络掩码。

范例 : 解除接口绑定

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

WebUI

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

Zone Name: Null

IP Address/Netmask: 0.0.0.0/0

CLI

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

修改接口

配置物理接口、子接口、冗余接口、聚合接口或 “虚拟安全接口” (VSI) 后，可根据需要更改以下各种设置：

- IP 地址和网络掩码
- 管理 IP 地址
- (第 3 层区段接口) 管理和网络服务
- (子接口) 子接口 ID 号和 VLAN 标记号
- (绑定到 trust-vr 中第 3 层安全区段的接口) 接口模式 — NAT 或 Route (路由)
- (物理接口) 信息流带宽设置 (请参阅第 7 章，第 341 页上的 “信息流整形”)
- (物理、冗余和聚合接口) 最大传输单位 (MTU) 大小
- (第 3 层接口) 阻止进出相同接口的信息流，包括主子网和辅助子网之间或两个辅助子网之间的信息流 (通过含有 **route-deny** 选项的 CLI 命令 **set interface** 来完成)

对于某些 NetScreen 设备上的物理接口，可以强迫链接的物理状态处于非活动状态或活动状态。通过强迫链接的物理状态处于非活动状态，可以模拟断开电缆与接口端口之间的连接。(通过含有 **phy link-down** 选项的 CLI 命令 **set interface** 来完成。)

范例 : 修改接口设置

在本例中，将对绑定到 Trust 区段的接口 ethernet1 进行某些修改。将管理 IP 地址从 10.1.1.2 更改为 10.1.1.12。为了确保管理信息流的绝对安全，还将通过启用 SCS 和 SSL 以及禁用 Telnet 和 WebUI 来更改管理服务选项。

WebUI

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

Manage IP: 10.1.1.12

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

CLI

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

创建子接口

可在根系统或虚拟系统中的任何物理接口[5] 上创建子接口。子接口使用 VLAN 标记区别绑定到该子接口的信息流与绑定到其它接口的信息流。请注意虽然子接口源自物理接口，并借用其需要的带宽，但是可将子接口绑定到任何区段，而不一定非要将其绑定到其 “父级” 接口绑定到的区段。此外，子接口的 IP 地址一定不要与所有其它物理接口和子接口的 IP 地址位于同一子网中。

范例 : 根系统中的子接口

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

WebUI

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

Interface Name: ethernet1.3

Zone Name: accounting

IP Address/Netmask: 10.2.1.1/24

VLAN Tag: 3

CLI

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

5. 还可配置冗余子接口和 VSI 上的子接口。有关配置冗余接口上子接口的范例，请参阅第 **10**-130 页上的 “虚拟系统故障切换”。

删除子接口

不能立即删除拥有映射 IP 地址 (MIP)、虚拟 IP 地址 (VIP) 或动态 IP (DIP) 地址池的子接口。删除拥有任何这些地址的子接口前，必须首先删除所有引用它们的策略或 IKE 网关。然后必须删除子接口上的 MIP、 VIP 和 DIP 池。

范例 : 删除安全区段接口

在本例中，将删除子接口 ethernet1:1。

WebUI

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

会出现一条系统消息，提示您确认移除。

单击 **Yes** 删除子接口。

CLI

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

二级 IP 地址

每个 NetScreen 接口都有一个唯一的*一级* IP 地址。不过，在某些情况下要求一个接口具有多个 IP 地址。例如，某个机构可能会分配额外的 IP 地址，而不希望添加路由器来满足其需要。此外，如有连接到 LAN 的主机多于 254 台，则某个机构子网的处理能力将无法满足网络设备的需要。要解决这类问题，可将*二级* IP 地址添加到 Trust、 DMZ 或用户定义区段的接口中。

注意：*不能为 Untrust 区段中的接口设置多个二级 IP 地址。*

二级 IP 地址属性

二级地址的某些属性会影响您实施此类地址的方式。这些属性如下：

- 任意两个二级 IP 地址之间不能出现子网地址重迭现象。此外， NetScreen 设备上的二级 IP 和任何现有子网间不能出现子网地址重迭现象。
- 通过二级 IP 地址管理 NetScreen 设备时，该地址的管理属性总是与一级 IP 地址的管理属性相同。因此，不能为二级 IP 地址指定单独的管理配置。
- 不能为二级 IP 地址配置网关。
- 创建新的二级 IP 地址时， NetScreen 设备会自动创建相应的路由表条目。删除二级 IP 地址时，设备会自动删除其路由表条目。

启用或禁用两个二级 IP 地址之间的路由不会使路由表发生改变。例如，如果禁用两个此类地址之间的路由，NetScreen 设备会丢弃从一个接口到另一个接口的所有数据包，但路由表并不会发生改变。

范例 : 创建二级 IP 地址

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

WebUI

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

IP Address/Netmask: 192.168.2.1/24

CLI

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

回传接口

回传接口是一个逻辑接口，它模拟 NetScreen 设备上的物理接口。然而，与物理接口不同的是，只要其所在的设备开启，该接口始终处于活动状态。回传接口的名称为 loopback.*id_num*，其中 *id_num* 为大于或等于 1[6] 的数字，表示设备上唯一的回传接口。与物理接口相似，必须给回传接口分配 IP 地址，并将其绑定到安全区段。

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

范例：创建回传接口

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

WebUI

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

Interface Name: loopback.1

Zone: Untrust (选择)

IP Address/Netmask: 1.1.1.27./24

CLI

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

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

6. 可以指定的最大 *id_num* 值根据平台而定。

使用回传接口

可通过多种方式来使用回传接口，其使用方式同物理接口。本节将通过范例来说明如何配置回传接口。

***注意：**不能将回传接口绑定到 HA 区段，也不能为第 2 层操作配置回传接口，或者将回传接口配置为冗余 / 聚合接口。不能在回传接口上配置以下特征：NTP、 DNS、 VIP、二级 IP、跟踪 IP 或 Webauth。*

可以在回传接口上定义 MIP。这样，接口组就可访问 MIP，此功能为回传接口所特有。有关使用具有 MIP 的回传接口的信息，请参阅第 **7**-105 页上的 “MIP 和回传接口”。

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

范例：用于管理的回传接口

在下例中，将先前定义的 loopback.1 接口配置为设备的管理接口。

WebUI

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

CLI

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

范例：回传接口上的 BGP

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

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

WebUI

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

CLI

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

范例：回传接口上的 VSI

可以在回传接口上为 NSRP 配置“虚拟安全接口”(VSI)。回传接口上的 VSI 物理状态始终处于活动状态。接口可能处于活动状态，也可能处于非活动状态，这取决于该接口所属的 VSD 组的状态。

WebUI

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

Interface Name: VSI Base: loopback.1

VSD Group: 1

IP Address/Netmask: 1.1.1.1/24

CLI

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

范例：回传接口作为源接口

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

WebUI

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

Enable Syslog Messages: (选择)

Source Interface: loopback.1 (选择)

Syslog Servers:

No.: 1 (选择)

IP/Hostname: 10.1.1.1

Traffic Log: (选择)

Event Log: (选择)

CLI

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

接口状态更改

接口可以处于以下几种状态：

- **物理活动状态** – 适用于在“开放式系统互连”(OSI) 模式下运行在第 2 层 (透明模式) 或第 3 层 (路由模式) 的物理以太网接口。当用电缆将接口连接到另一台网络设备且可建立一个到该设备的链接时，该接口即处于物理活动状态。
- **逻辑活动状态** – 适用于物理接口和逻辑接口 (子接口、冗余接口和聚合接口)。当通过接口的信息流能够到达网络上的指定设备 (在被跟踪的 IP 地址处) 时，该接口处于逻辑活动状态。
- **物理非活动状态** – 当未使用电缆将接口连接到另一台网络设备或者虽然使用电缆将其连接到了另一台网络设备但却不能建立链接时，该接口处于物理非活动状态。也可以使用以下 CLI 命令迫使接口处于物理非活动状态：**set interface interface phy link-down**。
- **逻辑非活动状态** – 当通过接口的信息流不能到达网络上的指定设备 (在被跟踪的 IP 地址处) 时，该接口处于逻辑非活动状态。

接口的物理状态优先于其逻辑状态。接口可以处于物理连接状态，也可以处于逻辑连接或逻辑中断状态。如果接口处于物理非活动状态，则其逻辑状态如何将无关紧要。

当接口处于活动状态时，所有使用该接口的路由将保持活动和可用状态。当接口处于非活动状态时， NetScreen 设备将中断使用该接口的所有路由 — 虽然信息流仍可能流经处于非活动状态的接口，这要因该接口是处于物理非活动状态还是逻辑非活动状态而定 (请参阅第 95 页上的 “非活动接口和信息流”)。要补偿因丢失接口而引起的路由丢失，可以使用备用接口来配置备用路由。

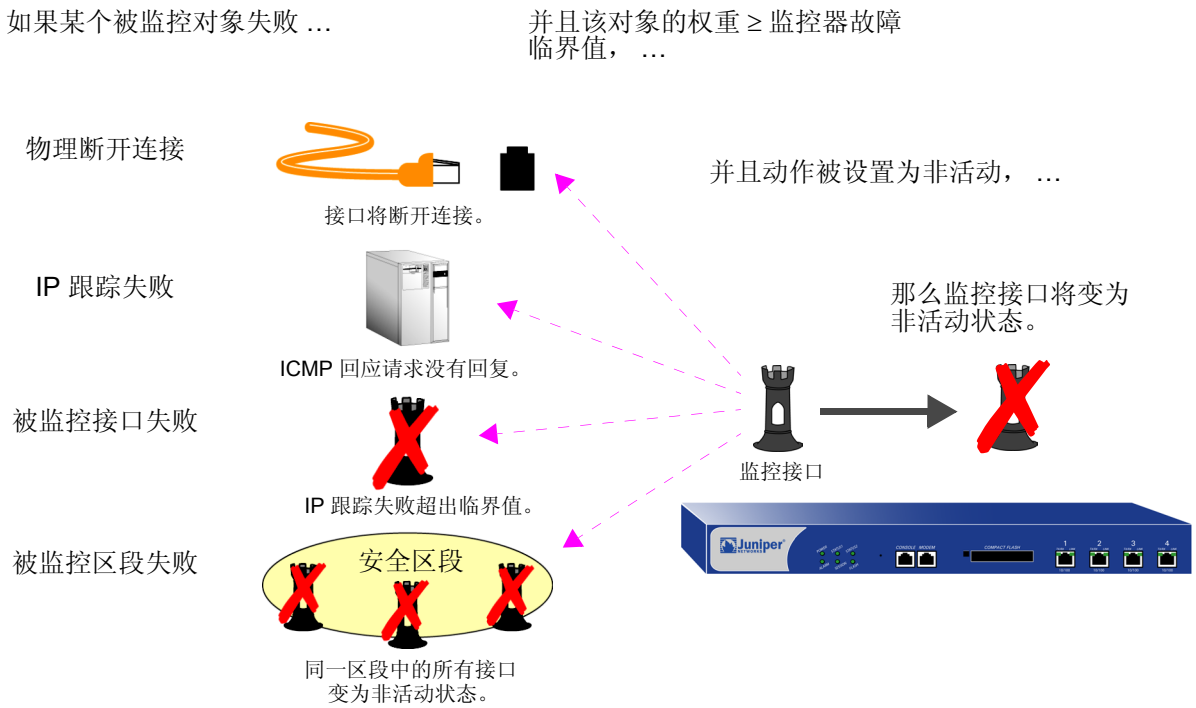
依据对观察到的接口状态更改所导致动作的设置情况，被监控接口的状态更改 (由活动状态变为非活动状态) 可能会导致监控接口的状态发生更改 (由非活动状态变为活动状态)。要配置这种行为，可以使用以下 CLI 命令：

```
set interface interface monitor threshold number action up { logically |
    physically }
```

输入上面的命令后， NetScreen 设备将自动迫使监控接口处于非活动状态。如果被监控对象 (被跟踪的 IP 地址、接口、区段) 失败，则监控接口的状态将变为活动状态 — 可能为逻辑活动状态，也可能是物理活动状态，这取决于您的具体配置。

接口可以监控对象的以下一个或多个事件。这些事件中的每个事件或其组合均可导致监控接口由活动状态变为非活动状态以及由非活动状态变为活动状态：

- 物理断开连接 / 重新连接
- IP 跟踪失败 / 成功
- 被监控接口失败 / 成功
- 被监控安全区段失败 / 成功



如果被监控对象在失败后又实现了成功 (接口被重新连接或 IP 跟踪再次成功)，则监控接口将恢复为活动状态。从被监控对象成功到监控接口重新激活自身大约有一秒钟的延迟时间。

随后各节将对上述各个事件逐一进行介绍。

物理连接监控

所有 NetScreen 设备上的物理接口监控它们到其它网络设备的物理连接的状态。当将接口连接到其它网络设备并建立了到该设备的链接时，该接口将处于物理活动状态，并且所有使用该接口的路由都将处于活动状态。

可以在 **get interface** 命令的输出中的 State 列以及在 WebUI 的 Network > Interfaces 页面上的 Link 列中查看接口状态。可能为活动或非活动状态。

可以在 **get route id** *number* 命令的 Status 字段以及 WebUI 的 Network > Routing > Routing Entries 页面中查看路由的状态。如果标有一个星号，则表明该路由处于活动状态。如果没有星号，则表明该路由处于非活动状态。

跟踪 IP 地址

NetScreen 设备可以通过接口跟踪指定的 IP 地址，使得当一个或多个 IP 地址不可到达时，即使物理链接仍处于活动状态[7]，NetScreen 设备也可中断所有与该接口相关的路由。当 NetScreen 设备同那些 IP 地址之间恢复通信后，中断的路由将再次变为活动状态。

类似于 NSRP 中使用的功能， NetScreen 使用第 3 层路径监控 (或 *IP 跟踪*) 通过接口来监控指定 IP 地址的可到达性。例如，如果接口直接连接到路由器，则可跟踪接口的下一跳跃地址，以确定该路由器是否仍可到达。当接口上配置了 IP 跟踪时， NetScreen 设备将以用户定义的时间间隔在该接口上将 ping 请求发送给多达四个目标 IP 地址。NetScreen 设备监控这些目标以查看其是否收到了响应。如果在向该目标发送指定次数的请求后，仍没有来自该目标的响应，那么该 IP 地址将被认为是不可到达的。无法从一个或多个目标得到响应可能使 NetScreen 设备中断与该接口相关的路由。如果到同一目标的另一路由可用，则 NetScreen 设备将重新定向信息流以使用新路由。

7. 对于某些 ScreenOS 设备，该动作还将导致备份接口的故障切换，该备份接口与配置了 IP 跟踪的接口绑定到同一区段 (请参阅第 **10**-72 页上的 “确定接口故障切换”)。

配置 IP 跟踪

可以在以下配置有管理 IP 地址的接口上定义 IP 跟踪 :

- 绑定到安全区段 (非 HA 或 MGT 功能区段) 的物理接口

  注意 : *该接口可以在第 2 层 (透明模式) 或第 3 层 (路由模式) 运行。*

- 子接口
- 冗余接口
- 聚合接口

  注意 : *尽管该接口可以是冗余接口或聚合接口，但它不能是冗余接口或聚合接口的成员。*

在支持虚拟系统的设备上，设置有 IP 跟踪的接口可以属于根系统或虚拟系统 (vsys)。不过，要在共享接口上设置 IP 跟踪，只能在根级进行设置[8]。

对于每个接口，最多可为 NetScreen 设备配置四个 IP 地址进行跟踪。在单个设备上，最多可配置 64 个跟踪 IP 地址。这 64 个跟踪 IP 地址将包括所有跟踪 IP 地址在内，不论它们是用于根级别的基于接口的 IP 跟踪和用于基于 NSRP 的 IP 跟踪，还是用于 vsys 级别的基于接口的 IP 跟踪和用于基于 NSRP 的 IP 跟踪。

被跟踪的 IP 地址不必与接口位于同一子网中。对于每个要跟踪的 IP 地址，可以进行如下指定 :

- 发送 ping 到指定 IP 地址的时间间隔 (以秒为单位)。
- 在到 IP 地址的连接被认为失败之前的连续不成功的 ping 尝试次数。
- 失败的 IP 连接的权重 (一旦所有失败的 IP 连接的总权重超过指定临界值，则与该接口相关的路由即被中断)。

8. 可以从 vsys 设置接口监控以便从属于该 vsys 的一个接口监控共享接口。不过，从一个 vsys 内部，不能从共享接口设置接口监控。有关详细信息，请参阅 第 87 页上的 “接口监控”。

还可对 NetScreen 设备进行配置，使其跟踪充当 PPPoE 或 DHCP 客户端的接口的缺省网关。要实现这一操作，请使用 “Dynamic” 选项 : (CLI) **set interface** *interface* **monitor dynamic** 或者 (WebUI) Network > Interfaces > Edit (对于 DHCP 或 PPPoE 客户端接口) > Monitor > Track IP > Add: 选择 **Dynamic**。

注意：*当配置 NetScreen 设备要对其进行跟踪的 IP 地址时， NetScreen 设备不会将该 IP 地址的主机路由添加到路由表中。*

存在两种用于配置跟踪 IP 地址的临界值 :

- 被跟踪的特定 IP 地址的故障临界值 — 从特定 IP 地址获得 ping 响应连续失败的次数，当失败次数达到此临界值后，即宣告无法到达该 IP 地址。不超过临界值表示可以接受该地址的连通性；超过临界值则表示不可以接受。可以将每个 IP 地址的此临界值设置为介于 1 与 200 之间的任意值，缺省值为 3。
- 接口上 IP 跟踪的故障临界值 — 到达接口上 IP 地址的累积失败尝试的总权重，这些失败尝试可导致与该接口相关的路由中断。可将该临界值设置为介于 1 与 255 之间的任意值。缺省值为 1，它表示对任何已配置的被跟踪 IP 地址的访问失败都将导致与接口相关的路由中断。

通过在被跟踪 IP 地址上应用*权重*或权值，可以调整该地址连通性的重要程度 (与其它被跟踪 IP 地址相比)。可以将较大的权重分配给相对重要的地址，将较小的权重分配给相对次要的地址。注意，仅当达到指定的被跟踪 IP 地址的故障临界值时，分配的权重才会起作用。例如，当某个接口上 IP 跟踪的故障临界值是 3 时，由于权重为 3 的单一的被跟踪的 IP 地址的故障满足该接口上 IP 跟踪的故障临界值，因此这将导致与该接口相关的路由中断。而权重为 1 的单一的被跟踪的 IP 地址的故障不满足接口上 IP 跟踪的故障临界值，因此与接口相关的路由将保持活动状态。

范例：配置接口 IP 跟踪

在下例中，将接口 ethernet1 绑定到了 Trust 区段，为其分配的网络地址为 10.1.1.1/24。将接口 ethernet3 和 ethernet4 绑定到了 Untrust 区段。为接口 ethernet3 分配了网络地址 1.1.1.1/24 并将其连接到位于 1.1.1.250 处的路由器。为接口 ethernet4 分配了网络地址 2.2.2.1/24 并将其连接到位于 2.2.2.250 处的路由器。

存在两个已配置的缺省路由：一个使用 ethernet3 作为出站接口，路由器地址 1.1.1.250 作为网关；另一个使用 ethernet4 作为出站接口，路由器地址 2.2.2.250 作为网关，并配置了度量值 10。使用 ethernet3 的缺省路由是首选路由，这是因为它有较低的度量值 (静态路由选择的缺省度量值是 1)。 **get route** 命令的以下输出显示了 trust-vr 的四个活动路由 (活动路由标有星号)。通过 ethernet3 的缺省路由是活动的。而通过 ethernet4 的缺省路由不是活动的，因为它不是首选的。

```
ns-> get route
untrust-vr (0 entries)
--------------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
--------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref     Mtr      Vsys
--------------------------------------------------------------------------------
*   4          0.0.0.0/0            eth3       1.1.1.250   S   20       1      Root
*   2        1.1.1.0/24             eth3         0.0.0.0   C    0       0      Root
    3          0.0.0.0/0            eth4       2.2.2.250   S   20      10      Root
*   6        2.2.2.0/24             eth4         0.0.0.0   C    0       1      Root
*   5       10.1.1.0/24             eth1         0.0.0.0   C   20       1      Root
```

如果通过 ethernet3 的路由变为不可用，则通过 ethernet4 的缺省路由将变为活动路由。启用和配置 ethernet3 接口上的 IP 跟踪监控路由器地址 1.1.1.250。如果 IP 跟踪不能到达 1.1.1.250，则 NetScreen 设备上同接口 ethernet3 相关的所有路由都将变为非活动的。因而，通过 ethernet4 的缺省路由将变为活动的。当 IP 跟踪再次能够到达 1.1.1.250 时，通过 ethernet3 的缺省路由将变为活动的。同时通过 ethernet4 的缺省路由将变为非活动的，因为它的优先级要比通过 ethernet3 的缺省路由的优先级低。

以下示例将使 IP 跟踪的接口故障临界值为 5，并在接口 ethernet3 上配置 IP 跟踪，以便监控被分配了权重 10 的路由器 IP 地址 1.1.1.250。

WebUI

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

Enable Track IP: (选择)

Threshold: 5

> Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)

Track IP: 1.1.1.250

Weight: 10

CLI

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

在本例中，目标地址的故障临界值设置为缺省值 3。也就是说，如果目标对连续三个 ping 请求没有响应，则权重 10 将被应用到接口上 IP 跟踪的故障临界值。由于接口上 IP 跟踪的故障临界值为 5，因此权重 10 将导致同该接口相关的路由在 NetScreen 设备上被中断。

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

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

get route 命令显示通过 ethernet4 的缺省路由现在为活动状态，而通过 ethernet3 的所有路由不再为活动状态。

```
ns-> get route
untrust-vr (0 entries)
------------------------------------------------------------------------------
C - Connected, S - Static, A - Auto-Exported, I - Imported, R - RIP
iB - IBGP, eB - EBGP, O - OSPF, E1 - OSPF external type 1
E2 - OSPF external type 2
trust-vr (4 entries)
------------------------------------------------------------------------------
   ID          IP-Prefix      Interface         Gateway   P Pref     Mtr      Vsys
------------------------------------------------------------------------------
    4           0.0.0.0/0           eth3       1.1.1.250   S   20       1      Root
    2         1.1.1.0/24            eth3         0.0.0.0   C    0       0      Root
*   3           0.0.0.0/0           eth4       2.2.2.250   S   20      10      Root
*   6         2.2.2.0/24            eth4         0.0.0.0   C    0       1      Root
*   5        10.1.1.0/24            eth1         0.0.0.0   C   20       1      Root
```

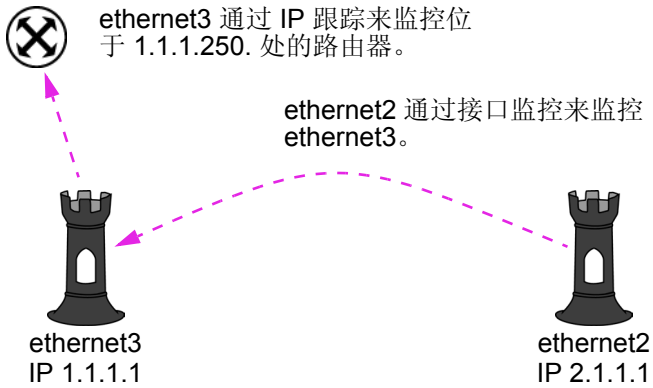
注意，即使通过 ethernet3 的路由不再为活动状态， IP 跟踪仍将使用同 ethernet3 相关的路由继续向目标 IP 地址发送 ping 请求。当 IP 跟踪又能到达 1.1.1.250 时，通过 ethernet3 的缺省路由将再次在 NetScreen 设备上变为活动状态。同时，通过 ethernet4 的缺省路由将变为非活动状态，这是因为它的优先级要比通过 ethernet3 的缺省路由的优先级低。

接口监控

NetScreen 设备能够对接口的物理和逻辑状态进行监控，然后根据观察到的变化采取相应的行动。例如，如果被监控接口的状态由活动变为非活动，则可能会发生以下情况：

如果	那么
接口的物理状态由活动变为非活动	该状态变化可能会促使监控刚刚变为非活动状态的接口的另一个接口也变为非活动状态。可以指定希望第二个接口变为物理非活动状态还是逻辑非活动状态。 变为物理非活动状态的任一接口的状态变化或一起变为物理非活动状态的两个接口的相加后的权重均可以触发 NSRP 故障切换。只有当接口的物理状态发生改变时，才会发生 NSRP 设备或 VSD 组故障切换。
当 IP 跟踪失败时，接口的逻辑状态将由活动状态变为非活动状态	该状态变化可能会促使监控刚刚变为非活动状态的接口的另一个接口也变为非活动状态。尽管第一个接口为逻辑非活动状态，不过，您仍可以指定希望第二个接口的非活动状态为逻辑非活动状态还是物理非活动状态。

监控另一个接口的接口



ethernet3 的状态变化

如果

- 到 1.1.1.250 的失败 ping 尝试次数超过了该被跟踪 IP 地址的故障临界值，
- 1.1.1.250 的跟踪 IP 权重 ≥ 跟踪对象故障临界值，
- 跟踪对象权重 ≥ 监控器故障临界值，并且
- 故障动作为由活动状态变为非活动状态，

那么， ethernet3 的状态将由活动变为非活动。

ethernet2 的状态变化

如果

- ethernet3 的故障权重 ≥ 监控器故障临界值，并且
- 故障动作为由活动状态变为非活动状态，

那么， ethernet2 的状态将由活动变为非活动。

要设置接口监控，请执行以下任一操作：

WebUI

Network > Interfaces > Edit (对于要进行监控的接口) > Monitor > Edit Interface: 输入以下内容，然后单击 **Apply**:

Interface Name 选择要对其进行监控的接口。

Weight: 输入介于 1 和 255 之间的权重。

CLI

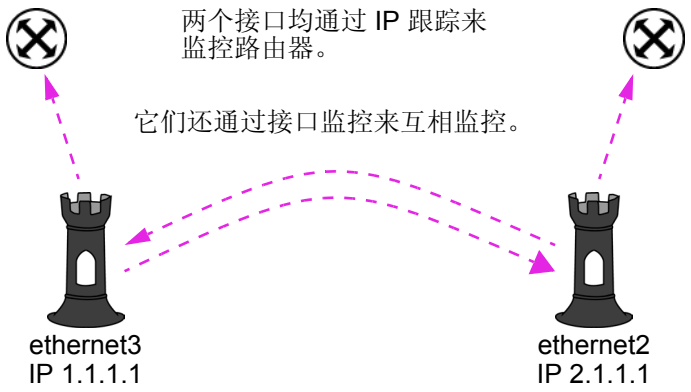
```
set interface interface1 monitor interface interface2 [ weight number ]
```

如果没有设置权重，则 NetScreen 设备将使用缺省值 : 255。

如果两个接口互相监控，则它们形成一个环。此时，如果任意一个接口的状态发生改变，那么该环中另外一个接口的状态也将随之发生改变。

注意： *不能将一个接口同时置于两个环中。 Juniper Networks 不支持一个接口属于多个环的配置。*

环 — 两个接口互相监控



第一个状态变化

如果

- 到任一路由器的失败 ping 尝试次数超过了该被跟踪的 IP 地址的故障临界值，
- 失败的跟踪 IP 的权重 ≥ 跟踪对象故障临界值，
- 跟踪对象权重 ≥ 监控器故障临界值，并且
- 故障动作为由活动状态变为非活动状态，

那么，该接口的状态将由活动变为非活动。

第二个状态变化

如果

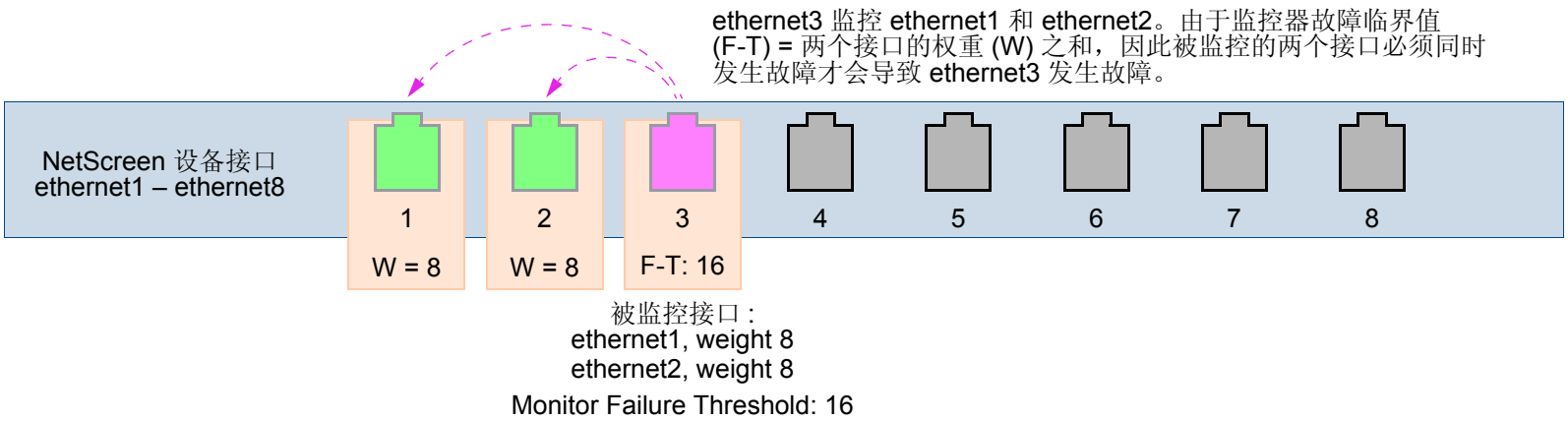
- 第一个接口故障权重 ≥ 第二个接口的监控器故障临界值，并且
- 故障动作为由活动状态变为非活动状态，

那么，第二个接口的状态也将由活动变为非活动。

范例：两个被监控接口

在本例中，将配置 ethernet3 来监控两个接口 — ethernet1 和 ethernet2。由于每个被监控接口的权重 (8 + 8) 等于监控器故障临界值 (16)，因此只有 ethernet1 和 ethernet2 同时发生故障 (并将它们的状态由活动变为非活动) 才能导致 ethernet3 发生故障 (并将其状态由活动变为非活动)[9]。

注意：*本例忽略了配置 ethernet1 和 ethernet2 接口上的 IP 跟踪 (请参阅第 80 页上的“跟踪 IP 地址”)。在没有 IP 跟踪的情况下，ethernet1 和 ethernet2 可能发生故障的唯一方式就是它们与其它网络设备物理上断开连接或者它们不能保持与那些设备的链接。*



WebUI

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

ethernet1: (选择); Weight: 8

ethernet2: (选择); Weight: 8

Network > Interfaces > Edit (对于 ethernet3) > Monitor: 在 Monitor Threshold 字段中输入 **16**，然后单击 **Apply**。

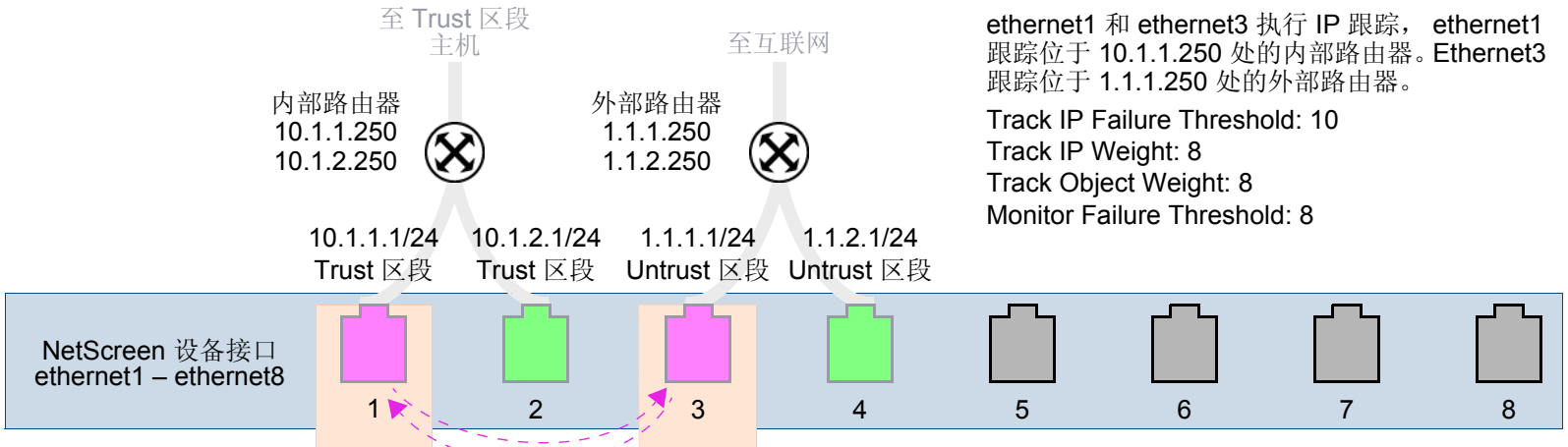
9. 如果将监控器故障临界值设置为 8 (或保持其值为 16 不变，并将每个被监控接口的权重设置为 16)，则 ethernet1 或 ethernet2 的故障均会导致 ethernet3 发生故障。

CLI

```
set interface ethernet3 monitor interface ethernet1 weight 8
set interface ethernet3 monitor interface ethernet2 weight 8
set interface ethernet3 monitor threshold 16
save
```

范例：接口监控环

在本例中，首先为两个接口 (ethernet1 和 ethernet3) 配置 IP 跟踪。然后配置这些接口互相监控，以便当其中的一个接口状态改变时，另一个接口的状态也会随之发生改变。最后再定义两组路由。第一组路由通过 ethernet1 和 ethernet3 转发信息流。第二组路由具有相同的目标地址，但这些路由具有较低级别的度量，所用的接口 (ethernet2 和 ethernet4) 和网关不同于第一组路由。有了这样的配置后，当第一组接口发生故障时， NetScreen 设备可以通过第二组接口重新路由所有信息流。所有区域都在 trust-vr 路由选择域中。



ethernet1 和 ethernet3 执行 IP 跟踪， ethernet1 跟踪位于 10.1.1.250 处的内部路由器。Ethernet3 跟踪位于 1.1.1.250 处的外部路由器。

Track IP Failure Threshold: 10
Track IP Weight: 8
Track Object Weight: 8
Monitor Failure Threshold: 8

ethernet1 和 ethernet3 互相监控。由于被监控接口的权重 = 监控器故障临界值，因此任一接口的故障都将导致另一个接口也发生故障。

监控接口环：
ethernet1 和 ethernet3
Monitored Interface Weight: 8
Monitor Failure Threshold: 8

如果 ethernet1 和 ethernet3 变为非活动状态，则引用这些接口的路由将变为非活动状态。然后， NetScreen 设备将使用通过 ethernet2 和 ethernet4 转发信息流的路由。

路由

```
set route 10.1.0.0/16 interface ethernet1 gateway 10.1.1.250 metric
set route 10.1.0.0/16 interface ethernet2 gateway 10.1.2.250 metric
set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250 metric 10
set route 0.0.0.0/0 interface ethernet4 gateway 1.1.2.250 metric 12
```

WebUI

1. IP 跟踪

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

Enable Track IP: (选择)
Monitor Threshold: 8[10]
Track IP Option: Threshold: 8
Weight: 8

> Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)
Track IP: 10.1.1.250
Weight: 8
Interval: 3 Seconds
Threshold: 10

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

Enable Track IP: (选择)
Monitor Threshold: 8
Track IP Option: Threshold: 8
Weight: 8

10. 要对接口的状态将变为逻辑非活动 (或活动) 还是物理非活动 (或活动) 进行控制，必须使用 CLI 命令 **set interface** *interface* **monitor threshold** *number* **action** { **down** | **up** } { **logically** | **physically** }。只有绑定到除 Null 区段之外的任意安全区段的物理接口才能处于物理活动或非活动状态。

> Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)

Track IP: 1.1.1.250

Weight: 8

Interval: 3 Seconds

Threshold: 10

2. 接口监控

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

ethernet3: (选择); Weight: 8

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

ethernet1: (选择); Weight: 8

3. 路由

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

Network Address/Netmask: 10.1.0.0/16

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.250

Metric: 10

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

Network Address/Netmask: 10.1.0.0/16

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 10.1.2.250

Metric: 12

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

Metric: 10

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: ethernet4

Gateway IP Address: 1.1.2.250

Metric: 12

CLI

1. IP 跟踪

```
set interface ethernet1 track-ip ip 10.1.1.250 weight 8
set interface ethernet1 track-ip threshold 8
set interface ethernet1 track-ip weight 8
set interface ethernet1 track-ip

set interface ethernet3 track-ip ip 1.1.1.250 weight 8
set interface ethernet3 track-ip threshold 8
set interface ethernet3 track-ip weight 8
set interface ethernet3 track-ip
```

2. 接口监控

```
set interface ethernet1 monitor interface ethernet3 weight 8
set interface ethernet1 monitor threshold 8 action down physically
set interface ethernet3 monitor interface ethernet1 weight 8
set interface ethernet3 monitor threshold 8 action down physically
```

3. 路由

```
set vrouter trust-vr route 10.1.0.0/16 interface ethernet1 gateway 10.1.1.250
    metric 10
set vrouter trust-vr route 10.1.0.0/16 interface ethernet2 gateway 10.1.2.250
    metric 12
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
    metric 10
set vrouter trust-vr route 0.0.0.0/0 interface ethernet4 gateway 1.1.2.250
    metric 12
save
```

安全区段监控

除了可监控单个接口外，接口还可监控安全区段 (除了其自身之外的任意安全区段) 中的所有接口。要让整个安全区段发生故障，绑定到该区段的所有接口必须都发生故障。只要绑定到被监控区段的一个接口处于活动状态，则 NetScreen 设备即认为整个区段处于活动状态。

要配置接口监控安全区段，请执行以下任一操作 :

WebUI

Network > Interfaces > Edit (对于要进行监控的接口) > Monitor > Edit Zone: 输入以下内容，然后单击 **Apply**:

Zone Name: 选择要对其进行监控的区段。

Weight: 输入介于 1 和 255 之间的权重。

CLI

```
set interface interface monitor zone zone [ weight number ]
```

如果没有设置权重，则 NetScreen 设备将使用缺省值 : 255。

非活动接口和信息流

如果某些 IP 地址通过第一个接口不能到达，则配置接口上的 IP 跟踪可使得 NetScreen 通过其它接口重新路由外向信息流。不过，当由于 IP 跟踪故障致使 NetScreen 设备可能会中断同某个接口相关的路由时，该接口可以保持物理活动状态并仍可发送和接收信息流。例如， NetScreen 设备针对可能到达 IP 跟踪失败的初始接口上的现有会话继续处理内向信息流。 NetScreen 设备还将继续使用该接口向目标 IP 地址发送 ping 请求以确定目标是否可以再次到达。在这些情况下，信息流仍将通过 IP 跟踪已失败并且 NetScreen 设备已中断了其路由的接口。 NetScreen 设备如何处理这样的接口上的会话信息流取决于以下情况：

- 如果配置有 IP 跟踪的接口充当了会话的出口接口，则会话回复可以继续到达该接口并且 NetScreen 设备仍将对这些回复进行处理。
- 如果配置有 IP 跟踪的接口充当了会话入口接口，则应用 **set arp always-on-dest** 命令将导致 NetScreen 设备向另一路由重新路由会话回复。如果未设置该命令，即使 NetScreen 设备中断了使用该接口的路由，NetScreen 设备仍会通过 IP 跟踪失败的接口转发会话回复。 (缺省情况下，未设置该命令。)

  缺省情况下，当 NetScreen 设备接收到一个新会话的初始数据包时，它将缓存会话发起方的 MAC 地址。当输入 CLI 命令 **set arp always-on-dest** 时， NetScreen 设备不会缓存会话发起方的 MAC 地址。而是在处理该初始数据包的回复时执行 ARP 查找。如果发起方的 MAC 地址在 ARP 表中，则 NetScreen 设备将使用该地址。如果该 MAC 地址不在 ARP 表中，则 NetScreen 设备将发送一个 ARP 请求以获取目标 MAC 地址，然后再将所接收到的 MAC 地址添加到其 ARP 表中。当路由发生更改时， NetScreen 设备将执行另外一个 ARP 查找。

下面一节将针对在出口接口和入口接口上 IP 跟踪失败的情况分别予以介绍，并说明当在入口接口上 IP 跟踪失败的情况下使用命令 **set arp always-on-dest** 后所导致的结果。

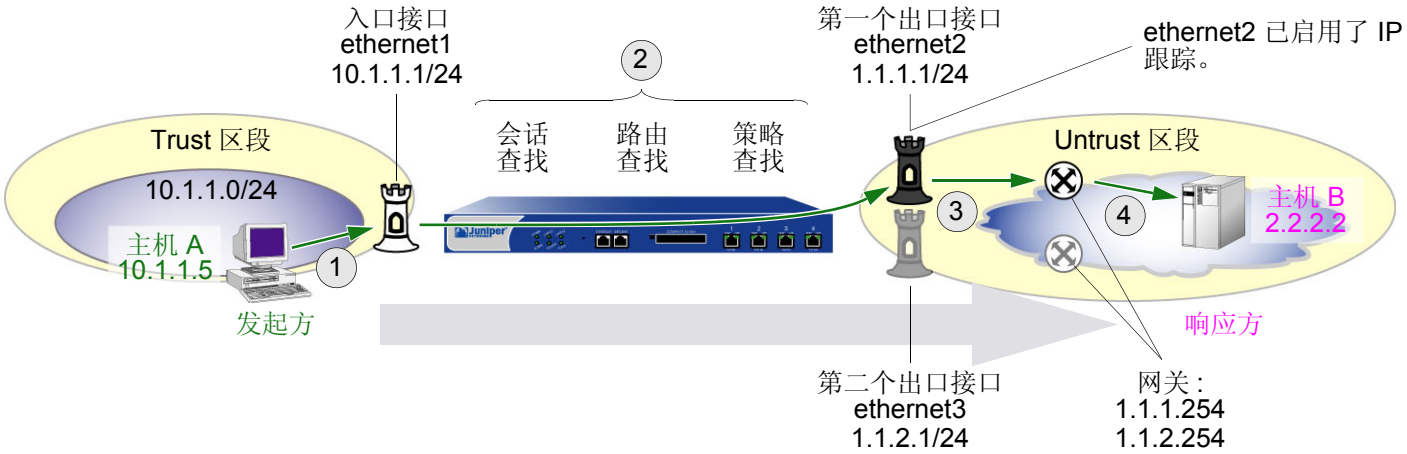
注意：*下面一节将介绍 IP 跟踪如何触发路由变化以及这些路由变化如何通过除 NetScreen-5XT 和 -5GT 之外的所有 NetScreen 设备来影响数据包流。对于这些设备， IP 跟踪失败可触发接口故障切换。有关详细信息，请参阅第* ***10****-69 页上的 “Dual Untrust 接口”。*

出口接口上的故障

在下面的示例中，将在 ethernet2 上配置 IP 跟踪， ethernet2 是从主机 A 到主机 B 的会话的出口接口。主机 A 通过发送一个数据包到主机 B 来启动会话，如下所示。

***注意：**必须首先创建两个到主机 B 的路由，且两个出口接口都必须处于同一区段内以便在重新路由前后对信息流应用相同的策略。*

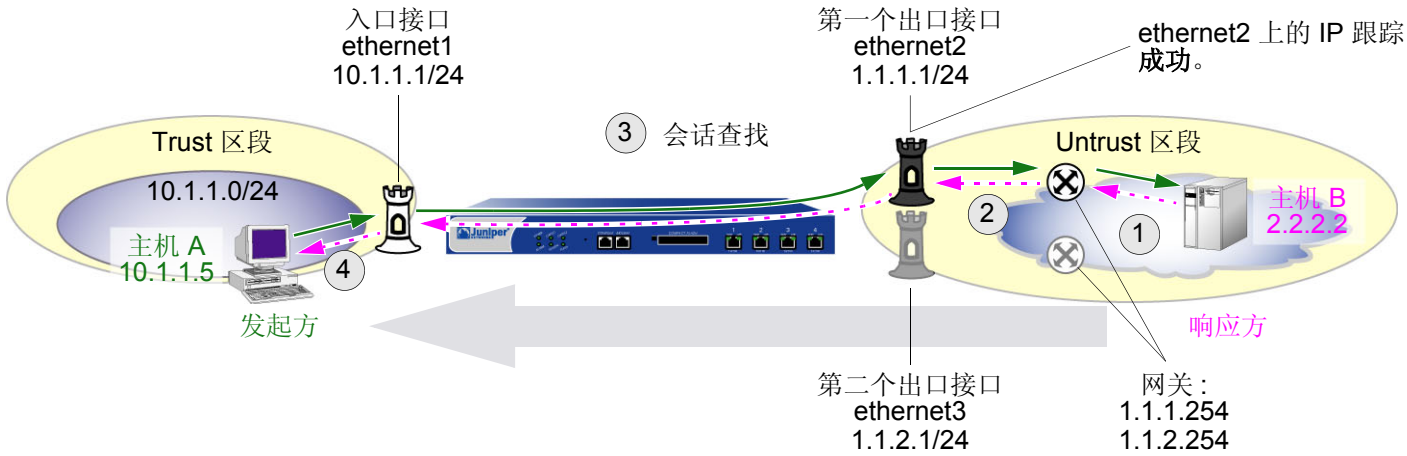
从主机 A 到主机 B 的信息流 – 请求 (启动会话)



1. 位于 10.1.1.5 处的主机 A 将目的地为位于 2.2.2.2 处的主机 B 的数据包发送到 ethernet1 (10.1.1.1)。
2. NetScreen 设备执行以下任务 :
   - 2.1 **会话查找** – 如果该数据包为第一个数据包，则 NetScreen 设备将创建一个会话。如果其属于一个现有会话，则将刷新会话表条目。
   - 2.2 **路由查找** – NetScreen 设备针对会话中的第一个数据包执行路由查找，如果路由发生变化，则将重新执行路由查找。路由查找将产生以下路由 : 要到达 0.0.0.0/0，将数据包从接口 ethernet2 发送到网关 1.1.1.254。
   - 2.3 **策略查找** – NetScreen 设备针对主机 A 正在发送信息流的类型，将安全策略应用到从 Trust 区段中的主机 A 流向 Untrust 区段中的主机 B 的区段间信息流。
3. NetScreen 设备通过 ethernet2 将数据包转发到位于 1.1.1.254 处的网关。
4. 位于 1.1.1.254 处的网关将数据包转发到其下一个跳跃。继续路由，直到主机 B 接收到它为止。

当主机 B 回复主机 A 时，返回的信息流将沿着相似的路径通过 NetScreen 设备，如下所示。

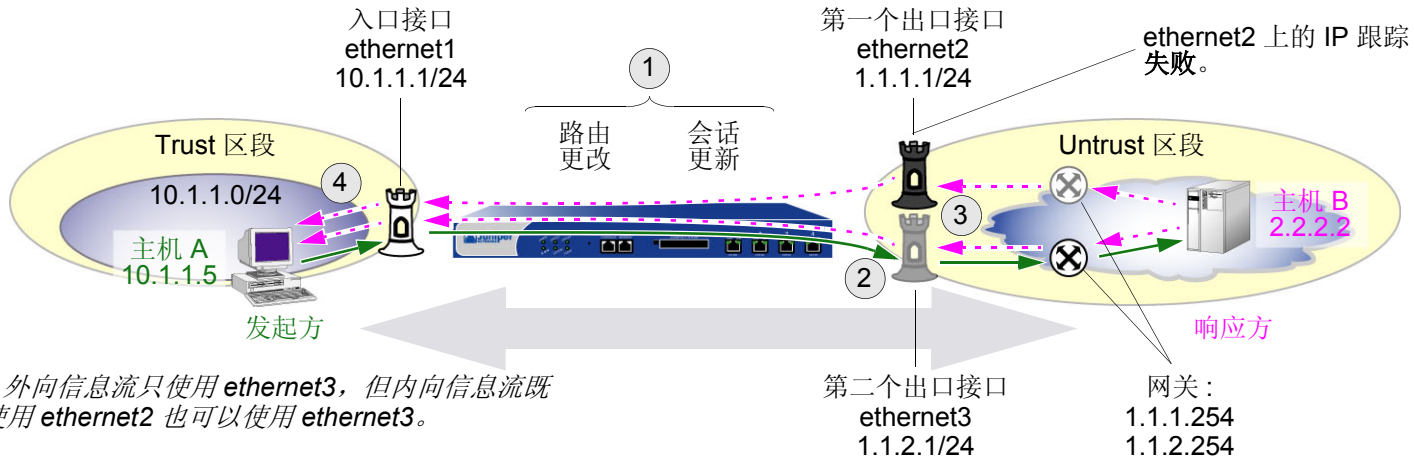
从主机 A 到主机 B 的信息流 – 回复



1. 位于 2.2.2.2 处的主机 B 通过旨在发往 10.1.1.5 处的主机 A 的数据包进行回复 (为清楚起见忽略了 NAT)。
2. 当位于 1.1.1.254 处的网关接收到回复时，它会将该回复转发给其下一个跳跃，即 ethernet2 的 IP 地址 1.1.1.1。
3. NetScreen 设备执行会话查找。由于这是一个回复，因此 NetScreen 设备用一个现有会话与其匹配并刷新会话表条目。
4. 通过使用存入高速缓存的主机 A 的 MAC 地址或者通过执行 ARP 查找来发现其 MAC 地址， NetScreen 设备通过 ethernet1 将数据包转发给主机 A。

如果 ethernet2 上的 IP 跟踪失败，NetScreen 设备将中断使用 ethernet2 的路由并将 ethernet3 用于到主机 B 的出站信息流。但是，从主机 B 到主机 A 的回复可以通过 ethernet2 或 ethernet3 到达，并且 NetScreen 设备将通过 ethernet1 将回复转发给主机 A。

从主机 A 到主机 B 的信息流 – IP 跟踪失败触发重新路由



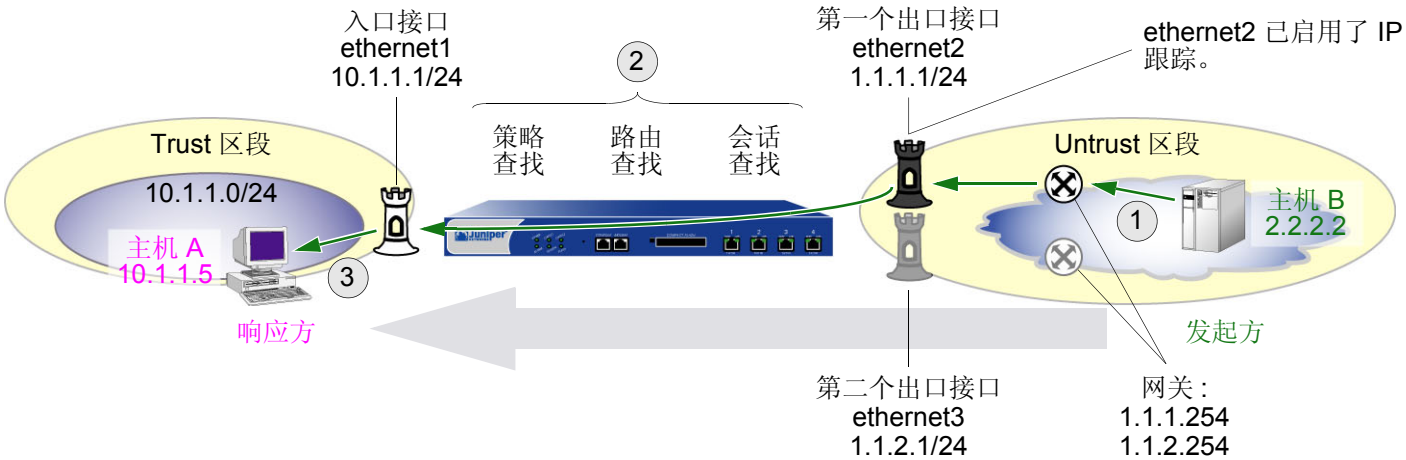
注意：*外向信息流只使用 ethernet3，但内向信息流既可以使用 ethernet2 也可以使用 ethernet3。*

1. 当 ethernet2 上的 IP 跟踪失败时， NetScreen 设备将执行以下任务：
   1.1 **路由更改** – NetScreen 设备中断使用 ethernet2 的所有路由。将执行路由查找并将使用 ethernet2 和网关 1.1.1.254 的到 2.2.2.2 的路由替换为使用 ethernet3 和网关 1.1.2.254 的路由。
   1.2 **会话更新** – NetScreen 设备扫描会话表以查找使用 ethernet2 的所有条目，并通过 ethernet3 将其重新路由到网关 1.1.2.254。
2. 此时， NetScreen 设备将来自主机 A 的信息流经由 ethernet3 重新定向到 1.1.2.254。
3. 来自主机 B 的回复可以到达 ethernet2 或 ethernet3。NetScreen 设备执行会话查找并将数据包与一个现有会话匹配。不论它们到达哪一个接口， NetScreen 设备都会将数据包通过 ethernet1 转发给主机 A。
4. NetScreen 设备将数据包通过 ethernet1 转发给主机 A。

入口接口上的故障

在接下来的示例中，将再次在 ethernet2 上配置 IP 跟踪，不过对于从主机 B 到主机 A 的会话而言， ethernet2 为 NetScreen 设备上的入口接口。主机 B 通过向主机 A 发送数据包来启动会话。

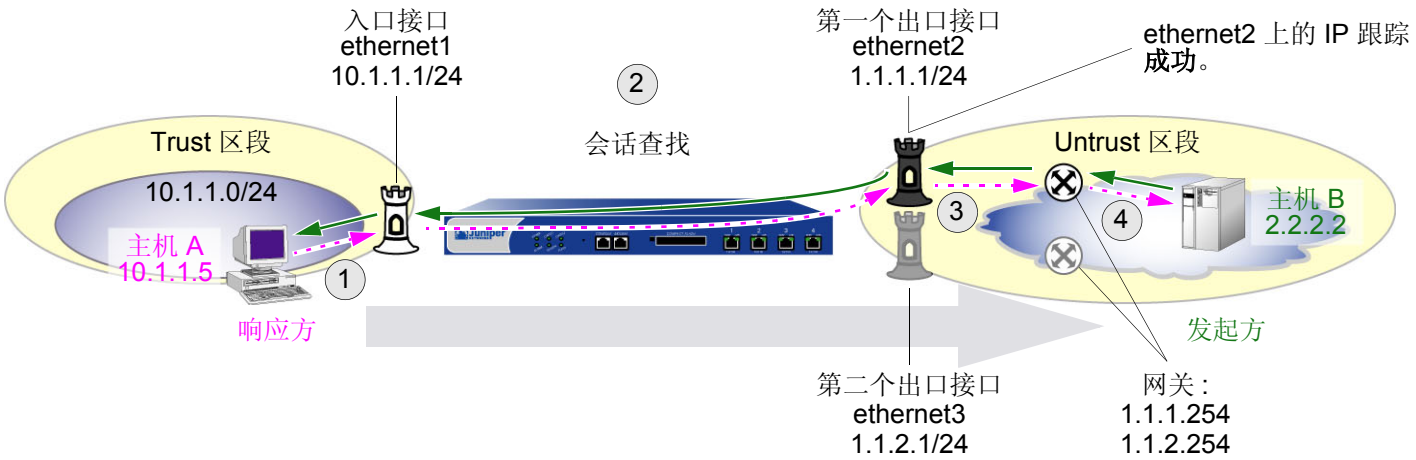
从主机 B 到主机 A 的信息流 – 请求 (启动会话)



1. 位于 2.2.2.2 处的主机 B 发送目的地为 10.1.1.5 处的主机 A 的数据包 (为清楚起见忽略了 NAT)。
2. 当数据包到达 ethernet2 时， NetScreen 设备将执行以下任务 :
   - 2.1 会话查找 (由于这是会话中的第一个数据包，因此将创建一个新会话表条目)
   - 2.2 路由查找
   - 2.3 策略查找
3. NetScreen 设备将数据包通过 ethernet1 转发给位于 10.1.1.5 处的主机 A。

当主机 A 回复主机 B 时，返回的信息流将沿着相似的路径通过 NetScreen 设备，如下所示。

从主机 B 到主机 A 的信息流 – 回复



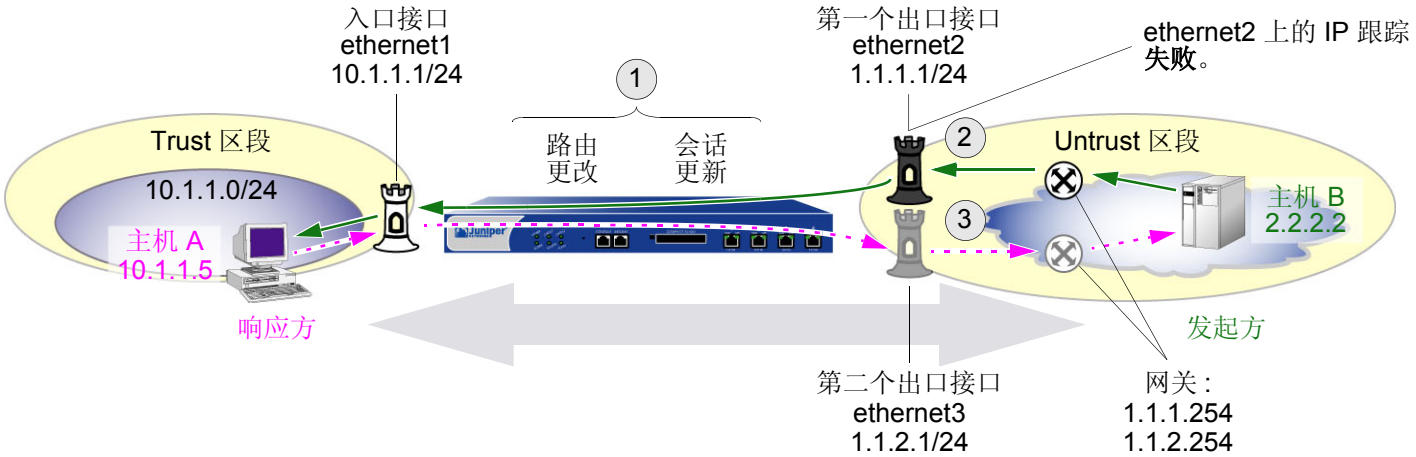
1. 位于 10.1.1.5 处的主机 A 将目的地为主机 B (2.2.2.2) 的回复数据包发送到位于 10.1.1.1 处的 ethernet1。
2. NetScreen 设备执行会话查找。由于这是一个回复，因此 NetScreen 设备用一个现有会话与其匹配并刷新会话表条目。
3. 通过使用存入高速缓存的位于 1.1.1.254 处的网关的 MAC 地址或者通过执行 ARP 查找来发现其 MAC 地址， NetScreen 设备通过 ethernet2 将数据包转发给网关。
4. 当位于 1.1.1.254 处的网关接收到回复时，会将该回复转发给其下一个跳跃。继续路由，直到主机 B 接收到它为止。

如果 ethernet2 上的 IP 跟踪失败，NetScreen 设备将中断使用 ethernet2 的路由并将 ethernet3 用于到主机 B 的出站信息流。不过，从主机 B 到主机 A 的请求仍可通过 ethernet2 到达，且 NetScreen 设备仍将通过 ethernet1 将请求转发给主机 A。IP 跟踪失败后，从主机 B 到主机 A 的请求数据流同 IP 跟踪失败前相比表面上看起来没有发生任何变化。不过，来自主机 A 的回复可以采用两种不同的路径，具体采用哪个路径，这要取决于是否应用了 **set arp always-on-dest** 命令。

如果设置了命令 **set arp always-on-dest**，那么，当处理对会话中第一个数据包的回复或者发生路由更改时，NetScreen 设备将发送一个 ARP 请求以获取目标 MAC 地址。(当取消设置这个命令时，NetScreen 设备将会话发起方的 MAC 地址存入高速缓存并在处理回复时使用该地址。缺省情况下，未设置该命令。)

当 ethernet2 上的 IP 跟踪失败时，NetScreen 设备将首先中断所有使用 ethernet2 的路由，然后再执行路由查找。它找到另外一个可通过 ethernet3 和位于 1.1.2.254 处的网关到达主机 B 的路由。然后扫描其会话表并将所有会话重新定向到该新路由。如果启用了 **set arp always-on-dest** 命令，由于处于受路由更改影响的会话中，当 NetScreen 设备接收到来自主机 A 的下一个数据包时，将执行 ARP 查找。不论来自主机 B 的数据包到达哪一个入口接口，NetScreen 设备都会通过 ethernet3 将来自主机 A 的所有进一步回复发送到位于 1.1.2.254 处的网关。

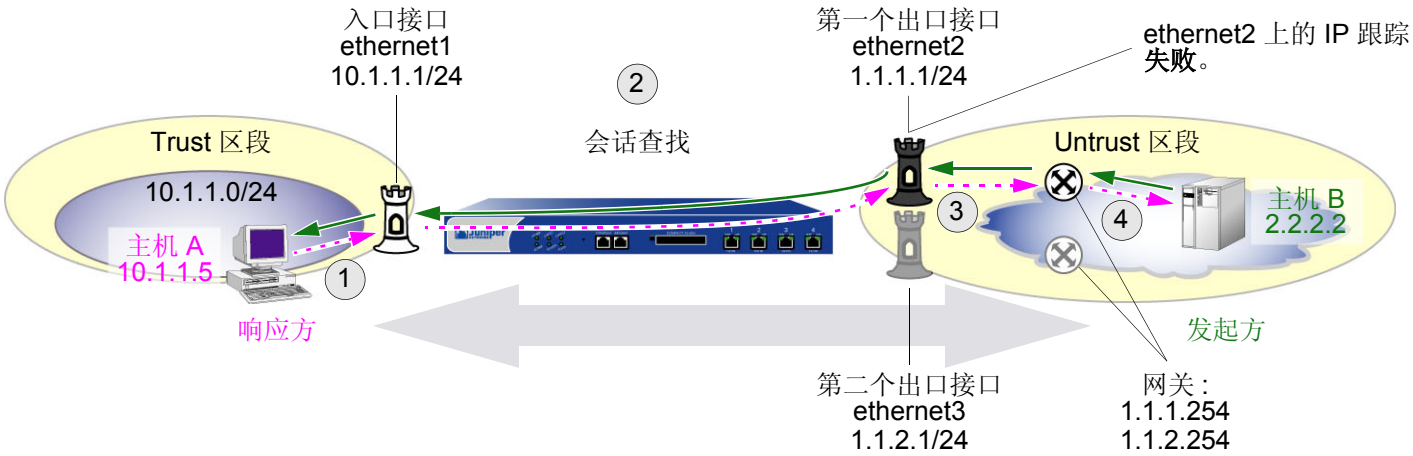
从主机 B 到主机 A 的信息流 – IP 跟踪失败触发重新路由



1. 当 ethernet2 上的 IP 跟踪失败时， NetScreen 设备将执行以下任务 :
   - 1.1 **路由更改** – NetScreen 设备中断使用 ethernet2 的所有路由。它将到 2.2.2.2 的使用 ethernet2 和网关 1.1.1.254 的路由替换为使用 ethernet3 和网关 1.1.2.254 的路由。
   - 1.2 **会话更新** – NetScreen 设备扫描会话表以查找使用 ethernet2 的所有条目，并通过 ethernet3 将其重新路由到网关 1.1.2.254。
2. 来自主机 B 的请求仍可到达 ethernet2，否则，路由结构可能会将其重新定向到 ethernet3。 NetScreen 设备执行会话查找并将数据包与一个现有会话匹配。
3. 由于输入了 **set arp always-on-dest** 命令，因此，NetScreen 设备将执行 ARP 查找以获取主机 A 的回复，并会将该回复通过 ethernet3 发送到位于 1.1.2.254 处的网关。

如果设置了命令 **unset arp always-on-dest** (缺省配置)，则 NetScreen 设备将使用位于 1.1.1.1 处的网关的 MAC 地址，当主机 B 发送初始会话数据包时 NetScreen 设备将该地址存入高速缓存。NetScreen 设备继续通过 ethernet2 发送会话回复。在这种情况下， IP 跟踪失败不会导致通过 NetScreen 设备的数据流发生任何变化。

从主机 B 到主机 A 的信息流 – IP 跟踪失败不触发重新路由



1. 当 ethernet2 上的 IP 跟踪失败时， NetScreen 设备将执行以下任务 :
   1.1 **路由更改** – NetScreen 设备中断使用 ethernet2 的所有路由。它将到 2.2.2.2 的使用 ethernet2 和网关 1.1.1.254 的路由替换为使用 ethernet3 和网关 1.1.2.254 的路由。
   1.2 **会话更新** – NetScreen 设备扫描会话表以查找使用 ethernet2 的所有条目，并通过 ethernet3 将其重新路由到网关 1.1.2.254。不过，由于 NetScreen 设备将位于 1.1.1.254 处的网关的 MAC 地址存入了高速缓存，因此会继续将该 MAC 地址用于来自主机 A 的回复。
2. 来自主机 B 的请求仍可到达 ethernet2。 NetScreen 设备执行会话查找，将数据包与一个现有会话匹配，并通过 ethernet1 将该数据包转发给位于 10.1.1.5 处的主机 A。
3. 当主机 A 进行回复时，NetScreen 设备会将回复从 ethernet2 转发至位于 1.1.1.254 处的网关。由于没有设置 **set arp always-on-dest** 命令，因此从最初创建会话表条目时起， MAC 地址在会话表中将保持不变。

4

接口模式

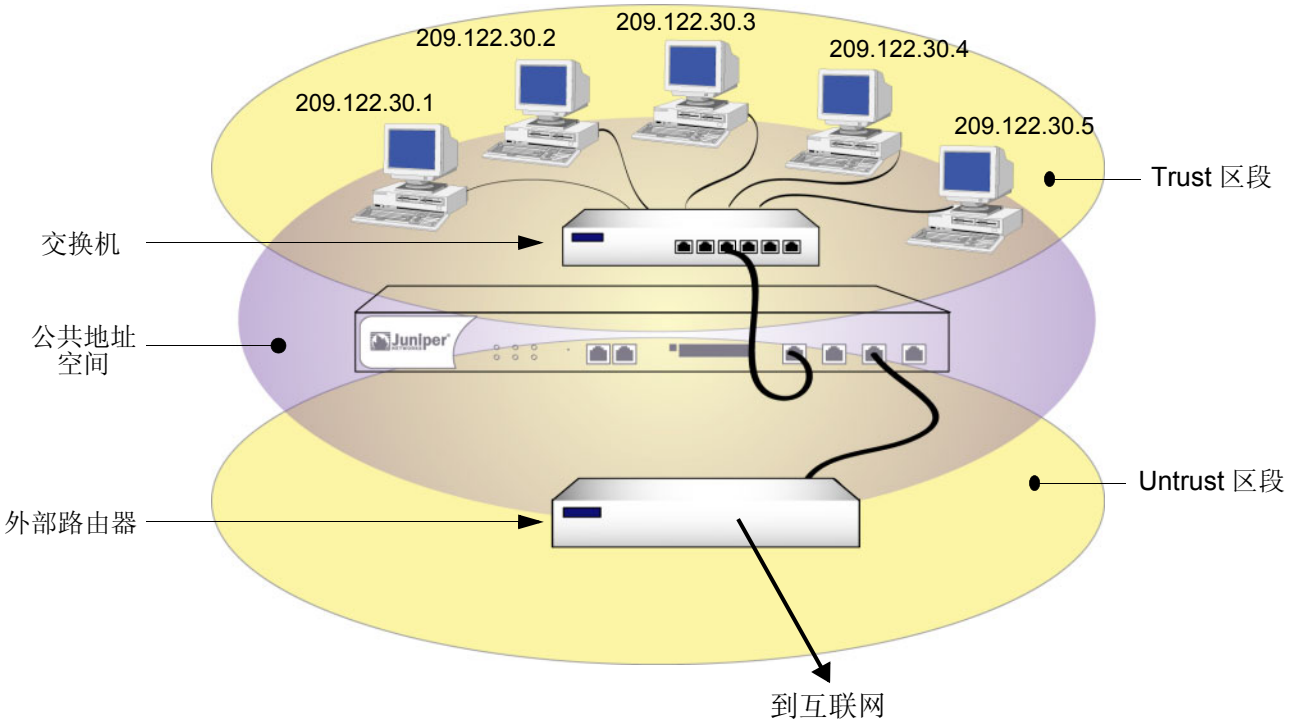
接口能以三种不同模式运行，分别是：网络地址转换 (NAT)、路由和透明。如果绑定到第 3 层区段的接口具有 IP 地址，则可将该接口的操作模式定义为 NAT[1] 或路由。绑定到第 2 层区段 (如预定义的 v1-trust、 v1-untrust 和 v1-dmz，或用户定义的第 2 层区段) 的接口必须为透明模式。在配置接口时选择操作模式。

本章包括以下各节：

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

透明模式

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



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

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

区段设置

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

VLAN 区段

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

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

预定义的第 2 层区段

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

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

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

信息流转发

在第 2 层 (L2) 运行的 NetScreen 设备不允许任何区段间或区段内信息流，除非在该设备上配置了相应的策略。有关如何设置策略的详细信息，请参阅第 293 页上的 “策略”。在 NetScreen 设备上配置了策略后，该策略执行以下任务：

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

可以按如下所述内容更改设备的转发行为：

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

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

未知单播选项

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

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

注意：*透明模式下的 NetScreen 设备不允许区段间的任何信息流，除非在该设备上配置了策略。有关透明模式下的设备如何转发信息流的详细信息，请参阅**第 106 页上的 “信息流转发”**。*

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

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

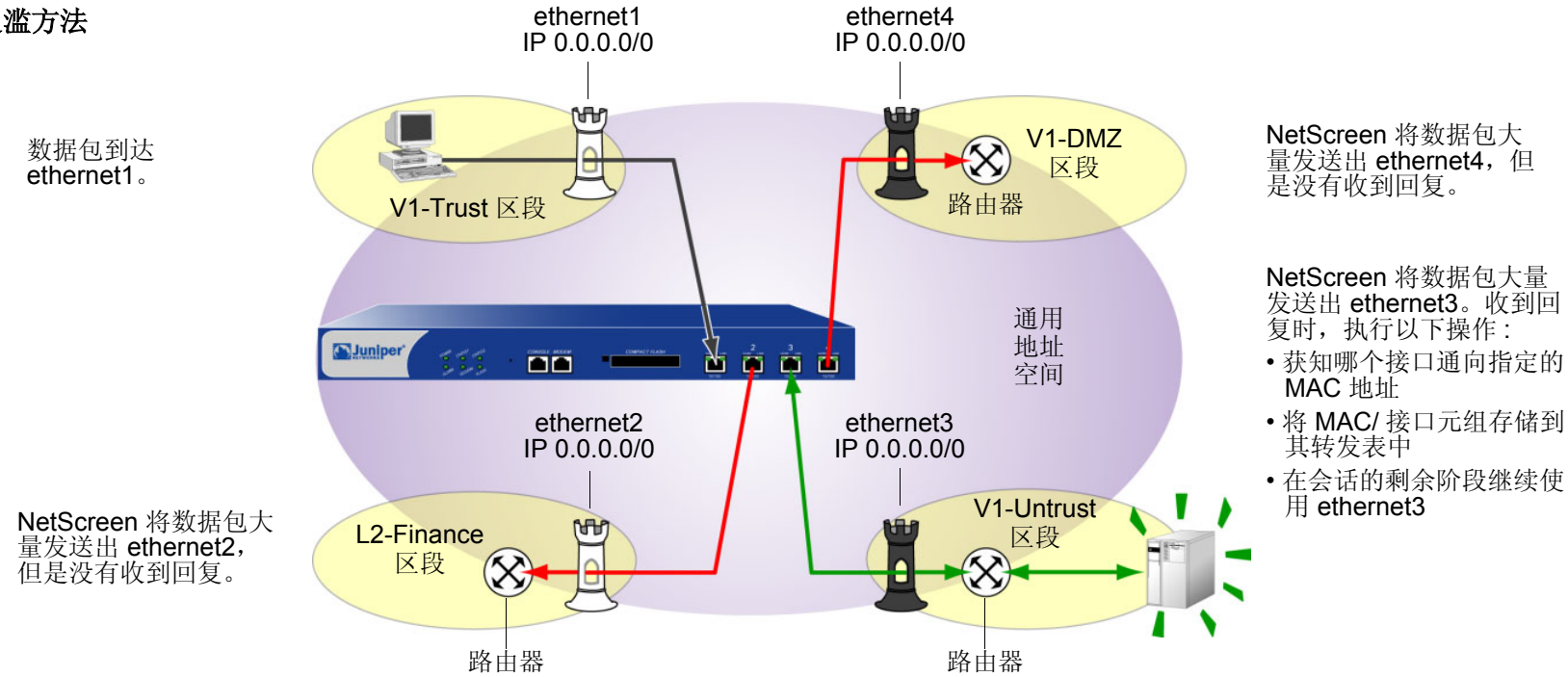
> ***注意：****泛滥和 ARP/trace-route 这两种方法中， ARP/trace-route 更安全，因为 NetScreen 设备将 ARP 查询和 trace-route 数据包 (而非初始数据包) 大量发送出所有接口。*

泛滥方法

泛滥方法用与多数第 2 层交换机相同的方式转发数据包。交换机维护转发表，该表中包含 MAC 地址和每个第 2 层域的相关端口。该表还包含相应的接口，通过该接口，交换机能将信息流转发到每个设备。每次在其帧头中带有新的源 MAC 地址的数据包到达时，交换机都会将该 MAC 地址添加到其转发表中。它还跟踪数据包到达的接口。如果交换机无法识别目标 MAC 地址，交换机将复制数据包并将其大量发送出所有接口 (数据包到达的接口除外)。当带有该 MAC 地址的回复到达这些接口之一时，它即获知先前未知的 MAC 地址及其相应接口。

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

泛滥方法



要启用泛滥方法来处理未知的单播数据包，请执行以下操作之一：

WebUI

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

CLI

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

ARP/Trace-Route 方法

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

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

   如果目标 IP 地址属于与入口 IP 地址[3] 在同一子网中的设备，则主机返回一条带有其 MAC 地址的 ARP 回复 (arp-r)，从而指示出 NetScreen 设备必须通过它转发以该地址为目的地的信息流的接口。 (请参阅第 112 页上的 “ARP 方法”。)

   如果目标 IP 地址属于入口 IP 地址所在子网之外的其它子网中的设备，则 trace-route 返回通向目的地[4] 的路由器的 IP 地址和 MAC 地址，更重要的是，指出了 NetScreen 设备必须通过它转发流向该 MAC 地址的信息流的接口。 (请参阅第 113 页上的 “Trace-Route”。)
4. NetScreen 设备将从初始数据包中收集的目标 MAC 地址与通向该 MAC 地址的接口相结合，添加新的条目到其转发表中。
5. NetScreen 设备将其收到的所有后续数据包从正确接口转发到达目的地。

---

2. 启用 ARP 方法时，缺省情况下将启用 trace-route 选项。也可启用不带 trace-route 选项的 ARP 方法。但是，如果目标 IP 地址与入口 IP 地址在同一子网中，则该方法只允许 NetScreen 设备发现单播数据包的目标 MAC 地址。 (有关入口 IP 地址的详细信息，请参阅下一脚注。)
3. 入口 IP 地址指将数据包发送到 NetScreen 设备的最后设备的 IP 地址。此设备可能是发送数据包的源，或者是转发数据包的路由器。
4. 实际上，trace-route 返回子网中所有路由器的 IP 地址和 MAC 地址。然后，NetScreen 设备将初始数据包的目标 MAC 地址与 arp-r 数据包中的源 MAC 地址相匹配，以确定目标路由器，进而确定使用哪个接口到达该目的地。

要启用 ARP/trace-route 方法来处理未知的单播数据包，请执行以下操作之一：

WebUI

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

CLI

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

注意：*缺省情况下将启用 trace-route 选项。如果要使用不带 trace-route 选项的 ARP, 请输入以下命令：* ***unset interface vlan1 broadcast arp trace-route****。此命令将取消设置 trace-route 选项，但仍会将 ARP 设置为处理未知单播数据包的方法。*

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

ARP 方法

注意： *以下仅显示数据包包头的相关元素和 MAC 地址中的后四位数字。*

如果下列数据包

以太网帧			IP 数据包	
目标	源	类型	源	目标
11bb	11aa	0800	210.1.1.5	210.1.1.75

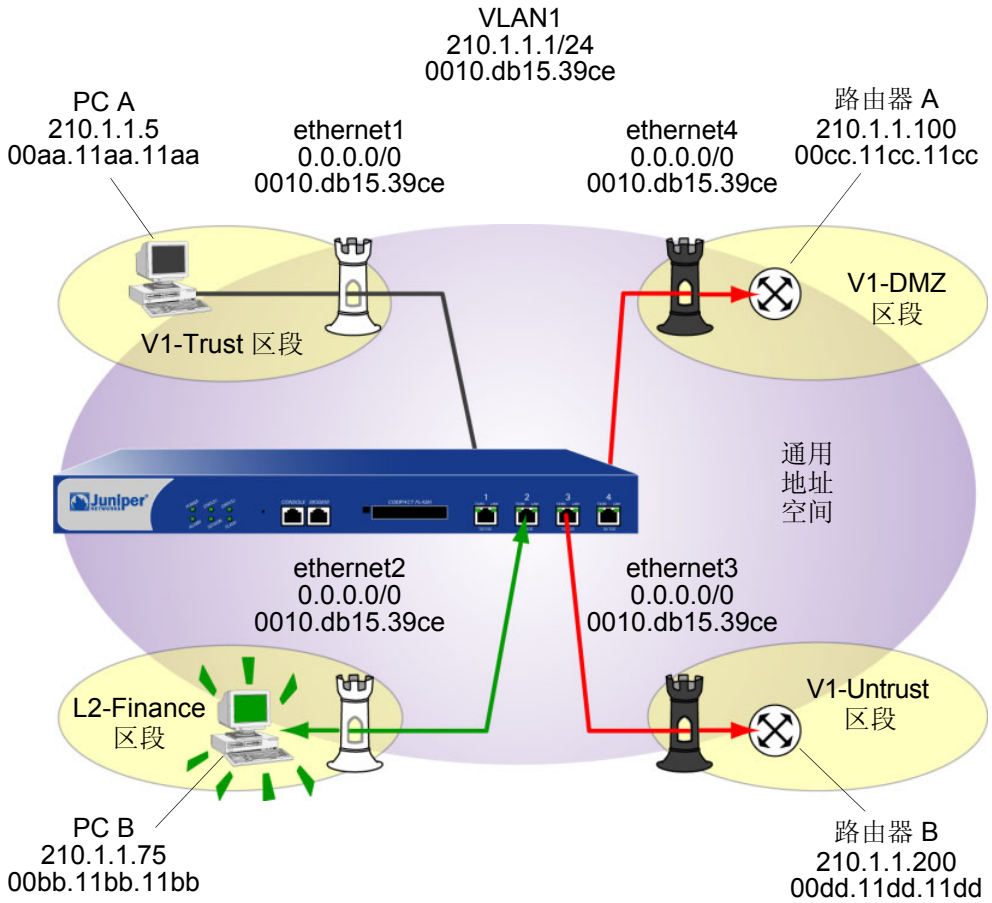
到达 ethernet1，并且转发表中没有 MAC 地址 00bb.11bb.11bb 的条目，NetScreen 设备将以下 arp-q 数据包大量发送出 eth2、 eth3 和 eth4。

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

当 NetScreen 设备在 eth2 收到以下 arp-r 时，

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

它现在能将 MAC 地址与通向该地址的接口相关联。



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

Trace-Route

注意：*以下仅显示数据包包头的相关元素和 MAC 地址中的后四位数字。*

如果下列数据包

以太网帧			IP 数据包	
目标	源	类型	源	目标
11dd	11aa	0800	210.1.1.5	195.1.1.5

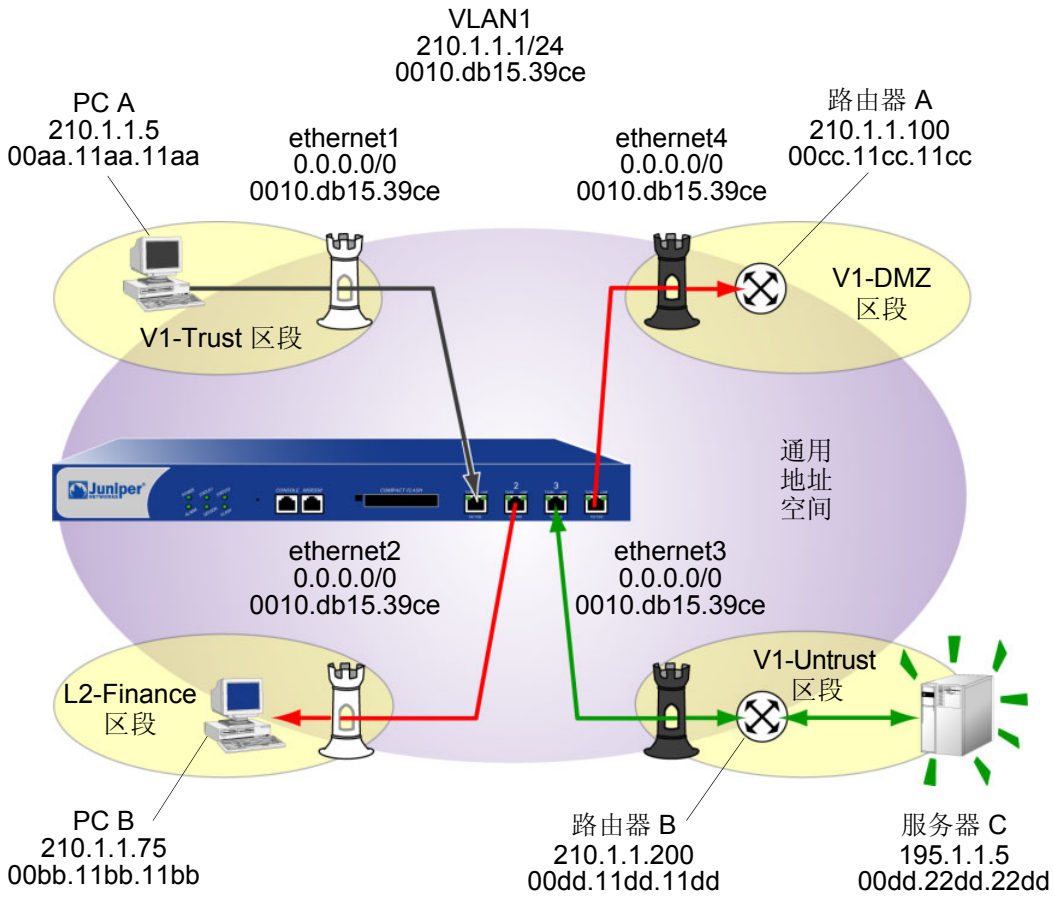
到达 ethernet1，并且转发表中没有 MAC 地址 00dd.11dd.11dd 的条目，NetScreen 设备将以下 trace-route 数据包大量发送出 eth2、 eth3 和 eth4。

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

NetScreen 设备在 eth3 收到以下回应时，

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

它现在能将 MAC 地址与通向该地址的接口相关联。



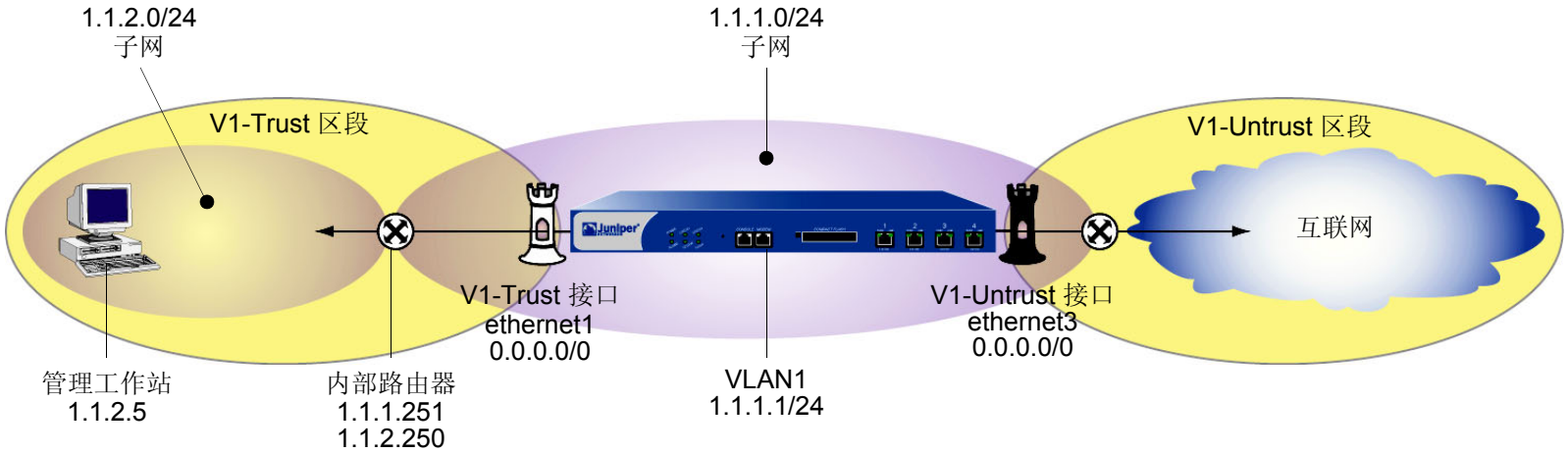
范例：用于管理的 VLAN1 接口

在本例中，可按下述内容对 NetScreen 设备进行配置，使用其 VLAN1 接口进行管理：

- 为 VLAN1 接口分配 IP 地址 1.1.1.1/24。
- 在 VLAN1 接口和 V1-Trust[5] 安全区段上启用 Web、 Telnet、 SSH 和 Ping。

> ***注意：****要从第 2 层安全区段管理设备，必须在 VLAN1 接口和第 2 层安全区段上设置相同的管理选项。*

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



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

WebUI

1. VLAN1 接口

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

   IP Address/Netmask: 1.1.1.1/24

   Management Services: WebUI, Telnet, SSH (选择)

   Other Services: Ping (选择)

2. V1-Trust 区段

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

   Management Services: WebUI, Telnet, SSH

   Other Services: Ping

3. 路由

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

   Network Address/Netmask: 1.1.2.0/24

   Gateway: (选择)

   Interface: vlan1(trust-vr)

   Gateway IP Address: 1.1.1.251

   Metric: 1

CLI

1. VLAN1 接口

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

2. V1-Trust 区段

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

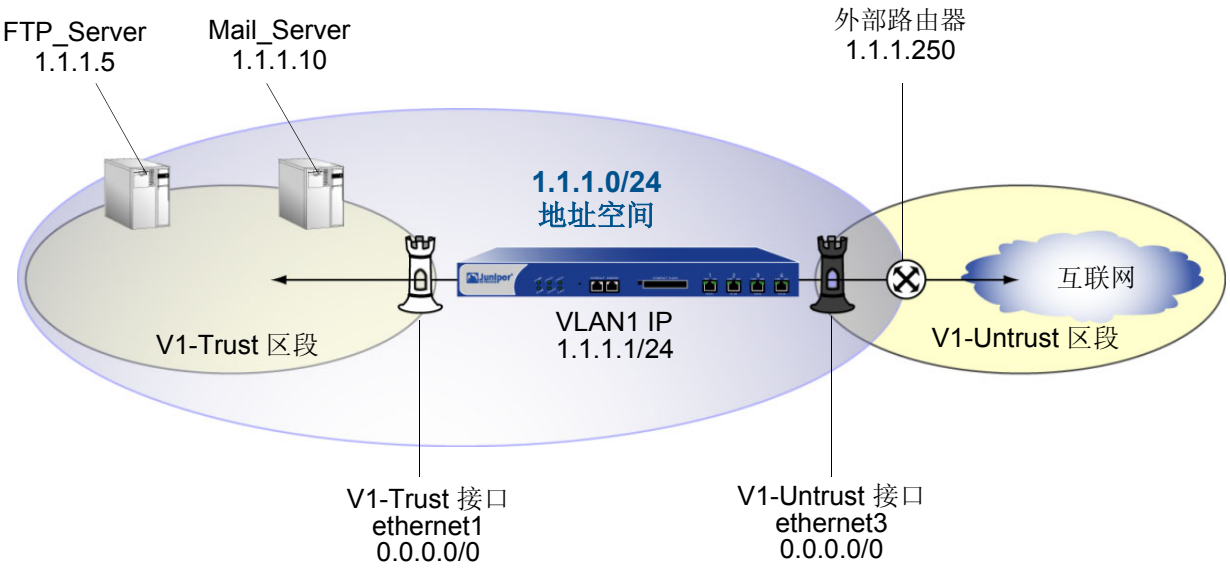
3. 路由

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

范例：透明模式

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

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



6. 有关为接口处于透明模式的 NetScreen 设备配置 VPN 通道的范例，请参阅第 **5**-217 页上的 “透明模式 VPN”。

WebUI

1. VLAN1 接口

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

   IP Address/Netmask: 1.1.1.1/24

   Management Services: WebUI, Telnet (选择)

   Other Services: Ping (选择)

2. HTTP 端口

   Configuration > Admin > Management: 在 HTTP Port 字段中，键入 5555[7]，然后单击 **Apply**。

3. 接口

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

   Zone Name: V1-Trust

   IP Address/Netmask: 0.0.0.0/0

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

   Zone Name: V1-Untrust

   IP Address/Netmask: 0.0.0.0/0

4. V1-Trust 区段

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

   Management Services: WebUI, Telnet

   Other Services: Ping

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

5. 地址

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

Address Name: FTP_Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/32

Zone: V1-Trust

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

Address Name: Mail_Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.10/32

Zone: V1-Trust

6. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: vlan1(trust-vr)

Gateway IP Address: 1.1.1.250

Metric: 1

7. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Mail_Server

Service: Mail

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), FTP_Server

Service: FTP-GET

Action: Permit

CLI

1. VLAN1

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

2. Telnet

```
set admin telnet port 4646[8]
```

3. 接口

```
set interface ethernet1 ip 0.0.0.0/0
set interface ethernet1 zone v1-trust
set interface ethernet3 ip 0.0.0.0/0
set interface ethernet3 zone v1-untrust
```

4. V1-Trust 区段

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

5. 地址

```
set address v1-trust FTP_Server 1.1.1.5/32
set address v1-trust Mail_Server 1.1.1.10/32
```

6. 路由

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

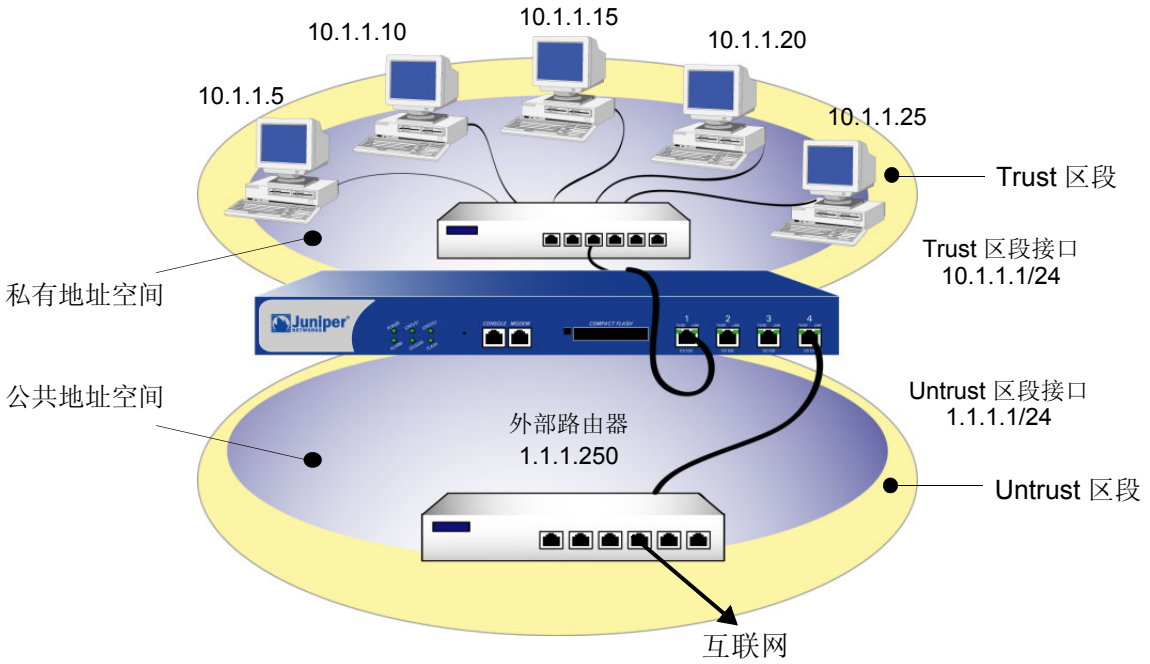
7. 策略

```
set policy from v1-trust to v1-untrust any any any permit
set policy from v1-untrust to v1-trust any Mail_Server mail permit
set policy from v1-untrust to v1-trust any FTP_Server ftp-get permit
save
```

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

NAT 模式

入口接口处于“网络地址转换 (NAT)”模式下时， NetScreen 设备的作用与第 3 层交换机 (或路由器) 相似，转换通往 Untrust 区段的外向 IP 数据包包头中的两个组件 : 其源 IP 地址和源端口号。 NetScreen 设备用 Untrust 区段接口的 IP 地址替换发端主机的源 IP 地址。另外，它用由 NetScreen 设备随机生成的另一端口号替换源端口号。



当回复数据包到达 NetScreen 设备时，该设备转换内向数据包的 IP 包头中的两个组件 : 目标地址和端口号，它们被转换回初始号码。 NetScreen 设备于是将数据包转发到其目的地。

NAT 添加透明模式中未提供的一个安全级别 : 通过 NAT 模式下的入口接口 (如 Trust 区段接口) 发送信息流的主机地址从来不会对出口区段 (如 Untrust 区段) 中的主机公开，除非这两个区段位于同一个虚拟路由选择域中并且 NetScreen 设备正通过动态路由协议 (DRP) 向对等方通告路由。尽管这样，如果有策略允许入站信息流到达，则只能到达 Trust 区段地址。 (如果希望在使用 DRP 时隐藏 Trust 区段地址，则可将 Untrust 区段放置在 untrust-vr 中，将 Trust 区段放置在 trust-vr 中，并且不将 trust-vr 中内部地址的路由导出到 untrust-vr。)

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

另外，NAT 还保留对公共 IP 地址的使用。在许多环境中，资源不可用，不能为网络上的所有设备提供公共 IP 地址。NAT 服务允许多个私有 IP 地址通过一个或几个公共 IP 地址访问互联网资源。以下 IP 地址范围保留给私有 IP 网络，并且一定不要在互联网上设定路由：

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

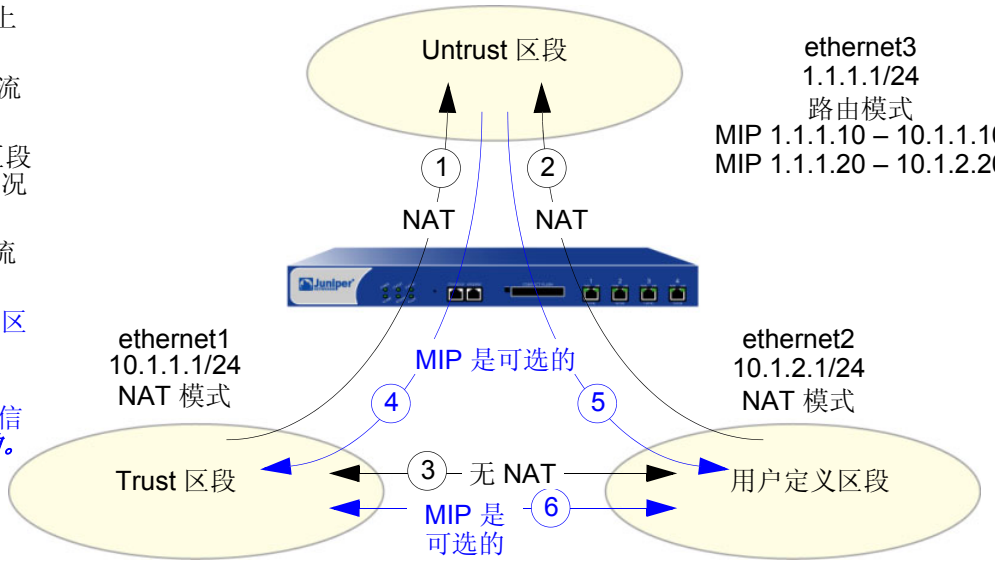
192.168.0.0 – 192.168.255.255

入站和出站 NAT 信息流

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

1. 从 Trust 区段到 Untrust 区段的信息流上的基于接口的 NAT。
2. 从用户定义区段到 Untrust 区段的信息流上的基于接口的 NAT。

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



注意：*有关 MIP 的详细信息，请参阅第* ***7****-90 页上的“映射 IP 地址”。有关 VIP 的详细信息，请参阅第* ***7****-115 页上的“虚拟 IP 地址”。*

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

接口设置

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

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

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

† 用于信息流整型的可选设置。

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

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

范例 : NAT 模式

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

> ***注意 :*** *将此范例与第 132 页上 “路由” 模式的范例进行比较。*

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT[10]

10. 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 > 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[11]: 1.1.1.1/24

Interface Mode: Route

2. VIP[12]

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

Virtual IP Address: 1.1.1.5

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

Virtual Port: 25

Map to Service: Mail

Map to IP: 10.1.1.5

3. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

12. 有关虚拟 IP (VIP) 地址的信息，请参阅第 **7**-115 页上的 “虚拟 IP 地址”。

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

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

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat[13]

set interface ethernet3 zone untrust[14]
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 route
```

2. VIP

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

3. 路由

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

4. 策略

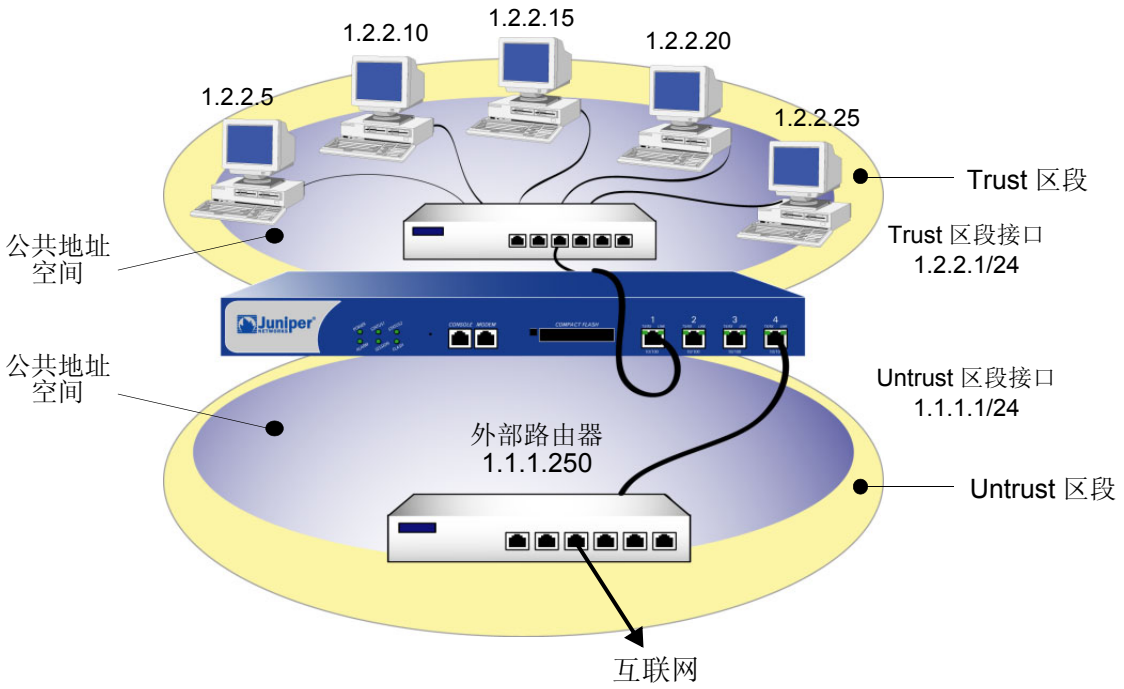
```
set policy from trust to untrust any any any permit
set policy from untrust to global any vip(1.1.1.5) mail permit
save
```

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

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

路由模式

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



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

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

***注意：**有关配置基于策略的 NAT-src 的详细信息，请参阅第 **7-15** 页上的 “源网络地址转换”。*

接口设置

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

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

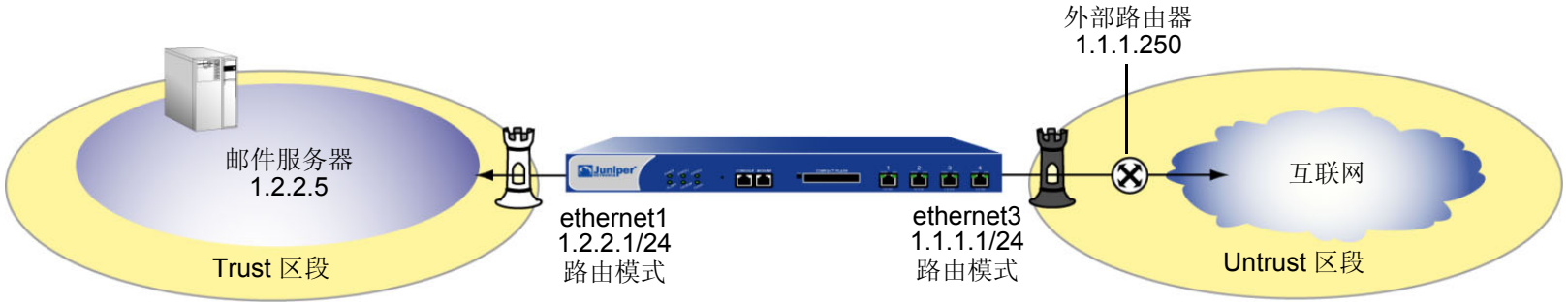
* 可在每个接口的基础上设置管理 IP 地址。主要目的是为从网络信息流中分离出来的管理信息流提供 IP 地址。当某特定设备具备高可用性配置时，也可使用管理 IP 地址来访问它。

† 用于信息流整形的可选设置。

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

范例：路由模式

在上一范例第 126 页上的 “范例：NAT 模式”中， Trust 区段 LAN 中的主机具有私有 IP 地址和邮件服务器的映射 IP。在以下相同网络 (受运行在路由模式下的 NetScreen 设备保护) 的范例中，要注意，主机具有公共 IP 地址，且邮件服务器不需要 MIP。所有安全区段都在 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: 1.2.2.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: Route[15]

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

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask[16] : 1.1.1.1/24

2. 地址

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

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: Trust

3. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Mail Server

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 1.2.2.1/24
set interface ethernet1 route[17]

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

2. 地址

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

3. 路由

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

4. 策略

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

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

5

策略的构建块

本章讨论了可以在策略中引用的组件或构建块。讨论的具体主题如下：

- 第 267 页上的 “DIP 池”
  - 第 270 页上的 “附着 DIP 地址”
  - 第 271 页上的 “扩展接口和 DIP”
  - 第 279 页上的 “回传接口和 DIP”
  - 第 285 页上的 “DIP 组”
- 第 289 页上的 “时间表”

***注意：**有关用户认证的信息，请参阅第 8 卷，“用户认证”。*

地址

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

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

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

要想配置策略以允许、拒绝信息流或设置出入单个主机和子网的通道信息流，首先必须在按区段组织的 NetScreen 地址列表中为其构造条目。

注意：*不必为 “Any” 构建地址条目。此术语会自动应用到所有实际设备，这些设备都位于它们各自区段中。*

地址条目

首先必须在一个或多个地址列表中定义地址，然后才能设置各种 NetScreen 防火墙、 VPN 及信息流整形功能。安全区段的地址列表包含主机或子网的 IP 地址或域名[1]，对这些主机或子网的信息流可以采取允许、阻塞、加密或用户验证等操作。

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

范例：添加地址

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

WebUI

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

Address Name: Sunnyvale_Eng

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.10.0/24

Zone: Trust

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

Address Name: Juniper

IP Address/Domain Name:

Domain Name: (选择), www.juniper.net

Zone: Untrust

1. 必须为 NetScreen 设备配置 “域名系统 (DNS)”服务，才能使用地址条目域名。有关 DNS 配置的信息，请参阅第 359 页上的 “域名系统支持”。

CLI

```
set address trust Sunnyvale_Eng 10.1.10.0/24
set address untrust Juniper www.juniper.net
save
```

范例：修改地址

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

WebUI

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

Address Name: Sunnyvale_SW_Eng

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.40.0/24

Zone: Trust

CLI

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

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

范例：删除地址

在本例中，将移除地址 “Sunnyvale_SW_Eng”的地址条目。

WebUI

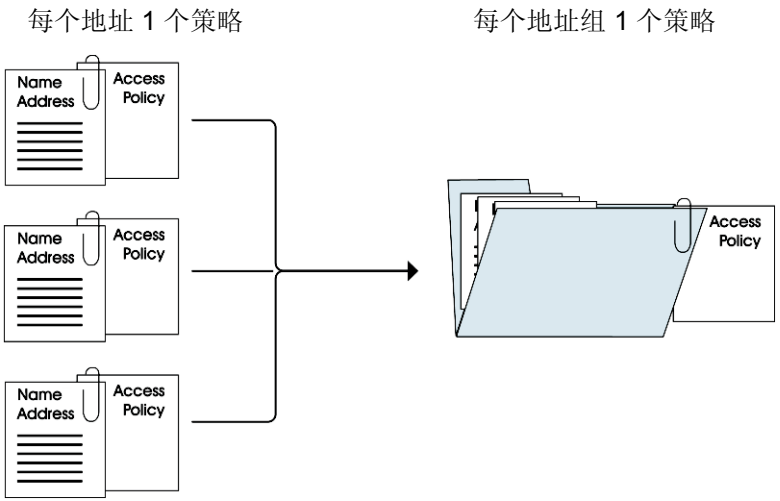
Objects > Addresses > List: 在 Sunnyvale_SW_Eng 的 Configure 栏中，单击 **Remove**。

CLI

```
unset address trust “Sunnyvale_SW_Eng”
save
```

地址组

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



地址组选项具有下列功能：

- 可以在任何区段中创建地址组。
- 可以创建有现有用户的地址组，也可以创建空地址组而在以后使用用户填充它们。
- 某一地址组可以是其他地址组的成员[2]。
- 可以在策略中引用地址组条目，如同单个通讯簿条目一样。
- NetScreen 可在内部为每个组成员创建单个策略，从而将策略应用到组的每个成员。虽然只需为组创建一个策略，但 NetScreen 实际上会为组中的每个成员 (还为针对每个用户配置的各项服务) 都创建一个内部策略。[3]
- 从通讯簿中删除单个通讯簿条目时， NetScreen 设备将会从它所属的所有组中自动将其移除。

地址组适用以下限制：

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

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

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

范例：创建地址组

在下例中，将创建一个名为 “HQ 2nd Floor” 的组，该组包括 “Santa Clara Eng” 和 “Tech Pubs” 两个地址，它们都已输入 Trust 区段的通讯簿。

WebUI

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

Group Name: HQ 2nd Floor

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

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

CLI

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

范例：编辑地址组条目

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

WebUI

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

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

CLI

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

范例：移除成员和组

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

WebUI

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

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

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

CLI

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

注意：*NetScreen 设备不会自动删除已经移除其中所有名称的组。*

服务

服务是信息流的类型，它们有相应的协议标准。每种服务都有与之关联的传输协议和目标端口号，如 FTP 的 TCP/ 端口 21 及 Telnet 的 TCP/ 端口 23。创建策略时，必须为其指定服务。可以从服务簿中选择一个预定义的服务，或者选择一个创建的定制服务或服务组。通过查看 Policy Configuration 页面中的 Service 下拉列表 (WebUI)，或使用 **get service** 命令 (CLI)，可以查看能够在策略中使用的服务。

预定义的服务

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

- 第 154 页上的 “ICMP 服务”
- 第 156 页上的 “RSH ALG”
- 第 156 页上的 “Sun 远程过程调用应用程序层网关”
- 第 159 页上的 “Microsoft 远程过程调用应用程序层网关”
- 第 164 页上的 “实时流协议应用程序层网关”
- 第 176 页上的 “IP 语音通信的 H.323 协议”
- 第 195 页上的 “会话启动协议 (SIP)”

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

使用 WebUI:

Objects > Services > Predefined

Objects > Services > Custom

Objects > Services > Groups

使用 CLI:

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

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

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

注意：*每个预定义服务的源端口范围都为 1-65535，其中包括有效端口号的完整集合。这样可以阻止潜在的攻击者通过使用范围以外的源端口获得访问权。对于所有预定义的服务，如果需要使用不同的源端口范围，请创建一个定制服务。有关信息，请参阅**第 149 页上的 “定制服务”**。*

定制服务

您可轻松创建定制服务而不使用预定义的服务。可为每个定制服务指定以下属性：

- 名称
- 传输协议
- 使用 TCP 或 UDP 的服务的源和目标端口号
- 使用 ICMP 的服务的类型和代码值
- 超时值

如果在虚拟系统 (vsys) 中创建的定制服务与先前在根系统中定义的定制服务具有相同名称，则 vsys 中的服务将采用特定传输协议 (TCP、 UDP 或 ICMP) 的缺省超时值。当根系统中具有相同名称的定制服务有其自己的超时值时，要为 vsys 中的服务定义不同于缺省值的定制超时值，请按以下顺序创建 vsys 中和根系统中的定制服务：

1. 首先，在 vsys 中创建具有定制超时的定制服务。
2. 然后，在根系统中创建名称相同但超时值不同的另一定制服务。

以下范例介绍如何添加、修改和移除定制服务。

注意：*有关 ScreenOS 命名约定的信息 (用于为定制服务创建的名称)，请参阅**第 xii 页上的 “命名约定和字符类型”**。*

范例：添加定制服务

要将定制服务添加到服务簿中，需要以下信息：

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

WebUI

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

Service Name: cust-telnet

Service Timeout: Custom (选择), 30 (输入)

Transport Protocol: TCP (选择)

Source Port Low: 1

Source Port High: 65535

Destination Port Low: 23000

Destination Port High: 23000

CLI

```
set service cust-telnet protocol tcp src-port 1-65535 dst-port 23000-23000
set service cust-telnet timeout 30[4]
save
```

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

范例：修改定制服务

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

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

WebUI

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

Destination Port Low: 23230

Destination Port High: 23230

CLI

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

范例：移除定制服务

在本例中，将移除定制服务 cust-telnet。

WebUI

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

CLI

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

服务超时

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

以下是有关服务超时行为的一些详细信息 :

- 当策略引用设有定制超时的单个定制或预定义服务时， NetScreen 设备将应用该超时。
- 当策略引用服务组、多个服务或预定义的服务 ANY 时， NetScreen 设备将应用已配置的、与协议 (TCP 或 UDP) + 目标端口号匹配的上一服务的超时。例如，如果按以下顺序定义下面两个服务，

```
set service ftp-1 protocol tcp src 0-65535 dst 2121-2121 timeout 20
set service telnet-1 protocol tcp src 0-65535 dst 2100-2148 timeout 15
```

  然后在同一策略中与其它服务一起引用 ftp-1，则 NetScreen 设备将应用为 telnet-1 定义的 15 分钟超时，而不应用 ftp-1 的 20 分钟超时。这是因为 NetScreen 设备使用两个表 (一个用于 TCP，另一个用于 UDP) 中的 TCP 和 UDP 协议存储服务超时。当 NetScreen 设备查找在服务组、有多个服务的策略或通配符服务 ANY 中所引用服务的超时值时，它将应用在表中找到的第一个服务的超时，如果有具有重叠目标端口号的多个服务，该服务将是最后一个进行配置并输入到表中的服务。在上面的范例中， NetScreen 设备应用 15 分钟超时，因为 telnet-1 (2100-2148) 与 ftp-1 (2121) 的目标端口号重叠，而且 telnet-1 是在您定义了 ftp-1 之后定义的。因此，查找具有目标端口 2121 的服务时将首先找到 telnet-1 的超时并应用该超时。

  为防止意外将不同的超时应用于某个服务，请避免出现有重叠目标端口号的服务或避免应用先前在策略中自行定义的服务。
- 对于使用 ICMP 的服务或使用 TCP 或 UDP 以外的其它协议的服务，当策略刚好引用该服务时， NetScreen 设备将应用定制超时。策略引用多个服务时， NetScreen 设备将对使用非 TCP 或 UDP 协议的服务应用缺省超时 (一分钟)。
- 当虚拟系统 (vsys) 中的策略引用定制服务且根系统中有具有同样的协议 + 目标端口号的先前定义服务时，NetScreen 设备会将在根级定义的服务的超时应用于 vsys 级的服务。

- 不能为在 vsys 级创建的定制服务明确定义定制超时。但是，如果在 vsys 中创建定制服务则可在 vsys 级间接应用定制超时，然后在根级将需要的定制超时应用到具有相同协议 + 端口号的服务。为此，请按以下顺序进行下列操作：
  1. 在 vsys 中创建定制服务。
  2. 然后，在根系统中创建具有相同协议和目标端口号的另一定制服务，并且该服务还应具有要在 vsys 级应用的超时。

范例：设置服务超时

本例中，将把 BGP 预定义服务的超时临界值更改为 75 分钟：

WebUI

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

Service Timeout: Custom (选择), 75 (输入)

CLI

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

ICMP 服务

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

类型 0 = 回应请求消息

类型 3 = 目标无法到达消息

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

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

ScreenOS 支持 0-255 范围内的任何类型或代码。

5. 有关 ICMP 类型和代码的详细信息，请参阅 RFC 792 “Internet Control Message Protocol”。

范例 : 定义 ICMP 服务

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

WebUI

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

Service Name: host-unreachable

Service Timeout: Custom (选择), 2 (输入)

Transport Protocol: ICMP (选择)

ICMP Type: 3

ICMP Code: 1

CLI

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

RSH ALG

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

Sun 远程过程调用应用程序层网关

Sun RPC [也称作“开放网络计算”(ONC) RPC] 可以提供一种方法，使某台主机上运行的程序能够调用另一台主机上所运行程序中的过程。由于大量的 RPC 服务及广播需要，RPC 服务的传输地址将基于服务的程序号和版本号动态进行协商。将会定义多个绑定协议以将 RPC 程序号和版本号映射到传输地址。

NetScreen 设备支持将 Sun RPC 作为预定义服务，并可以根据配置的策略来允许和拒绝信息流。应用程序层网关 (ALG) 为 NetScreen 设备提供了一种功能，可用来处理 Sun RPC 的动态传输地址协商机制，并可确保基于程序号的防火墙策略的实施。可定义防火墙策略以允许或拒绝所有 RPC 请求，或者按特定程序号允许或拒绝。ALG 还支持内向和外向请求的 “路由”和 NAT 模式。

典型 RPC 调用场景

客户端调用远程服务时，它需要查找到该服务的传输地址，如果使用 TCP/UDP 则需查找端口号。此范例的典型过程如下 :

1. 客户端将 GETPORT 消息发送到远程机器上的 RPCBIND 服务。 GETPORT 消息包括程序号及要调用的远程服务的版本和程序号。
2. RPCBIND 服务通过端口号进行回复。
3. 客户端使用返回的端口号调用远程服务。
4. 远程服务回复客户端。

客户端也可使用 CALLIT 消息直接调用远程服务，而不必知晓服务的端口号。这种情况下的过程如下 :

1. 客户端将 CALLIT 消息发送到远程机器上的 RPCBIND 服务。 CALLIT 消息包括程序号及要调用的远程服务的版本和程序号。
2. RPCBIND 为客户端调用服务。
3. 如果调用成功， RCPBIND 将回复客户端。回复将包含调用结果和服务的端口号。

Sun RPC 服务

下表列出了预定义的 Sun RPC 服务。

名称	程序号	说明
SUN-RPC-PORTMAPPER	100000	Sun RPC Portmapper 协议，它是基于 TCP/UDP 端口的服务，包括 TCP/UDP 端口 111。此表中的所有其它服务均为基于程序号的服务。
SUN-RPC-ANY	不适用	任何 Sun RPC 服务
SUN-RPC-MOUNTD	100005	Sun RPC 安装守护程序
SUN-RPC-NFS	100003 100227	Sun RPC 网络文件系统
SUN-RPC-NLOCKMGR	100021	Sun RPC 网络锁定管理器
SUN-RPC-RQUOTAD	100011	Sun RPC 远程空间分配守护程序
SUN-RPC-RSTATD	100001	Sun RPC 远程状态守护程序
SUN-RPC-RUSERD	100002	Sun RPC 远程用户守护程序
SUN-RPC-SADMIND	100232	Sun RPC 系统管理守护程序
SUN-RPC-SPRAYD	100012	Sun RPC SPRAY 守护程序
SUN-RPC-STATUS	100024	Sun RPC STATUS
SUN-RPC-WALLD	100008	Sun RPC WALL 守护程序
SUN-RPC-YPBIND	100007	Sun RPC 黄页绑定服务

范例 : Sun RPC 服务

因为 Sun RPC 服务使用动态协商端口，所以不能在安全策略中使用基于固定 TCP/UDP 端口的规则服务对象来允许它们。相反，必须使用程序号创建 sun rpc 服务对象。例如， NFS 使用两个程序号 : 100003 和 100227。相应的 TCP/UDP 端口为动态端口。为了允许使用程序号，需创建包含这两个号码的 sun-rpc-nfs 服务对象。 ALG 将程序号映射到动态协商的 TCP/UDP 端口，并根据配置的策略允许或拒绝服务。

在此范例中，将创建名为 my-sunrpc-nfs 的服务对象，以使用通过以下两个程序 ID 标识的 “Sun RPC 网络文件系统” : 100003 和 100227。

WebUI

Objects > Services > Sun RPC Services > New: 输入以下内容，然后单击 **Apply**:

Service Name: my-sunrpc-nfs

Service Timeout: (选择)

Program ID Low: 100003

Program ID High: 100003

Program ID Low: 100227

Program ID High: 100227

CLI

```
set service my-sunrpc-nfs protocol sun-rpc program 100003-100003
set service my-sunrpc-nfs + sun-rpc program 100227-100227
save
```

Microsoft 远程过程调用应用程序层网关

MS RPC 是分布式计算环境 (DCE) RPC 的 Microsoft 实现。与 Sun RPC 类似 (请参阅第 156 页上的 “Sun 远程过程调用应用程序层网关”)， MS RPC 也可以提供一种方法，使某台主机上运行的程序能够调用另一台主机上所运行程序中的过程。由于大量的 RPC 服务及广播需要， RPC 服务的传输地址将基于服务程序的 “通用唯一标识符” (UUID) 动态进行协商。将在 ScreenOS 中定义 “端点映射程序”绑定协议以将特定 UUID 映射到传输地址。

NetScreen 设备支持将 MS RPC 作为预定义服务，并可以根据配置的策略来允许和拒绝信息流。ALG 为 NetScreen 设备提供了一种功能，可用来处理 MS RPC 的动态传输地址协商机制，并可确保基于 UUID 的防火墙策略的实施。可定义防火墙策略以允许或拒绝所有 RPC 请求，或者按特定 UUID 号允许或拒绝。 ALG 还支持内向和外向请求的 “路由”和 NAT 模式。

MS RPC 服务

下表列出了预定义的 MS RPC 服务 :

名称	UUID	说明
MS-RPC-EPM	e1af8308-5d1f-11c9-91a4-08002b14a0fa	Microsoft 远程过程调用 (RPC) 端点映射程序 (EPM) 协议，它是基于 TCP/UDP 端口的服务，包括 TCP/UDP 端口 135。此表中的所有其它服务均为基于 UUID 的服务。
MS-RPC-ANY	不适用	任何 Microsoft 远程过程调用 (RPC) 服务
MS-AD-BR	ecec0d70-a603-11d0-96b1-00a0c91ece30 16e0cf3a-a604-11d0-96b1-00a0c91ece30	Microsoft Active Directory 备份和还原服务
MS-AD-DRSUAPI	e3514235-4b06-11d1-ab04-00c04fc2dcd2	Microsoft Active Directory 复制服务
MS-AD-DSROLE	1cbcad78-df0b-4934-b558-87839ea501c9	Microsoft Active Directory DSROLE 服务
MS-AD-DSSETUP	3919286a-b10c-11d0-9ba8-00c04fd92ef5	Microsoft Active Directory 安装服务
MS-DTC	906b0ce0-c70b-1067-b317-00dd010662da	Microsoft 分布式事务协调器服务
MS-EXCHANGE-DATABASE	1a190310-bb9c-11cd-90f8-00aa00466520	Microsoft Exchange 数据库服务

名称	UUID	说明
MS-EXCHANGE-DIRECTORY	f5cc5a18-4264-101a-8c59-08002b2f8426 f5cc5a7c-4264-101a-8c59-08002b2f8426 f5cc59b4-4264-101a-8c59-08002b2f8426	Microsoft Exchange Directory 服务
MS-EXCHANGE-INFO-STORE	0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde 1453c42c-0fa6-11d2-a910-00c04f990f3b 10f24e8e-0fa6-11d2-a910-00c04f990f3b 1544f5e0-613c-11d1-93df-00c04fd7bd09	Microsoft Exchange 信息存储服务
MS-EXCHANGE-MTA	9e8ee830-4459-11ce-979b-00aa005ffebe 38a94e72-a9bc-11d2-8faf-00c04fa378ff	Microsoft Exchange MTA 服务
MS-EXCHANGE-STORE	99e66040-b032-11d0-97a4-00c04fd6551d 89742ace-a9ed-11cf-9c0c-08002be7ae86 a4f1db00-ca47-1067-b31e-00dd010662da a4f1db00-ca47-1067-b31f-00dd010662da	Microsoft Exchange 存储服务
MS-EXCHANGE-SYSATD	67df7c70-0f04-11ce-b13f-00aa003bac6c f930c514-1215-11d3-99a5-00a0c9b61b04 83d72bf0-0d89-11ce-b13f-00aa003bac6c 469d6ec0-0d87-11ce-b13f-00aa003bac6c 06ed1d30-d3d3-11cd-b80e-00aa004b9c30	Microsoft Exchange 系统维护服务
MS-FRS	f5cc59b4-4264-101a-8c59-08002b2f8426 d049b186-814f-11d1-9a3c-00c04fc9b232 a00c021c-2be2-11d2-b678-0000f87a8f8e	Microsoft 文件复制服务
MS-IIS-COM	70b51430-b6ca-11d0-b9b9-00a0c922e750 a9e69612-b80d-11d0-b9b9-00a0c922e70	Microsoft 互联网信息服务器 COM GUID/UUID 服务
MS-IIS-IMAP4	2465e9e0-a873-11d0-930b-00a0c90ab17c	Microsoft 互联网信息服务器 IMAP4 服务
MS-IIS-INETINFO	82ad4280-036b-11cf-972c-00aa006887b0	Microsoft 互联网信息服务器 INETINFO 服务
MS-IIS-NNTP	4f82f460-0e21-11cf-909e-00805f48a135	Microsoft 互联网信息服务器 NNTP 服务

名称	UUID	说明
MS-IIS-POP3	1be617c0-31a5-11cf-a7d8-00805f48a135	Microsoft 互联网信息服务器 POP3 服务
MS-IIS-SMTP	8cfb5d70-31a4-11cf-a7d8-00805f48a135	Microsoft 互联网信息服务器 SMTP 服务
MS-ISMSERV	68dcd486-669e-11d1-ab0c-00c04fc2dcd2 130ceefb-e466-11d1-b78b-00c04fa32883	Microsoft 结点间通信服务
MS-MESSENGER	17fdd703-1827-4e34-79d4-24a55c53bb37 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc	Microsoft Messenger 服务
MS-MQQM	fdb3a030-065f-11d1-bb9b-00a024ea5525 76d12b80-3467-11d3-91ff-0090272f9ea3 1088a980-eae5-11d0-8d9b-00a02453c33 5b5b3580-b0e0-11d1-b92d-0060081e87f0 41208ee0-e970-11d1-9b9e-00e02c064c39	Microsoft Windows 消息队列管理服务
MS-NETLOGON	12345678-1234-abcd-ef00-01234567cffb	Microsoft Netlogon 服务
MS-SCHEDULER	1ff70682-0a51-30e8-076d-740be8cee98b 378e52b0-c0a9-11cf-822d-00aa0051e40f 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53	Microsoft Scheduler 服务
MS-WIN-DNS	50abc2a4-574d-40b3-9d66-ee4fd5fba076	Microsoft Windows DNS 服务器
MS-WINS	45f52c28-7f9f-101a-b52b-08002b2efabe 811109bf-a4e1-11d1-ab54-00a0c91e9b45	Microsoft WINS 服务

MS RPC 服务组

下表列出了预定义的 MS RPC 服务组。

名称	说明
MS-AD	Microsoft Active Directory，包括 MS-AD-BR、 MS-AD-DRSUAPI、MS-AD-DSROLE 和 MS-AD-DSSETUP
MS-EXCHANGE	Microsoft Exchange，包括 MS-EXCHANGE-DATABASE、MS-EXCHANGE-DIRECTORY、 MS-EXCHANGE-INFO-STORE、MS-EXCHANGE-MTA、 MS-EXCHANGE-STORE 和 MS-EXCHANGE-SYSATD
MS-IIS	Microsoft 互联网信息服务器，包括 MS-IIS-COM、 MS-IIS-IMAP4、MS-IIS-INETINFO、 MS-IIS-NNTP、 MS-IIS-POP3 和 MS-IIS-SMTP

范例 : MS RPC 服务

因为 MS RPC 服务使用动态协商端口，所以不能在安全策略中使用基于固定 TCP/UDP 端口的规则服务对象来允许它们。相反，必须使用 UUID 创建 MS RPC 服务对象。例如， MS Exchange 信息存储服务使用以下四个 UUID:

- 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
- 1453c42c-0fa6-11d2-a910-00c04f990f3b
- 10f24e8e-0fa6-11d2-a910-00c04f990f3b
- 1544f5e0-613c-11d1-93df-00c04fd7bd09

相应的 TCP/UDP 端口为动态端口。要允许它们，需创建一个包含这四个 UUID 的 ms-exchange-info-store 服务对象。 ALG 基于这四个 UUID 将程序号映射到动态协商的 TCP/UDP 端口，并根据配置的策略允许或拒绝服务。

在本例中，将创建一个名为 my-ex-info-store 的服务对象，其中包括 MS Exchange 信息存储服务的 UUID。

WebUI

Objects > Services > MS RPC: 输入以下内容，然后单击 **Apply**:

Service Name: my-ex-info-store

UUID: 0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde

UUID: 1453c42c-0fa6-11d2-a910-00c04f990f3b

UUID: 10f24e8e-0fa6-11d2-a910-00c04f990f3b

UUID: 1544f5e0-613c-11d1-93df-00c04fd7bd09

CLI

```
set service my-ex-info-store protocol ms-rpc uuid
    0e4a0156-dd5d-11d2-8c2f-00c04fb6bcde
set service my-ex-info-store + ms-rpc uuid 1453c42c-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid 10f24e8e-0fa6-11d2-a910-00c04f990f3b
set service my-ex-info-store + ms-rpc uuid 1544f5e0-613c-11d1-93df-00c04fd7bd09
save
```

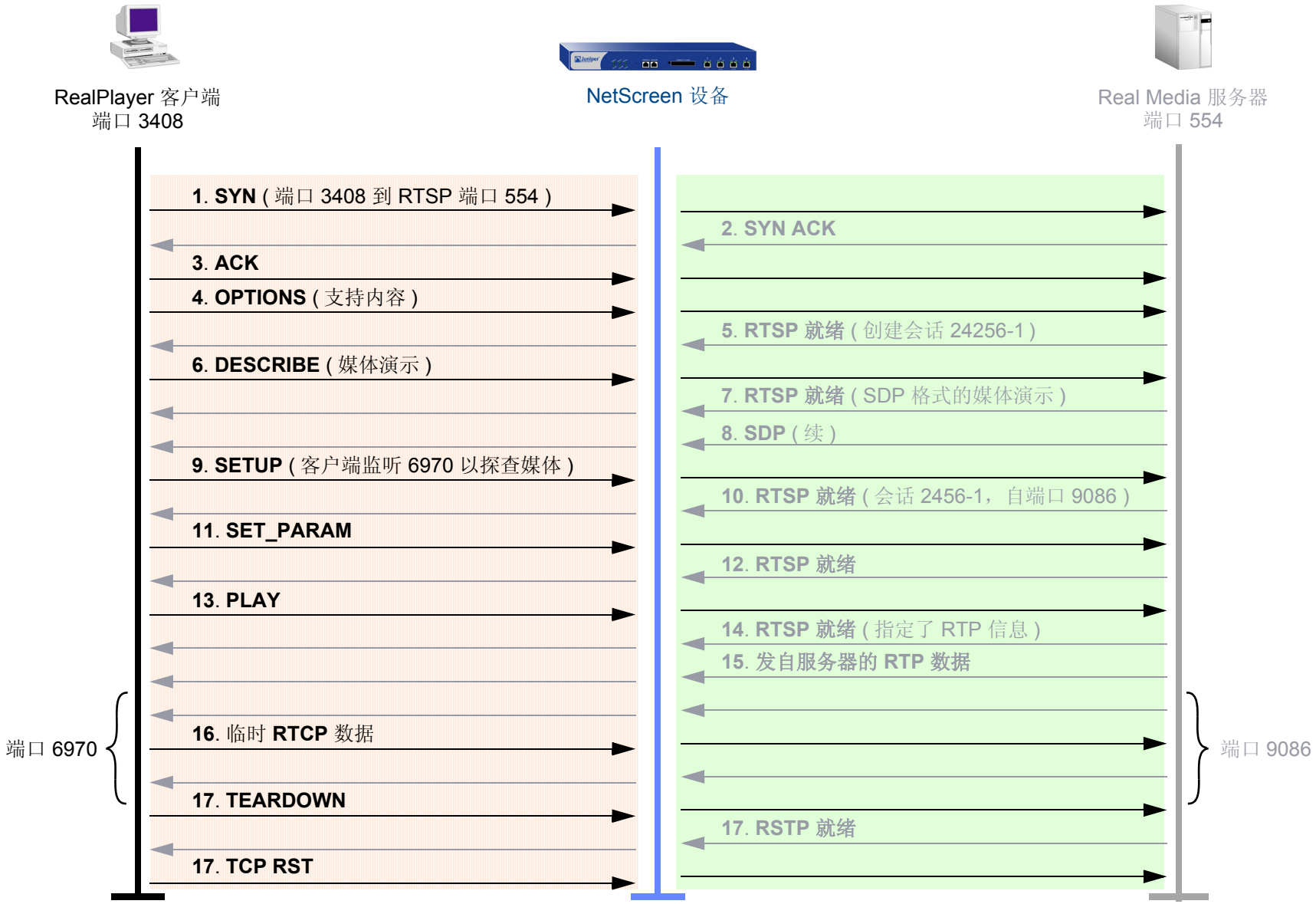
实时流协议应用程序层网关

RTSP 属应用程序层协议，用于控制一个或多个同步多媒体流 (如音频和视频) 的传输。尽管 RTSP 能够独自完成数据流的传输 (通过控制流交叉存取连续的媒体流)，但通常将其用作多媒体服务器的一种 “网络远程控制”。该协议被设计为基于 “实时协议” (RTP) 来选择传输通道 (如 UDP、组播 UDP 和 TCP) 和传输机制。 RTSP 也可使用 “会话说明协议” (SDP) (请参阅第 200 页上的 “SDP”) 作为向客户端提供信息的一种方法，它可以集中控制由来自一个或多个服务器的数据流组成的演示，也可以分别控制由来自单个服务器的多种数据流组成的演示。数据源可以是实时提供的，也可以是已存储在其中的剪辑。

NetScreen 设备支持 RTSP 作为一项服务，并可根据配置的策略允许和拒绝 RTSP 信息流。由于 RTSP 使用控制连接建立期间在数据包负载中传输的动态分配的端口号，因此会用到 ALG。 ALG 将跟踪动态分配的端口号并相应地打开针孔 (请参阅第 201 页上的 “针孔创建”)。在 NAT 模式下， ALG 将根据需要转换 IP 地址和端口。在 “路由” 模式、“透明” 模式及基于接口和基于策略的 NAT 模式下， NetScreen 设备支持 RTSP。

下面的图表说明了一个典型的 RTSP 会话。客户端启动会话 (例如，当用户在 RealPlayer 中单击 Play 按钮时) 并在端口 554 建立一个到 RTSP 服务器的 TCP 连接，然后发送消息 OPTIONS (消息也称作方法) 以确定服务器支持的音频和视频功能。服务器通过指定服务器名称和版本及会话标识符 (例如，24256-1) 响应 OPTIONS 消息。(有关方法的详细信息，请参阅第 196 页上的 “SIP 请求方法”及 RFC 2326 第 11 节。)

接下来，客户端将发送 DESCRIBE 消息，其中包含它所需要的实际媒体文件的 URL。服务器将以 SDP 格式通过媒体说明来响应 DESCRIBE 消息。然后，客户端将发送 SETUP 消息，该消息指定客户端对流媒体可接受的传输机制 (例如， RTP/RTCP 或 RDT) 以及接收媒体时使用的端口。使用 NAT 时， RTSP ALG 将跟踪这些端口并在必要时对其进行转换。服务器将响应 SETUP 方法并选择一种传输协议，通过这种方法客户端和服务器可就媒体传输机制达成一致。接下来，客户端将发送 PLAY 方法，服务器开始将媒体传输到客户端。


RealPlayer 客户端
端口 3408
NetScreen 设备
Real Media 服务器
端口 554
1. SYN (端口 3408 到 RTSP 端口 554)
2. SYN ACK
3. ACK
4. OPTIONS (支持内容)
5. RTSP 就绪 (创建会话 24256-1)
6. DESCRIBE (媒体演示)
7. RTSP 就绪 (SDP 格式的媒体演示)
8. SDP (续)
9. SETUP (客户端监听 6970 以探查媒体)
10. RTSP 就绪 (会话 2456-1，自端口 9086)
11. SET_PARAM
12. RTSP 就绪
13. PLAY
14. RTSP 就绪 (指定了 RTP 信息)
15. 发自服务器的 RTP 数据
端口 6970
16. 临时 RTCP 数据
端口 9086
17. TEARDOWN
17. RSTP 就绪
17. TCP RST

RTSP 请求方法

下表列出了可对资源 (媒体对象) 执行的方法、信息流动的方向以及是必需、推荐还是可选方法。演示是指各种信息，如网络地址、编码以及作为完整的媒体资料向客户端提供的一组或多组流内容。“流”指单个媒体实例 (如音频或视频) 以及源在会话中创建的所有数据包。

方法	方向	对象	必要性
OPTIONS	客户端到服务器	演示，流	客户端到服务器时必需
	服务器到客户端	演示，流	服务器到客户端时可选
DESCRIBE	客户端到服务器	演示，流	建议
ANNOUNCE	客户端到服务器	演示，流	可选
	服务器到客户端	演示，流	
SETUP	客户端到服务器	流	必需
GET_PARAMETER	客户端到服务器	演示，流	可选
	服务器到客户端		
SET_PARAMETER	客户端到服务器	演示，流	可选
	服务器到客户端		
PLAY	客户端到服务器	演示，流	必需
PAUSE	客户端到服务器	演示，流	建议
RECORD	客户端到服务器	演示，流	可选
REDIRECT	服务器到客户端	演示，流	可选
TEARDOWN	客户端到服务器	演示，流	必需

注意：*其它方法可在以后定义。*

方法的定义过程如下所示：

- OPTIONS — 客户端就支持的音频或视频功能以及服务器的名称、版本、会话 ID 等信息向服务器进行查询。
- DESCRIBE — 用于交换媒体初始化信息，如时钟率、颜色表及客户端需要媒体流回放的任何与传输无关的信息。通常，客户端发送它所请求的文件的 URL，然后服务器以 SDP 格式的媒体说明进行响应。(请参阅第 200 页上的 “SDP”。)
- ANNOUNCE — 客户端使用此方法张贴演示说明或媒体对象 (通过请求 URL 所标识的)。服务器使用此方法实时更新会话说明。
- SETUP — 客户端指定将使用的可接受传输机制 (如接收媒体流的端口) 及传输协议。
- GET_PARAMETER — 检索在 URL 中指定的演示或流参数的值。此方法可用于无实体主体以测试客户端或服务器的活动性。 Ping 也可用于活动性测试。
- SET_PARAMETER — 客户端使用此方法来设置由 URL 指定的演示或流参数的值。出于防火墙的原因，此方法不能用于设置传输参数。
- PLAY — 指示服务器使用在 SETUP 中指定的机制开始发送数据。直到所有 SETUP 请求均成功后，客户端才发出 PLAY 请求。服务器将按顺序将 PLAY 请求排队，并在活动的 PLAY 请求完成前延迟执行任何新 PLAY 请求。 PLAY 请求可以包括指定的范围，但也可以不包括。该范围可包含用于开始回放的时间参数 [以 “协调世界时” (UTC) 指定]，此参数也可用于同步来自不同源的流。
- PAUSE — 暂时停止传送活动演示。如果请求 URL 指定了特定的流 (例如音频)，则此方法等同于静音。如果 SETUP 在超时参数中指定 PAUSE 用于持续期间，则即使服务器可能会关闭会话，但在恢复回放或录音时仍可维护曲目同步。 PAUSE 请求将取消所有排队的 PLAY 请求。
- RECORD — 开始录制演示说明中定义的媒体范围。 UTC 时戳指示开始和结束时间，否则服务器将使用演示说明中的开始和结束时间。
- REDIRECT — 通知客户端必须连接到不同的服务器，同时包含新 URL 的位置信息及可能的范围参数。要继续检索此 URL 的媒体，客户端必须为当前会话发出 TEARDOWN 请求，为新会话发出 SETUP 请求。
- TEARDOWN — 停止给定 URL 的流传输并释放与其关联的资源。除非会话说明定义了所有传输参数，否则必须发出 SETUP 请求，然后才能再次播放该会话。

RTSP 状态代码

RTSP 使用状态代码提供有关客户端和服务器请求的信息。状态代码包括可由机器读取的三位数字结果代码及可由人工读取的简短原因。是否显示简短原因由客户端决定。状态代码分类如下：

- 提示 (100 - 199) — 已接收到请求并正在进行处理
- 成功 (200 - 299) — 已成功接收操作结果，而且能够理解并已接受
- 重新定向 (300 - 399) — 需要进一步操作以完成请求
- 客户端错误 (400 - 499) — 请求包含错误语法，无法完成
- 服务器错误 (500 - 599) — 服务器未能完成显然有效的请求

下表列出了为 RTSP 1.0 定义的所有状态代码及提示的简短原因。可修改或重新定义简短原因，这不会影响协议的实施。

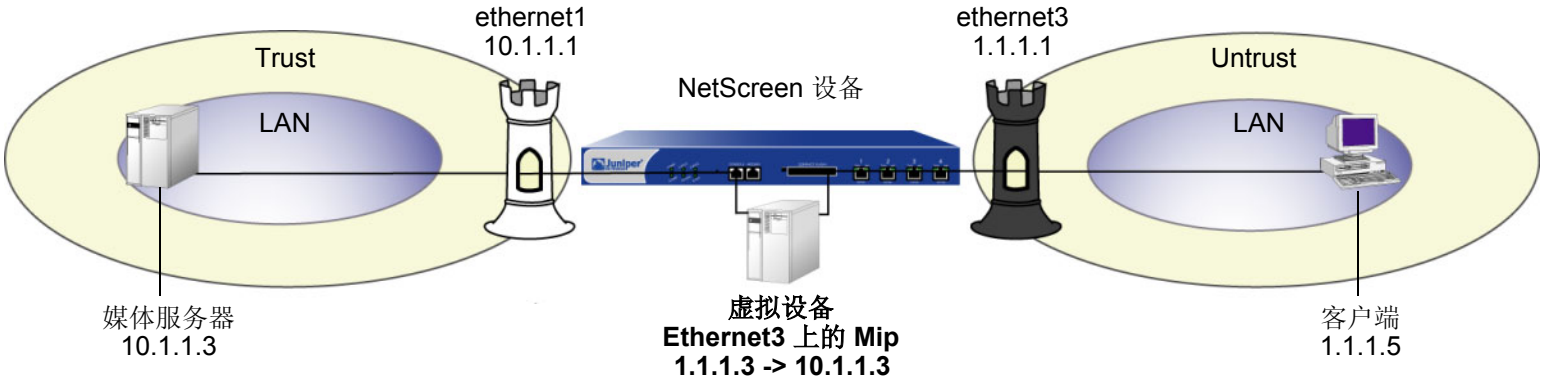
状态代码	简短原因	状态代码	简短原因
100	继续	414	请求 URL 过多
200	OK	415	不支持的媒体类型
201	已创建	451	不支持的媒体类型
250	存储空间不足	452	未找到会议
300	有多重选择	453	带宽不足
301	永久移除	454	未找到会话
303	参见其它	455	此状态下方法无效
304	未进行修改	456	资源的包头字段无效
305	使用代理	457	范围无效
400	错误的请求	458	参数为只读
401	未经授权	459	不允许集中操作
402	需要付款	460	仅允许集中操作
403	禁止	461	不支持的传输

状态代码	简短原因	状态代码	简短原因
404	未找到	462	目标无法到达
405	不允许的方法	500	内部服务器错误
406	不可接受	501	未执行
407	需要代理认证	502	网关错误
408	请求超时	503	服务不可用
410	遗失	504	网关超时
411	需要长度	505	不支持的 RTSP 版本
412	预处理失败	551	不支持的选项
413	请求实体过多		

注意：*有关状态代码的完整定义，请参阅 RFC 2326, “Real Time Streaming Protocol (RTSP)”。*

范例：专用域中的媒体服务器

在本例中，媒体服务器位于 Trust 区段中，客户端位于 Untrust 区段中。在 Trust 区段中，在连接到媒体服务器的 ethernet3 接口上配置 MIP，然后创建一个策略以允许 RTSP 信息流从 Untrust 区段中的客户端流动到 Trust 区段中的媒体服务器。



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

Manage IP: 10.1.1.2

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

2. 地址

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

Address Name: media_server

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: client

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.5/24

Zone: Untrust

3. MIP

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

Mapped IP: 1.1.1.3

Host IP Address: 10.1.1.5

4. 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), client

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.3)

Service: RTSP

Action: Permit

CLI

1. 接口

```
set interface ethernet1 trust
set interface ethernet1 ip 10.1.1.1

set interface ethernet3 untrust
set interface ethernet3 ip 1.1.1.1
```

2. 地址

```
set address trust media_server 10.1.1.3/24
set address untrust client 1.1.1.5
```

3. MIP

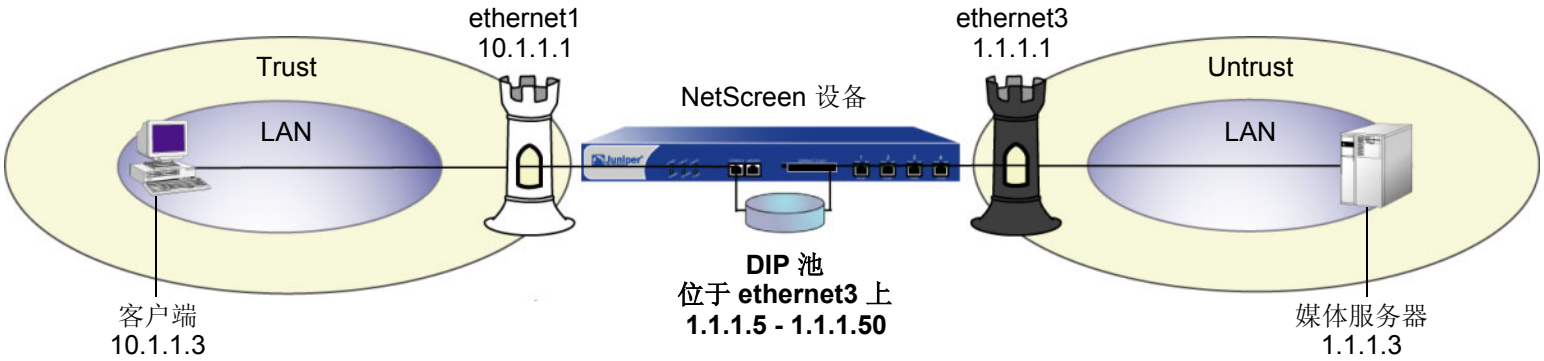
```
set interface ethernet3 mip (1.1.1.3) host 10.1.1.3
```

4. 策略

```
set policy from untrust to trust client mip(1.1.1.3) rtsp permit
save
```

范例：公共域中的媒体服务器

在本例中，媒体服务器位于 Untrust 区段中，客户端位于 Trust 区段中。媒体服务器从 Untrust 区段对客户端做出响应时，在 ethernet3 端口上配置 DIP 池以执行 NAT，然后创建一个策略以允许 RTSP 信息流从 Trust 区段流动到 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

Manage IP: 10.1.1.2

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

2. 地址

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

Address Name: client

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: media_server

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.3/24

Zone: Untrust

3. DIP 池

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

ID: 5

IP Address Range: (选择) 1.1.1.5 ~ 1.1.1.50

Port Translation: (选择)

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): client

Destination Address:

Address Book Entry (选择): media_server

Service: RTSP

Action: Permit

> Advanced: 输入以下内容，然后单击 **OK**:
NAT:
Source Translation: (选择)
(DIP on): 5 (1.1.1.5-1.1.1.50)/port-xlate

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1

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

2. 地址

```
set address trust client ip 10.1.1.3/24
set address untrust media_server ip 1.1.1.3/24
```

3. DIP 池

```
set interface ethernet3 dip 5 1.1.5 1.1.1.50
```

4. 策略

```
set policy from trust to untrust client media_server rtsp nat dip 5 permit
save
```

IP 语音通信的 H.323 协议

利用 H.323 协议可保证终端主机 (如 IP 电话和多媒体设备) 间的 IP 语音通信 (VoIP) 安全。在此类电话系统中，关守设备管理呼叫注册、许可和 VoIP 呼叫的呼叫状态。关守设备可驻留在两个不同的区段，或驻留在同一区段中。

注意：*下面将以 IP 电话为例进行说明，但也可以对使用 VoIP 协议的其它主机进行配置，如 NetMeeting© 多媒体设备。*

范例 : Trust 区段中的关守设备 (透明或路由模式)

在下面的范例中将设置两个策略，它们允许 H.323 信息流在 Trust 区段中的 IP 电话主机和关守设备以及在 Untrust 区段中的 IP 电话主机 (2.2.2.5) 间通过。在本例中，NetScreen 设备可处于透明模式或路由模式。Trust 和 Untrust 安全区段都在 trust-vr 路由选择域中。

WebUI

1. 地址

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

   Address Name: IP_Phone

   IP Address/Domain Name:

   IP/Netmask: (选择), 2.2.2.5/32

   Zone: Untrust

2. 策略

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

   Source Address:

   Address Book Entry: (选择), Any

   Destination Address:

   Address Book Entry: (选择), IP_Phone

   Service: H.323

   Action: Permit

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

   Source Address:

   Address Book Entry: (选择), IP_Phone

   Destination Address:

   Address Book Entry: (选择), Any

   Service: H.323

   Action: Permit

CLI

1. 地址

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

2. 策略

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

范例 : Untrust 区段中的关守设备 (透明或路由模式)

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

在下面的范例中将设置两个策略，它们允许 H.323 信息流在 Trust 区段中的 IP 电话主机与 Untrust 区段中 IP 地址为 2.2.2.5 的 IP 电话 (及关守设备) 间通过。设备可以处于透明或路由模式。 Trust 和 Untrust 安全区段都在 trust-vr 路由选择域中。

WebUI

1. 地址

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

Address Name: IP_Phone

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.10/32

Zone: Untrust

2. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), IP_Phone

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone

Destination Address:

Address Book Entry: (选择), Any

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Gatekeeper

Service: H.323

Action: Permit

CLI

1. 地址

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

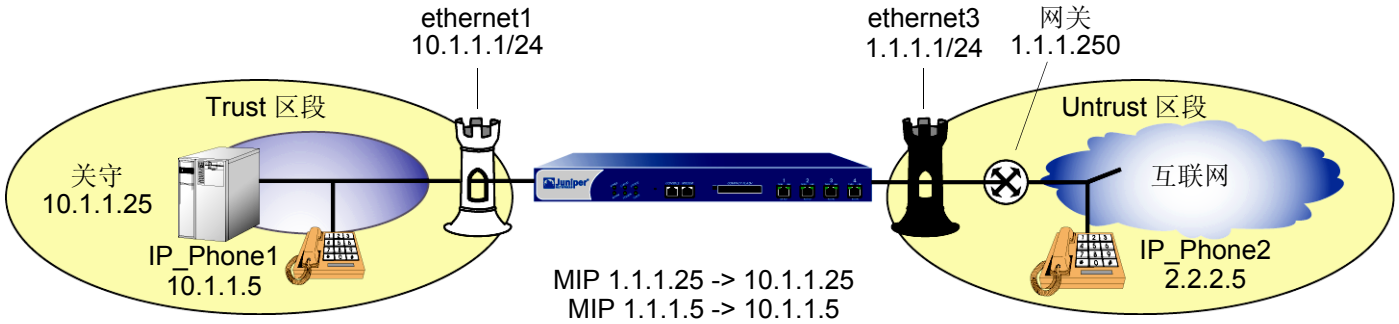
2. 策略

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

范例：使用 NAT 的外向呼叫

NetScreen 设备使用 NAT (网络地址转换) 时， Trust 区段中的关守设备或端点设备将拥有私有地址，如果该设备位于 Untrust 区段中则有公共地址。在 NAT 模式下设置 NetScreen 设备时，必须将公共 IP 地址映射到需要通过私有地址接收内向信息流的每个设备。

在本例中， Trust 区段中的设备包括端点主机 (10.1.1.5) 和关守设备 (10.1.1.25)。 IP_Phone2 (2.2.2.5) 在 Untrust 区段中。配置 NetScreen 设备以允许信息流在端点主机 IP_Phone1 和 Trust 区段中的关守设备以及 Untrust 区段中的端点主机 IP_Phone2 间通过。 Trust 和 Untrust 安全区段都在 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: IP_Phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.25/32

Zone: Trust

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

Address Name: IP_Phone2

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 映射 IP 地址

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

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

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

Mapped IP: 1.1.1.25

Netmask: 255.255.255.255

Host IP Address: 10.1.1.25

Host Virtual Router Name: trust-vr

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

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

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), IP_Phone2

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), Gatekeeper

Destination Address:

Address Book Entry: (选择), IP_Phone2

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

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

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

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

Service: H.323

Action: Permit

CLI

1. 接口

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

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

2. 地址

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

3. 映射 IP 地址

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

4. 路由

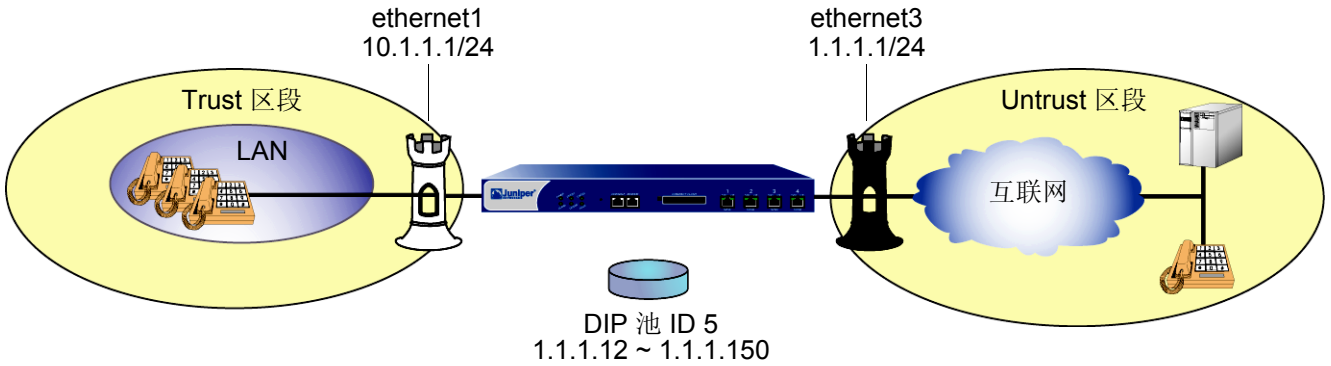
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

5. 策略

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

范例 : 使用 NAT 的内向呼叫

在本例中，将配置 NetScreen 设备以在 NAT 边界接受内向呼叫。为此，可创建 DIP 地址池以动态分配目标地址。这与大多数配置均不相同，其中的 DIP 池仅提供源地址。



用户定义 DIP 的 DIP 池的名称可以是 DIP(*id_num*)，或者如果 DIP 池使用与接口 IP 地址相同的地址时，则名称为 DIP(*接口*)。可将此类地址条目作为策略中的目标地址，与服务 H.323、SIP 或其它 VoIP (语音 IP) 协议一起支持内向呼叫。

下例使用 H.323 VoIP 配置中的 DIP。关键字 “incoming” (内向) 指示设备将 DIP 和接口地址添加到 global 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

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 内向 NAT 的 DIP

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

ID: 5

IP Address Range: (选择), 1.1.1.12 ~ 1.1.1.150

Port Translation: (选择)

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

Incoming NAT: (选择)

3. 地址

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

Address Name: IP_Phones1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/24

Zone: Trust

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

Address Name: IP_Phone2

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

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), IP_Phones1

Destination Address:

Address Book Entry: (选择), Any

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

Address Book Entry: (选择), DIP(5)

Service: H.323

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 内向 NAT 的 DIP

```
set interface ethernet3 dip 5 1.1.1.12 1.1.1.150 incoming
```

3. 地址

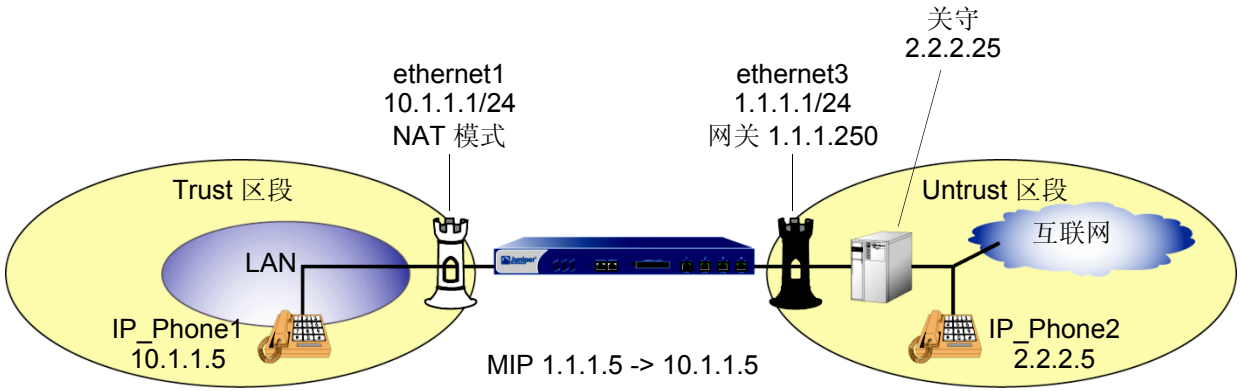
```
set address trust IP_Phones1 10.1.1.5/24
set address untrust IP_Phone2 2.2.2.5/32
```

4. 策略

```
set policy from trust to untrust IP_Phones1 any h.323 nat src dip 5 permit
set policy from untrust to trust IP_Phone2 dip(5) h.323 permit
save
```

范例 : Untrust 区段中的关守设备 (采用 NAT)

本例中，关守设备 (2.2.2.25) 和主机 IP_Phone2 (2.2.2.5) 都在 Untrust 区段中，而主机 IP_Phone1 (10.1.1.5) 在 Trust 区段中。配置 NetScreen 设备以允许信息流在 Trust 区段中的主机 IP_Phone1 和 Untrust 区段中的主机 IP_Phone2 (及关守设备) 间通过。 Trust 和 Untrust 安全区段都在 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**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: IP_Phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

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

Address Name: Gatekeeper

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.25/32

Zone: Untrust

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

Address Name: IP_Phone2

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 映射 IP 地址

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

Mapped IP: 1.1.1.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

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

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), IP_Phone2

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone1

Destination Address:

Address Book Entry: (选择), Gatekeeper

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), IP_Phone2

Destination Address:

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

Service: H.323

Action: Permit

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

Source Address:

Address Book Entry: (选择), Gatekeeper

Destination Address:

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

Service: H.323

Action: Permit

CLI

1. 接口

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

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

2. 地址

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

3. 映射 IP 地址

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

4. 路由

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

5. 策略

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

会话启动协议 (SIP)

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

NetScreen 设备支持将 SIP 作为服务并可以筛选 SIP 信息流，根据所配置的策略允许或拒绝信息流。 SIP 是 ScreenOS 中的预定义服务，使用端口 5060 作为目标端口。

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

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

SDP 提供系统可以使用的信息，以便与多媒体会话结合。 SDP 可包括如 IP 地址、端口号、时间和日期等信息。请注意， SDP 报头中的 IP 地址和端口号 (分别为 “c=” 和 “m=” 字段) 是客户端希望接收媒体流的地址和端口，而不是发出 SIP 请求的 IP 地址和端口号 (尽管它们可能是相同的)。有关详细信息，请参阅第 200 页上的 “SDP”。

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

SIP 请求方法

SIP 事务模型包括一些请求和响应消息，其中每条消息都包含一个指示消息目的的*方法*字段。 ScreenOS 支持以下方法类型和响应代码 :

- INVITE — 用户发送 INVITE 请求，邀请其他用户参与会话。 INVITE 请求的主体可能包含会话说明。在 NAT 模式下，将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- ACK — 发出 INVITE 的用户发送 ACK 请求，以确认是否接收到对 INVITE 的最终响应。如果初始 INVITE 请求不包含会话说明，则 ACK 请求中必须包括它。在 NAT 模式下，将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- OPTIONS — “用户代理” (UA) 将使用它来获取有关 SIP 代理功能的信息。服务器将以有关方法、会话说明协议及其支持的消息编码等信息响应。在 NAT 模式下，将 OPTIONS 请求从 NAT 外的 UA 发送到 NAT 内的代理时，SIP ALG 会将 Request-URL 中的地址及 To: 字段中的 IP 地址转换为内部客户端相应的 IP 地址。UA 位于 NAT 内而代理位于 NAT 之外时， SIP ALG 将如第 210 页上的 “SIP 包头”表中所示转换 From:、Via: 和 Call-ID: 字段。
- BYE — 用户发送 BYE 请求以放弃会话。来自任一用户的 BYE 请求都将自动终止会话。在 NAT 模式下，将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- CANCEL — 用户可以发送 CANCEL 请求，以取消等待中的 INVITE 请求。如果处理 INVITE 的 SIP 服务器在接收到 CANCEL 之前已经发出了 INVITE 请求的最终响应，则 CANCEL 请求不起作用。在 NAT 模式下，将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- REGISTER — 用户向 SIP *registrar* 服务器发送 REGISTER 请求，将用户的当前位置告知服务器。 SIP registrar 服务器将记录在 REGISTER 请求中接收到的所有信息，并允许试图查找用户的任何 SIP 服务器使用此信息。在 NAT 模式中， REGISTER 请求的处理方式为 :
  - 从外部客户端到内部 Registrar 的 REGISTER 请求 - 接收到内向 REGISTER 请求时，SIP ALG 将转换 Request-URL 中的 IP 地址 (如果存在)。仅允许内向 REGISTER 消息到达 MIP 或 VIP 地址。无需对外向响应进行转换。

  - 从内部客户端到外部 Registrar 的 REGISTER 请求 - 接收到外向 REGISTER 请求时，SIP ALG 将转换 To:, From:, Via:, Call-ID: 和 Contact: 包头字段中的 IP 地址。对内向响应将执行反向转换。

- Info — 用于沿呼叫的信号发送路径传送中间会话信号发送信息。在 NAT 模式下，将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- Subscribe — 用于从远程节点请求当前状态和状态更新。在 NAT 模式下，如果消息从外部网络进入内部网络，则 Request-URL 中的地址将改为私有 IP 地址。将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- Notify — 发送此消息以正式通知预订者对其预订进行的更改。在 NAT 模式下，如果消息从外部网络进入内部网络，则 Request-URL: 包头字段中的 IP 地址将改为私有 IP 地址。将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。
- Refer — 通过在请求中提供的联系信息将接受方 (通过 Request-URL 确定) 指定为第三方。在 NAT 模式下，如果消息从外部网络进入内部网络，则 Request-URL 中的地址将改为私有 IP 地址。将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段中的 IP 地址进行修改。

  例如，如果专用网络中的用户 A 将公用网络中的用户 B 指定为同样位于专用网络中的用户 C，则 SIP ALG 将为用户 C 分配新的 IP 地址和端口号，以便用户 B 可以联系用户 C。但是，如果用户 C 通过 Registrar 进行注册，其端口映射将存储在 ALG NAT 表中并将被重用以执行转换。
- Update — 用于打开新的或已更新 SDP 信息的针孔。将如第 210 页上的 “SIP 包头”中所示对 Via:, From:, To:, Call-ID:, Contact:, Route: 和 Record-Route: 包头字段进行修改。
- 1*xx*、202、2*xx*、3*xx*、4*xx*、5*xx*、6*xx* 响应代码 — 用于指示事务的状态。包头字段的修改如第 210 页上的 “SIP 包头”中的表所示。

SIP 响应的类别

响应代码指示 SIP 事务的状态，由分组为下列类别的代码组成：

- 提示 (100 - 199) — 已接收到请求，继续对请求进行处理
- 成功 (200 - 299) — 已成功接收操作结果，而且能够理解并已接受
- 重新定向 (300 - 399) — 需要进一步操作以完成请求
- 客户端错误 (400 - 499) — 请求包含错误语法，或无法在此服务器上完成
- 服务器错误 (500 - 599) — 服务器未能完成显然有效的请求
- 全局错误 (600 - 699) — 在任何服务器上都无法完成请求

以下是当前 SIP 响应代码的完整列表。 NetScreen 对其均能够支持。

1xx	100 正在尝试	180 正在呼叫	181 呼叫正在转移
	182 已排队	183 会话进程	
2xx	200 OK	202 已接受	
3xx	300 有多重选择	301 永久移除	302 临时移除
	305 使用代理	380 可选服务	
4xx	400 错误的请求	401 未经授权	402 需要付款
	403 禁止	404 未找到	405 不允许的方法
	406 不可接受	407 需要代理认证	408 请求超时
	409 冲突	410 遗失	411 需要长度
	413 请求实体过多	414 请求的 URL 过多	415 不支持的媒体类型
	420 扩展名错误	480 暂时不可用	481 呼叫路线 / 事务不存在
	482 检测到回路	483 跳跃太多	484 地址不完整
	485 不明确	486 此处正忙	487 取消请求
	488 此处不可接受		

5xx	500 服务器内部错误	501 未执行	502 网关错误
	502 服务不可用	504 网关超时	505 不支持的 SIP 版本
6xx	600 全域忙碌中	603 谢绝	604 全域均不存在
	606 不可接受		

ALG – 应用程序层网关

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

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

SIP ALG 监控 SIP 事务，根据从这些事务中提取的信息动态创建并管理针孔。 NetScreen SIP ALG 支持所有 SIP 方法和响应 (请参阅第 196 页上的 “SIP 请求方法”和第 198 页上的 “SIP 响应的类别”)。通过创建允许 SIP 服务的静态策略，可以允许 SIP 事务通过 NetScreen 防火墙。此策略允许 NetScreen 设备截取 SIP 信息流，并执行下列操作之一 : 允许或拒绝信息流，或允许 SIP ALG 打开针孔以便通过媒体流。SIP ALG 只需要为包含媒体信息 (SDP) 的 SIP 请求和响应打开针孔。对于不包含 SDP 的 SIP 消息， NetScreen 设备就会让它们通过。

SIP ALG 截取包含 SDP 的 SIP 消息，并使用剖析器提取创建针孔所需的信息。 SIP ALG 检查数据包的 SDP 部分，而剖析器会提取 SIP ALG 在针孔表中记录的信息，如 IP 地址和端口号。 SIP ALG 使用针孔表中记录的 IP 地址和端口号来打开针孔并允许媒体流通过 NetScreen 设备。

注意 : *NetScreen 设备不支持加密的 SDP。如果 NetScreen 设备接收到其中 SDP 加密的 SIP 消息，SIP ALG 将允许该消息通过防火墙，但会生成日志消息通知用户无法处理该数据包。如果 SDP 加密，则 SIP ALG 无法从 SDP 提取打开针孔所需的信息。从而使 SDP 描述的媒体内容不能通过 NetScreen 设备。*

6. 我们将针孔称为端口的有限开口，它允许唯一信息流通过。

SDP

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

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

- **c=** 表示连接信息

  此字段可能出现在会话级或媒体级。其显示格式为：

  c=< 网络类型 >< 地址类型 >< 连接地址 >

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

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

- **m=** 表示媒体声明

  此字段出现在媒体级，并且包含媒体说明。其显示格式为：

  m=< 媒体 >< 端口 >< 传输 >< fmt 列表 >

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

  在 ScreenOS 的这一版本中，NetScreen 设备仅为 RTP 和 RTCP 打开端口。每个 RTP 会话都有一个相应的 RTCP[9] (实时传输控制协议) 会话。因此，每当媒体流使用 RTP 时， SIP ALG 必须为 RTP 和 RTCP 信息流保留端口 (创建针孔)。缺省情况下， RTCP 的端口号比 RTP 的端口号大一。

7. 在 SDP 会话说明中，媒体级信息以 m= 字段开始。
8. 通常，目标 IP 地址也可以是组播的 IP 地址，但 NetScreen 当前并不支持带有 SIP 的组播。
9. RTCP 提供媒体同步和有关会话成员及通信质量的信息。

针孔创建

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

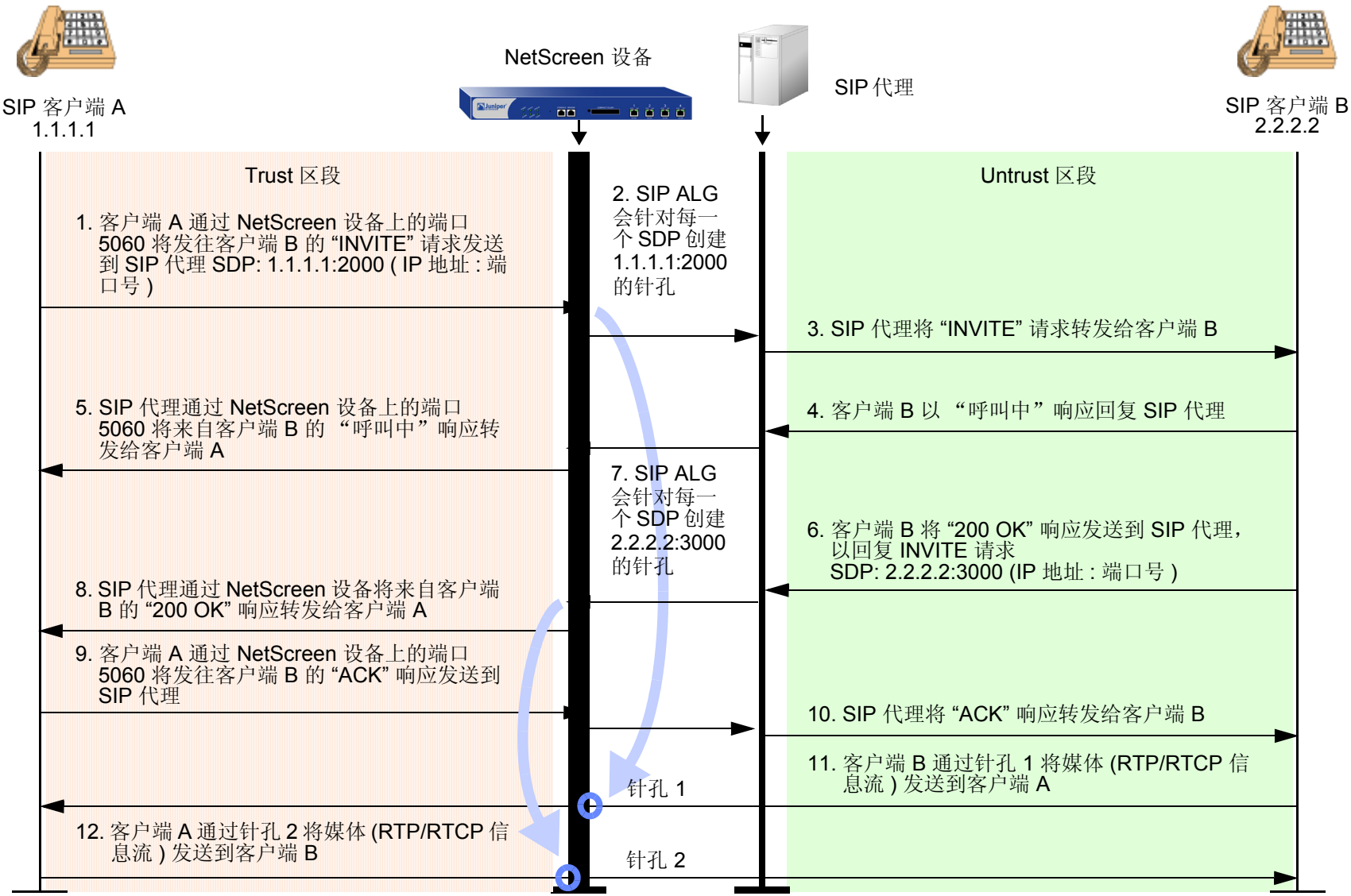
- 首先， SIP ALG 剖析器验证媒体级中是否有包含 IP 地址的 c= 字段。如果有，剖析器将提取该 IP 地址，然后 SIP ALG 使用该地址为媒体创建针孔。
- 如果媒体级中没有 c= 字段， SIP ALG 剖析器将从会话级的 c= 字段中提取 IP 地址，然后 SIP ALG 使用该地址为媒体创建针孔。如果会话说明的两个级中均不包含 c= 字段，表明协议栈中存在错误，NetScreen 设备将丢弃该数据包并记录事件。

以下列出了 SIP ALG 创建针孔所需的信息。此信息来源于 NetScreen 设备上的 SDP 会话说明和参数 :

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

  数据包在生存期内通过针孔后， SIP ALG 会立即移除数据包来源方向的针孔。

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


SIP 客户端 A
1.1.1.1
NetScreen 设备
SIP 代理
SIP 客户端 B
2.2.2.2
Trust 区段
Untrust 区段
1. 客户端 A 通过 NetScreen 设备上的端口 5060 将发往客户端 B 的 “INVITE” 请求发送到 SIP 代理 SDP: 1.1.1.1:2000 (IP 地址 : 端口号)
2. SIP ALG 会针对每一个 SDP 创建 1.1.1.1:2000 的针孔
3. SIP 代理将 “INVITE” 请求转发给客户端 B
4. 客户端 B 以 “呼叫中” 响应回复 SIP 代理
5. SIP 代理通过 NetScreen 设备上的端口 5060 将来自客户端 B 的 “呼叫中” 响应转发给客户端 A
6. 客户端 B 将 “200 OK” 响应发送到 SIP 代理，以回复 INVITE 请求
SDP: 2.2.2.2:3000 (IP 地址 : 端口号)
7. SIP ALG 会针对每一个 SDP 创建 2.2.2.2:3000 的针孔
8. SIP 代理通过 NetScreen 设备将来自客户端 B 的 “200 OK” 响应转发给客户端 A
9. 客户端 A 通过 NetScreen 设备上的端口 5060 将发往客户端 B 的 “ACK” 响应发送到 SIP 代理
10. SIP 代理将 “ACK” 响应转发给客户端 B
11. 客户端 B 通过针孔 1 将媒体 (RTP/RTCP 信息流) 发送到客户端 A
针孔 1
12. 客户端 A 通过针孔 2 将媒体 (RTP/RTCP 信息流) 发送到客户端 B
针孔 2

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

会话静止超时

通常，如果一方客户端发送 BYE 或 CANCEL 请求，呼叫随即终止。 SIP ALG 会截取 BYE 或 CANCEL 请求，并移除该呼叫的所有媒体会话。一些特殊原因或问题 (如电源故障) 可能会阻止呼叫中的客户端发送 BYE 或 CANCEL 请求。在这种情况下，呼叫可能会一直进行下去，并消耗 NetScreen 设备上的资源。静止超时功能有助于 NetScreen 设备监控呼叫的活动状况，如果在某特定时期内没有活动即终止呼叫。

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

有两种静止超时类型可决定组的生存期：

- 信号发送静止超时：此参数指出呼叫不进行任何 SIP 信号信息流发送而能够维持活动的最大时间长度 (以秒为单位)。每次呼叫中进行 SIP 信号消息发送时，都会重设超时。缺省设置为 43200 秒 (12 小时)。
- 媒体静止超时：此参数指出组中不进行任何媒体 (RTP 或 RTCP) 信息流传送而呼叫能够维持活动的最大时间长度 (以秒为单位)。每次呼叫中出现 RTP 或 RTCP 数据包时，都会重设超时。缺省值为 120 秒。

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

SIP 攻击保护

SIP 代理服务器处理呼叫的能力可能会受到开始时被拒绝的重复 SIP INVITE 请求的影响 (无论是恶意请求，还是由于客户端或服务器错误)。为防止 SIP 代理服务器受到此类请求的影响，可使用 **sip protect deny** 命令配置 NetScreen 设备以监控 INVITE 请求及代理服务器对其的回复。如果回复中包含 3*xx*、 4*xx* 或 5*xx* 响应代码 (请参阅第 198 页上的 “SIP 响应的类别”)，则 ALG 会将请求的源 IP 地址和代理服务器的 IP 地址存储在一个表中。接下来， NetScreen 设备将根据此表按可配置的秒数 (缺省为 3 秒) 核实所有 INVITE 请求，然后丢弃与表中条目匹配的所有数据包。也可通过指定目标 IP 地址对 NetScreen 设备进行配置以监控对特定代理服务器的 INVITE 请求。 SIP 攻击保护是全局配置的。

范例 : SIP 保护拒绝

在本例中，将对 NetScreen 设备进行配置以防止单个 SIP 代理服务器 (1.1.1.3/24) 受到已拒绝对其提供服务的重复 INVITE 请求的影响。所有数据包在接下来的 5 秒内都将被丢弃，然后 NetScreen 设备再恢复转发来自这些源的 INVITE 请求。

WebUI

> ***注意 :*** *必须使用 CLI 来防止 SIP 代理服务器被 INVITE 请求塞满。*

CLI

```
set sip protect deny dst-ip 1.1.1.3/24
set sip protect deny timeout 5
save
```

范例：信号发送与媒体静止超时

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

WebUI

***注意：**必须使用 CLI 来设置 SIP 信号发送和媒体静止超时。*

CLI

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

范例：UDP 泛滥保护

可利用区段和目标地址来防止 NetScreen 设备出现 UDP 泛滥。对本例而言，将在 Untrust 区段中设置一个 80000/ 秒的阈值，此值即为在 NetScreen 设备生成警报并丢弃随后的数据包之前 (丢弃的持续时间为该秒的剩余时间)，可在 IP 地址 1.1.1.5 上接收的 UDP 数据包数。

***注意：**本例使用的是常规 ScreenOS 命令，无需使用专门针对 SIP 的命令。有关 UDP 泛滥保护及如何确定有效设置的详细信息，请参阅第 **4**-65 页上的 “UDP 泛滥”。*

WebUI

Screening > Screen: 输入以下内容，然后单击 **Apply**:

Zone: Untrust

UDP Flood Protection (选择)

>Destination IP: 输入以下信息，然后单击 Web 浏览器上的后退箭头返回 Screen 配置页：

Destination IP: 1.1.1.5

Threshold: 80000

Add: (选择)

CLI

```
set zone untrust screen udp-flood dst-ip 1.1.1.5 threshold 80000
save
```

范例：SIP 最大连接数

在本例中，通过将来自单个 IP 地址的并发会话最大值设置为 20 来防止 SIP 网络受到 Untrust 区段攻击者的泛滥攻击。如果 NetScreen 设备检测到来自同一 IP 地址的 20 个以上的连接尝试，将开始丢弃随后的尝试直到会话数降至指定的最大值以下。

注意：*本例使用的是常规 ScreenOS 命令，无需使用专门针对 SIP 的命令。有关基于源的会话限制及如何确定有效设置的详细信息，请参阅第* ***4****-40 页上的 “基于源和目标的会话限制”。*

WebUI

Screening > Screen (Zone: Untrust): 输入以下内容，然后单击 **OK**:

Source IP Based Session Limit: (选择)

Threshold: 20 Sessions

CLI

```
set zone untrust screen limit-session source-ip-based 20
save
```

使用网络地址转换的 SIP

网络地址转换 (NAT) 协议可使专用子网中的多个主机共享一个公用 IP 地址来访问互联网。对于外向信息流，NAT 将使用公用 IP 地址来替换专用子网中的主机的私有 IP 地址。对于内向信息流，公用 IP 地址将被转换回私有地址并且消息将被路由到专用子网中的相应主机。

对 SIP 服务使用 NAT 较为复杂，因为 SIP 消息在 SIP 包头及 SIP 正文中均包含 IP 地址。 SIP 包头中包含有关呼叫方和接收方的信息， NetScreen 设备将会对此信息进行转换以使其对外部网络不可见。 SIP 正文包含 “会话说明协议” (SDP) 信息，其中包括用于媒体传输的 IP 地址和端口号。NetScreen 设备将转换 SDP 信息以分配资源来发送和接收媒体。

SIP 消息中的 IP 地址和端口号的替换方法取决于消息传送方向。对于外向消息，客户端的私有 IP 地址和端口号将替换为 NetScreen 防火墙的公用 IP 地址和端口号。对于内向消息，防火墙的公共地址将替换为客户端的私有地址。

穿过防火墙发送 INVITE 消息时， SIP ALG 会将信息从消息包头收集到呼叫表中 (该表用于将后继消息转发到正确的端点)。接收到新消息 (例如，ACK 或 200 OK) 时，ALG 会将 From:、To: 和 Call-ID: 字段与呼叫表加以比较以确定消息的呼叫内容。如果接收到与现有呼叫匹配的新 INVITE 消息， ALG 会将其作为 REINVITE 进行处理。

接收到包含 SDP 信息的消息时， ALG 将分配端口并在这些端口与 SDP 中的端口间创建 NAT 映射。由于 SDP 对 “实时协议” (RTP) 和 “实时控制协议” (RTCP) 通道需要用到有序端口，所以 ALG 将提供连续的奇偶端口。如果找不到成对端口，它将丢弃 SIP 消息。

外向呼叫

当 SIP 呼叫由 SIP 请求消息从内部到外部网络发起时，NAT 将替换 SDP 中的 IP 地址和端口号，并创建一个绑定将 IP 地址和端口号映射到 NetScreen 防火墙。如果显示 Via:、 Contact:、 Route: 和 Record-Route: SIP 包头字段，则它们也将被绑定到防火墙 IP 地址。 ALG 将存储这些映射以用于重新传输和 SIP 响应消息中。

然后，SIP ALG 将在防火墙中打开针孔以允许媒体在动态分配的端口上通过 NetScreen 设备，这些端口是基于 SDP 及 Via:、Contact: 和 Record-Route: 包头字段中的信息进行协商的。这些针孔还允许内向数据包到达 Contact:、Via: 和 Record-Route: IP 地址和端口。处理返回信息流时， ALG 会将原来的 Contact:、 Via:、 Route: 和 Record-Route: SIP 字段插回数据包。

内向呼叫

内向呼叫从公用网络发起并到达公用映射 IP (MIP) 地址，或到达 NetScreen 设备的接口 IP 地址。MIP 是静态配置的指向内部主机的 IP 地址，当 ALG 监控由内部主机发送到 SIP Registrar 的 REGISTER 消息时，将会动态记录接口 IP 地址。 (有关详细信息，请参阅第 216 页上的 “使用 SIP Registrar 的内向 SIP 呼叫支持”。) 接收到内向 SIP 数据包时， NetScreen 设备会建立会话并将数据包负载转发到 SIP ALG。

ALG 将检查 SIP 请求消息 (最初为 INVITE)，然后基于 SDP 中的信息为外向媒体打开入口。接收到 200 OK 响应消息时， SIP ALG 对 IP 地址和端口执行 NAT 并在出站方向打开针孔。(打开的入口有短暂的活动时间，如果未很快接收到 200 OK 响应消息则会超时。)

接收到 200 OK 响应后， SIP 代理将检查 SDP 信息并读取每个媒体会话的 IP 地址和端口号。 NetScreen 设备上的 SIP ALG 将对地址和端口号执行 NAT、为出站信息流打开针孔并刷新入站方向入口的超时值。

当接收到 200 OK 的 ACK 后，ACK 也将通过 SIP ALG。如果消息包含 SDP 信息，SIP ALG 将确保 IP 地址和端口号不是从先前的 INVITE 更改的地址和端口号 — 如果是，ALG 将删除原有针孔并创建新的针孔以允许媒体通过。ALG 还将监控 Via:、 Contact: 和 Record-Route: SIP 字段并在确定这些字段已发生更改后打开新的针孔。

已转移呼叫

举例来说，已转移呼叫是指网络外部的用户 A 呼叫网络内部的用户 B，而用户 B 又将呼叫转移到网络外部的用户 C。SIP ALG 将来自用户 A 的 INVITE 作为一般的内向呼叫进行处理。如果 ALG 在检查从 B 到网络外部的 C 的已转移呼叫时发现 B 和 C 使用相同的接口，则将不会在防火墙中打开针孔，因为媒体将在用户 A 和用户 C 间直接流动。

呼叫终止

BYE 消息用来终止呼叫。 NetScreen 设备接收到 BYE 消息后，会象处理任何其它消息一样对包头字段进行转换。但由于接收方必须通过 200 OK 消息确认 BYE 消息，所以 ALG 将延迟 5 秒钟再终止呼叫以留出传输 200 OK 的时间。

呼叫 Re-INVITE 消息

Re-INVITE 消息用于将新媒体会话添加到呼叫以及删除现有的媒体会话。新媒体会话添加到某一呼叫后，将在防火墙中打开新针孔并创建新的地址绑定。该过程与初始呼叫设置相同。从呼叫中删除一个或多个媒体会话时，会象接收到 BYE 消息一样关闭针孔并解除绑定。

呼叫会话计时器

如果未接收到 Re-INVITE 或 UPDATE 消息，则 SIP ALG 将使用 Session-Expires 值暂停会话。ALG 从对 INVITE 的 200 OK 响应获取 Session-Expires 值 (如果存在)，并将此值用于发出暂停信号。如果在会话超时前接收到其它 INVITE， ALG 会将所有超时值重置为这一新的 INVITE 或缺省值，并将重复该过程。

作为一种预防措施， SIP ALG 将使用硬超时值设置呼叫可持续的最长时间。这样可确保在以下情况下对 NetScreen 设备提供保护 :

- 呼叫期间终端系统崩溃，未接收到 BYE 消息。
- 恶意用户不发送 BYE 消息，试图攻击 SIP ALG。
- 糟糕的 sip 代理实施未能处理 Record-Route，导致无法发送 BYE 消息。
- 由于网络故障导致无法接收 BYE 消息。

呼叫取消

任何一方均可通过发送 CANCEL 消息取消呼叫。接收到 CANCEL 消息后， SIP ALG 将关闭通过防火墙的针孔 (如果曾经打开过) 并解除地址绑定。释放资源前， ALG 将延迟控制通道超时约 5 秒钟，以便为最终的 200 OK 通过留出时间。无论是否接收到 487 或 non-200 响应，达到 5 秒钟的超时时间后都将终止呼叫。

分支

利用分支 SIP 代理可将单个 INVITE 消息同时发送到多个目标。如果接收到单个呼叫的多个 200 OK 响应消息， SIP ALG 将会对其进行分析，但会用接收到的第一个 200 OK 消息更新所有信息。

SIP 消息

SIP 消息的格式包括 SIP 包头部分和 SIP 正文。在请求消息中，包头部分的第一行为请求行，其中包括方法类型、Request-URL 及协议版本。在响应消息中，第一行为状态行，其中包括状态代码。 SIP 包头包含用于信号发送的 IP 地址和端口号。SIP 正文部分由一个空白行与包头隔开，它专用于会话说明信息，此部分是可选的。 NetScreen 设备当前仅支持 “会话说明协议” (SDP)。 SIP 正文包含用于传输媒体的 IP 地址和端口号。

在 NAT 模式下， NetScreen 设备将对 SIP 包头中的信息进行转换以防止该信息被外部网络看到。对于 SIP 正文信息，需要执行 NAT 以分配资源 (指要用来接收媒体的端口号)。

SIP 包头

在下面的示例 SIP 请求消息中， NAT 将替换包头字段中的 IP 地址 (以粗体显示)，以使其对外部网络不可见。

```
INVITE bob@10.150.20.5 SIP/2.0
Via: SIP/2.0/UDP 10.150.20.3:5434
From: alice@10.150.20.3
To: bob@10.150.20.5
Call-ID: a12abcde@10.150.20.3
Contact: alice@10.150.20.3:5434
Route: <sip:netscreen@10.150.20.3:5060>
Record-Route: <sip:netscreen@10.150.20.3:5060>
```

IP 地址转换的执行方式取决于消息的类型和方向，可以是以下任一种 :

- 入站请求
- 出站响应
- 出站请求
- 入站响应

下表列出了各种情况下 NAT 的执行方法。请注意，对于有些包头字段，除了需要了解消息是来自网络内部还是网络外部外， ALG 还必须了解一些其它信息。它必须知道是哪个客户端发起的呼叫以及该消息是请求还是响应。

消息类型	字段	动作
入站请求 (从公用网络到专用网络)	To:	用本机地址替换 ALG 地址
	From:	无
	Call-ID:	无
	Via:	无
	Request-URL:	用本机地址替换 ALG 地址
	Contact:	无
	Record-Route:	无
	Route:	无
出站响应 (从专用网络到公用网络)	To:	用本机地址替换 ALG 地址
	From:	无
	Call-ID:	无
	Via:	无
	Request-URL:	不适用
	Contact:	用 ALG 地址替换本机地址
	Record-Route:	用 ALG 地址替换本机地址
	Route:	无

消息类型	字段	动作
出站请求 (从专用网络到公用网络)	To:	无
	From:	用 ALG 地址替换本机地址
	Call-ID:	用 ALG 地址替换本机地址
	Via:	用 ALG 地址替换本机地址
	Request-URL:	无
	Contact:	用 ALG 地址替换本机地址
	Record-Route:	用 ALG 地址替换本机地址
	Route:	用本机地址替换 ALG 地址
出站响应 (从公用网络到专用网络)	To:	无
	From:	用本机地址替换 ALG 地址
	Call-ID:	用本机地址替换 ALG 地址
	Via:	用本机地址替换 ALG 地址
	Request-URL:	不适用
	Contact:	无
	Record-Route:	用本机地址替换 ALG 地址
	Route:	用本机地址替换 ALG 地址

SIP 正文

SIP 正文中的 SDP 信息包括 ALG 用来为媒体流创建通道的 IP 地址。对 SDP 部分的转换也将会分配资源 (指发送和接收媒体的端口号)。

下面的示例 SDP 节选部分显示了为资源分配而转换的字段。

```
o=user 2344234 55234434 IN IP4 10.150.20.3
c=IN IP4 10.150.20.3
m=audio 43249 RTP/AVP 0
```

SIP 消息可包含多个媒体流。这一概念与将多个文件附加到电子邮件消息类似。例如，从 SIP 客户端发送到 SIP 服务器的 INVITE 消息可能包含以下字段 :

```
c=IN IP4 10.123.33.4
m=audio 33445 RTP/AVP 0

c=IN IP4 10.123.33.4
m=audio 33447 RTP/AVP 0

c=IN IP4 10.123.33.4
m=audio 33449 RTP/AVP 0
```

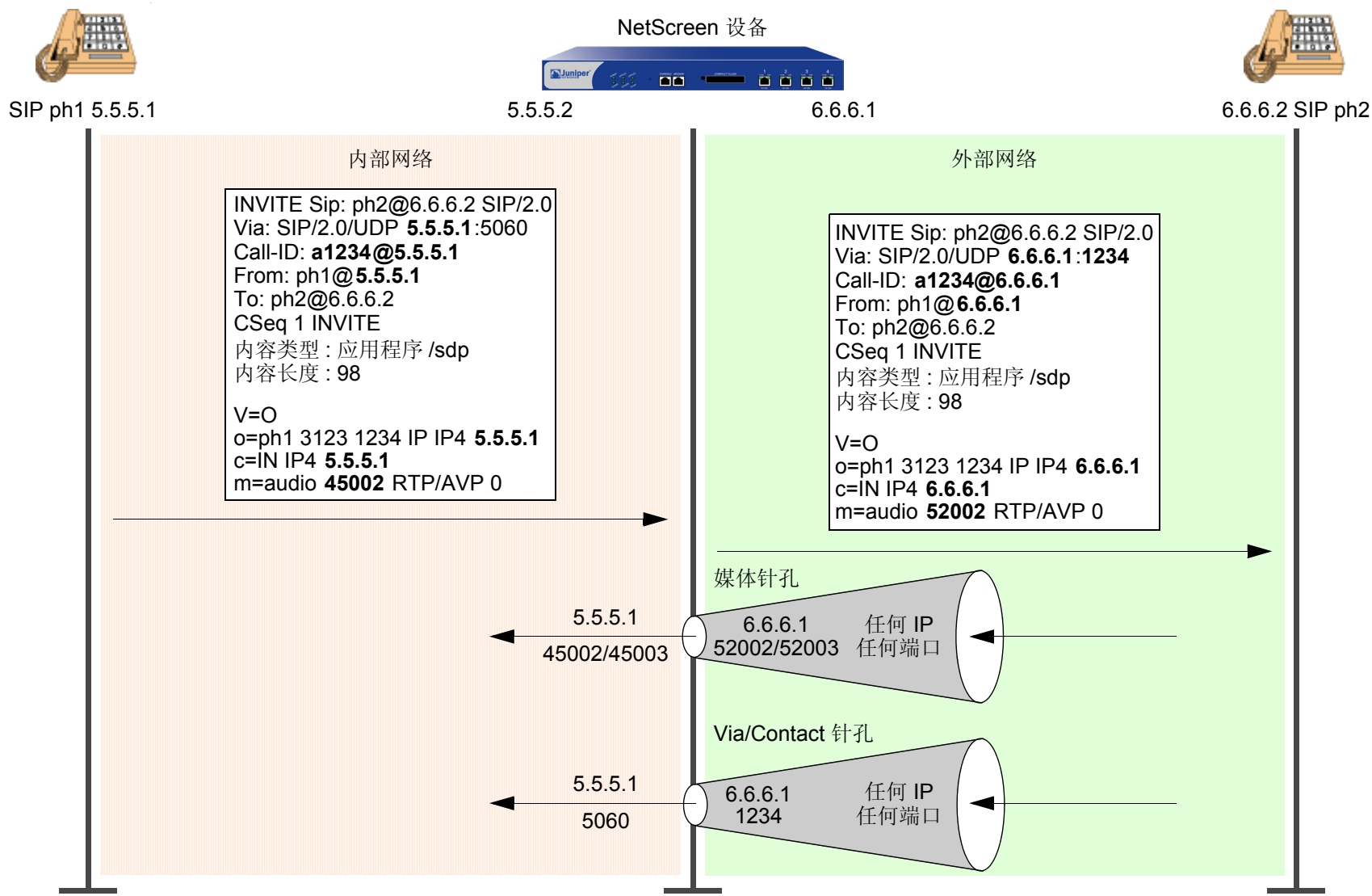
NetScreen 设备最多支持为每个方向协商的六个 SDP 通道 (每个呼叫共计 12 个通道)。有关详细信息，请参阅第 200 页上的 “SDP”。

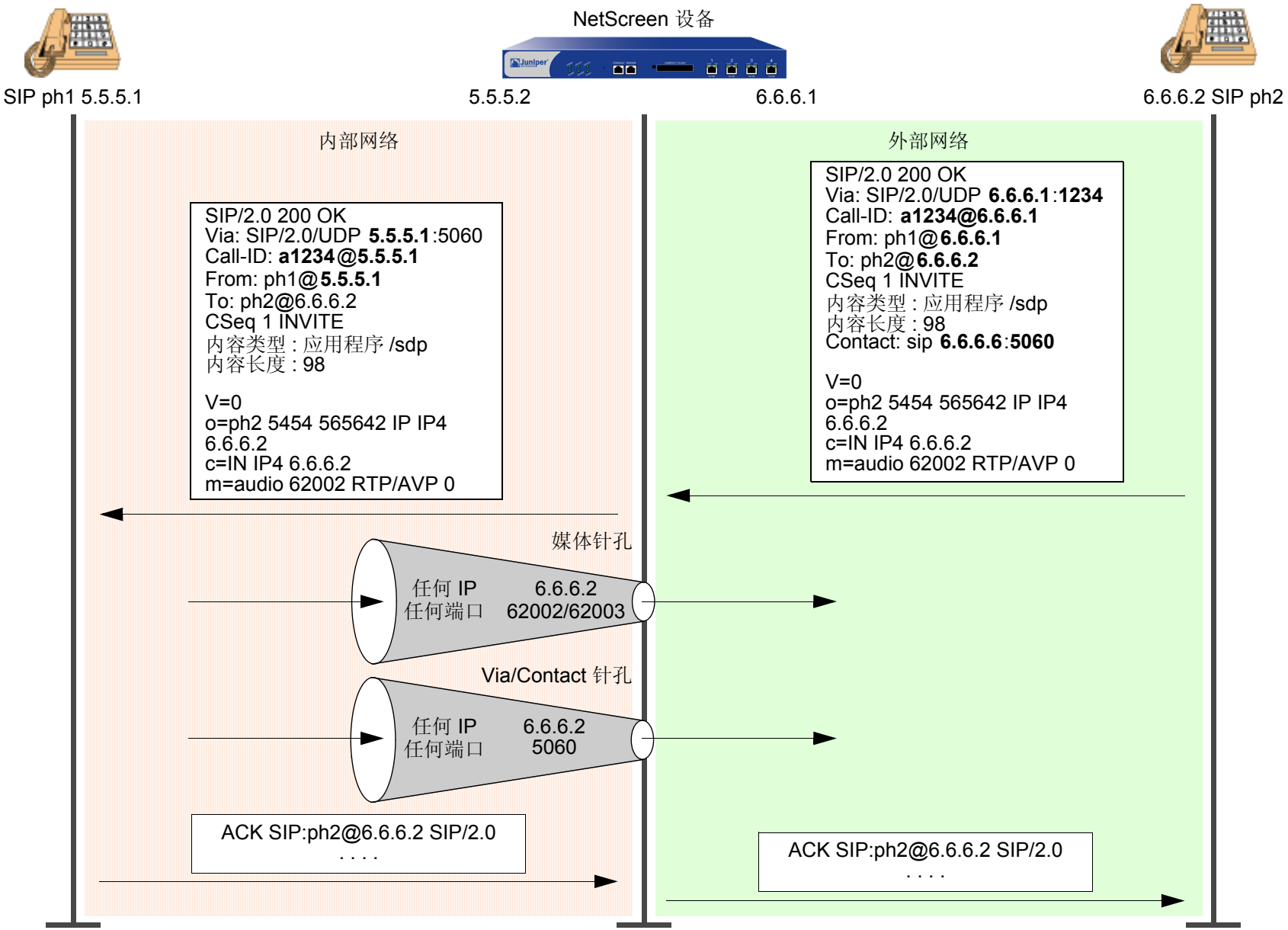
SIP NAT 场景

在下面的图示中，ph1 将向 ph2 发送一条 SIP INVITE 消息。请注意，NetScreen 设备将对包头字段中的 IP 地址 (以粗体显示) 进行转换。

INVITE 消息的 SDP 部分指示呼叫方希望接收媒体的位置。请注意，“媒体针孔”包含两个端口号，即用于 RTCP 和 RTP 的 52002 和 52003。“Via/Contact 针孔”为 SIP 信号发送提供了端口号 5060。

在 200 OK 响应消息中，注意观察在 INVITE 消息中执行的转换是如何反向的。此消息中的 IP 地址 (公用地址) 未进行转换，但入口被打开以允许媒体流访问专用网络。


NetScreen 设备
SIP ph1 5.5.5.1
5.5.5.2
6.6.6.1
6.6.6.2 SIP ph2
内部网络
外部网络
INVITE Sip: ph2@6.6.6.2 SIP/2.0
Via: SIP/2.0/UDP 5.5.5.1:5060
Call-ID: a1234@5.5.5.1
From: ph1@5.5.5.1
To: ph2@6.6.6.2
CSeq 1 INVITE
内容类型 : 应用程序 /sdp
内容长度 : 98
V=O
o=ph1 3123 1234 IP IP4 5.5.5.1
c=IN IP4 5.5.5.1
m=audio 45002 RTP/AVP 0
INVITE Sip: ph2@6.6.6.2 SIP/2.0
Via: SIP/2.0/UDP 6.6.6.1:1234
Call-ID: a1234@6.6.6.1
From: ph1@6.6.6.1
To: ph2@6.6.6.2
CSeq 1 INVITE
内容类型 : 应用程序 /sdp
内容长度 : 98
V=O
o=ph1 3123 1234 IP IP4 6.6.6.1
c=IN IP4 6.6.6.1
m=audio 52002 RTP/AVP 0
媒体针孔
5.5.5.1
45002/45003
6.6.6.1
52002/52003
任何 IP
任何端口
Via/Contact 针孔
5.5.5.1
5060
6.6.6.1
1234
任何 IP
任何端口


NetScreen 设备
SIP ph1 5.5.5.1
5.5.5.2
6.6.6.1
6.6.6.2 SIP ph2
内部网络
外部网络
SIP/2.0 200 OK
Via: SIP/2.0/UDP 5.5.5.1:5060
Call-ID: a1234@5.5.5.1
From: ph1@5.5.5.1
To: ph2@6.6.6.2
CSeq 1 INVITE
内容类型 : 应用程序 /sdp
内容长度 : 98
V=0
o=ph2 5454 565642 IP IP4 6.6.6.2
c=IN IP4 6.6.6.2
m=audio 62002 RTP/AVP 0
SIP/2.0 200 OK
Via: SIP/2.0/UDP 6.6.6.1:1234
Call-ID: a1234@6.6.6.1
From: ph1@6.6.6.1
To: ph2@6.6.6.2
CSeq 1 INVITE
内容类型 : 应用程序 /sdp
内容长度 : 98
Contact: sip 6.6.6.6:5060
V=0
o=ph2 5454 565642 IP IP4 6.6.6.2
c=IN IP4 6.6.6.2
m=audio 62002 RTP/AVP 0
媒体针孔
任何 IP
任何端口
6.6.6.2
62002/62003
Via/Contact 针孔
任何 IP
任何端口
6.6.6.2
5060
ACK SIP:ph2@6.6.6.2 SIP/2.0
. . . .
ACK SIP:ph2@6.6.6.2 SIP/2.0
. . . .

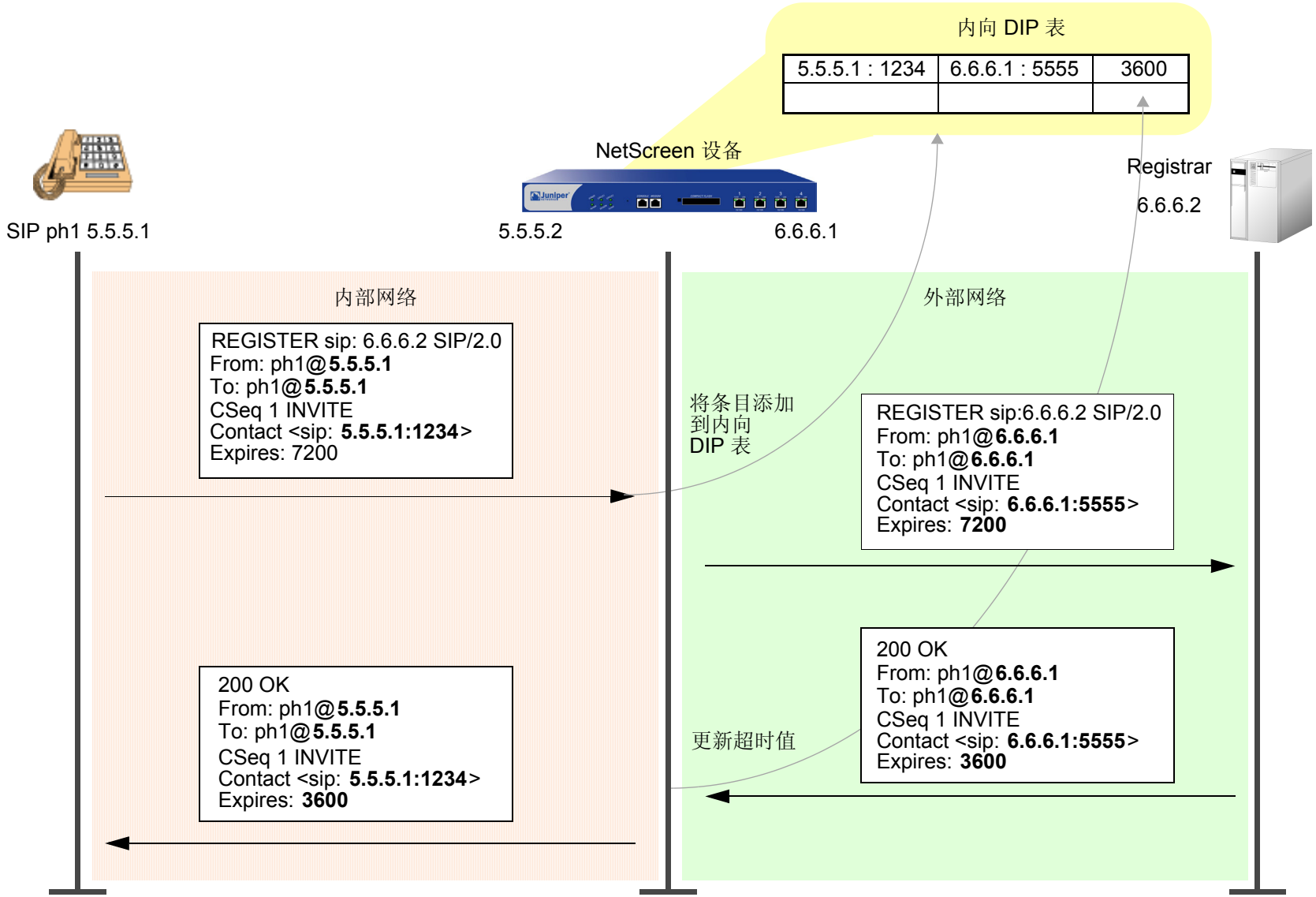
使用 SIP Registrar 的内向 SIP 呼叫支持

SIP 注册提供了一种查找功能，通过此功能 SIP 代理和位置服务器能够确定用户希望与之联系的位置。用户通过向 registrar 发送 REGISTER 消息可注册一个或多个联系位置。如下图所示， REGISTER 消息中的 To: 和 Contact: 字段包含记录地址 URL 以及一个或多个联系 URL。在将记录位置与一个或多个联系地址相关联的位置服务中，注册可创建绑定。

NetScreen 设备将对外向 REGISTER 消息进行监控、对这些地址执行 NAT 并可在 “内向 DIP” 表中存储信息。然后，当从网络外部接收到 INVITE 消息时， NetScreen 设备将使用 “内向 DIP” 表来确定将 INVITE 消息路由到哪一个内部主机。通过在 NetScreen 设备的出口接口上配置接口 DIP 或 DIP 池，可充分利用 SIP 代理注册服务来允许内向呼叫。在小型办公室中，接口 DIP 足够用以处理内向呼叫，但在大型网络或企业环境中建议建立 DIP 池。

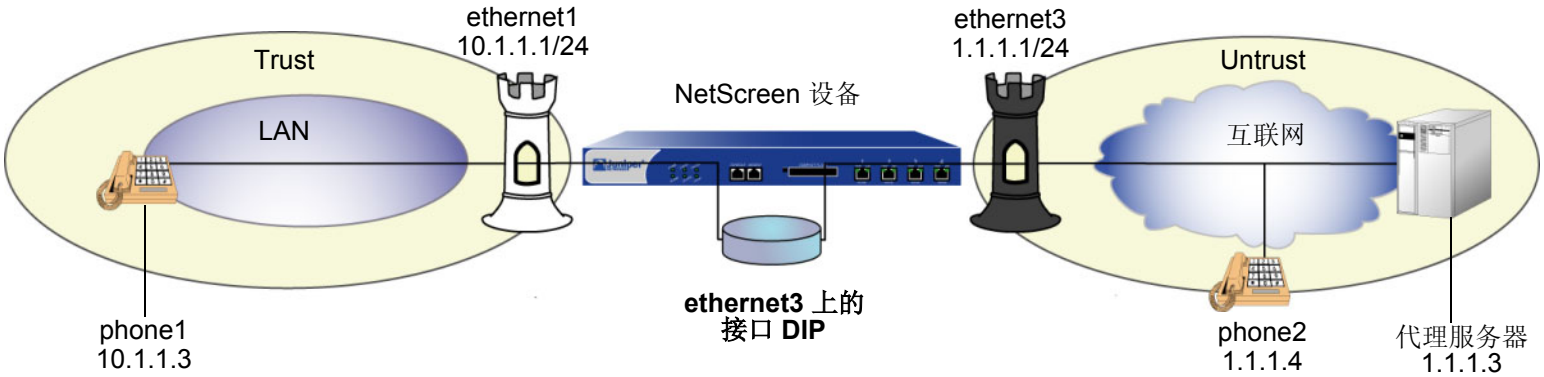
注意：*使用接口 DIP 或 DIP 池的内向呼叫支持仅支持 SIP 和 H.323 服务。*

对于内向呼叫， NetScreen 设备当前仅支持 UDP 和 TCP。当前也不支持域名解析，因此 URL 必须包含 IP 地址，如下图所示。


内向 DIP 表
5.5.5.1 : 1234
6.6.6.1 : 5555
3600
NetScreen 设备
Registrar
6.6.6.2
SIP ph1 5.5.5.1
5.5.5.2
6.6.6.1
内部网络
外部网络
REGISTER sip: 6.6.6.2 SIP/2.0
From: ph1@5.5.5.1
To: ph1@5.5.5.1
CSeq 1 INVITE
Contact <sip: 5.5.5.1:1234>
Expires: 7200
将条目添加
到内向
DIP 表
REGISTER sip:6.6.6.2 SIP/2.0
From: ph1@6.6.6.1
To: ph1@6.6.6.1
CSeq 1 INVITE
Contact <sip: 6.6.6.1:5555>
Expires: 7200
200 OK
From: ph1@6.6.6.1
To: ph1@6.6.6.1
CSeq 1 INVITE
Contact <sip: 6.6.6.1:5555>
Expires: 3600
更新超时值
200 OK
From: ph1@5.5.5.1
To: ph1@5.5.5.1
CSeq 1 INVITE
Contact <sip: 5.5.5.1:1234>
Expires: 3600

范例：内向呼叫 (接口 DIP)

在本例中， phone1 在 Trust 区段的 ethernet1 接口上， phone2 和代理服务器在 Untrust 区段的 ethernet3 接口上。首先在 ethernet3 接口设置 “接口 DIP” 以对内向呼叫执行 NAT，然后创建一个策略，以允许 SIP 信息流从 Untrust 区段到达 Trust 区段，并在这一策略中引用该 DIP。还将使用 NAT 源创建一个允许 SIP 信息流从 Trust 到达 Untrust 区段的策略。这将使得 Trust 区段中的 phone1 能够通过 Untrust 区段中的代理进行注册。有关内向 DIP 如何与 SIP 注册服务协同工作的说明，请参阅第 216 页上的 “使用 SIP Registrar 的内向 SIP 呼叫支持”。



WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Interface Mode: Route

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.3/24

Zone: Untrust

3. 内向 NAT 的 DIP

Network > Interface > Edit (对于 ethernet3) > DIP > New: 选择 **Incoming NAT** 选项，然后单击 **OK**。

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) phone1

Destination Address:

Address Book Entry: (选择) any

Service: SIP

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)

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), DIP (ethernet3)

Service: SIP

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 ethernet3 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. 内向 NAT 的 DIP

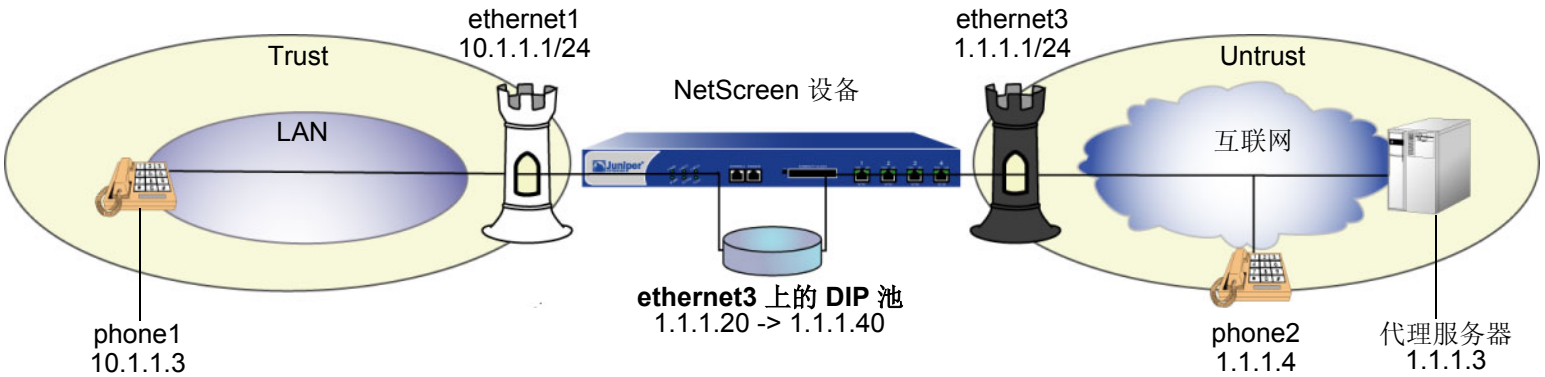
```
set interface ethernet3 dip interface-ip incoming
set dip sticky
```

4. 策略

```
set policy from trust to untrust phone1 any sip nat src permit
set policy from untrust to trust any dip(ethernet3) sip permit
save
```

范例：内向呼叫 (DIP 池)

在本例中，phone1 位于 Trust 区段中，phone2 和代理服务器位于 Untrust 区段中。首先在 ethernet3 接口设置 DIP 池以对内向呼叫执行 NAT，然后建立一个策略，以允许 SIP 信息流从 Untrust 区段到达 Trust 区段，并在这一策略中引用该 DIP 池。还将使用 NAT 源创建一个允许 SIP 信息流从 Trust 到达 Untrust 区段的策略。这将使得 Trust 区段中的 phone1 能够通过 Untrust 区段中的代理进行注册。有关 DIP 如何与 SIP 注册服务协同工作的说明，请参阅第 216 页上的 “使用 SIP Registrar 的内向 SIP 呼叫支持”。



WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Interface Mode: Route

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.3/24

Zone: Untrust

3. 内向 NAT 的 DIP 池

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

ID: 5

IP Address Range: (选择), 1.1.1.20 ~ 1.1.1.40

Port Translation: (选择)

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

Incoming NAT: (选择)

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), phone1

Destination Address:

Address Book Entry: (选择), Any

Service: SIP

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 (1.1.1.20-1.1.1.40)/port-xlate

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) DIP(5)

Service: SIP

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 ethernet3 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. 内向 NAT 的 DIP 池

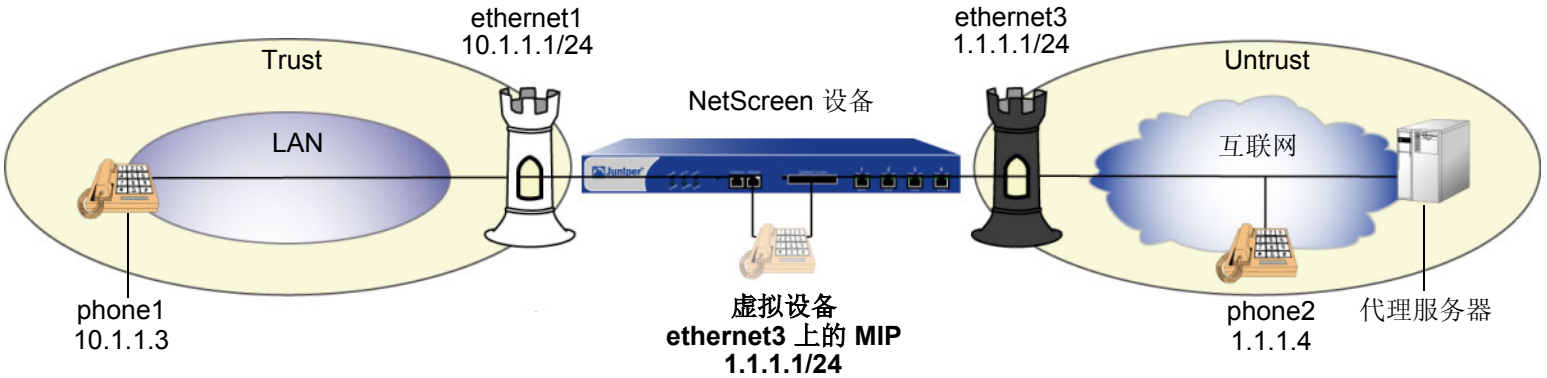
```
set interface ethernet3 dip 5 1.1.1.20 1.1.1.40 incoming
set dip sticky
```

4. 策略

```
set policy from trust to untrust phone1 any sip nat src dip 5 permit
set policy from untrust to trust any dip(5) sip permit
save
```

范例：使用 MIP 的内向呼叫

在本例中， phone1 在 Trust 区段的 ethernet1 接口上， phone2 和代理服务器在 Untrust 区段的 ethernet3 接口上。首先在到 phone1 的 ethernet3 接口上设置 MIP，然后创建一个策略，以允许 SIP 信息流从 Untrust 区段到达 Trust 区段，并在这一策略中引用该 MIP。还将创建一个策略，以允许 phone1 通过 Untrust 区段中的代理服务器注册。本例与前两个范例类似 [第 218 页上的 “范例：内向呼叫 (接口 DIP)” 和第 222 页上的 “范例：内向呼叫 (DIP 池)”]，不同之处在于使用 MIP 时， Trust 区段中的每个私有地址都需要有一个公共地址，而使用 “接口 DIP”或 DIP 池时，单个接口地址可为多个私有地址提供服务。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone: Untrust

IP Address/Netmask: 1.1.1.1/24

Interface Mode: Route

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.3/24

Zone: Untrust

3. MIP

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

Mapped IP: 1.1.1.3

Netmask: 255.255.255.255

Host IP Address: 10.1.1.3

4. 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(1.1.1.3)

Service: SIP

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 ethernet3 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. MIP

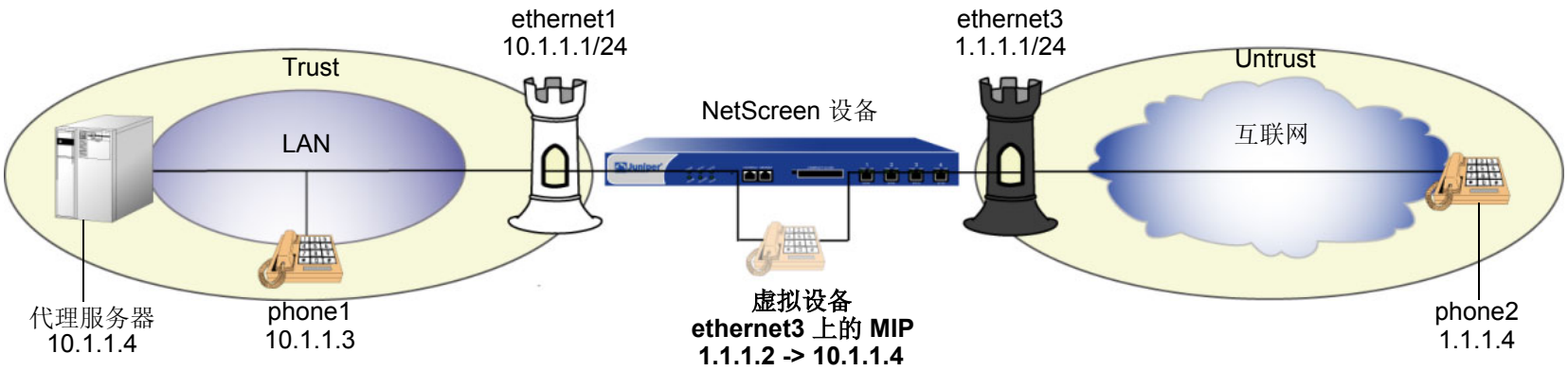
```
set interface ethernet3 mip 1.1.1.3 host 10.1.1.3
```

4. 策略

```
set policy from untrust to trust any mip(1.1.1.3) sip permit
save
```

范例：私有区段中的代理

在本例中， phone1 和 SIP 代理服务器在 Trust (专用) 区段的 ethernet1 接口上， phone2 在 Untrust 区段的 ethernet3 接口上。首先在到代理服务器的 ethernet3 接口上设置 MIP 以允许 phone2 通过代理注册，然后创建一个策略，以允许 SIP 信息流从 Untrust 到达 Trust 区段，并在这一策略中引用该 MIP。还将创建一个从 Trust 到 Untrust 区段的策略以允许 phone1 拨出。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone: Untrust
IP Address/Netmask: 1.1.1.1/24
Interface Mode: Route

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.4/24

Zone: Trust

3. MIP

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

Mapped IP: 1.1.1.2

Netmask: 255.255.255.255

Host IP Address: 10.1.1.4

Host Virtual Router Name: trust-vr

4. 策略

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

Source Address:

Address Book Entry: (选择) any

Destination Address:

Address Book Entry: (选择) phone2

Service: SIP

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)

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

Source Address:

Address Book Entry: (选择), phone2

Destination Address:

Address Book Entry: (选择), MIP(1.1.1.2)

Service: SIP

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 ethernet3 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address trust proxy 10.1.1.4/24
```

3. MIP

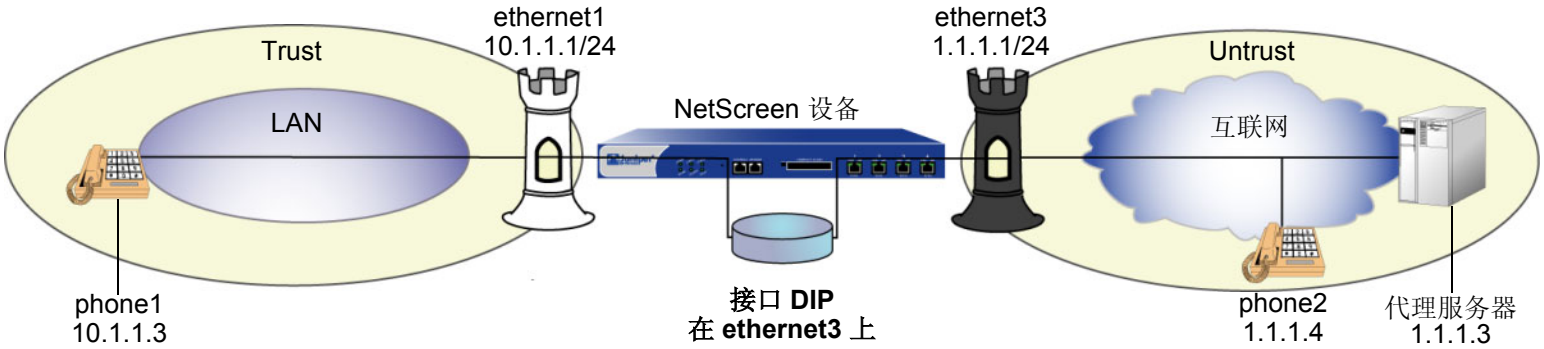
```
set interface ethernet3 mip 1.1.1.2 host 10.1.1.4
```

4. 策略

```
set policy from trust to untrust any phone2 sip nat src permit
set policy from untrust to trust phone2 mip(1.1.1.2) sip permit
save
```

范例：公用区段中的代理

在本例中，phone1 在 Trust 区段的 ethernet1 接口上，代理服务器和 phone2 在 Untrust (公用) 区段的 ethernet3 接口上。首先在 Untrust 接口上配置 “接口 DIP”，然后创建一个策略，以允许 SIP 信息流从 Untrust 区段到达 Trust 区段，并在这一策略中引用该 DIP。还将创建一个从 Trust 到 Untrust 的策略，以允许 phone1 通过 Untrust 区段中的代理服务器注册。本例与前面的内向呼叫范例类似 [请参阅第 222 页上的 “范例：内向呼叫 (DIP 池)”和第 226 页上的 “范例：使用 MIP 的内向呼叫”]，与这些范例一样，您也可以在 Untrust 接口上使用 DIP 或 MIP。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone: Untrust

IP Address/Netmask: 1.1.1.1/24

Interface Mode: Route

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.3/24

Zone: Untrust

3. 接口 DIP

Network > Interface > Edit (对于 ethernet3) > DIP: 选中 **Incoming NAT** 复选框。

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) phone1

Destination Address:

Address Book Entry: (选择) Any

Service: SIP

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)

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) DIP(ethernet3)

Service: SIP

Action: Permit

CLI

1. 接口

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

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

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address untrust proxy 1.1.1.3/24
```

3. 接口 DIP

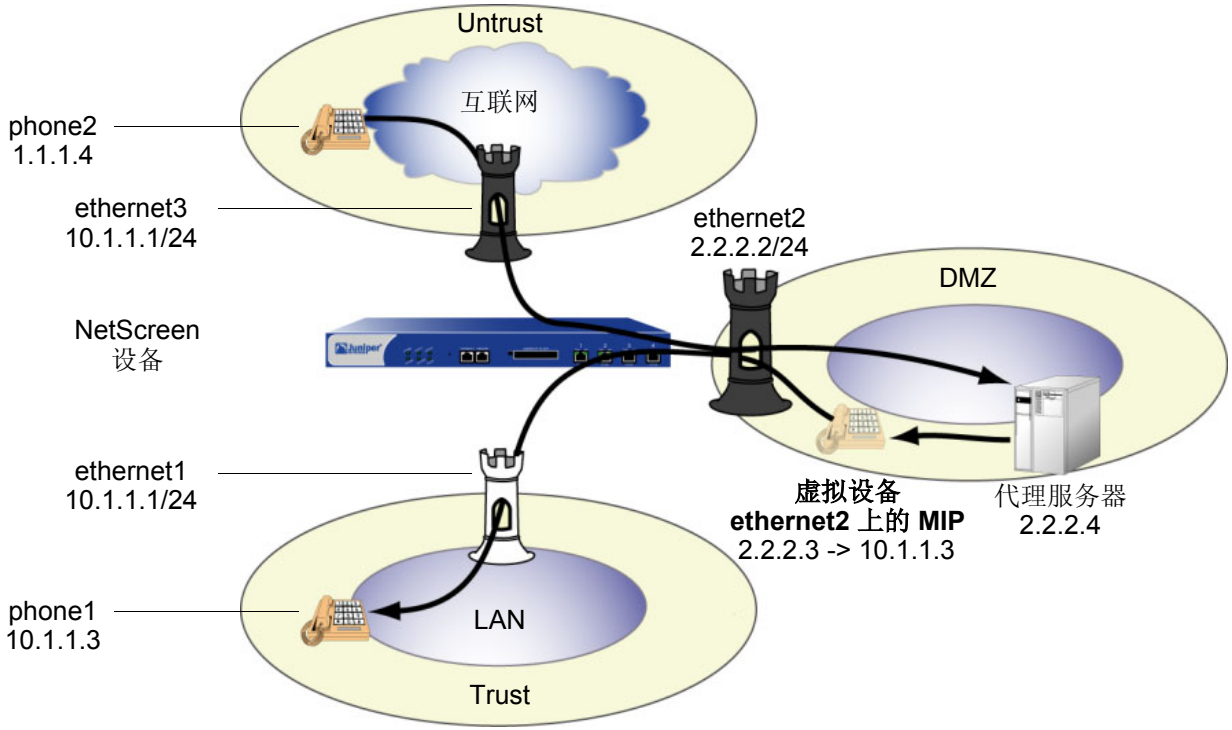
```
set interface ethernet3 dip interface-ip incoming
```

4. 策略

```
set policy from trust to untrust phone1 any sip nat src permit
set policy from untrust to trust any dip(ethernet3) sip permit
save
```

范例：三区段， DMZ 中的代理

在本例中， phone1 在 Trust 区段的 ethernet1 接口上， phone2 在 Untrust 区段的 ethernet3 接口上，代理服务器在 DMZ 的 ethernet2 接口上。首先在到 Trust 区段 phone1 的 ethernet2 接口上设置 MIP，然后创建一个从 DMZ 到 Trust 区段的策略并在这一策略中引用该 MIP。实际上，使用三个区段时在每两个区段间都需要创建双向策略。下图中的箭头表示 Untrust 区段中的 phone2 向 Trust 区段中的 phone1 拨打电话时 SIP 信息流的流向。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/24

Zone: Untrust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.4/24

Zone: DMZ

3. MIP

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

Mapped IP: 2.2.2.3

Netmask: 255.255.255.255

Host IP Address: 10.1.1.3

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), phone1

Destination Address:

Address Book Entry: (选择), proxy

Service: SIP

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: Enable

(DIP on): None (Use Egress Interface IP)

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

Source Address:

Address Book Entry: (选择), proxy

Destination Address:

Address Book Entry: (选择), phone2

Service: SIP

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), phone2

Destination Address:

Address Book Entry: (选择), phone1

Service: SIP

Action: Permit

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

Source Address:

Address Book Entry: (选择), phone2

Destination Address:

Address Book Entry: (选择), proxy

Service: SIP

Action: Permit

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

Source Address:

Address Book Entry: (选择), proxy

Destination Address:

Address Book Entry: (选择), MIP(2.2.2.3)

Service: SIP

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), phone1

Destination Address:

Address Book Entry: (选择), phone2

Service: SIP

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: Enable

(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
set interface ethernet3 route
set interface ethernet2 zone dmz
set interface ethernet2 ip 2.2.2.2/24
set interface ethernet2 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address untrust phone2 1.1.1.4/24
set address dmz proxy 2.2.2.4
```

3. MIP

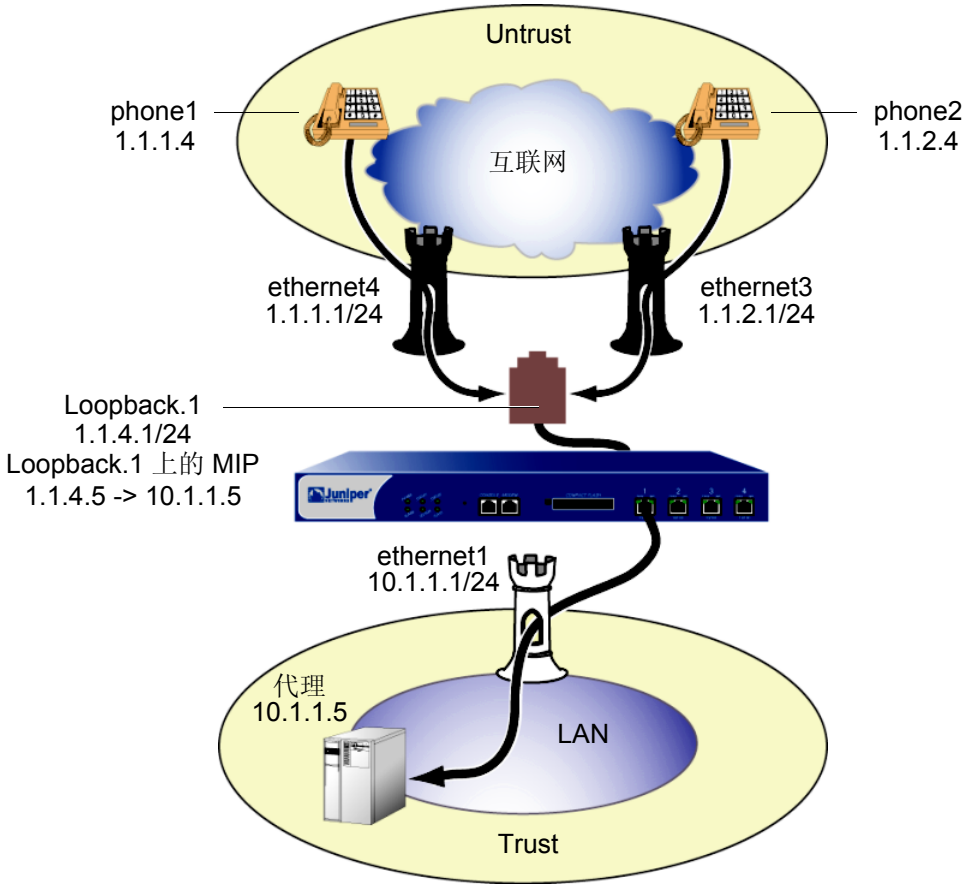
```
set interface2 mip 2.2.2.3 host 10.1.1.3
```

4. 策略

```
set policy from trust to dmz phone1 proxy sip nat src permit
set policy from dmz to untrust proxy phone2 sip permit
set policy from untrust to trust phone2 phone1 sip permit
set policy from untrust to dmz phone2 proxy sip permit
set policy from dmz to trust proxy mip(2.2.2.3) sip permit
set policy from trust to untrust phone1 phone2 sip nat src permit
save
```

范例 : Untrust 区段内部

在本例中， phone2 在 Untrust 区段的 ethernet2 接口上， phone3 在 Untrust 区段 ethernet3 接口上的子网中，代理服务器在 Trust 区段的 ethernet1 接口上。为允许 Untrust 区段中两个电话间的区段内部 SIP 信息流，需要创建一个回传接口并将 ethernet2 和 ethernet3 添加到回传组中，然后在回传接口与代理服务器的 IP 地址之间设置 MIP。创建回传接口将使您能够在 Trust 区段中对代理服务器使用单一 MIP。因为在 Untrust 区段中会缺省打开阻塞，所以还必须关闭阻塞才能允许区段内部通信。有关使用回传接口的详细信息，请参阅第 **7**-105 页上的 “MIP 和回传接口”。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet4): 输入以下内容，然后单击 **OK**:

Zone: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Zone: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.2.1/24

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

Interface Name: loopback.1

Zone: Untrust (trust-vr)

IP Address/Netmask: 1.1.4.1/24

2. 地址

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.4/32

Zone: Untrust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.2.4/32

Zone: Untrust

3. 回传组

Network > Interfaces > Edit (对于 ethernet4): 输入以下内容，然后单击 **OK**:

As member of loopback group: (选择) loopback.1

Zone Name: Untrust

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

As member of loopback group: (选择) loopback.1

Zone Name: Untrust

4. MIP

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

Mapped IP: 1.1.4.5

Netmask: 255.255.255.255

Host IP Address: 10.1.1.5

Host Virtual Router Name: trust-vr

5. 阻塞

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

Block Intra-Zone Traffic: (清除)

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), proxy

Destination Address:

Address Book Entry: (选择), Any

Service: SIP

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: Enable

(DIP on): None (Use Egress Interface IP)

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(1.1.4.5)

Service: SIP

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 1.1.2.1/24
set interface ethernet1 route

set interface ethernet4 zone untrust
set interface ethernet4 ip 1.1.1.1/24
set interface ethernet4 route

set interface loopback.1 zone untrust
set interface loopback.1 ip 1.1.4.1/24
set interface loopback.1 route
```

2. 地址

```
set address trust proxy 10.1.1.5/32
set address untrust phone1 1.1.1.4/32
set address untrust phone2 1.1.2.4/32
```

3. 回传组

```
set interface ethernet2 loopback-group loopback.1
set interface ethernet3 loopback-group loopback.1
```

4. MIP

```
set interface loopback.1 mip 1.1.4.5 host 10.1.1.5
```

5. 阻塞

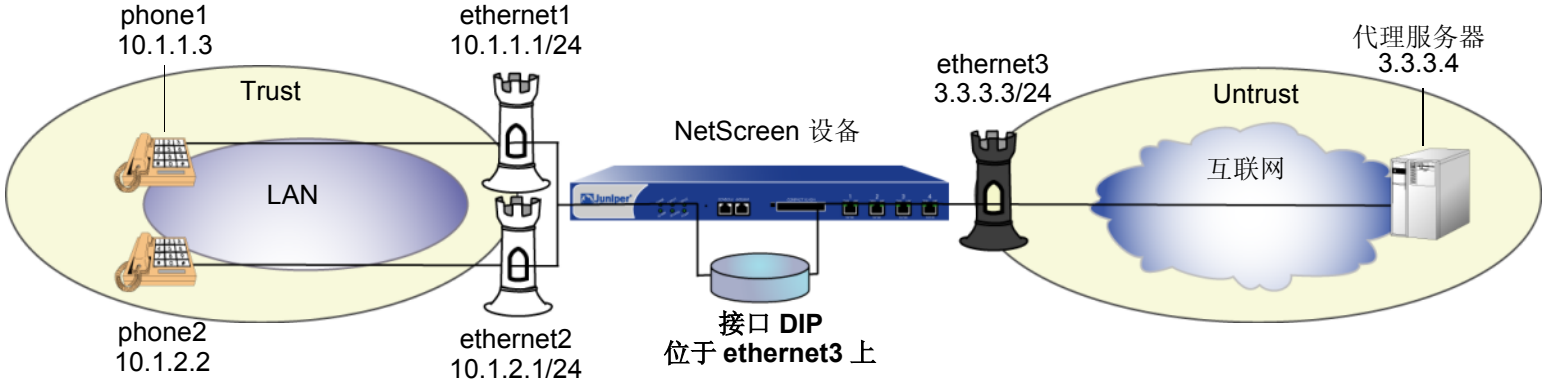
```
unset zone untrust block
```

6. 策略

```
set policy from trust to untrust proxy any sip nat src permit
set policy from untrust to trust any mip(1.1.4.5) sip permit
save
```

范例 : Trust 内部区段

在本例中， phone1 在 Trust 区段的 ethernet1 接口上， phone2 在 Trust 区段某一子网的 ethernet2 接口上，代理服务器在 Untrust 区段的 ethernet3 接口上。为使 Trust 区段中的两个电话可彼此通信，需要在 ethernet3 接口上配置接口 DIP 以允许它们与代理服务器进行联系，然后设置策略以允许 Trust 和 Untrust 区段间的双向 SIP 信息流。 Trust 区段中会缺省关闭阻塞 (因其位于定义的定制区段中)。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.2.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

2. 地址

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

Address Name: phone1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.3/24

Zone: Trust

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

Address Name: phone2

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.2.2/24

Zone: Trust

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

Address Name: proxy

IP Address/Domain Name:

IP/Netmask: (选择), 3.3.3.4/24

Zone: Untrust

3. 内向 NAT 的 DIP

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

Incoming NAT: (选择)

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), proxy

Service: SIP

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: Enable

(DIP on): None (Use Egress Interface IP)

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

Source Address:

Address Book Entry: (选择) proxy

Destination Address:

Address Book Entry: (选择) Any

Service: SIP

Action: Permit

> Advanced: 输入以下内容，然后单击 **Return** 以设置高级选项 :

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 ethernet2 zone trust
set interface ethernet2 ip 10.1.2.1/24
set interface ethernet2 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface ethernet3 route
```

2. 地址

```
set address trust phone1 10.1.1.3/24
set address trust phone2 10.1.2.2/24
set address untrust proxy 3.3.3.4/24
```

3. 接口 DIP

```
set interface ethernet3 dip interface-ip incoming
```

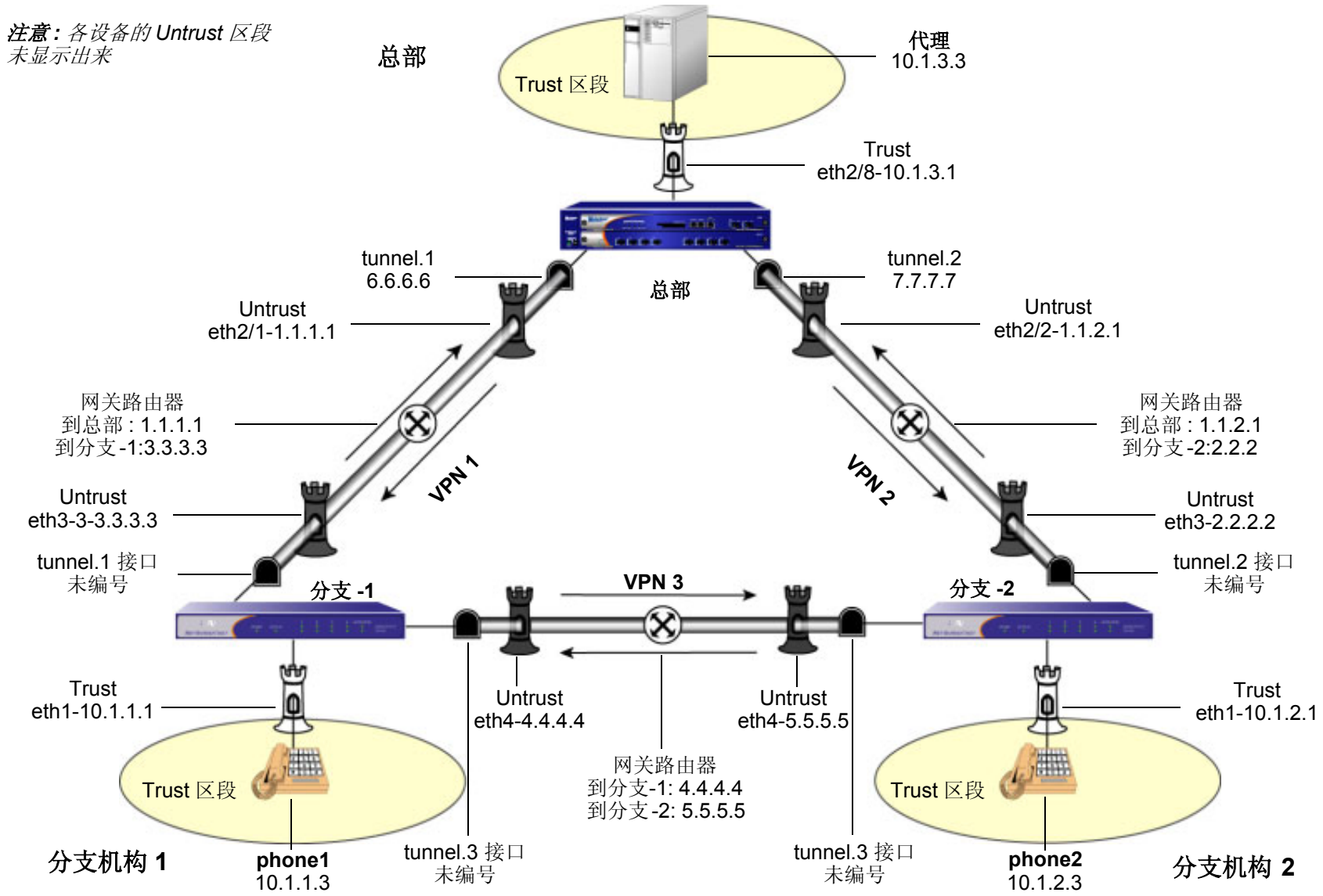
4. 策略

```
set policy from trust to untrust any proxy sip nat src permit
set policy from untrust to trust proxy dip(ethernet3) sip permit
save
```

范例：SIP 的全网状 VPN

在本例中，总部与分支机构通过全网状 VPN 链接在一起。每个站点都有一个单独的 NetScreen 设备。代理服务器位于“总部”的 Trust 区段中，phone1 位于“分支机构 1”的 Trust 区段中，phone2 位于“分支机构 2”的 Trust 区段中。连接这些设备的所有接口均位于其各自的 Untrust 区段中。对每台设备您都可以配置通向彼此设备的两个通道以创建全网状网络。

注意：*本例中使用的 NetScreen 设备必须有四个可用的可独立配置接口。*


注意：各设备的 Untrust 区段未显示出来
总部
Trust 区段
代理
10.1.3.3
Trust
eth2/8-10.1.3.1
tunnel.1
6.6.6.6
总部
tunnel.2
7.7.7.7
Untrust
eth2/1-1.1.1.1
Untrust
eth2/2-1.1.2.1
网关路由器
到总部 : 1.1.1.1
到分支-1:3.3.3.3
网关路由器
到总部 : 1.1.2.1
到分支-2:2.2.2.2
VPN 1
VPN 2
Untrust
eth3-3-3.3.3.3
Untrust
eth3-2.2.2.2
tunnel.1 接口
未编号
tunnel.2 接口
未编号
分支 -1
VPN 3
分支 -2
Trust
eth1-10.1.1.1
Untrust
eth4-4.4.4.4
Untrust
eth4-5.5.5.5
Trust
eth1-10.1.2.1
网关路由器
到分支-1: 4.4.4.4
到分支-2: 5.5.5.5
Trust 区段
Trust 区段
分支机构 1
phone1
10.1.1.3
tunnel.3 接口
未编号
tunnel.3 接口
未编号
phone2
10.1.2.3
分支机构 2

注意：*在本例中，每个 WebUI 部分仅列出了进入设备配置页面的导航路径。要查看需要为所有 WebUI 部分设置的特定参数和值，请参阅随后的 CLI 部分。*

WebUI (对于总部)

1. 接口

   Network > Interfaces > Edit (对于 ethernet2/1)

   Network > Interfaces > Edit (对于 ethernet2/2)

   Network > Interfaces > Edit (对于 ethernet2/8)

   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. VPN

   VPNs > AutoKey IKE > New: > Advanced

4. 路由

   Network > Routing > Routing Entries > New

5. 策略

   Policies > (From: Untrust, To: Trust) New

   Policies > (From: Trust, To: Untrust) New

CLI (对于总部)

1. 接口

```
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 1.1.1.1/24

set interface ethernet2/2 zone untrust
set interface ethernet2/2 ip 1.1.2.1/24

set interface ethernet2/8 zone trust
set interface ethernet2/8 ip 10.1.1.1/24
set interface ethernet2/8 nat

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 6.6.6.6/24

set interface tunnel.2 zone untrust
set interface tunnel.2 ip 7.7.7.7/24
```

2. 地址

```
set address trust proxy 10.1.3.3/32
```

3. VPN

```
set ike gateway to-branch-1 address 3.3.3.3 main outgoing-interface ethernet2/1
    preshare “netscreen” sec-level standard
set ike gateway to-branch-2 address 2.2.2.2 main outgoing-interface ethernet2/2
    preshare “netscreen” sec-level standard
set vpn vpn_branch-1 gateway to-branch-1 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-1 id 1 bind interface tunnel.1
set vpn vpn-branch-2 gateway to-branch-2 no-reply tunnel idletime 0 sec-level
    standard
set vpn vpn-branch-2 id 2 bind interface tunnel.2
```

4. 路由

```
set route 10.1.2.0/24 interface tunnel.2
set route 10.1.1.0/24 interface tunnel.1
```

5. 策略

```
set policy from untrust to trust any proxy sip permit
set policy from trust to untrust proxy any sip permit
save
```

WebUI (对于分支机构 2)

1. 接口

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > Edit (对于 ethernet2)

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. VPN

   VPNs > AutoKey IKE > New: > Advanced

4. 路由

   Network > Routing > Routing Entries > New

5. 策略

   Policies > (From: Untrust, To: Trust) New

   Policies > (From: Trust, To: Untrust) New

CLI (对于分支机构 2)

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 2.2.2.2/24

set interface ethernet4 zone untrust
set interface ethernet4 ip 5.5.5.5/24


set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3

set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. 地址

```
set address trust phone1 10.1.1.3/32
```

3. VPN

```
set ike gateway to-central address 1.1.1.1 Main outgoing-interface ethernet3
    preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 5.5.5.5 Main outgoing-interface ethernet4
    preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level
    standard
set vpn vpncentral id 4 bind interface tunnel.1
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 id 5 bind interface tunnel.3
```

4. 路由

```
set route 10.1.3.0/24 interface tunnel.1
set route 10.1.2.0/24 interface tunnel.3
```

5. 策略

```
set policy from trust to untrust phone1 any sip permit
set policy from untrust to trust any phone1 sip permit
save
```

WebUI (对于分支机构 1)

1. 接口

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interfaces > Edit (对于 ethernet4)

   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. VPN

   VPNs > AutoKey IKE > New: > Advanced

4. 路由

   Network > Routing > Routing Entries > New

5. 策略

   Policies > (From: Untrust, To: Trust) New

   Policies > (From: Trust, To: Untrust) New

CLI (对于分支机构 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 3.3.3.3/24

set interface ethernet4 zone untrust
set interface ethernet4 ip 4.4.4.4/24

set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3

set interface tunnel.3 zone untrust
set interface tunnel.3 ip unnumbered interface ethernet4
```

2. 地址

```
set address trust phone2 10.1.2.1/32
```

3. VPN

```
set ike gateway to-central address 1.1.2.1 main outgoing-interface ethernet3
    preshare "netscreen" sec-level standard
set ike gateway to-ns50 address 4.4.4.4 main outgoing-interface ethernet4
    preshare "netscreen" sec-level standard
set vpn vpncentral gateway to-central no-replay tunnel idletime 0 sec-level
    standard
set vpn vpncentral bind interface tunnel.2
set vpn vpn-ns50 gateway to-ns50 no-replay tunnel idletime 0 sec-level standard
set vpn vpn-ns50 bind interface tunnel.3
```

4. 路由

```
set route 10.1.1.0/24 interface tunnel.3
set route 10.1.3.0/24 interface tunnel.2
```

5. 策略

```
set policy from trust to untrust phone2 any sip permit
set policy from untrust to trust any phone2 sip permit
save
```

VoIP 服务的带宽管理

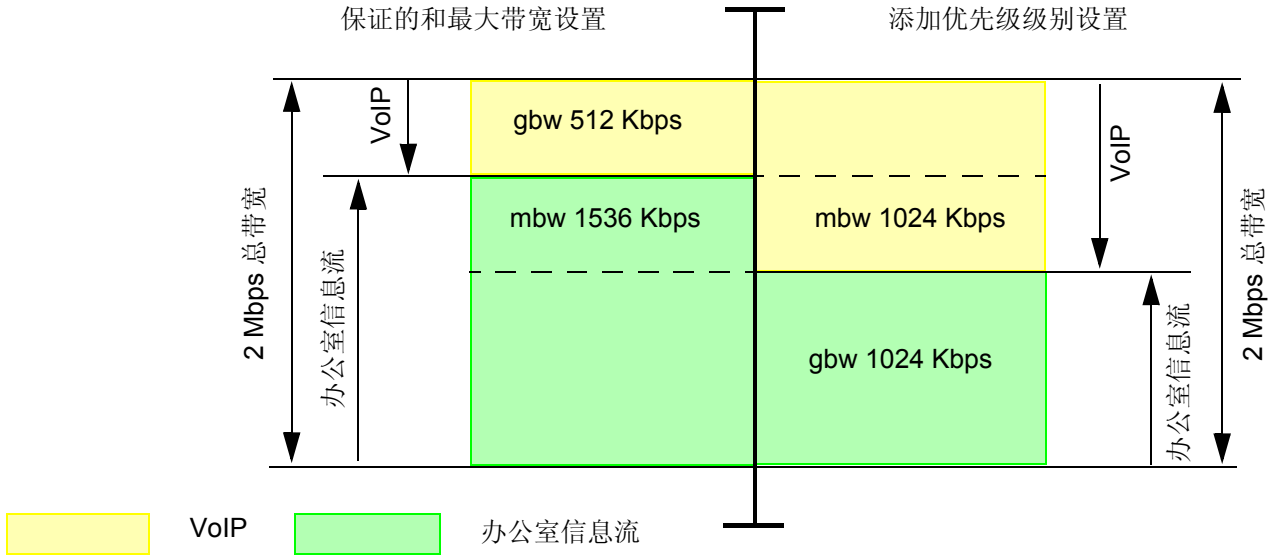
Juniper Networks 建议使用标准 ScreenOS 信息流整形机制并通过以下方法来管理 VoIP 服务的带宽。

- 保证 VoIP 信息流的带宽 — 在保证 VoIP 服务质量的前提下允许其它类型信息流通过接口的最有效方法是：创建一个策略来保证通过接口的 VoIP 信息流量所需的最小带宽，并将优先级排列设置为最高级别。此策略的优势在于当需要 VoIP 服务时可使用其它带宽，而其它类型的信息流在不需要 VoIP 服务时可使用未为其保证的带宽。
- 限制非 VoIP 信息流的带宽 — 通过为非 VoIP 信息流设置最大带宽，可使 VoIP 信息流能够使用剩余的带宽。还可将 VoIP 信息流的优先级排列设置为最高级别。此方法的缺点是非 VoIP 信息流不能使用其它带宽，即使 VoIP 信息流并未加以使用。
- 使用优先级排列和差异服务码点 (DSCP) 标记 — 保证 VoIP 信息流的带宽及限制非 VoIP 信息流的带宽均可控制 NetScreen 设备的吞吐量。 DSCP 标记允许您向下游保留其优先级排队设置，并允许通过始发网络设备或上游路由器来保持或更改接收到的 DSCP 值设置，从而使下一跳跃路由器 (通常指 LAN 或 WAN 边缘路由器) 能够在 “差异服务” 域中加强 “服务质量” (QoS)。缺省情况下， NetScreen 设备会在 VPN 配置中将 DSCP 标记从 IP 数据包的内部包头复制到外部包头，以便下一跳跃路由器可对加密信息流执行正确的 QoS。有关策略中 DSCP 如何与优先级级别协同工作的信息，请参阅第 310 页上的 “信息流整形”。

下图显示了优先级级别设置如何才能影响 ethernet1 (2 Mbps) 接口上的保障带宽 (gbw) 和最大带宽 (mbw) 使用量。该图假设已确定需要支持至少八个 VoIP 呼叫 (8 x 每个呼叫的 64 Kbps 带宽，总计为 512 Kbps)，有时呼叫数可达 16 个。您已保证将剩余的带宽用于总部信息流，并将所在办公室的信息流的最大带宽设置为包括未保证用于 VoIP 的带宽。这将为 VoIP 和办公室信息流服务创建一个 512 Kbps 的最大带宽重叠 (以虚线表示)。

图的左侧显示接口上在办公室信息流使用率较高而 VoIP 使用率较低的情况下这些设置的带宽使用情况。如果 VoIP 带宽需要量突然增多，除非它具有比办公室信息流服务更高的优先级，否则将得不到更多带宽。图的右侧显示同样情况下当将 VoIP 设置为具有较高优先级而将办公室信息流设置为较低优先级时带宽的使用情况。有关配置带宽和优先级级别的详细信息，请参阅第 341 页上的 “信息流整形”。

使用优先级级别和带宽设置



服务组

服务组是集合在某一名称下的一组服务。在创建了一个包含多个服务的组后，即可在组级将服务应用到策略，从而简化管理。

NetScreen 服务组选项具有下列功能：

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

服务组受到以下限制：

- 服务组不能与服务同名；因此，如果有一项服务名为 “FTP”，则不能将服务组命名为 “FTP”。
- 如果某服务组被策略所引用，则可以编辑但不能移除该组，除非事先在策略中移除对它的引用。
- 从服务薄中删除定制服务簿条目时，同时也将该条目从所有引用它的组中移除。
- 一个服务组不能将其它服务组当作成员包含在内。
- 全包含式服务术语 “ANY”不能添加到组中。
- 服务每次只能作为一个组的一部分。

范例：创建服务组

在本范例中，将创建一个名为 grp1 的服务组，其中包括 IKE、 FTP 和 LDAP 服务。

WebUI

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

Group Name: grp1

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

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

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

CLI

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

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

范例：修改服务组

在本范例中，将更改名为 grp1 的服务组中的成员，此组是您在第 264 页上的 “范例：创建服务组”中创建的。您将移除 IKE、 FTP 和 LDAP 服务，然后添加 HTTP、 FINGER 和 IMAP。

WebUI

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

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

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

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

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

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

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

CLI

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

范例：移除服务组

在本例中，将删除名为 grp1 的服务组。

WebUI

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

CLI

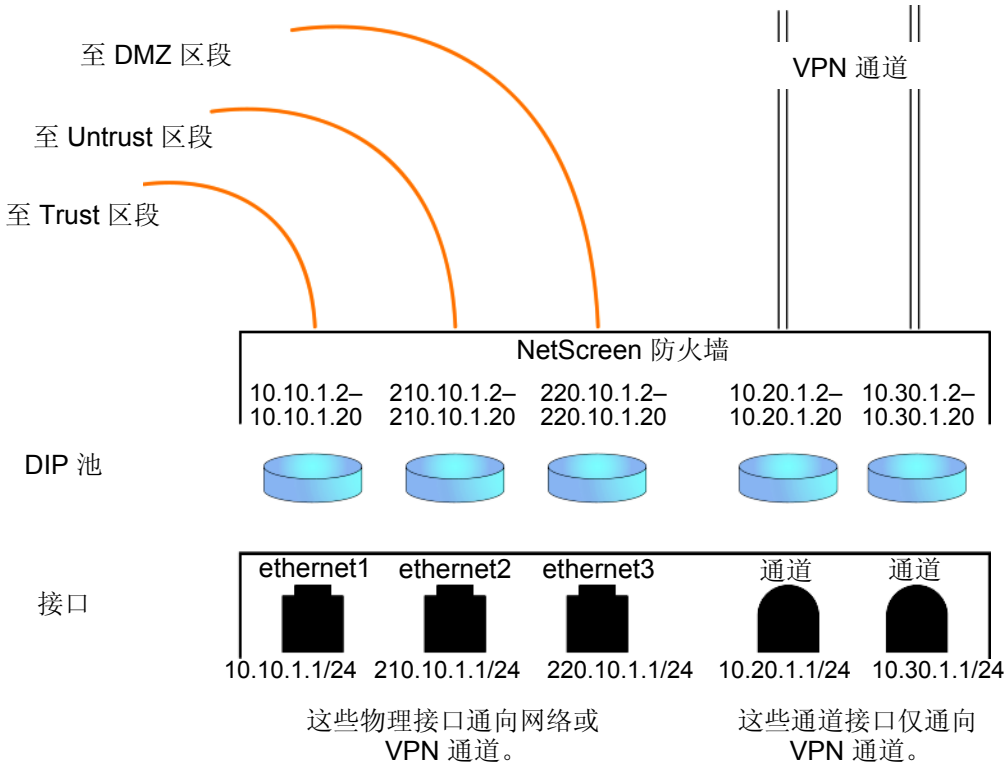
```
unset group service grp1
save
```

注意：*NetScreen 设备不会自动删除已经从中移除所有成员的组。*

DIP 池

动态 IP (DIP) 池包含某一范围内的 IP 地址， NetScreen 设备在对 IP 数据包包头中的源 IP 地址执行网络地址转换时，可从中动态地或固定地提取地址。 [有关确定源地址转换的信息，请参阅第 **7**-24 页上的 “来自 DIP 池 (带有地址变换) 的 NAT-Src”。] 如果 DIP 池的地址范围与接口 IP 地址在相同子网内，则该池必须排除可能同样也位于此子网内的接口 IP 地址、路由器 IP 地址及任何映射 IP (MIP) 或虚拟 IP (VIP) 地址。如果地址范围在扩展接口的子网中，则该池必须排除扩展接口的 IP 地址。

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



端口地址转换

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

一些应用，如 “NetBIOS 扩展用户接口” (NetBEUI) 及 “Windows 互联网命名服务” (WINS) 需要具体的端口号，如果将 PAT 应用于它们，它们将无法正常运行。对于此类应用，可在应用 DIP 时指定不执行 PAT (即使用固定端口)。对于固定端口 DIP，NetScreen 设备将散列原始主机 IP 地址并将其保存在主机散列表中，从而允许 NetScreen 设备将正确的会话与各个主机关联起来。

范例 : 创建使用 PAT 的 DIP 池

在本例中，将为本地站点的用户创建一个 VPN 通道，以到达远程站点的 FTP 服务器。但是，这两个站点的内部网络使用相同的私有地址空间 10.1.1.0/24。为了解决地址重叠问题，将在本地 NetScreen 设备的 Untrust 区段中创建一个通道接口并为其分配 IP 地址 10.10.1.1/24，然后将其与某一地址范围为 10.10.1.2–10.10.1.2 且已启用端口地址转换的 DIP 池相关联。

远程站点的 admin 也必须创建一个通道接口，其 IP 地址位于中性地址空间中，如 10.20.2.1/24，然后建立一个 “映射 IP” (MIP) 地址到其 FTP 服务器，如 10.20.2.5 到主机 10.1.1.5。

注意：*本例仅包括通道接口配置及其伴随的 DIP 池。有关此方案所有必要配置步骤的完整范例，请参阅第* ***5*** *-199 页上的 “具有重叠地址的 VPN 站点”。*

WebUI

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.10.1.1/24

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

ID: 5[10]

IP Address Range: 10.10.1.2 ~ 10.10.1.2

Port Translation: (选择)

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

CLI

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

***注意：**由于 PAT 是缺省启用的，因此没有用来启用它的参数。要创建与上述相同的 DIP 池但不使用 PAT (即使用固定端口号)，请执行以下操作：*

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

10. 可以使用所显示的 ID 号，它是按顺序排列的下一个可用数字，也可键入不同的号码。

范例 : 修改 DIP 池

在本例中，将把一个现有 DIP 池 (ID 5) 的地址范围从 10.20.1.2 - 10.20.1.2 更改为 10.20.1.2 - 10.20.1.10。此 DIP 池与 tunnel.1 相关联。请注意，要通过 CLI 更改 DIP 池范围，必须首先移除 (或撤消) 现有 dip 池，然后再创建一个新池。

注意：*没有使用此特定 DIP 池的策略。如果某一策略使用 DIP 池，必须先删除该策略或将其修改为不使用 DIP 池，然后才能修改 DIP 池。*

WebUI

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

IP Address Range: 10.20.1.2 ~ 10.20.1.10

CLI

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

附着 DIP 地址

当主机发起与要求进行网络地址转换 (NAT) 的策略相匹配的数个会话并获得 DIP 池 (已启用端口转换) 所分配的地址时[11]， NetScreen 设备会为每个会话分配不同的源 IP 地址。对于创建多个会话 (每个会话都需要同一源 IP 地址) 的服务，这种随机地址分配可能会产生问题。

例如，使用 “AOL 即时消息” (AIM) 客户端时，多个会话必须具有相同的 IP 地址。登录时将创建一个会话，并且还将为每个聊天创建一个。对于验证新聊天是否属于认证用户的 AIM 服务器，它需要将登录会话的源 IP 地址与聊天会话的源 IP 地址进行匹配。如果它们不同 (可能由于它们是在 NAT 过程中从 DIP 池随机分配的)， AIM 服务器将拒绝聊天会话。

11. 如果 DIP 池未执行端口转换， NetScreen 设备会为来自同一主机的所有并发会话分配一个 IP 地址。

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

扩展接口和 DIP

根据实际情况，如果需要将出站防火墙信息流中的源 IP 地址从出口接口的地址转换为不同子网中的地址，可使用扩展接口选项。此选项允许将第二个 IP 地址与和一个伴随 DIP 池连接到位于不同子网中的接口。然后可基于每个策略启用 NAT 并指定 DIP 池 (该池是在用于转换的扩展接口上创建的)。

范例 : 在不同子网中使用 DIP

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

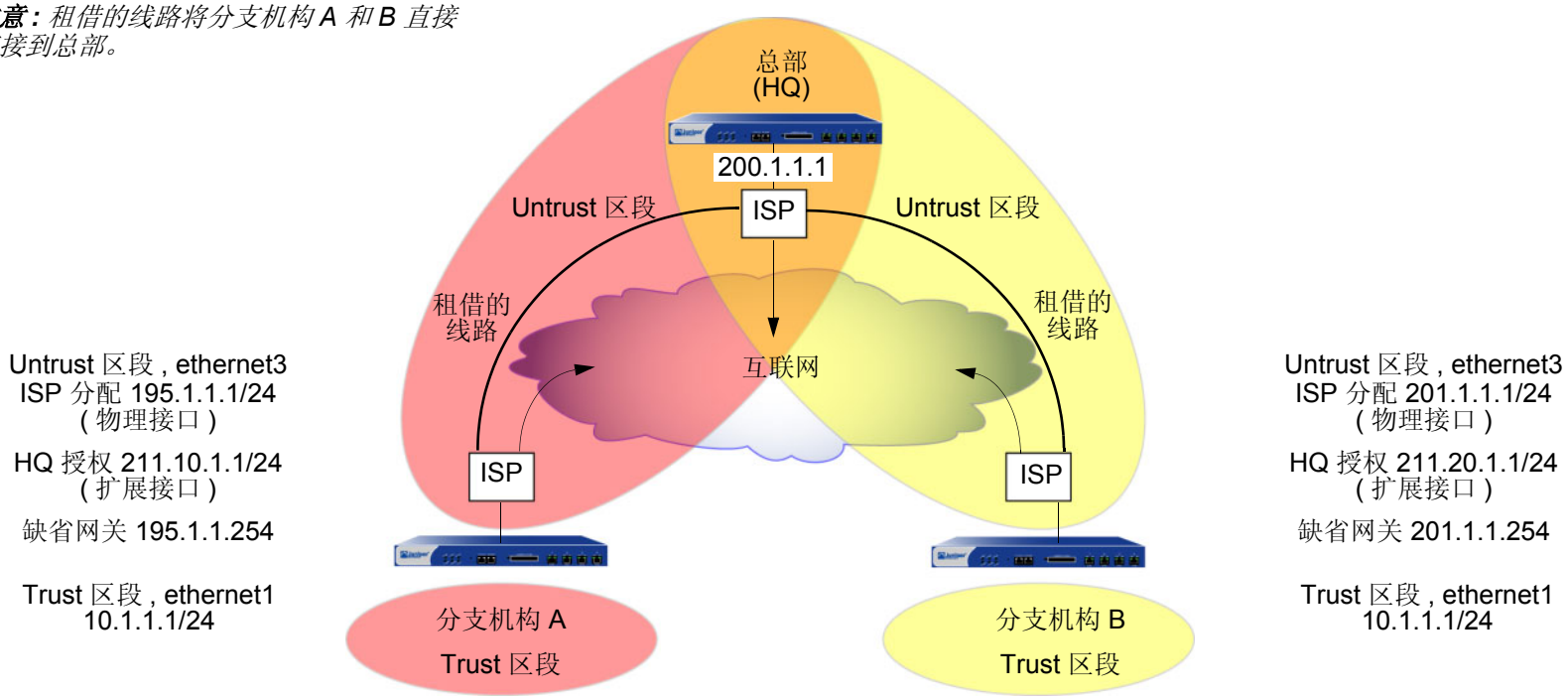
	分配的 IP 地址 (来自 ISP) 用于 Untrust 区段物理接口	**授权的 IP 地址 (来自总部) 用于 Untrust 区段扩展接口 DIP**
分支机构 A	195.1.1.1/24	211.10.1.1/24
分支机构 B	201.1.1.1/24	211.20.1.1/24

两个站点的 NetScreen 设备都有 Trust 区段和 Untrust 区段。所有安全区段都在 trust-vr 路由选择域中。将 ethernet1 绑定到 Trust 区段并为其分配 IP 地址 10.1.1.1/24。将 ethernet3 绑定到 Untrust 区段并为其指定由 ISP 分配的 IP 地址 :“分支机构 A”为 195.1.1.1/24，“分支机构 B”为 201.1.1.1/24。然后在 ethernet3 上创建一个具有 DIP 池的扩展接口，其中包含授权 IP 地址 :

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

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

注意：*租借的线路将分支机构 A 和 B 直接连接到总部。*



注意：*为了使用租借线路，每个 ISP 都必须在租借线路端点为流向某一站点的信息流设置路由。 ISP 将他们从本地 NetScreen 设备接收到的所有其它信息流路由到互联网。*

WebUI (分支机构 A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 195.1.1.1/24

Interface Mode: Route

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

ID: 5

IP Address Range: 211.10.1.1 ~ 211.10.1.1

Port Translation: (选择)

Extended IP/Netmask: 211.10.1.10/255.255.255.0

2. 地址

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

Address Name: HQ

IP Address/Domain Name:

IP/Netmask: (选择), 200.1.1.1/32

Zone: Untrust

3. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 195.1.1.254

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), HQ

Service: ANY

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

(DIP on): 5 (211.10.1.1-211.10.1.1)/X-late

WebUI (分支机构 B)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 201.1.1.1/24

Interface Mode: Route

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

ID: 5

IP Address Range: 211.20.1.1 ~ 211.20.1.1

Port Translation: (选择)

Extended IP/Netmask: 211.20.1.10/255.255.255.0

2. 地址

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

Address Name: HQ

IP Address/Domain Name:

IP/Netmask: (选择), 200.1.1.1/32

Zone: Untrust

3. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 201.1.1.254

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), HQ

Service: ANY

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP On: (选择), 5 (211.20.1.1-211.20.1.1)/X-late

CLI (分支机构 A)

1. 接口

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

set interface ethernet3 zone untrust
set interface ethernet3 ip 195.1.1.1/24
set interface ethernet3 rout
set interface ethernet3 ext ip 211.10.1.10 255.255.255.0 dip 5 211.10.1.1
```

2. 地址

```
set address untrust hq 200.1.1.1/32
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 195.1.1.254
```

4. 策略

```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

CLI (分支机构 B)

1. 接口

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

set interface ethernet3 zone untrust
set interface ethernet3 ip 201.1.1.1/24
set interface ethernet3 route
set interface ethernet3 ext ip 211.20.1.10 255.255.255.0 dip 5 211.20.1.1
```

2. 地址

```
set address untrust hq 200.1.1.1/32
```

3. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.1.1.254
```

4. 策略

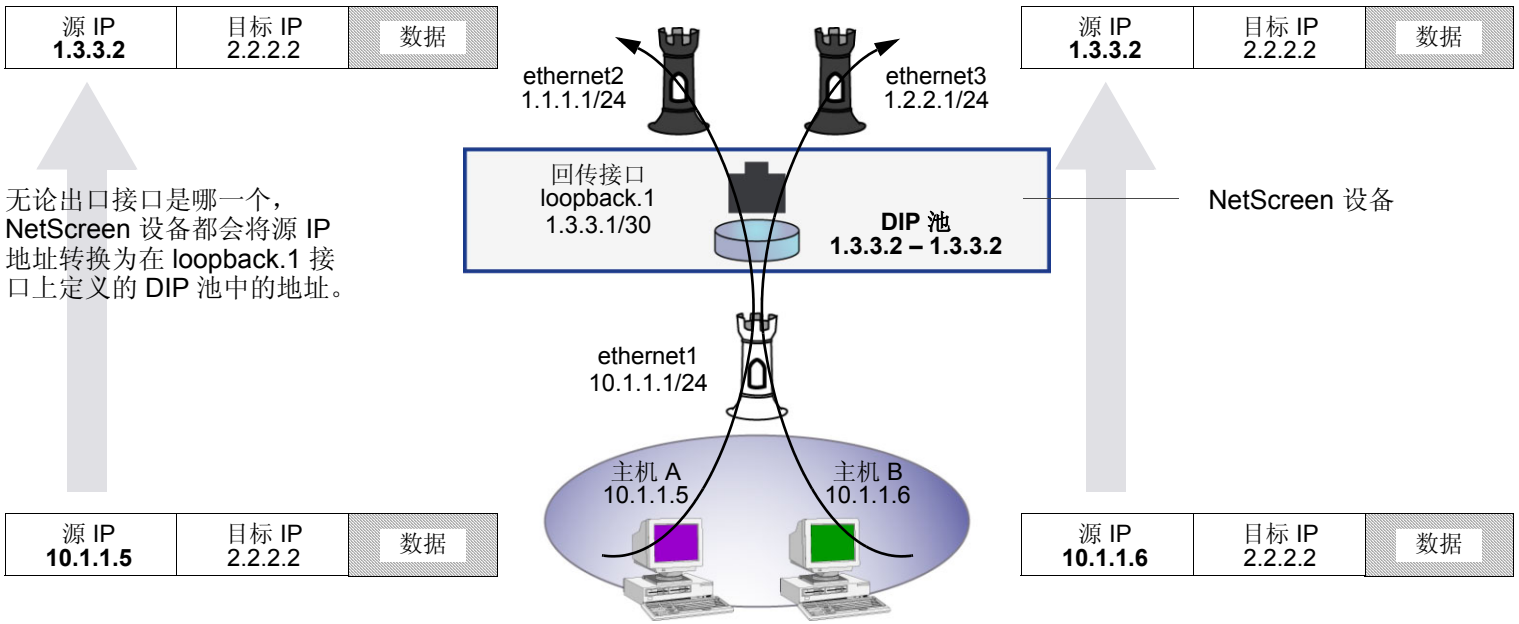
```
set policy from trust to untrust any any any permit
set policy top from trust to untrust any hq any nat src dip 5 permit
save
```

回传接口和 DIP

回传接口是一个逻辑接口，只要其所在的设备开启，该接口就始终处于工作状态[12]。可以在回传接口上创建一个动态 IP (DIP) 地址池，从而在执行源地址转换时，属于其相关回传接口组的接口组可访问该池。 NetScreen 设备从此类 DIP 池中提取的地址与回传接口 IP 地址处于相同的子网内，而不是在任何成员接口的子网中。(请注意， DIP 池中的地址不能与接口 IP 地址或任何已在回传接口定义的 MIP 地址重叠。)

在 DIP 池中设置回传接口的主要应用是将源地址转换为相同地址或地址范围，尽管不同的数据包可能会使用不同的出口接口。

使用回传接口上的 DIP 池转换源地址



12. 有关回传接口的信息，请参阅第 74 页上的 “回传接口”。

范例：回传接口上的 DIP

在本例中，NetScreen 设备将从两个不同的互联网服务提供商 ISP-1 和 ISP-2 处接收来自两个 Untrust 区段接口的下列 IP 地址：

- ethernet2, 1.1.1.1/24, ISP-1
- ethernet3, 1.2.2.1/24, ISP-2

将这些接口绑定到 Untrust 区段，然后为其分配上述 IP 地址。还需要将 ethernet1 绑定到 Trust 区段并为其分配 IP 地址 10.1.1.11/24。

您希望 NetScreen 设备将 Trust 区段内出站信息流中的源地址转换为 Untrust 区段中的远程办公室。转换的地址必须是相同的 IP 地址 (1.3.3.2)，因为远程办公室的策略仅允许来自该 IP 地址的入站信息流。您先前已经获得公共 IP 地址 1.3.3.1 和 1.3.3.2 并已通知两个 ISP: 除使用他们为设备分配的地址外，也将使用这些地址。

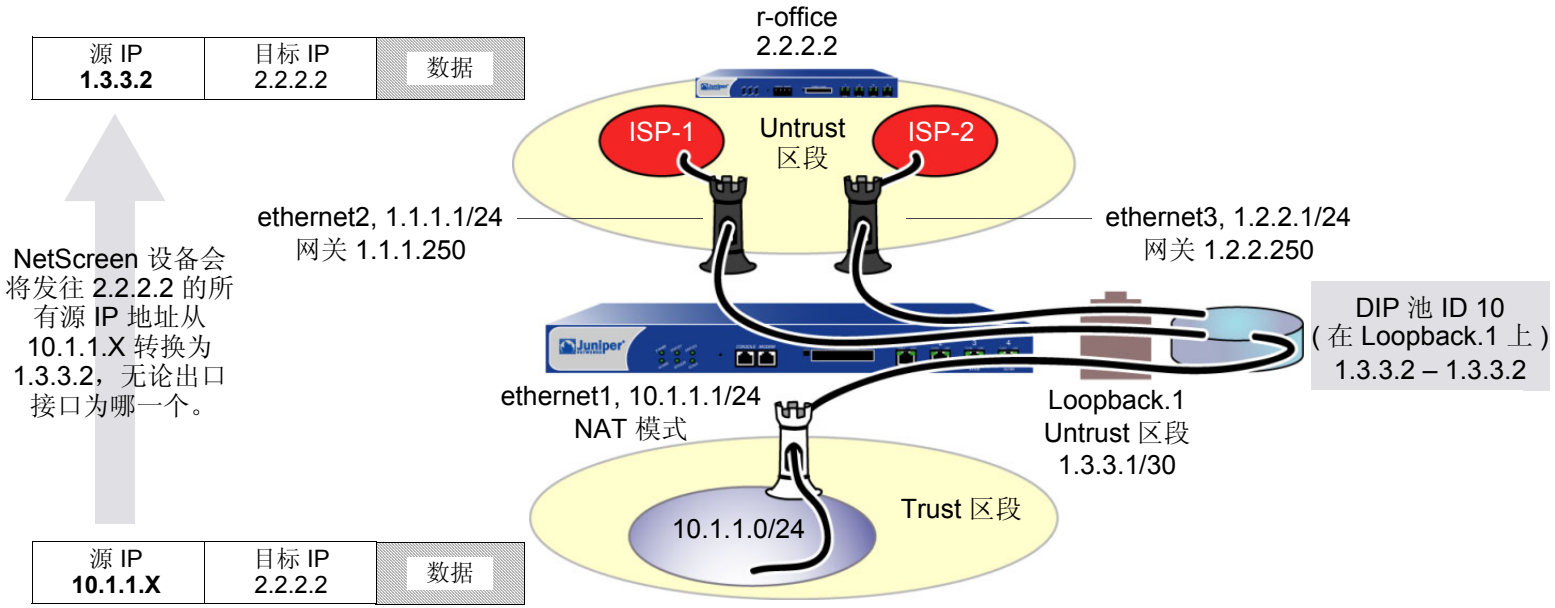
用 IP 地址 1.3.3.1/30 配置回传接口 loopback.1，用 1.3.3.2 – 1.3.3.2 配置该接口上的 DIP 池。DIP 池的 ID 号为 10。然后，将 ethernet1 和 ethernet2 加入 loopback.1 回传组，使其成为该组成员。

为名为 “r-office” 的远程办公室定义 IP 地址 2.2.2.2/32，并为分别指向 ISP-1 和 ISP-2 路由器的 ethernet1 和 ethernet2 接口定义缺省路由。

为出站信息流定义要使用的两个网关路由。由于对这两个路由未定义优先选择，因此将不在其中加入任何度量。出站信息流可能会流向任一个路由[13]。

最后，创建一个策略，该策略应用源网络地址转换 (NAT-src) 将出站信息流转换为远程办公室。策略将引用 DIP 池 ID 10。

13. 要指出路由优先级 (即将度量加入两个路由中)，请给首选路由较高的度量 (即比较接近 1 的一个数值)。



WebUI

1. 接口

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

Interface Name: loopback.1
Zone: Untrust (trust-vr)
IP Address/Netmask: 1.3.3.1/30

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

As member of loopback group: loopback.1
Zone Name: Trust
Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24
Interface Mode: NAT

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

As member of loopback group: loopback.1

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Interface Mode: Route

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Interface Mode: Route

2. DIP 池

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

ID: 5

IP Address Range: 1.3.3.2 ~ 1.3.3.2

Port Translation: (选择)

3. 地址

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

Address Name: r-office

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.2/32

Zone: Untrust

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet2

Gateway IP address: 1.1.1.250

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP address: 1.2.2.250

5. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), r-office

Service: ANY

Action: Permit

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

NAT:

Source Translation: (选择)

DIP On: (选择), 10 (1.3.3.2-1.3.3.2)/port-xlate

CLI

1. 接口

```
set interface loopback.1 zone untrust
set interface loopback.1 ip 1.3.3.1/30

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

set interface ethernet2 zone untrust
set interface ethernet2 ip 1.1.1.1/24
set interface ethernet2 loopback-group loopback.1

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.2.2.1/24
set interface ethernet3 loopback-group loopback.1
```

2. DIP 池

```
set interface loopback.1 dip 10 1.3.3.2 1.3.3.2
```

3. 地址

```
set address untrust r-office 2.2.2.2/32
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet2 gateway 1.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.2.2.250
```

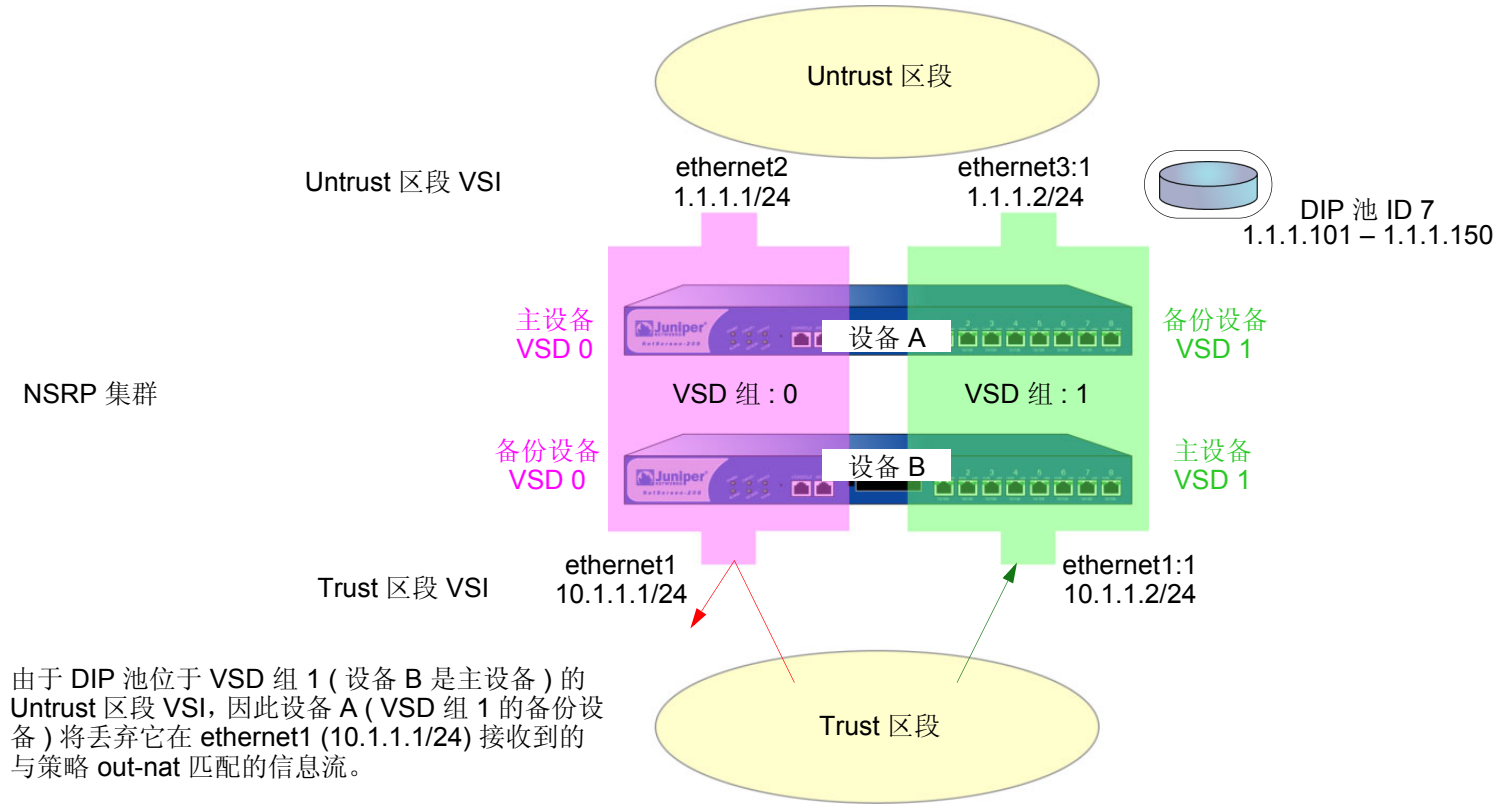
5. 策略

```
set policy from trust to untrust any r-office any nat src dip-id 10 permit
save
```

DIP 组

当您将两个 NetScreen 设备组成一个冗余集群以提供双主动配置的高可用性 (HA) 时，这两个设备将共享同一配置并且同时处理信息流。定义使用 DIP 池 (位于一个 VSI 上) 来执行网络地址转换 (NAT) 的策略时，可能会出现问题。因为仅当 NetScreen 设备作为绑定 VSI 的 VSD 组的主设备时该 VSI 才处于活动状态，因此任何发送到其它 NetScreen 设备 (作为该 VSD 组的备份设备) 的信息流都将无法使用该 DIP 池而被丢弃。

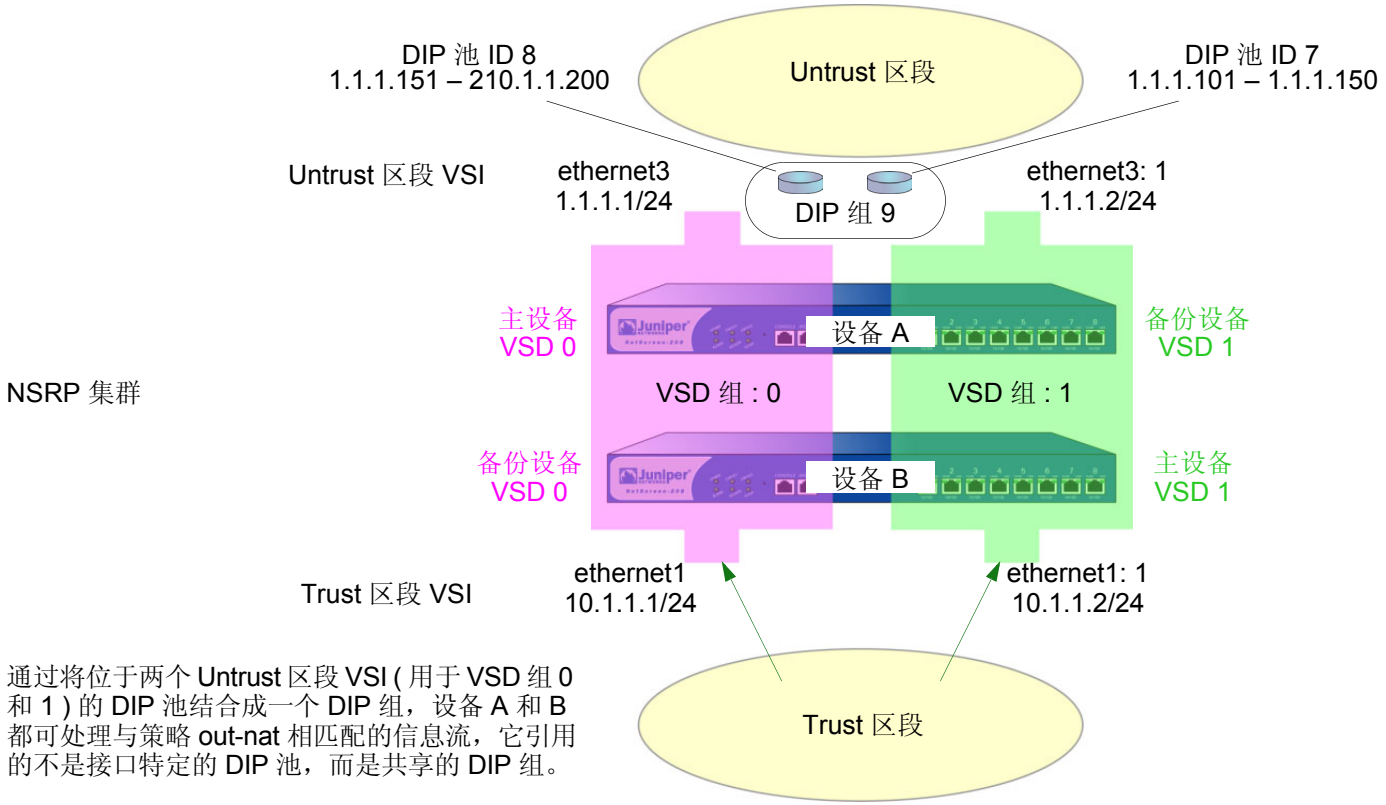
在 NSRP 集群中时，不当使用 DIP 池的策略 :
set policy name out-nat from trust to untrust any any any nat src dip-id 7 permit



由于 DIP 池位于 VSD 组 1 (设备 B 是主设备) 的 Untrust 区段 VSI，因此设备 A (VSD 组 1 的备份设备) 将丢弃它在 ethernet1 (10.1.1.1/24) 接收到的与策略 out-nat 匹配的信息流。

为了解决此问题，需要创建两个 DIP 池 (一个在各个 VSD 组的 Untrust 区段 VSI 上)，然后将两个 DIP 池结合成一个 DIP 组并在策略中加以引用。即使策略指定 DIP 组，每个 VSI 仍使用其自己的 VSD 池。

在 NSRP 集群中时，策略中 DIP 组的推荐用法 :
set policy name out-nat from trust to untrust any any any nat dip-id 9 permit



通过将位于两个 Untrust 区段 VSI (用于 VSD 组 0 和 1) 的 DIP 池结合成一个 DIP 组，设备 A 和 B 都可处理与策略 out-nat 相匹配的信息流，它引用的不是接口特定的 DIP 池，而是共享的 DIP 组。

***注意：**有关为 HA 设置 NetScreen 设备的详细信息，请参阅第 10 卷，“高可用性”。*

范例 : DIP 组

在本例中，将在双活动 HA 对的两个 NetScreen 设备 (设备 A 和 B) 上提供 NAT 服务。

将创建两个 DIP 池 — ethernet3 上的 DIP 5 (1.1.1.20 –1.1.1.29)，ethernet3:1 上的 DIP 6 (1.1.1.30 –1.1.1.39)。然后将它们组合成一个 DIP 组并标识为 DIP 7 并在策略中加以引用。

VSD 组 0 和 1 的 VSI 如下 :

- Untrust 区段 VSI ethernet3 1.1.1.1/24 (VSD 组 0)
- Untrust 区段 VSI ethernet3:1 1.1.1.2/24 (VSD 组 1)
- Trust 区段 VSI ethernet1 10.1.1.1/24 (VSD 组 0)
- Trust 区段 VSI ethernet1:1 10.1.1.1/24 (VSD 组 1)

本例假设已在 NSRP 集群中建立了设备 A 和 B、创建了 VSD 组 1 (将设备置入 NSRP 集群时，NetScreen 将自动创建 VSD 组 0) 并对上述接口进行了配置。 (有关为 NSRP 配置 NetScreen 设备的信息，请参阅第 10 卷，“高可用性”。)

WebUI

1. DIP 池

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

   ID: 5

   IP Address Range: 1.1.1.20 – 1.1.1.29

   Port Translation: (选择)

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

   ID: 6

   IP Address Range: 1.1.1.30 – 1.1.1.39

   Port Translation: (选择)

   注意：*本版发行时，只能通过 CLI 定义 DIP 组。*

2. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

NAT:

Source Translation: (选择)

DIP On: (选择), 7

CLI

1. DIP 池

```
set interface ethernet3 dip 5 1.1.1.20 1.1.1.29
set interface ethernet3:1 dip 6 1.1.1.30 1.1.1.39
```

2. DIP 组

```
set dip group 7 member 5
set dip group 7 member 6
```

3. 策略

```
set policy from trust to untrust any any any nat src dip-id 7 permit
save
```

时间表

时间表是一个可配置的对象，它可与一个或多个策略相关联以定义策略生效的时间。通过应用时间表，可以控制网络信息流量并加强网络安全。

定义时间表时，请输入下列参数的值：

Schedule Name: 出现在 Policy Configuration 对话框的 Schedule 下拉列表中的名称。请选择描述性的名称以帮助识别时间表。名称必须是唯一的，并且限制在 19 个字符以内。

Comment: 要添加的任何额外信息。

Recurring: 在希望时间表每周重复时启用此项。

Start and End Times: 必须配置开始和结束时间。同一天内最多可指定两个时间段。

Once: 希望时间表只开始和结束一次时启用此项。

mm/dd/yyyy hh:mm: 必须输入开始和停止的日期和时间。

范例：循环时间表

在本例中，有一个名为 Tom 的短期职员，他在下班后使用公司的互联网进行私人访问。您可以创建一个非上班时间的时间表，然后关联策略，以拒绝发自该职员计算机 (10.1.1.5/32) 的正常上班时间以外的出站 TCP/IP 信息流。

WebUI

1. 时间表

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

   Schedule Name: After Hours

   Comment: For non-business hours

   Recurring: (选择)

时段 1:

Week Day	Start Time	End Time
Sunday	00:00	23:59
Monday	00:00	06:00
Tuesday	00:00	06:00
Wednesday	00:00	06:00
Thursday	00:00	06:00
Friday	00:00	06:00
Saturday	00:00	23:59

时段 2:

Week Day	Start Time	End Time
Sunday	17:00	23:59
Monday	17:00	23:59
Tuesday	17:00	23:59
Wednesday	17:00	23:59
Thursday	17:00	23:59
Friday	17:00	23:59
Saturday	17:00	23:59

2. 地址

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

Address Name: Tom

Comment: Temp

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 策略

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

Name: No Net

Source Address:

Address Book Entry: (选择), Tom

Destination Address:

Address Book Entry: (选择), Any

Service: HTTP

Action: Deny

Schedule: After Hours

CLI

1. 时间表

```
set schedule “after hours” recurrent sunday start 00:00 stop 23:59
set schedule “after hours” recurrent monday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule “after hours” recurrent tuesday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule “after hours” recurrent wednesday start 00:00 stop 06:00 start
    17:00 stop 23:59
set schedule “after hours” recurrent thursday start 00:00 stop 06:00 start
    17:00 stop 23:59
set schedule “after hours” recurrent friday start 00:00 stop 06:00 start 17:00
    stop 23:59
set schedule “after hours” recurrent saturday start 00:00 stop 23:59 comment
    “for non-business hours”
```

2. 地址

```
set address trust tom 10.1.1.5/32 “temp”
```

3. 策略

```
set policy from trust to untrust tom any http deny schedule “after hours”
save
```

6

策略

NetScreen 设备的缺省行为是拒绝安全区段间的所有信息流 (区段间信息流)[1] (Untrust 区段内的信息流除外)，并允许绑定到同一区段的接口间的所有信息流 (区段内部信息流)。为了允许选定的区段间信息流通过 NetScreen 设备，必须创建覆盖缺省行为的区段间策略。同样，为了防止选定的区段内部信息流通过 NetScreen 设备，必须创建区段内部策略。

本章介绍各种策略的功能以及组成策略的不同元素是如何关联的。本章分为以下几个部分：

1. 在缺省情况下， NetScreen-5XP 和 NetScreen-5XT 允许从 Trust 区段到 Untrust 区段的信息流。

- 第 337 页上的 “修改和禁用策略”
- 第 338 页上的 “策略验证”
- 第 339 页上的 “重新排序策略”
- 第 340 页上的 “移除策略”

***注意：**如果在 NetScreen 设备上配置组播路由，则必须配置组播策略。有关组播策略的详细信息，请参阅第 **6** -202 页上的 “组播策略”。*

基本元素

策略可允许、拒绝两点间指定类型的单向信息流或对该信息流执行通道[2] 动作。信息流类型 (或 “服务”)、两端点的位置以及所调用的动作构成了策略的基本元素。尽管可以有其它组件，但是共同构成策略核心部分的必要元素如下 :

- Direction – 两个安全区段间信息流的方向 (从源区段到目标区段)
- Source address – 信息流发起的地址
- Destination address – 信息流发送到的地址
- Service – 所传输信息流的类型
- Action – NetScreen 设备接收到满足前四个标准的信息流时所执行的动作，这些动作为 : deny、 permit、reject 或 tunnel

例如，在下列 CLI 命令中声明的策略允许 FTP 信息流从 Trust 区段中的任何地址流向 DMZ 区段中名为 “server1” 的 FTP 服务器 :

set policy from trust to untrust any server1 ftp permit

- Direction: **from trust to untrust** (即从 Trust 区段到 Untrust 区段)
- Source Address: **any** (即 Trust 区段中的任何地址。术语 “any” 代表应用到区段中任何地址的预定义地址)
- Destination Address: **server1** (Untrust 区段通讯簿中用户定义的地址)
- Service: **ftp** (文件传输协议)
- Action: **permit** (NetScreen 设备允许此信息流通过其防火墙)

2. “tunnel” 动作 (VPN 或 L2TP 通道)，隐含 “permit” 的概念。

三种类型的策略

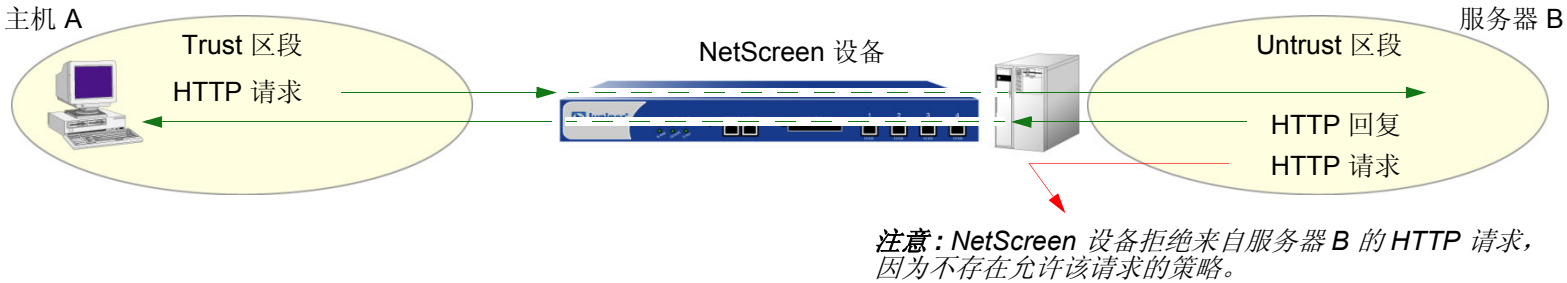
可通过以下三种策略控制信息流的流动：

- 通过创建区段间策略，可以控制允许其从一个安全区段流向另一个安全区段的信息流。
- 通过创建区段内部策略，也可控制允许其通过绑定到同一区段的接口的信息流。
- 通过创建全局策略，可以控制地址间的信息流，而不必考虑它们的安全区段。

区段间策略

区段间策略提供安全区段间信息流的控制。可通过设置区段间策略来拒绝、允许、丢弃从一个区段到另一个区段的信息流或对该信息流执行通道动作。NetScreen 设备通过使用状态式检查技术来维护活动 TCP 会话表和活动 UDP 伪会话表，以便允许对服务请求的回复。例如，如果有一个策略允许从 Trust 区段中的主机 A 到 Untrust 区段中的服务器 B 的 HTTP 请求，则当 NetScreen 设备接收到从服务器 B 到主机 A 的 HTTP 回复时， NetScreen 设备将接收到的数据包与它的表进行对照检查。当发现数据包为某个已批准 HTTP 请求的回复时，NetScreen 设备即允许该来自 Untrust 区段中服务器 B 的数据包穿越防火墙到达 Trust 区段中的主机 A。要允许由服务器 B 发起的流向主机 A 的信息流 (不只是回复由主机 A 发起的信息流)，必须再创建一个从 Untrust 区段中服务器 B 到 Trust 区段中主机 A 的策略。

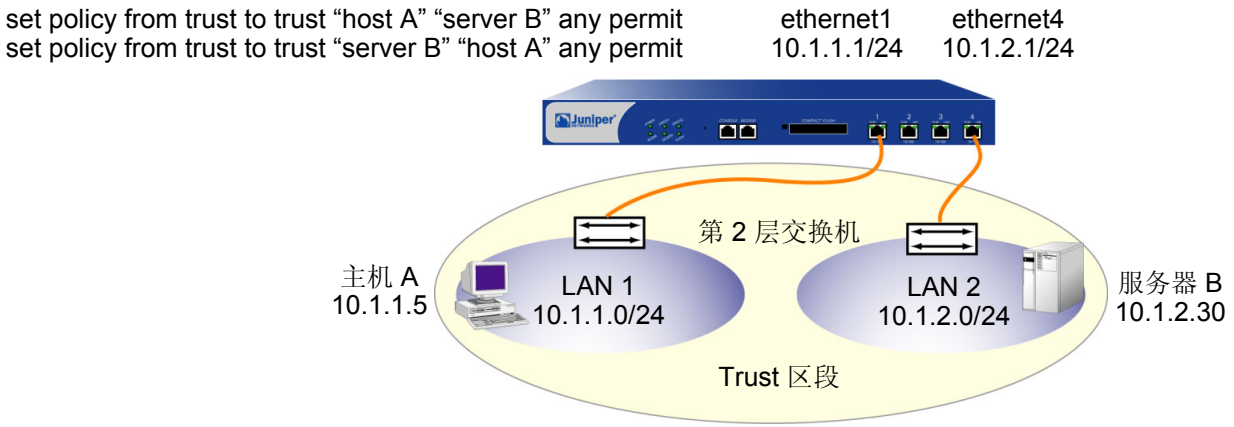
set policy from trust to untrust “host A” “server B” http permit



***注意：** NetScreen 设备拒绝来自服务器 B 的 HTTP 请求，因为不存在允许该请求的策略。*

区段内部策略

区段内部策略提供对绑定到同一安全区段的接口间信息流的控制。源地址和目标地址都在同一安全区段中，但是通过 NetScreen 设备上的不同接口到达。与区段间策略一样，区段内部策略也控制信息流的单向流动。要允许从数据路径任一端发起的信息流，必须创建两个策略，即为每个方向各创建一个策略。



在接口级设置时 (**set interface** *interface* **nat**)，区段内部策略不支持 VPN 通道或源网络地址转换 (NAT-src)。但是，区段内部策略支持基于策略的 NAT-src 和 NAT-dst。当策略将映射 IP (MIP) 引用为目标地址时，它们还支持目标地址转换。 (有关 NAT-src、 NAT-dst 和 MIP 的信息，请参阅第 7 卷，“地址转换”。)

全局策略

与区段间策略和区段内部策略不同，全局策略不引用特定的源区段和目标区段。全局策略引用用户定义的 Global 区段地址或预定义的 Global 区段地址 “any”。这些地址可以跨越多个安全区段。例如，如果要提供对多个区段的访问或从多个区段进行访问，则可以创建具有 Global 区段地址 “any” 的全局策略，它包含所有区段中的所有地址。

注意：*本版发行时，全局策略不支持源网络地址转换 (NAT-src)、VPN 通道或“透明”模式。不过，可以将 MIP 或 VIP 指定为全局策略中的目标地址。*

策略组列表

NetScreen 设备维护三种不同的策略组列表，每种策略组列表对应于以下三种策略之一：

- 区段间策略
- 区段内部策略
- 全局策略

NetScreen 设备接收到发起新会话的数据包时，将记录入口接口，从而获知该接口所绑定的源区段。然后 NetScreen 设备执行路由查询以确定出口接口，从而确定该接口所绑定的目标区段。使用源区段和目标区段， NetScreen 设备可以执行策略查找，按以下顺序查阅策略组列表：

1. 如果源区段和目标区段不同，则 NetScreen 设备在区段间策略组列表中执行策略查找。

   (或)

   如果源区段和目标区段相同，则 NetScreen 设备在区段内部策略组列表中执行策略查找。

2. 如果 NetScreen 设备执行了区段间或区段内部策略查找，但是没有找到相匹配的策略，则 NetScreen 设备会检查全局策略组列表以查找匹配策略。
3. 如果 NetScreen 设备执行了区段间和全局策略查找，但是没有找到相匹配的策略，则 NetScreen 设备会将缺省的允许 / 拒绝策略应用到数据包：**unset/set policy default-permit-all**。

   (或)

   如果 NetScreen 设备执行了区段内部和全局策略查找，但是没有找到相匹配的策略，则 NetScreen 设备会将该区段的区段内部阻塞设置应用到数据包：**unset/set zone** *zone* **block**。

NetScreen 设备从上至下搜索每个策略组列表。因此，必须在列表中将较为特殊的策略置于不太特殊的策略的上面。(有关策略顺序的信息，请参阅第 339 页上的 “重新排序策略”。)

定义的策略

防火墙提供具有单个进入和退出点的网络边界。由于所有信息流都必须通过此点，因此可以通过执行策略 (区段间策略、区段内部策略和全局策略) 组列表来筛选并引导这些信息流。

策略能拒绝、允许、丢弃 (拒绝并向源主机发送一个 TCP RST 或 ICMP 端口不可到达的消息)、加密和解密、认证、排定优先次序、调度、过滤以及监控尝试从一个安全区段流向另一个安全区段的信息流。可以决定哪些用户和数据能进出，以及它们进出的时间和地点。

***注意：** 对于支持虚拟系统的 NetScreen 设备，根系统中的策略组不影响虚拟系统中的策略组。*

策略和规则

单个用户定义的策略内部生成一个或多个逻辑规则，而每个逻辑规则都由一组组件 (源地址、目标地址和服务) 组成。组件占用内存资源。引用组件的逻辑规则不占用内存资源。

依据对策略中源地址、目标地址和服务组件的多个条目或组的使用情况，逻辑规则的数量可能要比创建单个策略时显而易见的逻辑规则数量大得多。例如，以下策略产生 125 个逻辑规则 :

1 个策略 : 5 个源地址 x 5 个目标地址 x 5 个服务 = 125 个逻辑规则

但是， NetScreen 设备不为每个逻辑规则复制组件。规则以不同的组合使用同一组组件。例如，产生 125 个逻辑规则的上述策略仅有 15 个组件 :

5 个源地址 + 5 个目标地址 + 5 个服务 = 15 个组件

这 15 个组件以不同方式组合，生成 125 个由单个策略产生的逻辑规则。允许多个逻辑规则以不同组合使用同一组组件，与每个逻辑规则与其组件具有一对一关系相比， NetScreen 设备占用的资源少得多。

由于新策略的安装时间与 NetScreen 设备添加、删除或修改的组件数量成比例，因此组件较少时策略的安装更快。同样，与每个规则都需要专用组件相比，通过允许大量的逻辑规则共享一小组组件， NetScreen 使用户能创建更多的策略， NetScreen 设备能创建更多的规则。

策略的结构

策略必须包含下列元素：

- ID (自动生成的，但可能是 CLI 中用户定义的)
- 区段 (源区段和目标区段)
- 地址 (源地址和目标地址)
- 服务
- 动作 (deny、 permit、 reject、 tunnel)

策略也可包含下列元素：

- 应用
- 名称
- VPN 通道
- L2TP 通道
- 深入检查
- 放置在策略列表的顶部
- 源地址转换
- 目标地址转换
- 用户认证
- HA 会话备份
- URL 过滤
- 记录
- 计数
- 信息流报警临界值
- 时间表
- 防病毒扫描
- 信息流整形

本节的余下部分将依次分析上述每一元素。

ID

不管是您定义还是 NetScreen 设备自动分配，每个策略都具有一个 ID 号。您只能通过 CLI 中的设置策略命令为策略定义一个 ID 号：**set policy id** *number...* 一旦知道了该 ID 号，即可输入策略环境以发出修改策略的其它命令。（有关策略环境的详细信息，请参阅第 331 页上的 “输入策略环境”。）

区段

区段可以是网络空间中应用了安全措施的部分（安全区段）、绑定了 VPN 通道接口的逻辑部分（通道区段），或者是执行特定功能的物理或逻辑实体（功能区段）。策略允许信息流在两个安全区段之间流动（区段间策略），或在两个绑定到同一区段的接口间流动（区段内部策略）。（有关详细信息，请参阅第 29 页上的 “区段”、第 296 页上的 “区段间策略”和第 297 页上的 “区段内部策略”。）

地址

地址是通过相对于防火墙（在一个安全区段中）的位置来识别网络设备（如主机和网络）的对象。单个主机使用掩码 255.255.255.255 指定，表示所有 32 位地址都有意义。网络使用其子网掩码指定，指示有意义的位数。要为特定地址创建策略，必须首先在通讯簿中创建相关主机和网络的条目。

也可创建地址组，并将策略应用到地址组，就象应用到其它通讯簿条目一样。将地址组用作策略的元素时，应注意由于 NetScreen 设备将策略应用到组中的每个地址，可用的内部逻辑规则数和组成这些规则的组件数将会比预期更快耗尽。源地址和目标地址都使用地址组时尤其危险。（有关详细信息，请参阅第 299 页上的 “策略和规则”。）

服务

服务是使用第 4 层信息（如应用程序服务 Telnet、FTP、SMTP 和 HTTP 的标准和接受的 TCP 和 UDP 端口号）识别应用程序协议的对象。 ScreenOS 包括预定义的核心互联网服务。另外，还可以定义定制服务。

可以定义策略，指定允许、拒绝、加密、认证、记录或统计哪些服务。

动作

动作是描述防火墙如何处理接收到的信息流的对象。

- **Deny** 阻塞数据包，使之不能通过防火墙。
- **Permit** 允许数据包通过防火墙。
- **Reject** 阻塞数据包，使之不能通过防火墙。 NetScreen 设备丢弃数据包，并且对于 TCP 信息流发送一个 TCP 重置 (RST) 段给源主机[3]，对于 UDP 信息流发送一个 ICMP “destination unreachable, port unreachable”消息 (类型 3，代码 3)。对于不同于 TCP 和 UDP 类型的信息流， NetScreen 设备将丢弃数据包而不通知源主机，当动作为 “deny”时也会发生此种情况。

  注意：*当入口接口在第 2 层或第 3 层运行且协议为 TCP 时， TCP RST 中的源 IP 地址是初始 (丢弃的) 数据包中的目的 IP 地址。当入口接口在第 2 层运行且协议为 UDP 时， ICMP 消息中的源 IP 地址也是初始数据包中的目标 IP 地址。但是，当入口接口在第 3 层运行且协议为 UDP 时， ICMP 消息中的源 IP 地址是入口接口的源 IP 地址。*

- **Tunnel** 封装外向 IP 数据包和解封内向 IP 数据包。对于 IPSec VPN 通道，指定要使用哪个 VPN 通道。对于 L2TP 通道，指定要使用哪个 L2TP 通道。对于 IPSec 上的 L2TP，指定一个 IPSec VPN 通道和一个 L2TP 通道[4]。

NetScreen 设备将指定动作应用到与预先提供的标准匹配的信息流，这些标准为 : 区段 (源区段和目标区段)、地址 (源地址和目标地址) 以及服务。

3. NetScreen 设备在接收 (并丢弃) 一个带有不同于另一个 RST 的任意代码位设置的 TCP 段之后发送一个 TCP RST。
4. 对于 IPSec 上的 L2TP， IPSec VPN 通道的源地址和目标地址必须与 L2TP 通道的源地址和目标地址相同。

应用

应用选项指定映射到策略中引用的第 4 层服务的第 7 层应用。预定义服务已经有到第 7 层应用的映射。不过，对于定制服务，必须将服务明确链接到某个应用，尤其是希望策略将应用层网关 (ALG[5]) 或 “深入检查”应用于定制服务时。

将 ALG 应用于定制服务包括以下两个步骤 :

- 使用名称、超时值、传输协议和源端口及目标端口定义定制服务
- 配置策略时，引用该服务和希望应用的 ALG 的应用类型

有关将 “深入检查”应用于定制服务的信息，请参阅第 **4** -173 页上的 “将定制服务映射到应用程序”。

名称

可以给策略一个描述性的名称，便于识别该策略。

注意 : *有关 ScreenOS 命名约定 (适用于为策略创建的名称) 的信息，请参阅第 xii 页上的 “命名约定和字符类型”。*

VPN 通道

可以将单个或多个策略应用到已配置的任何 VPN 通道。在 WebUI 中， VPN Tunnel 选项提供所有这些通道的下拉列表。在 CLI 中，可以用 **get vpn** 命令查看所有可用的通道。 (有关详细信息，请参阅第 **5** -99 页上的 “站点到站点 VPN”和第 **5** -230 页上的 “拨号 VPN”。)

当 VPN 通道两端的 VPN 配置都使用基于策略的 NAT 时，两个网关设备的管理员都需要创建入站和出站策略 (总共四个策略)。当 VPN 策略构成匹配对 (即，除源地址和目标地址反向外，入站和出站策略配置中的任何内容都相同) 时，可以配置一个策略，然后选中 **Modify matching bidirectional VPN policy** 复选框，自动为相反方向创建第二个策略。对于新策略的配置，默认情况下，不选中 matching VPN policy 复选框。对于是匹配对成员的现有策略的修改，在缺省情况下，复选框被选中，并且对一个策略所作的更改会传播到另一个策略。

注意 : *此选项只能通过 WebUI 获得。以下任一策略组件若有多个条目时不可用 : 源地址、目标地址或服务。*

5. NetScreen 支持多个服务的 ALG，包括 DNS、 FTP、 H.323、 HTTP、 RSH、 SIP、 telnet 和 TFTP。

L2TP 通道

可以将单个或多个策略应用到已配置的任何 “第 2 层通道协议 (L2TP)” 通道。在 WebUI 中， L2TP 选项提供所有这些通道的下拉列表。在 CLI 中，您可以使用 **get l2tp** *tunn_str* **active** 命令显示活动 L2TP 通道的状态，也可以使用 **get l2tp all** 命令查看所有可用通道。也可以将 VPN 通道和 L2TP 通道组合在一起 (如果两者都具有相同的端点)，创建结合每个通道特征的通道。这称为 IPSec 上的 L2TP。

***注意：** 处于透明模式的 NetScreen 设备不支持 L2TP。*

深入检查

“深入检查” 是用于过滤网络和 “传输层” 允许的信息流的机制，不仅检查这些层，而且检查 “应用层”[6] 的内容和协议特征。“深入检查” 的目的是检测和防护任何攻击或异常行为，它们可能存在于 NetScreen 防火墙允许的信息流中。

要为攻击保护配置策略，必须进行两项选择 : 要使用的攻击组和要采取的攻击动作 (如果检测到了攻击)。(有关详细信息，请参阅第 **4** -131 页上的 “深入检查”。)

放置在策略列表的顶部

在缺省情况下，NetScreen 将最近创建的策略定位在策略组列表的底部。如果需要重新定位策略，可以使用在第 339 页上的 “重新排序策略”中说明的任一策略重新排序方法。为了避免执行将最近创建的策略重新定位到策略列表顶部这一额外步骤，可以在 WebUI 中选择 **Position at Top** 选项，或在 CLI 中的 **set policy** 命令中使用关键字 **top** (**set policy top …**)。

6. 在 “开放式系统互连” (OSI) 模式中，“网络层” 是第 3 层，“传输层” 是第 4 层，“应用层” 是第 7 层。OSI 模式是网络业在网络协议体系结构方面的标准模式。 OSI 模式由七层组成。

源地址转换

可以在策略级应用源地址转换 (NAT-src)。使用 NAT-src，可以转换内向或外向网络和 VPN 信息流中的源地址。新的源地址可以来自动态 IP (DIP) 池或出口接口。NAT-src 还支持源端口地址转换 (PAT)。要了解所有可用的 NAT-src 选项，请参阅第 **7**-15 页上的 “源网络地址转换”。

注意：*还可在接口级执行源地址转换，称为网络地址转换 (NAT)。有关接口级 NAT-src 或只是 NAT 的信息，请参阅第 122 页上的 “NAT 模式”。*

目标地址转换

可以在策略级应用目标地址转换 (NAT-dst)。使用 NAT-dst，可以转换内向或外向网络和 VPN 信息流中的目标地址。NAT-dst 还支持目标端口映射。要了解所有可用的 NAT-dst 选项，请参阅第 **7**-33 页上的 “目标网络地址转换”。

用户认证

若选择了此选项，则在允许信息流穿越防火墙或进入 VPN 通道前，会要求源地址的 auth 用户通过提供用户名和密码的方式对其身份进行认证。 NetScreen 设备可使用本地数据库或外部 RADIUS、 SecurID 或 LDAP auth 服务器，执行认证检查。

注意：*如果要将需要认证的策略应用到 IP 地址的子网，则该子网中的每个 IP 地址都需要认证。*

如果主机支持多个 auth 用户帐户 (如运行 Telnet 的 Unix 主机)，则在 NetScreen 设备对第一个用户进行认证后，该主机的所有其它用户都可以继承第一个用户的权限，让信息流通过 NetScreen 设备而不必经过认证。

NetScreen 提供两种认证方案 :

- 运行时认证，在收到与启用认证的策略相匹配的 HTTP、 FTP 或 Telnet 信息流时， NetScreen 设备提示 auth 用户登录
- WebAuth，通过 NetScreen 设备发送信息流前，用户必须认证自己

运行时认证

运行时认证的过程如下 :

1. 当 auth 用户发送 HTTP、FTP 或 Telnet 连接请求到目标地址时，NetScreen 设备截取数据包并对其进行缓冲。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备认证 auth 用户的登录信息。

   如果认证成功，则在 auth 用户和目标地址间建立连接。

对于初始的连接请求，策略必须包括下列三个服务中的一项或所有服务 : Telnet、 HTTP 或 FTP。只有具有这些服务中的一个或所有服务的策略才能启动认证过程。可以在涉及用户认证的策略中使用以下任一服务 :

- Any (因为 “any” 包括所有三项必需的服务)
- Telnet、 FTP 或 HTTP。
- 包含所需服务的服务组，外加启动认证过程必需的三个服务中的一个或多个 (Telnet、 FTP 或 HTTP)。例如，可以创建名为 “Login” 的定制服务组，支持 FTP、 NetMeeting© 和 H.323 服务。然后，在创建策略时，指定服务为 “Login”。

对于成功认证后的任何连接，策略中指定的所有服务都有效。

注意 : *启用了认证的策略不支持将 DNS (端口 53) 作为服务。*

策略前检查认证 (WebAuth)

WebAuth 认证的过程如下 :

1. auth 用户建立到 WebAuth 服务器 IP 地址的 HTTP 连接。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备或外部 auth 服务器认证 auth 用户的登录信息。

   如果认证尝试成功，则 NetScreen 设备允许 auth 用户启动信息流，使其流向在强制通过 WebAuth 方法执行认证的策略中指定的目标位置。

注意 : *有关这两种用户认证方法的详细信息，请参阅第* ***8*** *-42 页上的 “在策略中引用 Auth 用户”。*

通过选择特定的用户组、本地或外部用户或组表达式，可以限制或扩展应用策略的 auth 用户的范围。(有关组表达式的信息，请参阅第 **8**-6 页上的 “组表达式”。) 如果在策略中没有引用 auth 用户或用户组 (在 WebUI 中，选择 **Allow Any** 选项)，则策略应用到指定 auth 服务器中的所有 auth 用户。

***注意：** NetScreen 用 auth 用户登录的主机的 IP 地址链接认证权限。如果 NetScreen 设备认证来自某 NAT 设备后主机的用户，且该 NAT 设备对所有 NAT 指派都使用同一个 IP 地址，则该 NAT 设备后其它主机的用户自动具有相同的权限。*

HA 会话备份

当两台 NetScreen 设备都在高可用性 (HA) 的 NSRP 集群中时，可以指定哪个会话要备份，哪个会话不要备份。对于不想备份的会话的信息流，应用 HA 会话备份选项禁用的策略。在 WebUI 中，清除 **HA Session Backup** 复选框。在 CLI 中，在 **set policy** 命令中使用 **no-session-backup** 参数。在缺省情况下， NSRP 集群中的 NetScreen 设备备份会话。

URL 过滤

URL 过滤，也称为 web 过滤，使您能管理互联网访问并阻止访问不合适的 web 内容。当您在策略中启用 URL 过滤时，必须配置以下 URL 过滤解决方案之一：

- 集成 URL 过滤，使用该解决方案时， NetScreen 设备将截取每个 HTTP 请求，然后基于被绑定到防火墙策略的 URL 过滤配置文件来确定是要允许还是阻塞对请求站点的访问。
- 重新定向 URL 过滤，使用该解决方案时， NetScreen 设备将 TCP 连接中的第一个 HTTP 请求发送给 Websense 服务器或 SurfControl 服务器，使您能够基于其 URL、域名和 IP 地址阻塞或允许对不同站点的访问。

***注意：** 有关 URL 过滤的详细信息，请参阅第 **4**-106 页上的 “URL 过滤”。*

记录

在策略中启用记录时， NetScreen 设备记录应用特定策略的所有连接。可通过 WebUI 或 CLI 查看日志。在 WebUI 中，单击 **Reports > Policies >**  (对于要查看其日志的策略)。在 CLI 中，使用 **get log traffic policy** *id_num* 命令。

注意：*有关查看日志和图表的详细信息，请参阅第* ***3****-73 页上的 “监控 NetScreen 设备”。*

计数

在策略中启用计数时，NetScreen 设备计算应用此策略的信息流的总字节数，并将信息记录在历史记录图表中。要在 WebUI 中查看策略的历史记录图表，请单击 **Reports > Policies >**  (对于要查看其信息流计数的策略)。

信息流报警临界值

可以设置当策略允许的信息流超过指定的每秒字节数、每分钟字节数 (或两者) 时触发警报的临界值。由于信息流报警要求 NetScreen 设备监控字节总数，因此还必须启用计数功能。

注意：*有关信息流报警的详细信息，请参阅第* ***3****-92 页上的 “流量报警”。*

时间表

通过将时间表与策略相关联，可以确定策略生效的时间。可以将时间表配置为循环生效，也可配置为单次事件。时间表为控制网络信息流的流动以及确保网络安全提供了强有力的工具。在稍后的一个范例中，如果您担心职员向公司外传输重要数据，则可设置一个策略，阻塞正常上班时间以外的出站 FTP-Put 和 MAIL 信息流。

在 WebUI 中，在 **Objects > Schedules** 部分中定义时间表。在 CLI 中，使用 **set schedule** 命令。

注意：*在 WebUI 中，已排定进度的策略如有灰色背景，表示当前时间不在定义的时间表内。已排定进度的策略活动时，背景为白色。*

防病毒扫描

某些 NetScreen 设备支持内部 AV 扫描器，可以配置此扫描器以过滤 FTP、 HTTP、 IMAP、 POP3 和 SMTP 信息流。如果嵌入的 AV 扫描器检测到病毒，将丢弃数据包，并向发起信息流的客户端发送消息，报告病毒。

注意：有关防病毒扫描的详细信息，请参阅第 4-81 页上的 “防病毒扫描”。

信息流整形

可以为每个策略设置控制和整形信息流的参数。信息流整形参数包括：

Guaranteed Bandwidth: 以千比特每秒 (kbps) 表示的保障吞吐量。低于此临界值的信息流以最高优先级通过，不受任何信息流管理或整形机制的限制。

Maximum Bandwidth: 以千比特每秒 (kbps) 表示的连接类型可用的安全带宽。超过此临界值的信息流被抑制并丢弃。

注意：建议不要使用低于 10 kbps 的额定值。低于此临界值的额定值会导致数据包被丢弃以及过多的重试，从而无法实现对信息流的管理。

Traffic Priority: 当信息流带宽处于保障带宽和最大带宽设定值之间时， NetScreen 设备将首先让较高优先级的信息流通过，并且只有在没有其它更高优先级的信息流时，才让较低优先级的信息流通过。有八个优先级。

DiffServ Codepoint Marking: 差异服务 (DiffServ) 是标记信息流在优先级层次结构中位置的系统。可以将八个 NetScreen 优先级映射到 DiffServ 系统中。在缺省情况下，NetScreen 系统中的最高优先级 (优先级 0) 映射到 DiffServ 字段 (请参阅 RFC 2474) 中的前三位 (0111)，或映射到 IP 数据包包头的 ToS 字节 (请参阅 RFC 1349) 的 IP 优先级字段中。NetScreen 系统中的最低优先级 (优先级 7) 映射到 ToS DiffServ 系统中的 (0000)。

注意：有关信息流管理和整形的更详细讨论，请参阅第 341 页上的 “信息流整形”。

要更改 NetScreen 优先级和 DiffServ 系统间的映射，请使用以下 CLI 命令 :

set traffic-shaping ip_precedence *number0 number1 number2 number3 number4 number5 number6 number7*

其中 *number0* 是优先级 0 (TOS DiffServ 系统中的最高优先级) 的映射， *number1* 是优先级 1 的映射，依次类推。

要将 IP 优先级包含到类选择器码点中 — 即，要把 DiffServ 字段的第二个三位置 0 并保证您使用 **ip_precedence** 设置的优先级被下游路由器保存并正确处理 — 请使用以下 CLI 命令 :

set traffic-shaping dscp-class-selector

注意 : *只能通过 CLI 来配置* ***set traffic-shaping dscp-class-selector*** *命令。*

策略应用

本节说明策略的管理：查看、创建、修改、排序和重新排序以及移除策略。

查看策略

要通过 WebUI 查看策略，请单击 **Policies**。通过从 **From** 和 **To** 下拉列表中选择区段名称，然后单击 **Go**，可以按源区段和目标区段分类显示策略。在 CLI 中，使用 **get policy** [**all** | **from** *zone* **to** *zone* | **global** | **id** *number*] 命令。

策略图标

查看策略列表时， WebUI 使用图标提供策略组件的图形化汇总。下表解释了策略页中使用的不同图标。

图标	功能	说明
	允许	NetScreen 设备通过应用该策略的所有信息流。
	拒绝	NetScreen 设备阻塞应用该策略的所有信息流。
	丢弃	NetScreen 设备阻塞应用该策略的所有信息流。NetScreen 设备丢弃数据包，并且对于 TCP 信息流发送一个 TCP 重置 (RST) 段给源主机，对于 UDP 信息流发送一个 ICMP “destination unreachable, port unreachable”消息 (类型 3，代码 3)。对于不同于 TCP 和 UDP 类型的信息流， NetScreen 设备将丢弃数据包而不通知源主机，当动作为“deny”时也会发生此种情况。
	策略级 NAT	NetScreen 设备对应用该策略的所有信息流都执行基于策略的源或目标网络地址转换 (NAT-src 或 NAT-dst)。
	封装以及解除封装	NetScreen 设备封装所有出站 VPN 信息流并解封应用该策略的所有入站 VPN 信息流。

图标	功能	说明
	双向 VPN 策略	存在相反方向的匹配 VPN 策略。
	认证	用户在启动连接时必须认证自己。
	防病毒	NetScreen 设备将应用该策略的所有信息流发送到其内部防病毒 (AV) 扫描器。
	深入检查	NetScreen 设备对应用该策略的所有信息流执行 “深入检查” (DI)。
	深入检查与防病毒	NetScreen 设备对应用该策略的所有信息流执行 “深入检查”和防病毒保护。
	URL 过滤	NetScreen 设备将应用该策略的所有信息流发送到一个外部 URL 过滤服务器。
	L2TP	NetScreen 设备封装所有出站 L2TP 信息流并解封应用该策略的所有入站 L2TP 信息流。
	记录	如果启用，则记录所有信息流，并使其可用于系统日志和电子邮件。
	计数	NetScreen 设备计算 (以字节为单位) 应用该策略的信息流的量。
	报警	当信息流总量超过您设定的临界值时， NetScreen 设备在该策略的信息流日志中创建一个条目。单击该图标可浏览到位于 “报告”部分的信息流日志。

创建策略

要允许信息流在两个区段之间流动，应创建策略以便在这些区段之间拒绝、允许、丢弃信息流或为信息流创建通道。如果 NetScreen 设备是唯一能够在源地址和目标地址 (策略中所引用的) 之间发送区段内部信息流的网络设备，则也可创建策略，控制同一区段内的信息流。也可创建全局策略，使用 Global 区段通讯簿中的源地址和目标地址。

要允许两个区段间 (例如， Trust 区段和 Untrust 区段) 的双向信息流，需要首先创建从 Trust 到 Untrust 的策略，然后再创建一个从 Untrust 到 Trust 的策略。根据需要，两个策略可以使用相同或不同的 IP 地址，只是源地址和目标地址需反向。

策略位置

可以在同一系统 (根系统或虚拟系统) 中的任意区段间定义策略。要在根系统和虚拟系统间定义策略，其中一个区段必须为共享区段。 (有关与虚拟系统有关的共享区段的信息，请参阅第 9 卷，“虚拟系统”。)

范例：区段间策略邮件服务

在本例中，将创建三个策略以控制电子邮件信息流的流动。

第一个策略允许 Trust 区段中的内部用户发送并检索来自 DMZ 区段中本地邮件服务器的电子邮件。此策略允许来自内部用户的服务 MAIL (即 SMTP) 和 POP3 穿越 NetScreen 防火墙到达本地邮件服务器。

第二个和第三个策略允许服务 MAIL 穿越 DMZ 区段中本地邮件服务器和 Untrust 区段中远程邮件服务器之间的防火墙。

不过，在创建策略来控制不同安全区段间信息流之前，必须首先设计应用这些策略的环境。第一，首先将接口绑定到区段并分配接口 IP 地址：

- 将 ethernet1 绑定到 Trust 区段并将其 IP 地址指派为 10.1.1.1/24。
- 将 ethernet2 绑定到 DMZ 区段并将其 IP 地址指派为 1.2.2.1/24。
- 将 ethernet3 绑定到 Untrust 区段并将其 IP 地址指派为 1.1.1.1/24。

  所有安全区域都在 trust-vr 路由选择域中。

第二，创建在策略中使用的地址：

- 在 Trust 区段中定义名为 “corp_net” 的地址并将其 IP 地址指派为 10.1.1.0/24。
- 在 DMZ 区段中定义名为 “mail_svr” 的地址并将其 IP 地址指派为 1.2.2.5/32。
- 在 Untrust 区段中定义名为 “r-mail_svr” 的地址并将其 IP 地址指派为 2.2.2.5/32。

第三，创建名为 “MAIL-POP3” 的服务组，包含两个预定义服务 MAIL 和 POP3。

第四，在 trust-vr 路由选择域中配置缺省路由，通过 ethernet3，指向 1.1.1.250 处的外部路由器。

完成步骤 1 – 4 之后，即可创建允许传输、检索及发送电子邮件进出受保护的网络所必需的策略。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone Name: DMZ

Static IP: (出现时选择此选项)
IP Address/Netmask: 1.2.2.1/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)
IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: corp_net

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

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

Address Name: mail_svr

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

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

Address Name: r-mail_svr

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.5/32

Zone: Untrust

3. 服务组

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

Group Name: MAIL-POP3

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

选择 **POP3**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

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

Source Address:

Address Book Entry: (选择), corp_net

Destination Address:

Address Book Entry: (选择), mail_svr

Service: Mail-POP3

Action: Permit

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

Source Address:

Address Book Entry: (选择), mail_svr

Destination Address:

Address Book Entry: (选择), r-mail_svr

Service: MAIL

Action: Permit

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

Source Address:

Address Book Entry: (选择), r-mail_svr

Destination Address:

Address Book Entry: (选择), mail_svr

Service: MAIL

Action: Permit

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address trust corp_net 10.1.1.0/24
set address dmz mail_svr 1.2.2.5/32
set address untrust r-mail_svr 2.2.2.5/32
```

3. 服务组

```
set group service MAIL-POP3
set group service MAIL-POP3 add mail
set group service MAIL-POP3 add pop3
```

4. 路由

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

5. 策略

```
set policy from trust to dmz corp_net mail_svr MAIL-POP3 permit
set policy from dmz to untrust mail_svr r-mail_svr MAIL permit
set policy from untrust to dmz r-mail_svr mail_svr MAIL permit
save
```

范例：区段间策略设置

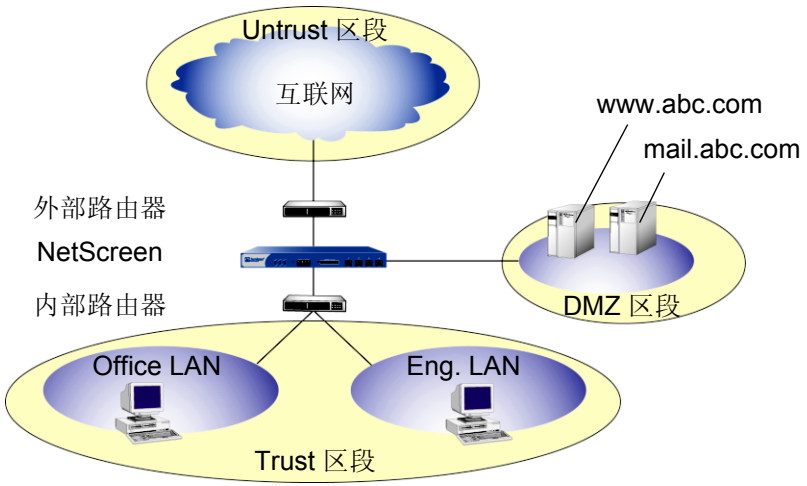
某个小型软件公司 (ABC Design) 已将其内部网络分成两个子网，这两个子网都在 Trust 区段中。这两个子网为：

- 工程 (所定义的地址为 “Eng”)
- 公司的其余部分 (所定义的地址为 “Office”)。

其 Web 和邮件服务器也有一个 DMZ 区段。

下例介绍了对以下用户的一组典型策略：

- “Eng” 可使用用于出站信息流的所有服务， FTP-Put、 IMAP、 MAIL 和 POP3 除外。
- 只要通过 WebAuth 对自己进行了认证，“Office” 即可使用电子邮件和访问互联网。 (有关 WebAuth 用户认证的信息，请参阅第 **8**-41 页上的 “认证用户”。)
- Trust 区段中的任何用户都可访问 DMZ 区段中的 Web 和邮件服务器。
- Untrust 区段中的远程邮件服务器可访问 DMZ 区段中的本地邮件服务器。
- 还有一组系统管理员 (用户定义的地址为 “sys-admins”)，对 DMZ 区段中的服务器具有全部用户和管理访问权限。



本例仅重点介绍了策略，并假定已经对必须到位的接口、地址、服务组和路由进行了配置。有关配置这些项目的详细信息，请参阅第 51 页上的 “接口”、第 139 页上的 “地址”、第 263 页上的 “服务组”和第 6 卷，“动态路由”。

从区段 (源地址)	到区段 (目标地址)	服务	动作
Trust - Any	Untrust - Any	Com (服务组 : FTP-Put、 IMAP、 MAIL、 POP3)	Reject
Trust - Eng	Untrust - Any	Any	Permit
Trust - Office	Untrust - Any	Internet (服务组 : FTP-Get、 HTTP、 HTTPS)	Permit (+ WebAuth)

从区段 (源地址)	到区段 (目标地址)	服务	动作
Untrust - Any	DMZ - mail.abc.com	MAIL	Permit
Untrust - Any	DMZ - www.abc.com	Web (服务组 : HTTP、 HTTPS)	Permit

从区段 (源地址)	到区段 (目标地址)	服务	动作
Trust - Any	DMZ - mail.abc.com	e-mail (服务组 : IMAP、 MAIL、 POP3)	Permit
Trust - Any	DMZ - www.abc.com	Internet (服务组 : FTP-Get、 HTTP、 HTTPS)	Permit
Trust - sys-admins	DMZ - Any	Any	Permit

从区段 (源地址)	到区段 (目标地址)	服务	动作
DMZ - mail.abc.com	Untrust - Any	MAIL	Permit

注意：*缺省策略为全部拒绝。*

WebUI

1. 从 Trust，到 Untrust

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

Source Address:

Address Book Entry: (选择), Eng

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), Office

Destination Address:

Address Book Entry: (选择), Any

Service: Internet[7]

Action: Permit

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

Authentication: (选择)

WebAuth: (选择)

7. “Internet”是具有以下成员的服务组：FTP-Get、 HTTP 和 HTTPS。

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: Com[8]

Action: Reject

Position at Top: (选择)

***注意：**对于从 Untrust 区段到 Trust 区段的信息流，缺省的拒绝策略拒绝所有信息流。*

2. 从 Untrust，到 DMZ

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mail.abc.com

Service: MAIL

Action: Permit

8. “Com”是具有以下成员的服务组 : FTP-Put、 MAIL、 IMAP 和 POP3。

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), www.abc.com

Service: Web[9]

Action: Permit

3. 从 Trust，到 DMZ

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), mail.abc.com

Service: e-mail[10]

Action: Permit

9. “Web”是具有以下成员的服务组 : HTTP 和 HTTPS。

10. “e-mail”是具有以下成员的服务组 : MAIL、 IMAP 和 POP3。

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), www.abc.com

Service: Internet

Action: Permit

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

Source Address:

Address Book Entry: (选择), sys-admins

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

4. 从 DMZ，到 Untrust

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

Source Address:

Address Book Entry: (选择), mail.abc.com

Destination Address:

Address Book Entry: (选择), Any

Service: MAIL

Action: Permit

CLI

1. 从 Trust，到 Untrust

```
set policy from trust to untrust eng any any permit
set policy from trust to untrust office any Internet[11] permit webauth
set policy top from trust to untrust any any Com[12] reject
```

2. 从 Untrust，到 DMZ

```
set policy from untrust to dmz any mail.abc.com mail permit
set policy from untrust to dmz any www.abc.com Web[13] permit
```

3. 从 Trust，到 DMZ

```
set policy from trust to dmz any mail.abc.com e-mail[14] permit
set policy from trust to dmz any www.abc.com Internet[11] permit
set policy from trust to dmz sys-admins any any permit
```

4. 从 DMZ，到 Untrust

```
set policy from dmz to untrust mail.abc.com any mail permit
save
```

11. “Internet”是具有以下成员的服务组：FTP-Get、 HTTP 和 HTTPS。
12. “Com”是具有以下成员的服务组：FTP-Put、 MAIL、 IMAP 和 POP3。
13. “Web”是具有以下成员的服务组：HTTP 和 HTTPS。
14. “e-mail”是具有以下成员的服务组：MAIL、 IMAP 和 POP3。

范例：区段内部策略

在本例中，将创建一个区段内部策略，允许一组帐户访问 Trust 区段中企业 LAN 上的机密服务器。首先将 ethernet1 绑定到 Trust 区段，并指派其 IP 地址为 10.1.1.1/24。然后将 ethernet2 绑定到 Trust 区段，并指派其 IP 地址为 10.1.5.1/24。启用 Trust 区段中的区段内部阻塞。接着，定义两个地址，一个是用于公司存储财务记录的服务器的地址 (10.1.1.100/32)，另一个是会计部门主机所在子网的地址 (10.1.5.0/24)。然后创建区段内部策略，允许从这些主机访问服务器。

WebUI

1. Trust 区段 – 接口和阻塞

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.5.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Block Intra-Zone Traffic: (选择)

2. 地址

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

Address Name: Hamilton

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.100/32

Zone: Trust

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

Address Name: accounting

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.5.0/24

Zone: Trust

3. 策略

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

Source Address:

Address Book Entry: (选择), accounting

Destination Address:

Address Book Entry: (选择), Hamilton

Service: ANY

Action: Permit

CLI

1. Trust 区段 – 接口和阻塞

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

set interface ethernet2 zone trust
set interface ethernet2 ip 10.1.5.1/24
set interface ethernet2 nat

set zone trust block
```

2. 地址

```
set address trust Hamilton 10.1.1.100/32
set address trust accounting 10.1.5.0/24
```

3. 策略

```
set policy from trust to trust accounting Hamilton any permit
save
```

范例：全局策略

在本例中，将创建一个全局策略，使每个区段中的所有主机都可以访问公司的 Web 网站，网址为 www.juniper.net[15]。当存在许多安全区段时，使用全局策略是一种便捷方式。在本例中，一个全局策略即可实现 *n* 个区段间策略所能实现的任务 (其中 *n* = 区段数)。

WebUI

1. 全局地址

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

   Address Name: server1

   IP Address/Domain Name:

   Domain Name: (选择), www.juniper.net

   Zone: Global

2. 策略

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

   Source Address:

   Address Book Entry: (选择), Any

   Destination Address:

   Address Book Entry: (选择), server1

   Service: HTTP

   Action: Permit

15. 要使用域名而非 IP 地址，应确保已在 NetScreen 设备上对 DNS 服务进行了配置。

CLI

1. 全局地址

```
set address global server1 www.juniper.net
```

2. 策略

```
set policy global any server1 http permit
save
```

输入策略环境

通过 CLI 配置策略时，首先创建策略，然后输入策略环境进行添加和修改。例如，可能首先创建以下策略：

```
set policy id 1 from trust to untrust host1 server1 HTTP permit attack
    HIGH:HTTP:SIGS action close
```

如果想对该策略进行某些修改，如添加其它源地址或目标地址、其它服务或其它攻击组，则可输入策略 1 的环境，然后输入相应的命令：

```
set policy id 1
ns(policy:1)-> set src-address host2
ns(policy:1)-> set dst-address server2
ns(policy:1)-> set service FTP
ns(policy:1)-> set attack CRITICAL:HTTP:SIGS
```

也可从单个策略组件中移除多个条目，只要不将它们全部移除即可。例如，可从上述配置移除 server2，但不能同时移除 server2 和 server1，因为同时移除之后就不再有目标地址了：

可移除 server2，

```
ns(policy:1)-> unset dst-address server2
```

或移除 server1，

```
ns(policy:1)-> unset dst-address server1
```

但不能同时将它们移除。

```
ns(policy:1)-> unset dst-address server2
ns(policy:1)-> unset dst-address server1
```

每个策略组件含多个条目

ScreenOS 允许将多个条目添加到下列策略组件中：

- 源地址
- 目标地址
- 服务
- 攻击组

在 ScreenOS 5.0.0 之前的版本中，具有多个源地址和目标地址或服务的唯一方法是首先创建具有多个成员的地址或服务组，然后在策略中引用该组。 ScreenOS 5.0.0 版本中策略的地址和服务组仍可使用。此外，也可以直接添加新条目到策略组件。

***注意：**如果策略中引用的第一个地址或服务是 “Any”，则逻辑上不能向策略组件添加任何其它条目。 NetScreen 防止此类错误配置，如果出现，会显示错误消息。*

要向策略组件添加多个条目，请执行下列操作之一：

WebUI

要添加多个地址和服务，请单击要向其中添加条目的组件旁的 **Multiple** 按钮。要添加多个攻击组，请单击 **Attack Protection** 按钮。在 Available Members 栏中选择一个条目，然后使用 **<<** 键将该条目移动到 Active Members 栏中。可对其它条目重复此操作。完成后，单击 **OK** 返回策略配置页。

CLI

使用以下命令输入策略环境：

```
set policy id number
```

然后使用下列命令中相应的命令：

```
ns(policy:number)-> set src-address string
ns(policy:number)-> set dst-address string
ns(policy:number)-> set service string
ns(policy:number)-> set attack string
```

地址排除

可以配置策略，使其应用到除指定为源地址或目标地址之外的其它所有地址。例如，可创建允许互联网访问除“P-T_contractors”地址组之外的其它所有地址的策略。要实现此目的，可使用地址排除选项。

在 WebUI 中，单击策略配置页上源地址或目标地址旁的 **Multiple** 按钮时，此选项会出现在弹出菜单中。

在 CLI 中，在源地址或目标地址的前面插入感叹号 (!)。

***注意：**地址排除出现在策略组件级，应用于排除组件的所有条目。*

范例：目标地址排除

在本例中，将创建一个区段内部策略，允许 Trust 区段中的所有地址访问除名为 “vulcan”的 FTP 服务器之外的所有 FTP 服务器，工程部门用此服务器发送功能规格给其他使用者。

不过，在创建策略之前，必须首先设计应用策略的环境。第一，启用 Trust 区段的区段内部阻塞。在 NetScreen 设备通过两个接口 (绑定到同一区段) 间的信息流之前，区段内部阻塞要求进行策略查找。

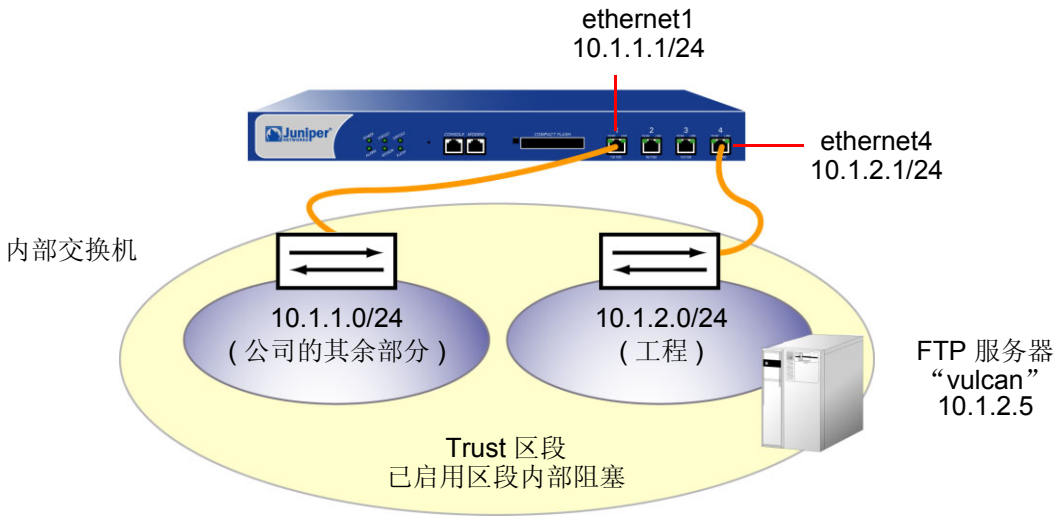
第二，将两个接口绑定到 Trust 区段并为其分配 IP 地址：

- 将 ethernet1 绑定到 Trust 区段并将其 IP 地址指派为 10.1.1.1/24。
- 将 ethernet4 绑定到 Trust 区段并将其 IP 地址指派为 10.1.2.1/24。

第三，在 Trust 区段中为名为 “vulcan”的 FTP 服务器创建地址 (10.1.2.5/32)。

完成这两个步骤之后，即可创建区段内部策略。

***注意：**不必为工程部门创建到达其 FTP 服务器的策略，因为工程师也在 10.1.2.0/24 子网中，并且不必穿越 NetScreen 防火墙到达他们自己的服务器。*



WebUI

1. 区段内部阻塞

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

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (选择)

2. Trust 区段接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

Network > Interfaces > Edit (对于 ethernet4): 输入以下内容，然后单击 **Apply**:

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

3. 地址

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

Address Name: vulcan

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.2.5/32

Zone: Trust

4. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), vulcan

> 单击 **Multiple**，选中 **Negate Following** 复选框，然后单击 **OK** 返回基本 Policy 配置页。

Service: FTP

Action: Permit

CLI

1. 区段内部阻塞

```
set zone trust block
```

2. Trust 区段接口

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

set interface ethernet4 zone trust
set interface ethernet4 ip 10.1.2.1/24
set interface ethernet1 nat
```

3. 地址

```
set address trust vulcan 10.1.2.5/32
```

4. 策略

```
set policy from trust to trust any !vulcan ftp permit
save
```

修改和禁用策略

创建策略后，始终都可以返回到该策略进行修改。在 WebUI 中，单击要更改的策略 Configure 栏中的 **Edit** 链接。在出现的 Policy configuration 页面中对该策略进行更改，然后单击 **OK**。在 CLI 中，使用 **set policy** 命令。

ScreenOS 还提供了一种启用和禁用策略的方式。在缺省情况下，策略被启用。要禁用策略，请执行以下操作：

WebUI

Policies: 在要禁用的策略的 Configure 栏中，清除 **Enable** 复选框。

被禁用策略的文本行以灰色显示。

CLI

```
set policy id id_num disable
save
```

注意：*要再次启用策略，请在要启用的策略的 Configure 栏中选择* ***Enable*** *(WebUI)，或键入* ***unset policy id*** *id_num* ***disable*** *(CLI)。*

策略验证

ScreenOS 提供一种工具，用于验证策略列表中策略的顺序是否有效。可能会出现一种策略掩蔽或 “遮盖” 另一种策略的现象。考虑以下示例：

```
set policy id 1 from trust to untrust any any HTTP permit
set policy id 2 from trust to untrust any dst-A HTTP deny
```

因为 NetScreen 设备从列表顶部开始查找策略，所以找到所接收信息流的匹配策略后，就不再向下查找策略列表中的其它策略。在上例中， NetScreen 设备从未到达策略 2，因为策略 1 中的目标地址 “any” 包括策略 2 中更具体的 “dst-A” 地址。某 HTTP 数据包从 Trust 区段 (为 Untrust 区段中的 dst-A 绑定) 中的一个地址到达 NetScreen 设备时， NetScreen 设备始终首先找到与之匹配的策略 1。

要纠正上述范例，只需颠倒策略顺序，将较为具体的策略放在第一位：

```
set policy id 2 from trust to untrust any dst-A HTTP deny
set policy id 1 from trust to untrust any any HTTP permit
```

当然，本例的目的只是为了说明基本概念。在有很多策略的情况下，一个策略对另一个策略的掩蔽可能就不会这么容易发现。要检查策略列表中是否有策略遮盖[16]，可使用下列 CLI 命令：

```
exec policy verify
```

此命令报告遮盖策略和被遮盖的策略。然后，则由管理员负责纠正此情形。

策略验证工具无法检测出一个策略组合遮盖另一个策略的情况。在下例中，没有任何单一策略遮盖策略 3，但是，策略 1 和策略 2 的组合遮盖了策略 3:

```
set group address trust grp1 add host1
set group address trust grp1 add host2
set policy id 1 from trust to untrust host1 server1 HTTP permit
set policy id 2 from trust to untrust host2 server1 HTTP permit
set policy id 3 from trust to untrust grp1 server1 HTTP deny
```

16. 策略 “遮盖” 的概念是指策略列表中位置较高的策略始终在之后策略前生效的情况。因为策略查找始终使用找到的第一个策略 (与源区段和目标区段、源地址和目标地址及服务类型 5 部分元组相匹配)，所以，如果另一个策略应用于同一元组 (或元组子网)，则策略查找将使用列表中的第一个策略，且绝不会到达第二个策略。

重新排序策略

NetScreen 设备将所有穿越防火墙的尝试与策略进行对照检查，从列在相应列表 (请参阅第 298 页上的 “策略组列表”) 的策略组中的第一个开始，并检查整个列表。由于 NetScreen 设备将策略中指定的动作应用到列表中第一个匹配的策略，因此，必须按照从最特殊到最一般的顺序安排策略。 (特殊策略不排除位于列表下部的更一般性策略的应用，但位于特殊策略前的一般性策略会产生此排除效应。)

在缺省情况下，最近创建的策略出现在策略组列表的底部。有一个选项允许将策略定位在列表的顶部。在 WebUI 的 Policy configuration 页面中，选中 **Position at Top** 复选框。在 CLI 中，将关键字 **top** 添加到 **set policy** 命令中 : **set policy top** …

要将策略移动到列表中的不同位置，请执行以下操作之一 :

WebUI

在 WebUI 中可使用两种方法来重新排序策略 : 在要移动策略的 Configure 栏中，单击圆形箭头或单击单箭头。

如果单击圆形箭头 :

出现 User Prompt 对话框。

要将策略移到列表的最底端，请输入 <-1>。要在列表中将策略向上移动，输入要移动到其前面的策略的 ID 号。

单击 **OK**，执行移动操作。

如果单击单箭头 :

出现 Policy Move 页面，显示要移动的策略以及显示其它策略的表格。

在显示其它策略的表格的第一栏 (Move Location) 中含有指向不同位置的箭头，可将策略移动到这些位置。单击指向策略要移动到的列表中位置的箭头。

出现 Policy List 页面，移动的策略出现在新位置。

CLI

```
set policy move id_num { before | after } number
save
```

移除策略

除修改和重新排序策略外，还可以删除策略。在 WebUI 中，在要移除的策略的 Configure 栏中单击 **Remove**。当系统消息提示您确认是否要执行该移除操作时，请单击 **Yes**。在 CLI 中，使用 **unset policy** *id_num* 命令。

7

信息流整形

本章论述在不牺牲所有用户的网络连接质量及可用性的情况下，使用 NetScreen 设备来管理有限带宽的各种方法。讨论的主题包括：

应用信息流整形

信息流整形是指为接口上的每一位用户和应用程序分配适当的网络带宽数量。适当的带宽数量指在保证服务质量 (QoS) 的前提下具有成本效益的载流容量。通过创建策略并将适当的速率控制应用到流经 NetScreen 设备的每一种信息流类别，您可使用 NetScreen 设备对信息流进行整形。

注意：*只有那些目标区段有单个物理接口绑定到其中的策略才可以应用信息流整形。如果目标区段含有一个 (或多个) 子接口或者多个物理接口，则 NetScreen 不支持信息流整形。*

在策略级管理带宽

要将信息流分类，可创建一个指定每类信息流的保障带宽数量、最大带宽及优先级等内容的策略。每一接口的物理带宽都分配给所有策略的保障带宽参数。如果有带宽剩余，可由其它信息流共享。换句话说，每个策略可得到其保障带宽并基于其优先级共享剩余的带宽 (直至达到其最大带宽规格的限制)。

信息流整形功能适用于所有策略的信息流。如果您关闭特定策略的信息流整形但其它策略的信息流整形仍然开启，则系统将对此特定策略应用缺省信息流整形策略，使用的参数如下：

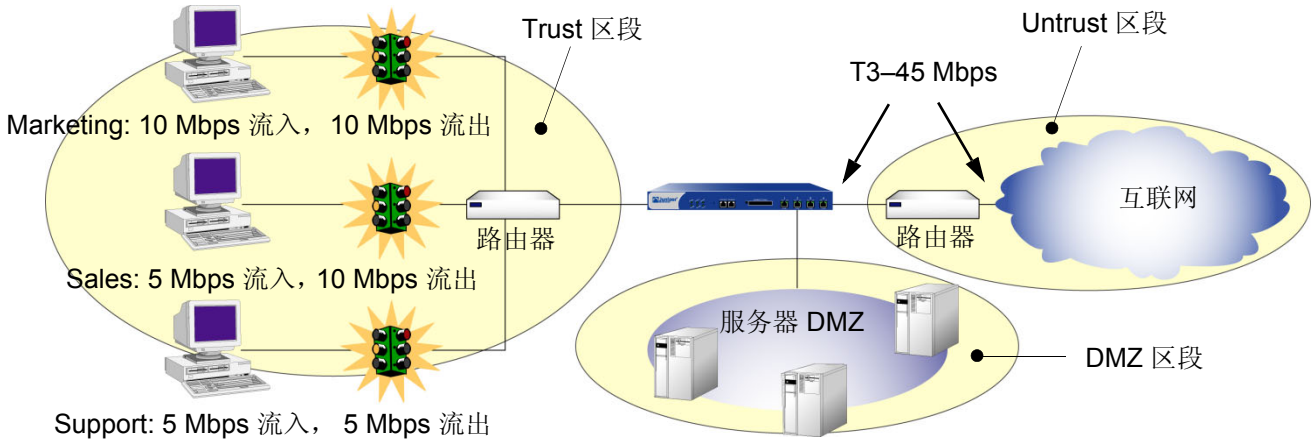
- 保障带宽为 0
- 最大带宽无限制
- 优先级为 7 (最低的优先级设置)[1]

如果您不希望系统将此缺省信息流整形策略指派给已关闭其信息流整形的策略，则可通过 CLI 命令 **set traffic-shaping mode off** 关闭整个系统的信息流整形。可将信息流整形设置为自动：**set traffic-shaping mode auto**。这允许系统在策略需要时开启信息流整形，在策略不需要时将其关闭。

1. 您可启用 NetScreen 优先级到 DiffServ 码点标记系统的映射。有关 “DS 码点标记” 的详细信息，请参阅第 6-310 页上的 “信息流整形”。

范例：信息流整形

在本例中，您需要在 T3 接口上划分 45Mbps 的带宽，其中该接口处于同一子网的三个部门之间。 ethernet1 接口被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。



WebUI

1. 接口带宽

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

Traffic Bandwidth: 45000[2]

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

Traffic Bandwidth: 45000

2. 如果您未指定接口的带宽设置，NetScreen 将使用所有可用的物理带宽。

2. 策略带宽

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

Name: Marketing Traffic Shaping

Source Address:

Address Book Entry: (选择), Marketing

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

VPN Tunnel: None[3]

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 15000

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

Name: Sales Traffic Shaping Policy

Source Address:

Address Book Entry: (选择), Sales

Destination Address:

Address Book Entry: (选择), Any

Service: Any

3. 您也可在参考 VPN 通道的策略中启用信息流整形。

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 10000

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

Name: Support Traffic Shaping Policy

Source Address:

Address Book Entry: (选择), Support

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 10000

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

Name: Allow Incoming Access to Marketing

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Marketing

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 10000

Maximum Bandwidth: 10000

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

Name: Allow Incoming Access to Sales

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Sales

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 10000

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

Name: Allow Incoming Access to Support

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Support

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 5000

CLI

要通过策略启用信息流整形，请执行以下操作：

1. 接口带宽

```
set interface ethernet1 bandwidth 45000[4]
set interface ethernet3 bandwidth 45000
```

2. 策略带宽

```
set policy name "Marketing Traffic Shaping" from trust to untrust marketing any
    any permit traffic gbw 10000 priority 0 mbw 15000
set policy name "Sales Traffic Shaping Policy" from trust to untrust sales any
    any permit traffic gbw 10000 priority 0 mbw 10000
set policy name "Support Traffic Shaping Policy" from trust to untrust support
    any any permit traffic gbw 5000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Marketing" from untrust to trust any
    marketing any permit traffic gbw 10000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Sales" from untrust to trust any
    sales any permit traffic gbw 5000 priority 0 mbw 10000
set policy name "Allow Incoming Access to Support" from untrust to trust any
    support any permit traffic gbw 5000 priority 0 mbw 5000
save
```

4. 如果您未指定接口的带宽设置， NetScreen 将使用所有可用的物理带宽。

设置服务优先级

通过 NetScreen 设备上的信息流整形功能，可对未分配给保障带宽的或未使用的保障带宽执行优先级排列。优先级排列功能允许所有用户和应用程序在需要时访问可用带宽，同时又确保重要的信息流能够得以通过，必要时可以牺牲次重要信息流的带宽作为代价。通过排列功能， NetScreen 能够以八种不同的优先级排列对信息流进行缓冲。这八种排列为：

- High priority
- 2nd priority
- 3rd priority
- 4th priority
- 5th priority
- 6th priority
- 7th priority
- Low priority (缺省)

策略的优先级设置意味着尚未分配给其它策略的带宽将基于高优先级在前和低优先级在后的原则进行排列。具有相同优先级设置的策略将以轮询方式竞争带宽。NetScreen 设备首先处理具有较高优先级策略的所有信息流，然后再处理具有次优先级设置策略的信息流，依此类推，直至处理完所有信息流请求。如果信息流请求超过可用带宽，则将丢弃优先级最低的信息流。

小心：*应注意不要为接口分配超过其支持能力的带宽。策略配置过程本身不能避免创建不支持的策略配置。如果竞争策略的保障带宽超过接口上设置的信息流带宽，将有可能丢失数据。*

如果您未分配任何保障带宽，则可使用优先级排列来管理网络的所有信息流。也就是说，必须在发送完所有高优先级的信息流之后，才能发送第 2 优先级的信息流，依此类推。只有在处理完其它所有信息流之后， NetScreen 设备才处理低优先级的信息流。

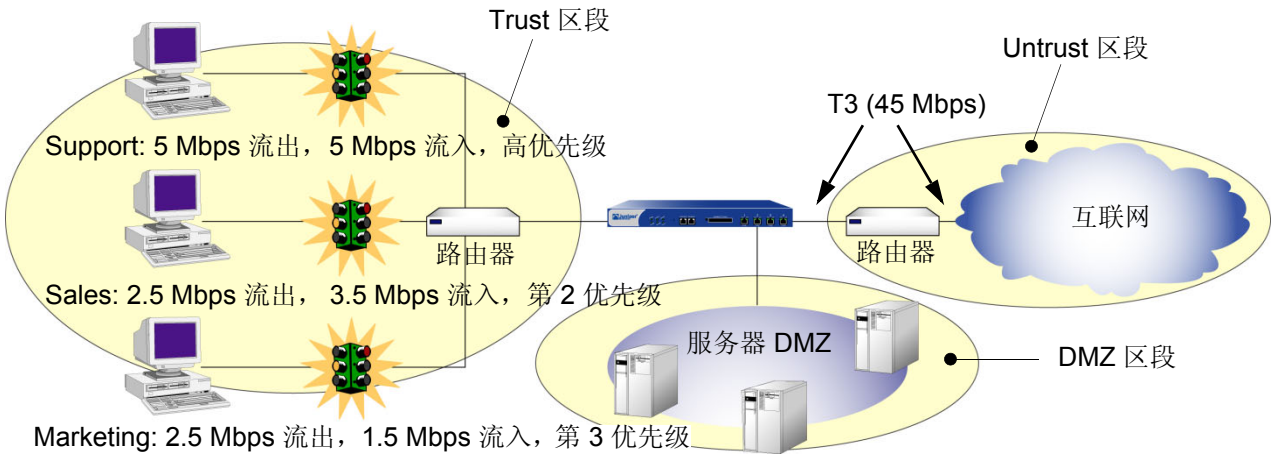
范例：优先级排列

在本例中，您需要为三个部门 (Support、 Sales 和 Marketing) 配置保障带宽和最大带宽，如下所示：

	出站保证	入站保证	组合保证	优先级
Support	5*	5	10	高
Sales	2.5	3.5	6	2
Marketing	2.5	1.5	4	3
总计	10	10	20	

* 兆位每秒 (Mbps)

如果三个部门同时通过 NetScreen 防火墙发送和接收信息流，那么 NetScreen 设备必须分配 20 Mbps 的带宽以满足保证的策略要求。 ethernet1 接口被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。



WebUI

1. 接口带宽

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

   Traffic Bandwidth: 40000

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

   Traffic Bandwidth: 40000

2. 策略带宽

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

   Name: Sup-out

   Source Address:

   Address Book Entry: (选择), Support

   Destination Address:

   Address Book Entry: (选择), Any

   Service: Any

   Action: Permit

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

   Traffic Shaping: (选择)

   Guaranteed Bandwidth: 5000

   Maximum Bandwidth: 40000

   Traffic Priority: High priority

   DiffServ Codepoint Marking[5] : (选择)

5. 差异服务 (DS) 是在优先级层次结构中的某一位置对信息流进行标记 (或 “做记号”) 的系统。 DS 码点标记将 NetScreen 的策略优先级映射到 IP 数据包包头中 DS 字段的码点的前三位。有关 “DS 码点标记” 的详细信息，请参阅第 310 页上的 “信息流整形”。

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

Name: Sal-out

Source Address:

Address Book Entry: (选择), Sales

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 2500

Maximum Bandwidth: 40000

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: Enable

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

Name: Mar-out

Source Address:

Address Book Entry: (选择), Marketing

Destination Address:

Address Book Entry: (选择), Any

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 2500

Maximum Bandwidth: 40000

Traffic Priority: 3rd priority

DiffServ Codepoint Marking: (选择)

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

Name: Sup-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Support

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 5000

Maximum Bandwidth: 40000

Traffic Priority: High priority

DiffServ Codepoint Marking: (选择)

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

Name: Sal-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Sales

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 3500

Maximum Bandwidth: 40000

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: (选择)

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

Name: Mar-in

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Marketing

Service: Any

Action: Permit

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

Traffic Shaping: (选择)

Guaranteed Bandwidth: 1500

Maximum Bandwidth: 40000

Traffic Priority: 3rd priority

DiffServ Codepoint Marking: (选择)

CLI

1. 接口带宽

```
set interface ethernet1 bandwidth 40000
set interface ethernet3 bandwidth 40000
```

2. 策略带宽

```
set policy name sup-out from trust to untrust support any any permit traffic
    gbw 5000 priority 0 mbw 40000 dscp enable
set policy name sal-out from trust to untrust sales any any permit traffic gbw
    2500 priority 2 mbw 40000 dscp enable
set policy name mar-out from trust to untrust marketing any any permit traffic
    gbw 2500 priority 3 mbw 40000 dscp enable
set policy name sup-in from untrust to trust any support any permit traffic gbw
    5000 priority 0 mbw 40000 dscp enable
set policy name sal-in from untrust to trust any sales any permit traffic gbw
    3500 priority 2 mbw 40000 dscp enable
set policy name mar-in from untrust to trust any marketing any permit traffic
    gbw 1500 priority 3 mbw 40000 dscp enable
save
```

8

系统参数

本章重点介绍与建立系统参数有关的概念，这些参数会影响 NetScreen 安全装置的下列方面：

域名系统支持

NetScreen 设备集成了 “域名系统” (DNS) 支持，允许您既可使用 IP 地址也可使用域名来识别位置。 DNS 服务器保留有与域名相关联的 IP 地址表。除了使用可路由的 IP 地址 (域名 www.juniper.net 对应的 IP 地址是 207.17.137.68) 来引用位置以外，还可以通过 DNS 用域名 (如 www.juniper.net) 来引用位置。下列所有程序均支持 DNS 转换 :

- 通讯簿
- 系统日志
- 电子邮件
- WebTrends
- Websense
- LDAP
- SecurID
- RADIUS
- NetScreen-Security Manager

在将 DNS 用于域名 / 地址解析之前，必须在 NetScreen 设备中输入 DNS 服务器 (主 DNS 服务器和辅 DNS 服务器) 的地址。

注意 : *在启用 NetScreen 设备作为 “动态主机配置协议” (DHCP) 服务器 (请参阅第 370 页上的 “DHCP”) 时，还必须在 WebUI 的 DHCP 页中输入 DNS 服务器的 IP 地址，也可使用 CLI 中的* ***set interface*** *interface* ***dhcp*** *命令。*

DNS 查找

出现以下情况时，NetScreen 设备会使用特定的 DNS 服务器检查 DNS 表中的所有条目，从而将这些条目全部刷新：

- 发生 HA 故障切换后
- 到达每天固定的预定时间及一天中固定的预定时间间隔
- 手动控制设备执行 DNS 查找时
  - WebUI: Network > DNS: 单击 Refresh DNS cache。
  - CLI: exec dns refresh

除使用现有方法设置每天自动刷新 DNS 表的时间外，还可以自行定义刷新的时间间隔 (介于 4 小时与 24 小时之间)。

***注意：**如果通过 WebUI 来添加诸如地址或 IKE 网关等完全合格的域名 (FQDN)，则单击 **Apply** 或 **OK** 后，NetScreen 设备将会对该域名进行解析。如果键入引用 FQDN 的 CLI 命令，则 NetScreen 设备将在输入命令后尝试对其进行解析。*

当 NetScreen 设备与 DNS 服务器相连以解析域名 /IP 地址映射时，会将该条目存储在其 DNS 状态表中。下面的列表包含 DNS 查找涉及到的一些具体内容：

- 当 DNS 查找返回多个条目时，通讯簿会接受所有条目。第 359 页列出的其它程序只接受第一个条目。
- 当使用 WebUI 中的 **Refresh** 按钮或输入 CLI 命令 **exec dns refresh** 刷新查找时，如果 NetScreen 设备发现域名表中的内容发生了变化，则将重新安装所有策略。
- 如果 DNS 服务器发生故障，NetScreen 设备会重新查找所有内容。
- 如果查找失败，NetScreen 设备将从高速缓存表中将其删除。
- 如果在向通讯簿中添加地址时域名查找失败，NetScreen 设备会给出一条错误消息，指出已成功添加地址，但是 DNS 名查找失败。

NetScreen 设备必须每天进行一次新的查找，您可以安排 NetScreen 设备在指定时间进行查找：

WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:

DNS refresh every day at: 选中复选框而后输入时间 <hh:mm>

CLI

```
set dns host schedule time_str
save
```

DNS 状态表

DNS 状态表会报告查找到的所有域名、相应的 IP 地址、查找是否成功以及每个域名 /IP 地址上次解析的时间。报告格式如下面的例子所示：

Name	IP Address	Status	Last Lookup
www.yahoo.com	204.71.200.74 204.71.200.75 204.71.200.67 204.71.200.68	Success	8/13/2000 16:45:33
www.hotbot.com	209.185.151.28 209.185.151.210 216.32.228.18	Success	8/13/2000 16:45:38

要查看 DNS 状态表，请按下列任一方法进行操作：

WebUI

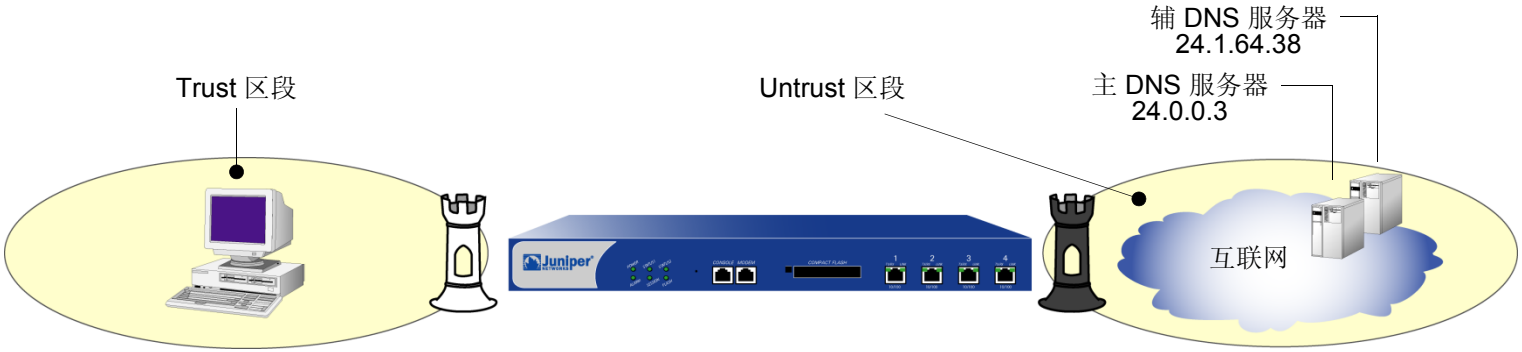
Network > DNS > Show DNS Table

CLI

```
get dns host report
```

范例: DNS 服务器和刷新时间安排

要实现 DNS 功能，在 NetScreen 设备中为 24.1.64.38 和 24.0.0.3 上的 DNS 服务器输入 IP 地址，保护总公司仅有的一台主机。安排 NetScreen 设备，使其在每天晚上 11:00 刷新存储在 DNS 状态表中的 DNS 设置。



WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:

Primary DNS Server: 24.0.0.3

Secondary DNS Server: 24.1.64.38

DNS Refresh: (选择)

Every Day at: 23:00

CLI

```
set dns host dns1 24.0.0.3
set dns host dns2 24.1.64.38
set dns host schedule 23:00
save
```

范例：设置 DNS 刷新时间间隔

在本例中，将配置 NetScreen 设备自每天凌晨 00:01 起，每隔 4 小时刷新一次 DNS 表。

WebUI

Network > DNS: 输入以下内容，然后单击 **Apply**:

DNS Refresh: (选择)

Every Day at: 00:01

Interval: 4

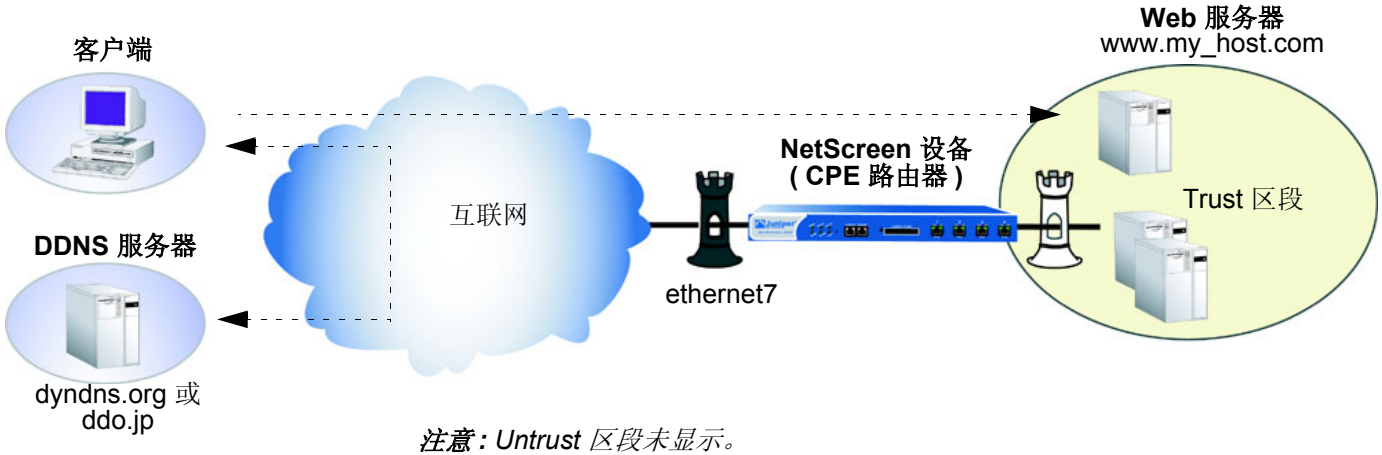
CLI

```
set dns host schedule 00:01 interval 4
save
```

动态 DNS

“动态 DNS”(DDNS) 是一种允许客户端动态更新已注册域名 IP 地址的机制。当 ISP 使用 PPP、DHCP 或 XAuth 以动态更改保护 web 服务器的 CPE 路由器 (例如 NetScreen 设备) 的 IP 地址时，此更新非常有用。这样，即使 CPE 路由器的 IP 地址先前已被更改，互联网上的客户端仍可以使用域名访问 web 服务器。通过 DDNS 服务器 (例如 dyndns.org 或 ddo.jp) 可以实现此更改，其中包括动态更改的地址及其相关联的域名。 CPE 使用此信息定期更新 DDNS 服务器，或响应 IP 地址的更改。

要使用 DDNS，需在 DDNS 服务器上创建一个帐户 (用户名和密码)。服务器使用此帐户信息配置客户端设备。



***注意：** Untrust 区段未显示。*

在上图中，接口 ethernet7 的 IP 地址可能已进行了更改。当更改发生后，客户端使用主机名 (www.my_host.com) 或者通过 dyndns.org 服务器或 ddo.jp 服务器仍可访问受保护的 Web 服务器。所有这些服务器在 NetScreen 设备的配置相互之间需有所不同。

范例 : dyndns 服务器的 DDNS 设置

在下例中，将针对 DDNS 操作对 NetScreen 设备进行配置。该设备使用 dyndns.org 服务器来解析更改的地址。对于该服务器，使用 Host Name 设置来指定受保护的主机，该主机明确绑定到 DNS 接口 (ethernet7) ；因而，当设备向 ddo.jp 服务器发送更新内容时，它就会将主机名同该接口的 IP 地址相关联。

WebUI

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

ID: 12

Server Settings:

Server Type: dyndns

Server Name: dyndns.org

Refresh Interval: 24

Minimum Update Interval: 15[1]

Account Settings:

Username: swordfish

Password: ad93lvb

Bind to Interface: ethernet7

Host Name: www.my_host.com

1. 此设置指定 DDNS 更新之间的最小时间间隔 (以分表示)。缺省值为 10 分钟，允许的范围是 1-1440。某些情况下，由于 DNS 服务器首先需要超时其高速缓存中的 DDNS 条目，所以设备可能不会更新该时间间隔。此外，如果将 Minimum Update Interval 设置为很小的值，那么 NetScreen 设备可能会锁定；因此建议使用 10 分钟或更大的值。

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 12 server dyndns.org server-type dyndns refresh-interval 24
    minimum-update-interval 15
set dns ddns id 12 src-interface ethernet7 host-name www.my_host.com
set dns ddns id 12 username swordfish password ad93lvb
save
```

范例 : ddo 服务器的 DDNS 设置

在下例中，将为 NetScreen 设备配置 DDNS。该设备使用 ddo.jp 服务器来解析地址。对于 ddo.jp 服务器，将受保护的主机 FQDN 指定为 DDNS 条目的 Username，而不是使用 Host Name 设置来指定受保护的主机。该服务自动从 Username 值导出主机名。例如， ddo.jp 服务器将用户名 my_host 转变为 my_host.ddo.jp。确保在 ddo.jp 上注册的域名与导出的 DNS 相匹配。

WebUI

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

ID: 25

Server Settings:

Server Type: ddo

Server Name: juniper.net

Refresh Interval: 24

Minimum Update Interval: 15

Account Settings:

Username: my_host

Password: ad93lvb

Bind to Interface: ethernet7

CLI

```
set dns ddns
set dns ddns enable
set dns ddns id 25 server ddo.jp server-type ddo refresh-interval 24
    minimum-update-interval 15
set dns ddns id 25 src-interface ethernet7
set dns ddns id 25 username my_host password ad93lvb
save
```

代理 DNS 地址分隔

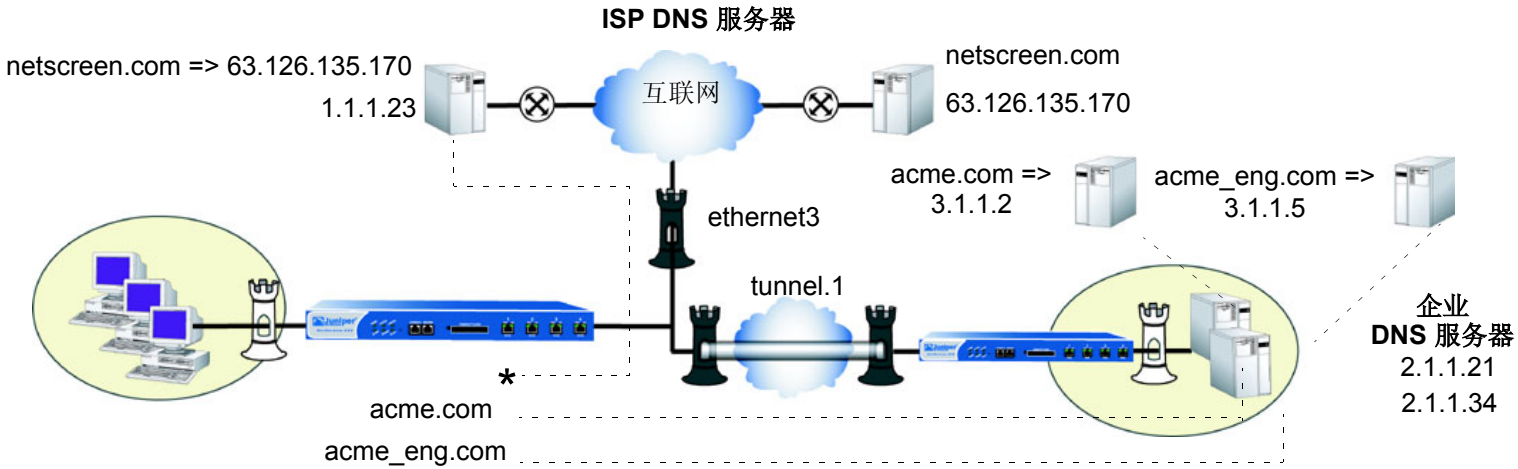
代理 DNS 功能提供了一种允许客户端进行分隔的 DNS 查询的透明机制。使用此技术，代理依据部分或全部域名有选择地将 DNS 查询重定向到特定的 DNS 服务器。当 VPN 通道或 PPPoE 虚拟链接提供有多个网络连接时此技术非常有用，并且必须通过该技术将一些 DNS 查询引导到一个网络以及将其它查询引导到另一网络。

以下是 DNS 代理最重要的优点。

- 域查找通常更有效。例如，针对企业域 (例如 acme.com) 的 DNS 查询可能仅转到企业 DNS 服务器，而所有其它的 DNS 查询转到 ISP DNS 服务器，这样就减少了企业服务器上的负载。此外，这样做还可防止企业域信息泄漏到互联网上。
- DNS 代理允许您通过通道接口传输选定的 DNS 查询，因而可以阻止恶意用户知道内部网络配置。例如，绑定到企业服务器的 DNS 查询可以通过通道接口，并使用安全功能 (例如，认证、加密和反回放)。

范例：分隔 DNS 请求

下列命令创建两个代理 DNS 条目，这些条目有选择地将 DNS 查询转发给不同的服务器。



- 包括域名 acme.com 的具有 FQDN 的任何 DNS 查询都要经过通道接口 tunnel.1，到达 IP 地址为 2.1.1.21 的企业 DNS 服务器。

  例如，如果主机发出 www.acme.com 的 DNS 查询，则设备会自动将查询引导到此服务器。（对于此范例，假设服务器将查询解析为 IP 地址 3.1.1.2。）

- 包括域名 acme_engineering.com 的具有 FQDN 的任何 DNS 查询都要经过通道接口 tunnel.1，到达 IP 地址为 2.1.1.34 的 DNS 服务器。

  例如，如果主机发出 intranet.acme_eng.com 的 DNS 查询，则设备会将查询引导到此服务器。（对于此范例，假设服务器将查询解析为 IP 地址 3.1.1.5。）

- 所有其它的 DNS 查询（以星号标明）均绕过企业服务器，并经过接口 ethernet3 到达 IP 地址为 1.1.1.23 的 DNS 服务器。

  例如，如果主机名和域名是 www.juniper.net，则设备自动绕过企业服务器，并将查询引导到此服务器，该服务器将查询解析为 IP 地址 207.17.137.68。

WebUI

1. Network > DNS > Proxy: 输入以下内容，然后单击 **Apply**:
   Initialize DNS Proxy: Enable
   Enable DNS Proxy: Enable
2. Network > DNS > Proxy > New: 输入以下内容，然后单击 **OK**:
   Domain Name: acme.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.21
3. Network > DNS > Proxy > New: 输入以下内容，然后单击 **OK**:
   Domain Name: acme_eng.com
   Outgoing Interface: tunnel.1
   Primary DNS Server: 2.1.1.34
4. Network > DNS > Proxy > New: 输入以下内容，然后单击 **OK**:
   Domain Name: *
   Outgoing Interface: ethernet3
   Primary DNS Server: 1.1.1.23

CLI

```
set dns proxy
set dns proxy enable
set interface ethernet3 proxy dns
set dns server-select domain acme.com outgoing-interface tunnel.1
    primary-server 2.1.1.21
set dns server-select domain acme_eng.com outgoing-interface tunnel.1
    primary-server 2.1.1.34
set dns server-select domain * outgoing-interface ethernet3 primary-server
    1.1.1.23
save
```

DHCP

“动态主机配置协议” (DHCP) 旨在通过自动为网络中的主机分配 TCP/IP 设置来减少对网络管理员的需求。 DHCP 会代替管理员自动为网络中的每台机器分配、配置、跟踪和更改 (必要时) 所有 TCP/IP 设置。此外， DHCP 还可以确保不使用重复地址、重新分配未使用的地址，并且可以自动为主机连接的子网分配适当的 IP 地址。

不同的 NetScreen 设备支持不同的 DHCP 角色 :

- **DHCP 客户端 :** 某些 NetScreen 设备可以充当 DHCP 客户端，接收为任意区段中的任意物理接口动态分配的 IP 地址。
- **DHCP 服务器 :** 某些 NetScreen 设备还可充当 DHCP 服务器，为任意区段内的任意物理接口或 VLAN 接口上的主机 (充当 DHCP 客户端) 动态分配 IP 地址。

  注意 : *使用 DHCP 服务器模块为区段内的主机 (如工作站) 分配地址时，仍然可以为其它机器 (如邮件服务器和 WINS 服务器) 使用固定 IP 地址。*

- **DHCP 中继代理 :** 还有一些 NetScreen 设备可以充当 DHCP 中继代理，接收来自 DHCP 服务器的 DHCP 信息，然后将这些信息转交给任意区段内的任意物理接口或 VLAN 接口上的主机。
- **DHCP 客户端 / 服务器 / 中继代理 :** 某些 NetScreen 设备可以同时充当 DHCP 客户端、服务器和中继代理。注意，一个接口上只能配置一个 DHCP 角色。例如，不能在同一接口上同时配置 DHCP 客户端和服务器。还可配置 DHCP 客户端模块，将其收到的 TCP/IP 设置转发给 DHCP 服务器模块，以便将 TCP 设置提供给 Trust 区段内充当 DHCP 客户端的主机时使用。

DHCP 由两部分组成 : 用于传送特定于主机的 TCP/IP 配置设置的协议和用于分配 IP 地址的机制。当 NetScreen 设备充当 DHCP 服务器时，它会在每一主机启动时为其提供下面的 TCP/IP 设置 :

- 缺省网关的 IP 地址和网络掩码。如果将这些设置保留为 0.0.0.0/0，DHCP 服务器模块会自动使用缺省 Trust 区段接口[2] 的 IP 地址和网络掩码。
- 下列服务器的 IP 地址 :
  - WINS 服务器 (2):[3] “Windows 互联网命名服务” (WINS) 服务器将 Windows NT 网络环境使用的 NetBIOS 名称映射为基于 IP 的网络中使用的 IP 地址。
  - NetInfo 服务器 (2): NetInfo 是一种 Apple 网络服务，用于在 LAN 内分发管理数据。
  - NetInfo 标记 (1): Apple NetInfo 数据库使用的识别标记。
  - DNS 服务器 (3): “域名系统” (DNS) 服务器可将统一资源定位器 (URL) 映射为 IP 地址。
  - SMTP 服务器 (1): “简单邮件传输协议” (SMTP) 服务器可向存储内向邮件的邮件服务器 (如 POP3 服务器) 传送 SMTP 消息。
  - POP3 服务器 (1): “邮局协议版本 3” (POP3) 服务器可存储内向邮件。 POP3 服务器必须与 SMTP 服务器联合使用。
  - 新闻服务器 (1): 新闻服务器接收并存储新闻组寄来的信息。

注意 : *当 NetScreen 设备向某一 DHCP 客户端传递上述参数时，如果该客户端有指定的 IP 地址，该地址将忽略从 DHCP 服务器接收到的所有动态信息。*

2. 在可以将多个接口绑定到 Trust 区段的装置上，缺省接口是第一个被绑定到该区段并分配了 IP 地址的接口。
3. 括号中的数字表示所支持的服务器数量。

DHCP 服务器

一台 NetScreen 设备最多可支持八个 DHCP 服务器，这些服务器可以位于任意区段内的任一物理接口或 VLAN 接口上。充当 DHCP 服务器时， NetScreen 设备以两种模式分配 IP 地址和子网掩码：

- 在“动态”模式下，充当 DHCP 服务器的 NetScreen 设备会将地址池[4] 中的 IP 地址分配（或“租借”）给 DHCP 客户端主机。可在一定时间内租用该 IP 地址，也可无限期租用，直到客户端放弃该 IP 地址为止。（要定义无限租用期，请输入 0。）
- 在“保留”模式下，特定客户端每次联机时， NetScreen 设备都会从地址池中专门为其分配一个指定的 IP 地址。

> ***注意：****NetScreen 设备将通过 DHCP 分配的所有 IP 地址保存到闪存中。因此，重新启动 NetScreen 设备不影响地址分配。*

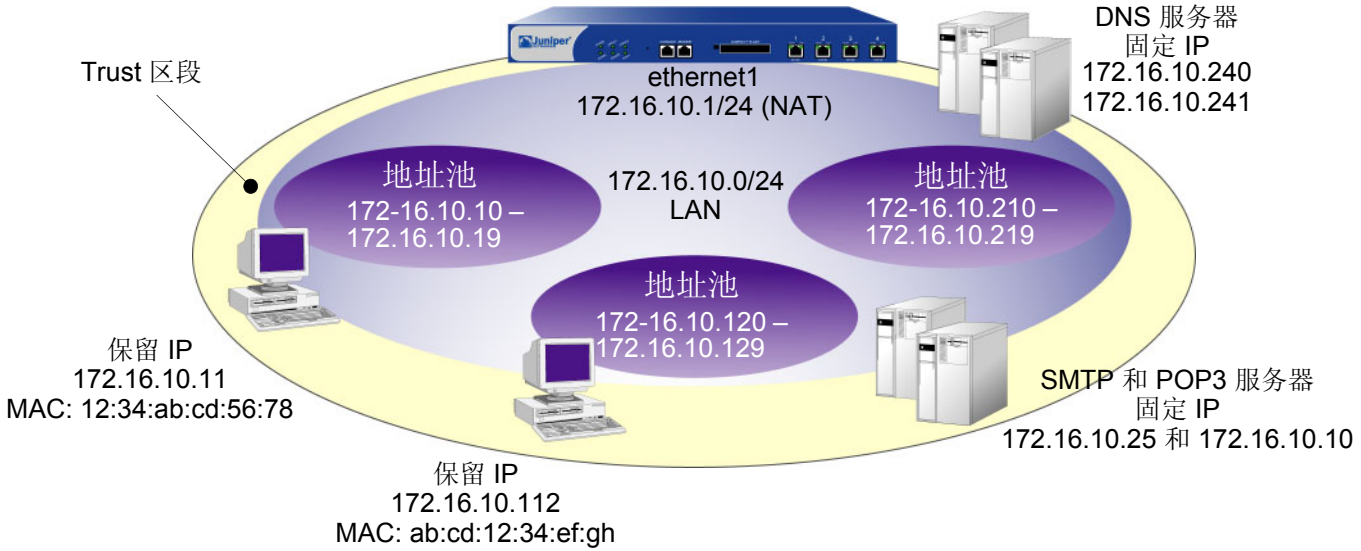
范例：充当 DHCP 服务器的 NetScreen 设备

用 DHCP 将 Trust 区段内的 172.16.10.0/24 网络分成三个 IP 地址池。

- 172.16.10.10 through 172.16.10.19
- 172.16.10.120 through 172.16.10.129
- 172.16.10.210 through 172.16.10.219

DHCP 服务器将动态分配所有 IP 地址，只有使用预留 IP 地址的两个工作站和使用静态 IP 地址的四个服务器除外。接口 ethernet1 绑定到 Trust 区段，其 IP 地址为 172.16.10.1/24，并且处于 NAT 模式。域名是 dynamic.com。

4. 地址池是指同一子网内的 IP 地址的定义范围， NetScreen 设备可以从中提取 DHCP 地址进行分配。最多可以编组 255 个 IP 地址。



WebUI

1. 地址

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

   Address Name: DNS#1

   Comment: Primary DNS Server

   IP Address/Domain Name:

   IP/Netmask: (选择), 172.16.10.240/32

   Zone: Trust

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

Address Name: DNS#2

Comment: Secondary DNS Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.241/32

Zone: Trust

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

Address Name: SMTP

Comment: SMTP Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.25/32

Zone: Trust

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

Address Name: POP3

Comment: POP3 Server

IP Address/Domain Name:

IP/Netmask: (选择), 172.16.10.110/32

Zone: Trust

2. DHCP 服务器

Network > DHCP > Edit (对于 ethernet1) > DHCP Server: 输入以下内容，然后单击 **Apply**:[5]

Lease: Unlimited (选择)

WINS#1: 0.0.0.0

DNS#1: 172.16.10.240

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

WINS#2: 0.0.0.0

DNS#2: 172.16.10.241

DNS#3: 0.0.0.0

SMTP: 172.16.10.25

POP3: 172.16.10.110

NEWS: 0.0.0.0

NetInfo Server #1: 0.0.0.0

NetInfo Server #2: 0.0.0.0

NetInfo Tag: (保留字段为空)

Domain Name: dynamic.com

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

Dynamic: (选择)

IP Address Start: 172.16.10.10

IP Address End: 172.16.10.19

5. 如果将 Gateway 和 Netmask 字段保留为 0.0.0.0，DHCP 服务器模块会将设置给 ethernet1 的 IP 地址和网络掩码发送到其客户端 (本例中为 172.16.10.1 和 255.255.255.0)。但是，如果让 DHCP 客户端模块将 TCP/IP 设置转发给 DHCP 服务器模块 (请参阅第 390 页上的 “TCP/IP 设置传播”)，则必须在 Gateway 和 Netmask 字段中手动输入 172.16.10.1 和 255.255.255.0。

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

Dynamic: (选择)

IP Address Start: 172.16.10.120

IP Address End: 172.16.10.129

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

Dynamic: (选择)

IP Address Start: 172.16.10.210

IP Address End: 172.16.10.219

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

Reserved: (选择)

IP Address: 172.16.10.11

Ethernet Address: 1234 abcd 5678

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

Reserved: (选择)

IP Address: 172.16.10.112

Ethernet Address: abcd 1234 efgh

CLI

1. 地址

```
set address trust dns1 172.16.10.240/32 "primary dns server"
set address trust dns2 172.16.10.241/32 "secondary dns server"
set address trust snmp 172.16.10.25/32 "snmp server"
set address trust pop3 172.16.10.110/32 "pop3 server"
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server option domainname dynamic.com[6]
set interface ethernet1 dhcp server option lease 0
set interface ethernet1 dhcp server option dns1 172.16.10.240
set interface ethernet1 dhcp server option dns2 172.16.10.241
set interface ethernet1 dhcp server option smtp 172.16.10.25
set interface ethernet1 dhcp server option pop3 172.16.10.110
set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19
set interface ethernet1 dhcp server ip 172.16.10.120 to 172.16.10.129
set interface ethernet1 dhcp server ip 172.16.10.210 to 172.16.10.219
set interface ethernet1 dhcp server ip 172.16.10.11 mac 1234abcd5678
set interface ethernet1 dhcp server ip 172.16.10.112 mac abcd1234efgh
set interface ethernet1 dhcp server service
save
```

6. 如果不设置网关或网络掩码的 IP 地址，DHCP 服务器模块会向其客户端发送 ethernet1 的 IP 地址和网络掩码 (本例中为 172.16.10.1 和 255.255.255.0)。但是，如果让 DHCP 客户端模块将 TCP/IP 设置转发给 DHCP 服务器模块 (请参阅第 390 页上的 “TCP/IP 设置传播”)，则必须手动设置这些选项 : **set interface ethernet1 dhcp server option gateway 172.16.10.1** 和 **set interface ethernet1 dhcp server option netmask 255.255.255.0**。

DHCP 服务器选项

当您为接口指定 DHCP 服务器时，可能需要指定一些选项来标识服务器或提供由服务器使用的信息。例如，可以指定主 DNS 服务器和辅 DNS 服务器的 IP 地址，或设置 IP 地址租用时间。

以下为预定义的 DHCP 服务，*RFC 2132, "DHCP Options and BOOTP Vendor Extensions"* 中对这些服务进行了阐述。

术语	NetScreen CLI 术语	选项代码
Subnet Mask	netmask	1
Router Option	gateway	3
Domain Name Server	dns1, dns2, dns3	6
Domain Name	domainname	15
NetBIOS over TCP/IP Name Server Option	wins1, wins2	44
IP Address Lease Time	lease	51
SMTP Server Option	smtp	69
POP3 Server Option	pop3	70
NNTP Server Option	news	71
(不适用)	nis1, nis2	112
(不适用)	nistag	113

当预定义的服务器选项无法满足需要时，您可以定义定制的 DHCP 服务器选项。例如，对于某些 VoIP (IP 语音) 配置而言，发送预定义服务器选项不支持的额外配置信息是必需的。在这种情况下，您必须定义相应的定制选项。

范例 : 定制 DHCP 服务器选项

在下例中，您将为充当 DHCP 客户端的 IP 电话创建 DHCP 服务器定义。这些电话使用下列定制选项 :

- 选项代码 444，包含字符串 “Server 4”
- 选项代码 66，包含 IP 地址 1.1.1.1
- 选项代码 160，包含整数 2004

CLI

1. 地址

```
set address trust dns1 172.16.10.240/32 “primary dns server”
set address trust dns2 172.16.10.241/32 “secondary dns server”
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server option domainname dynamic.com
set interface ethernet1 dhcp server option lease 0
set interface ethernet1 dhcp server option dns1 172.16.10.240
set interface ethernet1 dhcp server option dns2 172.16.10.241
set interface ethernet1 dhcp server option custom 444 string “Server 4”
set interface ethernet1 dhcp server option custom 66 ip 1.1.1.1
set interface ethernet1 dhcp server option custom 160 integer 2004
set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19
```

NSRP 集群中的 DHCP 服务器

当冗余 NSRP 集群中的主单元行使 DHCP 服务器的功能时，该集群中的所有成员都将维护全部的 DHCP 配置以及 IP 地址分配。一旦发生故障切换，新的主单元将负责维护所有 DHCP 分配。但是，终止 HA 通信将破坏集群成员之间现有 DHCP 分配的同步。恢复 HA 通信后，通过在集群的两个单元上使用以下 CLI 命令，可以再次同步 DHCP 分配 : **set nsrp rto-mirror sync**。

DHCP 服务器检测

在 NetScreen 设备上启动 DHCP 服务器时，系统首先要检查该接口上是否已存在 DHCP 服务器。如果检测到网络上存在其它 DHCP 服务器， ScreenOS 会自动终止本地 DHCP 服务器进程的启动。为检测其它 DHCP 服务器，设备每隔两秒自动发送一次 DHCP 启动请求。如果发出启动请求后没有收到任何响应，设备随即会启动本地的 DHCP 服务器进程。

如果 NetScreen 设备收到其它 DHCP 服务器发出的响应，系统会生成一条消息，指出已在 NetScreen 设备上启用了 DHCP 服务，但由于网络上存在另一 DHCP 服务器，因此没有启动该服务器。日志消息中存在现有 DHCP 服务器的 IP 地址。

可以设置以下三种操作模式以便在接口上检测 DHCP 服务器 : Auto、 Enable 或 Disable[7]。在 Auto 模式下，NetScreen 设备启动时始终检测现有的 DHCP 服务器。通过将 NetScreen DHCP 服务器设置为 Enable 或 Disable 模式，可以将设备配置为不尝试检测接口上的其它 DHCP 服务器。在 Enable 模式下， DHCP 服务器始终开启，设备不检测网络上是否存在现有 DHCP 服务器。在 Disable 模式下， DHCP 服务器始终关闭。

7. 对于 NetScreen-5XP 和 NetScreen-5XT 设备， Auto 模式是缺省的 DHCP 服务器检测模式。对于支持 DHCP 服务器的其它 NetScreen 设备， Enable 模式是缺省的 DHCP 服务器检测模式。

范例 : 打开 DHCP 服务器检测

在本例中，将设置 ethernet1 接口上的 DHCP 服务器，在其启动前首先检测该接口上是否存在 DHCP 服务器。

WebUI

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

Server Mode: Auto (选择)

CLI

```
set interface ethernet1 dhcp server auto
save
```

范例 : 关闭 DHCP 服务器检测

在本例中，将设置 ethernet1 接口上的 DHCP 服务器，在其启动时不检测网络上是否存在 DHCP 服务器。

WebUI

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

Server Mode: Enable (选择)

CLI

```
set interface ethernet1 dhcp server enable
save
```

注意 : *发出 CLI 命令* ***set interface*** interface ***dhcp server service*** *后， DHCP 服务器将被激活。如果将接口的 DHCP 服务器检测模式设置为 Auto，那么只有当 NetScreen 设备在网络上找不到现有服务器时，才会启动该 DHCP 服务器。发出* ***unset interface*** interface ***dhcp server service*** *命令后，将禁用 NetScreen 设备上的 DHCP 服务器，并删除任何现有的 DHCP 配置。*

DHCP 中继代理

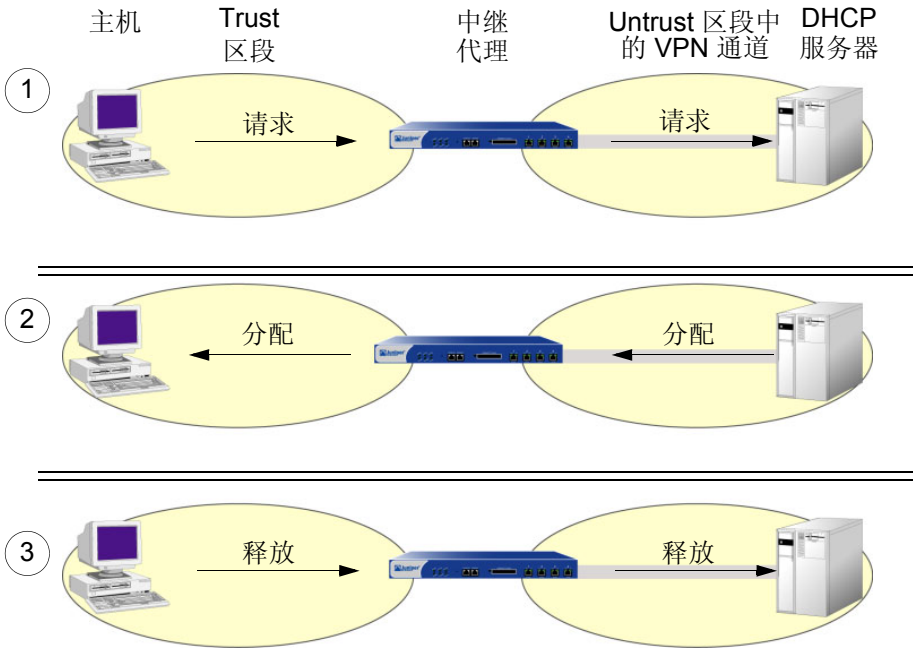
充当 DHCP 中继代理时，NetScreen 设备负责在一个区段内的主机与另一个区段内的 DHCP 服务器之间转发 DHCP 请求和分配信息。 DHCP 消息可以在 NetScreen 设备与 DHCP 服务器之间公开传送，或通过 VPN 通道进行传送。

虽然您不能在同一接口上配置 DHCP 中继代理和 DHCP 服务器或客户端功能，但却可以在 NetScreen 设备中的一个或多个物理接口或 VLAN 接口上配置 DHCP 中继代理。当 NetScreen 设备用作 DHCP 中继代理时，其接口必须处于 Route (路由) 模式或 Transparent (透明) 模式。对于 “路由” 模式的接口，必须为预定义的 DHCP 中继服务配置从一个区段到另一个区段的策略。对于 “透明” 模式的接口， DHCP 客户端必须在 V1-Trust 区段中，而 DHCP 服务器既可以在 V1-Untrust 区段中，也可以在 V1-DMZ 区段中。不必为 “透明” 模式的接口配置策略。

一个 DHCP 中继代理最多可以配置三个 DHCP 服务器。中继代理将 DHCP 客户端的地址请求单播到所有已配置的 DHCP 服务器上。随后，中继代理将收到的第一个服务器响应转发给客户端。

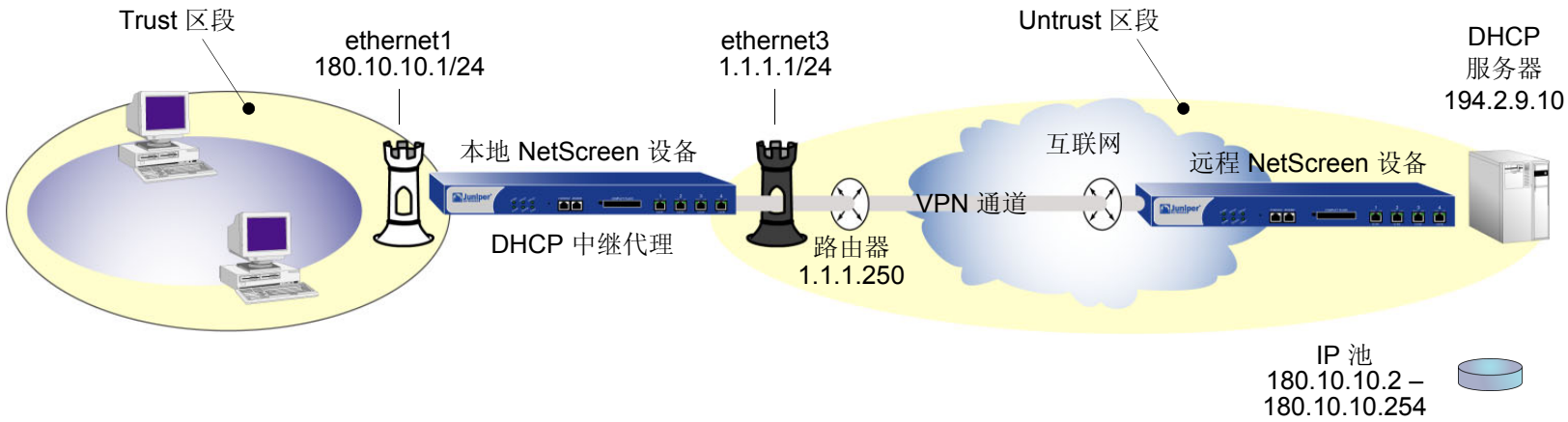
注意：*当 NetScreen 设备充当 DHCP 中继代理时，由于远程 DHCP 服务器控制着所有 IP 地址分配，所以 NetScreen 设备不会生成 DHCP 分配状态报告。*

下面的示意图展示了使用 NetScreen 设备作为 DHCP 中继代理的相关过程。请注意，当 DHCP 消息在不可信网络中传送时，为确保安全，这些消息将通过 VPN 通道进行传送。



范例 : NetScreen 设备作为 DHCP 中继代理

在本例中， NetScreen 设备从 IP 地址为 194.2.9.10 的 DHCP 服务器接收 DHCP 信息，而后将其转递给 Trust 区段中的主机。主机从 DHCP 服务器上定义的 IP 池中接收 IP 地址。地址范围是 180.10.10.2—180.10.10.254。 DHCP 消息流经本地 NetScreen 设备和 DHCP 服务器之间的 VPN 通道，该 DHCP 服务器位于 Untrust 区段接口 IP 地址为 2.2.2.2/24 的远程 NetScreen 设备之后。接口 ethernet1 被绑定到 Trust 区段， IP 地址为 180.10.10.1/24，且处于“路由”模式。接口 ethernet3 被绑定到 Untrust 区段中， IP 地址为 1.1.1.1/24。所有安全区段都在 trust-vr 路由选择域中。



WebUI

1. 接口

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 180.10.10.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: Route

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

Zone: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: DHCP Server

IP Address/Domain Name:

IP/Netmask: (选择), 194.2.9.10/32

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: dhcp server

Security Level: Custom

Remote Gateway Type:

Static IP: (选择), Address/Hostname: 2.2.2.2

Outgoing Interface: ethernet3

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

Security Level:

User Defined: Custom (选择)

Phase1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: to_dhcp

Security Level: Compatible

Remote Gateway:

Predefined: (选择), to_dhcp

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

Bind To: None

4. DHCP 中继代理

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

Relay Agent Server IP or Domain Name: 194.2.9.10

Use Trust Zone Interface as Source IP for VPN: (选择)

5. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250[8]

6. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), DHCP Server

Service: DHCP-Relay

Action: Tunnel

Tunnel VPN: to_dhcp

Modify matching outgoing VPN policy: (选择)

8. 对于出站 VPN 和网络信息流，设置到指定为缺省网关的外部路由器的路由至关重要。在本例中，NetScreen 设备将向这个路由器发送经过封装的 VPN 信息流，该路由器是路由到远程 NetScreen 设备路径上的首个跳跃。在本范例的图解中，通过对经过该路由器的通道的描述介绍此概念。

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 180.10.10.1/24
set interface ethernet1 route
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address untrust dhcp_server 194.2.9.10/32
```

3. VPN

```
set ike gateway "dhcp server" ip 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set vpn to_dhcp gateway "dhcp server" proposal g2-esp-3des-sha
```

4. DHCP 中继代理

```
set interface ethernet1 dhcp relay server-name 194.2.9.10
set interface ethernet1 dhcp relay vpn
```

5. 路由

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

6. 策略

```
set policy from trust to untrust any dhcp_server dhcp-relay tunnel vpn to_dhcp
set policy from untrust to trust dhcp_server any dhcp-relay tunnel vpn to_dhcp
save
```

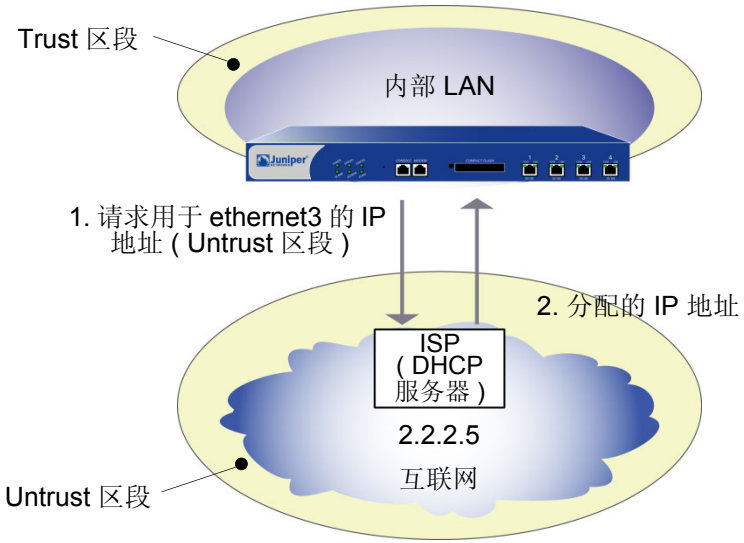
DHCP 客户端

充当 DHCP 客户端时， NetScreen 设备接收服务器为任意安全区段内的任意物理接口动态分配的 IP 地址。如果有多个接口绑定到同一安全区段，则可为所有接口配置一个 DHCP 客户端，前提是任意两个接口都没有连接到同一网络区段。如果为连接到同一网络区段的两个接口配置了一个 DHCP 客户端，则只使用 DHCP 服务器分配的第一个地址。 (如果 DHCP 客户端收到同一 IP 地址的地址更新，则不必重新指定 IKE 密钥。)

注意：*由于某些 NetScreen 设备可以同时充当 DHCP 服务器、 DHCP 中继代理或 DHCP 客户端，因此不能在同一接口上配置多个 DHCP 角色。*

范例 : NetScreen 设备作为 DHCP 客户端

在本例中，绑定到 Untrust 区段的接口有一个动态分配的 IP 地址。当 NetScreen 设备向其 ISP 请求 IP 地址时，它会接收到 IP 地址、子网掩码、网关 IP 地址以及租用该地址的期限。 DHCP 服务器的 IP 地址为 2.2.2.5。



注意：在设立 DHCP 服务站点之前，您必须拥有下列设备：

- *数字用户线 (DSL) 调制解调器和线缆*
- *ISP 帐户*

WebUI

Network > Interfaces > Edit (对于 ethernet3): 选择 **Obtain IP using DHCP**[9]，然后单击 **OK**。

CLI

```
set interface ethernet3 dhcp client
set interface ethernet3 dhcp settings server 2.2.2.5
save
```

9. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址，但可通过 CLI 执行这一操作。

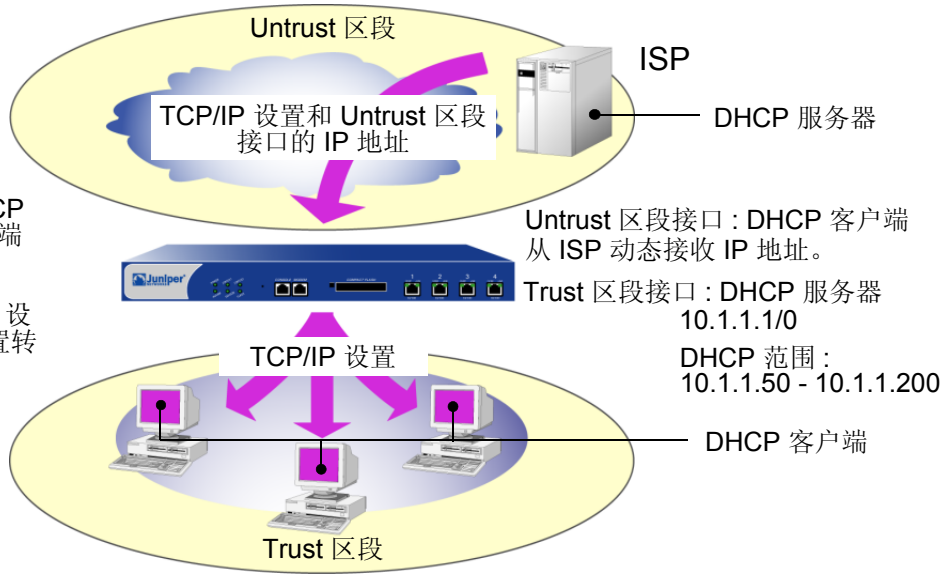
TCP/IP 设置传播

某些 NetScreen 设备可以充当 “动态主机控制协议” (DHCP) 客户端，从外部 DHCP 服务器接收任意安全区段内的任意物理接口的 TCP/IP 设置和 IP 地址。某些 NetScreen 设备可以充当 DHCP 服务器，为任意区段内的客户端提供 TCP/IP 设置和 IP 地址。当 NetScreen 设备同时充当 DHCP 客户端和 DHCP 服务器时，可将通过 DHCP 客户端模块获知的 TCP/IP 设置传送给缺省的 DHCP 服务器模块[10]。 TCP/IP 设置包括缺省网关的 IP 地址和子网掩码，以及下列服务器的全部或部分 IP 地址 :

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)

NetScreen 设备既是 Untrust 区段中 DHCP 服务器的客户端，又是 Trust 区段中客户端的 DHCP 服务器。

该设备先作为 DHCP 客户端接收 TCP/IP 设置，然后再作为 DHCP 服务器将这些设置转发给 Trust 区段中的客户端。



10. 尽管每个物理接口或 VLAN 接口上最多可以配置八个 DHCP 服务器，但设备的缺省 DHCP 服务器只能位于每个平台的特定接口上。在 NetScreen-5XP 上，缺省 DHCP 服务器在 Trust 接口上。在 NetScreen-5XT 上，缺省 DHCP 服务器位于以下特定接口上 : Trust-Untrust 端口模式的 Trust 接口、Dual-Untrust 端口模式的 ethernet1 接口以及 Home-Work 和 Combined 端口模式的 ethernet2 接口。对于其它设备，缺省 DHCP 服务器在 ethernet1 接口上。

使用 **set interface** *interface* **dhcp-client settings update-dhcpserver** 命令，可以对 DHCP 服务器模块进行配置，使其传播从 DHCP 客户端模块接收的所有 TCP/IP 设置。还可以使用其它设置覆盖某个设置。

范例：转发 TCP/IP 设置

在本例中，将对 NetScreen 设备进行配置，使其既充当 ethernet3 接口上的 DHCP 客户端又充当 ethernet1 接口上的 DHCP 服务器。（缺省 DHCP 服务器位于 ethernet1 接口上。）

作为 DHCP 客户端， NetScreen 设备可从外部 DHCP 服务器（地址为 211.3.1.6）接收 ethernet3 接口的 IP 地址和 TCP/IP 设置。随后，您需要启用 NetScreen 设备的 DHCP 客户端模块，将收到的 TCP/IP 设置传送到 DHCP 服务器模块。

您需配置 NetScreen DHCP 服务器模块，对从 DHCP 客户端模块接收到的 TCP/IP 设置执行下列操作：

- 转发 DNS IP 地址到其在 Trust 区段中的 DHCP 客户端。
- 用下列信息覆盖缺省网关[11]、网络掩码、 SMTP 服务器和 POP3 服务器的 IP 地址：
  - 10.1.1.1（这是 ethernet1 接口的 IP 地址）
  - 255.255.255.0（这是 ethernet1 接口的网络掩码）
  - SMTP: 211.1.8.150
  - POP3: 211.1.8.172

您还需配置 DHCP 服务器模块以发送下列未从 DHCP 客户端模块接收到的 TCP/IP 设置：

- Primary WINS server: 10.1.2.42
- Secondary WINS server: 10.1.5.90

最后，需要配置 DHCP 服务器模块，将以下 IP 池中的 IP 地址分配给 Trust 区段内充当 DHCP 客户端的主机：10.1.1.50 – 10.1.1.200。

11. 如果 DHCP 服务器已在 Trust 接口上启用并有已定义的 IP 地址池（这是某些 NetScreen 设备上的缺省行为），您必须先删除 IP 地址池，然后才能更改缺省网关和网络掩码。

WebUI

注意：只能通过 CLI 设置此功能。

CLI

1. DHCP 客户端

```
set interface ethernet3 dhcp-client settings server 211.3.1.6
set interface ethernet3 dhcp-client settings update-dhcpserver
set interface ethernet3 dhcp-client settings autoconfig
set interface ethernet3 dhcp-client enable
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server option gateway 10.1.1.1
set interface ethernet1 dhcp server option netmask 255.255.255.0
set interface ethernet1 dhcp server option wins1 10.1.2.42
set interface ethernet1 dhcp server option wins2 10.1.5.90
set interface ethernet1 dhcp server option pop3 211.1.8.172
set interface ethernet1 dhcp server option smtp 211.1.8.150
set interface ethernet1 dhcp server ip 10.1.1.50 to 10.1.1.200
set interface ethernet1 dhcp server service
save
```

PPPoE

“以太网点对点协议” (PPPoE) 结合了 “点对点协议” (PPP) 和以太网协议，前者 (PPP) 通常用于拨号连接，后者用于将一个站点上的多个用户连接到同一用户端设备。虽然多个用户可以共享同一物理连接，但访问控制、计费以及服务类型等仍按单个用户处理。某些 NetScreen 设备支持 PPPoE 客户端，允许使用 PPPoE 访问其客户端互联网，以兼容方式在 ISP 管理的 DSL、 Ethernet Direct 和电缆网络上运行。

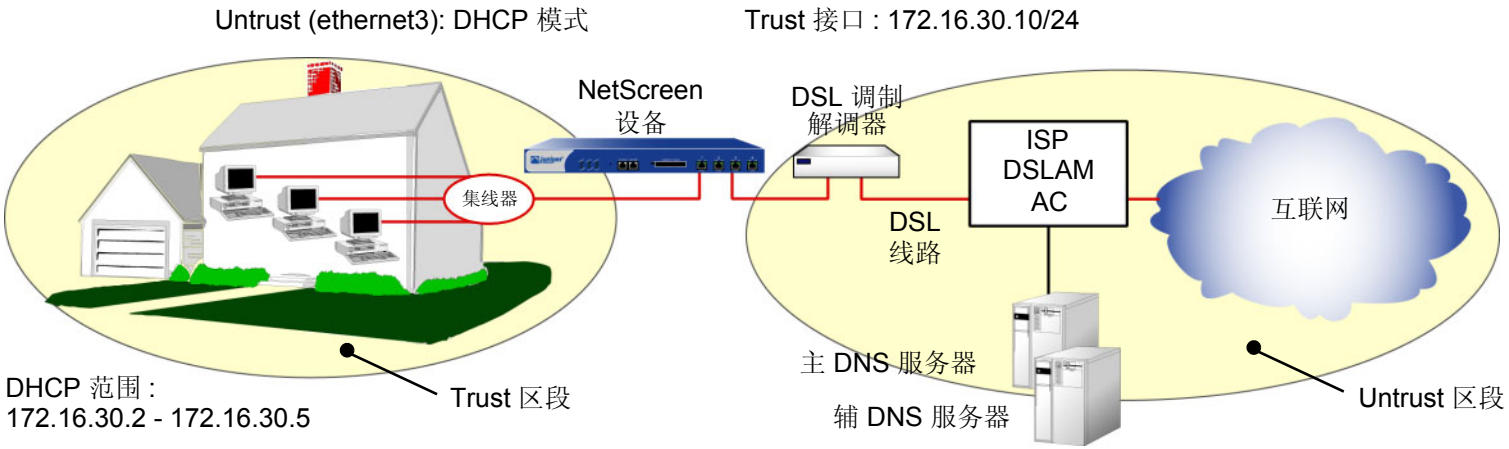
在支持 PPPoE 的设备上，可以在部分或全部接口上配置 PPPoE 客户端实例。可以使用用户名、密码和其它参数配置特定的 PPPoE 实例，然后将该实例绑定到接口上。当有两个 Ethernet 接口 (主接口和备份接口) 绑定到 Untrust 区段时，可以只配置一个接口，也可以在两个接口上全部配置 PPPoE。例如，处于 Dual Untrust 端口模式[12] 时，可以在主接口 (ethernet3) 上配置 DHCP，而在备份接口 (ethernet2) 上配置 PPPoE。也可以在主接口和备份接口上全部配置 PPPoE。

范例：设置 PPPoE

下面的例子将阐述如何为 PPPoE 连接定义 NetScreen 设备的不可信接口，以及如何启动 PPPoE 服务。

在本例中， NetScreen 设备将从 ISP 那里接收为 Untrust 区段接口 (ethernet3) 动态分配的 IP 地址，并为 Trust 区段内的三台主机动态分配 IP 地址。在本例中，NetScreen 设备既充当 PPPoE 客户端又充当 DHCP 服务器。Trust 区段接口必须处于 NAT 模式或 “路由” 模式。在本例中，它处于 NAT 模式。

12. 某些 NetScreen 设备支持端口模式，例如 NetScreen-5XT。



在为 PPPoE 服务设立本例中的站点之前，必须具有以下设备 :

- 数字用户线 (DSL) 调制解调器和线缆
- ISP 帐户
- 用户名及密码 (ISP 提供)

WebUI

1. 接口和 PPPoE

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

Zone: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 172.16.30.10/24

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

Zone: Untrust

Obtain IP using PPPoE: (选择)

User Name/Password: < 名称 >/< 密码 >

Network > Interfaces > Edit (对于 ethernet3): 要测试 PPPoE 连接，请单击 **Connect**。

注意：*建立 PPPoE 连接后， ISP 会自动为 Untrust 区段接口和 “域名服务” (DNS) 服务器提供 IP 地址。如果 NetScreen 设备通过 PPPoE 接收 DNS 地址，则缺省情况下，新的 DNS 设置将覆盖本地设置。如果不希望新的 DNS 设置取代本地设置，可使用 CLI 命令* ***unset pppoe dhcp-updateserver*** *禁止此行为。如果使用 Untrust 区段接口的静态 IP 地址，则必须先获得 DNS 服务器的 IP 地址，然后在 NetScreen 设备和 Trust 区段的主机上手动输入这些地址。*

2. DHCP 服务器

Network > Interfaces > Edit (对于 ethernet1) > DHCP: 选择 **DHCP Server**，然后单击 **Apply**。

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

Lease: 1 hour

Gateway: 0.0.0.0

Netmask: 0.0.0.0

DNS#1: 0.0.0.0

> Advanced: 输入以下内容，然后单击 **Return**:

DNS#2: 0.0.0.0

Domain Name: (保留空白)

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

Dynamic: (选择)
IP Address Start: 172.16.30.2
IP Address End: 172.16.30.5

3. 激活 NetScreen 设备上的 PPPoE

关闭 DSL 调制解调器、 NetScreen 设备和三台工作站的电源。

打开 DSL 调制解调器。

打开 NetScreen 设备。

NetScreen 设备与 ISP 建立 PPPoE 连接，并通过 ISP 获得 DNS 服务器的 IP 地址。

4. 激活内部网络上的 DHCP

打开工作站。

工作站自动接收 DNS 服务器的 IP 地址。在它们尝试进行 TCP/IP 连接时，它们会获得自己的 IP 地址。

注意：*使用 DHCP 为 Trust 区段的主机分配 IP 地址时， NetScreen 设备会自动将从 ISP 接收的 DNS 服务器的 IP 地址转发给该主机。*

如果不通过 DHCP 动态分配主机 IP 地址，必须在每台主机中手动输入 DNS 服务器的 IP 地址。

Trust 区段中的主机与 Untrust 区段建立的每个 TCP/IP 连接都要自动经过 PPPoE 封装处理。

CLI

1. 接口和 PPPoE

```
set interface ethernet1 zone trust
set interface ethernet1 ip 172.16.30.10/24
set interface ethernet3 zone untrust
set pppoe interface ethernet3
set pppoe username name_str password pswd_str
```

测试 PPPoE 连接：

```
exec pppoe connect
get pppoe
```

2. DHCP 服务器

```
set interface ethernet1 dhcp server service
set interface ethernet1 dhcp server ip 172.16.30.2 to 172.16.30.5
set interface ethernet1 dhcp server option lease 60
save
```

3. 激活 NetScreen 设备上的 PPPoE

关闭 DSL 调制解调器、 NetScreen 设备和三台工作站的电源。

打开 DSL 调制解调器。

打开 NetScreen 设备。

4. 激活内部网络上的 DHCP

打开工作站。

工作站自动接收 DNS 服务器的 IP 地址。在它们尝试进行 TCP/IP 连接时，它们会获得自己的 IP 地址。

Trust 区段中的主机与 Untrust 区段建立的每个 TCP/IP 连接都要自动经过 PPPoE 封装处理。

范例：在主 Untrust 接口和备份 Untrust 接口上配置 PPPoE

在本例中， NetScreen-5XT 处于 Dual Untrust 模式。在下例中，将为 Untrust 区段的主 (ethernet3) 接口和备份 (ethernet2) 接口配置 PPPoE。

WebUI

ethernet3 接口的 PPPoE 配置

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

PPPoE instance: eth3-pppoe

Bound to interface: ethernet3 (选择)

Username: user1

Password: 123456

Authentication: Any (选择)

Access Concentrator: ac-11

ethernet2 接口的 PPPoE 配置

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

PPPoE instance: eth2-pppoe

Bound to interface: ethernet2 (选择)

Username: user2

Password: 654321

Authentication: Any (选择)

Access Concentrator: ac-22

CLI

1. ethernet3 接口的 PPPoE 配置

```
set pppoe name eth3-pppoe username user1 password 123456
set pppoe name eth3-pppoe ac ac-11
set pppoe name eth3-pppoe authentication any
set pppoe name eth3-pppoe interface ethernet3
```

2. ethernet2 接口的 PPPoE 配置

```
set pppoe name eth2-pppoe username user2 password 654321
set pppoe name eth2-pppoe ac ac-22
set pppoe name eth2-pppoe authentication any
set pppoe name eth2-pppoe interface ethernet2
save
```

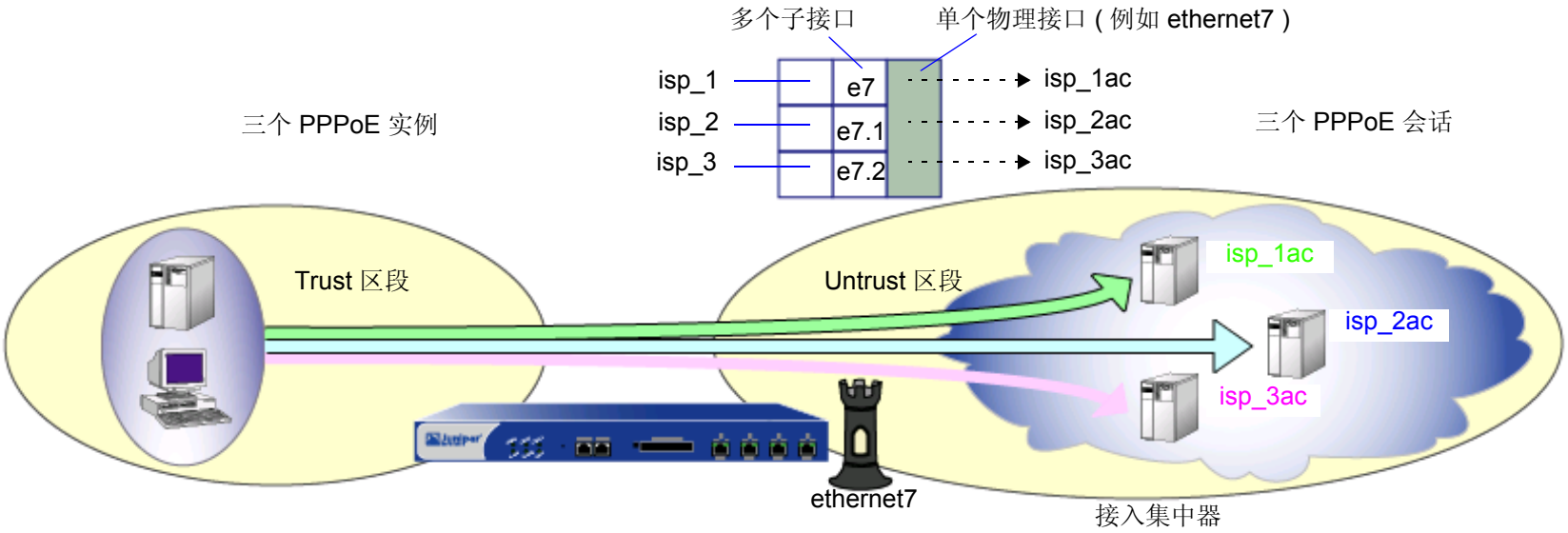
单个接口上的多个 PPPoE 会话

某些 NetScreen 设备支持为给定的物理接口创建多个 PPPoE 子接口 (所有子接口具有相同的 MAC 地址)。这种支持允许您与一个 ISP 建立专用网络连接，并使用同一个物理接口经由另一个 ISP 连接到互联网上。可以使用不同的用户名或域名建立这些连接或同时连接到不同的 ISP。

一个物理接口中并发 PPPoE 会话的最大数量仅通过设备允许的子接口的数量来限制。对可支持多个会话的物理接口数量没有进行限制。可以对每个 PPPoE 实例或会话分别指定用户名、静态 IP、空闲超时、自动连接和其它参数。

未标记的接口

要支持 PPPoE 会话，子接口必须是未标记的。未标记的接口不使用 VLAN 标记来标识子接口的 VLAN。而是使用一种被称为 encap 的功能，将子接口绑定到 PPPoE 封装中。这样，通过托管多个子接口，单个物理接口可以托管多个 PPPoE 实例。由于可配置每个实例转至指定的 “接入集中器” (AC)，因此允许单独实体 (例如 ISP) 通过单个接口管理 PPPoE 会话。有关 VLAN 和 VLAN 标记的详细信息，请参阅第 9 卷，“虚拟系统”。



范例：多个 PPPoE 实例

在下例中，您将定义三个 PPPoE 实例，并为每个实例指定一个接入集中器 (AC)，然后启动每个实例。

- 实例 isp_1，用户名 “user1@domain1”，密码 “swordfish”，绑定到接口 ethernet7。 AC 命名为 “isp_1ac”。
- 实例 isp_2，用户名 “user2@domain2”，密码 “marlin”，绑定到接口 ethernet7.1。 AC 命名为 “isp_2ac”。
- 实例 isp_3，用户名 “user3@domain3”，密码 “trout”，绑定到接口 ethernet7.2。 AC 命名为 “isp_3ac”。

WebUI

接口和子接口

1. Network > Interfaces > Edit (对于 ethernet7): 输入以下内容，然后单击 **OK**:

   Zone Name: Untrust

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

   Interface Name: ethernet7.1

   Zone Name: Untrust

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

   Interface Name: ethernet7.2

   Zone Name: Untrust

PPPoE 实例和 AC

4. Network > PPPoE > New: 输入以下内容，然后单击 **OK**:
   PPPoE Instance: isp_1
   Enable: Enable
   Bound to Interface: ethernet7
   Username: user1@domain1
   Access Concentrator: isp_1ac
5. Network > PPPoE > New: 输入以下内容，然后单击 **OK**:
   PPPoE Instance: isp_2
   Enable: Enable
   Bound to Interface: ethernet7.1
   Username: user2@domain2
   Access Concentrator: isp_2ac
6. Network > PPPoE > New: 输入以下内容，然后单击 **OK**:
   PPPoE instance: isp_3
   Enable: Enable
   Bound to interface: ethernet7.2
   Username: user3@domain3
   Access Concentrator: isp_3ac

启动 PPPoE

7. Network > PPPoE > Connect (对于 isp_1)
8. Network > PPPoE > Connect (对于 isp_2)
9. Network > PPPoE > Connect (对于 isp_3)

CLI

1. 接口和子接口

```
set interface ethernet7 zone untrust
set interface ethernet7.1 encap pppoe zone untrust
set interface ethernet7.2 encap pppoe zone untrust
```

2. PPPoE 实例和 AC

```
set pppoe name isp_1 username user1@domain1 password swordfish
set pppoe name isp_1 interface ethernet7
set pppoe name isp_1 ac isp_1ac
set pppoe name isp_2 username user2@domain2 password marlin
set pppoe name isp_2 interface ethernet7.1
set pppoe name isp_2 ac isp_2ac
set pppoe name isp_3 username user3@domain3 password trout
set pppoe name isp_3 interface ethernet7.2
set pppoe name isp_3 ac isp_3ac
save
```

3. 启动 PPPoE

```
exec pppoe name isp_1 connect
exec pppoe name isp_2 connect
exec pppoe name isp_3 connect
```

PPPoE 和高可用性

支持 PPPoE 的处于主动 / 被动模式下的两台 NetScreen 设备可以处理 PPPoE 连接的故障切换。启动连接时，主设备与备份设备的 PPPoE 状态同步。由于被动设备与主设备使用同一 IP 地址，因此当其成为主设备后，不必创建新的 PPPoE 连接。因此，当主设备发生故障后，被动设备可保持与接入集中器的通信。当 PPPoE 接口支持 VPN 连接，并且在发生故障后必须使用相同的接口 IP 继续保持这些连接时，这是必要的。有关高可用性配置的详细信息，请参阅第 10 卷，“高可用性”。

升级和降级固件

本节介绍三种升级 NetScreen 设备的方法：

- Web 用户界面 (WebUI)
- 命令行界面 (CLI)
- 启动加载程序或 ScreenOS 加载程序

这些方法的具体步骤会因您在单独设备还是在配置为高可用性的设备上下载固件而有所不同。

***注意：**如果您所用版本低于 5.0.0 (例如 4.0.X)，那么，首先需要将其升级到 5.0.0，然后再用 5.1.0 ScreenOS 固件对 NetScreen 进行升级。*

本节包括以下内容：

***重要：**请在开始升级 NetScreen 设备之前保存现有配置文件，并且还要确保一旦需要降级时有权访问 ScreenOS 5.0.0 固件。*

升级和降级设备固件的要求

本节列出了对 NetScreen 设备固件执行升级或降级操作时的要求。可以使用三种方法来升级 NetScreen 设备或将其从 ScreenOS 5.1.0 降级到 ScreenOS 5.0.0: WebUI、 CLI 或者通过启动加载程序或 ScreenOS 加载程序。

注意：*可以本地或远程升级或降级 NetScreen 设备，不过， Juniper Networks 建议您在设备所在位置处执行 NetScreen 设备的升级或降级操作。*

要使用 WebUI，必须具备：

- NetScreen 设备的根或读写权限
- 从您的计算机到 NetScreen 设备的网络访问
- 您的计算机上安装有互联网浏览器
- 新 ScreenOS 固件 (从 Juniper Networks Web 站点下载的且本地保存在您的计算机上)

要使用 CLI，必须具备：

- NetScreen 设备的根或读写权限
- 从您的计算机到 NetScreen 设备的控制台连接或 Telnet 访问
- 在您的计算机上安装有 TFTP 服务器
- 新 ScreenOS 固件 (从 Juniper Networks Web 站点下载的且保存在您计算机上的 TFTP 服务器目录中)

要通过启动加载程序升级或降级，您必须具备：

- NetScreen 设备的根或读写权限
- 在您的计算机或本地网络上安装有 TFTP 服务器
- 从您的计算机到 NetScreen 设备的以太网连接 (为了传输数据，即可传输您计算机中 TFTP 服务器中的数据)
- 从您的计算机到 NetScreen 设备的控制台连接 (为了管理 NetScreen 设备)
- 您的计算机中的 TFTP 服务器目录下保存有新 ScreenOS 固件

要升级或降级 NetScreen 设备，请参阅以下各节中对相应操作步骤的介绍：第 410 页上的 “上传新固件”或第 414 页上的 “升级 NSRP 配置中的 NetScreen 设备”。

NetScreen-Security Manager 服务器连接

如果您希望对其执行降级操作的 NetScreen 设备已连接到 NetScreen-Security Manager 2004 服务器上，那么在降级该设备之前，必须首先执行以下 CLI 命令：

```
unset nsm enable
unset nsm init otp
unset nsm init id
unset nsm server primary
delete nsm keys
save
```

在降级设备之前如果没有执行这些命令，那么下次将设备升级到最新 ScreenOS 版本时，设备将无法连接到 NetScreen-Security Manager 服务器上。

下载新固件

开始升级 NetScreen 设备之前，您必须具有最新的 ScreenOS 固件。您可以从 Juniper Networks Web 站点获得该固件。要访问固件下载，您必须是具有活动用户 ID 和密码的已注册用户。如果您尚未注册您的 NetScreen 产品，那么必须先注册，然后才能继续执行操作。可以在 Juniper Networks Web 站点上注册您的产品。

注意：*降级到 ScreenOS 5.0.0 后，加载到设备上的所有 ScreenOS 5.1.0 密钥都将丢失。不过，在升级到 ScreenOS 5.1.0 之前加载到设备上的密钥仍将保留。*

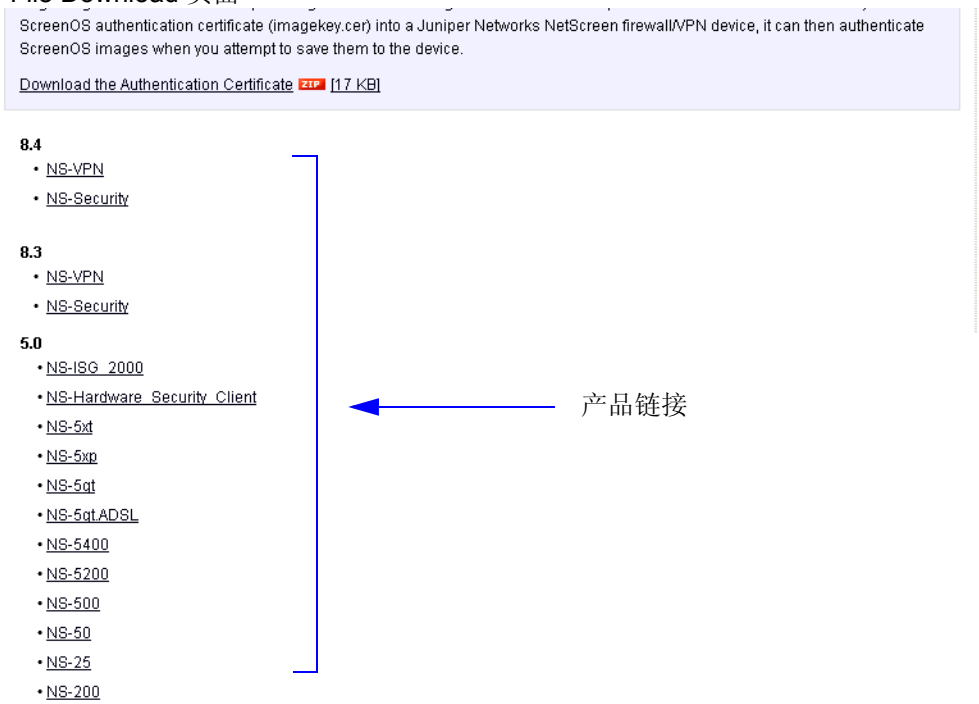
要获取最新的 ScreenOS 固件，请在您的 Web 浏览器中输入 http://www.juniper.net/support。单击 Support > Customer Support Center，然后按照以下步骤进行操作：

1. 输入您的用户 ID 和密码进行登录，然后单击 **LOGIN**。
2. 在 My Technical Assistance Center 下，单击 **Download Software**。

   Juniper 将给出可用下载列表。
3. 单击 **Continue**。

   出现 File Download 页面。

File Download 页面



4. 单击要下载固件的产品链接。

   出现 Upgrades 页面。

5. 单击要下载 ScreenOS 版本的链接。

   出现 Upgrades 页面。

6. 单击升级链接。

   出现 Download File 对话框。

7. 单击 **Save**，然后导航到您要保存固件 Zip 文件的位置。

   必须将固件保存到您要执行升级操作的计算机上。

   – 如果要使用 WebUI 升级 NetScreen 设备，则可将固件保存在任何目录中。
   – 如果要使用 CLI 升级 NetScreen 设备，则请将固件保存在计算机上的根 TFTP 服务器目录中。如果您的计算机上未安装 TFTP 服务器，那么可以从互联网上下载一个。如果没有可用的 TFTP 服务器，那么必须使用 WebUI 将新固件加载到 NetScreen 设备中。

上传新固件

以下是升级单个 NetScreen 设备以及将设备从 ScreenOS 5.1.0 降级到 ScreenOS 5.0.0 的步骤。这些步骤与 NetScreen 设备的运行模式无关。

***注意：**如果您要从早于 ScreenOS 5.0.0 的固件版本升级 NetScreen 设备，那么必须先将固件升级到 ScreenOS 5.0.0，然后再升级到 ScreenOS 5.1.0。请确保保存现有配置，以便先前输入的数据在升级时不会丢失。*

使用 WebUI

要使用 WebUI 加载固件，请执行以下步骤：

1. 确保您具有新 ScreenOS 固件。有关获得新固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 通过打开 Web 浏览器，然后在 Address 字段中输入管理 IP 地址来登录到 NetScreen 设备。以根 admin 或具有读写权限的 admin 身份进行登录。
3. 保存现有配置：
   a. 转至 Configuration > Update > Config File，然后单击 **Save to File**。
   b. 在 File Download 对话框中，单击 **Save**。
   c. 导航到要保存配置文件 (*cfg.txt*) 的位置，然后单击 **Save**。
4. Configuration > Update > ScreenOS/Keys > 选择 **Firmware Update**。
5. 单击 **Browse** 导航到新 ScreenOS 固件的位置或在 Load File 字段中键入该位置的路径。
6. 单击 **Apply**。

   将出现一个具有升级时间信息的消息框。
7. 单击 **OK** 继续。

   NetScreen 设备自动重新启动。当设备在浏览器中显示登录页面时，即完成了升级或降级操作。
8. 登录到 NetScreen 设备。在 WebUI 主页的 Device Information 部分，可以检验 NetScreen 设备 ScreenOS 固件的版本。

使用 CLI

要使用 CLI 加载固件，请执行以下步骤：

1. 确保您具有新 ScreenOS 固件。有关获得新固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 通过应用程序 [例如 Telnet 或安全外壳 (SSH)] 或超级终端 (如果通过控制台端口直接连接) 登录到 NetScreen 设备。以根 admin 或具有读写权限的 admin 身份进行登录。
3. 通过执行 **save config to { flash | slot1 | tftp }** 命令保存现有配置。
4. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。
5. 在 NetScreen 设备上，输入 **save soft from tftp** *ip_addr filename* **to flash**，其中 IP 地址是您的计算机的 IP 地址，文件名是 ScreenOS 固件的文件名。
6. 完成升级或降级后，必须重置 NetScreen 设备。执行 **reset** 命令，并在出现提示信息时输入 **y** 重置设备。
7. 等待几分钟，然后再次登录到 NetScreen 设备。
8. 使用 **get system** 命令检验 NetScreen 设备 ScreenOS 固件的版本。
9. 使用 **save config to { flash | slot1 | tftp }** 命令上传步骤 3 中保存的配置文件。

使用启动 / OS 加载程序

启动 / OS 加载程序可加载硬件系统，执行基本的并且有时是关键的硬件配置，同时加载用于运行 NetScreen 设备的系统软件。

***注意：**在 NetScreen-500 中，您不能使用此过程将 ScreenOS 5.1.0 固件保存到闪存中。使用 WebUI 或 CLI 将 ScreenOS 5.1.0 固件保存到闪存中。*

要使用启动 / OS 加载程序加载固件，请执行以下步骤：

1. 将计算机连接到 NetScreen 设备：
   a. 使用串行电缆将计算机的串行端口与 NetScreen 设备的控制台端口连接起来。通过此连接与一个终端应用程序，使您能够管理 NetScreen 设备。
   b. 使用以太网电缆将计算机的网络端口与 NetScreen 设备上的端口 1 或管理端口连接起来[13]。可通过此连接来实现计算机、 TFTP 服务器和 NetScreen 设备之间的数据传输。
2. 确保您的计算机中的 TFTP 服务器目录下存在新 ScreenOS 固件。有关获得新固件的信息，请参阅第 407 页上的 “下载新固件”。
3. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。您可以最小化 TFTP 服务器应用程序的窗口，但该程序必须在后台处于活动状态。
4. 使用终端机仿真器 (例如，超级终端) 登录到 NetScreen 设备。以根 admin 或具有读写权限的 admin 身份进行登录。
5. 重新启动 NetScreen 设备。
6. 当控制台显示器中出现 “Hit any key to run loader” 或 “Hit any key to load new firmware” 时，按计算机键盘上的任意键中断该启动过程。

   ***注意：**如果没有及时中断 NetScreen 设备，则将继续加载保存在闪存中的固件。*

13. 您连接哪个端口取决于 NetScreen 设备的型号。

7. 在 Boot File Name 提示下，输入要加载的 ScreenOS 固件的文件名。
如果您在指定的文件名之前键入了 **slot1:**，则加载程序将从外部 Compact Flash 卡或内存卡中读取指定的文件。如果您未在文件名之前键入 **slot1:**，则将从 TFTP 服务器下载该文件。如果 NetScreen 设备不支持 Compact Flash 卡，则将显示一条错误消息，且控制台会提示您重新键入文件名。
8. 在 Self IP Address 提示下，输入与 TFTP 服务器位于同一子网上的 IP 地址。
9. 在 TFTP IP Address 提示下，输入 TFTP 服务器的 IP 地址。

***注意：** Self IP 地址和 TFTP IP 地址必须属于同一子网，否则 TFTP 加载程序将拒绝 Self IP 地址并提示您重新输入。*

固件成功加载时，终端机仿真器屏幕上将显示一系列 “rtatatatatatata...”，且 TFTP 服务器窗口中将显示一系列符号。固件安装完成后，会有安装成功的消息通知您。

使用启动加载程序保存多个固件映像

固件成功下载后，控制台显示下列问题：

```
Save to on-board flash disk? (y/[n]/m)
```

回答 **y** (是) 将文件保存为缺省固件。如果不中断启动过程，则此映像将自动运行。

回答 **m** (多个) 将文件保存为多个固件。在下列提示下必须选择文件名：

```
Please input multiple firmware file name [BIMINITE.D]: test.d
```

括号中的名称是您在 TFTP 服务器中输入名称后自动生成的推荐名称。如果您不输入名称，则将使用该推荐名称。

***注意：** 必须输入 DOS 8.3 兼容的名称。加载程序使用的启动文件名称的最大长度不能超过 63 个字符。只有 NetScreen-5GT、 NetScreen-ISG200 和 NetScreen-5000 系列支持多个固件。最多可为 NetScreen-5GT 的内置闪存盘分配三个固件文件。 NetScreen-ISG2000 和 NetScreen-5000 系列对保存到内置闪存盘的固件文件的数量没有限制。*

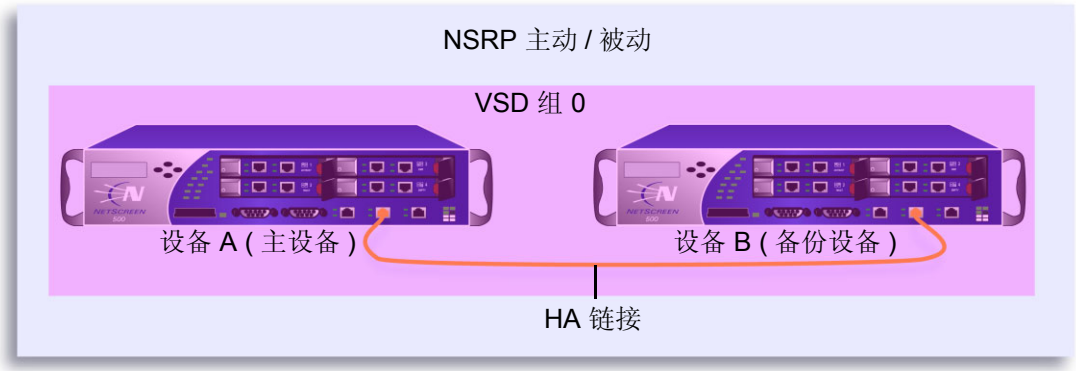
升级 NSRP 配置中的 NetScreen 设备

对于 NetScreen 冗余协议 (NSRP) 配置中的 NetScreen 设备，必须分别对每个设备进行升级。本节介绍两种不同的升级步骤，涉及两个不同的 NSRP 配置 : NSRP 主动 / 被动和 NSRP 主动 / 主动。

***注意：**如果您要从早于 ScreenOS 5.0.0 的版本升级 NetScreen 设备，那么必须先将设备升级到 ScreenOS 5.0.0，然后再升级到 ScreenOS 5.1.0。本节所介绍的内容为将 NetScreen 设备从 ScreenOS 5.0.0 升级到 ScreenOS 5.1.0 的步骤。*

升级 NSRP 主动 / 被动配置中的设备

下图说明了基本的 NSRP 主动 / 被动配置，其中设备 A 是主设备，设备 B 是备份设备。



执行升级操作前，请首先阅读执行升级的要求 (第 406 页上的 “升级和降级设备固件的要求”)。另外，请确保下载要将每个设备升级到该版本的 ScreenOS 固件。

***警告：**当 NetScreen 设备正升级到新固件时，请勿切断电源。若切断电源，则可能会对设备造成永久性损坏。*

升级步骤

要升级 NSRP 主动 / 被动配置中的两个设备，请按照以下步骤执行操作 (请注意，某些步骤只能使用 CLI):

A. 将设备 B 升级到 ScreenOS 5.1.0

B. 将设备 A 切换到设备 B (仅 CLI)

C. 将设备 A 升级到 ScreenOS 5.1.0

D. 同步设备 A (仅 CLI)

E. 将设备 B 切换到设备 A (仅 CLI)

A. 将设备 B 升级到 ScreenOS 5.1.0

WebUI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 通过打开 Web 浏览器 (例如 Internet Explorer 或 Netscape)，并在 Address 字段中输入管理 IP 地址来登录到设备 B。以根 admin 或具有读写权限的 admin 身份进行登录。
3. 保存现有配置 :
   a. 转至 Configuration > Update > Config File，然后单击 **Save to File**。
   b. 在 File Download 对话框中，单击 **Save**。
   c. 导航到要保存配置文件 (*cfg.txt*) 的位置，然后单击 **Save**。
4. 转至 Configuration > Update > ScreenOS/Keys，并选择 **Firmware Update**。
5. 单击 **Browse** 导航到 ScreenOS 5.1.0 固件的位置或在 Load File 字段中键入该位置的路径。
6. 单击 **Apply**。

   将出现一个具有升级时间信息的消息框。

7. 单击 **OK** 继续。

   NetScreen 设备自动重新启动。当设备在浏览器中显示登录页面时，就完成了升级操作。

8. 登录到 NetScreen 设备。在 WebUI 主页的 Device Information 部分，可以检验 NetScreen 设备 ScreenOS 固件的版本。

CLI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 通过应用程序 [例如 Telnet 或安全外壳 (SSH)] 或超级终端 (如果通过控制台端口直接连接) 登录到设备 B。以根 admin 或具有读写权限的 admin 身份进行登录。
3. 通过执行 **save config to { flash | slot1 | tftp }** 命令保存现有配置。
4. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。
5. 在 NetScreen 设备中，输入 **save soft from tftp** *ip_addr filename* **to flash**。其中， IP 地址是您的计算机的 IP 地址，文件名是 ScreenOS 5.1.0 固件的文件名。
6. 当升级完成后，必须重置 NetScreen 设备。执行 **reset** 命令，并在出现提示信息时输入 **y** 以重置设备。
7. 等待几分钟，然后再次登录到 NetScreen 设备。
8. 使用 **get system** 命令检验 NetScreen 设备 ScreenOS 固件的版本。

B. 将设备 A 切换到设备 B (仅 CLI)

手动将主设备切换到备份设备。

1. 登录到主设备。
2. 发出下列 CLI 命令之一。需要执行的命令取决于主设备上是否启用了抢先[14] 选项。
   - 如果启用了抢先功能 : **exec nsrp vsd-group 0 mode ineligible**
   - 如果未启用抢先选项 : **exec nsrp vsd-group 0 mode backup**

任一个命令都可迫使主设备让位，并使备份设备立即承担主地位。

C. 将设备 A 升级到 ScreenOS 5.1.0

WebUI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 登录到 NetScreen 设备 A。
3. 保存现有配置 :
   a. 转至 Configuration > Update > Config File，然后单击 **Save to File**。
   b. 在 File Download 对话框中，单击 **Save**。
   c. 导航到要保存配置文件 (*cfg.txt*) 的位置，然后单击 **Save**。
4. 转至 Configuration > Update > ScreenOS/Keys，并选择 **Firmware Update**。
5. 单击 **Browse** 导航到 ScreenOS 5.1.0 固件的位置或在 Load File 字段中键入该位置的路径。
6. 单击 **Apply**。

   将出现一个具有升级时间信息的消息框。
7. 单击 **OK** 继续。

   NetScreen 设备自动重新启动。当设备在浏览器中显示登录页面时，就完成了升级操作。

14. 有关常见的抢先选项和 NSRP 的详细信息，请参阅第 8 卷的 *NetScreen 概念与范例 ScreenOS 参考指南*。

8. 登录到 NetScreen 设备。在 WebUI 主页的 Device Information 部分，可以检验 NetScreen 设备 ScreenOS 固件的版本。

CLI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 登录到 NetScreen 设备 A。
3. 通过执行 **save config to { flash | slot1 | tftp }** 命令保存现有配置。
4. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。
5. 在 NetScreen 设备中，输入 **save soft from tftp** *ip_addr filename* **to flash**。其中， IP 地址是您的计算机的 IP 地址，文件名是 ScreenOS 5.1.0 固件的文件名。
6. 当升级完成后，必须重置 NetScreen 设备。执行 **reset** 命令，并在出现提示信息时输入 **y** 以重置设备。
7. 等待几分钟，然后再次登录到 NetScreen 设备。
8. 通过使用 **get system** 命令可以检验 NetScreen 设备 ScreenOS 固件的版本。

D. 同步设备 A (仅 CLI)

在将设备 A 升级到 ScreenOS 5.1.0 后，需手动同步这两个设备。在设备 A (备份设备) 上，发出 **exec nsrp sync rto all from peer** CLI 命令以从设备 B (主设备) 同步 RTO。

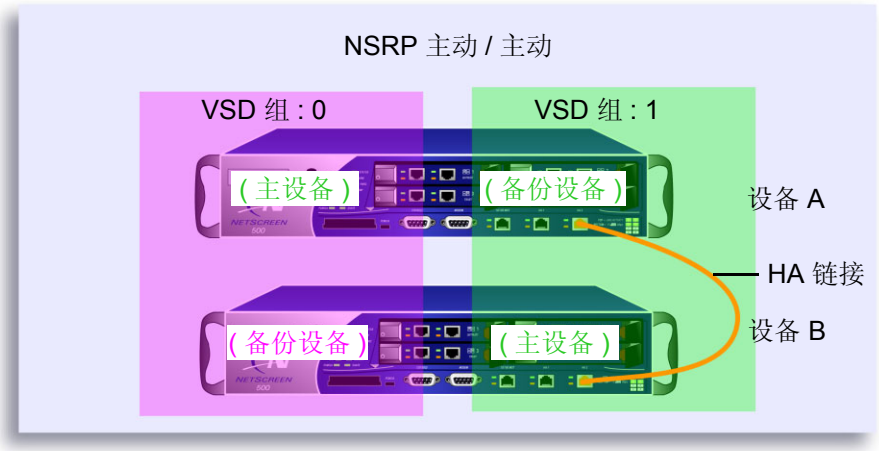
E. 将设备 B 切换到设备 A (仅 CLI)

在同步这些设备后，需手动将主设备切换到备份设备。除了应登录到设备 B 以及应切换设备 B 而不是切换设备 A 之外，所需步骤同第 417 页上的 “B. 将设备 A 切换到设备 B (仅 CLI)”。

升级 NSRP 主动 / 主动配置中的设备

此升级部分适用于 NSRP 配置，其中将两台 NetScreen 设备配对到两个虚拟安全设备 (VSD) 组中，每个物理设备在一个组中是主设备，而在另一个组中是备份设备。要进行升级操作，必须首先切换其中的一个设备，以便只有一个物理设备是两个 VSD 组的主设备。然后先升级备份设备，之后再升级主设备。

下图对典型的 NSRP 主动 / 主动配置进行了说明，其中设备 A 是 VSD 0 的主设备且又是 VSD 1 的备份设备，而设备 B 是 VSD 1 的主设备且又是 VSD 0 的备份设备。



执行升级操作前，请首先阅读执行升级的要求 (第 406 页上的 “升级和降级设备固件的要求”)。另外，确保您下载了 ScreenOS 5.1.0 固件。

***警告：**当 NetScreen 设备正升级到新固件时，请勿切断电源。若切断电源，则可能会对设备造成永久性损坏。*

升级步骤

要升级 NSRP 主动 / 主动配置中的两个设备，请按照以下步骤执行操作 (请注意，某些步骤只能使用 CLI):

A. 将 VSD 1 中的设备 B 切换到 VSD 1 中的设备 A (仅 CLI)

B. 将设备 B 升级到 ScreenOS 5.1.0

C. 将设备 A 切换到设备 B (仅 CLI)

D. 将设备 A 升级到 ScreenOS 5.1.0

E. 同步设备 A (仅 CLI)

F. 将 VSD 0 中的设备 B 切换到 VSD 0 中的设备 A (仅 CLI)

A. 将 VSD 1 中的设备 B 切换到 VSD 1 中的设备 A (仅 CLI)

将 VSD 组 1 中的主设备 B 手动切换到 VSD 组 1 中的备份设备 A。

1. 通过应用程序 (例如 Telnet 或安全外壳 (SSH)) 或超级终端 (如果通过控制台端口直接连接) 登录到设备 B。以根 admin 或具有读写权限的 admin 身份进行登录。
2. 发出下列 CLI 命令之一。需要执行的命令取决于主设备上是否启用了抢先[15] 选项。
   - 如果启用了抢先功能 : **exec nsrp vsd-group 1 mode ineligible**
   - 如果未启用抢先选项 : **exec nsrp vsd-group 1 mode backup**

任一个命令都可迫使设备 B 让位，并使设备 A 立即承担 VSD 1 的主地位。此时，设备 A 是 VSD 0 和 VSD 1 的主设备，而设备 B 是 VSD 0 和 VSD 1 的备份设备。

15. 有关常见的抢先选项和 NSRP 的详细信息，请参阅第 8 卷的 *NetScreen 概念与范例 ScreenOS 参考指南*。

B. 将设备 B 升级到 ScreenOS 5.1.0

WebUI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 通过打开 Web 浏览器 (例如 Internet Explorer 或 Netscape)，并在 Address 字段中输入管理 IP 地址来登录到 NetScreen 设备 B。以根 admin 或具有读写权限的 admin 身份进行登录。
3. 保存现有配置 :
   a. 转至 Configuration > Update > Config File，然后单击 **Save to File**。
   b. 在 File Download 对话框中，单击 **Save**。
   c. 导航到要保存配置文件 (*cfg.txt*) 的位置，然后单击 **Save**。
4. 转至 Configuration > Update > ScreenOS/Keys，并选择 **Firmware Update**。
5. 单击 **Browse** 导航到 ScreenOS 5.1.0 固件的位置或在 Load File 字段中键入该位置的路径。
6. 单击 **Apply**。

   将出现一个具有升级时间信息的消息框。
7. 单击 **OK** 继续。

   NetScreen 设备自动重新启动。当设备在浏览器中显示登录页面时，就完成了升级操作。
8. 登录到 NetScreen 设备。在 WebUI 主页的 Device Information 部分，可以检验 NetScreen 设备 ScreenOS 固件的版本。

CLI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 登录到设备 B。
3. 通过执行 **save config to { flash | slot1 | tftp }** 命令保存现有配置。
4. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。
5. 在 NetScreen 设备中，输入 **save soft from tftp** *ip_addr filename* **to flash**。其中， IP 地址是您的计算机的 IP 地址，文件名是 ScreenOS 5.0.0 固件的文件名。
6. 当升级完成后，必须重置 NetScreen 设备。执行 **reset** 命令，并在出现提示信息时输入 **y** 以重置设备。
7. 等待几分钟，然后再次登录到 NetScreen 设备。
8. 通过使用 **get system** 命令可以检验 NetScreen 设备 ScreenOS 固件的版本。

C. 将设备 A 切换到设备 B (仅 CLI)

完全以手动方式将设备 A 切换到设备 B。

1. 登录到设备 A。
2. 通过发出以下 CLI 命令之一将 VSD 0 中的主设备 A 切换到 VSD 0 中的备份设备 B。需要执行的命令取决于主设备上是否启用了抢先选项。
   - 如果启用了抢先功能 : **exec nsrp vsd-group 0 mode ineligible**
   - 如果未启用抢先选项 : **exec nsrp vsd-group 0 mode backup**
3. 通过发出以下 CLI 命令之一将 VSD 1 中的主设备 A 切换到 VSD 1 中的备份设备 B。需要执行的命令取决于主设备上是否启用了抢先选项。
   - 如果启用了抢先功能 : **exec nsrp vsd-group 1 mode ineligible**
   - 如果未启用抢先选项 : **exec nsrp vsd-group 1 mode backup**

此时，设备 B 是 VSD 0 和 VSD 1 的主设备，而设备 A 是 VSD 0 和 VSD 1 的备份设备。

D. 将设备 A 升级到 ScreenOS 5.1.0

WebUI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 登录到 NetScreen 设备 A。
3. 保存现有配置 :
   a. 转至 Configuration > Update > Config File，然后单击 **Save to File**。
   b. 在 File Download 对话框中，单击 **Save**。
   c. 导航到要保存配置文件 (*cfg.txt*) 的位置，然后单击 **Save**。
4. 转至 Configuration > Update > ScreenOS/Keys，并选择 **Firmware Update**。
5. 单击 **Browse** 导航到 ScreenOS 5.1.0 固件的位置或在 Load File 字段中键入该位置的路径。
6. 单击 **Apply**。

   将出现一个具有升级时间信息的消息框。
7. 单击 **OK** 继续。

   NetScreen 设备自动重新启动。当设备在浏览器中显示登录页面时，就完成了升级操作。
8. 登录到 NetScreen 设备。在 WebUI 主页的 Device Information 部分，可以检验 NetScreen 设备 ScreenOS 固件的版本。

CLI

1. 确保您具有 ScreenOS 5.1.0 固件。有关获得该固件的信息，请参阅第 407 页上的 “下载新固件”。
2. 登录到设备 A。
3. 通过执行 **save config to { flash | slot1 | tftp }** 命令保存现有配置。
4. 通过双击 TFTP 服务器应用程序来运行您的计算机中的 TFTP 服务器。
5. 在 NetScreen 设备中，输入 **save soft from tftp** *ip_addr filename* **to flash**。其中， IP 地址是您的计算机的 IP 地址，文件名是 ScreenOS 5.1.0 固件的文件名。
6. 当升级完成后，必须重置 NetScreen 设备。执行 **reset** 命令，并在出现提示信息时输入 **y** 以重置设备。
7. 等待几分钟，然后再次登录到 NetScreen 设备。
8. 通过使用 **get system** 命令可以检验 NetScreen 设备 ScreenOS 固件的版本。

E. 同步设备 A (仅 CLI)

在将设备 A 升级到 ScreenOS 5.1.0 后，需手动同步这两个设备。在设备 A 上，发出 **exec nsrp sync rto all from peer** CLI 命令以从设备 B 同步 RTO。

F. 将 VSD 0 中的设备 B 切换到 VSD 0 中的设备 A (仅 CLI)

作为最后的步骤，您必须恢复 NSRP 主动 / 主动配置中的两个 NetScreen 设备。

1. 登录到设备 A。
2. 通过发出以下 CLI 命令之一将 VSD 0 中的主设备 B 切换到 VSD 0 中的备份设备 A。需要执行的命令取决于主设备上是否启用了抢先选项。
   - 如果启用了抢先功能 : **exec nsrp vsd-group 1 mode ineligible**
   - 如果未启用抢先选项 : **exec nsrp vsd-group 1 mode backup**

此时，设备 A 是 VSD 0 的主设备且又是 VSD 1 的备份设备，而设备 B 是 VSD 1 的主设备又是 VSD 0 的备份设备。

认证固件和 DI 文件

从 ScreenOS 2.6.1r1 开始，映像认证签名就已经集成到每个 ScreenOS 构造中。如果您在 Juniper Networks NetScreen 防火墙 /VPN 设备中加载了认证证书 (imagekey.cer)，那么当您尝试将 ScreenOS 固件保存到设备时，此证书可以认证 ScreenOS 固件，并且当您尝试将 ScreenOS 固件下载到设备时，此证书可以认证深入检查 (DI) 攻击对象数据库文件。

认证映像和 DI 攻击对象数据库这一功能既提供了安全性又提供了稳定性。当您尝试保存经过修改的或已损坏的 ScreenOS 映像或数据库时，设备将首先对其进行拒绝，然后再将其保存到闪存。

获得认证证书

可从以下两个位置获取认证证书 zip 文件 :

- NetScreen 设备随附的文档 CD:
  1. 将文档 CD 插入到 CD 驱动器中。

     该文档 CD 将自动启动。(对于未在其系统上启用 “自动启动” 功能的 Macintosh 用户和 PC 用户，请双击 **index.htm** 以打开该 CD。)
  2. 单击 **Explore CD-ROM Contents**。
  3. 打开 *extra* 文件夹。

     image_key.zip 文件位于此文件夹中。
- Juniper Networks Web 站点的 Customer Support 区域[16]:
  1. 打开 Web 浏览器，在地址栏中输入以下 URL: http://www.juniper.net/support/。
  2. 在 Login to Support Center 部分中，输入用户 ID 和密码，然后单击 **LOGIN**。
  3. 在 Download Software 部分中，单击 **ScreenOS Software**。
  4. 在该页面的顶部存在一个标题为 Image Authentication 的部分。右键单击 **Download the Authentication Certificate**，选择 **Save Target As**，并将文件 *image_key.zip* 保存到本地目录中。

16. 要访问 Customer Support 区域，您必须是已注册的用户。如果您尚未拥有用户帐户，可通过访问 http://www.juniper.net/support/，单击 **Login Assistance**，然后按照在线注册说明的内容在线创建一个帐户。

一旦获得了证书 zip 文件，即可执行以下步骤：

1. 使用数据压缩实用程序 (例如 WinZip) 从 *image_key.zip* 中解压缩以下两个文件：*imagekey.cer* 和 *image_key_readme.pdf*[17]。
2. 将 *imagekey.cer* 保存到下列任一位置，这取决于您要使用 WebUI 还是 CLI 将该文件加载到 NetScreen 设备：
   - WebUI – 本地目录
   - CLI – TFTP 服务器的根目录

加载认证证书

在将认证证书加载到 NetScreen 设备之前，可以确认其完整性，方法是先计算加密的校验和或消息整理，然后再将其与下列 MD5 消息整理进行比较：

AC359646EDD723F541AA0E52E015E8F0

有一种名为 FastSum 的用于 Windows 系统的免费 MD5 实用程序，可在 www.fastsum.com 处获得该程序。在 UNIX/Linux 下，可以使用诸如 md5sum 等实用程序来计算消息整理。

当下载认证证书后，在运行或保存固件前，固件将与认证证书进行对照。如果固件认证失败，则会拒绝将其上传到 NetScreen 设备上。

当您对认证证书的完整性确信无疑后，请通过下列任一操作将该证书加载到 NetScreen 设备上：

WebUI

1. 创建到 NetScreen 设备的 HTTP 连接，然后登录。
2. Configuration > Update > ScreenOS/Keys: 输入以下内容，然后单击 **Apply**:

   Image Key Update (See Online Help): (选择)

   Load File: 输入 *imagekey.cer* 所在的位置或单击 **Browse** 导航到该文件所在位置，选择 *imagekey.cer*，然后单击 **Open**。

17. 实际上，该自述文件中所包含的信息与本节中所述信息相同。

CLI

1. 如有必要，请启动 TFTP 服务器。
2. 创建到 NetScreen 设备的控制台、 Telnet 或 SSH 连接，然后登录。
3. 输入以下 CLI 命令 :

   save image-key tftp *ip_addr* **imagekey.cer**

   其中， *ip_addr* 是 TFTP 服务器的地址。

认证 ScreenOS 固件

下载 NetScreen 设备时将使用认证证书来检查文件中内嵌的 ScreenOS 签名。在控制台上可以看到以下两种结果之一 :

- 由于 NetScreen 设备可以成功认证此固件，因此启动加载程序 / OS 加载程序将显示以下消息 :

  Loaded Successfully! . . .

  Image authenticated!

- 如果 NetScreen 设备不能认证 ScreenOS 固件，则此固件将被拒绝，然后提示您加载其它固件或设备自动重新启动 :

  ********Invalid DSA signature

  *******Bogus Image - not authenticated.

注意 : *如果未加载认证证书，那么 NetScreen 设备将不尝试认证 ScreenOS 固件或 DI 攻击对象数据库。要删除证书，请输入* ***delete crypto auth-key*** *命令。*

认证 DI 攻击对象数据库文件

下次您尝试下载用于深入检查 (DI) 的攻击对象数据库时，NetScreen 设备将使用认证证书来检查文件中内嵌的签名。此认证过程将产生下列两种结果之一：

- NetScreen 设备成功认证下载的攻击对象数据库，并创建以下事件日志条目：

  Attack database version <number> has been authenticated and saved to flash.

- 认证检查失败， NetScreen 设备将创建以下事件日志条目：

  Attack database was rejected because the authentication check failed.

  另外，当您尝试通过 WebUI 手动下载数据库且认证检查失败后，将出现以下弹出式消息：

  Rejected DI attack database because the authentication check was unable to verify its integrity.

注意：*如果未加载认证证书，那么 NetScreen 设备将不尝试认证 ScreenOS 映像或 DI 攻击对象数据库。要删除证书，请输入* ***delete crypto auth-key*** *命令。*

有关事件日志消息的信息，请参阅 NetScreen Message Log Reference Guide (NetScreen 消息日志参考指南)。

下载和上传配置

当对配置进行更改时，建议备份您的设置。 WebUI 允许您将配置下载至任何本地目录，作为预防备份。对于某些 NetScreen 设备，可以使用 CLI 将配置下载至 TFTP 服务器或闪存卡中。如果需要恢复为保存的备份配置，那么可以将其上传到 NetScreen 设备。

本节包括以下内容：

保存和导入配置

保存和导入配置设置的功能提供了大量分发配置模板的方法。

保存配置：

WebUI

1. Configuration > Update > Config File: 单击 **Save to File**。

   会出现一条系统消息，提示您打开文件或将其保存到计算机上。
2. 单击 **Save**。
3. 浏览到要保存配置文件的位置，然后单击 **Save**。

CLI

```
save config from flash to { tftp ip_addr | slot } filename [ from interface ]
```

注意：在某些 NetScreen 设备中，必须指定 slot1 或 slot2。

导入配置：

WebUI

Configuration > Update > Config File: 输入以下内容，然后单击 **Apply**:

如果要将新配置和当前配置合并在一起，请选择 **Merge to Current Configuration**；如果要用新配置覆盖当前配置，请选择 **Replace Current Configuration**。

> New Configuration File: 输入配置文件位置或单击 **Browse** 导航到该文件位置，选择配置文件，然后单击 **Open**。

CLI

```
save config from { tftp ip_addr | slot } filename to flash [ merge [ from
    interface ] ]
```

注意：在某些 NetScreen 设备中，必须指定 slot1 或 slot2。

配置回滚

如果加载配置文件时出现问题，例如 NetScreen 设备发生故障或远程用户失去了管理设备的能力，则可执行配置回滚，恢复到在闪存中已保存的上次已知正确 (LKG) 的配置文件。

***注意：**并非所有的 NetScreen 设备都支持配置回滚。要查看您的 NetScreen 设备是否支持此功能，请参阅您所用平台的相关数据表。*

上次已知正确的配置

执行配置回滚之前，请确保闪存中保存有 LKG 配置文件，以便出现错误时 NetScreen 设备可以进行恢复。要检查 LKG 文件，请打开 NetScreen CLI，然后键入 **get config rollback** 命令。LKG 配置文件的名称是 *lkg.cfg*。如果未出现此文件，则表明该文件不存在，因此必须手动创建它。

将某个配置文件作为 LKG 文件保存到闪存中：

1. 确保 NetScreen 设备的当前配置正确。
2. 使用 **save config to last-known-good** 命令将当前配置保存到闪存中。执行此命令后，当前配置文件会覆盖闪存中现有的 LKG 配置文件。

***注意：**如果既要备份最近的配置更改，又要保留最新的配置副本，则定期将 NetScreen 设备上的配置保存为 LKG 配置文件不失为一个两全其美的好办法。*

自动与手动配置回滚

您既可以使 NetScreen 设备自动恢复为 LKG 配置，也可以手动执行回滚。如果最新加载的配置有问题，可使用自动配置回滚功能将 NetScreen 设备回滚到 LKG 配置。

在缺省情况下，将禁用自动配置回滚功能。此外，无论设备启动前该功能处于禁用还是启用状态，每次启动后都会禁用它。要启用自动配置回滚，请使用 **exec config rollback enable** 命令。要禁用该功能，请使用 **exec config rollback disable** 命令。

要执行手动配置回滚，请使用 **exec config rollback** 命令。

***注意：** WebUI 不支持配置回滚功能。*

启用配置回滚功能后，命令提示符会相应改变，以指示其状态：

```
ns-> exec config rollback enable
ns(rollback enabled)->
```

禁用配置回滚功能后，命令提示符将改回至设备主机名：

```
ns(rollback enabled)-> exec config rollback disable
ns->
```

要检验是否启用了自动回滚功能，请使用 **get config rollback** 命令。如果已启用该功能，则 **get config rollback** 的第一行输出信息为：

```
config rollback is enabled
```

否则，第一行输出信息为：

```
config rollback is disabled
```

如果存在 LKG 配置文件，则 **get config rollback** 的第二行输出信息为：

```
Last-known-good config file flash:/$lkg$.cfg exists in the flash.
```

如果 LKG 配置文件不存在，则第二行 (即最后一行) 输出信息为：

```
Last-known-good config file flash:/$lkg$.cfg does not exist.
```

启用配置回滚功能后，可通过以下任一操作触发回滚操作：

- 重新启动 NetScreen 设备 (先关闭电源，再打开)
- 重置 NetScreen 设备 (输入 **reset** 命令)
- 输入 **exec config rollback** 命令

加载新的配置文件

以下内容介绍如何加载新的配置文件、如何启用配置回滚功能以及新配置文件引起故障时如何排除。

1. 使用 CLI 命令 **Save config to last-known-good**，将当前配置保存为 LKG。
2. 使用 **exec config rollback enable** 命令，在 NetScreen 设备上启用自动配置回滚功能。启用此功能的同时将锁定 LKG 文件，以防止其它用户覆盖该文件，从而破坏正在进行的配置回滚。
3. 可使用 WebUI 或 CLI 加载新的配置文件。有关详细信息，请参阅第 405 页上的 “升级和降级固件”。
4. 发出命令测试新的配置文件。可能出现以下几种情况：
   - 新配置文件运行正常。
   - 新配置文件有问题，无法继续访问及管理 NetScreen 设备。遇到此种情况，只能关闭设备。NetScreen 设备打开后，先读取闪存文件，这些文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。
   - 您发现新配置文件中存在某些问题或错误。此时，需要使用 **reset** 命令重置 NetScreen 设备。设备重启后，先读取闪存文件，该文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。
   - 新配置文件有问题，导致 NetScreen 设备无法运行。此时， NetScreen 设备会自动重启。设备重启后，先读取闪存文件，该文件指出已启用配置回滚功能。该信息会提示 NetScreen 设备自动加载 LKG 文件。

***注意：** NetScreen 冗余协议 (NSRP) — 在主动 / 主动设置中，如果加载新的配置文件失败，那么两个 NetScreen 设备都将恢复到 LKG 文件。在主动 / 被动设置中，如果加载新的配置文件失败，那么只有主设备恢复到 LKG 文件。只有将配置保存到文件后，主设备才能与备份设备同步。*

锁定配置文件

为防止闪存中的配置文件被其它管理员覆盖，可将其锁定；导入新的配置文件之前通常也要锁定原文件。锁定配置文件时，设备会启动一个锁定计时器。如果设备在先前指定的锁定期限内没有收到 CLI 命令，那么会使用闪存中锁定的配置文件自动重启。建议在开始导入配置文件之前锁定设备当前的配置文件。该操作可以有效防止因导入过程出错而导致设备进入无限期的死机状态。

一旦锁定配置文件，您和其它连接到设备 (例如通过 Telnet 或 WebUI) 的管理员将无法向配置文件中保存内容。必须先解除配置文件的锁定，然后才能使用 **save** 命令保存新的配置命令。

注意：*您只能通过 CLI 锁定 / 解锁配置文件。不能在 WebUI 上使用此功能。*

CLI

锁定配置文件 :

exec config lock start

解除文件锁定 :

exec config lock end

终止锁定并立即用之前在闪存中锁定的配置文件重启设备 :

exec config lock abort

更改缺省锁定期限 (5 分钟):

set config lock timeout *<number>*

向配置文件添加注释

可以为外部配置文件添加注释。注释可能是一行单独的文本，也可能在一行的结尾处。注释必须以井号 (#) 开头，后面接一个空格。注释位于一行的结尾时，还需要在井号前加一个空格。可采用两种方法将文件保存到 NetScreen 设备：合并新配置文件与现有配置文件；用新配置文件完全取代现有配置文件。设备分析配置文件时，会查找以井号开头的行并删除所有注释内容。

注意：**如果井号出现在引号内，则 NetScreen 设备不会将其视为特殊标记，而是当作对象名称的一部分，因此不会将其删除。例如，NetScreen 设备不会删除命令* ***set address trust "#5 server" 10.1.1.5/32 *中的* ***"#5 server"****，因为此处的井号出现在引号内。*

NetScreen 设备不会将以井号开头的注释保存到闪存的任一 RAM 中。例如，假设外部配置文件包含以下各行：

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24 # change IP address
# add new MIP addresses
set interface ethernet3 mip 1.1.1.10 host 10.1.1.10 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.11 host 10.1.1.11 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.12 host 10.1.1.12 netmask 255.255.255.255
# all MIPs use the trust-vr routing domain by default
```

加载文件后，再次查看配置文件时，您所看到的内容如下 (已无注释):

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 mip 1.1.1.10 host 10.1.1.10 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.11 host 10.1.1.11 netmask 255.255.255.255
set interface ethernet3 mip 1.1.1.12 host 10.1.1.12 netmask 255.255.255.255
```

此外，如果粘贴了大量的命令 (这些命令可将注释加入到控制台会话或 Telnet 会话中)，则运行这些命令时，NetScreen 设备会立即忽略所有注释。

设置 NETSCREEN-SECURITY MANAGER BULK-CLI

如果更新会话期间， NetScreen-Security Manager 连接丢弃，则可通过设置 bulk-CLI 来确定设备执行回滚的方式和时间。出现这种情况时，代理将对所有已配置的 NetScreen-Security Manager 服务器各重试一次，从而确定其是否可以建立另一连接。如果不能建立其它连接，则代理等待指定的时间段后，会重新启动设备以恢复到初始配置。重启超时值介于 60 秒与 86400 秒之间。缺省重启超时值为 60 秒。

代理将在以下两种情况下检查 NetScreen-Security Manager 连接状态：

- 所有 CLI 命令已执行完毕且需要将成功或未成功的消息发送到 NetScreen-Security Manager。
- 出现错误，因此需要向 NetScreen-Security Manager 报告该错误。

如果在 CLI 执行期间产生错误，则代理会首先将报告错误的消息发送到 NetScreen-Security Manager，然后再等待错误指令。关于错误指令有三种情况：

- 如果指示代理 “停止”，那么代理将停止执行剩余的 CLI 命令并重新启动。
- 如果指示代理 “继续”，那么代理将继续执行剩余的 CLI 命令。
- 如果在指定的重启超时值内没有任何代理指令，那么代理将检查是否已启用或禁用 bulk-cli reboot_timeout。
  - 如果已启用，则将立即重新启动。
  - 如果已禁用，则代理将不会重启设备。设备将继续执行剩余的 CLI 命令。

要设置重启超时值，请使用以下命令：

```
set nsmgmt bulkcli reboot_timeout number
```

其中， *number* 的单位为秒。

要禁用重启超时，请使用以下命令：

```
set nsmgmt bulkcli reboot_timeout disable
```

许可密钥

利用此许可密钥功能，无需将 NetScreen 设备升级为不同的设备或系统映像，即可对其能力进行扩展。您可以购买一个密钥来解锁固件中已加载的指定功能，比如下面的这些功能：

- 用户容量
- 虚拟系统、区段和虚拟路由器
- HA

每台 NetScreen 设备出厂时都已启用了标准功能集，而且可能会支持激活可选功能或提高现有功能的能力。要了解当前都有哪些功能可以进行升级，请参阅 Juniper Networks 的最新市场文献。

获得并应用许可密钥的过程如下：

1. 与向您销售 NetScreen 设备的增值分销商 (VAR) 联系，或者直接与 Juniper Networks 联系。
2. 提供您设备的序列号并说明您想要的功能选项。

   生成许可密钥，而后通过电子邮件将其发送给您。
3. 通过 WebUI 或 CLI 输入该密钥。(请参阅以下示例。)

范例：扩大用户容量

某家小公司使用了单台 NetScreen 设备，该设备只具有数量为 10 位用户的许可，随着公司的发展，它现在需要一种用户数不受限制的许可。此时， NetScreen 管理员只要获得一个不限制用户数目的固件密钥，即可扩展设备的能力。许可密钥号码为 6a48e726ca050192，该号码在 C:\netscreen\keys 目录下的名为 “A2010002.txt” 的文本文件中。

WebUI

Configuration > Update > ScreenOS/Keys: 执行下列操作，然后单击 **Apply**:

License Key Update: (选择)

Load File: C:\netscreen\keys\A2010002.txt

或者

单击 **Browse** 导航到 C:\netscreen\keys，选择 A2010002.txt，然后单击 **Open**。

CLI

```
exec license-key capacity 6a48e726ca050192
reset
```

预定服务的注册与激活

为了让 Juniper Networks NetScreen 设备定期收到防病毒 (AV) 模式的预定服务或深入检查 (DI) 签名或 URL 过滤，必须先订购服务，再注册服务，然后才能恢复预订密钥。收到预定服务后，设备上的服务会被激活。服务的激活过程取决于购买服务的方式和服务的具体内容。

临时服务

为确保用户有足够时间订购 AV 或 DI 服务， NetScreen 设备提供了一段临时宽限期。在此期限内，设备可以获得临时服务。

- 出厂后的 NetScreen 设备一律没有启用 DI 服务。要获得临时 DI 服务，必须先启动 WebUI 会话，然后在 Configuration > Update > ScreenOS/Keys 页面上单击 **Retrieve Subscriptions Now** 按钮。随后即可获得期限为一天的一次性 DI 密钥。
- 如果购买设备时捆绑了 AV 服务，则该设备已预先安装临时服务。此临时服务可持续长达 60 天。
- 出厂后的 NetScreen 设备一律没有启用 URL 过滤服务。此功能没有临时服务。

***警告！**为避免服务中断，必须在订购后尽早注册服务。通过注册，可以确保继续订购服务。*

新设备上捆绑的 AV、 URL 过滤和 DI 服务

如果新买的 NetScreen 设备自带 AV、 URL 过滤和 DI 服务，请执行以下步骤激活这些服务。

1. 配置设备连接到互联网。 (有关说明，请参阅 NetScreen 设备的 *Getting Started Guide* 和 User's Guide。)
2. 请在以下站点上注册设备 :

   www.juniper.net/support

   绑定了 AV 服务的设备带有一个预先安装的临时预订服务，从而可以免去安装，立即使用该服务。但是，*必须*先注册设备接收全额付款的预订服务。
3. 恢复设备的预订密钥。可以采取以下两种方法 :
   - 在 WebUI 中，单击 Configuration > Update > ScreenOS/Keys 页面上的 **Retrieve Subscriptions Now** 按钮。
   - 使用 CLI 时，请运行以下命令 :

     ```
     exec license-key update
     ```
4. 加载密钥后，必须重置设备。

现在即可配置设备自动恢复或手动恢复签名服务。有关配置 NetScreen 设备执行这些服务的说明，请参阅第 **4**-81 页上的 “防病毒扫描”、第 **4**-106 页上的 “URL 过滤”和第 **4**-131 页上的 “深入检查”。

在现有服务上升级 AV、 URL 过滤和 DI 服务

如果购买了要添加到现有 NetScreen 设备上的 AV、 URL 过滤和 DI 服务，请执行以下步骤激活服务。

1. 订购服务后，您将通过电子邮件从 Juniper Networks 或 NetScreen 设备授权转销商那里收到支持证书。此证书是一份简单易懂的文档，包含注册设备所需的信息。
2. 请确保设备已注册。如果目前尚未注册，请转到以下站点：

   www.juniper.net/support
3. 在设备上注册支持证书。
4. 如果只准备订购并注册 DI 或 URL 过滤服务，则进入步骤 5。

   如果正准备订购并注册 AV 服务，那么必须先等待四小时，让系统处理注册，然后再进入步骤 5。
5. 确认设备已连接到互联网。
6. 恢复设备上的预订密钥。可以采取以下两种方法之一：
   - 在 WebUI 中，单击 Configuration > Update > ScreenOS/Keys 页面上的 **Retrieve Subscriptions Now** 按钮。
   - 使用 CLI 时，请运行以下命令：

     ```
     exec license-key update
     ```
7. 在加载密钥后，必须重置设备。

现在即可配置设备自动恢复或手动恢复签名服务。有关配置 NetScreen 设备执行这些服务的说明，请参阅第 **4**-81 页上的 “防病毒扫描”、第 **4**-106 页上的 “URL 过滤”以及第 **4**-131 页上的 “深入检查”。

只升级 DI 服务

如果只购买了 DI 服务，且 NetScreen 设备与 DI 服务分开购买，则执行以下步骤激活服务。

1. 订购服务后，您将会以电子邮件的方式从 Juniper Networks 或经过授权的 NetScreen 设备分销商那里收到支持证书。此证书为一份可读文档，包含注册设备所需的信息。
2. 请确保设备已注册。如果目前尚未注册，请转到以下站点：

   www.juniper.net/support
3. 注册设备的支持证书。
4. 确认设备已连接到互联网。
5. 恢复设备的预订密钥。可以采取以下两种方法：
   - 在 WebUI 中，单击 Configuration > Update > ScreenOS/Keys 页面上的 **Retrieve Subscriptions Now** 按钮。
   - 使用 CLI 时，请运行以下命令：

     ```
     exec license-key update
     ```
6. 加载密钥后，必须重置设备。

现在即可配置设备自动恢复或手动恢复 DI 签名服务。有关配置 NetScreen 设备执行此服务的说明，请参阅第 **4**-131 页上的 “深入检查”。

系统时钟

NetScreen 设备应始终设置成正确的时间，这一点极为重要。其它情况下， NetScreen 设备的时间会直接影响 VPN 通道的设置和计划进度的定时。可采取多种方法确保 NetScreen 设备始终保持精确的时间。首先，必须将系统时钟设置成当前时间。接着，可以启用夏令时选项，并可配置多达三个 NTP 服务器 (一台主服务器和两台备份服务器)，NetScreen 设备将通过这些服务器定期更新系统时钟。

日期和时间

可以使用 WebUI 或 CLI，将时钟设置成当前时间与日期。使用 WebUI 时，会将系统时钟与计算机时钟同步，从而将系统时钟设置成当前时间 :

1. Configuration > Date/Time: 单击 **Sync Clock with Client** 按钮。

   会弹出一条消息，提示您指定是否已在计算机时钟上启用了夏令时选项。

2. 单击 **Yes** 将同步系统时钟，并根据夏令时调整系统时钟；单击 **No** 将只同步系统时钟，而不根据夏令时对其进行调整。

使用 CLI 设置时钟时，可以使用命令 “**set clock mm/dd/yyyy hh:mm:ss**” 手动输入日期与时间。

时区

可通过指定 NetScreen 设备的当地时间早于或晚于 GMT (格林威治标准时间) 的小时数来设置时区。例如，如果 NetScreen 设备的当地时区是 “太平洋标准时间”，则它要比 GMT 时间晚 8 小时。因此必须将时钟设置为 **-8**。

如果使用 WebUI 设置时区 :

Configuration > Date/Time > Set Time Zone_hours_minutes from GMT

如果使用 CLI 设置时区 :

ns -> set clock timezone *number* (介于 -12 与 12 之间的数字)

或

ns-> set ntp timezone *number* (介于 -12 与 12 之间的数字)

NTP

为确保 NetScreen 设备始终保持正确时间，可以使用 NTP (网络时间协议) 通过互联网将系统时钟与 NTP 服务器的时钟同步。您可以手动执行同步操作，也可以配置 NetScreen 设备以指定的时间间隔自动执行同步。

多个 NTP 服务器

一台 NetScreen 设备上最多可以配置三台 NTP 服务器 : 一台主服务器和两台备份服务器。如果配置 NetScreen 设备自动同步系统时钟，设备会依次查询已配置的每个 NTP 服务器。设备总是最先查询主 NTP 服务器。如果查询失败，设备会继续查询第一台备份 NTP 服务器，依此类推，直到从 NetScreen 设备上配置的某台 NTP 服务器那里得到有效回复。设备对每台 NTP 服务器均尝试四次查询，如果仍得不到有效回复，设备将终止更新，并在日志中留下失败记录。

手动同步系统时钟时，只能使用 CLI，可以指定特定的 NTP 服务器，也可以一个都不指定。如果指定了 NTP 服务器，NetScreen 设备会只查询该服务器。如果未指定 NTP 服务器，NetScreen 设备将依次查询 NetScreen 设备上配置的每台 NTP 服务器。可以使用服务器的 IP 地址或域名指定 NTP 服务器。

最大时间调整

对于自动同步，可以指定最大时间差值 (单位为秒)。最大时间差值是指 NetScreen 设备系统时钟与收到的 NTP 服务器时间之间允许的时间差。仅当设备时钟与 NTP 服务器时间的时间差小于设置的最大时间差值时， NetScreen 设备才会按照 NTP 服务器的时间调整时钟。例如，假设最大时间差值为 3 秒，设备系统时钟的时间为 4:00:00， NTP 服务器发送的时间为 4:00:02，由于两者之间的时间差在允许范围内，因此 NetScreen 设备会更新其时钟。如果时间差大于设定值， NetScreen 设备不会同步时钟，而是继续尝试查询该设备上配置的第一个备份 NTP 服务器。如果尝试查询所有配置的 NTP 服务器之后， NetScreen 设备仍未收到有效回复，设备会在事件日志中生成一条错误消息。此功能的缺省值为 3 秒，取值范围从 0 (无限制) 到 3600 (一小时)。

手动同步系统时钟时，只能使用 CLI，此时 NetScreen 设备不验证最大时间调整值。而是当 NetScreen 设备收到有效回复后，会显示一条消息，通知您访问的 NTP 服务器、时间差以及使用的认证方法类型。该消息还会要求您确认或取消对系统时钟的更新。

如果 NetScreen 设备未收到回复，则会显示超时消息。仅当 NetScreen 设备尝试访问该设备上配置的所有 NTP 服务器失败后，才会出现此消息。

注意：*使用 CLI 发出请求时，在键盘上按下 Ctrl-C 后，可以取消当前请求。*

NTP 与 NSRP

“NetScreen 冗余协议” (NSRP) 中包含一种机制，用于同步 NSRP 集群成员的系统时钟。尽管同步操作以秒为单位，但 NTP 服务器却采用次秒级的定时机制。由于处理延迟，可能导致每个集群成员的时间相差几秒。当两个集群成员同时启用 NTP 时， Juniper Networks 会建议您禁用 NSRP 时间同步，因为这两个成员要通过 NTP 服务器更新各自的系统时钟。要禁用 NSRP 时间同步功能，请输入以下命令 :

```
set ntp no-ha-sync
```

范例 : 配置 NTP 服务器和最大时间差值

在下例中，将配置 NetScreen 设备通过 NTP 服务器每隔五分钟更新一次时钟， NTP 服务器的 IP 地址为 1.1.1.1、1.1.1.2 和 1.1.1.3。同时还要将最大时间差值设置为 2 秒。

WebUI

Configuration > Date/Time: 输入以下内容，然后单击 **Apply**:

Automatically synchronize with an Internet Time Server (NTP): (选择)

Update system clock every minutes: 5

Maximum time adjustment seconds: 2

Primary Server IP/Name: 1.1.1.1

Backup Server1 IP/Name: 1.1.1.2

Backup Server2 IP/Name: 1.1.1.3

CLI

```
set clock ntp
set ntp server 1.1.1.1
set ntp server backup1 1.1.1.2
set ntp server backup2 1.1.1.3
set ntp interval 5
set ntp max-adjustment 2
save
```

保护 NTP 服务器

可以使用基于 MD5 的校验和来认证 NTP 数据包，以此来保护 NTP 信息流。无需创建 IPSec 通道。这种认证方法能确保 NTP 信息流的完整性。该方法不能阻止外来者查看数据，但可以防止任何人篡改数据。

要启用 NTP 信息流的认证机制，必须为 NetScreen 设备上配置的每个 NTP 服务器分配唯一的密钥 ID 和预共享密钥。密钥 ID 和预共享密钥用于生成校验和， NetScreen 设备和 NTP 服务器通过校验和来认证数据。

认证类型

存在两种认证 NTP 信息流的类型 : 必需认证和首选认证。

选择 **Required** 认证后， NetScreen 设备必须在发送给 NTP 服务器的所有数据包中加入认证信息 (密钥 ID 与校验和)，还必须认证从 NTP 服务器接收的所有 NTP 数据包。 NetScreen 设备和 NTP 服务器的管理员必须先交换密钥 ID 和预共享密钥，然后才能认证 NetScreen 设备与 NTP 服务器之间往来的信息流。必须以手动方式交换密钥 ID 和预共享密钥，可通过电子邮件、电话等方式来进行交换。

选择 **Preferred** 认证后， NetScreen 设备运行时必须首先尝试认证所有 NTP 信息流，就如同在 Required 模式下运行时一样。如果所有认证尝试都失败， NetScreen 设备将返回正常模式运行，就如同未选择认证时一样。同时向 NTP 服务器发送不含密钥 ID 和校验和的数据包。实际上，尽管 NetScreen 设备会优先执行认证，但即使认证失败，设备仍允许 NTP 信息流的往来流通。

索引

R

S

T

U

V

W

X

Y

Z