NetScreen 概念与范例

ScreenOS 参考指南

第 2 卷：基本原理

ScreenOS 4.0.0

编号 093-0520-000-SC

版本 F

Copyright Notice

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

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

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

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：

- 安全性、通道和功能区段
- 预定义和用户定义的虚拟路由器以及创建、修改和删除它们的方法
- 路由选择的概念，如静态和动态路由选择、路由重新分配、导出路由以及路由表配置
- 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
- 映射 IP (MIP) 地址、虚拟 IP (VIP) 地址、动态 IP (DIP) 地址和二级 IP 地址
- NetScreen 接口可以在其下运行的接口模式：网络地址转换 (NAT)、路由和透明
- 用来控制流过接口的信息流的策略，以及用来创建策略和虚拟专用网的元素，如地址、用户和服务
- NetScreen 设备可用的用户认证方法以及如何配置用户帐户和用户组
- 信息流管理方面的概念
- 下列功能的系统参数：
  - “域名系统” (DNS) 寻址
  - 用于分配或转递 TCP/IP 设置的 “动态主机配置协议” (DHCP)
  - URL 过滤
  - 向 NetScreen 设备上传以及从 NetScreen 设备下载配置设置和软件
  - 用来扩充 NetScreen 设备功能的软件密钥
  - 系统时钟配置

约定

本书介绍配置 NetScreen 设备的两种管理方法：Web 用户界面 (WebUI) 和命令行界面 (CLI)。下文介绍了二者使用的约定。

WebUI 导航约定

贯穿本书的全部篇章，用一个尖角符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。

范例：Objects > Addresses > List > New

要访问新地址配置对话框，请执行以下操作：

1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示 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. 单击右上角的 **New** 链接。
   出现新地址配置对话框。

CLI 约定

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

相关性定义符

每个语法说明中将介绍使用特殊字符来显示命令功能之间的相关性。

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

嵌套的相关性

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

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

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

以下例子说明一些 **set interface** 命令功能的相关性。

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

这个 { 和 } 括号说明指定的任一个 **flood** 或 **arp** 是必须遵循的。但是，[和] 括号说明，关于 **arp** 的 **trace-route** 选项不是必须遵循的。因而，这条命令可以采取以下任一种格式：

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

CLI 命令及功能的可用性

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

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

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

NETSCREEN 文档

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

欲在 NetScreen 产品版本上获得最新的技术信息，请参阅该版本的发行说明文档。欲获得发行说明，请浏览 www.netscreen.com/support 并选择 **Software Download**。选择产品及其版本，然后单击 **Go**。（欲执行此下载任务，您必须是注册用户。）

如果在以下内容中发现任何错误或遗漏，请使用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

1

ScreenOS 体系结构

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

本章对 ScreenOS 进行了简要介绍，包括以下几个主要内容：

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

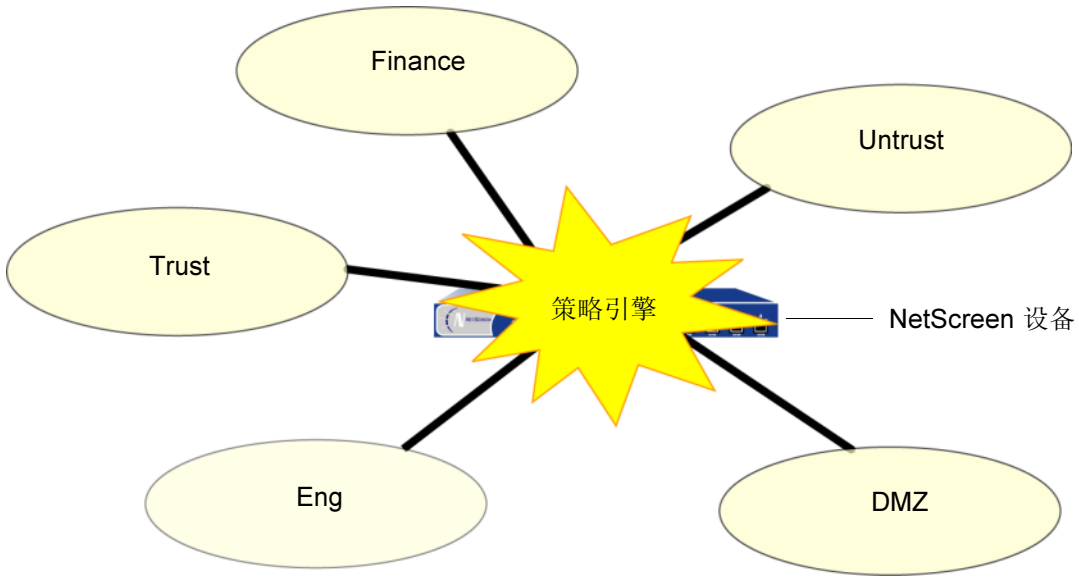
本章结束时给出了一个由四部分组成的范例，它例举了使用 ScreenOS 的 NetScreen 设备的基本配置：

多个安全区段

安全区段是由一个[1]或多个网段组成的集合，需要通过策略来对入站和出站信息流进行调整（参见第 7 页上的 “策略”）。您可以定义多个安全区段，确切数目可根据网络需要来确定。除用户定义的区段外，您还可以使用预定义的区段：Trust、Untrust 和 DMZ（用于 Layer 3（第 3 层）操作），或者 V1-Trust、V1-Untrust 和 V1-DMZ（用于 Layer 2（第 2 层）操作）。实际上，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。如果愿意，可以继续使用这些预定义区段。也可以忽略预定义区段[2]而只使用用户定义的区段。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 ScreenOS，您可以灵活使用和定义安全区段以最好地满足您的具体需要。

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）只有在策略允许的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，如果既没有绑定到它的接口也没有通讯簿条目，则也可以说它不包含任何网段。
2. 不能删除预定义安全区段。但是，可以删除用户定义的安全区段。删除安全区段时，还会同时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。

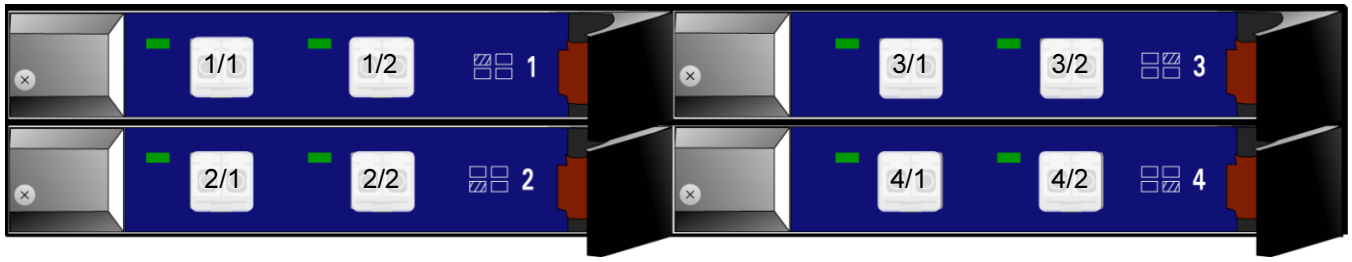
通过定义的策略，可以使两个区段间的信息流向一个或两个方向流动[3]。利用定义的路由，可指定信息流从一个区段到另一个区段必须使用的接口。由于可将多个接口绑定到一个区段上，所以您制定的路由对于将信息流引向您所选择的接口十分重要。

要为区段提供一个入口，需要将一个接口绑定到该区段，而且要 — 对于 “路由”或 NAT 模式的接口 （请参阅第 5 章，“接口模式”） — 为该接口分配一个 IP 地址。两种常见的接口类型为物理接口和 — 对于那些具有虚拟系统支持的设备 — 子接口 （即，物理接口在 Layer 2 （第 2 层）的具体体现）。有关详细信息，请参阅第 4 章，“接口”。

物理接口

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

物理接口分配

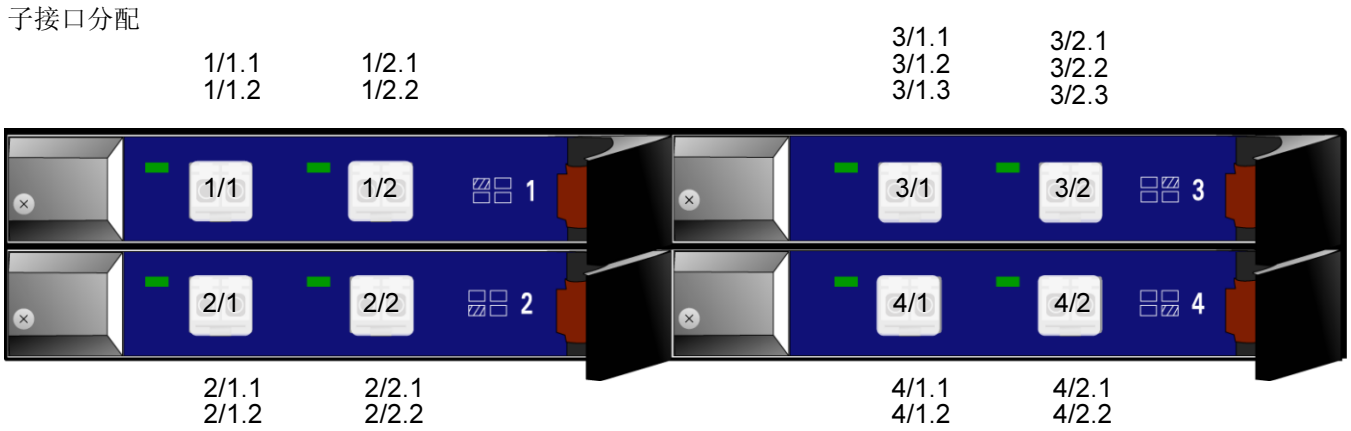


3. 对于在绑定到同一区段的两个接口间流动的信息流，因为两个接口具有相同的安全级别，所以不需要策略。 ScreenOS 对于两个区段间的信息流需要策略，如果是在一个区段内，则不需要。

子接口

在支持虚拟系统的设备上，可以在逻辑上将一个物理接口分为几个虚拟的子接口，每个子接口都从它来自的物理接口借用需要的带宽。子接口是一个抽象的概念，但它在功能上与实际端口的接口相同，子接口由 802.1Q VLAN 标记[4] 进行区分。 NetScreen 设备用子接口通过它的 IP 地址和 VLAN 标记来指引信息流流入和流出区段。为方便起见，网络管理员指定的 VLAN 标记通常与子接口号相同。例如，使用 VLAN 标记 3、名为 *ethernet1/2.3* 的接口表示接口模块在第一槽位，该模块上的第二个端口，子接口号为 **3** *(ethernet1/2.**3**)*。

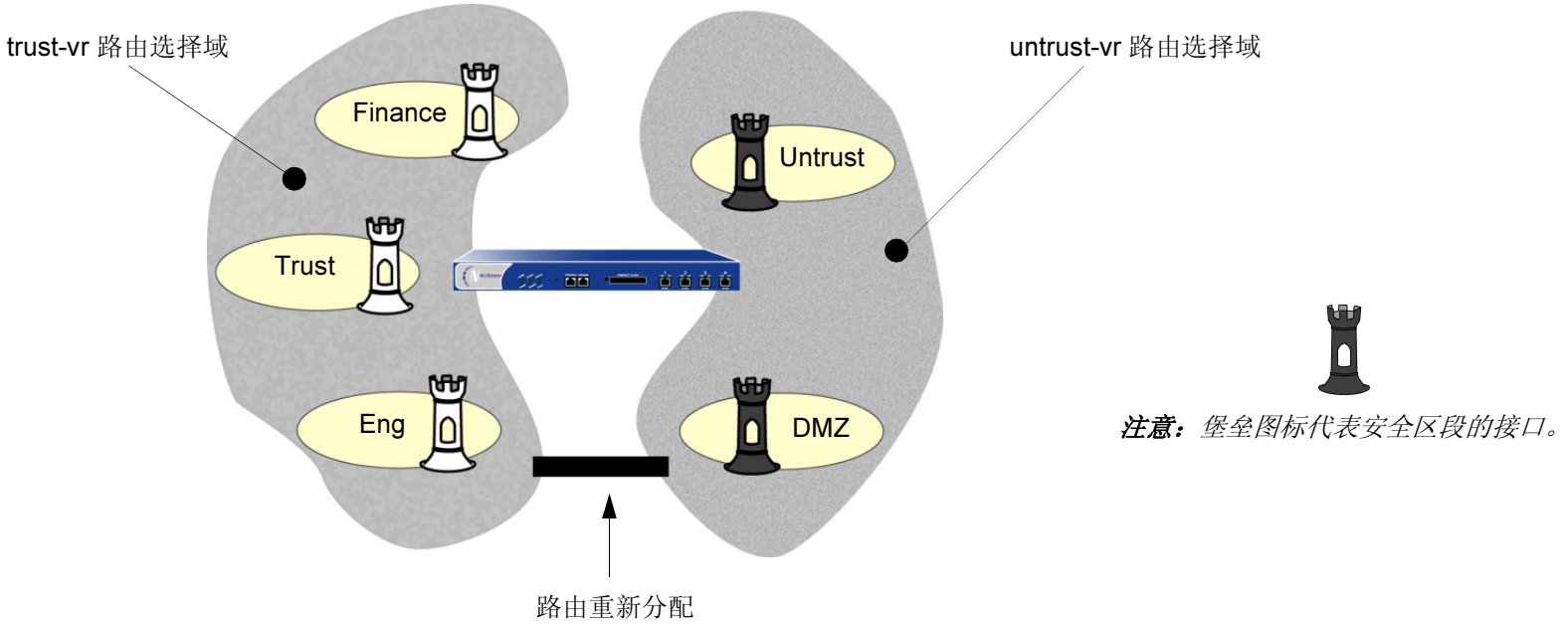
请注意，虽然子接口与物理接口共享部分标识，但是其绑定的区段并不依赖于物理接口绑定的区段。您可以将子接口 *ethernet1/2.3* 绑定到与物理接口 *ethernet1/2* 或 *ethernet1/2.2* 所绑定的不同区段上。同样， IP 地址的分配也没有限制。术语 *子接口*并不意味着它的地址在物理接口的地址空间的子网中。



4. 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

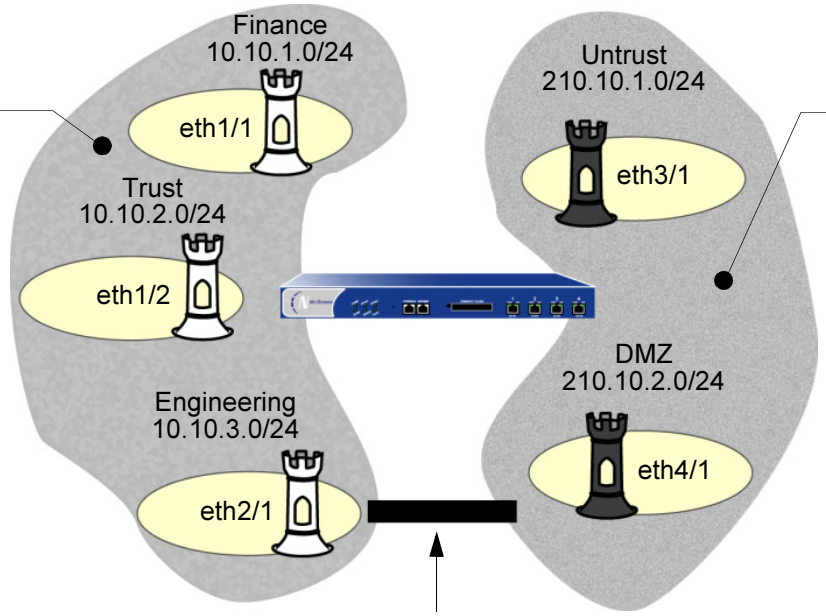
虚拟路由器 (VR) 与非虚拟路由器功能相同。它拥有自己的接口和路由表。在 ScreenOS 中， NetScreen 设备支持两个虚拟路由器。从而允许 NetScreen 设备维护两个单独的路由表，并隐藏虚拟路由器彼此之间的路由信息。例如，通常用来与不可信方进行通信的 untrust-vr 不含有任何保护区段的任何路由信息，这些信息由 trust-vr 进行维护。因此，通过从 untrust-vr 中秘密提取路由的方式，搜集不到任何内部网络信息。



注意：*要创建另外的 VR，必须先为 NetScreen 设备上的虚拟路由器获得并加载许可密钥。有关如何执行此项操作的信息，请参阅第 401 页上的 “许可密钥”。*

路由重新分配

每个虚拟路由器 (VR) 都维护着一个路由表，其中含有用于其路由选择域的唯一条目。也就是说， trust-vr 中的条目与那些在 untrust-vr 中维护的条目完全不同。因为在 trust-vr 中找不到 untrust-vr 中的路由表条目，所以对于 trust-vr 路由表没有而您又想使 trust-vr 中的信息流可以访问的任何路由，在 trust-vr 路由表中必须包含一条指向 untrust-vr 的路由。（同样，对于另一方向上的信息流，需要做的事情正好相反，即从 untrust-vr 到 trust-vr。）两个虚拟路由器之间的这种联系，在术语上叫做*路由重新分配*。



trust-vr 路由选择域

到	使用
10.10.1.0/24	eth1/1
10.10.2.0/24	eth1/2
10.10.3.0/24	eth2/1
0.0.0.0/0	**untrust-vr**

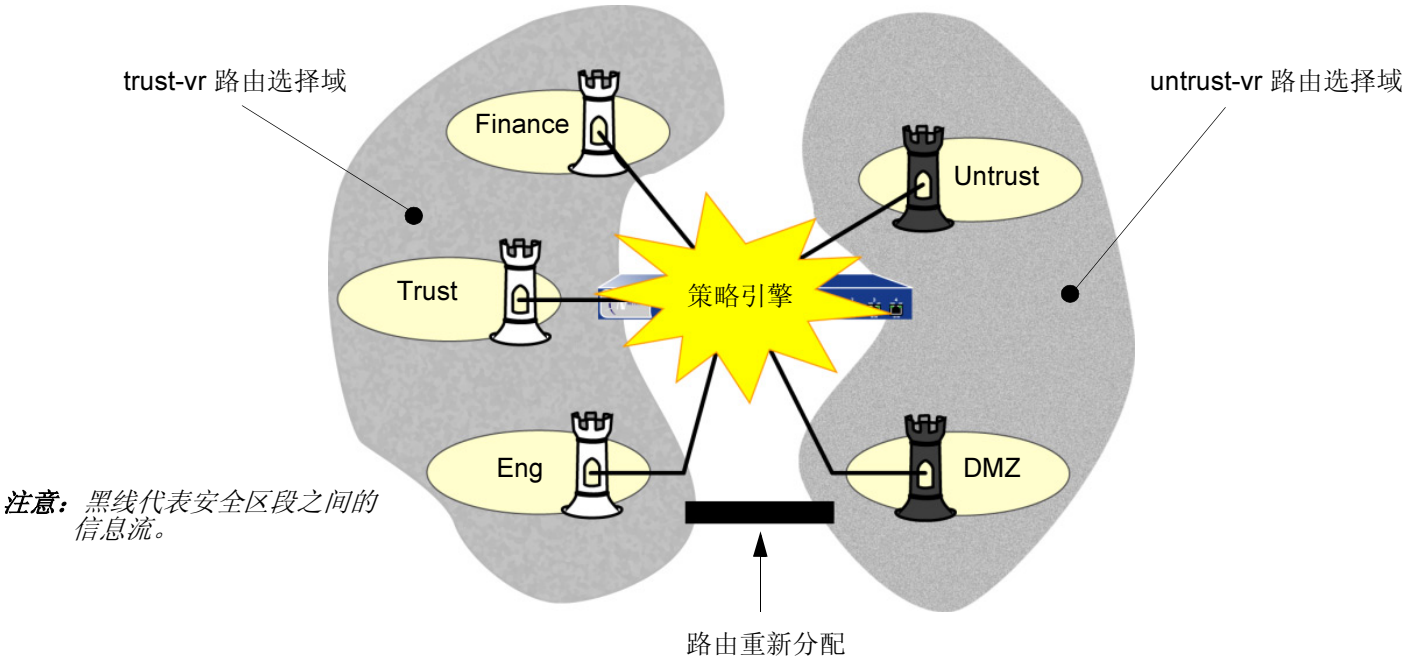
untrust-vr 路由选择域

到	使用
210.10.1.0/24	eth3/1
210.10.2.0/24	eth4/1
10.10.0.0/16	**trust-vr**
0.0.0.0/0	eth3/1

注意：*有关虚拟路由器的详细信息，请参阅第 3 章，“路由和虚拟路由器”。*

策略

每次当封包尝试从一个区段向另一区段或在绑定到同一区段的两个接口间传递时，NetScreen 设备会检查其策略组列表中是否有允许这种信息流的策略（请参阅第 219 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 发送信息流到区段 B 的策略。要使信息流向另一方向流动，则必须配置另一策略，允许信息流从区段 B 流向区段 A。对于从一个区段向另一区段传递的任何信息流，都必须有允许它的策略。同样，如果启用了内部区段阻塞，则必须要有允许信息流在该区段中从一个接口向另一个接口传递的策略。



注意： *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 7 章，“策略”。*

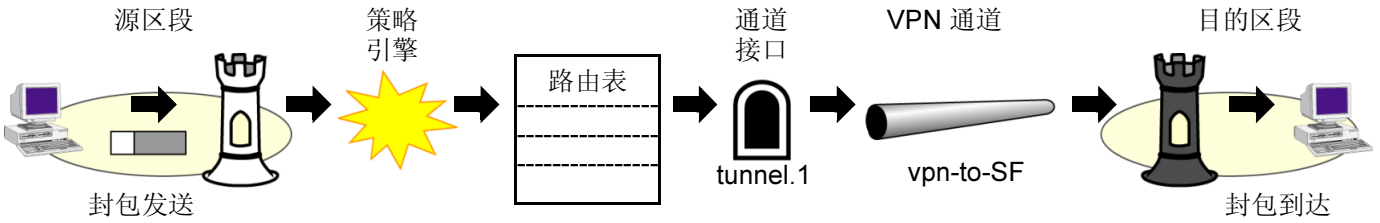
VPN

ScreenOS 支持多个虚拟专用网络 (VPN) 配置选项，其中的一些选项允许分离 VPN 通道和策略[5]。配置完成后，这些通道就成为可用的资源，用于保护一个安全区段与另一区段之间传递的信息流。

配置不依赖于任何策略的 VPN 通道的主要步骤，如下所示：

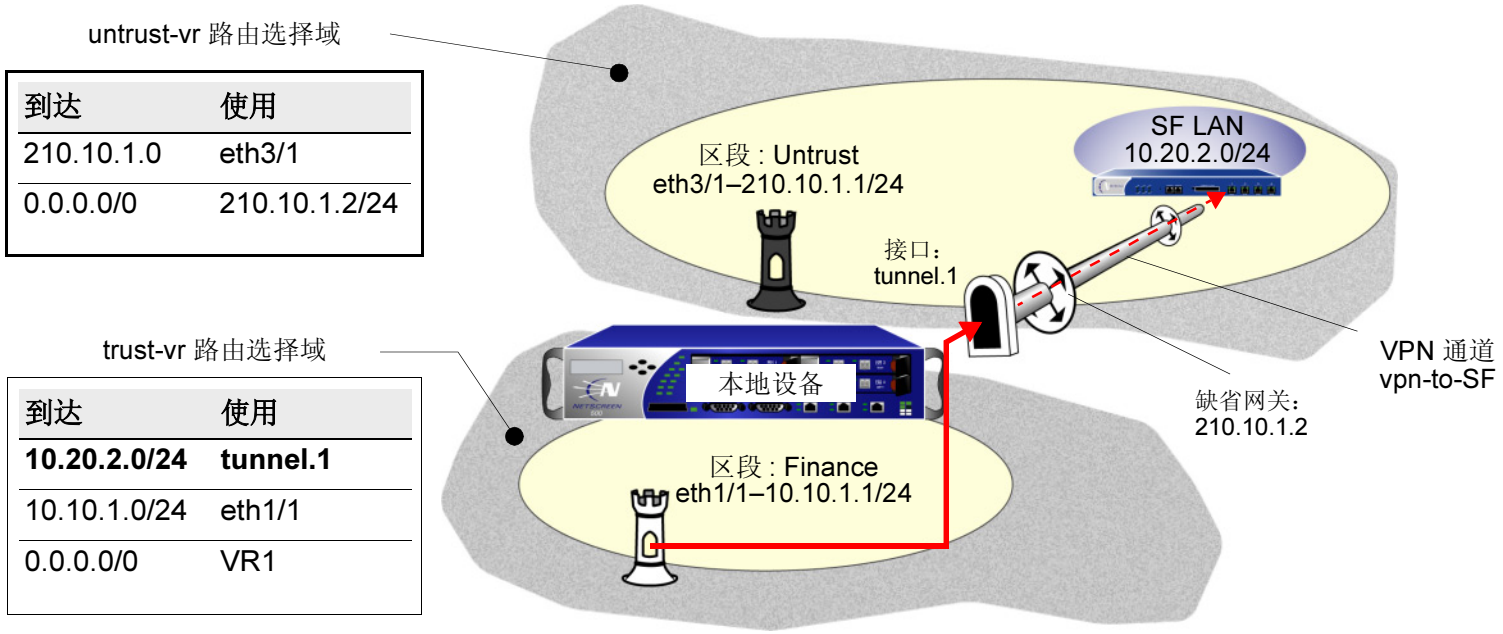
1. 配置 VPN 通道时（例如，*vpn-to-SF*，其中 *SF* 为目的或端实体），在本地设备上指定一个物理或子接口。（远程对等方配置其远程网关时，必须使用此接口的 IP 地址。）
2. 创建一个通道接口（例如，*tunnel.1*），将其绑定到一个安全区段[6]。
3. 将通道接口 *tunnel.1* 绑定到 VPN 通道 *vpn-to-SF* 上。
4. 要引导信息流通过此通道，请设置一个路由，指明到 *SF* 的信息流必须使用 *tunnel.1*。

此时，该通道已就绪，为 *SF* 绑定的信息流可以从中通过。现在可以设置策略，允许或阻止信息流从指定源传递到该目标。



5. 在 ScreenOS 的早期版本中， VPN 策略必须明确指定通道并命名具体的 VPN 通道。在当前发行的 ScreenOS 版本中，仍可以这样配置 VPN 策略。不过，您也可以将策略配置为仅允许或拒绝两个安全区段间的信息流。允许时，如果到指定目标的路由指向一个绑定到 VPN 通道的接口，则该信息流就会通过通道进行传递。
6. 不必将该通道接口绑定到本地发出 VPN 信息流的同一区段上。如果路由指向某通道接口，则来自于任何区段的信息流都可以访问该接口。

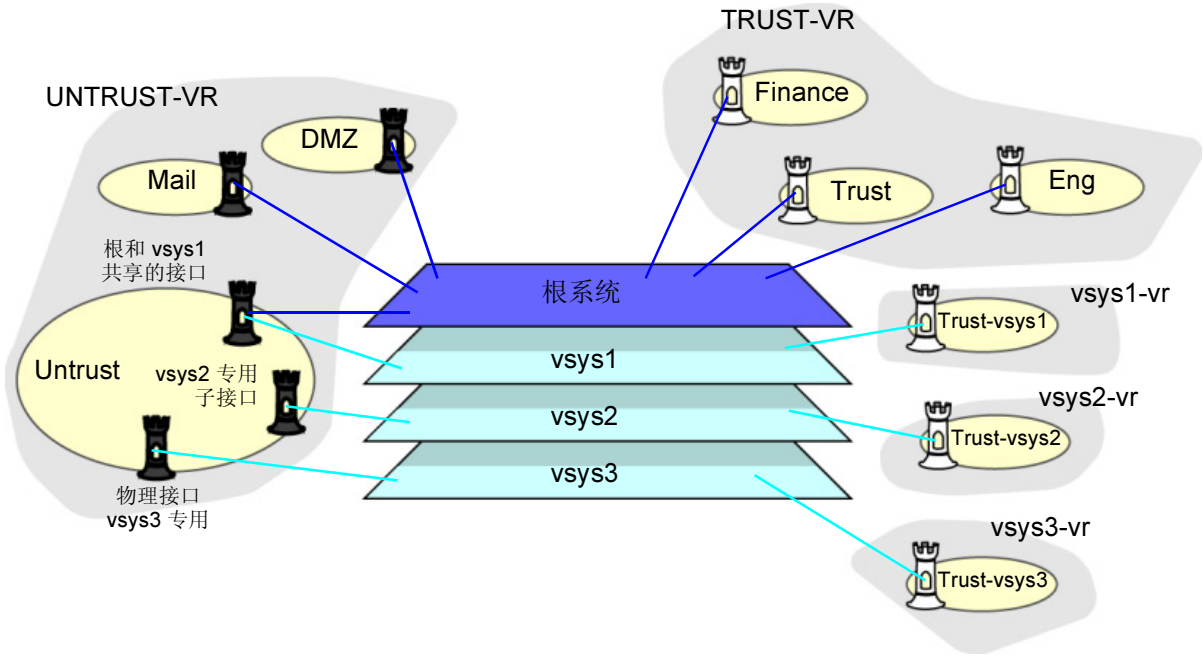
从安全区段 Finance 到安全区段 Untrust 中的 “SF LAN” 的信息流被路由到通道接口 tunnel.1。因为 tunnel.1 绑定到 VPN 通道 vpn-to-SF 上，所以信息流通过该通道发送到 “SF LAN” 上的远程网关。



虚拟系统

一些 NetScreen 设备支持虚拟系统 (vsys)[7]。将 ScreenOS 应用于虚拟系统需要协调三个主要成员：区段、接口和虚拟路由器。下面的图例从概念上简要说明 ScreenOS 如何同时在根级和 vsys 级上将这些成员紧密结合在一起。

注意： *堡垒图标代表安全区接口。*

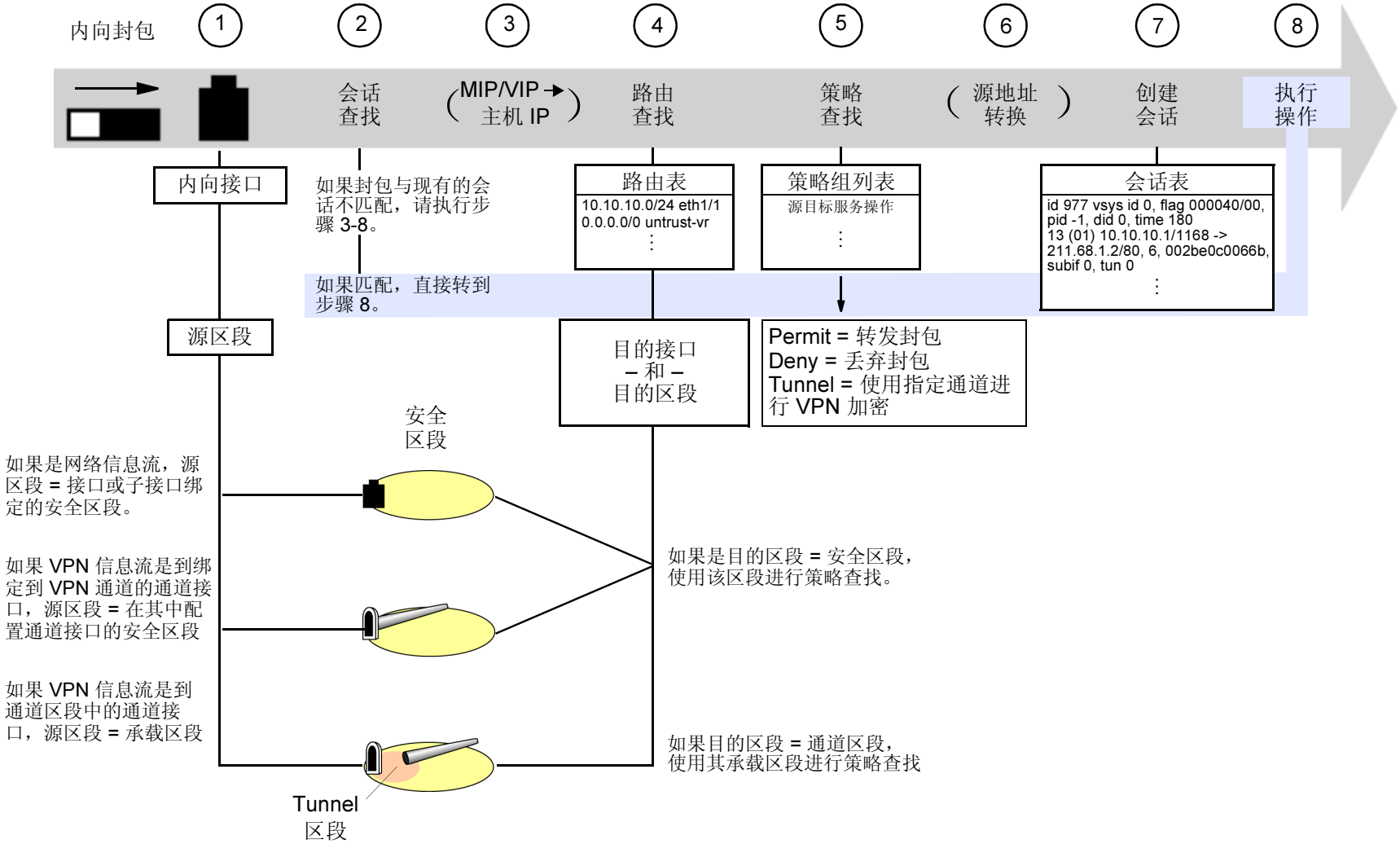


注意： *有关虚拟系统以及在虚拟系统环境中应用区段、接口和虚拟路由器的详细信息，请参阅第 6 卷，“虚拟系统”。*

7. 虚拟系统是对主系统的细分，在用户看来，它就像是一个独立的实体。虚拟系统相对于同一 NetScreen 设备中的任何其它虚拟系统以及根系统是独立存在的。

封包流序列

在 ScreenOS 中，内向封包的流序列按如下所示的方式进行。



1. 接口模块识别内向接口，进而识别绑定到该接口的源区段。

   源区段根据以下判别条件进行确定：

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

2. 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 3 到 8。

   如果该包与现有会话匹配， NetScreen 设备会执行 “快速处理”，用现有会话条目中可用的信息来处理该封包。“快速处理”会跳过步骤 3 到 7，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。

3. 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。

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

   目的区段根据以下判别条件进行确定：

   – 如果目的区段是安全区段，请使用该区段进行策略查找。
   – 如果目的区段是通道区段，请使用相应的承载区段进行策略查找。

5. 策略引擎搜寻策略组列表，以便在识别出来的源和目的区段中的地址之间查找策略。

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

   – 如果操作为 **permit （允许）**，防火墙会决定将包转发到其目标地点。
   – 如果操作为 **deny （拒绝）**，防火墙会决定将包丢弃。
   – 如果操作为 **tunnel （通道）**，防火墙会决定将包转发给 VPN 模块，该模块对包进行封装并用指定的 VPN 通道设置进行传送。

6. 如果指定进行源地址转换（基于接口的 NAT 或基于策略的 NAT），NAT 模块会在将源地址转发到目标地点或 VPN 模块前对其进行转换。
7. 会话模块在会话表中创建一个新条目，其中包含步骤 1 到 6 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。

8. NetScreen 设备执行在会话中指定的操作。

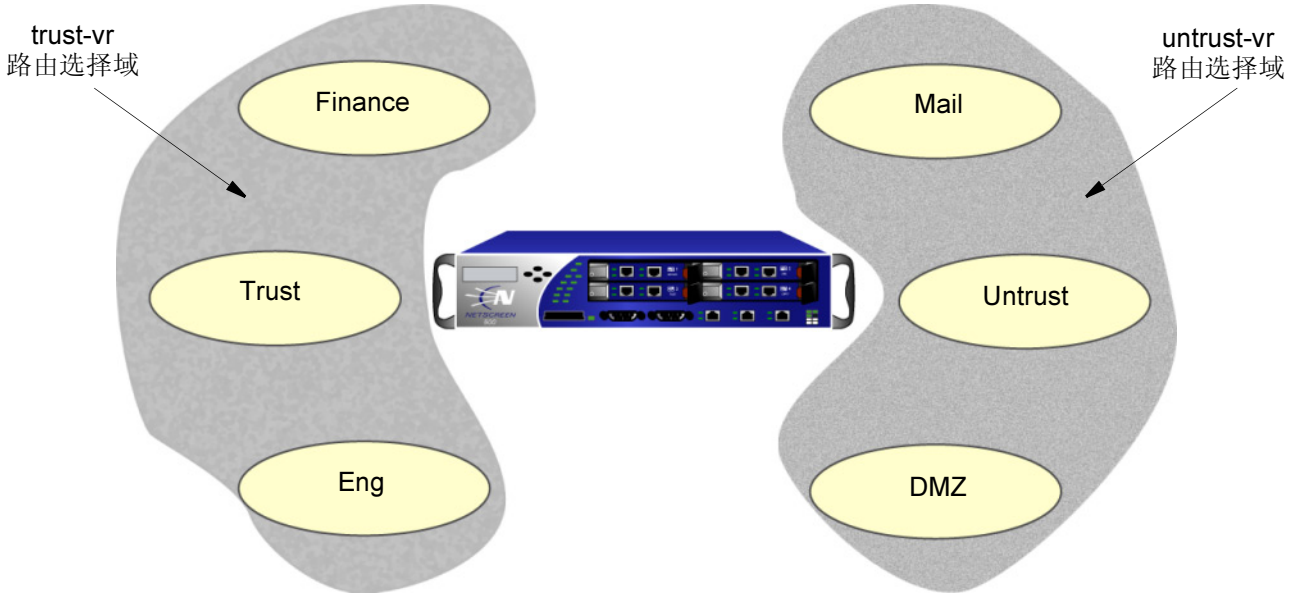
   典型的操作有源地址转换、 VPN 通道选择、加密、解密和包转发。

范例 （第 1 部分）：具有六个区段的企业

这是一个渐进式范例的第一部分。在下一部分中，将设置每个区段的接口，请参阅第 16 页上的“范例 （第 2 部分）：六个区段的接口”。在这里为企业配置以下六个区段：

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

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



8. 有关虚拟路由器及其路由选择域的详细信息，请参阅第 3 章，“路由和虚拟路由器”。

WebUI

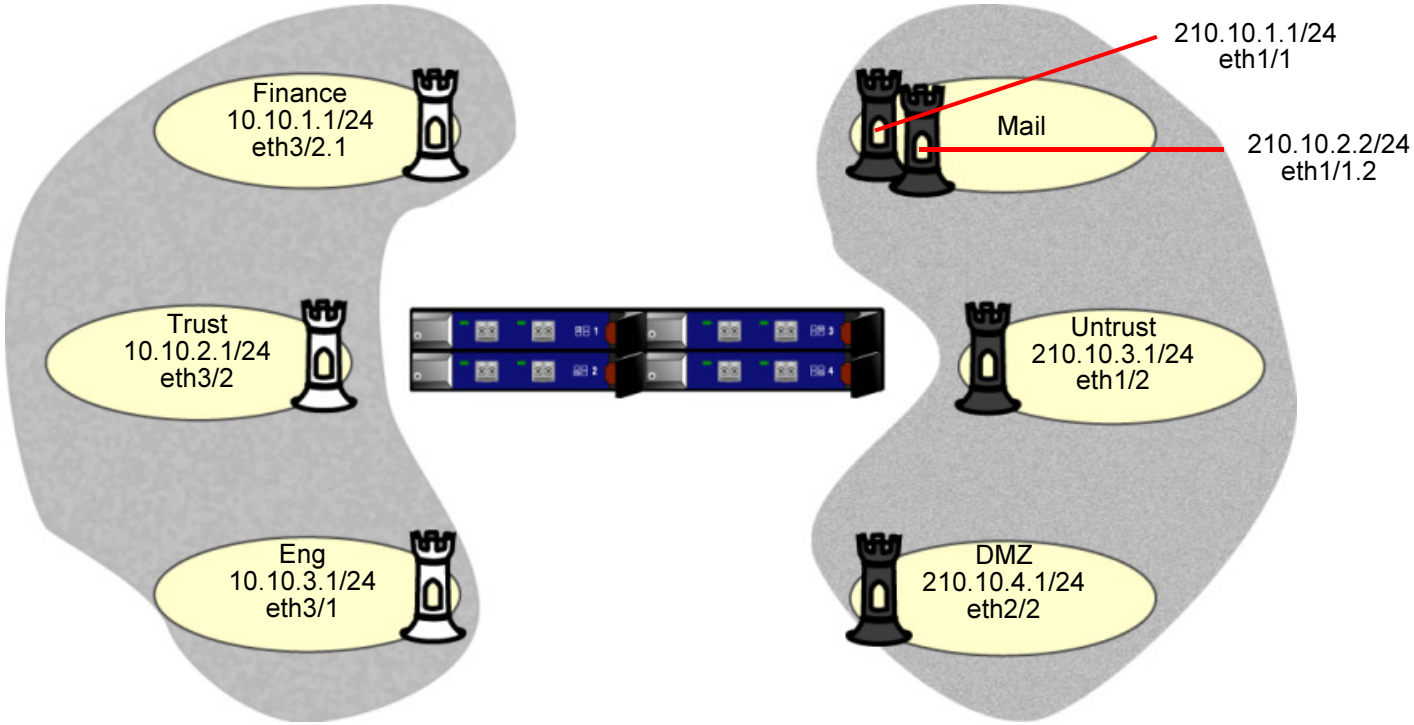
1. Network > Zones > New：输入以下内容，然后单击 **OK**：
   Zone Name: Finance
   Virtual Router Name: trust-vr
   Zone Type: Layer 3: （选择）
2. Network > Zones > New: 输入以下内容，然后单击 **OK**：
   Zone Name: Eng
   Virtual Router Name: trust-vr
   Zone Type: Layer 3: （选择）
3. Network > Zones > New: 输入以下内容，然后单击 **OK**：
   Zone Name: Mail
   Virtual Router Name: untrust-vr
   Zone Type: Layer 3: （选择）
4. Network > Zones > Edit（对于 Untrust）：在 Virtual Router Name 下拉列表中选择 **untrust-vr**，然后单击 **OK**。
5. 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

1. set zone name finance
2. set zone name eng
3. set zone name mail
4. set zone mail vrouter untrust-vr
5. set zone untrust vrouter untrust-vr
6. set zone dmz vrouter untrust-vr
7. save

范例 （第 2 部分）：六个区段的接口

这是一个渐进式范例的第二部分。在第一部分中，对区段进行了配置，请参阅第 14 页上的 “范例 （第 1 部分）：具有六个区段的企业”。在下一部分中，将对虚拟路由器进行配置，请参阅第 20 页上的 “范例 （第 3 部分）：具有两个路由选择域的企业”。范例的这一部分演示了如何配置接口并将其绑定到区段上。



WebUI

接口 ethernet3/2

1. Network > Interfaces > Edit（对于 ethernet3/2）：输入以下内容，然后单击 **Apply**：
   Zone Name: Trust
   IP Address/Netmask: 10.10.2.1/24
   Management Services: WebUI, Telnet, SNMP, SCS （选择）
   Other Services: Ping （选择）

接口 ethernet3/2.1

2. Network > Interfaces > Sub-IF New: 输入以下内容，然后单击 **OK**：
   Interface Name: ethernet3/2.1
   Zone Name: Finance
   IP Address/Netmask: 10.10.1.1/24
   VLAN Tag: 1
   Other Services: Ping （选择）

接口 ethernet3/1

3. Network > Interfaces > Edit（对于 ethernet3/1）：输入以下内容，然后单击 **OK**：
   Zone Name: Eng
   IP Address/Netmask: 10.10.3.1/24
   Other Services: Ping （选择）

接口 ethernet1/1

4. Network > Interfaces > Edit（对于 ethernet1/1）：输入以下内容，然后单击 **OK**：
   Zone Name: Mail
   IP Address/Netmask: 210.10.1.1/24

接口 ethernet1/1.2

5. Network > Interfaces > Sub-IF New: 输入以下内容，然后单击 **OK**：
   Interface Name: ethernet1/1.2
   Zone Name: Mail
   IP Address/Netmask: 210.10.2.2/24
   VLAN Tag: 2

接口 ethernet1/2

6. Network > Interfaces > Edit（对于 ethernet1/2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.10.3.1/24
   Management Services: SNMP （选择）

接口 ethernet2/2

7. Network > Interfaces > Edit（对于 ethernet2/2）：输入以下内容，然后单击 **OK**：
   Zone Name: DMZ
   IP Address/Netmask: 210.10.4.1/24

CLI

接口 ethernet3/2

1. set interface ethernet3/2 zone trust
2. set interface ethernet3/2 ip 10.10.2.1/24
3. set interface ethernet3/2 manage ping
4. set interface ethernet3/2 manage webui
5. set interface ethernet3/2 manage telnet
6. set interface ethernet3/2 manage snmp
7. set interface ethernet3/2 manage scs

接口 ethernet3/2.1

8. set interface ethernet3/2.1 zone finance
9. set interface ethernet3/2.1 ip 10.10.1.1/24 tag 1
10. set interface ethernet3/2.1 manage ping

接口 ethernet3/1

11. set interface ethernet3/1 zone eng
12. set interface ethernet3/1 ip 10.10.3.1/24
13. set interface ethernet3/1 manage ping

接口 ethernet1/1

14. set interface ethernet1/1 zone mail
15. set interface ethernet1/1 ip 210.10.1.1/24

接口 ethernet1/1.2

16. set interface ethernet1/1.2 zone mail
17. set interface ethernet1/1.2 ip 210.10.2.2 /24 tag 2

接口 ethernet1/2

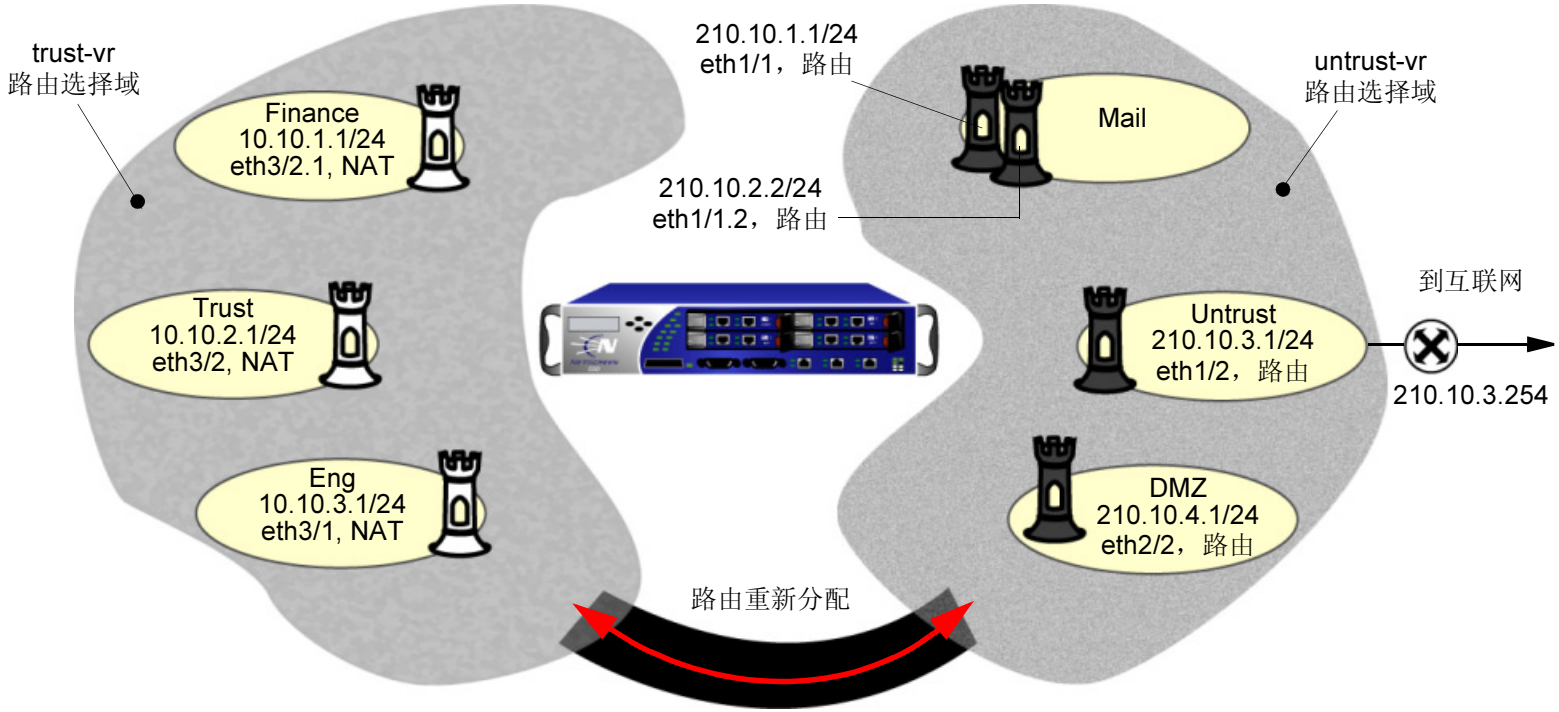
18. set interface ethernet1/2 zone untrust
19. set interface ethernet1/2 ip 210.10.3.1/24
20. set interface ethernet1/2 manage snmp

接口 ethernet2/2

21. set interface ethernet2/2 zone dmz
22. set interface ethernet2/2 ip 210.10.4.1/24
23. save

范例 （第 3 部分）：具有两个路由选择域的企业

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 16 页上的 “范例（第 2 部分）：六个区段的接口”。在下一部分中，将对策略进行设置，请参阅第 22 页上的 “范例 （第 4 部分）：具有六个区段的企业所用的策略”。在本例中，您只须为连接到互联网的缺省网关配置路由。其它路由在您创建接口 IP 地址时由 NetScreen 设备自动创建。



WebUI

Network > Routing > Routing Table > 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: 210.10.3.254

CLI

1. set vrouter untrust-vr route 0.0.0.0/0 interface eth1/2 gateway 210.10.3.254
2. save

NetScreen 设备自动创建以下路由 （黑色）：

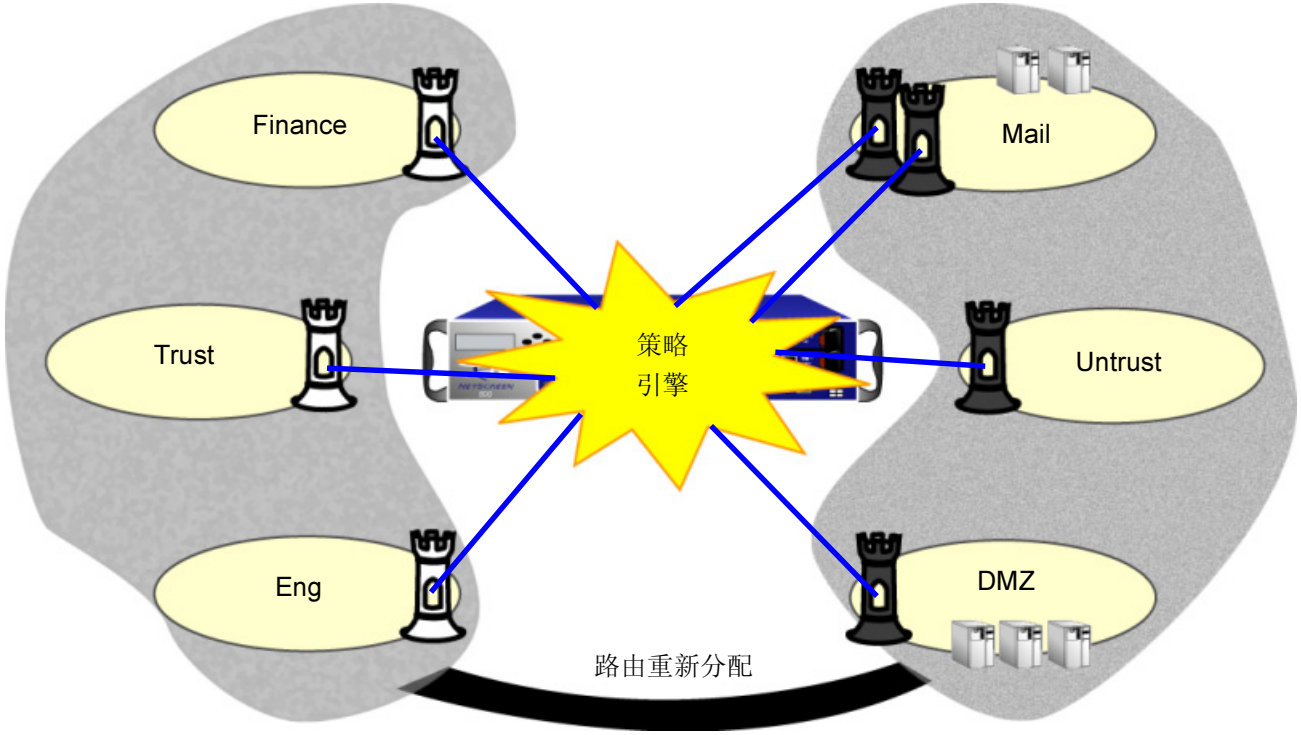
trust-vr		
到达：	**使用接口：**	**使用网关：**
0.0.0.0/0	n/a	untrust-vr
10.10.3.0/24	eth3/1	0.0.0.0
10.10.2.0/24	eth3/2	0.0.0.0
10.10.1.0/24	eth3/2.1	0.0.0.0

untrust-vr		
到达：	**使用接口：**	**使用网关：**
210.10.4.0/24	eth2/2	0.0.0.0
210.10.3.0/24	eth1/2	0.0.0.0
210.10.2.0/24	eth1/1.2	0.0.0.0
210.10.1.0/24	eth1/1	0.0.0.0
0.0.0.0/0	eth1/2	210.10.3.254

注意：只有这个条目由用户配置。

范例 （第 4 部分）：具有六个区段的企业所用的策略

这是一个渐进式范例的最后一部分。上一部分为第 20 页上的 “范例 （第 3 部分）：具有两个路由选择域的企业”。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

服务组

1. Objects > Services > Group > 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。

2. Object > Services > Group > 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。

策略

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

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （选择） , Any

   Service: Mail-Pop3

   Action: Permit

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

   Source Address:

   Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , Any

Service: Mail-Pop3

Action: Permit

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , Any

Service: Mail-Pop3

Action: Permit

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , Any

Service: Mail

Action: Permit

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , Any

Service: HTTP-FTPGet

Action: Permit

8. Policies > (From: Finance, To: DMZ) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , Any
   Destination Address:
   Address Book: （选择） , Any
   Service: HTTP-FTPGet
   Action: Permit
9. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , Any
   Destination Address:
   Address Book: （选择） , Any
   Service: HTTP-FTPGet
   Action: Permit
10. Policies > (From: Trust, To: DMZ) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Any
    Destination Address:
    Address Book: （选择） , Any
    Service: HTTP-FTPGet
    Action: Permit

11. Policies > (From: Eng, To: DMZ) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Any
    Destination Address:
    Address Book: （选择） , Any
    Service: HTTP-FTPGet
    Action: Permit
12. Policies > (From: Eng, To: DMZ) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Any
    Destination Address:
    Address Book: （选择） , Any
    Service: FTP-Put
    Action: Permit
13. Policies > (From: Untrust, To: DMZ) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Any
    Destination Address:
    Address Book: （选择） , Any
    Service: HTTP-FTPGet
    Action: Permit

CLI

服务组

1. set group service mail-pop3 add mail
2. set group service mail-pop3 add pop3
3. set group service http-ftpget add http
4. set group service http-ftpget add ftpget

策略

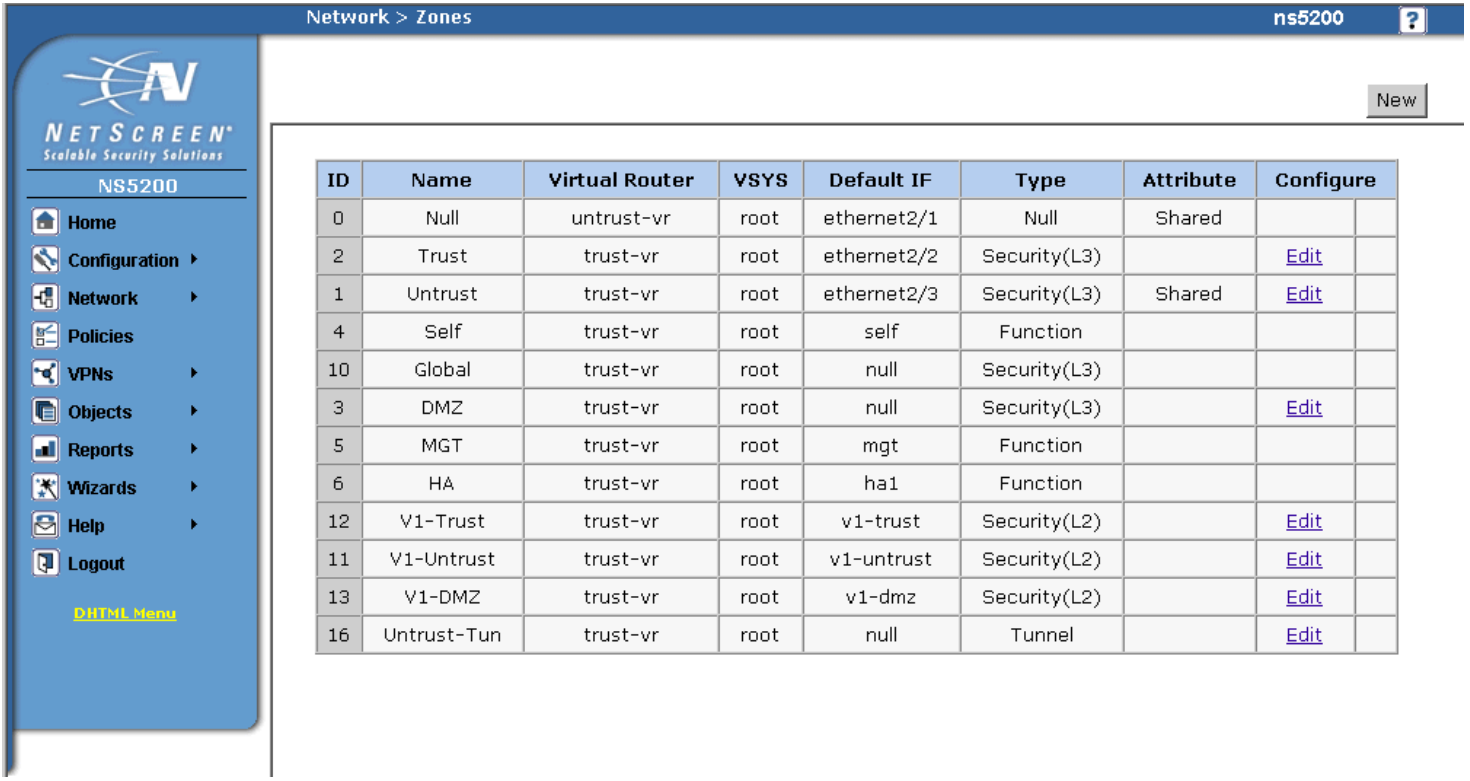
5. set policy from finance to mail any any mail-pop3 permit
6. set policy from trust to mail any any mail-pop3 permit
7. set policy from eng to mail any any mail-pop3 permit
8. set policy from untrust to mail any any mail permit
9. set policy from finance to untrust any any http-ftpget permit
10. set policy from finance to dmz any any http-ftpget permit
11. set policy from trust to untrust any any http-ftpget permit
12. set policy from trust to dmz any any http-ftpget permit
13. set policy from eng to untrust any any http-ftpget permit
14. set policy from eng to dmz any any http-ftpget permit
15. set policy from eng to dmz any any ftp-put permit
16. set policy from untrust to dmz any any http-ftpget permit
17. save

2

区段

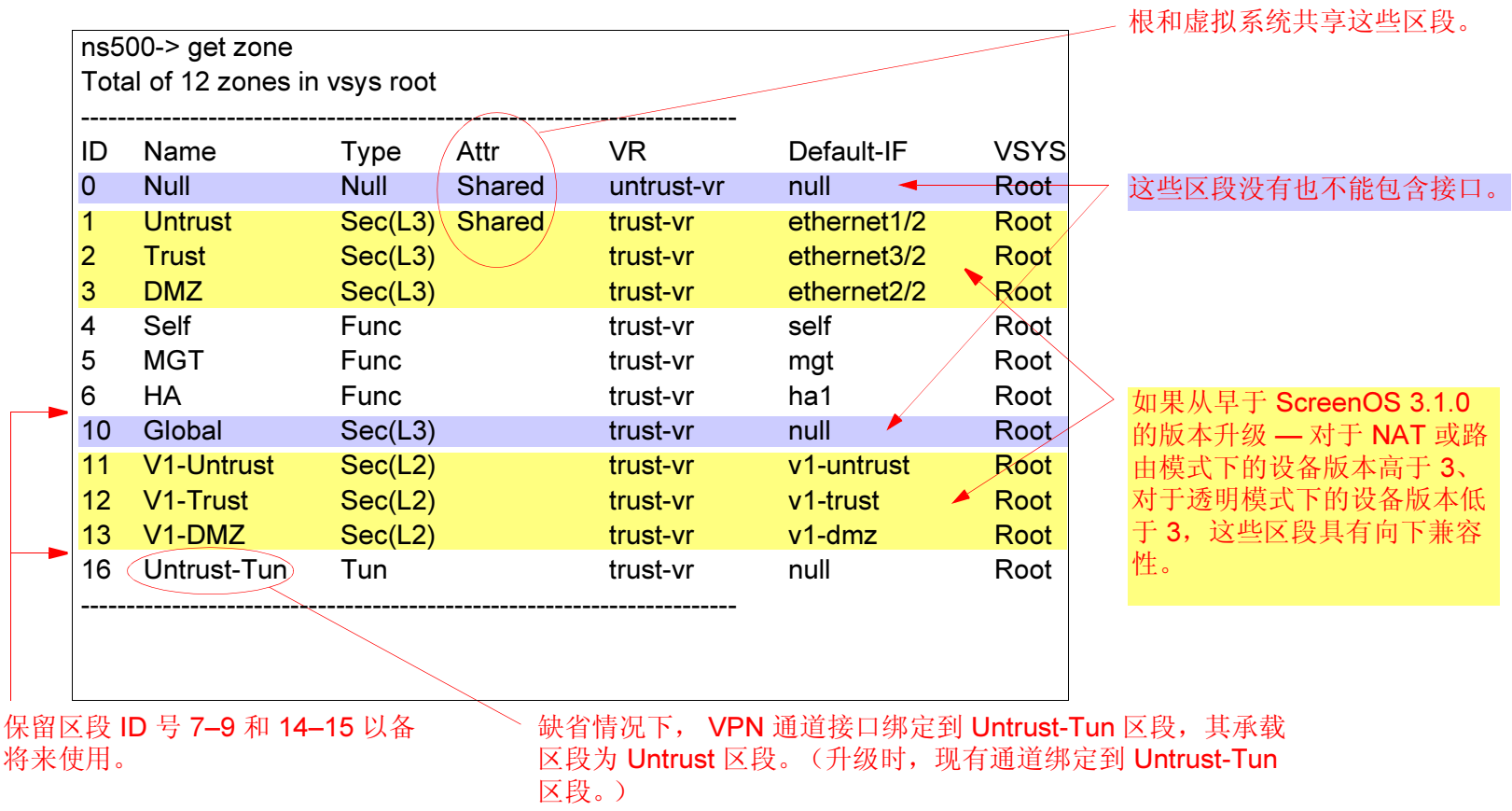
区段可以是网络空间中应用了安全措施的部分（安全区段）、绑定了 VPN 通道接口的逻辑部分（通道区段），或者是执行特定功能的物理或逻辑实体（功能区段）。本章研究各种类型的区段，特别将重点放在安全区段上。本章由以下几节组成：

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



ID	Name	Virtual Router	VSYS	Default IF	Type	Attribute	Configure	
0	Null	untrust-vr	root	ethernet2/1	Null	Shared		
2	Trust	trust-vr	root	ethernet2/2	Security(L3)		Edit	
1	Untrust	trust-vr	root	ethernet2/3	Security(L3)	Shared	Edit	
4	Self	trust-vr	root	self	Function			
10	Global	trust-vr	root	null	Security(L3)			
3	DMZ	trust-vr	root	null	Security(L3)		Edit	
5	MGT	trust-vr	root	mgt	Function			
6	HA	trust-vr	root	ha1	Function			
12	V1-Trust	trust-vr	root	v1-trust	Security(L2)		Edit	
11	V1-Untrust	trust-vr	root	v1-untrust	Security(L2)		Edit	
13	V1-DMZ	trust-vr	root	v1-dmz	Security(L2)		Edit	
16	Untrust-Tun	trust-vr	root	null	Tunnel		Edit	

get zone 命令的输出为：



上述预定义区段可分为三种不同类型：

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

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。必须最少定义两个安全区段，以便在网络的不同区域间分开提供基本的保护。在某些 NetScreen 平台上，您可以定义多个安全区段，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，因为它有地址簿而且可以在策略中引用。Global 区段满足这些条件。但是，它不具有其它安全区段都具有的一种元素 — 接口。Global 区段可充当映射 IP (MIP) 和虚拟 IP (VIP) 地址的存储区域。因为转向这些地址的信息流被映射到其它地址，所以 Global 区段不需要用于使信息流从中流过的接口。

Global 区段还包含全域策略中使用的地址。有关全域策略的详细信息，请参阅第 218 页上的 “全局策略”。

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

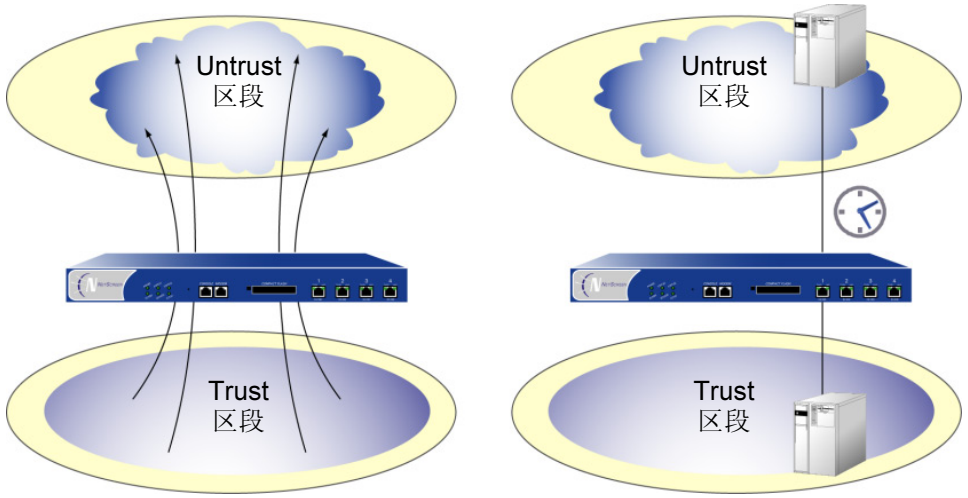
防火墙选项

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

缺省情况下，NetScreen 防火墙拒绝所有方向的所有信息流。[1] 通过创建策略，定义允许在预定时间通过指定源地点到达指定目的地点的信息流的种类，您可以控制区段间的信息流。范围最大时，可以允许所有类型的信息流从一个区段中的任何源地点到其它所有区段中的任何目的地点，而且没有任何预定时间限制。范围最小时，可以创建一个策略，只允许一种信息流在预定的时间段内、在一个区段中的指定主机与另一区段中的指定主机之间流动。

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

狭义的互联网访问：SMTP 服务可在 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



注意： *有关创建和应用策略的详细信息，请参阅第 7 章，第 215 页上的“策略”。*

1. 某些 NetScreen 设备出厂时设置的缺省策略为拒绝所有入站信息流但允许所有出站信息流。

为保护所有连接尝试的安全，NetScreen 设备使用了一种动态封包过滤方法，即通常所说的状态式检查。使用此方法，NetScreen 设备在 TCP 包头中记入各种不同的信息单元 — 源和目的 IP 地址、源和目的端口号，以及封包序列号 — 并保持穿越防火墙的每个 TCP 会话的状态。（NetScreen 也会根据变化的元素，如动态端口变化或会话终止，来修改会话状态。）当响应的 TCP 封包到达时，NetScreen 设备会将其包头中包含的信息与检查表中储存的相关会话的状态进行比较。如果相符，允许响应封包通过防火墙。如果不相符，则丢弃该封包。

NetScreen 防火墙选项用于保护区段的安全，具体做法是先检查要求经过某一接口离开和到达该区域的所有连接尝试，然后予以准许或拒绝。为避免来自其它区段的攻击，可以启用防御机制来检测并避开以下常见的网络攻击。下列选项可用于具有物理接口的区段 （这些选项不适用于子接口）：SYN Attack （SYN 攻击）、 ICMP Flood （ICMP 泛滥）、 UDP Flood （UDP 泛滥）和 Port Scan Attack （端口扫描攻击）。

- **SYN Attack（SYN 攻击）：** 当网络中充满了会发出无法完成的连接请求的 SYN 封包，以至于网络无法再处理合法的连接请求，从而导致拒绝服务 (DoS) 时，就发生了 SYN 泛滥攻击。
- **ICMP Flood（ICMP 泛滥）：** 当 ICMP ping 产生的大量回应请求超出了系统的最大限度，以至于系统耗费所有资源来进行响应直至再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。当启用了 ICMP 泛滥保护功能时，可以设置一个临界值，一旦超过此值就会调用 ICMP 泛滥攻击保护功能。（缺省的临界值为每秒 1000 个封包。）如果超过了该临界值，NetScreen 设备在该秒余下的时间和下一秒内会忽略其它的 ICMP 回应要求。
- **UDP Flood（UDP 泛滥）：** 与 ICMP 泛滥相似，当以减慢系统速度为目的向该点发送 UDP 封包，以至于系统再也无法处理有效的连接时，就发生了 UDP 泛滥。当启用了 UDP 泛滥保护功能时，可以设置一个临界值，一旦超过此临界值就会调用 UDP 泛滥攻击保护功能。（缺省的临界值为每秒 1000 个封包。）如果从一个或多个源向单个目表发送的 UDP 封包数超过了此临界值，NetScreen 设备在该秒余下的时间和下一秒内会忽略其它到该目标的 UDP 封包。
- **Port Scan Attack（端口扫描攻击）：** 当一个源 IP 地址在定义的时间间隔内（缺省值为 5,000 微秒）向位于相同目标 IP 地址 10 个不同的端口发送 IP 封包时，就会发生端口扫描攻击。这个方案的目的是扫描可用的服务，希望会有一个端口响应，因此识别出作为目标的服务。NetScreen 设备在内部记录从某一远程源地点扫描的不同端口的数目。使用缺省设置，如果远程主机在 0.005 秒内扫描了 10 个端口（5,000 微秒），NetScreen 会将这一情况标记为端口扫描攻击，并在该秒余下的时间内拒绝来自该源地点的其它封包（不论目标 IP 地址为何）。

余下的选项可用于具有物理接口和子接口的区段：

- **Limit session（限制会话）**：NetScreen 设备可限制由单个 IP 地址建立的会话数量。例如，如果从同一客户端发送过多的请求，就能耗尽 Web 服务器上的会话资源。此选项定义了每秒钟 NetScreen 设备可以为单个 IP 地址建立的最大会话数量。（缺省临界值为每个 IP 地址每秒 128 个会话。）
- **SYN-ACK-ACK Proxy 保护**：当认证用户初始化 Telnet 或 FTP 连接时，用户会 SYN 封包到 Telnet 或 FTP 服务器。NetScreen 设备会截取封包，通过 Proxy 将 SYN-ACK 封包发送给用户。用户用 ACK 封包响应。此时，初始的三方握手就已完成。NetScreen 设备在其会话表中建立项目，并向用户发送登录提示。如果用户怀有恶意而不登录，但继续启动 SYN-ACK-ACK 会话，NetScreen 会话表就可能填满到某个程度，让设备开始拒绝合法的连接要求。

  要阻挡这类攻击，您可以启用 SYN-ACK-ACK Proxy 保护 SCREEN 选项。从相同 IP 地址的连接数目到达 syn-ack-ack-proxy 临界值后，NetScreen 设备就会拒绝来自该 IP 地址的进一步连接要求。缺省情况下，来自单一 IP 地址的临界值是 512 次连接。您可以更改这个临界值（为 1 到 2,500,000 之间的任何数目）以更好地适合网络环境的需求。
- **SYN Fragment（SYN 碎片）**：SYN 碎片攻击使目标主机充塞过量的 SYN 封包碎片。主机接到这些碎片后，会等待其余的封包到达以便将其重新组合在起来。通过向服务器或主机堆积无法完成的连接，主机的内存缓冲区最终将会塞满。进一步的连接无法进行，并且可能会破坏主机操作系统。当协议字段指示是 ICMP 封包，并且片断标志被设置为 1 或指出了偏移值时，NetScreen 设备会丢弃 ICMP 封包。
- **SYN and FIN Bits Set（SYN 和 FIN 位的封包）**：通常不会在同一封包中同时设置 SYN 和 FIN 标志。但是，攻击者可以通过发送同时置位两个标志的封包来查看将返回何种系统应答，从而确定出接收端上的系统的种类。接着，攻击者可以利用已知的系统漏洞来实施进一步的攻击。启用此选项可使 NetScreen 设备丢弃在标志字段中同时设置 SYN 和 FIN 位的封包。
- **TCP Packet Without Flag（无标记的 TCP 封包）**：通常，在发送的 TCP 封包的标志字段中至少会有一位被置位。此选项将使 NetScreen 设备丢弃字段标志缺少或不全的 TCP 封包。

- **FIN Bit With No ACK Bit（有 FIN 位无 ACK 位）：**设置了 FIN 标志的 TCP 封包通常也会设置 ACK 位。此选项将使 NetScreen 设备丢弃在标志字段中设置了 FIN 标志，但没有设置 ACK 位的封包。
- **ICMP Fragment（ICMP 碎片）：**检测任何设置了“更多片断”标志，或在偏移字段中指出了偏移值的 ICMP 帧。
- **Ping of Death：**TCP/IP 规范要求用于数据包报传输的封包必须具有特定的大小。许多 ping 实现允许用户根据需要指定更大的封包大小。过大的 ICMP 封包会引发一系列负面的系统反应，如拒绝服务 (DoS)、系统崩溃、死机以及重新启动。如果允许 NetScreen 设备执行此操作，它可以检测并拒绝此类过大且不规则的封包。
- **Address Sweep Attack（地址扫描攻击）：**与端口扫描攻击类似，当一个源 IP 地址在定义的时间间隔（缺省值为 5,000 微秒）内向不同的主机发送 ICMP 响应要求（或 ping）时，就会发生地址扫描攻击。这个配置的目的是 Ping 数个主机，希望有一个会回复响应，以便找到可以作为目标的地址。NetScreen 设备在内部记录从一个远程源 ping 的不同地址的数目。使用缺省设置，如果某远程主机在 0.005 秒（5,000 微秒）内 ping 了 10 个地址，NetScreen 会将这一情况标记为地址扫描攻击，并在该秒余下的时间内拒绝来自于该主机的 ICMP 回应要求。
- **Large ICMP Packet（大的 ICMP 封包）：**NetScreen 设备丢弃长度大于 1024 的 ICMP 封包。
- **Tear Drop Attack（撕毁攻击）：**撕毁攻击利用了 IP 封包碎片的重新组合。在 IP 包头中，选项之一为偏移值。当一个封包碎片的偏移值与大小之和不同于下一封包碎片时，封包发生重叠，并且服务器尝试重新组合封包时会引起系统崩溃。如果 NetScreen 在某封包碎片中发现了这种不一致现象，将会丢弃该碎片。
- **Filter IP Source Route Option（过滤 IP 源路由选项）：**IP 包头信息有一个选项，其中所含的路由信息可指定与包头源路由不同的源路由。启用此选项可封锁所有使用“源路由选项”的 IP 信息流。“源路由选项”可允许攻击者以假的 IP 地址进入网络，并将数据送回到其真正的地址。
- **Record Route Option（记录路由选项）：**NetScreen 设备封锁 IP 选项为 7（记录路由）的封包。此选项用于记录封包的路由。记录的路由由一系列互联网地址组成，外来者经过分析可以了解到您的网络的编址方案及拓扑结构方面的详细信息。

- **IP Security Option（IP 安全性选项）**：此选项为主机提供了一种手段，可发送与 DOD 要求兼容的安全性、分隔、TCC（非公开用户组）参数以及“处理限制代码”。
- **IP Strict Source Route Option（IP 严格源路由选项）**：NetScreen 设备封锁 IP 选项为 9（严格源路由选择）的封包。此选项为封包源提供了一种手段，可在向目标转发封包时提供网关所要使用的路由信息。此选项为严格源路由，因为网关或主机 IP 必须将数据包报直接发送到源路由中的下一地址，并且只能通过下一地址中指示的直接连接的网络才能到达路由中指定的下一网关或主机。
- **Unknown Protocol（未知协议）**：NetScreen 设备丢弃协议字段设置为 101 或更大值的封包。目前，这些协议类型被保留，尚未定义。
- **IP Spoofing（IP 欺骗）**：当攻击者试图通过假冒有效的客户端 IP 地址来绕过防火墙保护时，就发生了欺骗攻击。如果启用了 IP 欺骗防御机制，NetScreen 设备会用自己的路由表对 IP 地址进行分析，来抵御这种攻击。如果 IP 地址不在路由表中，则不允许来自该源的信息流通过 NetScreen 设备进行通信，并且会丢弃来自该源的所有封包。

  在 CLI 中，您可以指示 NetScreen 设备丢弃没有包含源路由或包含已保留源 IP 地址（不可路由的，例如 127.0.0.1）的封包：**set zone** *zone* **screen ip-spoofing drop-no-rpf-route**。
- **Bad IP Option（坏的 IP 选项）**：当 IP 数据包包头中的 IP 选项列表不完整或残缺时，会触发此选项。
- **IP Timestamp Option（IP 时戳选项）**：NetScreen 设备封锁 IP 选项列表中包括选项 4（互联网时戳）的封包。
- **Loose Source Route Option**：NetScreen 设备封锁 IP 选项为 3（松散源路由）的封包。此选项为封包源提供了一种手段，可在向目标转发封包时提供网关所要使用的路由信息。此选项是松散源路由，因为允许网关或主机 IP 使用任何数量的其它中间网关的任何路由来到达路由中的下一地址。
- **IP Stream Option（IP 流选项）**：NetScreen 设备封锁 IP 选项为 8（流 ID）的封包。此选项提供了一种方法，用于在不支持流概念的网络中输送 16 位 SATNET 流标识符。

- **WinNuke Attack（WinNuke 攻击）：**WinNuke 是一种常见的应用程序，其唯一目的就是使互联网上任何运行 Windows 的计算机崩溃。WinNuke 通过已建立的连接向主机发送带外 (OOB) 数据 — 通常发送到 NetBIOS 端口 139— 并引起 NetBIOS 碎片重叠，以此来使多台机器崩溃。重新启动后，会显示下列信息，指示攻击已经发生：

  An exception OE has occurred at 0028:[address] in VxD MSTCP(01) + 000041AE. This was called from 0028:[address] in VxD NDIS(01) + 00008660. It may be possible to continue normally.（00008660。有可能继续正常运行。）

  Press any key to attempt to continue.（请按任意键尝试继续运行。）

  Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.（按 CTRL+ALT+DEL 可尝试继续运行。将丢失所有应用程序中的未保存信息。）

  Press any key to continue.（按任意键继续。）

  如果启用了 WinNuke 攻击防御机制，NetScreen 设备会扫描所有进入的“Microsoft NetBIOS 会话服务”（端口 139）封包。如果 NetScreen 设备发现某个封包上设置了 TCP URG 代码位，就会检查偏移值、删除碎片重叠并根据需要纠正偏移值以防止发生 OOB 错误。然后让经过修正的封包通过，并在“事件警报”日志中创建一个 WinNuke 攻击日志条目。

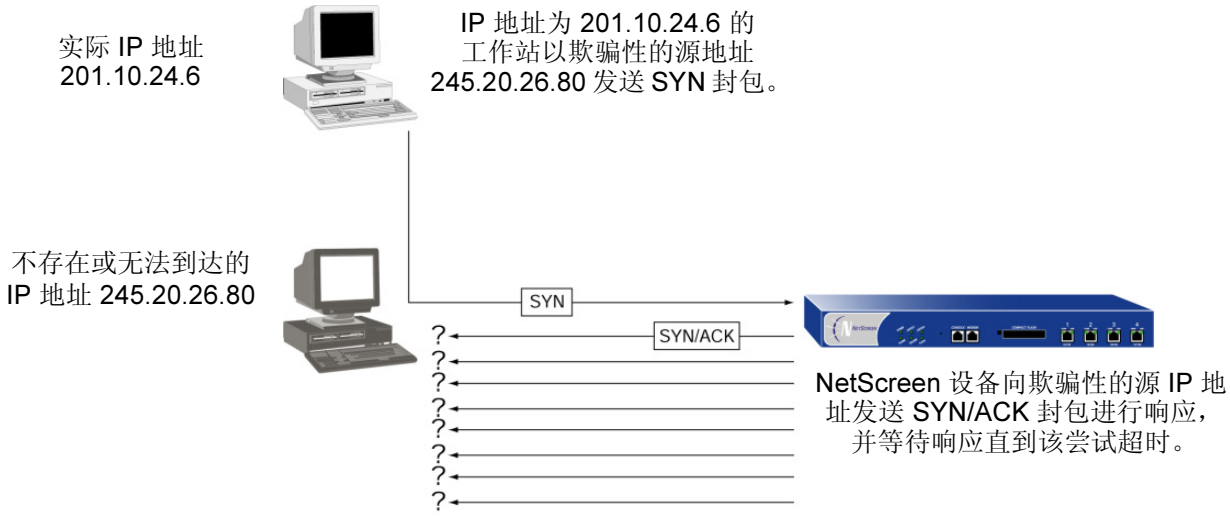
- **Land Attack：**“陆地”攻击将 SYN 攻击和 IP 欺骗结合在了一起，当攻击者发送含有受害方 IP 地址的欺骗性 SYN 封包，将其作为目的和源 IP 地址时，就发生了陆地攻击。接收系统通过向自己发送 SYN-ACK 封包来进行响应，同时创建一个空的连接，该连接将会一直保持到达到空闲超时值为止。向系统堆积过多的这种空连接会耗尽系统资源，导致 DoS。通过将 SYN 泛滥防御机制和 IP 欺骗保护措施结合在一起，NetScreen 设备将会封锁任何此类性质的企图。

- **Malicious URL Protection**：当启用“恶意 URL 检测”时，NetScreen 设备会监视每个 HTTP 封包并检测与若干用户定义模式中的任意一个相匹配的任何封包。设备会自动丢弃所有此类封包。
- **Block Java/ActiveX/ZIP/EXE Component**：Web 网页中可能藏有恶意的 Java 或 ActiveX 组件。下载完以后，这些 applet 会在您的计算机上安装特洛伊木马病毒。同样，特洛伊木马病毒[2]也可以隐藏在压缩文件（如 .zip）和可执行（.exe）文件中。在安全区中启用这些组件的阻塞时，NetScreen 设备会检查每个到达绑定到该区域的接口的 HTTP 包头。会检查包头中列出的内容类型是否指示封包负荷中有任何目的组件。如果内容类型为 ActiveX、Java、.exe 或 .zip，而且您将 NetScreen 设备配置为阻塞这些组件，NetScreen 设备会阻塞封包。如果内容类型仅列出“八位位组流”，而不是特定的组件类型，则 NetScreen 设备会检查负荷中的文件类型。如果文件类型为 ActiveX、Java、.exe 或 .zip，而且您将 NetScreen 设备配置为阻塞这些组件，NetScreen 设备会阻塞封包。
- **Deny Fragment**：封包通过不同的网络时，有时必须根据网络的最大传输单位 (MTU) 将封包分成更小的部分（片断）。攻击者可能会利用 IP 栈具体实现的封包重新组合代码中的漏洞，通过 IP 碎片进行攻击。当目标系统收到这些封包时，造成的结果小到无法正确处理封包，大到使整个系统崩溃。如果允许 NetScreen 设备拒绝安全区段上的 IP 碎片，设备将封锁在绑定到该区段的接口处接收到的所有 IP 封包碎片。

2. 特洛伊木马病毒是一种程序，如果被秘密安装在某台计算机上，外来者就可以直接控制这台计算机。

范例：SYN 泛滥攻击

利用三方封包交换，即常说的三方握手，建立一个 TCP 连接：A 向 B 发送 SYN 封包； B 用 SYN/ACK 封包进行响应；然后 A 又用 ACK 封包进行响应。SYN 泛滥攻击用含有伪造的（“欺骗”）IP 源地址（不存在或不可到达的地址）的 SYN 封包塞满某一站点。防火墙用 SYN/ACK 封包对这些地址进行响应，然后等待响应的 ACK 封包。因为 SYN/ACK 封包被发送到不存在或不可到达的 IP 地址，所以它们不会得到响应并最终超时。

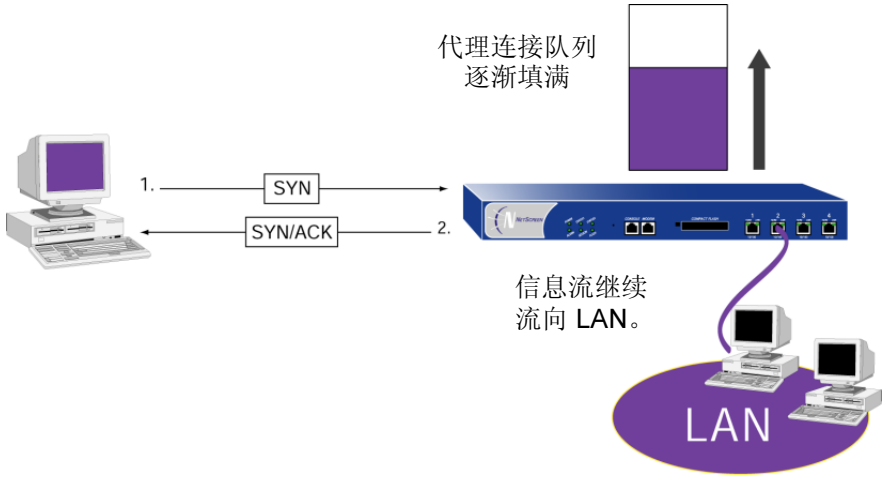


通过向服务器或主机堆积无法完成的连接，攻击者最终会填满主机的内存缓冲区。一旦缓冲区被填满，就无法继续进行连接，并且可能破坏主机的操作系统。无论哪种结果，攻击已使主机失去作用，无法进行正常的操作。SYN 泛滥攻击是典型的拒绝服务 (DoS) 式攻击。

SYN 泛滥攻击保护

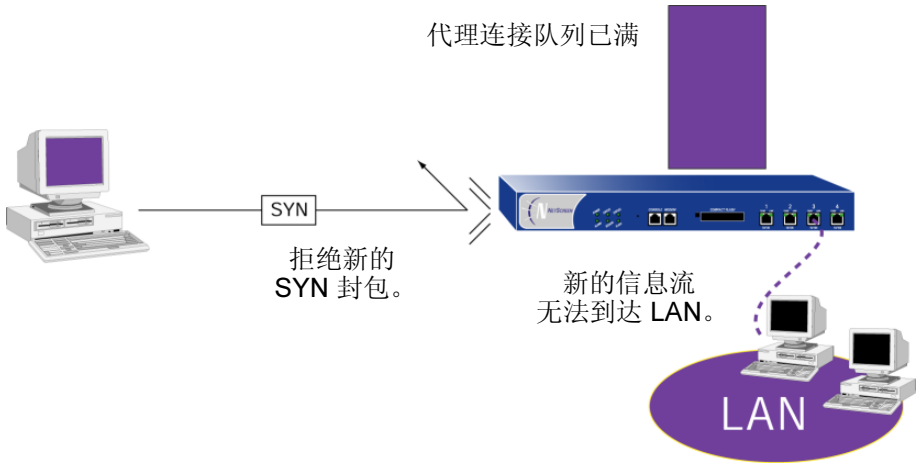
NetScreen 设备可以对每秒钟允许通过防火墙的 SYN 封包数加以限制。当达到该临界值时， NetScreen 设备开始代理进入的 SYN 封包，为主机发送 SYN/ACK 响应并将未完成的连接存储在连接队列中。[3] 未完成的连接保留在队列中，直到连接完成或请求超时。

在下面的示意图中，已超过了 SYN 临界值， NetScreen 设备已经开始代理 SYN 封包。



3. 因为 NetScreen-1000 代理所有进入的 SYN 封包，所以不需要设置临界值。

在下一个示意图中，代理连接队列已完全填满，因而拒绝新来的 SYN 封包。



下列操作尝试护卫受保护网络中的主机，使其免遭不完整三方握手的轰击。

注意：*代理超过设定临界值的不完整 SYN 连接的过程只适用于现有策略允许的信息流。没有相关策略的信息流将被自动丢弃。*

WebUI：启用 SYN 泛滥攻击保护

Network > Zones > Edit（对于要抵御攻击的区段）> SCREEN：输入以下设置，然后单击 **Apply**：

Deny SYN Attack: 选择

SYN Attack Threshold: 20,000/Sec .

注意：*通过 WebUI，您可以设置 NetScreen 设备开始代理会话时的攻击临界值。通过 CLI，您还可以设置队列长度、超时值以及警报临界值。*

CLI：启用 SYN 泛滥攻击保护并定义参数

1. 启用 SYN 泛滥攻击保护。

   ns-> **set zone** *zone* **screen syn-flood**

   您可以设置下列参数来代理未完成的 SYN 连接：

2. **Attack Threshold （攻击临界值）**：激活 SYN 代理机制所需的每秒钟的 SYN 封包数。虽然可以将该临界值设置为任意值，但您需要了解站点通常的流量模式，以便为其设置适当的临界值。例如，如果是一个通常每秒会收到 20,000 个 SYN 封包的电子商务站点，可将该临界值设为 30,000/ 秒。如果是一个通常每秒会收到 20 个 SYN 封包的小站点，则可将该临界值设为 40。

   ns-> **set zone** *zone* **screen syn-flood attack-threshold** *number*

3. **Queue size （队列长度）**：系统开始拒绝新的连接请求前，代理连接队列中的代理连接请求的数量。队列长度值越大，NetScreen 设备就需要更长的时间来扫描该队列，以找到与代理连接请求匹配的有效 ACK 响应。这会略微减慢初始连接的建立；但是，由于开始数据传输的时间往往远远大于建立初始连接时较小的延迟时间，所以用户不会注意到有任何明显的不同。

   ns-> **set zone** *zone* **screen syn-flood queue-size** *number*

4. **Timeout （超时）**：丢弃队列中完成一半的连接之前的最长时间。缺省值为 20 秒，您可以将该超时值设置为 0–50 秒。您可以试着缩短超时值，直到发现在正常的流量条件下开始有连接被丢弃。二十 (20) 秒对于三方握手 ACK 响应而言，是一个十分保守的超时值。

   ns-> **set zone** *zone* **screen syn-flood timeout** *number*

5. **Alarm Threshold（警报临界值）：**每秒钟代理的半完成连接数，此时会在“事件警报”日志中加入一条警报。为警报临界值设置的值，当每秒钟代理的半完成连接数超过该值时，就会触发警报。例如，如果 SYN 临界值设为每秒 2000 个 SYN 封包且警报值为 1000，则每秒钟的 SYN 封包总数必需达到 3001 时，才会触发警报并将其写入日志。更确切地来说：

   1. 每秒钟内满足策略要求的前 2000 个 SYN 封包可通过防火墙。
   2. 在同一秒内，防火墙代理后面的 1000 个 SYN 封包。
   3. 第 1001 个代理连接（或该秒内的第 3001 个连接请求）会触发警报。

   如果攻击继续，则“事件警报”日志每秒钟产生一个攻击警报直到攻击停止且队列被清空。

   ns-> **set zone** *zone* **screen syn-flood alarm-threshold** *number*

6. **Source Threshold（源临界值）：**当从同一源 IP 地址发送大量封包或将其发送到同一目的 IP 地址时，就可能发生 DoS 攻击。此选项允许您指定在 NetScreen 设备执行 SYN 代理机制前，从单个源 IP 地址收到的 SYN 封包数。（缺省临界值为每个源 IP 地址每秒 4000 个 SYN 封包。）

   ns-> **set zone** *zone* **screen syn-flood source-threshold** *number*

7. **Destination Threshold（目的临界值）：**当从同一源 IP 地址发送大量封包或将其发送到同一目的 IP 地址时，就可能会发生 DoS 攻击。此选项允许您指定在 NetScreen 设备执行 SYN 代理机制前，从单个目的 IP 地址收到的 SYN 封包数。（缺省临界值为每个目的 IP 地址每秒 4000 个 SYN 封包。）

   ns-> **set zone** *zone* **screen syn-flood destination-threshold** *number*

8. **Drop Unknown MAC（丢弃未知的 MAC）：**当 NetScreen 设备检测到 SYN 攻击时，它会代理所有的 TCP 连接请求。但是，如果目的 MAC 地址不在其 MAC 获知表中，则处于透明模式的 NetScreen 设备不能代理 TCP 连接请求。缺省情况下，检测到 SYN 攻击且处于透明模式的 NetScreen 设备将允许含有未知 MAC 地址的 SYN 封包通过。您可以使用此选项指示设备丢弃含有未知目的 MAC 地址的 SYN 封包，而不是让其通过。

   ns-> **set zone** *zone* **screen syn-flood drop-unknown-mac**

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。通道区段与安全区段相关联，后者充当前者的承载方。 NetScreen 设备使用路由信息来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[4]。

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

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

配置安全区段和通道区段

Layer 3 （第 3 层）或 Layer 2 （第 2 层）安全区段及通道区段的创建、修改和删除十分相似。

注意：*您不能删除预定义的安全区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 Layer 3 （第 3 层）或 Layer 2 （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[5]。

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

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

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

CLI

set zone name *zone* [l2 *vlan_id_num*[6] | tunnel *sec_zone*]

set zone *zone* block

set zone *zone* vrouter *name_str*

5. Layer 2 （第 2 层）安全区段的名称必须以 “L2-” 开头；例如，“L2-Corp” 或 “L2-Xnet”。
6. 创建 Layer 2 （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[7]，然后再以修改值重新创建它。您可以更改现有区段上的区段内部封锁选项和虚拟路由器[8]。

WebUI

修改区段名称

1. 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）。
2. 当出现提示，请求对删除操作进行确认时，单击 **Yes**。
3. Network > Zones > New：输入更改后的区段设置，然后单击 **OK**。

更改区段内部封锁选项或虚拟路由器

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

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

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

CLI

修改区段名称

1. unset zone *zone*
2. set zone name *zone* [l2 *vlan_id_num* | tunnel *sec_zone*]

7. 删除区段前，必须先解除所有绑定到它的接口。
8. 更改区段的虚拟路由器之前，必须先删除绑定到该区段的所有接口。

更改区段内部封锁选项或虚拟路由器

{ set | unset } zone *zone* block

set zone *zone* vrouter *name_str*

删除区段

要删除安全区段或通道区段，执行以下任一操作[9]：

WebUI

1. Network > Zones：单击 **Remove**（对于要删除的区段）。
2. 当出现提示，请求对删除操作进行确认时，单击 **Yes**。

CLI

unset zone *zone*

9. 删除区段前，必须先解除所有绑定到它的接口。要解除接口与区段间的绑定，请参阅第 89 页上的 “将接口绑定到安全区段”。

功能区段

共有四个功能区段，分别是 Null、 MGT、 HA 和 Self。每个区段的存在都有其专门的目的，如下所示。

注意：*尽管可以为 MGT 和 HA 区段设置接口，但是这些区段本身是不可配置的。*

Null 区段

此区段用于临时存储没有绑定到任何其它区段的接口。

MGT 区段

此区段是带外管理接口 MGT 的宿主区段。

HA 区段

此区段是高可用性接口 HA1 和 HA2 的宿主区段。

Self 区段

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

3

路由和虚拟路由器

路由选择是将 IP 信息流从一个位置转到另一位置的过程。路由器是在 OSI 模型的网络层（Layer 3（第 3 层））上工作的网络设备。虚拟路由器是执行路由选择功能的 ScreenOS 组件。本章介绍路由选择的基本概念并概述 NetScreen 如何将路由选择技术集成到其产品中。

本章包括以下各节：

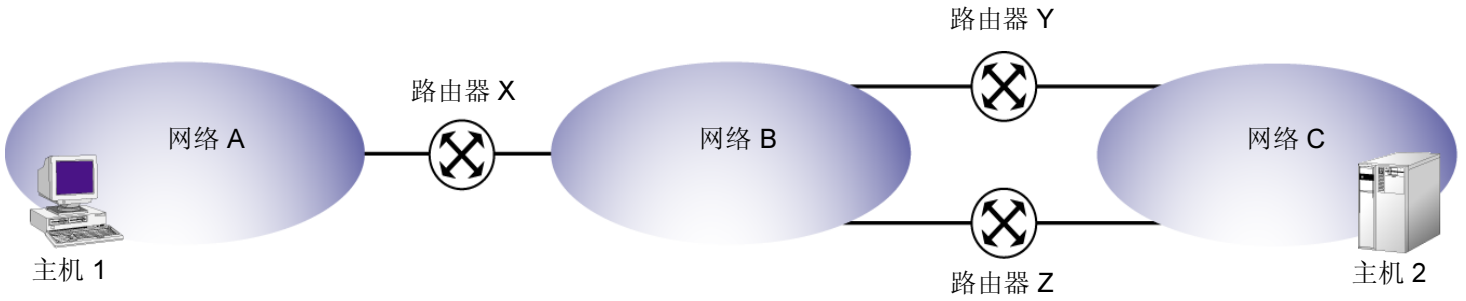
路由选择过程

当某一主机向位于不同网络的另一台主机发送封包时，每个封包包头都含有目的主机的地址。当路由器收到封包时，会将该目的地址与其路由表中的所有地址进行比较。路由器在其路由表中找到匹配的地址后，它会确定将封包路由至何处。

有静态和动态两种路由选择类型。当网络采用静态路由选择时，网络管理员必须手动配置路由并维护路由表。对于大型网络，在路由表中手动配置和维护路由是不切实际的。动态路由选择协议允许路由器在本地网络拓扑结构改变时，或在邻接路由器通告远处网络发生变化时，自动更新它们的路由表。

下面的示意图展示了一个采用静态路由选择的网络。为了便于说明，假设主机 1 要将信息发送到主机 2，因而创建了在包头中包含下列信息的封包：

源 IP 地址 / 网络掩码	**目的 IP 地址 / 网络掩码**	携带的数据
主机 1/ 网络 A	主机 2/ 网络 C	



路由表

路由器 X

网络	网关	度量
网 A	已连接	0
网 B	已连接	0
网 C	路由器 Y	1

路由器 Y

网络	网关	度量
网 A	路由器 X	1
网 B	已连接	0
网 C	已连接	0

路由器 Z

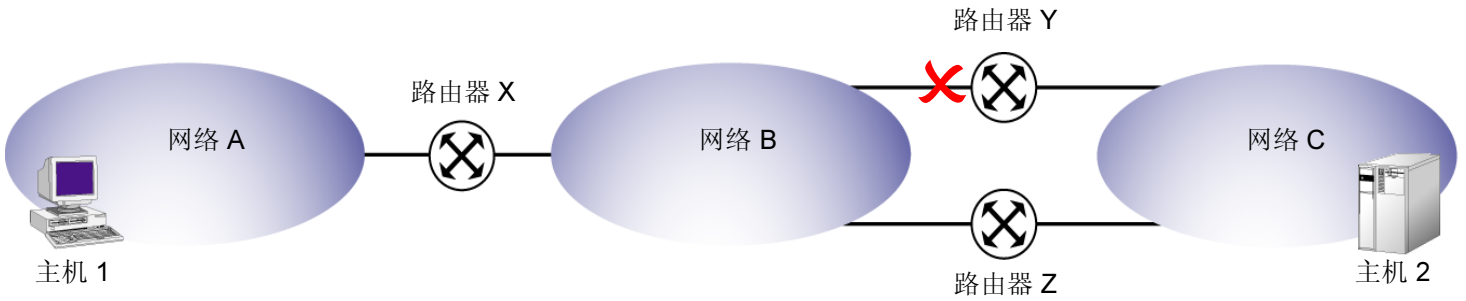
网络	网关	度量
网 A	路由器 X	1
网 B	已连接	0
网 C	已连接	0

在上例中，路由器 X 具有一个为网络 C 配置的静态路由，表明网关 （下一跳跃）为路由器 Y。当路由器 X 收到发往网络 C 中的主机 2 的封包时，会将封包中的目的地址与其路由表进行比较，并且会发现表中的最后一条路由条目是完全匹配的。最后一条路由条目指定将发往网络 C 的信息流发送到路由器 Y 进行传送。

路由器 Y 接收封包，而且由于它知道网络 C 是直接连接的，所以它会通过连接到该网络的接口来发送封包。请注意，如果路由器 Y 发生故障，或者路由器 Y 与网络 C 的链接不可用，则封包将无法到达主机 2。虽然还有一条通过路由器 Z 到达网络 C 的路由，但是该路由尚未静态配置，所以路由器 X 并不知道这条备用路由。

下面的示意图展示了一个采用动态路由选择的网络。为了便于说明，假设主机 1 要将信息发送到主机 2，因而创建了在包头中包含下列信息的封包：

源 IP 地址 / 网络掩码	**目的 IP 地址 / 网络掩码**	携带的数据
主机 1/ 网络 A	主机 2/ 网络 C	



路由表

路由器 X

网络	网关	度量
网 A	已连接	0
网 B	已连接	0
网 C	路由器 Y	1
网 C	路由器 Z	无穷大

路由器 Y

网络	网关	度量
网 A	路由器 X	1
网 B	已连接	0
网 C	已连接	0
网 C	路由器 Z	无穷大

路由器 Z

网络	网关	度量
网 A	路由器 X	1
网 B	已连接	0
网 C	已连接	无穷大
网 C	路由器 Y	1

在上例中，所有路由器都采用动态路由选择协议，因而，有关直接连接网络的所有路由选择信息会分发到所有的路由器中。

当路由器 X 收到封包时，会将封包中的目的地址与其路由表进行比较，并且会发现两条可能的路由。一条路由经过路由器 Y，另一条路由经过路由器 Z。因为经过路由器 Y 到网络 C 的路由断开，所以经过路由器 Z 的路由具有最小度量。因而，路由器 X 会将封包发送到路由器 Z。

当路由器 Z 收到封包时，会将封包中的目的地址与其路由表进行比较，并且会发现网络 C 是直接连接的，因此它会通过连接到该网络的接口来发送封包。

与上例不同的是，如果不存在经过路由器 Z 的路由且发往网络 C 的封包被发送到路由器 Y，则路由器 Y 会产生一条 ICMP 信息，指示目标不可到达，并将此信息发送到源路由器。

路由表

路由器通常会连接到多个网络 （至少两个），它们主要负责引导信息流通过这些网络。每个路由器都维护着一个路由表，该表是已知网络以及如何到达这些网络的指令的列表。路由表中的每一条目称为*路由条目*或*路由*。路由表包含下列信息：

- 所有直接连接的网络的记录
- 所有静态配置和动态获知的网络的记录
- 每个列出网络的下一跳跃 （网关）的记录
- 到达每一获知网络的距离的记录
- 相对于其它路由优先选择使用某一路由的记录

路由选择协议

可以通过逐个手动配置各路由条目的方式来静态配置路由器。也可以将路由器配置为使用诸如 OSPF 或 BGP 等路由选择协议，从邻接路由器中动态获取路由。虽然静态路由选择最好控制，但它没有动态路由选择灵活。使用静态路由选择，网络拓扑的任何变化（例如，某一接口变得不可操作）通常都需要网络管理员进行干预。使用动态路由选择，每当网络拓扑发生变化时，路由器可以自动更新其路由表，无需网络管理员帮助。

路由度量

对于同一网络，路由器常常具有多个路由条目。路由度量有助于确定封包到达给定目标可采取的最佳路径。路由器使用路由度量来权衡到达同一目标的两个路由，并确定选择使用哪个路由。路由度量可以根据封包到达目标必须经过的路由器数量、路径的相对速度和带宽、组成该路径的链接成本得出，也可以将这些因素（和其它因素）综合在一起来确定。

当到同一目的网络有多个路由时，度量最小的路由优先。如果路由是动态获知的，则由路由始发的邻接路由器提供度量。对于手动配置的静态路由，网络管理员可以指定度量，这样就可以对优先选择哪些路由进行更多控制。

路由优选级

路由器常常被配置为同时使用两个或多个动态路由选择协议，路由器将通过这些协议来获知去往同一目标的两个或多个路由，所以如果通过不同方法（如 OSPF 和静态，或 OSPF 和 BGP 等）获知的两个路由具有相同的度量，就需要一种方法来解决这种僵局。路由优选级可以解决这一难题。将优选级和度量结合起来就可以确定出在多个路由中应该优先选择哪一个。有关详细信息，请参阅第 80 页上的 “设置路由优选级”。

CLI 中的环境相关命令

可以使用“NetScreen Web 用户界面”(WebUI) 或“NetScreen 命令行界面”(CLI) 来配置虚拟路由器。本节将解释说明与虚拟路由器配置有关的 CLI 命令树中的元素。

有关使用 CLI 的详细信息，请参阅 *NetScreen CLI Reference Guide*。

命令的级别

在 NetScreen CLI 中，您可以从命令树的两个不同级别来执行命令和配置路由选择参数。可从下列两个级别发出命令：

- 根级，使用*显式*命令
- 环境级，使用*相对*命令

在根级执行命令

当系统提示符变为相应的设备主机名 （如 “ns200->”）时，您就处于根级。在根级键入命令仅仅表示您要发出整个命令行，包括所有必要的关键字和变量。

要在根级键入命令并执行它，必须提供所有必要的关键字和变量。如果漏掉命令中必需的关键字或变量， NetScreen 设备将无法理解该命令，会提示您输入更多的信息。例如，若想成功配置一个区域为 10 且采用剩余区域类型的 OSPF 区域，必须完整地键入以下命令：

```
ns-> set vrouter trust-vr protocol ospf area 10 stub
```

在环境级执行命令

环境是命令中的特定级别或层。进入某级别后，您就可以配置或查看和该级别相关的各种设置。例如，您可以进入虚拟路由器的环境，例如 trust-vr 或 untrust-vr 的环境。在该虚拟路由器的环境中，您就可以进入路由选择协议的环境—OSPF 或 BGP。

虚拟路由器环境

可以通过在根级提示符下键入下列命令来进入虚拟路由器环境：

```
ns-> set vrouter vrouter
```

例如：

```
ns-> set vrouter trust-vr
ns(trust-vr)->
```

第一行对应于提示符 (ns->)，后跟命令 (**set vrouter trust-vr**)。第二行是命令的执行结果，表明您已进入了虚拟路由器环境 （在此例中，为 trust-vr 虚拟路由器环境）。请注意，在第二行中，除原有提示符外，还显示有虚拟路由器的名称。因此，通过观看提示符就可以确定当前所处的环境。

路由选择协议环境

在虚拟路由器环境中输入以下命令可以进入路由选择协议环境：

```
ns(trust-vr)-> set protocol {OSPF | BGP}
```

例如：

```
ns(trust-vr)-> set protocol ospf
ns(trust-vr/ospf)->
```

第一行对应于虚拟路由器环境 (ns(trust-vr)->)，后跟命令 **set protocol ospf**。第二行表明您已进入了路由选择协议环境 (OSPF)。

一旦进入路由选择协议环境，就可以输入专用于该协议的命令。这种方法最大的好处就是方便。例如，请比较下面的命令行：第一行是根级提示符下的显式命令行，第二行是路由选择协议环境下的相对命令行。

命令行 1（提示符下的显示命令）：

```
ns-> set vrouter trust-vr protocol ospf area 10 stub
```

命令行 2（相对于路由选择协议环境）：

```
ns(trust-vr/ospf)-> set area 10 stub
```

命令行 2 只需键入较少的字符，因而更省力。

在某一环境下键入命令的好处有：

- 环境可以减少需要记忆的参数。
- 环境减小了出错的可能性。
- 环境可以使您在输入信息时不必记住路由选择类型或虚拟路由器名称。

NETSCREEN 设备上的虚拟路由器

ScreenOS 可以将其路由选择组件分成两个或多个虚拟路由器。这样做，您可以采纳重叠的 IP 地址空间，而且可以控制对任何给定路由选择域中的其他人可见的信息。

可以将多个安全区段绑定到一个虚拟路由器上，但是某一安全区段只能绑定到一个虚拟路由器上。将某一区段绑定到某一虚拟路由器后，该区段中的所有接口都属于该虚拟路由器。除支持静态路由选择外，虚拟路由器还支持动态路由选择协议，如 OSPF 和 BGP，可以在一个路由选择实例中同时启用这些协议。虚拟路由器可以将它的路由综合并重新分配到另一个路由器中，而且它还可以将另一虚拟路由器作为下一跳跃，或者甚至作为其缺省网关。

为使某一虚拟路由选择域中的任一设备都能与另一虚拟路由选择域中的设备进行通信，必须在这两个虚拟路由器之间定义一个路由。

配置虚拟路由器

通过将路由选择信息分给两个或多个虚拟路由器，您可以控制对任何给定路由选择域中的其他人可见的信息。例如，可以将企业网内部所有安全区段的路由选择信息保留在预定义的虚拟路由器 trust-vr 中，而将企业网外部所有区段的路由选择信息保留在另一预定义的虚拟路由器 untrust-vr 中。由于虚拟路由器路由表中的信息对于其它路由器是不可见的，所以您可以将内部网的路由选择信息与公司外部的不可信源分离开来。

某些 NetScreen 设备[1] 允许您除了使用两个预定义的虚拟路由器外，还可以创建自定义虚拟路由器。您可以对用户定义虚拟路由器的所有方面进行修改。对于预定义的 trust-vr 和 untrust-vr，您可修改虚拟路由器 ID、最大路由条目、路由优选级值，以及 （仅对于 trust-vr） — 启用或禁用为路由模式下配置的接口自动向 untrust-vr 导出路由。

1. 只有 NetScreen 系统 （NetScreen-500、 -1000、 -5200、 -5400）支持自定义虚拟路由器。要创建自定义虚拟路由器，需要有 VSYS 软件密钥。

要修改用户定义虚拟路由器的名称或更改虚拟路由器 ID，必须先删除该虚拟路由器，然后用新的名称或虚拟路由器 ID 重新创建它。

您可以将安全区段绑定的虚拟路由器由一个改为另一个。但是，必须先移除该区段的所有接口。（有关将接口绑定到安全区段以及解除绑定方面的详细信息，请参阅第 2 卷，“基本原理”中的 “接口”一章。）

不能删除预定义的 untrust-vr 和 trust-vr 虚拟路由器，但是可以删除任何用户定义的虚拟路由器。

您可以设置虚拟路由器可在其路由表中存储的最大路由数。此功能有助于管理虚拟路由器的性能，尤其是对于大型网域，在这种网域中，其它虚拟路由器可能会导出大量的路由。

范例：创建自定义虚拟路由器

在本例中，您将创建一个名为 trust2-vr 的自定义虚拟路由器，其最大路由条目值为 10，并且启用了向 untrust-vr 自动导出路由。

WebUI

Network > Routing > Virtual Routers > New：输入以下内容，然后单击 **OK**：

Virtual Router Name: trust2-vr

Maximum Route Entry:

Set limit at: （选择）, 10

Auto Export Route to Untrust-VR: （选择）

Use system default: （选择）

CLI

1. ns-> set vrouter trust2-vr
2. set max-routes 10
3. ns(trust2-vr)-> set auto-route-export
4. ns(trust2-vr)-> save

范例：修改虚拟路由器

在本例中，将 trust-vr 的最大路由条目值修改为 20。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）：输入以下内容，然后单击 **OK**：

Maximum Route Entry:

Set limit at: （选择）, 20

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set max-routes 20
3. ns(trust-vr)-> save

范例：将虚拟路由器绑定到区段

在本例中，您要将一个名为 “Xnet” 的用户定义区段绑定到 untrust-vr。

WebUI

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

CLI

1. set zone Xnet vrouter untrust-vr
2. save

范例：移除虚拟路由器

在本例中，您要删除一个名为 “trust2-vr”的现有用户定义虚拟路由器。

WebUI

1. Network > Routing > Virtual Routers：对于 trust2-vr，单击 **Remove** 。
2. 当出现提示，请求您确认删除操作时，单击 **OK**。

CLI

1. unset vrouter trust2-vr
2. 当出现提示，请求您确认删除操作时 (vrouter unset, are you sure? y/[n])，键入 Y。
3. save

路由表

为帮助确定路径，采用了路由选择算法来初始化并维护路由表。路由表是包含有关路由的主要路由选择信息的对象。当同一目标存在多个路由时，路由器通过比较度量来确定最优路由。这些度量根据网络的设计和使用的路由选择协议而有所不同。

可以静态或动态方式建立路由表。对于小型网络，由网络管理员手动构建路由表通常更为有效。对于大型网络，采用动态路由选择协议在成员网络之间交换信息以计算出最佳路由，同时以动态方式建立和维护路由表。

路由表配置

路由表提供的信息可帮助虚拟路由器将信息流导向不同的接口[2] 和子网。在下列情况下，您需要定义静态路由：

- 如果 Trust 区段接口或用户定义接口所在的子网具有多个引向其它子网的路由器，您必须定义静态路由，指定在转发去往那些子网的信息流时使用哪个路由器。
- 如果 Untrust 区段接口所在的子网具有多个引向多个互联网连接的路由器，您必须定义静态路由，指定向特定的 ISP 转发信息流时使用哪个路由器。

2. 当为 NAT 或路由模式的接口设置 IP 地址时，路由表会自动创建到邻接子网的静态路由以使信息流可以通过该接口。

- 您必须定义静态路由，指引始于设备自身的管理信息流 （相对于穿越防火墙的用户信息流）。例如，需要定义静态路由，将 syslog、 SNMP、 OneSecure 和 WebTrends 消息送往管理员地址。还必须定义路由，将认证请求发往 RADIUS、 SecurID 和 LDAP 服务器，并将 URL 检查信息发往 Websense 服务器。

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

- 当有多个外向接口时，对于出站 VPN 信息流，您需要设置路由来指引出站信息流通过所要接口到达外部路由器。
- 如果 trust-vr 路由选择域中的安全区段接口的运行模式为 NAT，且在该接口上配置了 MIP 或 VIP 以接收来自 untrust-vr 路由选择域中的信息源的内向信息流，则必须创建到 untrust-vr 中的 MIP 或 VIP 的路由，该路由指向 trust-vr 作为网关。

范例：配置路由表

在下面的例子中， NetScreen 设备用于保护一个多级网络，该设备运行在 NAT 模式下。本例既有本地管理又有远程管理 （通过 NetScreen-Global PRO）。 NetScreen 设备向本地管理员 （位于 Trust 区段中的某一网络）发送 SNMP 陷阱和 syslog 报告，并向远程管理员 （位于 Untrust 区段中的某一网络）发送 NetScreen-Global PRO 报告。该设备通过 DMZ 区段中的 SecurID 服务器来认证用户，通过 Trust 区段中的 Websense 服务器执行 URL 过滤。

trust-vr 和 untrust-vr 路由表中必须有指定目的网络地址和网络掩码，以及网关 IP 地址和接口[3] 的声明， NetScreen 设备将通过它们将信息流引向下列目标：

untrust-vr

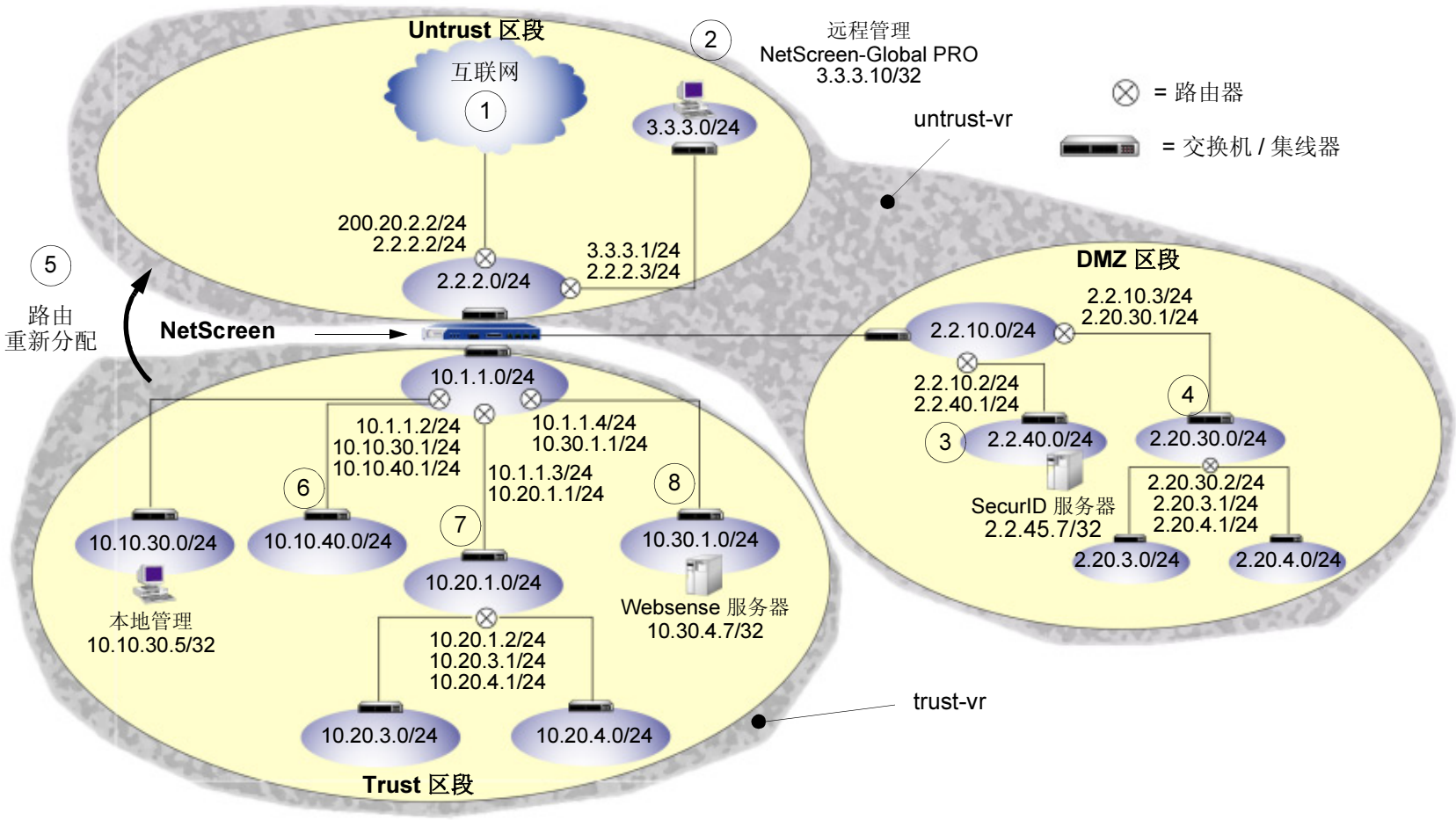
1. 到互联网的缺省网关
2. 3.3.3.0/24 子网中的远程管理员
3. DMZ 区段中的 2.2.40.0/24 子网
4. DMZ 区段中的 2.20.0.0/16 子网

trust-vr

5. 与未在 trust-vr 中找到的所有地址相对应的 untrust-vr
6. Trust 区段中的 10.10.0.0/16 子网
7. Trust 区段中的 10.20.0.0/16 子网
8. Trust 区段中的 10.30.1.0/24 子网

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

3. 对于每一路由表条目，还要有度量声明。此参数指定了路由的优先级；也就是说，当路由表中对于同一子网有多个路由条目时， NetScreen 设备将使用具有最小度量值的条目。输入接口、子接口以及通道接口地址时，会自动创建路由表条目，这些条目的度量值皆为 0，而用户定义路由的缺省度量值都是 1。


Untrust 区段
互联网
1
2
远程管理
NetScreen-Global PRO
3.3.3.10/32
= 路由器
= 交换机 / 集线器
untrust-vr
3.3.3.0/24
200.20.2.2/24
2.2.2.2/24
2.2.2.0/24
3.3.3.1/24
2.2.2.3/24
5
路由
重新分配
NetScreen
DMZ 区段
2.2.10.3/24
2.20.30.1/24
2.2.10.0/24
2.2.10.2/24
2.2.40.1/24
4
3
2.2.40.0/24
2.20.30.0/24
SecurID 服务器
2.2.45.7/32
2.20.30.2/24
2.20.3.1/24
2.20.4.1/24
2.20.3.0/24
2.20.4.0/24
10.1.1.0/24
10.1.1.2/24
10.10.30.1/24
10.10.40.1/24
10.1.1.4/24
10.30.1.1/24
10.1.1.3/24
10.20.1.1/24
6
7
8
10.10.30.0/24
10.10.40.0/24
10.20.1.0/24
10.30.1.0/24
本地管理
10.10.30.5/32
Websense 服务器
10.30.4.7/32
10.20.1.2/24
10.20.3.1/24
10.20.4.1/24
trust-vr
10.20.3.0/24
10.20.4.0/24
Trust 区段

WebUI

Untrust-VR

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3

   Gateway IP Address: 2.2.2.2

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

   Network Address/Netmask: 3.3.3.0/24

   Gateway: （选择）

   Interface: ethernet3

   Gateway IP Address: 2.2.2.3

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

   Network Address/Netmask: 2.2.40.0/24

   Gateway: （选择）

   Interface: ethernet2

   Gateway IP Address: 2.2.10.2

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

   Network Address/Netmask: 2.20.0.0/16

   Gateway: （选择）

   Interface: ethernet2

   Gateway IP Address: 2.2.10.3

Trust-VR

5. Network > Routing > Routing Table > 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
6. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
   Network Address/Netmask: 10.10.0.0/16
   Gateway: （选择）
   Interface: ethernet1
   Gateway IP Address: 10.1.1.2
7. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
   Network Address/Netmask: 10.20.0.0/16
   Gateway: （选择）
   Interface: ethernet1
   Gateway IP Address: 10.1.1.3
8. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
   Network Address/Netmask: 10.30.1.0/32
   Gateway: （选择）
   Interface: ethernet1
   Gateway IP Address: 10.1.1.4

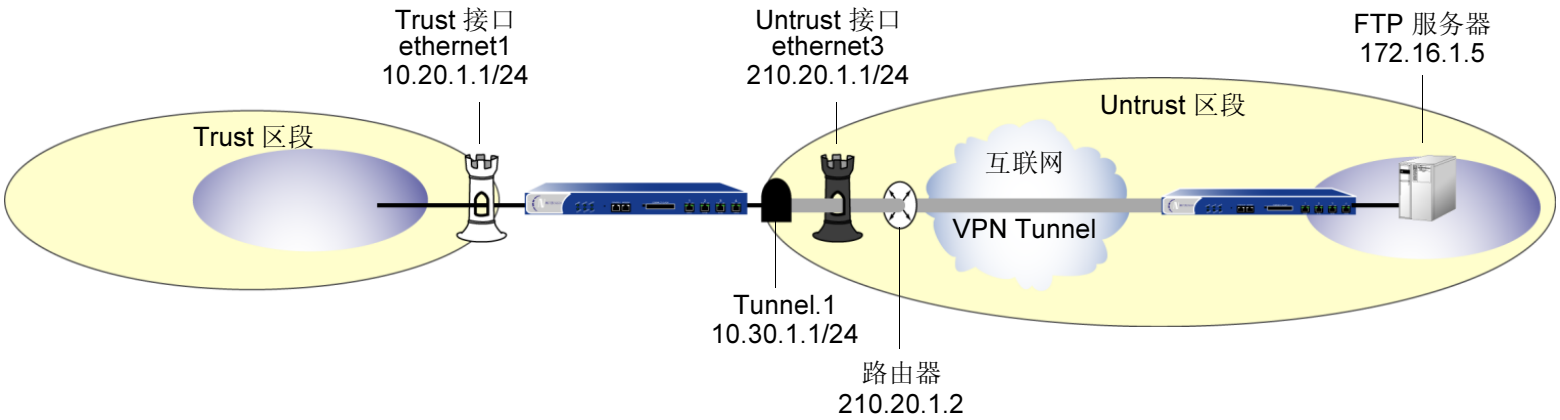
注意：*要移除条目，请单击* ***Remove****。会出现一条 “系统消息”，提示您确认移除操作。单击* ***OK*** *继续，或单击* ***Cancel*** *取消操作。*

CLI

1. set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
2. set vrouter untrust-vr route 3.3.3.0/24 interface ethernet3 gateway 2.2.2.3
3. set vrouter untrust-vr route 2.2.40.0/24 interface ethernet2 gateway 2.2.10.2
4. set vrouter untrust-vr route 2.20.0.0/16 interface ethernet2 gateway 2.2.10.3
5. set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
6. set vrouter trust-vr route 10.10.0.0/16 interface ethernet1 gateway 10.1.1.2
7. set vrouter trust-vr route 10.20.0.0/16 interface ethernet1 gateway 10.1.1.3
8. set vrouter trust-vr route 10.30.1.0/24 interface ethernet1 gateway 10.1.1.4
9. save

范例：设置通过通道接口到达远程网络的路由

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



WebUI

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

   Network Address/Netmask: 172.16.1.5/32

   Gateway: （选择）

   Interface: tunnel.1

   Gateway IP Address: 0.0.0.0

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

2. Network > Routing > Routing Table > 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: 210.20.1.2

CLI

1. set vrouter trust-vr route 172.16.1.5/32 interface tunnel.1
2. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 210.20.1.2
3. save

路由重新分配

路由重新分配是指在路由选择协议之间交换路由信息。当导入路由时，当前网域必须将从其它协议到其自身协议的所有信息进行转换，尤其是已知路由。例如，如果某路由选择域使用 OSPF 协议并且连接到某一使用 BGP 协议的路由选择域，则 OSPF 域必须从 BGP 域中导入所有路由，以通知其所有邻接路由器如何到达 BGP 域中的所有设备。

配置路由图

路由图由路由图条目列表组成。每一路由图条目包括以下内容：

- 序号
- 类型 — 匹配或设置
- 动作 — 允许或拒绝

路由图用于确定进入虚拟路由器的信息是否满足某些条件。如果信息符合条件，根据路由图中指定的动作，该信息可能会被允许或拒绝进入虚拟路由器。

范例：路由图创建

在本例中，您将在 trust-vr 虚拟路由器上创建一个名为 “rtmap1” 的路由图，它的序号为 1，过滤与含有标记值 111.111.111.111 的封包匹配的封包，并将权重 5 应用于匹配该标记值的封包。

WebUI

Network > Routing > Virtual Routers > Route Map > trust-vr New：输入以下内容，然后单击 **OK**：

Map Name: rtmap1

Action: permit （选择）

Sequence No.: 1

Match Properties:

Tag: 111.111.111.111

Set Properties:

Weight: 5

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set route-map name rtmap1 permit 1
3. ns(trust-vr/rtmap1)-> set match tag 111.111.111.111
4. ns(trust-vr/rtmap1)-> set weight 5
5. ns(trust-vr/rtmap1)-> save

路由导出和导入

两个虚拟路由器之间的路由重新分配受两类规则控制：导出和导入规则。要使某一虚拟路由器可向其它虚拟路由器导出路由，它必须具有导出规则。目的虚拟路由器可以拥有导入规则，用于控制可将哪些路由添加到其路由表中。如果虚拟路由器没有导入规则，则向其导出的所有路由都将被添加到其路由表中。

导出路由时，虚拟路由器将允许其它虚拟路由器了解其网络情况。导入路由时，虚拟路由器会了解其它虚拟路由器的网络情况。

缺省情况下，在 trust-vr 上启用路由导出。还可以配置一个用户定义的虚拟路由器，以便自动向其它虚拟路由器导出路由。网络中直接连接到处于 NAT 模式的接口的路由不能导出。

您可以配置一个虚拟路由器，使其可以导入从其它虚拟路由器收到的路由。

范例：创建路由导出规则

在本例中，您将使用路由图“rtmap1”并使用 BGP 作为路由选择协议，创建一个从 trust-vr 到 untrust-vr 虚拟路由器的路由导出规则。

WebUI

Network > Routing > Virtual Routers > Export Rules > trust-vr New：输入以下内容，然后单击 **OK**：

Destination Virtual Router: untrust-vr

Route Map: rtmap1

Protocol: BGP

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set export-to vrouter untrust-vr route-map rtmap1 protocol bgp
3. ns(trust-vr)-> save

范例：移除路由导出规则

在本例中，您将删除路由图 “rtmap1” 的从 trust-vr 到 untrust-vr 的导出规则。

WebUI

1. Network > Routing > Virtual Routers > Export Rules：对于路由图 rtmap1，单击 **Remove**。
2. 当出现提示，请求您确认删除操作时，单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> unset export-to vrouter untrust-vr route-map rtmap1 protocol bgp
3. ns(trust-vr)-> save

范例：创建路由导入规则

在本例中，您将用路由图 “ospf-to-trust” 和 OSPF 协议设置一个从 untrust-vr 到 trust-vr 虚拟路由器的路由导入规则。（本例假设已经创建了 “ospf-to-trust” 路由图。）

WebUI

Network > Routing > Virtual Routers > Import Rules > trust-vr New：输入以下内容，然后单击 **OK**：

Source Virtual Router: untrust-vr

Route Map: ospf-to-trust

Protocol: OSPF

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set import-from vrouter untrust-vr route-map ospf-to-trust protocol ospf
3. ns(trust-vr)-> save

范例：删除路由导入规则

在本例中，您将删除从 untrust-vr 到 trust-vr 且路由图为 “ospf-to-trust” 的路由导入规则。

WebUI

1. Network > Routing > Virtual Routers > Import Rules：对于从 untrust-vr 到 trust-vr 且路由图为 “ospf-to-trust”、协议为 OSPF 的路由导入规则，单击 **Remove**。
2. 当出现提示，请求您确认删除操作时，单击 **Yes**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> unset import-from vrouter untrust-vr route-map ospf-to-trust protocol ospf
3. ns(trust-vr)-> save

配置访问列表

访问列表为一组数据，用于通知 NetScreen 设备允许或拒绝哪些路由。当配置访问列表以测试允许或拒绝路由的条件时，必须指定访问列表 ID。

范例：访问列表配置

在本例中，您将在 trust-vr 上创建一个访问列表。该访问列表具有以下特征：

- ID: 2
- 转发状态：permit
- 过滤 IP 地址和网络掩码：1.1.1.1/24
- 序号：5

WebUI

Network > Routing > Virtual Routers > Access List: > trust-vr New：输入以下内容，然后单击 **OK**：

Access List ID: 2

Sequence No: 5

IP/Netmask: 1.1.1.1/24

Action: Permit

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set access-list 2 permit ip 1.1.1.1/24 5
3. ns(trust-vr)-> save

设置路由优选级

路由优选级是加到路由度量上的权重，它会影响信息流到达其目标所用的最佳路径的确定。导入路由时，虚拟路由器会在该路由的度量上加上一个优选级值—由获知该路由的协议确定。度量与优选级之和决定了虚拟路由器将优先选用哪个路由。低优选级值 （接近 0 的数）优先于高优选级值 （远离 0 的数）。

您还可以调整路由优选级值，将信息流沿着首选路径传送。

注意：*对于任何类型的路由 （如静态路由），如果路由优选级发生了变化，新的优选级将出现在路由表中，但在重新获知该路由或 （对于静态路由）删除并重新添加后，新的优选级才会生效。*

范例：设置路由优选级

在本例中，您将为任何 “connected[4]” 路由指定优选级值为 4，这些路由已被添加到 untrust-vr 的路由表中。

WebUI

Network > Routing > Virtual Routers > Edit (for untrust-vr)：输入以下内容，然后单击 **OK**：

Route Preference:

Connected: 4

CLI

1. ns-> set vrouter untrust-vr
2. ns(untrust-vr)-> set preference connected 4
3. ns(untrust-vr)-> save

4. 当路由器有一个 IP 地址在目标网络上的接口时，就会连接一条路由。

4

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 Layer 3（第 3 层）区段，给它分配一个 IP 地址。然后，必须配置允许信息流在区段之间从接口传递到接口的策略。可将多个接口指派给一个区段，但是不能将单个接口分配给多个区段。

本章包括以下部分：

接口类型

本部分描述安全区段、功能区段及通道接口。有关如何查看所有这些接口的表，请参阅第 87 页上的 “查看接口”。

安全区段接口

物理接口和子接口的目的是提供一个开口，网络信息流可通过它在区段之间流动。

物理

NetScreen 设备上的每个端口表示一个物理接口，且该接口的名称是预先定义的。物理接口的名称由媒体类型、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 “接口至区段绑定” 进行修改的 NetScreen 设备上，三个物理以太网接口被预先绑定到各特定 Layer 2（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 “多个安全区段”。）

子接口

子接口，与物理接口相似，充当信息流进出安全区段的开口。逻辑上，可将物理接口分成几个虚拟子接口。每个虚拟子接口都从其主干物理接口借用需要的带宽，因此它的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的相同区段，或将其绑定到不同区段。（有关详细信息，请参阅第 89 页上的 “将接口绑定到安全区段”和第 **6**-19 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失败，其它成员可以继续处理信息流—虽然可用的带宽比以前少。

注意： *有关聚合接口的详细信息，请参阅* NetScreen-5000 *系列安装程序指南。*

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升级到设备级故障切换前的首行冗余。

注意： *有关冗余接口的详细信息，请参阅第* ***7****-41 页上的 “安全区段冗余接口”。*

虚拟安全接口

虚拟安全接口 (VSI) 是在高可用性 (HA) 模式运行时，两个 NetScreen 设备形成虚拟安全设备 (VSD) 共享的虚拟接口。网络和 VPN 信息流使用 VSI 的 IP 地址和虚拟 MAC 地址。然后， VSD 将信息流映射到之前已经将该 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)。

Note: *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 7 卷，“NSRP”。*

功能区段接口

功能区段接口，例如，“管理”和 HA，每个都有专用目的。

管理接口

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

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。这两种配置在第 7 卷，“NSRP”中都有详尽说明。

虚拟 HA 接口

在没有专用 HA 接口的 NetScreen 设备上，虚拟高可用性 (HA) 接口提供相同的功能。由于没有 HA 信息流专用的独立物理端口，因此必须将“虚拟 HA”接口绑定到物理以太网端口之一。使用和将网络接口绑定到安全区段相同的方法，将网络接口绑定到 HA 区段（请参阅第 89 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* ***7-37*** *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。

通过将通道接口绑定到 VPN，可将策略从 VPN 通道分离。这样，便可配置一个通道，并定义多个允许或拒绝信息流通过该通道的策略。如果没有通道接口绑定到 VPN 通道，则必须在策略中指定 VPN 通道并选择 **tunnel** 作为操作。因为操作 **tunnel** 意味着允许，所以不能明确拒绝来自 VPN 通道的信息流。

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

如果将通道接口绑定到通道区段，则还可以将相同的通道接口和 DIP 池用于多个 VPN 通道。通过配置经由同一通道接口到达不同地址的路由，并在各种不同策略中指定不同的 VPN 通道，信息流可从一个通道接口进入多个 VPN 通道。

注意： *有关通道接口的信息，请参阅第* ***4*** *-48 页上的 “通道接口”。*

查看接口

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

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

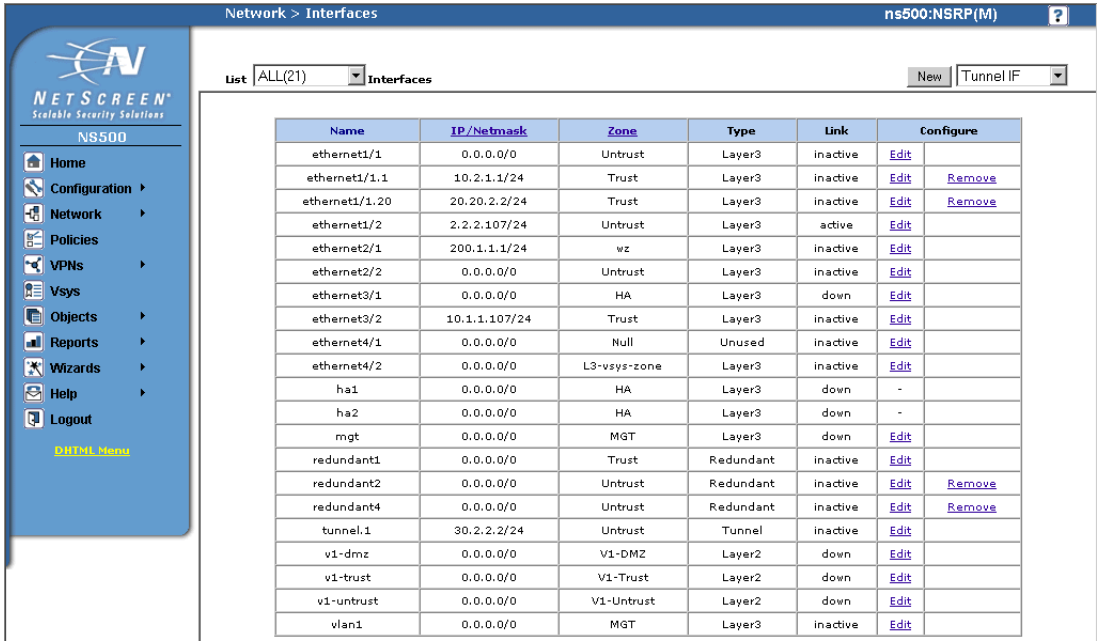
要在 CLI 中查看接口表，请使用 **get interface** 命令。

接口表

接口表显示每个接口的下列信息：

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

WebUI 物理接口
和子接口表

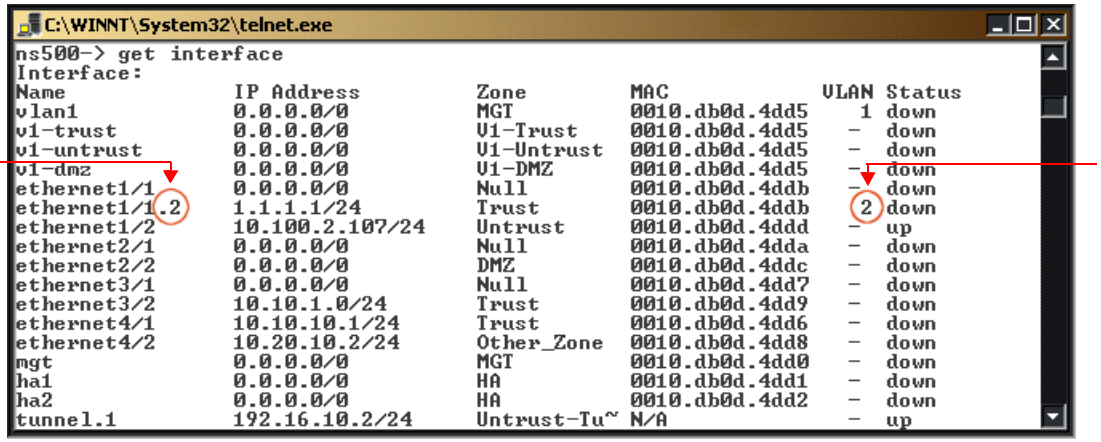


Name	IP/Netmask	Zone	Type	Link	Configure	
ethernet1/1	0.0.0.0/0	Untrust	Layer3	inactive	Edit	
ethernet1/1.1	10.2.1.1/24	Trust	Layer3	inactive	Edit	Remove
ethernet1/1.20	20.20.2.2/24	Trust	Layer3	inactive	Edit	Remove
ethernet1/2	2.2.2.107/24	Untrust	Layer3	active	Edit	
ethernet2/1	200.1.1.1/24	wz	Layer3	inactive	Edit	
ethernet2/2	0.0.0.0/0	Untrust	Layer3	inactive	Edit	
ethernet3/1	0.0.0.0/0	HA	Layer3	down	Edit	
ethernet3/2	10.1.1.107/24	Trust	Layer3	inactive	Edit	
ethernet4/1	0.0.0.0/0	Null	Unused	inactive	Edit	
ethernet4/2	0.0.0.0/0	L3-vsys-zone	Layer3	inactive	Edit	
ha1	0.0.0.0/0	HA	Layer3	down	-	
ha2	0.0.0.0/0	HA	Layer3	down	-	
mgt	0.0.0.0/0	MGT	Layer3	down	Edit	
redundant1	0.0.0.0/0	Trust	Redundant	inactive	Edit	
redundant2	0.0.0.0/0	Untrust	Redundant	inactive	Edit	Remove
redundant4	0.0.0.0/0	Untrust	Redundant	inactive	Edit	Remove
tunnel.1	30.2.2.2/24	Untrust	Tunnel	inactive	Edit	
v1-dmz	0.0.0.0/0	V1-DMZ	Layer2	down	Edit	
v1-trust	0.0.0.0/0	V1-Trust	Layer2	down	Edit	
v1-untrust	0.0.0.0/0	V1-Untrust	Layer2	down	Edit	
vlan1	0.0.0.0/0	MGT	Layer3	inactive	Edit	

CLI 物理接口
和子接口表

子接口号

VLAN 标记



```
C:\WINNT\System32\telnet.exe
ns500-> get interface
Interface:
Name            IP Address          Zone        MAC              VLAN Status
vlan1           0.0.0.0/0           MGT         0010.db0d.4dd5      1 down
v1-trust        0.0.0.0/0           V1-Trust    0010.db0d.4dd5      - down
v1-untrust      0.0.0.0/0           V1-Untrust  0010.db0d.4dd5      - down
v1-dmz          0.0.0.0/0           V1-DMZ      0010.db0d.4dd5      - down
ethernet1/1     0.0.0.0/0           Null        0010.db0d.4ddb      - down
ethernet1/1.2   1.1.1.1/24          Trust       0010.db0d.4ddb      2 down
ethernet1/2     10.100.2.107/24     Untrust     0010.db0d.4ddd      - up
ethernet2/1     0.0.0.0/0           Null        0010.db0d.4dda      - down
ethernet2/2     0.0.0.0/0           DMZ         0010.db0d.4ddc      - down
ethernet3/1     0.0.0.0/0           Null        0010.db0d.4dd7      - down
ethernet3/2     10.10.1.0/24        Trust       0010.db0d.4dd9      - down
ethernet4/1     10.10.10.1/24       Trust       0010.db0d.4dd6      - down
ethernet4/2     10.20.10.2/24       Other_Zone  0010.db0d.4dd8      - down
mgt             0.0.0.0/0           MGT         0010.db0d.4dd0      - down
ha1             0.0.0.0/0           HA          0010.db0d.4dd1      - down
ha2             0.0.0.0/0           HA          0010.db0d.4dd2      - down
tunnel.1        192.16.10.2/24      Untrust-Tu~ N/A                 - up
```

配置安全区段接口

本部分描述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
- 将地址分配到 L3 （第 3 层）安全区段接口
- 修改物理接口和子接口
- 创建子接口
- 删除子接口

> ***注意：****有关为接口设置信息流带宽的信息，请参阅第 9 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****-25 页上的 “管理接口选项”。*

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，因此仅可将子接口绑定到 L3 （第 3 层）安全区段。将接口绑定 L3 安全区后，才能将 IP 地址指定给接口。

范例：绑定接口

在本例中，将 ethernet5 绑定到 Trust 区段。

WebUI

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

CLI

1. set interface ethernet5 zone trust
2. save

为 L3 （第 3 层）安全区段接口定义地址

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

***注意：** 有关 NAT 和路由模式的配置，请参阅第 5 章，第 143 页上的 “接口模式”。*

进行接口地址分配时，要考虑的两种基本类型的 IP 地址如下：

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

公开 IP 地址

连接到公开网络的接口必须有公开 IP 地址。同样，如果 untrust-vr 中的 Layer 3 （第 3 层）安全区段连接到公开网络，并且 trust-vr 中区段的接口模式为路由，那么 trust-vr 的区段中所有地址 （包括接口和主机的地址）也必须为公开地址。公开 IP 地址分成三类， A、 B 和 C[1]，显示如下：

地址类别	地址范围	排除的地址范围
A	0.0.0.0 – 127.255.255.255	10.0.0.0 – 10.255.255.255, 127.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.16.255.255
C	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255

1. 还有 D 和 E 类地址，保留为专用。

IP 地址由四个八位位组组成，每个八位位组长为 8 位。在 A 类地址中，前 8 位表示网络 ID，后 24 位表示主机 ID (nnn.hhh.hhh.hhh)。在 B 类地址中，前 16 位表示网络 ID，后 16 位表示主机 ID (nnn.nnn.hhh.hhh)。在 C 类地址中，前 24 位表示网络 ID，后 8 位表示主机 ID (nnn.nnn.hhh.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[2] 指示，前 8 位（即第一个 8 位位组 — 010）确定此 A 类私有地址的网络部分，后 16 位（即第二个和第三个 8 位位组 — 002.003）确定地址的子网络部分，最后 8 位（最后一个 8 位位组 — 004）确定地址的主机部分。使用子网可将大的网络地址空间缩小为较小的子部分，这样大大增强了 IP 数据报的传输效率。

私有 IP 地址

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

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

2. 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 10.1.1.1/24、“管理 IP”地址 10.1.1.5。（请注意，“管理 IP”地址必须与安全区段接口 IP 地址在相同的子网中。）最后，将接口模式设置为 NAT，将所有内部 IP 地址转换至绑定到其它安全区段的缺省接口[3]。

WebUI

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

IP Address/Netmask: 10.1.1.1/24

Manage IP: 10.1.1.5

CLI

1. set interface ethernet5 ip 210.1.1.1/24
2. set interface ethernet5 manage-ip 210.1.1.5
3. save

3. 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，那么可解除其到一个安全区段的绑定，然后绑定到另一个安全区段。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，然后绑定到另一个安全区段，并（可选）给它分配 IP 地址 / 网络掩码。

范例：解除接口绑定

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

WebUI

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

Zone: Null

IP Address/Netmask: 0.0.0.0/0

CLI

1. set interface ethernet3 ip 0.0.0.0/0
2. set interface ethernet3 zone null
3. save

修改接口

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

- IP 地址和网络掩码
- 管理 IP 地址
- （L3 （第 3 层）和 L2 （第 2 层）区段接口）管理和网络服务
- （子接口）子接口 ID 号和 VLAN 标记号
- （trust-vr 中绑定到 L3 （第 3 层）安全区段的接口）接口模式 — NAT 或“路由”
- （物理接口）信息流带宽设置 （请参阅第 9 章，第 353 页上的“信息流整形”）

范例：修改接口上的设置

在本例中，对 ethernet5 进行一些修改，它是一个绑定到 Trust 区段的接口。将“管理 IP”地址从 10.1.1.2 更改为 10.1.1.12。为了确保管理信息流的绝对安全，还更改了管理服务选项，启用 SCS 和 SSL 并禁用 Telnet 和 WebUI。

WebUI

Network > Interfaces > Edit（对于 ethernet5）：进行以下修改，然后单击 **OK**：

Manage IP: 10.1.1.12

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

CLI

1. set interface ethernet5 manage-ip 10.1.1.12
2. set interface ethernet5 manage scs
3. set interface ethernet5 manage ssl
4. unset interface ethernet5 manage telnet
5. unset interface ethernet5 manage web
6. save

创建子接口

可在根系统或虚拟系统中的任何物理接口[4] 上创建子接口。子接口使用 VLAN 标记区别绑定到其的信息流与绑定到其它接口的信息流。请注意虽然子接口源自物理接口，并借用其需要的带宽，但是可将子接口绑定到任何区段，不必绑定到其“父级”接口绑定到的区段。此外，子接口的 IP 地址必须在不同于所有其它物理接口和子接口的 IP 地址的子网中。

范例：在根系统中创建子接口

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 ethernet5 的子接口。将子接口绑定到用户定义的区段，名为 “accounting”（在 trust-vr 中）。为其分配子接口 ID 3、 IP 地址 10.2.1.1/24 和 VLAN 标记 ID 3。接口模式为 NAT。

WebUI

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

Interface Name: ethernet5.3
Zone Name: accounting
IP Address/Netmask: 10.2.1.1/24
VLAN Tag: 3

CLI

1. set interface ethernet5.3 zone accounting
2. set interface ethernet5.3 ip 10.2.1.1/24 tag 3
3. save

4. 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 **7**-60 页上的 “虚拟系统支持”。

删除子接口

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

范例：删除安全区段接口

在本例中，将删除子接口 ethernet5:1。

WebUI

1. Network > Interfaces：单击 **Remove**（对于 ethernet5:1）。
   会出现一条系统消息，提示您确认移除。
2. 单击 **Yes** 删除子接口。

CLI

1. unset interface ethernet5:1
2. save

二级 IP 地址

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

***注意：** 不能为 Untrust 区段中的接口设置多个二级 IP 地址。*

二级 IP 地址属性

二级地址具有某些属性，这些属性会影响如何实施此类地址。这些属性如下：

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

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

范例：创建二级 IP 地址

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

WebUI

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

IP Address/Netmask: 192.168.2.1/24

CLI

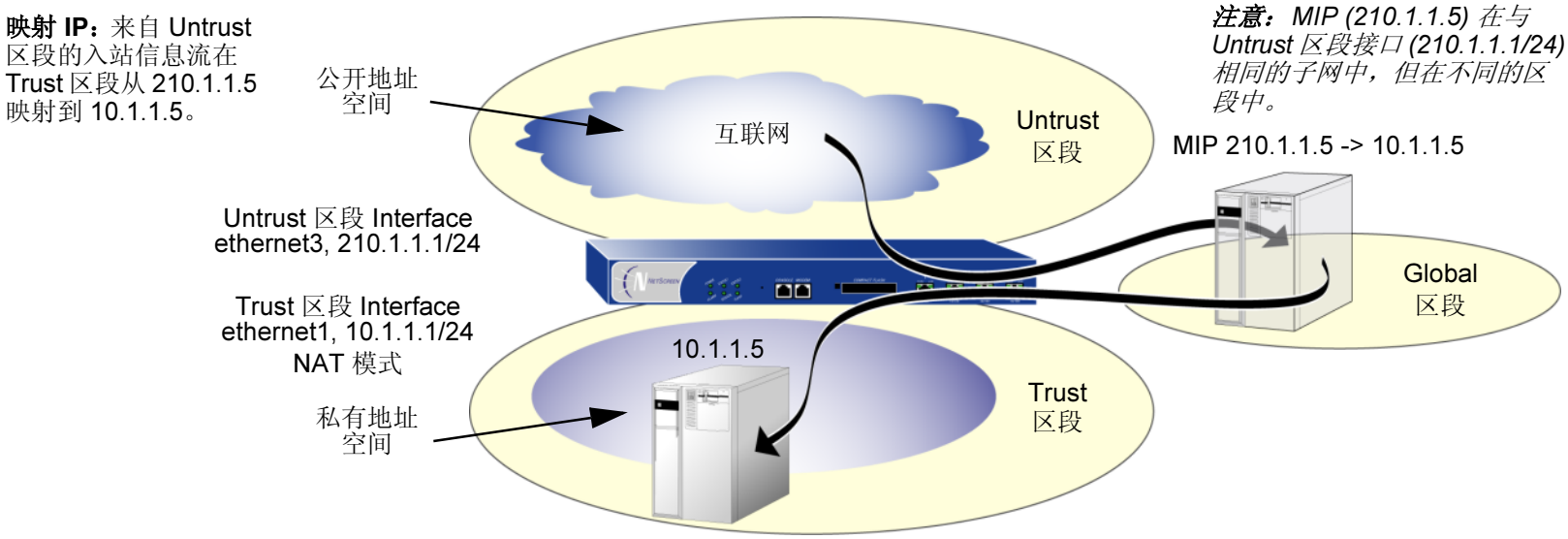
1. set interface ethernet1 ip 192.168.2.1/24 secondary
2. save

映射 IP 地址

映射 IP (MIP) 是一个 IP 地址到另一个 IP 地址的一对一直接映射。 NetScreen 设备将目的地为 MIP 的内向信息流转发至地址为 MIP 指向地址的主机。实际上， MIP 是静态目的地地址转换。“动态 IP” (DIP) 将 IP 封包包头中的源 IP 地址转换为 DIP 池中随机选择的地址，而 MIP 将 IP 封包包头中的目的地 IP 地址映射为另一个静态 IP 地址。（有关 DIP 的信息，请参阅第 125 页上的 “动态 IP 地址”。）

MIP 允许入站信息流到达接口模式为 NAT 的区段中的私有地址。MIP 还部分解决通过 VPN 通道连接的两个站点之间地址空间重叠的[5]问题。（有关此问题完整的解决方案，请参阅第 **4**-202 页上的“Tunnel 区段和基于策略的 NAT”。）

可在与任何已编号通道接口 （即带 IP 地址 / 网络掩码的接口）及任何绑定到第 3 层 (L3) 安全区段的已编号接口相同的子网中创建 MIP[6]。虽然 MIP 是为绑定到通道区段和安全区段的接口配置的，但是定义的 MIP 存储在 Global 区段。



5. 两个网络的 IP 地址范围部分或完全相同时发生地址空间重叠。

6. 为 Untrust 区段中接口定义的 MIP 例外。该 MIP 可以在不同于 Untrust 区段接口 IP 地址的子网中。但是，如果真是这样，就必须在外部路由器上添加一条路由，指向 Untrust 区段接口的，以便内向信息流能到达 MIP。

注意：在一些 NetScreen 设备上， MIP 可使用与接口相同的地址，但是 MIP 地址不能在 DIP 池中。可映射 “地址到地址” 或 “子网到子网” 关系。定义 “子网到子网” 映射 IP 配置后，映射 IP 子网和原始 IP 子网都将应用网络掩码。

MIP 和 Global 区段

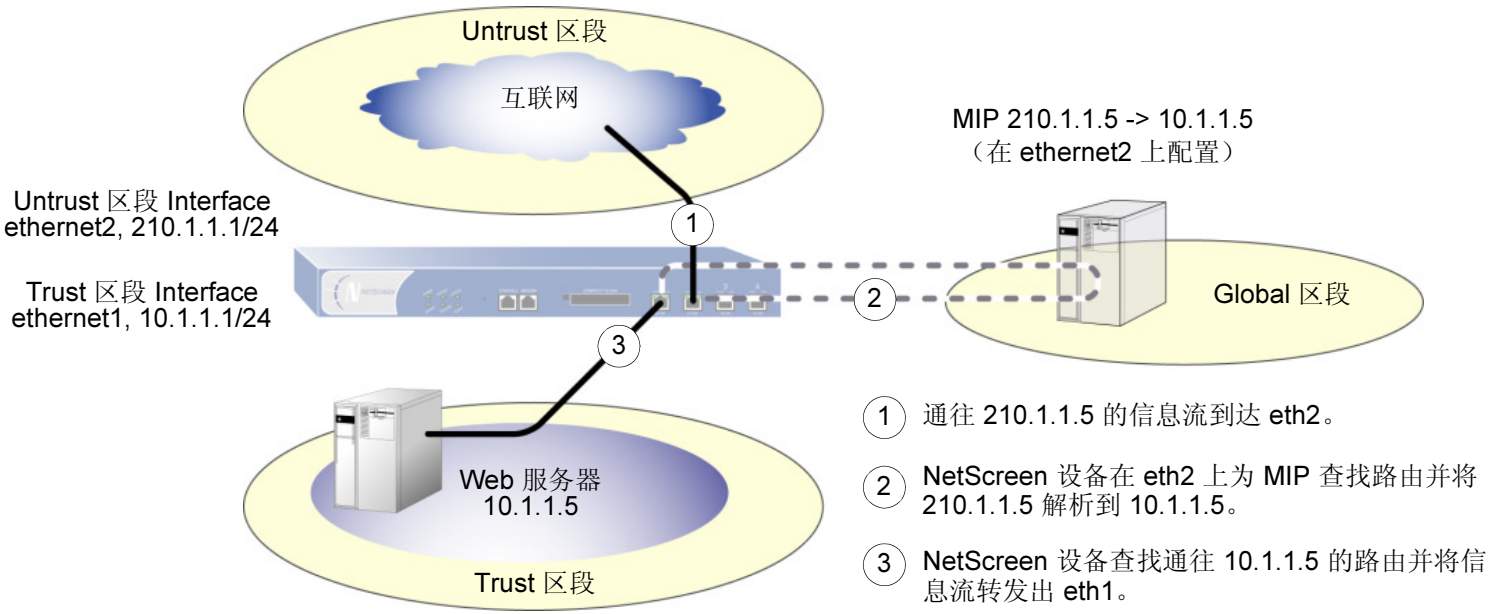
为任何区段中的接口设置 MIP 都将在 Global 区段通讯簿为该 MIP 生成通讯簿条目。Global 区段通讯簿保留所有接口的全部 MIP，不管接口属于哪个区段。可使用这些 MIP 地址充当策略中任何两个区段之间的目的地地址，以及定义从 Global 区段到任何其它区段的策略时的源地址。

注意：如果要将信息流整形应用于引用 MIP 的策略，就必须制定实际的源区段和目的地区段 （而非 Global 区段和另一区段）之间的策略。因为 Global 区段没有任何接口，它不支持信息流整形。

范例：将 MIP 添加到 Untrust 区段接口

在本例中，将 ethernet1 绑定到 Trust 区段并为其分配 IP 地址 10.1.1.1/24。将 ethernet2 绑定到 Untrust 区段并为其分配 IP 地址 210.1.1.1/24。然后，配置 MIP，将目的地为 Untrust 区段中 210.1.1.5 的内向 HTTP 信息流引导至 Trust 区段中地址为 10.1.1.5 的 Web 服务器。最后，创建一个策略，允许 HTTP 信息流从 Untrust 区段流向 Global 区段中的 MIP。所有安全区段都在 trust-vr 路由选择域中。

注意：*映射 IP 不需要通讯簿条目。*



WebUI

接口

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

MIP

3. Network > Interfaces > Edit（对于 ethernet2）> MIP > New：输入以下内容，然后单击 **OK**：
   Mapped IP: 210.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

策略

4. Policies > (From: Untrust, To: Global) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Any
   Destination Address:
   Address Book:（选择）, MIP(210.1.1.5)
   Service: HTTP
   Action: Permit

CLI

接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet2 zone untrust
4. set interface ethernet2 ip 210.1.1.1/24

MIP

5. set interface ethernet2 mip 210.1.1.5 host 10.1.1.5 netmask 255.255.255.255[7] vrouter trust-vr[8]

策略

6. set policy from untrust to global any mip(210.1.1.5) http permit
7. save

7. 缺省情况下， MIP 的网络掩码为 32 位 (255.255.255.255)，将地址映射到单个主机。还可为某个范围内的地址定义 MIP。例如，要通过 CLI，将 210.1.1.5 定义为 C 类子网中地址 10.1.10.129 – 10.1.10.254 的 MIP，请使用以下语法：**set interface** *interface* **mip 210.1.1.5 host 10.1.10.128 netmask 255.255.255.128**. 小心切勿使用包括接口或路由器地址的地址范围。

8. 缺省的虚拟路由器为 trust-vr。不必指定虚拟路由器为 trust-vr 或 MIP 有 32 位网络掩码。此命令中包含这些参数，以便和 WebUI 配置对称。

范例：从不同区段到达 MIP

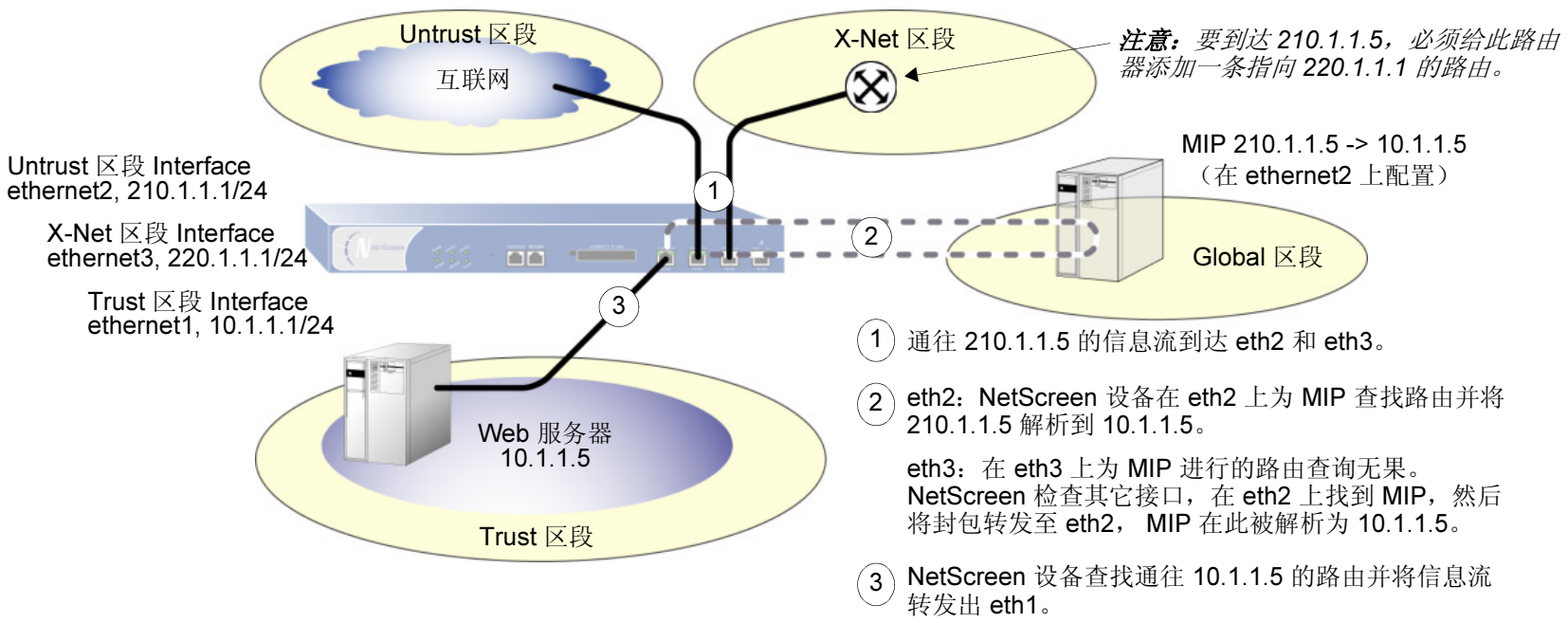
来自不同区段的信息流仍可通过其它接口（而非您在其上配置 MIP 的接口）到达 MIP。必须在其它每个区段的路由器上设置路由，将入站信息流指向它们各自接口的 IP 地址，以到达 MIP[9]。

在本例中，将在Untrust区段（ethernet2，210.1.1.1/24）中的接口上配置 MIP (210.1.1.5)，以映射Trust区段 (10.1.1.5) 中的 Web 服务器。绑定到 Trust 区段的接口是 IP 地址为 10.1.1.1/24 的 ethernet1。

创建名为 X-Net 的安全区段，将 ethernet3 绑定到该区段，然后给接口分配 IP 地址 220.1.1.1/24。为 210.1.1.5 定义一个地址，以用于策略，该策略允许 HTTP 信息流从 X-Net 区段的任何地址流向 Untrust 区段的 MIP。还将配置一个策略，允许 HTTP 信息流从 Untrust 区段流到 Global 区段。所有安全区段都在 trust-vr 路由选择域中。

注意：*必须在 X-Net 区段的路由器上输入一条路由，引导目的地为 210.1.1.5 (MIP) 的信息流流向 220.1.1.1（ethernet2 的 IP 地址）。*

9. 如果 MIP 与接口（在该接口上配置 MIP）在相同的子网中，则不必为了使信息流通过不同的接口到达 MIP，而添加到 NetScreen 设备的路由。但是，如果 MIP 在与其接口的 IP 地址不同的子网中（仅对于 Untrust 区段中接口上的 MIP 才可能出现这种情况），则必须将一条静态路由添加至 NetScreen 路由选择表。使用 **set vrouter** *name_str* **route** *ip_addr* **interface** *interface* 命令（或 WebUI 中的等同命令），其中，*name_str* 是指定接口所属的虚拟路由器，*interface* 是在其上配置 MIP 的接口。



WebUI

接口和区段

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

3. Network > Zones > New：输入以下内容，然后单击 **OK**：
   Zone Name: X-Net
   Virtual Router Name: untrust-vr
   Zone Type: Layer 3
4. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: X-Net
   IP Address/Netmask: 220.1.1.1/24

地址

5. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: 210.1.1.5
   IP Address/Domain Name:
   IP/Netmask:（选择）, 210.1.1.5/32
   Zone: Untrust

MIP

6. Network > Interfaces > Edit（对于 ethernet2）> MIP > New：输入以下内容，然后单击 **OK**：
   Mapped IP: 210.1.1.5
   Netmask: 255.255.255.255
   Host IP Address: 10.1.1.5
   Host Virtual Router Name: trust-vr

策略

7. Policies > (From: X-Net, To: Untrust) > New：输入以下内容，然后单击 **OK**：

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, 210.1.1.5

   Service: HTTP

   Action: Permit

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, MIP(210.1.1.5)

   Service: HTTP

   Action: Permit

CLI

接口和区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet2 zone untrust
4. set interface ethernet2 ip 210.1.1.1/24
5. set zone name X-Net
6. set interface ethernet3 zone X-Net
7. set interface ethernet3 ip 220.1.1.1/24

地址

8. set address untrust “210.1.1.5” 210.1.1.5/32

MIP

9. set interface ethernet2 mip 210.1.1.5 host 10.1.1.5 netmask 255.255.255.255 vrouter trust-vr[10]

策略

10. set policy from X-Net to untrust any “210.1.1.5” http permit
11. set policy from untrust to global any mip(210.1.1.5) http permit
12. save

10. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

范例：将 MIP 添加到 Tunnel 接口

在本例中，Trust 区段中网络的 IP 地址空间为 10.20.1.0/24，通道接口“tunnel.8”的 IP 地址为 10.20.3.1。Trust 区段中网络上服务器的物理 IP 地址为 10.20.1.25。为了允许一个远程网站（其网络在 Trust 区段中）使用重叠地址空间，通过 VPN 通道访问本地服务器，在 tunnel.8 接口所在的相同子网中创建 MIP。MIP 地址为 10.20.3.25/32。（有关带有通道接口的 MIP 的完整范例，请参阅第 **4**-204 页上的 “范例：具有 MIP 和 DIP 的 Tunnel 接口”。）

WebUI

Network > Interfaces > Edit（对于 tunnel.8）> MIP > New：输入以下内容，然后单击 **OK**：

Mapped IP: 10.20.3.25
Netmask: 255.255.255.255
Host IP Address: 10.20.1.25
Host Virtual Router Name: trust-vr

CLI

1. set interface tunnel.8 mip 10.20.3.25 host 10.20.1.25 netmask 255.255.255.255 vrouter trust-vr[11]
2. save

注意：*远程管理员为服务器将地址添加到他的 Untrust 区段通讯簿时，必须输入 MIP (10.20.3.25)，而不是服务器的物理 IP 地址 (10.20.1.25)。*

远程管理员还需要对通过 VPN 发往服务器的外向封包应用基于策略的 NAT（使用 DIP），以便本地管理员可添加与本地 Trust 区段地址不冲突的 Untrust 区段地址。否则，内向策略中的源地址会看似在 Trust 区段中。

11. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

MIP-Same-as-Untrust

由于 IPv4 地址越来越少， ISP 越来越不愿意分配给客户多于一个或两个 IP 地址。如果对于绑定到 Untrust 区段（绑定到 Trust 区段的接口模式为“网络地址转换”(NAT)）的接口，您只有一个 IP 地址，可使用 Untrust 区段接口 IP 地址充当映射 IP (MIP)，以提供到内部服务器或主机的入站访问。 MIP 将到达一个地址的信息流映射到另一个地址，因此，通过使用 Untrust 区段接口 IP 地址充当 MIP， NetScreen 设备将使用 Untrust 区段接口的所有入站信息流映射到指定内部地址。

如果创建一个策略，在该策略中，目的地地址是使用 Untrust 区段接口 IP 地址的 MIP，并且指定 HTTP 充当该策略中的服务，那么您就失去经由该接口对 NetScreen 设备进行 Web 管理的能力（因为流向该地址的所有入站 HTTP 信息流都被映射到内部服务器或主机）。通过更改 Web 管理的端口号，仍然可以使用 WebUI 通过 Untrust 区段接口管理该设备。要更改 Web 管理端口号，请执行以下操作：

1. Admin > Web：在“HTTP Port”字段输入注册的端口号（从 1024 到 65,535）。然后单击 **Apply**。
2. 下一次连接到 Untrust 区段接口管理该设备时，请将此端口号附加到 IP 地址 — 例如，http://209.157.66.170:5000。

范例：Untrust 接口上的 MIP

在本例中，选择 Untrust 区段接口（ethernet3，210.1.1.1/24）的 IP 地址充当 Web 服务器的 MIP，该服务器的实际 IP 地址为 Trust 区段中的 10.10.1.5。由于要保留对 ethernet3 的 Web 管理访问，因此将 web 管理端口号更改为 8080。然后创建一个策略，允许从 Untrust 区段到 Global 区段中 MIP 的 HTTP 服务。

注意：*本例假定已将 ethernet3 绑定到 Untrust 区段并分配 IP 地址为 210.1.1.1/24、已将 ethernet1 绑定到 Trust 区段并分配 IP 地址为 10.10.1.1/24（设置模式为 NAT），并且已设置网络需要的任何路由。*

WebUI

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

   失去 HTTP 连接。

2. 重新连接到 NetScreen 设备，将 8080 附加到 web 浏览器 URL 地址字段的 IP 地址。（如果您当前正通过 untrust 接口管理设备，请键入 **http://210.1.1.1:8080**。）
3. Network > Interface > Edit（对于 ethernet3）> MIP > New：输入以下内容，然后单击 **OK**：

   Mapped IP: 210.1.1.1

   Netmask: 255.255.255.255[12]

   Host IP Address: 10.10.1.5

   Host Virtual Router Name: trust-vr

12. 使用不可信接口 IP 地址的 MIP 的网络掩码必须为 32 位。

4. Policies > (From: Untrust, To: Global) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Any
   Destination Address:
   Address Book:（选择）, MIP(210.1.1.1)
   Service: HTTP
   Action: Permit

CLI

> ***注意：****只能通过 WebUI 更改用于 Web 管理的 HTTP 端口。*

1. set interface ethernet3 mip 210.1.1.1 host 10.10.1.5 netmask 255.255.255.255 vrouter trust-vr[13]
2. set policy from untrust to global any mip(210.1.1.1) http permit
3. save

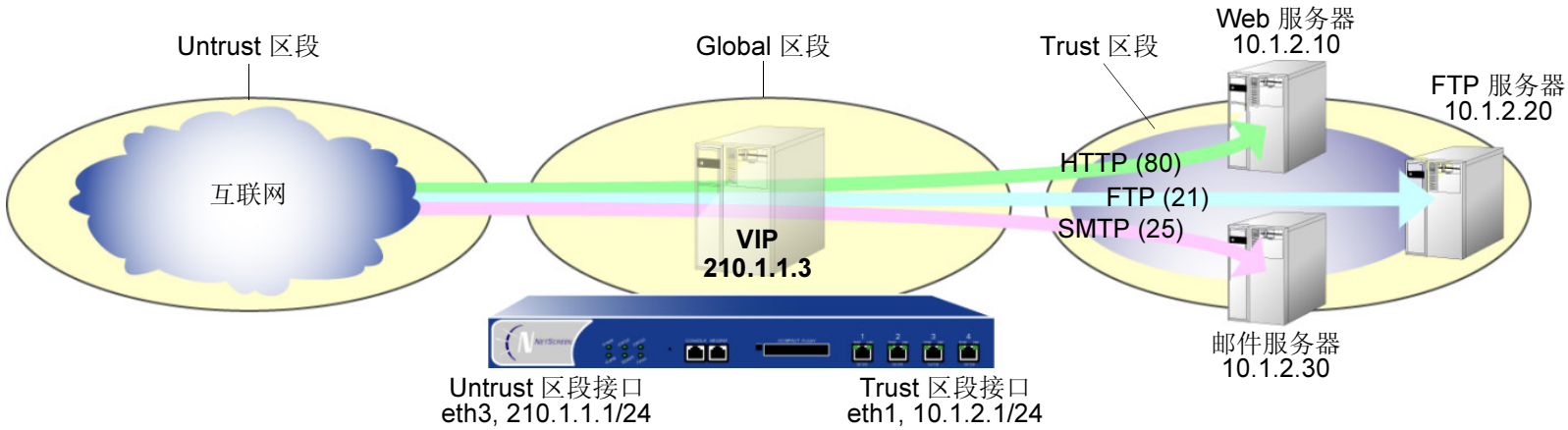
13. 缺省情况下，MIP 的网络掩码为 32 位 (255.255.255.255)，缺省虚拟路由器为 trust-vr。不必在命令中指定它们。此处包含这些参数，以便和 WebUI 配置对称。

虚拟 IP 地址

根据 TCP 或 UDP 片段包头的目的地端口号，虚拟 IP (VIP) 地址将在一个 IP 地址处接收到的信息流映射到另一个地址。例如，

- 目的地为 210.1.1.3:80（即，IP 地址为 210.1.1.3，端口为 80）的 HTTP 封包可能映射到地址为 10.1.2.10 的 web 服务器。
- 目的地为 210.1.1.3:21 的 FTP 封包可能映射到地址为 10.1.2.20 的 FTP 服务器。
- 目的地为 210.1.1.3:25 的 FTP 封包可能映射到地址为 10.1.2.30 的 FTP 服务器。

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



虚拟 IP 转发表

Untrust Zone 中的接口 IP	Global Zone 中的 VIP	端口	转发至	Trust Zone 中的主机 IP
210.1.1.1/24	*210.1.1.3*	*80 (HTTP)*	→	*10.1.2.10*
210.1.1.1/24	*210.1.1.3*	*21 (FTP)*	→	*10.1.2.20*
210.1.1.1/24	*210.1.1.3*	*25 (SMTP)*	→	*10.1.2.30*

可以对众所周知的服务使用虚拟端口号以增强安全性。例如，如果您只想允许分支机构的雇员在公司网站访问 FTP 服务器，可以指定从 1024 到 65,535 的注册端口号充当内向 FTP 信息流的端口号。 NetScreen 设备拒绝任何尝试在其众所周知的端口号 (21) 到达 FTP 服务器的信息流。只有预先知道虚拟端口号并将其附加到封包包头的人员才能访问该服务器。

需要以下信息来定义 “虚拟 IP”：

- VIP 的 IP 地址，它必须与发出信息流的区段的接口在相同子网中 （或与接口的 IP 地址相同）
- 处理请求的服务器的 IP 地址
- 要 NetScreen 设备从 VIP 转发至主机 IP 地址的服务类型

> ***注意：****只能在 Untrust 区段接口上设置 VIP。*

以下为一些有关 NetScreen VIP 的注释：

- 最多可将 64 项服务从单个的 VIP 映射到一个或多个服务器[14]。
- 可映射预先定义的服务和用户定义的服务。
- 单个 VIP 可识别具有相同源及目的地端口号但传输方式不同的定制服务。
- 定制服务可使用任何目的地端口号或端口号范围，从 1 到 32,767，而不仅是从 1024 到 32,767。
- 通过在单个 VIP 下创建多个服务条目，单个 VIP 可支持具有多个端口条目的定制服务（服务中的每个端口条目在 VIP 中对应有一个服务条目）。缺省情况下，可在 VIP 中使用单端口服务。要在 VIP 中使用多端口服务，必须首先发出 CLI 命令 **set vip multi-port**，然后重新设置 NetScreen 设备。（请参阅第 118 页上的 “范例：具有定制和多端口服务的 VIP” 。）
- 必须可从 trust-vr 到达 NetScreen 设备将 VIP 信息流映射到的主机。如果该主机不在 trust-vr 的路由选择域中，则必须定义到达它的路由。

14. 在支持负载均衡的 NetScreen 设备上，每个 VIP 最多可映射 8 项服务。

VIP 和 Global 区段

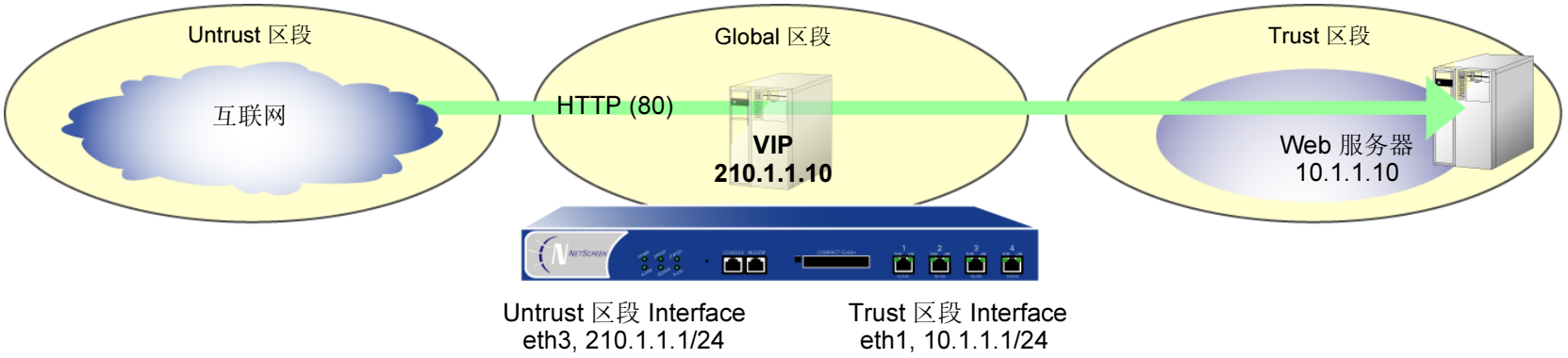
为 Untrust 区段中的接口设置 VIP 将在 Global 区段通讯簿中生成一条条目。不管接口属于哪个区段，Global 区段通讯簿保留所有接口的全部 VIP。可使用这些 VIP 地址充当任何两个区段之间策略的目的地地址。

范例：配置虚拟 IP 服务器

在本例中，将接口 ethernet1 绑定到 Trust 区段并分配 IP 地址为 10.1.1.1/24。将接口 ethernet3 绑定到 Untrust 区段并分配 IP 地址为 210.1.1.1/24。

然后，在 210.1.1.10 配置 VIP，以将入站 HTTP 信息流转发至地址为 10.1.1.10 的 Web 服务器，并且创建一个策略，允许信息流从 Untrust 区段到达 Global 区段的 VIP。

由于 VIP 与 Untrust 区段接口 (210.1.1.0/24) 在相同的子网中，因此无需为从 Untrust 区段到达它的信息流定义路由[15]。此外， VIP 将信息流转发到的主机不需要通讯簿条目。所有安全区段都在 trust-vr 路由选择域中。



15. 如果希望 HTTP 信息流从安全区段（而非 Untrust 区段）到达 VIP，则必须在该区段路由器上为 210.1.1.10 设置路由，指向绑定到该区段的接口。例如，设想 ethernet2 被绑定到一个用户定义的区段，并且已配置该区段中的路由器，将流向 210.1.1.10 的信息流发送到 ethernet2。路由器将信息流发送到 ethernet2 后，NetScreen 设备中的转发机制将 VIP 定位在 ethernet3，它将信息流映射到 10.1.1.10 并发送出 ethernet1，到达 Trust 区段。此过程与第 104 页上的“范例：从不同区段到达 MIP”中描述的类似。此外，还必须设置一个策略，允许 HTTP 信息流从其它区段流向 Global 区段中的 VIP。

WebUI

安全区段接口

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **Apply**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

VIP

3. Network > Interfaces > Edit（对于 ethernet3）> VIP：输入以下地址，然后单击 **Add**：
   Virtual IP Address: 210.1.1.10
4. Network > Interfaces > Edit（对于 ethernet3）> VIP > New VIP Service：输入以下内容，然后单击 **OK**：
   Virtual Port: 80
   Map to Service: HTTP (80)
   Map to IP: 10.1.1.10

策略

5. Policies > (From: Untrust, To: Global) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, ANY
   Destination Address:
   Address Book:（选择）, VIP(210.1.1.10)
   Service: HTTP
   Action: Permit

CLI

安全区段接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet2 ip 210.1.1.1/24

VIP

5. set interface ethernet3 vip 210.1.1.10 80 http 10.1.1.10

策略

6. set policy from untrust to trust any vip(210.1.1.10) http permit
7. save

范例：编辑 VIP 配置

在本例中，将修改在上一范例中创建的“虚拟 IP”服务器配置。为了限制对 Web 服务器的访问，将 HTTP 信息流的虚拟端口号从 80（缺省值）更改为 2211。现在，只有那些连接 Web 服务器时知道使用端口号 2211 的人员才能访问它。

WebUI

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

Virtual Port: 2211

CLI

1. set interface ethernet3 vip 210.1.1.10 2211 http 10.1.1.10
2. save

范例：移除 VIP 配置

在本例中，将删除以前创建并修改的 VIP 配置。必须首先移除与其有关的任何现有策略，才能移除 VIP。在第 115 页上的 “范例：配置虚拟 IP 服务器”中创建的策略 ID 号为 5。

WebUI

1. Policies > (From: Untrust, To: Global) > Go：为策略 ID 5，单击 **Remove**。
2. Network > Interfaces > Edit（对于 ethernet3）> VIP：单击 **Remove**。

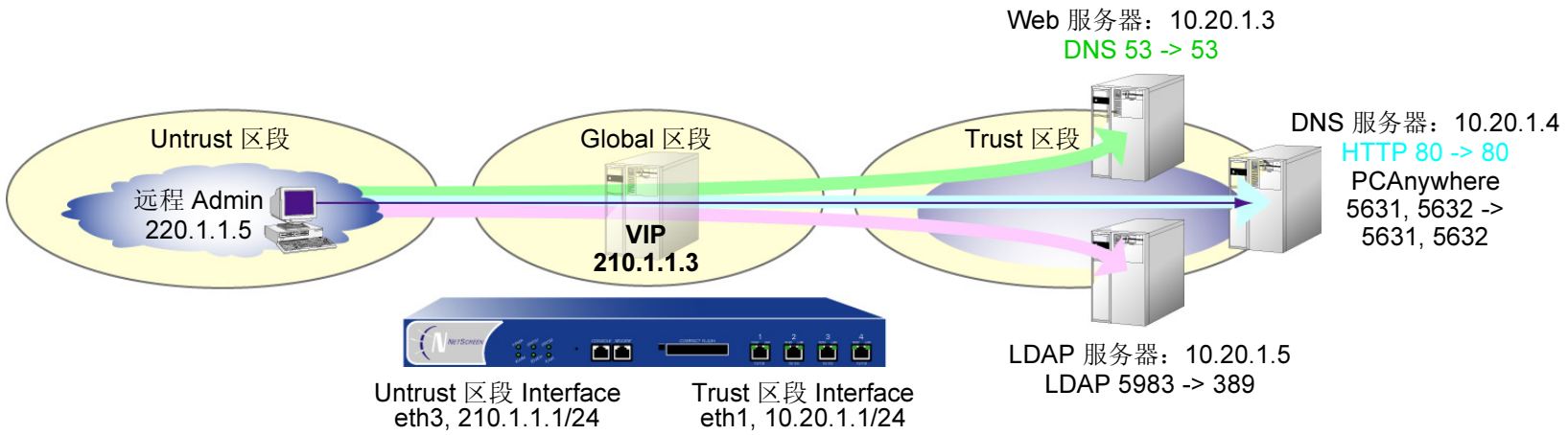
CLI

1. unset policy id 5
2. unset interface ethernet3 vip 210.1.1.10
3. save

范例：具有定制和多端口服务的 VIP

在以下范例中，在 210.1.1.3 配置 VIP，将以下服务发送到下列内部地址：

服务	传送	虚拟端口号	实际端口号	主机 IP 地址
DNS	TCP, UDP	53	53	10.20.1.3
HTTP	TCP	80	80	10.20.1.4
PCAnywhere	TCP, UDP	5631, 5632	5631, 5632	10.20.1.4
LDAP	TCP, UDP	5983	389	10.20.1.5



注意：*支持负载均衡的 NetScreen 设备不支持每个 VIP 多于 8 个端口。在这样的设备上，您必须配置额外的 VIP 来完成本例中的配置。*

VIP 将 DNS 查询发送到 DNS 服务器 (10.20.1.3)，将 HTTP 信息流发送到 web 服务器 (10.20.1.4)，并将认证检查发送到 LDAP 服务器 (10.20.1.5) 上的数据库。对于 HTTP、DNS 和 PCAnywhere，虚拟端口号与实际端口号保持一致。对于 LDAP，虚拟端口号 (5983) 用于将额外的安全级别添加到 LDAP 认证信息流。

为了远程管理 HTTP 服务器，定义一个定制服务并且命名为 PCAnywhere。PCAnywhere 是一项多端口服务，它发送并监听 TCP 端口 5631 上的数据以及 UDP 端口 5632 上的状态检查。

还要在 Untrust 区段通讯簿中输入“远程 Admin”(220.1.1.5) 的地址，并且为所有要使用 VIP 的信息流配置从 Untrust 区段到 Global 区段的策略。

所有安全区段都在 trust-vr 路由选择域中。

WebUI

安全区段接口

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **Apply**：
   Zone Name: Trust
   IP Address/Netmask: 10.20.1.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

地址

3. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: Remote Admin
   IP Address/Domain Name:
   IP/Netmask: 220.1.1.5/32
   Zone: Untrust

定制服务

4. Object > Services > Custom > New：输入以下内容，然后单击 **OK**：
   Service Name: PCAnywhere
   No 1:
   Transport: TCP
   Source Port Low: 0
   Source Port High: 65535
   Destination Port Low: 5631
   Destination Port High: 5631

No 2:
Transport: UDP
Source Port Low: 0
Source Port High: 65535
Destination Port Low: 5632
Destination Port High: 5632

VIP 地址和服务[16]

5. Network > Interfaces > Edit（对于 ethernet3）> VIP：单击此处进行配置：在“Virtual IP Address”字段中键入 **210.1.1.3**，然后单击 **Add**。

> New VIP Service：输入以下内容，然后单击 **OK**：
Virtual Port: 53
Map to Service: DNS
Map to IP: 10.20.1.3[17]

> New VIP Service：输入以下内容，然后单击 **OK**：
Virtual Port: 80
Map to Service: HTTP
Map to IP: 10.20.1.4

> New VIP Service：输入以下内容，然后单击 **OK**：
Virtual Port: 5631[18]
Map to Service: PCAnywhere
Map to IP: 10.20.1.4

16. 要启用 VIP 支持多端口服务，就必须输入 CLI 命令 **set vip multi-port**，保存配置，然后重新启动设备。
17. 对于具有负载均衡功能的 NetScreen 设备，请从 Load Balance 下拉列表中选择 **None**，然后在 Server Weight 字段中键入 **1**。
18. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

> New VIP Service：输入以下内容，然后单击 **OK**：

Virtual Port: 5983[19]

Map to Service: LDAP

Map to IP: 10.20.1.5

策略

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

Source Address:

Address Book:（选择）, Any

Destination Address:

Address Book:（选择）, VIP(210.1.1.3)

Service: DNS

Action: Permit

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

Source Address:

Address Book:（选择）, Any

Destination Address:

Address Book:（选择）, VIP(210.1.1.3)

Service: HTTP

Action: Permit

19. 使用非标准端口号可添加另一安全层，阻挡查找位于标准端口号的服务的攻击。

8. Policies > (From: Untrust, To: Global) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Any
   Destination Address:
   Address Book:（选择）, VIP(210.1.1.3)
   Service: LDAP
   Action: Permit
9. Policies > (From: Untrust, To: Global) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Remote Admin
   Destination Address:
   Address Book:（选择）, VIP(210.1.1.3)
   Service: PCAnywhere
   Action: Permit

CLI

安全区段接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.20.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 210.1.1.1/24

地址

5. set address untrust “Remote Admin” 220.1.1.5/32

定制服务

6. set service pcanywhere protocol udp src-port 0-65535 dst-port 5631-5631
7. set service pcanywhere protocol tcp src-port 0-65535 dst-port 5632-5632

VIP 地址和服务

8. set vip multi-port
9. save
10. reset

    当提示是否确定要重新启动该设备时，请按 Y 键。

11. set vip 210.1.1.3 53 dns 10.20.1.3/1
12. set vip 210.1.1.3 + 80 http 10.20.1.4/1
13. set vip 210.1.1.3 + 5631 pcanywhere 10.20.1.4/1[20]
14. set vip 210.1.1.3 + 5983 ldap 10.20.1.5/1

策略

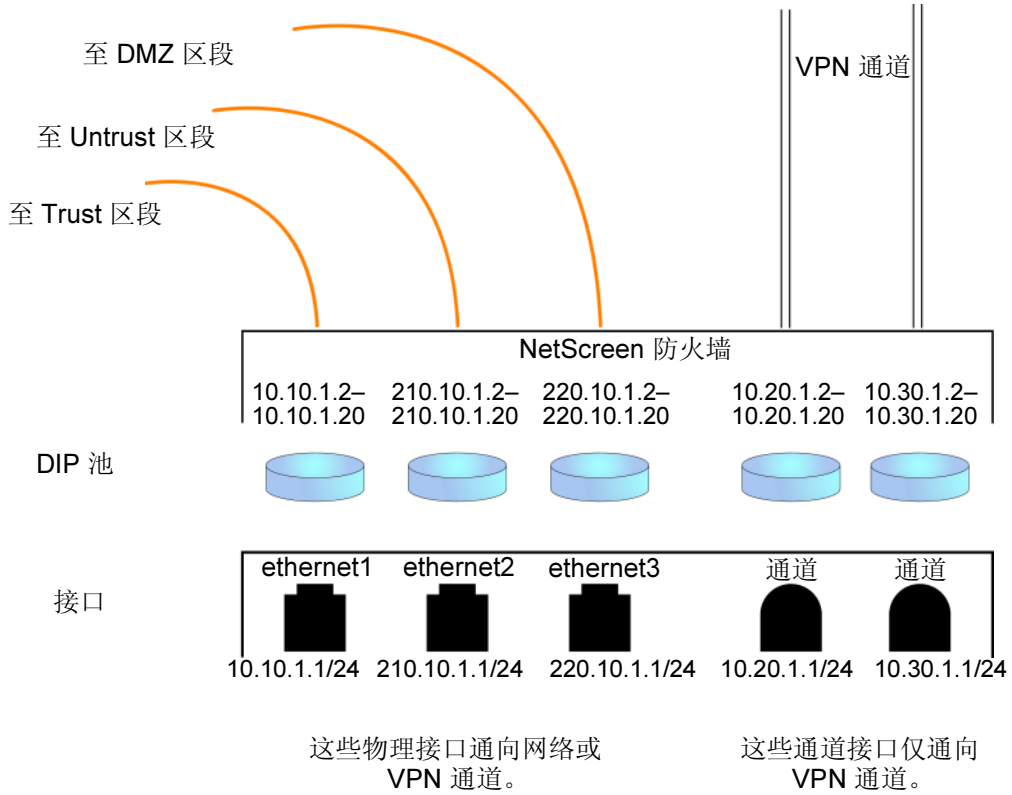
15. set policy from untrust to global any vip(210.1.1.3) dns permit
16. set policy from untrust to global any vip(210.1.1.3) http permit
17. set policy from untrust to global any vip(210.1.1.3) ldap permit
18. set policy from untrust to global “Remote Admin” vip(210.1.1.3) pcanywhere permit
19. save

20. 对于多端口服务，输入服务的最低端口号作为虚拟端口号。

动态 IP 地址

DIP 池包含一个范围内的 IP 地址， NetScreen 设备在对 IP 封包包头中的源 IP 地址执行网络地址转换 (NAT) 时，可从中动态地提取地址。如果 DIP 池的地址范围与接口 IP 地址在相同的子网中，那么该池必须排除也可能在该子网中的接口 IP 地址、路由器 IP 地址及任何 “映射” 或 “虚拟 IP” 地址。如果地址范围在扩展接口的子网中，那么该池必须排除扩展接口的 IP 地址。

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



端口地址转换

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

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

范例：创建带有 PAT 的 DIP 池

在本例中，将为本地网站的用户创建 VPN 通道，以到达远程网站的 FTP 服务器。但是，这两个网站的内部网络使用相同的私有地址空间 （10.10.1.0/24）。为了解决重叠地址的问题，在本地 NetScreen 设备的 Untrust-Tun 通道区段中创建通道接口，给它分配 IP 地址 10.20.1.1/24，然后将它与地址范围为 10.20.1.10 – 10.20.1.20（来自中性地址空间 10.20.1.0/24）的 DIP 池相关联。

在远程网站的远程 admin，也必须创建 IP 地址在中性地址空间的通道接口，如 10.30.1.1/24，然后设置到其 FTP 服务器的 “映射 IP” (MIP) 地址，如到主机 10.10.1.5 的 10.30.1.5。

注意: *有关此方案所有必要配置步骤的完整范例，请参阅第* ***4****-204 页上的“范例: 具有 MIP 和 DIP 的 Tunnel 接口”。*

WebUI

1. Network > Interfaces > New Tunnel IF：输入以下内容，然后单击 **OK**：
   Tunnel Interface Name: tunnel .: 8
   Zone: Untrust-Tun
   Fixed IP:（选择）
   IP Address/Netmask: 10.20.1.1/24
2. Network > Interfaces > Edit（对于 tunnel.8）> DIP > New：输入以下内容，然后单击 **OK**：
   ID: 5[21]
   IP Address Range:
   Start: 10.20.1.10
   End: 10.20.1.20
   Port Translation:（选择）

CLI

1. set interface tunnel.8 zone untrust-tun
2. set interface tunnel.8 ip 10.20.1.1/24
3. set interface tunnel.8 dip 5 10.20.1.10 10.20.1.20
4. save

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

- **(WebUI)** *Network > Interfaces > Edit（对于 tunnel.8）> DIP > New：清除* **Port Translation** *复选框，然后单击* **OK**。
- **(CLI)** *set interface tunnel.8 dip 5 10.20.1.10 10.20.1.20 fix-port*

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

范例：修改 DIP 池

在本例中，将更改一个现有 DIP 池 (ID 8) 的地址范围，从 10.20.1.10 – 10.20.1.100 到 10.20.1.10 – 10.20.1.20。此 DIP 池与 tunnel.2 相关联。请注意，要通过 CLI 更改 DIP 池范围，必须首先移除 （或撤消）现有 dip 池，然后创建新池。

注意：*没有使用此特定 DIP 池的策略。如果有策略，则需要删除策略或在该策略中不使用此 DIP 池。*

WebUI

Network > Interfaces > Edit（对于 tunnel.2）> DIP > Edit（对于 ID 8）：输入以下内容，然后单击 **OK**：

IP Address Range End: 10.20.1.20

CLI

1. unset interface tunnel.2 dip 8
2. set interface tunnel.2 dip 8 10.20.1.10 10.20.1.20
3. save

扩展接口和 DIP

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

范例：在不同子网中使用 DIP

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

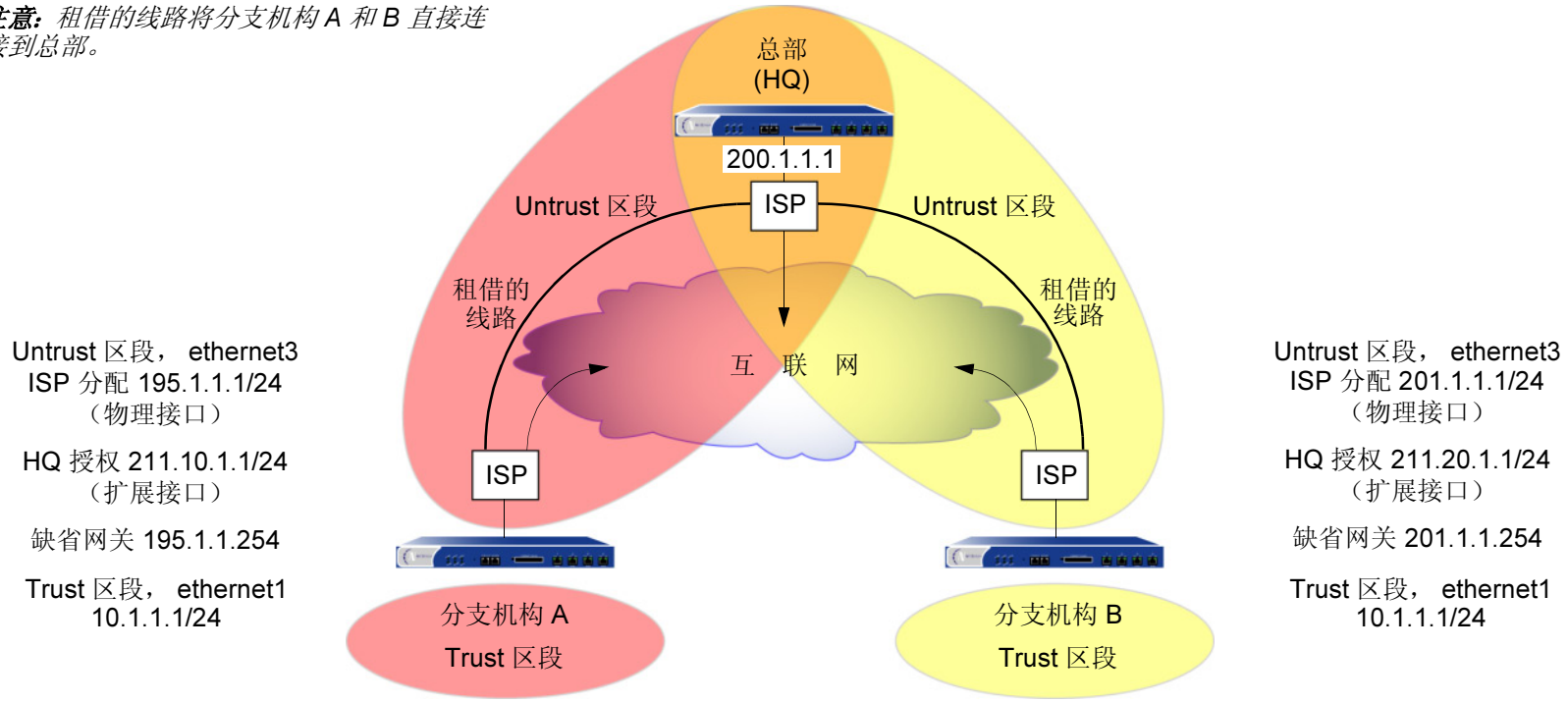
	分配的 IP 地址 （从 ISP） 用于 Untrust 区段物理接口	**授权的 IP 地址 （从总部） 用于 Untrust 区段扩展接口 DIP**
分支机构 A	195.1.1.1/24	211.10.1.1/24
分支机构 B	201.1.1.1/24	211.20.1.1/24

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

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

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

注意：*租借的线路将分支机构 A 和 B 直接连接到总部。*



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

WebUI (分支机构 A)

接口

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

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 195.1.1.1/24
3. Network > Interfaces > Edit（对于 ethernet3）> DIP > New：输入以下内容，然后单击 **OK**：
   ID: 5
   IP Address Range:
   Start: 211.10.1.1
   End: 211.10.1.1
   Port Translation:（选择）
   Extended IP/Netmask: 211.10.1.10/255.255.255.0

地址

4. 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

路由

5. Network > Routing > Routing Table > 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

策略

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, Any

   Service: ANY

   Action: Permit

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（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:（选择）

   DIP On:（选择）, 5 (211.10.1.1-211.10.1.1)/X-late

WebUI (分支机构 B)

接口

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **Apply**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 201.1.1.1/24
3. Network > Interfaces > Edit（对于 ethernet3）> DIP > New：输入以下内容，然后单击 **OK**：
   ID: 5
   IP Address Range:
   Start: 211.20.1.1
   End: 211.20.1.1
   Port Translation:（选择）
   Extended IP/Netmask: 211.20.1.10/255.255.255.0

地址

4. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: HQ
   IP Address/Domain Name:
   IP/Netmask: 200.1.1.1/32
   Zone: Untrust

路由

5. Network > Routing > Routing Table > 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

策略

6. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Any
   Destination Address:
   Address Book:（选择）, Any
   Service: ANY
   Action: Permit
7. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Any
   Destination Address:
   Address Book:（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:（选择）
   DIP On:（选择）, 5 (211.20.1.1-211.20.1.1)/X-late

CLI (分支机构 A)

接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 195.1.1.1/24
5. set interface ethernet3 ext ip 211.10.1.10 255.255.255.0 dip 5 211.10.1.1

地址

6. set address untrust hq 200.1.1.1/32

路由

7. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 195.1.1.254

策略

8. set policy from trust to untrust any any any permit
9. set policy top from trust to untrust any hq any nat dip 5 permit
10. save

CLI (分支机构 B)

接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 201.1.1.1/24
5. set interface ethernet3 ext ip 211.20.1.10 255.255.255.0 dip 5 211.20.1.1

地址

6. set address untrust hq 200.1.1.1/32

路由

7. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.1.1.254

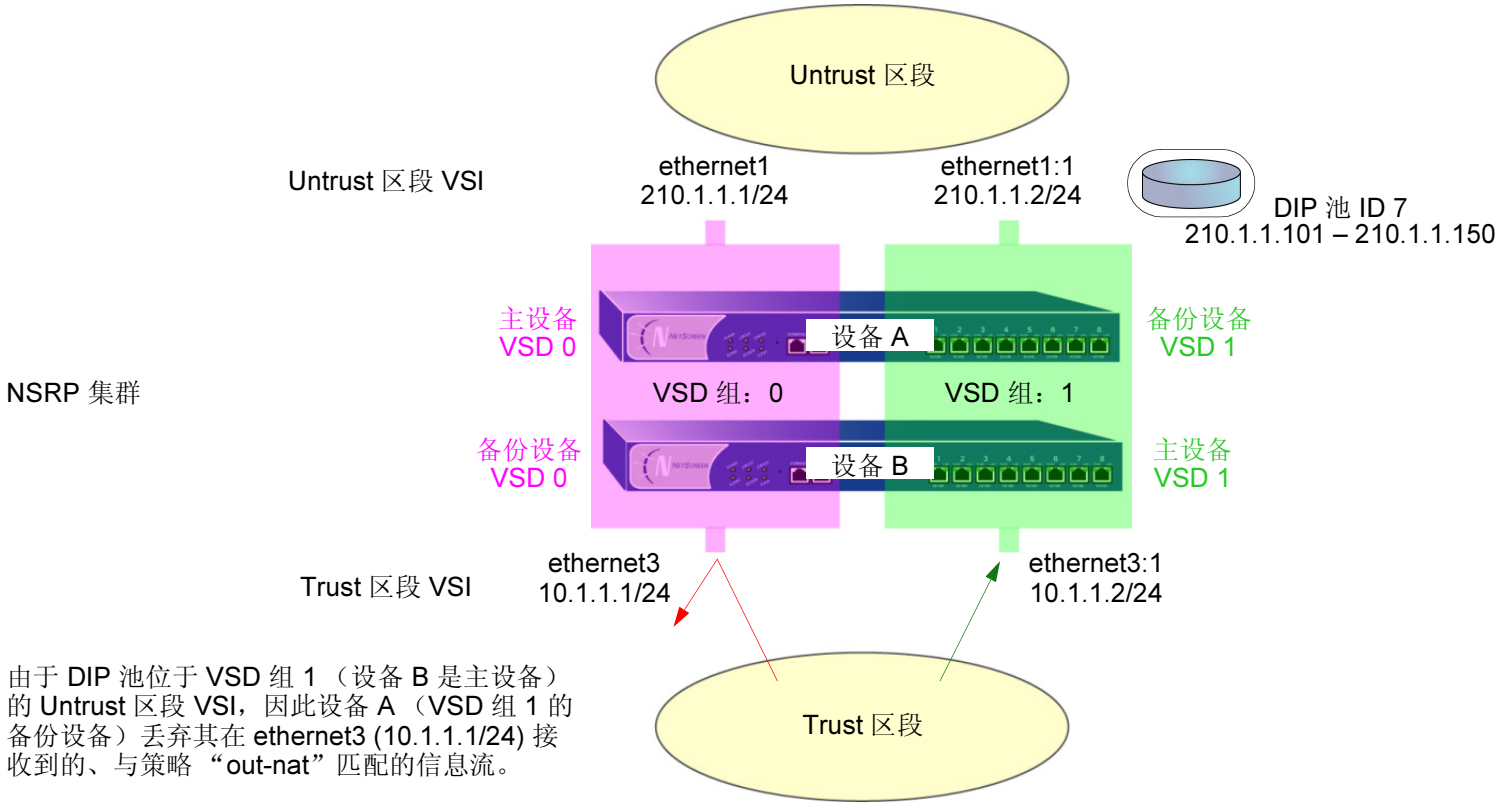
策略

8. set policy from trust to untrust any any any permit
9. set policy top from trust to untrust any hq any nat dip 5 permit
10. save

DIP 组

当您将两个 NetScreen 设备组成一个冗余集群，以提供双主动配置的高可用性 (HA) 时，两个设备都共享同一配置并且同时处理信息流。定义使用 DIP 池 （位于一个 VSI 上）执行网络地址转换 (NAT) 的策略时，可能会出现问题。因为仅在 NetScreen 设备充当绑定 VSI 的 VSD 组的主设备时，该 VSI 才活动，因此任何发送到其它 NetScreen 设备（充当该 VSD 组的备份设备）的信息流无法使用该 DIP 池并被丢弃。

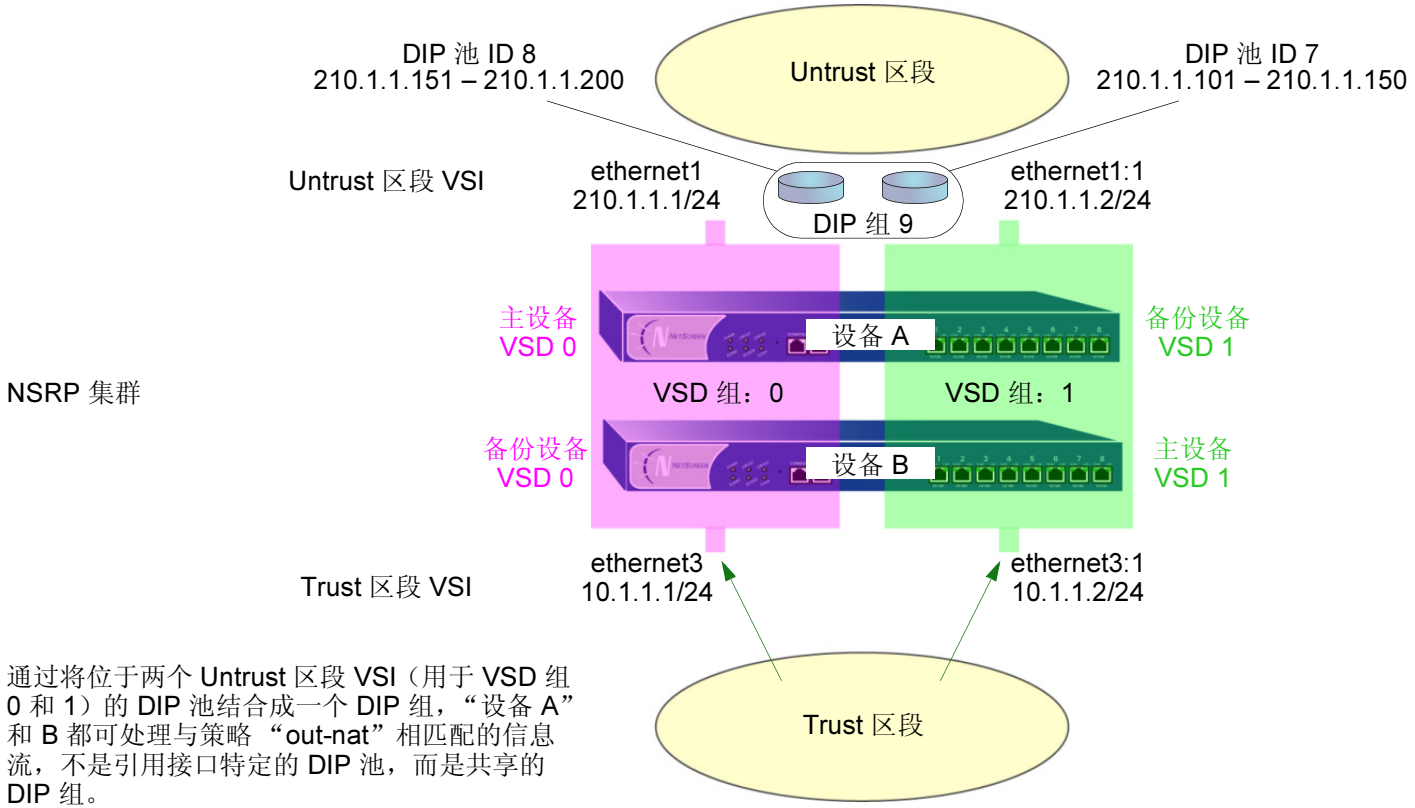
在 NSRP 集群中时，不当使用 DIP 池的策略：
set policy name out-nat from trust to untrust any any any nat dip-id 7 permit



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）丢弃其在 ethernet3 (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，创建两个 DIP 池 （一个在每个 VSD 组的 Untrust 区段 VSI 上），并将两个 DIP 池结合成一个 DIP 组，以在策略中引用。即使策略指定 DIP 组，每个 VSI 仍使用其自己的 VSD 池。

在 NSRP 集群中时，策略中 DIP 组的推荐用法：
set policy name out-nat from trust to untrust any any 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，不是引用接口特定的 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 7 卷，“NSRP”。*

范例：DIP 组

在本例中，在双活动 HA 对的两个 NetScreen 设备 （设备 A 和 B）上提供 NAT 服务。

创建两个 DIP 池 — ethernet3 上的 DIP 5 (210.1.1.20 – 210.1.1.29)， ethernet3:1 上的 DIP 6 (210.1.1.30 – 210.1.1.39)。然后将它们组合成一个 DIP 组并标识为 DIP 7，在策略中引用。

VSD 组 0 和 1 的 VSI 如下：

- Untrust 区段 VSI ethernet1 210.1.1.1/24 （VSD 组 0）
- Untrust 区段 VSI ethernet1:1 210.1.1.2/24 （VSD 组 1）
- Trust 区段 VSI ethernet3 10.1.1.1/24 （VSD 组 0）
- Trust 区段 VSI ethernet3:1 10.1.1.1/24 （VSD 组 1）

本例假设已设置 NSRP 集群中的设备 A 和 B，创建 VSD 组 1（将设备置入 NSRP 集群时，NetScreen 自动创建 VSD 组 0），并配置上述接口。（有关为 NSRP 配置 NetScreen 设备的信息，请参阅*第 7 卷，“NSRP”*。）

WebUI

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

   ID: 5

   IP Address Range:

   Start: 210.1.1.20

   End: 210.1.1.29

   Port Translation:（选择）

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

   ID: 6

   IP Address Range:

   Start: 210.1.1.30

   End: 210.1.1.39

   Port Translation:（选择）

注意：本版发行时，只能通过 CLI 定义 DIP 组。

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（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:（选择）

   DIP On:（选择）, 7

CLI

1. set interface ethernet1 dip 5 210.1.1.20 210.1.1.29
2. set interface ethernet1:1 dip 6 210.1.1.30 210.1.1.39
3. set dip group 7 member 5
4. set dip group 7 member 6
5. set policy from trust to untrust any any any nat dip-id 7 permit
6. save

附着 DIP 地址

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

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

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

5

接口模式

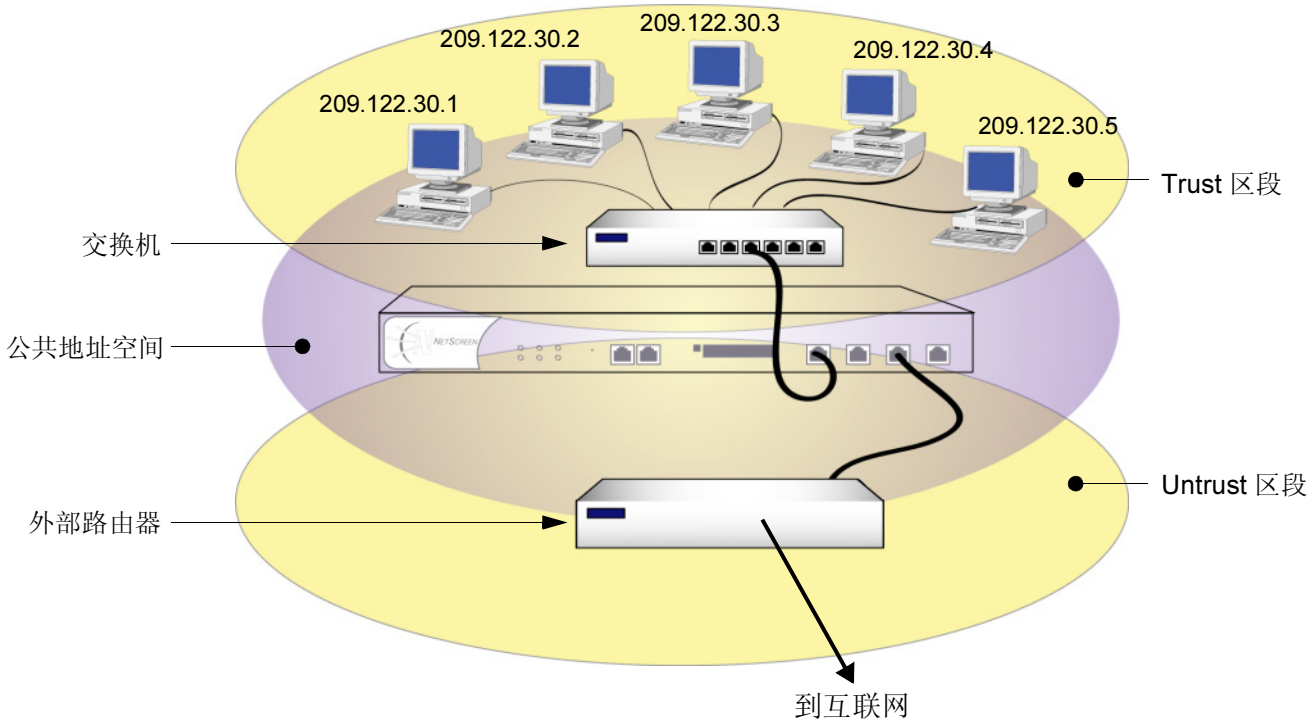
接口能以三种不同模式运行，分别是：网络地址转换 (NAT)、路由和透明。如果绑定到 Layer 3 （第 3 层）区段的接口具有 IP 地址，则可为该接口定义 NAT[1] 或路由操作模式。绑定到 Layer 2 （第 2 层）区段 （如预定义的 v1-trust、v1-untrust 和 v1-dmz，或用户定义的 Layer 2（第 2 层）区段）的接口必须为透明模式。在配置接口时选择操作模式。

本章包括以下部分：

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

透明模式

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



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

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

接口设置

NetScreen 设备处于透明模式时，必须使用 VLAN1 接口来管理设备和终止 VPN 信息流。缺省情况下，ScreenOS 会始终创建一个 VLAN1 接口和三个 VLAN1 区段：V1-Trust、 V1-Untrust、 V1-DMZ。

VLAN1 接口

VLAN1 接口具有与物理接口相同的配置和管理能力。

可将 VLAN1 接口配置为允许 VLAN1 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 V1 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。

VLAN1 区段

VLAN1 区段也称为 Layer 2 （第 2 层）安全区段，因为它们共享同一第 2 层域。在某个 VLAN1 区段中配置接口时，它被添加到由所有 VLAN1 区段中的所有接口共享的第 2 层域中。

VLAN1 区段中的所有主机必须在同一子网中通信，而且必须定义允许主机在区段间通信的策略。有关如何设置策略的详细信息，请参阅第 215 页上的 “策略”。

注意：*要了解哪个物理接口被预先绑定到每个 NetScreen 平台的 VLAN1 区段，请参阅该平台的安装程序指南。*

未知 Unicast 选项

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

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

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

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

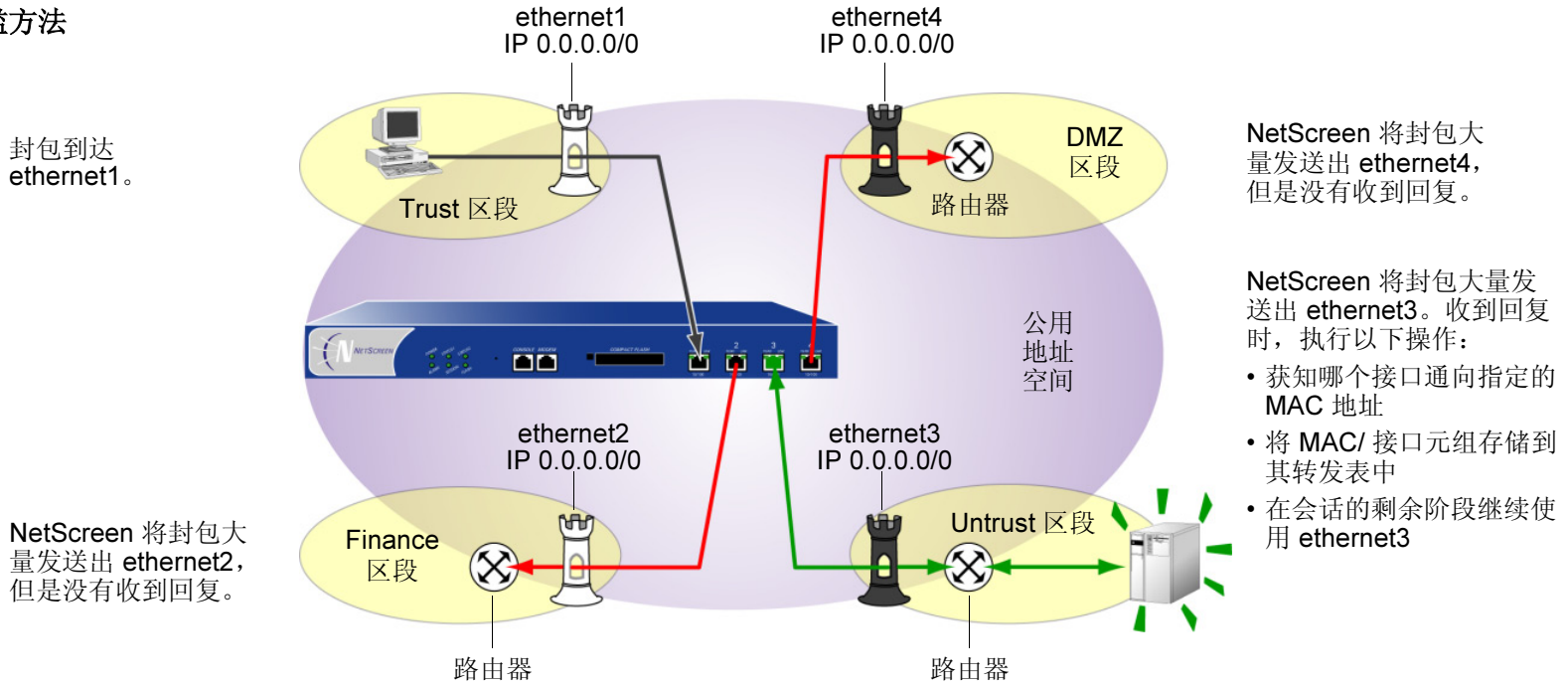
> ***注意：****泛滥和 ARP/trace-route 这两种方法中， ARP/trace-route 更安全，因为 NetScreen 设备将 ARP 查询和 trace-route 封包 （而非初始封包）大量发送出所有接口。*

泛滥方法

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

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

泛滥方法



要启用泛滥方法来处理未知的 unicast 封包，请执行以下操作之一：

WebUI

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

CLI

1. set interface vlan1 broadcast flood
2. save

ARP/Trace-Route 方法

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

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

   如果目的地 IP 地址属于与入口 IP 地址[3] 在同一子网中的设备，则主机返回一条带有其 MAC 地址的 ARP 回复 (arp-r)，从而指示出 NetScreen 设备必须通过它转发以该地址为目的地的信息流的接口。（请参阅第 150 页上的 “ARP 方法”。）

2. 启用 ARP 方法时，缺省情况下 trace-route 选项启用。也可启用不带 trace-route 选项的 ARP 方法。但是，如果目的地 IP 地址与入口 IP 地址在同一子网中，则该方法只允许 NetScreen 设备发现 unicast 封包的目的地 MAC 地址。（关于入口 IP 地址的详细信息，请参阅下一脚注。）
3. 入口 IP 地址指将封包发送到 NetScreen 设备的最后设备的 IP 地址。此设备可能是发送封包的源，或者是转发封包的路由器。

如果目的地 IP 地址属于入口 IP 地址所在子网外的其它子网中的设备，则 trace-route 返回通向目的地[4] 的路由器的 IP 和 MAC 地址，尤其重要的是，指出了 NetScreen 设备必须通过它转发流向该 MAC 地址的信息流的接口。（请参阅第 151 页上的 “Trace-Route”。）

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

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

WebUI

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

CLI

1. set interface vlan1 broadcast arp
2. save

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

4. 实际上，trace-route 返回子网中所有路由器的 IP 和 MAC 地址。NetScreen 设备于是将初始封包的目的地 MAC 地址与 arp-r 封包中的源 MAC 地址相匹配，来确定指向哪个路由器，并进而确定使用哪个接口到达该目的地。

ARP 方法

注意：*以下仅显示封包包头的相关元素和 MAC 地址中的最后四位数字。*

如果下列封包

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

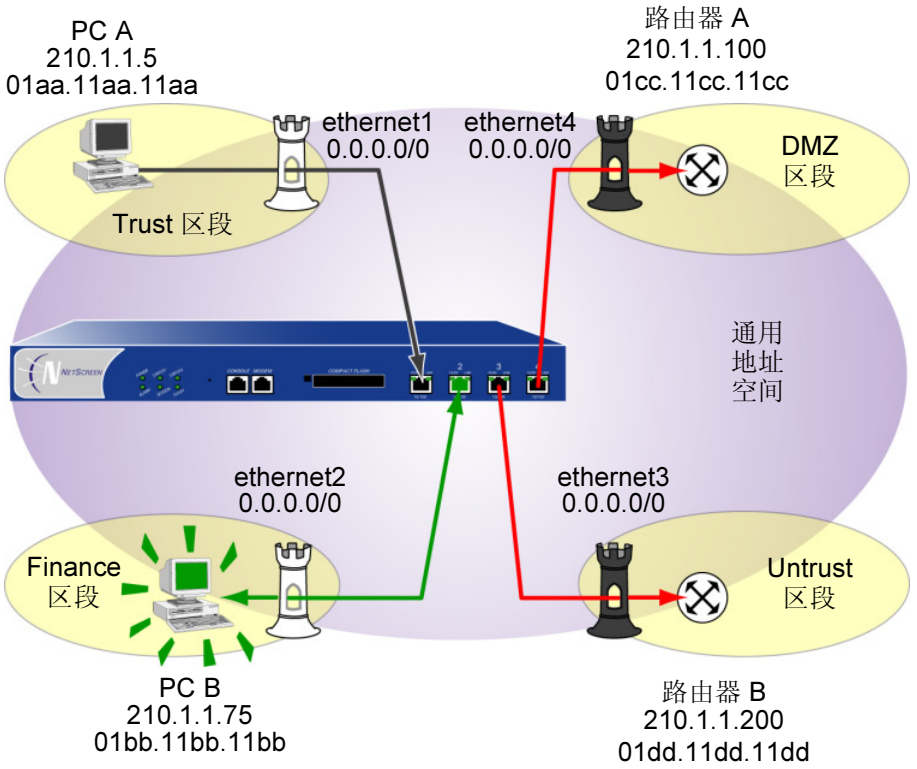
到达 ethernet1，并且转发表中没有 MAC 地址 11bb.11bb.11bb 的条目，NetScreen 设备将以下 arp-q 封包大量发送出 eth2、 eth3 和 eth4。

以太网帧			ARP 消息	
目的地	源	类型	源	目的地
ffff	11aa	0806	210.1.1.5	210.1.1.75

当 NetScreen 设备在 eth2 收到以下 arp-r 时，

以太网帧			ARP 消息	
目的地	源	类型	源	目的地
11aa	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。



Trace-Route

注意：*以下仅显示封包包头的相关元素和 MAC 地址中的最后四位数字。*

如果下列封包

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

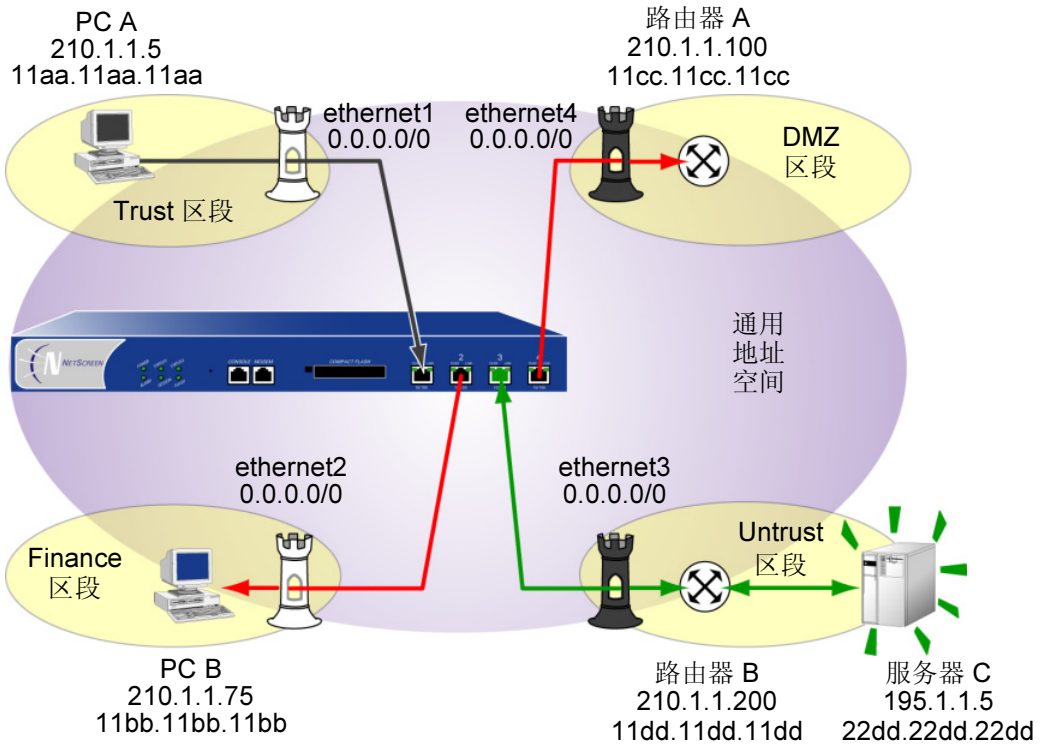
到达 ethernet1，并且转发表中没有 MAC 地址 11dd.11dd.11dd 的条目，NetScreen 设备将以下 trace-route 封包大量发送出 eth2、 eth3 和 eth4。

以太网帧			ICMP 消息		
目的地	源	类型	源	目的地	TTL
ffff	11aa	0806	210.1.1.5	195.1.1.5	1

NetScreen 设备在 eth3 收到以下回应时，

以太网帧			ICMP 消息		
目的地	源	类型	源	目的地	消息
11aa	11dd	0806	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。



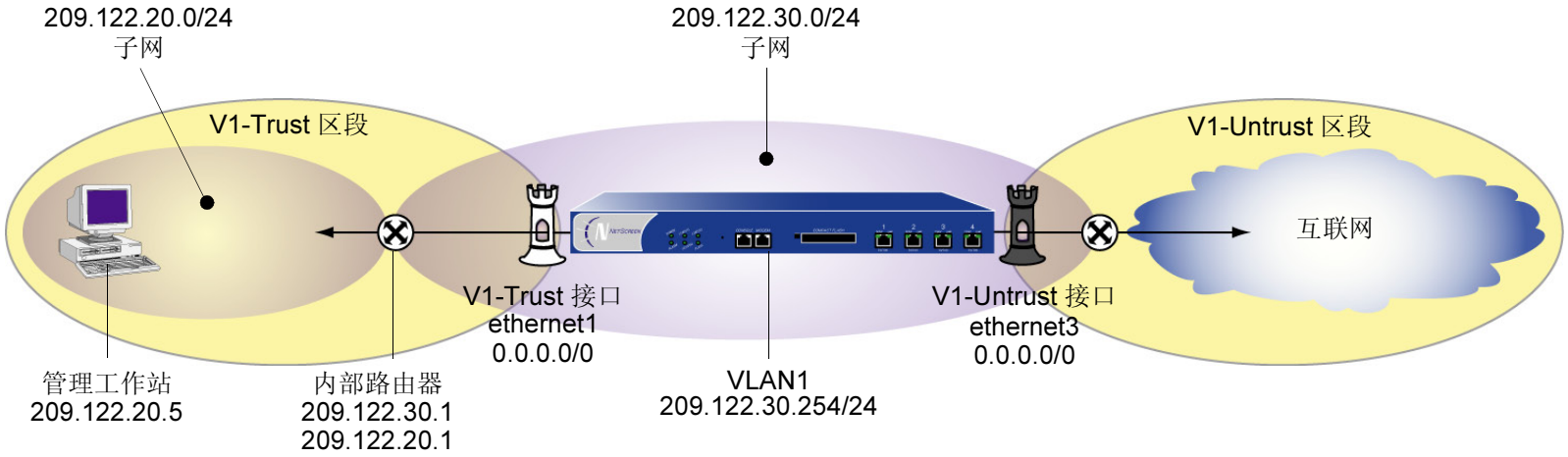
范例：定义 VLAN1 接口

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

- 为 VLAN1 接口分配 IP 地址 209.122.30.254/24。
- 在 VLAN1 和 V1-Trust[5] 接口上启用 Web、 Telnet、 SCS 和 Ping。

  注意：*要从 Layer 2（第 2 层）安全区段管理设备，必须在 VLAN1 接口和 Layer 2（第 2 层）安全区段接口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 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。



5. 缺省情况下， NetScreen 启用 VLAN1 和 V1-Trust 接口的管理选项。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. Network > Interfaces > Edit（对于 VLAN1）：输入以下内容，然后单击 **OK**：

   IP Address/Netmask: 209.122.30.254/24

   Management Services: WebUI, Telnet, SCS （选择）

   Other Services: Ping （选择）

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

   Management Services: WebUI, Telnet, SCS

   Other Services: Ping

3. Network > Routing > Routing Table：单击 **Remove**，删除从 trust-vr 到 untrust-vr、将信息流引导到 IP/Netmask 0.0.0.0/0 的缺省路由。

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

   Network Address/Netmask: 209.122.20.0/24

   Gateway: （选择）

   Interface: vlan1(trust-vr)

   Gateway IP Address: 209.122.30.1

   Metric: 1

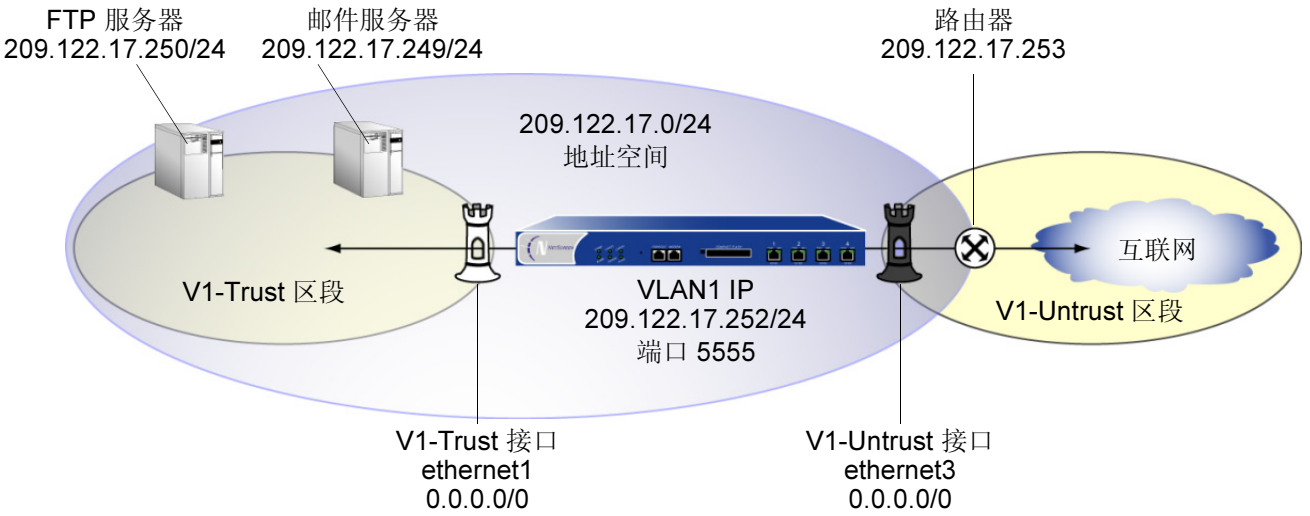
CLI

1. set interface vlan1 ip 209.122.30.254/24
2. set interface vlan1 manage web
3. set interface vlan1 manage telnet
4. set interface vlan1 manage scs
5. set interface vlan1 manage ping
6. set interface v1-trust manage web
7. set interface v1-trust manage telnet
8. set interface v1-trust manage scs
9. set interface v1-trust manage ping
10. unset vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
11. set vrouter trust-vr route 209.122.20.0/24 interface vlan1 gateway 209.122.30.1 metric 1
12. 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 5555。使用 VLAN1 IP 地址 209.122.17.252/24 来管理 V1-Trust 安全区段的设备。也可配置到外部路由器的缺省路由（于 209.122.17.253 处），以便 NetScreen 设备能向其发送出站 VPN 信息流。（V1-Trust 区段中所有设备的缺省网关也是 209.122.17.253。）



WebUI

管理设置和接口

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

   IP Address/Netmask: 209.122.17.252/24

   Management Services: WebUI, Telnet （选择）

   Other Services: Ping （选择）

2. Configuration > Admin > Management：在“HTTP Port”字段中，键入 5555[6]，然后单击 **Apply**。

6. 缺省端口号为 80。建议将此号码改为 1024 和 32,767 间的数值，以阻止对配置的未授权访问。以后登录以管理设备时，请在 Web 浏览器的 URL 区输入以下内容：http://209.122.17.252:5555。

3. 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
4. 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
5. Network > Interfaces > Edit（对于 v1-trust）：选择以下内容，然后单击 **OK**：
   Management Services: WebUI, Telnet
   Other Services: Ping

路由

6. Network > Routing > Routing Table > 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: 209.122.17.253
      Metric: 1

地址

7. 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: 209.122.17.249/32
   Zone: Trust
8. 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: 209.122.17.250/32
   Zone: Trust

策略

9. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择）, Any
   Destination Address:
   Address Book: （选择）, Any
   Service: Any
   Action: Permit
10. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择）, Any
    Destination Address:
    Address Book: （选择）, Mail Server
    Service: Mail
    Action: Permit

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

    Source Address:

    Address Book: （选择）, Any

    Destination Address:

    Address Book: （选择）, FTP Server

    Service: FTP-Get

    Action: Permit

CLI

管理设置和接口

1. set interface vlan1 ip 209.122.17.252
2. set interface vlan1 manage web
3. set interface vlan1 manage telnet
4. set interface vlan1 manage ping
5. set admin telnet port 5555[7]
6. set interface ethernet1 ip 0.0.0.0/0
7. set interface ethernet1 zone v1-trust
8. set interface ethernet3 ip 0.0.0.0/0
9. set interface ethernet3 zone v1-untrust
10. set interface v1-trust manage web
11. set interface v1-trust manage telnet
12. set interface v1-trust manage ping

7. Telnet 的缺省端口号为 23。建议将此号码改为介于 1024 和 32,767 间的数值，以阻止对配置的未授权访问。以后登录 Telnet 来管理设备时，输入以下地址：209.122.17.252 5555

路由

13. set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 209.122.17.253 metric 1

地址

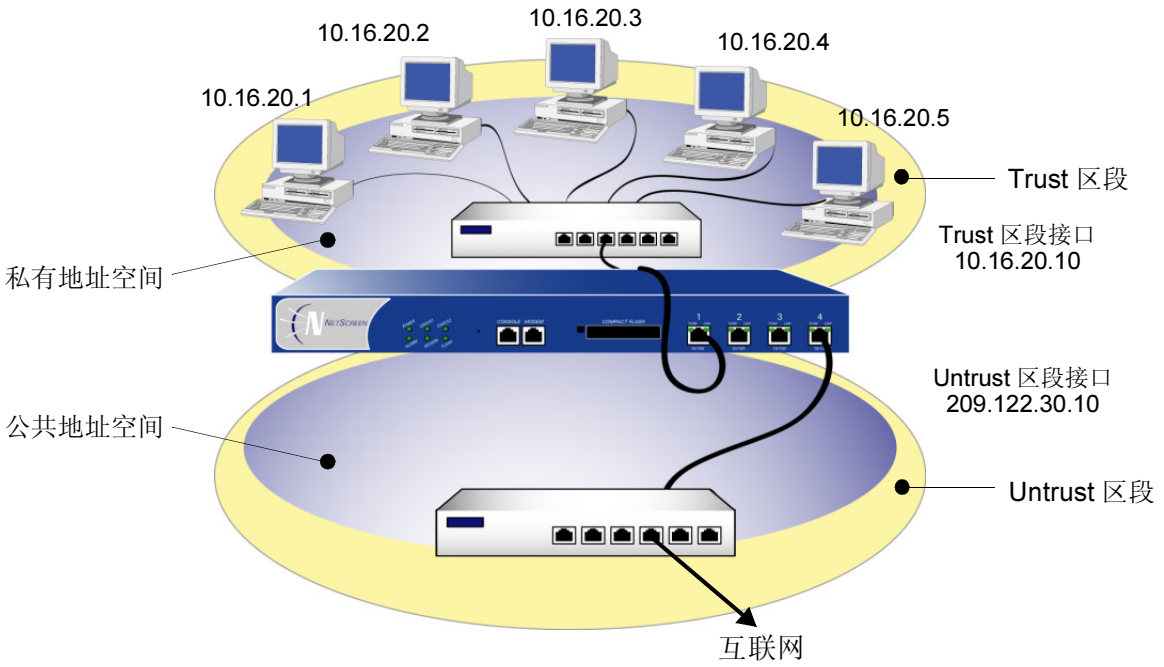
14. set address v1-trust Mail_Server 209.122.17.249/24
15. set address v1-trust FTP_Server 209.122.17.250/24

策略

16. set policy from v1-trust to v1-untrust any any any permit
17. set policy from v1-untrust to v1-trust any Mail_Server mail permit
18. set policy from v1-untrust to v1-trust any FTP_Server ftp-get permit
19. save

NAT 模式

接口处于 “网络地址转换 (NAT)” 模式下时， NetScreen 设备的作用与 Layer 3 （第 3 层）交换机 （或路由器）相似，将绑定到 Untrust 区段的 IP 封包包头中的两个组件进行转换：其源 IP 地址和源端口号。 NetScreen 设备用目的地区段接口的 IP 地址替换发送封包的主机的源 IP 地址。另外，它用另一个由 NetScreen 设备生成的任意端口号替换源端口号。



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

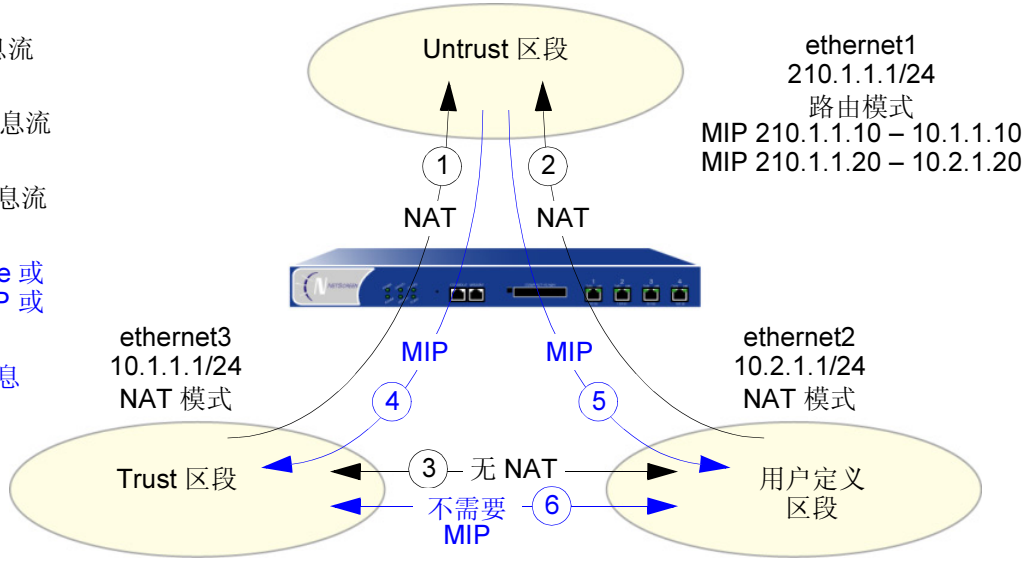
NAT 添加透明模式中未提供的一个安全级别：连接到 NAT 模式接口的主机的地址对Untrust 区段中的主机从不公开。

另外， NAT 还保留对互联网可路由的 IP 地址的使用。只用一个公共、互联网可路由的 IP 地址（Untrust 区段中的接口的 IP 地址）时， Trust 区段或任意使用 NAT 服务的其它区段中的 LAN 可拥有具有私有 IP 地址的大量主机。以下 IP 地址范围保留给私有 IP 网络，并且不必在互联网上设定路由：

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

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（如果策略允许），但是不能够接收来自 Untrust 区段的信息流，除非为其设置了映射 IP (MIP)、虚拟 IP (VIP) 或 VPN 通道。从 Untrust 区段外的其它任意区段向拥有已启用 NAT 的接口的区段发送信息流时，不需要使用 MIP、 VIP 或 VPN。如果要保护某区段内地址的私密性，可定义 MIP 并为该区段创建一个策略，将该 MIP 引用为目的地地址。

1. 从 Trust Zone 到 Untrust Zone 的信息流上的基于接口的 NAT。
2. 从用户定义区段到 Untrust Zone 的信息流上的基于接口的 NAT。
3. Trust Zone 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. 从 Untrust Zone 到达 Trust Zone 或用户定义区段的信息流需要 MIP、VIP 或 VPN。
6. Trust Zone 和用户定义区段之间的信息流***不***需要 MIP、 VIP 或 VPN。



注意： *有关 MIP 的详细信息，请参阅第 99 页上的 “映射 IP 地址”。有关 VIP 的详细信息，请参阅第 113 页上的 “虚拟 IP 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 的信任、 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。

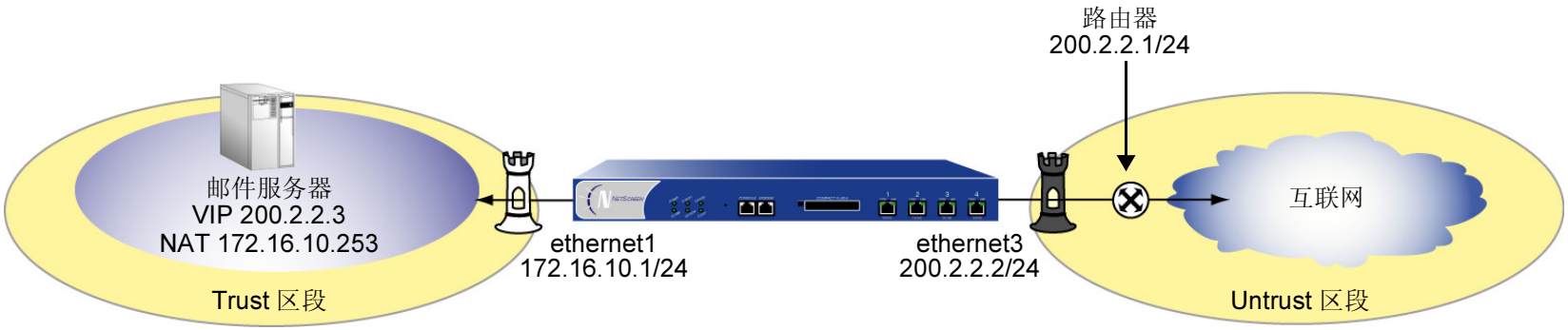
[‡] 选择 NAT 可将接口模式定义为 NAT。选择 “路由”可将接口模式定义为 “路由”。

[**] 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 169 页上路由模式的范例比较。*



WebUI

接口

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

   Zone Name: Trust

   IP Address/Netmask: 172.16.10.1/24

   输入以下内容，然后单击 **OK**：

   NAT:[8]（选择）

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

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

   Zone Name: Untrust

   IP Address[9] /Netmask: 200.2.2.2/24

VIP

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

   Virtual IP Address: 200.2.2.3

4. 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: 172.16.10.253

路由

5. Network > Routing > Routing Table > 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: 200.2.2.1

9. 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 DHCP。如果 ISP 使用 “以太网点对点传输协议”，则选择 PPPoE 并输入名称和密码。

策略

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

   Source Address:

   Address Book: （选择）, Any

   Destination Address:

   Address Book: （选择）, Any

   Service: Any

   Action: Permit

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

   Source Address:

   Address Book: （选择）, Any

   Destination Address:

   Address Book: （选择）, VIP(200.2.2.3)

   Service: Mail

   Action: Permit

CLI

接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.16.10.1/24
3. set interface ethernet1 NAT[10]
4. set interface ethernet3 zone untrust[11]
5. set interface ethernet3 ip 200.2.2.2/24

VIP

6. set vip ethernet3 200.2.2.3 25 mail 172.16.10.253

路由

7. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 200.2.2.1

策略

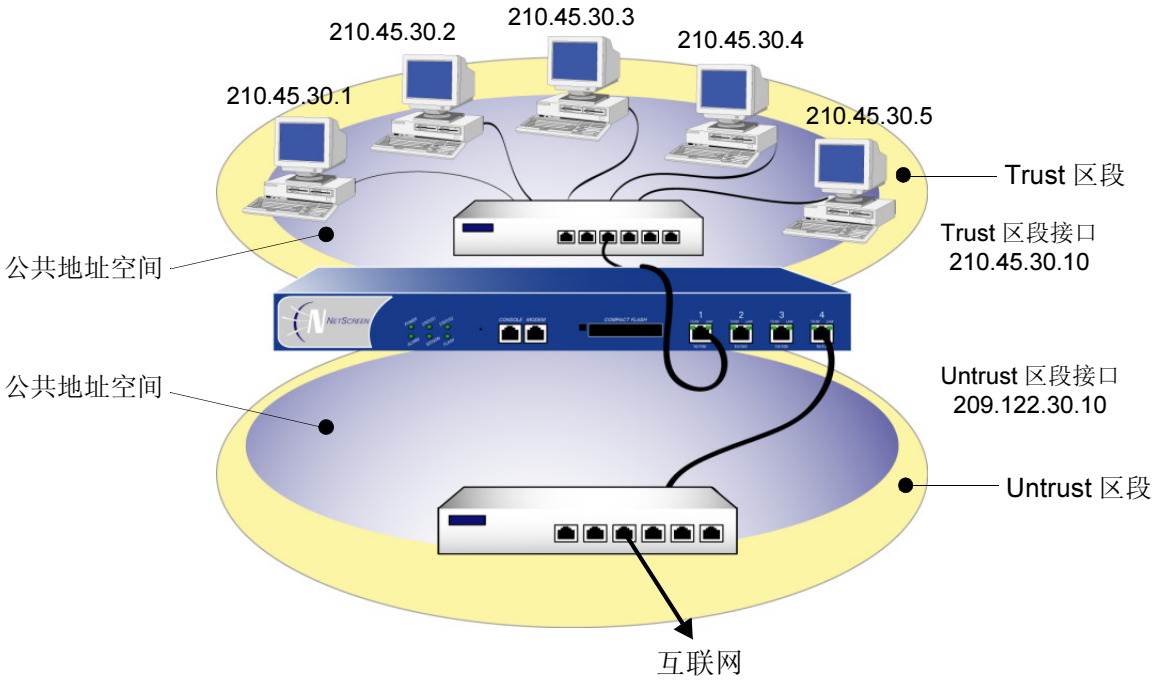
8. set policy from trust to untrust any any any permit
9. set policy from untrust to trust any “vip 200.2.2.3” mail permit
10. save

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

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

路由模式

接口为路由模式时，NetScreen 设备在不同区段间转发信息流时不执行 NAT ； 即，当信息流穿过 NetScreen 设备时，IP 封包包头中的源地址和端口号保持不变。与 NAT 不同，不需要为了允许入站会话到达主机而建立路由模式接口的映射和虚拟 IP 地址。与透明模式不同， Trust 区段中的接口和 Untrust 区段中的接口在不同的子网中。



接口运行在路由模式时，可在策略级选择性地执行 NAT，而不是在接口级应用 NAT （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接口的 IP 地址）。通过为内向或外向信息流上的指定源地址创建启用 NAT 的策略，可确定要确定路由的网络和 VPN 信息流，以及对哪些信息流执行 NAT。对于网络信息流，可使用

IP 地址或动态 IP (DIP) 池的目的地区段接口地址来执行 NAT，动态 IP 池与目的地区段接口在同一子网中。对于 VPN 信息流，可使用目的地区段接口 IP 地址或其相关 DIP 池的地址，或者通道接口 IP 地址或其相关 DIP 池的地址，来执行 NAT。

注意：*关于配置基于策略的 NAT 的详细信息，请参阅**第 173 页上的 “基于策略的 NAT”**。*

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）

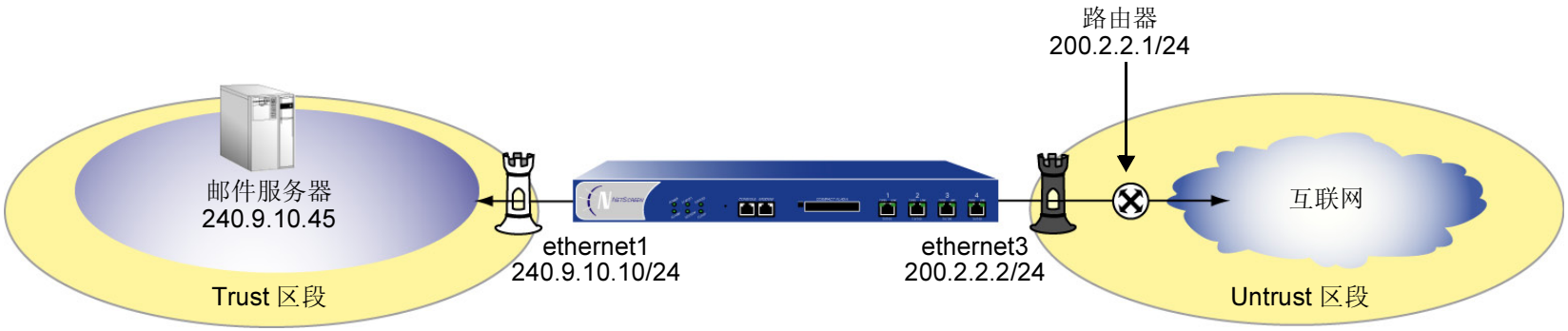
[*] 可在每个接口的基础上设置管理 IP 地址。主要目的是为从网络信息流中分离出来的管理信息流提供 IP 地址。当某特定设备具备高可用性配置时，也可使用管理 IP 地址来访问它。

[†] 用于信息流整型的可选设置。

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

范例：路由模式

在上一范例第 163 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

接口

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

   Zone Name: Trust

   IP Address/Netmask: 240.9.10.10/24

   输入以下内容，然后单击 **OK**：

   Route[12]：（选择）

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

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

   Zone Name: Untrust

   IP Address[13] /Netmask: 200.2.2.2/24

地址

3. 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: 240.9.10.45/32

   Zone: Trust

路由

4. Network > Routing > Routing Table > 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(untrust-vr)

   Gateway IP Address: 200.2.2.1

13. 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 DHCP。如果 ISP 使用 “以太网点对点传输协议”，则选择 PPPoE 并输入名称和密码。

策略

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

   Source Address:

   Address Book: （选择）, Any

   Destination Address:

   Address Book: （选择）, Any

   Service: Any

   Action: Permit

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

   Source Address:

   Address Book: （选择）, Any

   Destination Address:

   Address Book: （选择）, Mail Server

   Service: Mail

   Action: Permit

CLI

接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 240.9.10.10/24
3. set interface ethernet1 route[14]
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 200.2.2.2/24

地址

6. set address trust mail_server 240.9.10.45/24

路由

7. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 200.2.2.1

策略

8. set policy from trust to untrust any any any permit
9. set policy from untrust to trust any mail_server mail permit
10. save

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

基于策略的 NAT

本部分描述了基于策略的 NAT 以及它如何使用 “动态 IP (DIP)” 池和 “映射 IP (MIP)” 地址。虽然在接口级或策略级[15] 都可应用 “网络地址转换 (NAT)”，但本部分仅针对策略级应用。

注意：*关于 NAT 接口级应用的详细信息，请参阅第 160 页上的 “NAT 模式”。有关 MIP 的信息，请参阅第 99 页上的 “映射 IP 地址”。*

网络信息流的基于策略的 NAT

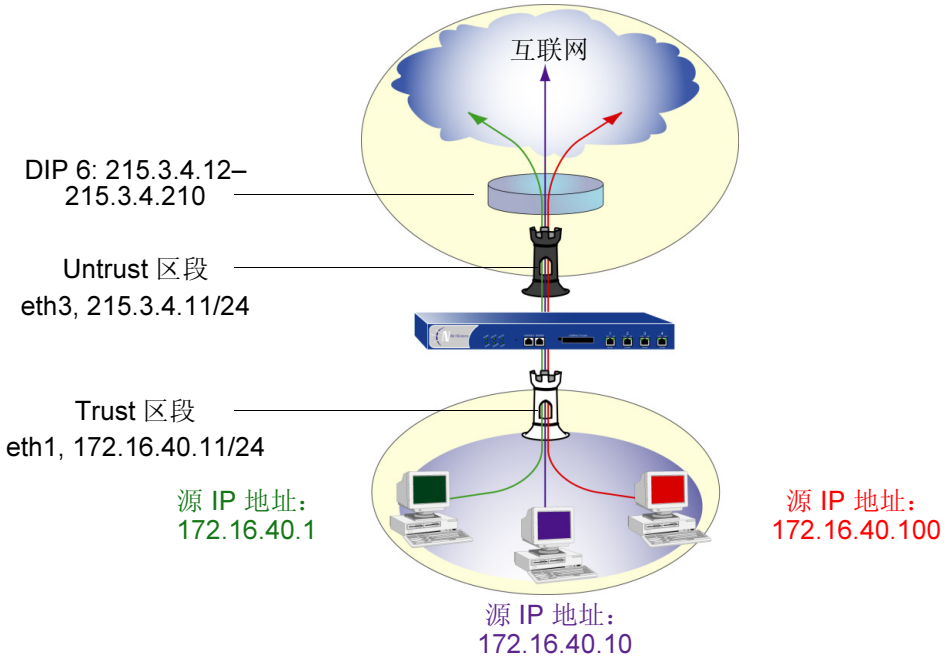
可使用 Untrust 区段中接口的 DIP 池，来转换外向网络信息流上的源地址。从 IP 地址池应用 NAT 会使 Untrust 区段中接口的实际 IP 地址难于辨识，增加了任何人将其作为攻击目标的难度。

注意：*关于 VPN 信息流的基于策略的 NAT 的信息和范例，请参阅第 **4**-202 页上的 “Tunnel 区段和基于策略的 NAT”。*

15. 对于路由模式或 NAT 模式下的 NetScreen 设备，可使用基于策略的 NAT。当 NetScreen 设备处于 NAT 模式时，策略级 NAT 参数将取代接口级 NAT 参数。例如， NetScreen 设备为 NAT 模式时，可在策略中指定一个并非链接到不可信接口的 DIP 池。

范例：外向网络信息流上的 NAT

在本例中，将使用 Untrust 区段中接口上的 DIP 池对外向网络信息流执行 NAT。Untrust 区段中 NetScreen 设备的 IP 地址为 215.3.4.11/24。 DIP 池中的地址范围为 215.3.4.12 到 215.3.4.210。



WebUI

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

   Zone Name: Trust

   IP Address/Netmask: 172.16.40.11/24

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 215.3.4.11/24
3. Network > Interfaces > Edit（对于 ethernet3）> DIP > New：输入以下内容，然后单击 **OK**：
   ID: 6
   IP Address Range
   Start: 215.3.4.12
   End: 215.3.4.210
   Port Translation: Enable
4. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择）, Any
   Destination Address:
   Address Book: （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: On
   DIP On: （选择）, 6 (215.3.4.12–215.3.4.210)

CLI

1. set interface ethernet3 zone untrust
2. set interface ethernet3 ip 215.3.4.11/24
3. set interface ethernet3 dip 6 215.3.4.12 215.3.4.210
4. set policy from untrust to trust any any nat dip 6 any permit
5. save

6

为策略构建块

本章论述了策略和 “虚拟专用网 (VPN)” 都适用的概念。讨论的具体主题如下：

> ***注意：****有关用户认证的信息，请参阅第 8 章，第 249 页上的 “用户认证”。*

地址

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

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

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

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

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

地址条目

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

范例：添加地址

在本例中，将 IP 地址为 192.10.10.0/24 的子网 “Santa Clara Eng”添加为 Trust 区段中的地址，并将地址 www.firenet.com 添加为 Untrust 区段中的地址。

WebUI

1. Objects > Addresses > List > New：输入以下信息，然后单击 **OK**：
   Address Name: Santa Clara Eng
   IP Address/Domain Name:
   IP/Netmask: 192.10.10.0/24
   Zone: Trust （选择）
2. Objects > Addresses > List > New：输入以下信息，然后单击 **OK**：
   Address Name: FireNet
   IP Address/Domain Name:
   Domain Name: www.firenet.com
   Zone: Untrust （选择）

1. 必须为 NetScreen 设备配置 “域名系统 (DNS)”服务，才能使用地址条目的域名。有关 DNS 配置的信息，请参阅第 370 页上的 “域名系统支持”。

CLI

1. set address trust “Santa Clara Eng” 192.10.10.0 255.255.255.0
2. set address untrust www.firenet.com 255.255.255.255
3. save

范例：修改地址

在本例中，将更改主机 “Santa Clara Eng”的地址条目，以反映此主机已被移动到 Dallas，并已被重新指定 IP 地址 192.10.40.0/24。

WebUI

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

Address Name: Dallas Eng

IP Address/Domain Name:

IP/Netmask: 192.10.40.0

CLI

1. unset address trust “Santa Clara Eng”
2. set address trust “Dallas Eng” 192.10.40.0 255.255.255.0
3. save

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

范例：删除地址

在本例中，将移除子网 “Dallas Eng”的地址条目。

WebUI

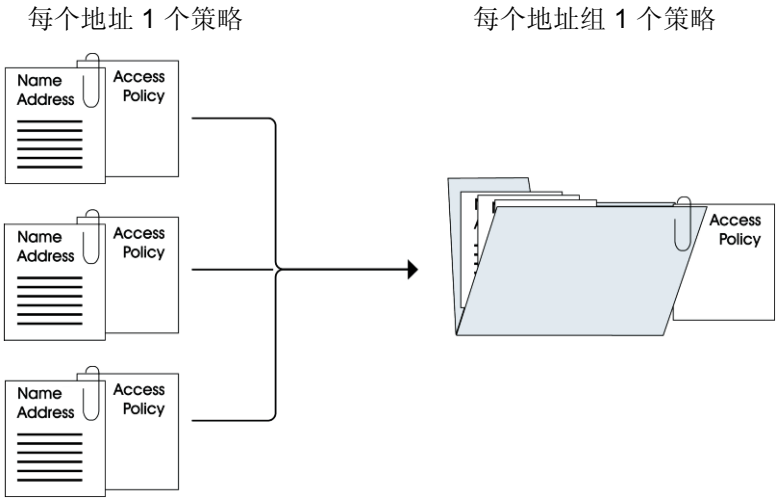
Objects > Addresses > List：在 Dallas Eng 的配置栏中，单击 **Remove**。

CLI

1. unset address trust “Dallas Eng”
2. save

地址组

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



地址组选项具有下列功能：

- 可以在任何区段中创建地址组。
- 可以创建有现有用户的地址组，或者可以创建空的地址组并在以后使用用户填充它们。
- 地址组条目可以像单个通讯簿条目一样使用。
- NetScreen 通过在内部为每个组成员创建单个策略，将策略应用到组的每个成员。只需为组创建一个策略，NetScreen 实际上为组中的每个成员（以及为每个用户配置的每项服务）都创建了一个内部策略。[2]
- 从通讯薄中删除单个通讯簿条目时，也从所有引用它的组中将它移除。

地址组适用以下限制：

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

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

范例：创建地址组

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

WebUI

Objects > Addresses > Group >（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

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

范例：编辑组地址条目

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

WebUI

Objects > Addresses > Group >（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

1. set group address trust “HQ 2nd Floor” add Support
2. save

范例：移除地址组成员和组

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

WebUI

1. Objects > Addresses > Group >（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。

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

CLI

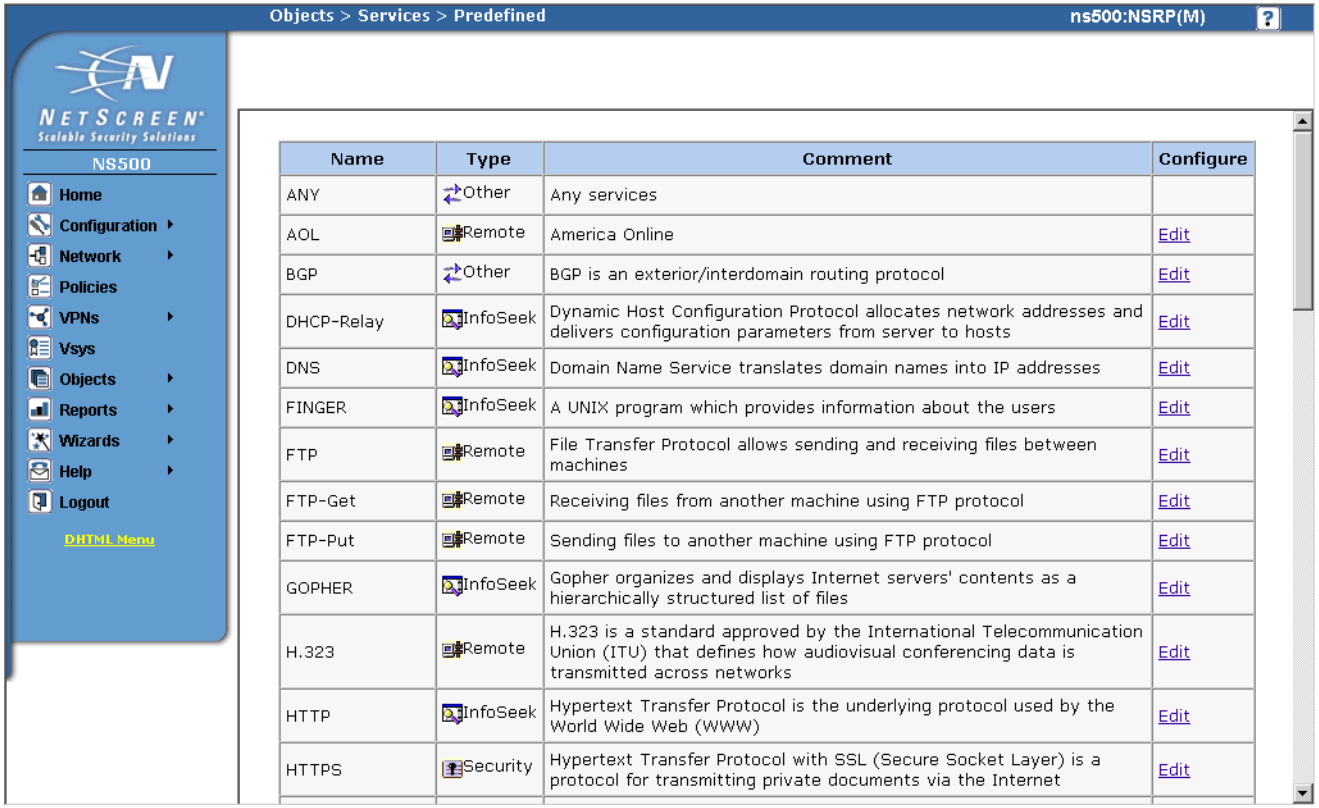
1. unset group address trust “HQ 2nd Floor” remove Support
2. unset group address trust Sales
3. save

注意：*NetScreen 设备不会自动删除已经移除其中所有名称的组。*

服务

服务是 IP 信息流的类型，它们有相应的协议标准。每个服务都有一个端口号与之相关联，如 FTP 的端口号为 21，Telnet 的端口号为 23。本节是可用服务的概述，并且不深入说明其中每一项（第 190 页上的“IP 语音通信的 H.323 协议”除外）。

下图说明了本版 ScreenOS 支持的预定义服务的局部视图。



Name	Type	Comment	Configure
ANY	Other	Any services	
AOL	Remote	America Online	Edit
BGP	Other	BGP is an exterior/interdomain routing protocol	Edit
DHCP-Relay	InfoSeek	Dynamic Host Configuration Protocol allocates network addresses and delivers configuration parameters from server to hosts	Edit
DNS	InfoSeek	Domain Name Service translates domain names into IP addresses	Edit
FINGER	InfoSeek	A UNIX program which provides information about the users	Edit
FTP	Remote	File Transfer Protocol allows sending and receiving files between machines	Edit
FTP-Get	Remote	Receiving files from another machine using FTP protocol	Edit
FTP-Put	Remote	Sending files to another machine using FTP protocol	Edit
GOPHER	InfoSeek	Gopher organizes and displays Internet servers' contents as a hierarchically structured list of files	Edit
H.323	Remote	H.323 is a standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks	Edit
HTTP	InfoSeek	Hypertext Transfer Protocol is the underlying protocol used by the World Wide Web (WWW)	Edit
HTTPS	Security	Hypertext Transfer Protocol with SSL (Secure Socket Layer) is a protocol for transmitting private documents via the Internet	Edit

创建策略时，必须为它指定服务。可以从服务簿中选择一个预配置的服务、创建的定制服务或服务组。通过查看 Policy Configuration 对话框中的 Service 下拉列表 (WebUI)，或使用 **get service** 命令 (CLI)，可以查看能够在策略中使用的服务。

下节提供了查看服务簿以及创建、修改和删除定制服务的范例。

范例：查看服务簿

本例中，将查看服务簿中的预定义和定制服务。

WebUI

1. Objects > Services > Predefined
2. Objects > Services > Custom

CLI

get service

CLI 的输出与如下所示内容类似。

单项服务：

Name	Proto	Port	Group	Timeout	Flag
ANY	0	0/65535	other	0	Predefined
AOL	6	5190/5194	remote	0	Predefined
BGP	6	179	other	0	Predefined
DHCP-Relay	17	67	info seeking	0	Predefined
DNS	17	53	info seeking	0	Predefined
FINGER	6	79	info seeking	0	Predefined

Name	Proto	Port	Group	Timeout	Flag
FTP	6	21	remote	0	Predefined
FTP-Get	6	21	remote	0	Predefined
FTP-Put	6	21	remote	0	Predefined
GOPHER	6	70	info-seeking	0	Predefined
H.323	6	389	remote	0	Predefined
--- more ---					

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 “corp”
- 服务的有效内部端口号范围。例如， 1500-10000。
- 接收服务请求的外部端口号范围；例如， 15000-25000。
- 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**：

Transport Protocol: TCP （选择）
Service Name: corp
Source Port Low: 1500
Source Port High: 1500
Destination Port Low: 15000
Destination Port High: 15000

CLI

1. set service corp protocol tcp src-port 1500-1500 dst-port 15000-55000
2. set service corp timeout 30[3]
3. save

范例：修改定制服务

在本例中，将更改定制服务 *corp*。传输协议从 TCP 更改为 UDP，且源端口的范围更改为 1 到 1000。

使用 **set service** *name_str* **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 > New：输入以下内容，然后单击 **OK**：

Transport Protocol: UDP （选择）
Service Name: corp
Source Port Low: 1
Source Port High: 1000
Destination Port Low: 15000
Destination Port High: 15000

CLI

1. set service corp clear
2. set service corp protocol udp src-port 1-1000 dst-port 15000-15000
3. save

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

范例：移除定制服务

在本例中，将移除定制服务 “corp”。

WebUI

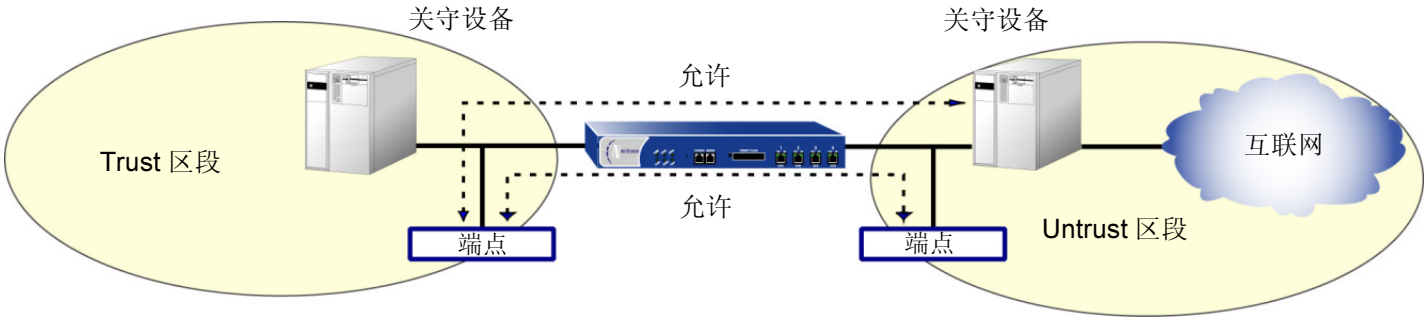
Objects > Services > Custom：在“corp”的 Configure 栏中，单击 **Remove**。

CLI

1. unset service corp
2. save

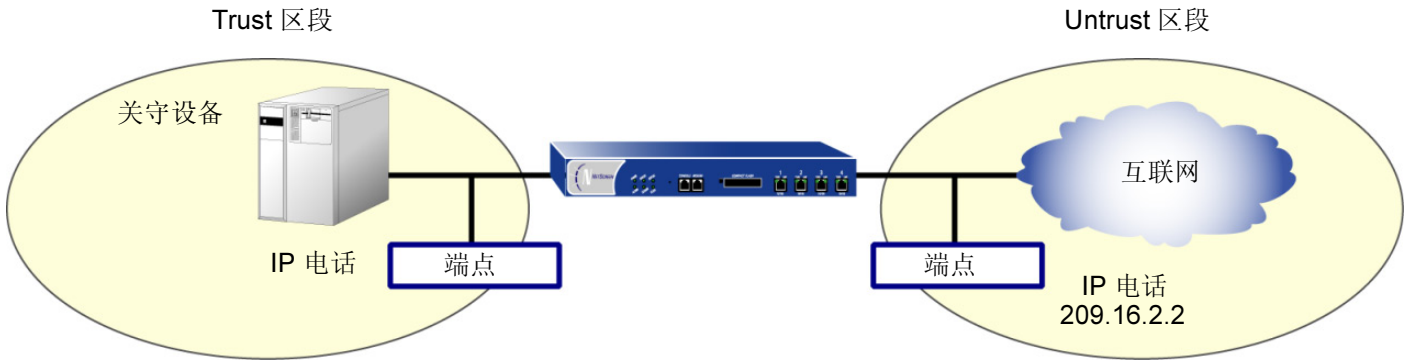
IP 语音通信的 H.323 协议

为了实现终端主机间的安全 IP 语音通信 (VoIP)， NetScreen 设备支持 H.323 协议。在该电话系统中，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。



范例：Trust 区段中的关守设备 （透明或路由模式）

在以下范例中，将设置两个策略。这些策略共同允许 H.323 信息流在 IP 电话主机与Trust 区段的关守设备以及Untrust 区段的 IP 电话主机 (209.16.2.2) 间流动。在本例中， NetScreen 设备可处于透明模式或路由模式。 Trust 和 Untrust 安全区段都在 trust-vr 路由域中。



WebUI

1. 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: 209.16.2.2/32

   Zone: Untrust

2. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , Any
   Destination Address:
   Address Book: （选择） , IP_Phone
   Service: H.323
   Action: Permit
3. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , IP_Phone
   Destination Address:
   Address Book: （选择） , Any
   Service: H.323
   Action: Permit

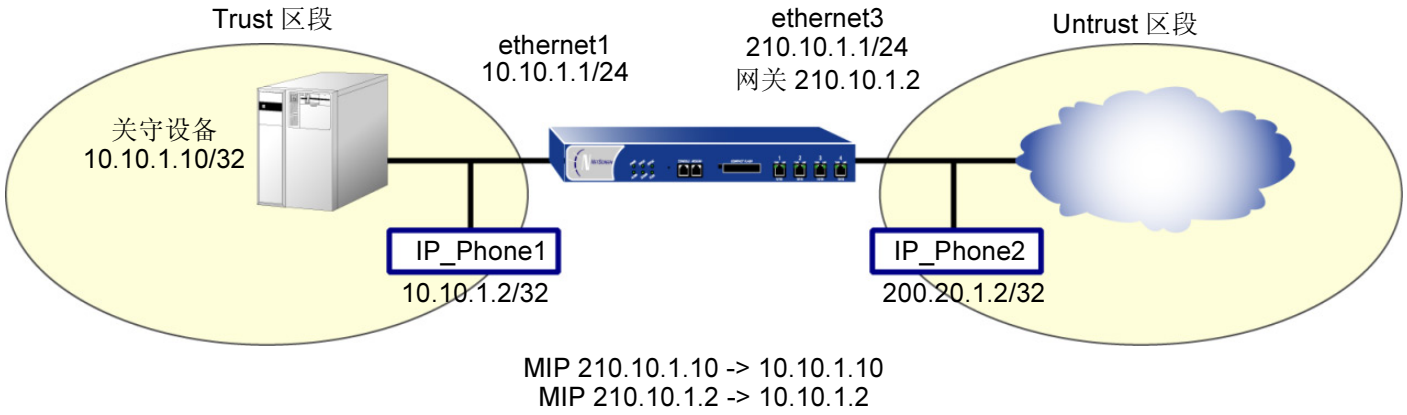
CLI

1. set address untrust IP_Phone 209.16.2.2/32
2. set policy from trust to untrust any IP_Phone h.323 permit
3. set policy from untrust to trust IP_Phone any h.323 permit
4. save

范例：Trust 区段中的关守设备 （NAT 模式）

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

在本例中，Trust 区段中的设备包括端点主机 (10.10.1.2/32) 和关守设备 (10.10.1.10/32)。IP_Phone2 (200.20.1.2/32) 在 Untrust 区段中。配置 NetScreen 设备以允许信息流在端点主机 IP_Phone1 和 Trust 区段中的关守设备，以及 Untrust 区段中的端点主机 IP_Phone2 (210.10.1.2) 间通过。 Trust 和 Untrust 安全区段都在 trust-vr 路由域中。



WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.1.1/24

   输入以下内容，然后单击 **OK**：

   Interface Mode: NAT

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.10.1.1/24

地址

3. 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: 10.10.1.2/32
   Zone: Trust
4. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: Gatekeeper
   IP Address/Domain Name:
   IP/Netmask: 10.10.1.10/32
   Zone: Trust
5. 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: 200.20.1.2/32
   Zone: Untrust

映射 IP 地址

6. Network > Interfaces > Edit（对于 ethernet3）> MIP > New：输入以下内容，然后单击 **OK**：
   Mapped IP: 210.10.1.2
   Netmask: 255.255.255.255
   Host IP Address: 10.10.1.2
   Host Virtual Router Name: trust-vr
7. Network > Interfaces > Edit（对于 ethernet3）> MIP > New：输入以下内容，然后单击 **OK**：
   Mapped IP: 210.10.1.10
   Netmask: 255.255.255.255
   Host IP Address: 10.10.1.10
   Host Virtual Router Name: trust-vr

路由

8. Network > Routing > Routing Table > 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: 210.10.1.2

策略

9. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , IP_Phone1
   Destination Address:
   Address Book: （选择） , Phone2
   Service: H.323
   Action: Permit
10. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , Gatekeeper
   Destination Address:
   Address Book: （选择） , Phone2
   Service: H.323
   Action: Permit
11. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , IP_Phone2
   Destination Address:
   Address Book: （选择） , MIP(210.10.1.10)
   Service: H.323
   Action: Permit

12. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book:（选择）, IP_Phone2
    Destination Address:
    Address Book:（选择）, MIP(210.10.1.2)
    Service: H.323
    Action: Permit

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.1.1/24
3. set interface ethernet1 nat
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 210.10.1.1/24

地址

6. set address trust IP_Phone1 10.10.1.2/32
7. set address trust gatekeeper 10.10.1.10/32
8. set address untrust IP_Phone2 200.20.1.2/32

映射 IP 地址

9. set interface ethernet3 mip 210.10.1.2 host 10.10.1.2
10. set interface ethernet3 mip 210.10.1.10 host 10.10.1.10

路由

11. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.22.3.20

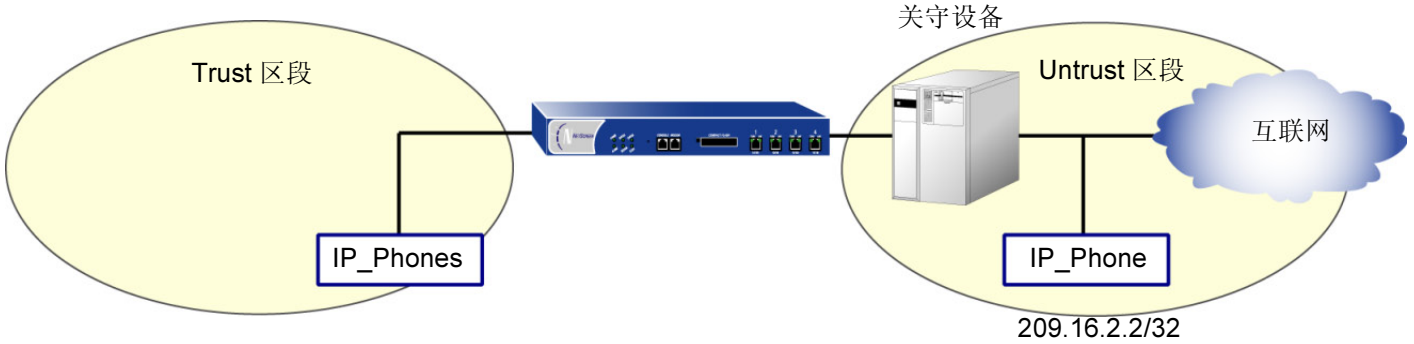
策略

12. set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
13. set policy from trust to untrust gatekeeper IP_Phone2 h.323 permit
14. set policy from untrust to trust IP_Phone2 mip(210.10.1.2) h.323 permit
15. set policy from untrust to trust IP_Phone2 mip (210.10.1.10) h.323 permit
16. save

范例：Untrust 区段中的关守设备 （Trust 区段处于透明或路由模式）

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

在下例中，设置两个允许 H.323 信息流在 Trust 区段中的 IP 电话主机 （和关守设备），与 Untrust 区段中 IP 地址为 209.16.2.2 的 IP 电话间流动的策略。设备可以处于透明或路由模式。Trust 和Untrust 安全区段都在 trust-vr 路由域中。



WebUI

1. 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: 209.16.2.2/32
   Zone: Untrust

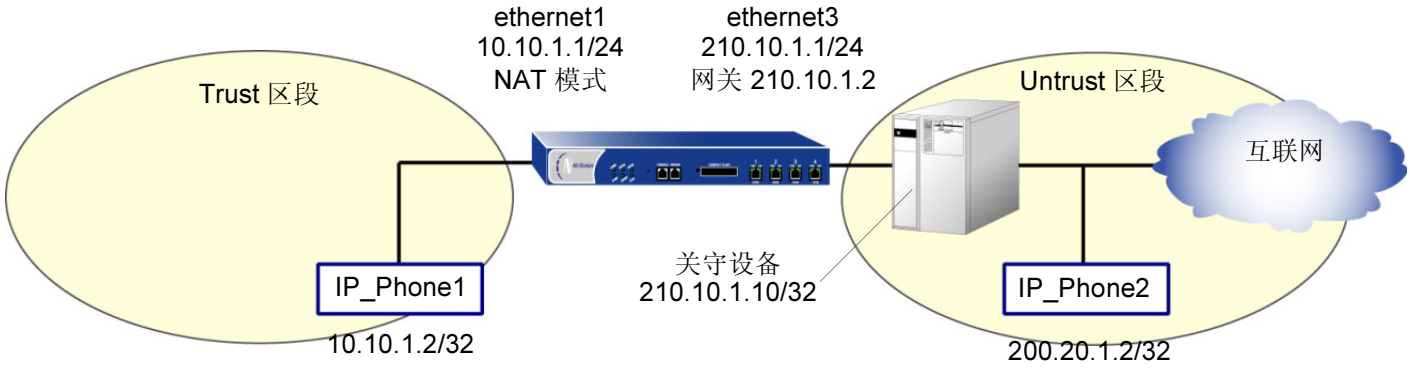
2. Policies > (From: Trust, To: Untrust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择）, Any
   Destination Address:
   Address Book: （选择）, IP_Phone
   Service: H.323
   Action: Permit
3. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择）, IP_Phone
   Destination Address:
   Address Book: （选择）, Any
   Service: H.323
   Action: Permit

CLI

1. set address untrust IP_Phone 209.16.2.2/32
2. set policy from trust to untrust any IP_Phone h.323 permit
3. set policy from untrust to trust IP_Phone any h.323 permit
4. save

范例：Untrust 区段中的关守设备 （Trust 区段处于 NAT 模式）

本例中，关守设备 (210.10.1.10/32) 和主机 IP_Phone2 都在 Untrust 区段中，并且主机 IP_Phone1 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 区段中的关守设备间通过。 Trust 和 Untrust 安全区段都在 trust-vr 路由域中。



WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.1.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 210.10.1.1/24

地址

3. 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: 10.10.1.2/32
   Zone: Trust
4. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: Gatekeeper
   IP Address/Domain Name:
   IP/Netmask: 210.10.1.10/32
   Zone: Untrust
5. 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: 200.20.1.2/32
   Zone: Untrust

映射 IP 地址

6. Network > Interfaces > Edit（对于 ethernet3）> MIP > New：输入以下内容，然后单击 **OK**：
   Mapped IP: 210.10.1.2
   Netmask: 255.255.255.255
   Host IP Address: 10.10.1.2

路由

7. Network > Routing > Routing Table > 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: 210.10.1.2

策略

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

   Source Address:

   Address Book: （选择）, IP_Phone1

   Destination Address:

   Address Book: （选择）, IP_Phone2

   Service: H.323

   Action: Permit

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

   Source Address:

   Address Book: （选择）, IP_Phone1

   Destination Address:

   Address Book: （选择）, Gatekeeper

   Service: H.323

   Action: Permit

10. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
    Source Address:
      Address Book:（选择）, IP_Phone2
    Destination Address:
      Address Book:（选择）, MIP(210.10.1.2)
    Service: H.323
    Action: Permit
11. Policies > (From: Untrust, To: Trust) > New：输入以下内容，然后单击 **OK**：
    Source Address:
      Address Book:（选择）, Gateway
    Destination Address:
      Address Book:（选择）, MIP(210.10.1.2)
    Service: H.323
    Action: Permit

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 210.10.1.1/24

地址

5. set address trust IP_Phone1 10.10.1.2/32
6. set address untrust gatekeeper 210.10.1.10/32
7. set address untrust IP_Phone2 200.20.1.2/32

映射 IP 地址

8. set interface ethernet3 mip 210.10.1.2 host 10.10.1.2

路由

9. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 210.10.1.2

策略

10. set policy from trust to untrust IP_Phone1 IP_Phone2 h.323 permit
11. set policy from trust to untrust IP_Phone1 gatekeeper h.323 permit
12. set policy from untrust to trust IP_Phone2 mip(210.10.1.2) h.323 permit
13. set policy from untrust to trust gatekeeper mip(210.10.1.2) h.323 permit
14. save

服务组

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

NetScreen 服务组选项具有下列功能 :

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

服务组受到以下限制：

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

范例：创建服务组

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

WebUI

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

Group Name: Wiget

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

1. set group service Wiget
2. set group service Wiget add ike
3. set group service Wiget add ftp
4. set group service Wiget add ldap
5. 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，您更改名为 Wiget 的服务组中的成员，此组是您在 [crossref: 第 207 页的 “范例：建立服务组”] 中创建的。您删除 IKE、 FTP 和 LDAP 服务，并添加 HTTP、 FINGER 和 IMAP。

WebUI

Objects > Services > Group > Edit（对于 Wiget）：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

1. clear group service Wiget
2. set group service Wiget add http
3. set group service Wiget add finger
4. set group service Wiget add imap
5. save

范例：移除服务组

在本例中，将删除服务组 Wiget。

WebUI

Objects > Services > Group：单击 **Remove**（对于 Wiget）。

CLI

1. unset group service Wiget remove http
2. get service Wiget
3. save

注意：*NetScreen 设备不会自动删除已经移除其中所有成员的组。*

时间表

时间表是一个可配置的对象，可将其与一个或多个策略相关联以定义策略生效的时间。通过应用时间表，可以控制网络信息流量并确保网络安全。

定义时间表时，请输入下列参数的值：

Schedule Name：出现在 Policy Configuration 对话框的 Schedule 下拉列表中的名称。请选择描述性的名称以帮助识别时间表。名称必须是唯一的，并且限制在 19 个字符以内。

Comment：要添加的任何额外信息。

Recurring：在希望时间表每周重复时启用此项。

Start and End Times：必须配置开始和结束时间。同一天内最多可指定两个时间段。

Once：希望时间表只开始和结束一次时启用此项。

mm/dd/yyyy hh:mm：必须输入开始和停止的日期和时间。

范例：循环时间表

在本例中，有一个名为 Tom 的短期销售职员，他在下班后使用公司的互联网进行私人访问。创建非上班时间的时间表，然后关联策略，以拒绝发自该职员计算机 (10.10.4.5/24) 的、正常上班时间以外的出站 TCP/IP 信息流。

WebUI

1. 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）

Period 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

Period 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. 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: 10.10.4.5/32

   Zone: Trust

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

   Name: No Net

   Source Address:

   Address Book: （选择）, Tom

   Destination Address:

   Address Book: （选择）, Any

   Service: HTTP

   Action: Deny

   Schedule: After Hours

CLI

1. set schedule “after hours” recurrent sunday start 00:00 stop 23:59
2. set schedule “after hours” recurrent monday start 00:00 stop 06:00 start 17:00 stop 23:59
3. set schedule “after hours” recurrent tuesday start 00:00 stop 06:00 start 17:00 stop 23:59
4. set schedule “after hours” recurrent wednesday start 00:00 stop 06:00 start 17:00 stop 23:59
5. set schedule “after hours” recurrent thursday start 00:00 stop 06:00 start 17:00 stop 23:59
6. set schedule “after hours” recurrent friday start 00:00 stop 06:00 start 17:00 stop 23:59
7. set schedule “after hours” recurrent saturday start 00:00 stop 23:59 comment “for non-business hours”
8. set address trust tom 10.10.4.5/32 “temp”
9. set policy from marketing to untrust tom any http deny schedule “after hours”
10. save

7

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. 缺省情况下， NetScreen-5XP 和 NetScreen-5XT 缺省允许信息流从 Trust 区段到 Untrust 区段。

基本元素

允许、拒绝或设置[2] 两点间指定类型单向信息流通道的策略。信息流 （或 “服务”）的类型、两端点的位置以及调用的动作构成了策略的基本元素。尽管可以有其它组件，但是共同构成策略核心的必要元素如下：

- 方向 – 两个安全区段 （从源区段到目的区段）间信息流的方向
- 源地址 – 信息流发起的地址
- 目的地址 – 信息流发送到的地址
- 服务 – 信息流传输的类型
- 动作 – NetScreen 设备接收到满足头四个标准的信息流时执行的动作，这些标准为：permit、 deny、 NAT，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

- 方向：**from trust to untrust**（即从 Trust 区段到 Untrust 区段）
- 源地址：**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）
- 目的地址：**server1**（Untrust 区段通讯簿中用户定义的地址）
- 服务：**ftp**（文件传输协议）
- 动作：**permit**（NetScreen 设备允许此信息流通过其防火墙）

2. “tunnel”动作 （VPN 或 L2TP 通道），隐含“permit”（允许）的概念。

三种类型的策略

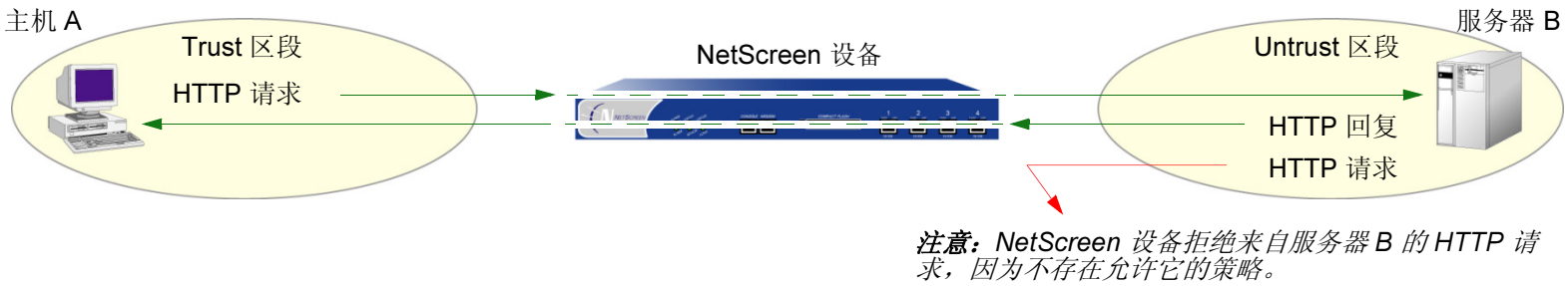
可通过以下三种策略控制信息流的流动：

- 通过创建区段间策略，可以管理允许从一个安全区段到另一个安全区段的信息流的种类。
- 通过创建区段内部策略，也可以控制允许通过绑定到同一区段的接口间的信息流的类型。
- 通过创建全局策略，可以管理地址间的信息流，而不考虑它们的安全区段。

区段间策略

区段间策略提供对安全区段间信息流的控制。可以设置区段间策略来允许、拒绝或设置从一个区段到另一个区段的信息流通道。使用状态式检查技术，NetScreen 设备保持活动 TCP 会话表和活动 UDP“pseudo”会话表，以便允许它能回应服务请求。例如，如果有一个策略允许从 Trust 区段中的主机 A 到 Untrust 区段中的服务器 B 的 HTTP 请求，则当 NetScreen 设备接收到从服务器 B 到主机 A 的 HTTP 回应时，NetScreen 设备将接收到的封包与它的表进行对照检查。找到回应批准 HTTP 请求的封包时，NetScreen 设备允许来自 Untrust 区段中服务器 B 的封包穿越防火墙到达 Trust 区段中的主机 A。要控制由服务器 B 发起的流向主机 A 的信息流（不只是回应由主机 A 发起的信息流），必须创建从 Untrust 区段中服务器 B 到 Trust 区段中主机 A 的第二个策略。

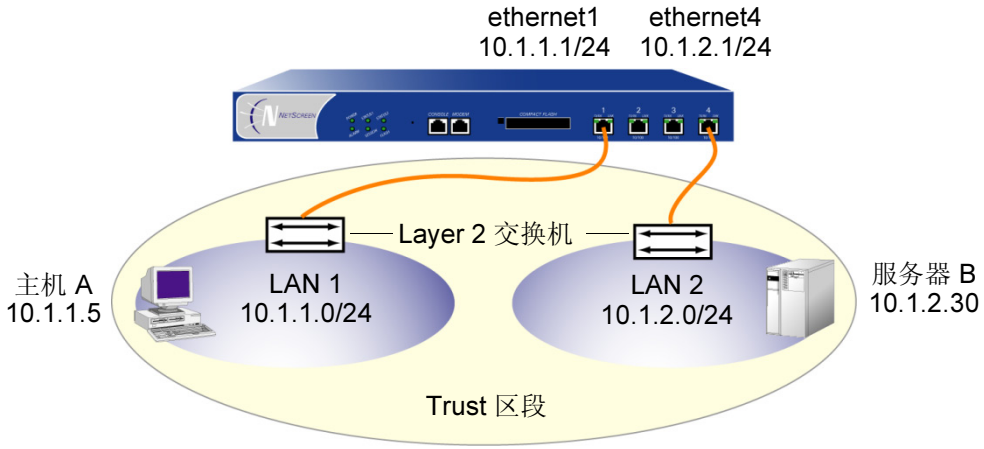
set policy from trust to untrust “host A” “server B” http permit



区段内部策略

区段内部策略提供对绑定到同一安全区段的接口间信息流的控制。源地址和目的地址都在同一安全区段中，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单向流动。要允许从数据路径任一端发起的信息流，必须创建两个策略，每个方向一个策略。

```
set policy from trust to trust “host A” “server B” any permit
set policy from trust to trust “server B” “host A” any permit
```



全局策略

与区段间和区段内部策略不同，全局策略不引用特定的源和目的区段。全局策略引用用户定义的 Global 区段地址或预定义的 Global 区段地址 “any”。这些地址可以跨越多个安全区段。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：*本版本发行时，全局策略不支持基于策略的 NAT、MIP、VIP、DIP、VPN 通道或透明模式。全局策略对于防火墙信息流控制很严格。*

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封包时，会记录入口接口，从而获知接口所绑定的源区段。然后 NetScreen 设备执行路由查询以确定出口接口，从而确定该接口所绑定的目的区段。使用源区段和目的区段， NetScreen 设备可以执行策略查询，按以下顺序查阅策略组列表：

1. 如果源区段和目的区段不同，则 NetScreen 设备在区段间策略组列表中执行策略查询。

   （或）

   如果源区段和目的区段相同，则 NetScreen 设备在区段内部策略组列表中执行策略查询。

2. 如果 NetScreen 设备执行区段间或区段内部策略查询，但是没有找到匹配策略，则 NetScreen 设备会检查全局策略组列表以查找匹配策略。
3. 如果 NetScreen 设备执行区段间和全局策略查询，但是没有找到匹配项，NetScreen 设备会将缺省的允许 / 拒绝策略应用到封包：**unset/set policy default-permit-all**。

   （或）

   如果 NetScreen 设备执行区段内部和全局策略查询，但是没有找到匹配策略， NetScreen 设备会将该区段的区段内部阻塞设置应用到封包：**unset/set zone** *zone* **block**。

NetScreen 设备从上至下搜索每个策略组列表。因此，必须在列表中将较为特殊的策略定位在不太特殊的策略上面。（有关策略顺序的信息，请参阅第 246 页上的 “重新排序策略”。）

策略定义

防火墙提供具有单个进入和退出点的网络边界。由于所有信息流都必须通过此点，因此可以筛选并引导所有通过执行策略组列表 （区段间策略、内部区段策略和全局策略）产生的信息流。

策略能允许、拒绝、加密、认证、排定优先次序、调度以及监控尝试从一个安全区段流到另一个安全区段的信息流。可以决定哪些用户和信息能进入和离开，以及它们进入和离开的时间和地点。

注意：*对于某些 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

单个用户可配置的策略内部生成一个或多个逻辑规则，而每个逻辑规则都由一组组件（源地址、目的地址和服务）组成。组件占用内存资源。引用组件的逻辑规则不占用内存资源。

根据源地址组和目的地址组以及策略中服务组的使用，逻辑规则的数量可比创建单个策略时明显可见的大得多。例如，以下策略产生 125 个逻辑规则：

1 个策略：5 个源地址 x 5 个目的地址 x 5 个服务 = 125 个逻辑规则

但是，NetScreen 设备不为每个逻辑规则复制组件。规则以不同的组合使用同一组组件。例如，产生 125 个逻辑规则的上述策略只生成 15 个组件：

5 个源地址 + 5 个目的地址 + 5 个服务 = 15 个组件

这 15 个组件以不同方式组合，生成由单个策略产生的 125 个逻辑规则。允许多个逻辑规则以不同组合使用同一组组件，与每个逻辑规则与其组件具有一对一关系相比， NetScreen 设备占用的资源少得多。

由于新策略的安装时间与 NetScreen 设备添加、删除或修改的组件数量成比例，因此组件较少策略的安装更快。同样，与每个规则都需要专用组件相比，通过允许大量的逻辑规则共享一小组组件， NetScreen 使用户能创建更多的策略， NetScreen 设备能创建更多的规则。

策略的结构

策略必须包含下列元素：

- 区段 （源区段和目的区段）
- 地址 （源地址和目的地址）
- 服务
- 动作 （permit、 deny、 tunnel）

策略也可包含下列元素：

- VPN 通道确定
- Layer 2 （第 2 层）传输协议 (L2TP) 通道确定
- 策略组列表顶部位置
- 网络地址转换 (NAT)，使用动态 IP (DIP) 池
- 用户认证
- 备份 HA 会话
- 记录
- 计数
- 信息流报警设置
- 时间表
- 信息流整形

本节的余下部分将依次分析上述每一元素。

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 217 页上的 “区段间策略”和第 218 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，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。源和目的地址都使用地址组时尤其危险。（有关详细信息，请参阅第 220 页上的 “策略和规则”。）

服务

服务是使用第 4 层信息 （如应用程序服务 Telnet、 FTP、 SMTP 和 HTTP 的标准和公认的 TCP 和 UDP 端口号）识别应用程序协议的对象。 ScreenOS 包括预定义的核心互联网服务。另外，还可以定义定制服务。

可以定义策略，指定允许、拒绝、加密、认证、记录或统计哪些服务。

动作

动作是描述防火墙如何处理接收到的信息流的对象。

- **Permit** 允许封包通过防火墙。
- **Deny** 阻塞封包，使之不能通过防火墙。
- **Tunnel** 封装外向 IP 封包和解除内向 IP 封包的封装。对于 IPSec VPN 通道，指定要使用哪个 VPN 通道。对于 L2TP 通道，指定要使用哪个 L2TP 通道。对于 IPSec 上的 L2TP，指定一个 IPSec VPN 通道和一个 L2TP 通道[3]。

NetScreen 设备将指定动作应用到与预先提供的标准匹配的信息流，这些标准为：区段 （源区段和目的区段）、地址（源地址和目的地址）以及服务。

VPN 通道确定

可以将单个或多个策略应用到已配置的任何 VPN 通道。在 WebUI 中， VPN Tunnel 选项提供所有这些通道的下拉列表。在 CLI 中，可以用 **get vpn** 命令查看所有可用的通道。（有关详细信息，请参阅第 **4**-47 页上的 “基于路由的 VPN”和第 **4**-123 页上的 “基于策略的 VPN”。）

当 VPN 通道两端的 VPN 配置都使用基于策略的 NAT 时，两个网关设备的管理员都需要创建入站和出站策略 （总共四个策略）。当 VPN 策略构成匹配对 （即，除源地址和目的地址反向外，入站和出站策略配置中的任何内容都相同）时，可以配置一个策略，然后选择 **Modify matching bidirectional VPN policy** 复选框，自动为相反方向创建第二个策略。对于新策略的配置， matching VPN policy 复选框缺省情况下是清除的。对于是匹配对成员的现有策略的修改，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。（请注意，此选项只能通过 WebUI 获得。）

3. 对于 IPSec 上的 L2TP， IPSec VPN 通道的源地址和目的地址必须与 L2TP 通道的源地址和目的地址相同。

L2TP 通道确定

可以将单个或多个策略应用到已配置的任何“第 2 层通道协议 (L2TP)”通道。在 WebUI 中， L2TP 选项提供所有这些通道的下拉列表。在 CLI 中，可以用 **get l2tp all** 命令查看所有可用的通道。也可以将 VPN 通道和 L2TP 通道组合在一起 （如果两者都具有相同的端点），创建结合每个通道特征的通道。这称为 IPSec 上的 L2TP。

注意：*在透明模式中不支持 L2TP。*

定位在顶部

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 246 页上的“重新排序策略”中说明的任一策略重新排序方法。在将最近创建的策略重新定位到策略列表的顶部时，为避免额外的步骤，可以在 WebUI 中选择 **Position at Top** 选项，或在 CLI 中的 **set policy** 命令中使用关键字 **top** (**set policy top ...**)。

网络地址转换 (NAT)

可以在接口级 （绑定到 Untrust 区段的接口除外）或在策略级应用 NAT。使用基于策略的 NAT，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”池，或来自“映射 IP”（对于内向网络信息流以及内向和外向 VPN 信息流）。

用户认证

选择此选项要求源地址的 auth 用户，在允许信息流穿越防火墙或进入 VPN 通道前，通过提供用户名和密码，以认证他 / 她的身份。NetScreen 设备可使用本地数据库或外部 RADIUS、SecurID 或 LDAP auth 服务器，执行认证检查。

注意：*如果将需要认证的策略应用到 IP 地址的子网，则每个 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），则在第一个用户认证后，该主机的所有其它用户都可以继承第一个用户的权限，让信息流通过 NetScreen 设备而不必经过认证。

NetScreen 提供两种认证方案：

- 运行时认证，在收到与启用认证的策略相匹配的 HTTP、FTP 或 Telnet 信息流时，NetScreen 设备提示 auth 用户登录
- WebAuth，通过 NetScreen 设备发送信息流前，用户必须认证自己

运行时认证

运行时认证的过程如下：

1. 当 auth 用户发送 HTTP、FTP 或 Telnet 连接请求到目的地址时，NetScreen 设备截取封包并对其进行缓冲。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备认证 auth 用户的登录信息。

   如果认证成功，则在 auth 用户和目的地址间建立连接。

对于初始的连接请求，策略必须包括下列三个服务中的一项或所有服务：Telnet、 HTTP 或 FTP。只有具有这些服务中的一个或所有服务的策略才能启动认证过程。可以在涉及用户认证的策略中使用以下任一服务：

- Any （因为 “any”包括所有三项必需的服务）
- Telnet、 HTTP 或 FTP。
- 包括所希望的服务或多个服务的服务组，加上启动认证过程必需的三个服务中的一个或多个 （Telnet、 FTP 或 HTTP）。例如，可以创建名为 “Login”的定制服务组，支持 FTP、网络会议系统和 H.323 服务。然后，在创建策略时，指定服务为 “Login”。

对于成功认证后的任何连接，策略中指定的所有服务都有效。

注意： *启用了认证的策略不支持将 DNS （端口为 53）作为服务。*

策略前检查认证 (WebAuth)

WebAuth 认证的过程如下：

1. auth 用户为 WebAuth 服务器建立到 IP 地址的 HTTP 连接。
2. NetScreen 设备向 auth 用户发出登录提示。
3. auth 用户用自己的用户名和密码响应此提示。
4. NetScreen 设备或外部 auth 服务器认证 auth 用户的登录信息。

   如果认证尝试成功，则 NetScreen 设备允许 auth 用户启动信息流，使其流向在强制通过 WebAuth 方法执行认证的策略中指定的目的位置。

注意： *有关这两种用户认证方法的详细信息，请参阅第 274 页上的 “Auth 用户和用户组”。*

通过选择特定的用户组、本地或外部用户或组表达式，可以限制或扩展应用策略的 auth 用户的范围。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。缺省情况下， NSRP 集群中的 NetScreen 设备备份会话。

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*** *-55 页上的 “监控 NetScreen 设备”。*

计数

在策略中启用计数时， NetScreen 设备计算应用此策略的信息流的总字节数，并将信息记录在历史记录图表中。要在 WebUI 中查看策略的历史记录图表，请单击 **Reports > Policies >**  （对于要查看其信息流计数的策略）。

信息流报警临界值

可以设置当策略允许的信息流超过指定的每秒字节数、每分钟字节数（或两者）时，触发警报的临界值。由于信息流报警要求 NetScreen 设备监控字节总数，因此也必须启用计数功能。

*注意：有关信息流报警的详细信息，请参阅第 **3**-82 页上的 “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。

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 （保障带宽）： 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 （最大带宽）： 以千比特每秒 (kbps) 表示的连接类型可用的安全带宽。超过此临界值的信息流被抑制并丢弃。

注意：建议不要使用低于 10 kbps 的额定值。低于此临界值的额定值会导致封包被丢弃以及过多的重试，从而使信息流的管理目的失败。

Traffic Priority （信息流优先级）： 当信息流带宽在保障带宽和最大带宽设置之间时， NetScreen 设备首先让较高优先级的信息流通过，并且只有在没有其它更高优先级的信息流时，才让较低优先级的信息流通过。有八个优先级。

DiffServ Codepoint Marking （差异服务码点标记）：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。缺省情况下， NetScreen 系统中的最高优先级 （优先级 0）映射到 DiffServ 字段 （请参阅 RFC 2474）中的头三位 (0111)，或映射到 IP 封包包头的 ToS 字节 （请参阅 RFC 1349）的 IP 前字段中。 NetScreen 系统中的最低优先级 （优先级 7）映射到 ToS DiffServ 系统中的 (0000)。

***注意：**有关信息流管理和整形的更详细讨论，请参阅第 353 页上的 “信息流整形”。*

要更改 NetScreen 优先级和 DiffServ 系统间的映射，请使用以下 CLI 命令：

set traffic-shaping ip_precedence *number0 number1 number2 number3 number4 number5 number6 number7*

其中 *number0* 是优先级 0（TOS DiffServ 系统中的最高优先级）的映射，*number1* 是优先级 1 的映射，依次类推。

策略应用

本节说明策略的管理：查看、创建、修改、排序和重新排序以及移除策略。

查看策略

要通过 WebUI 查看策略，请单击 **Policies**。通过从 **From** 和 **To** 下拉列表中选择区段名称，然后单击 **Go**，可以按源区段和目的区段分类显示策略。在 CLI 中，使用 **get policy [all | from** *zone* **to** *zone* **| global | id** *number* **]** 命令。

策略图标

查看策略列表时， WebUI 使用图标提供策略组件的图形化汇总。下表解释了策略页中使用的不同图标。

图标	功能	说明
	允许	所有满足标准的信息流都通过。
	拒绝	所有满足标准的信息流都被拒绝。
	启用封装 或解除封装	所有满足标准的出站信息流都被封装。所有满足标准的入站信息流都被解除封装。
	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。

图标	功能	说明
	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	以每秒字节数为单位计算信息流的量。
	信息流报警	指示已经设置信息流报警临界值。

创建策略

要允许信息流在两个区段间流动，应在这些区段间创建允许、拒绝或设置信息流通道的策略。如果 NetScreen 设备唯一能够设置（在策略中引用的）源和目的地址间区段内部信息流的路由的网络设备，则也可创建策略，控制同一区段内的信息流。也可创建全局策略，使用 Global 区段通讯簿中的源和目的地址。

要允许两个区段间（例如，“abc”和“xyz”区段）的双向信息流，需要创建从“abc”到“xyz”的策略，然后创建从“xyz”到“abc”的第二个策略。两个策略使用相同的 IP 地址，只是源地址和目的地址反向。根据需要，策略可以具有相同或不同的配置。

策略位置

可以在同一系统（根或虚拟系统）中的任何区段间定义策略。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 6 卷，“虚拟系统”。）

范例：区段间策略

在本例中，将创建两个策略。第一个策略允许服务组 Mail-POP3 中的服务穿越 NetScreen 防火墙，从 “主机 A” 到达 “邮件服务器”[4]。第二个策略允许服务 “邮件” 穿越防火墙从 “邮件服务器” 到达 “主机 A”。

WebUI

1. Policies > (From: abc, To: xyz) > New：输入以下内容，然后单击 **OK**：

   Source Address:

   Address Book: （选择） , Host A

   Destination Address:

   Address Book: （选择） , Mail Server

   Service: Mail-POP3

   Action: Permit

2. Policies > (From: xyz, To: abc) > New：输入以下内容，然后单击 **OK**：

   Source Address:

   Address Book: （选择） , Mail Server

   Destination Address:

   Address Book: （选择） , Host A

   Service: Mail

   Action: Permit

4. 要创建服务组，请参阅第 206 页上的 “服务组”。

CLI

1. set policy from abc to xyz “host a” “mail server” mail-pop3 permit
2. set policy from xyz to abc “mail server” “host a” mail permit
3. save

范例：区段间策略设置

本例假定已经配置了地址和缺省路由。有关配置地址的详细信息，请参阅第 178 页上的 “地址”。有关如何设置缺省路由的详细信息，请参阅第 51 页上的 “路由和虚拟路由器”一章。

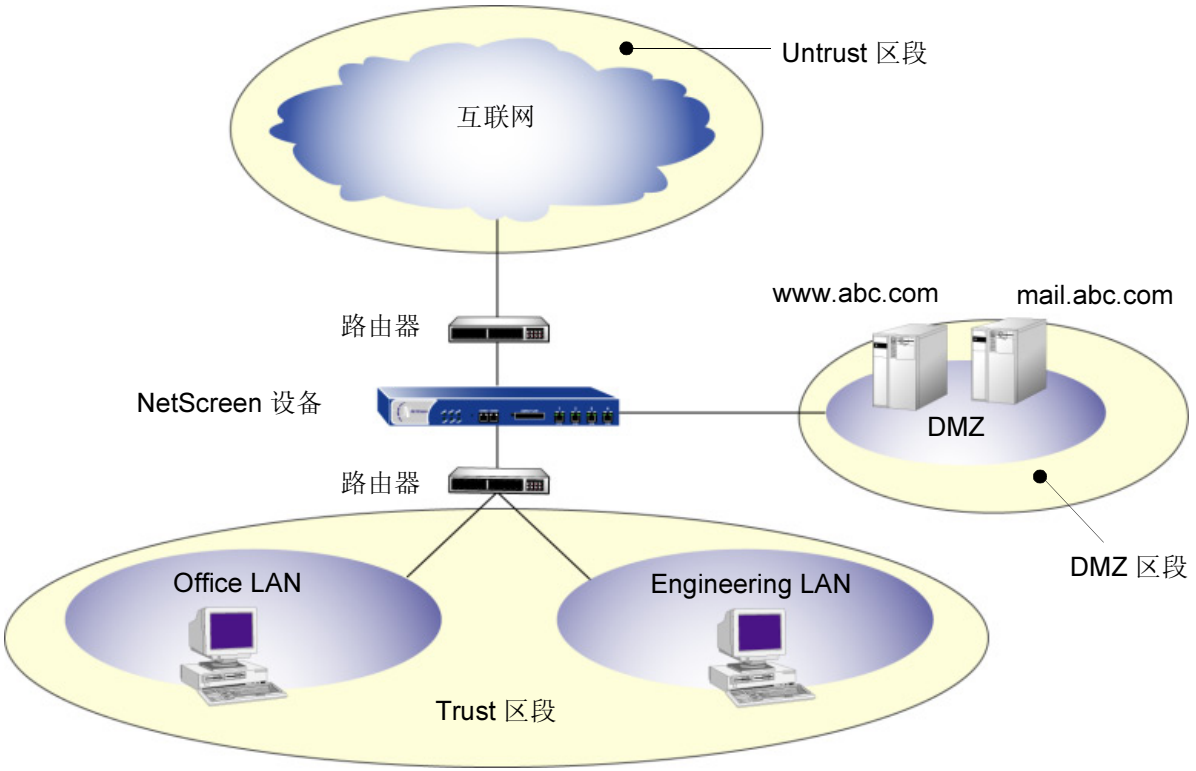
一个小的软件公司 （ABC Design）已将其内部网络分成两个子网，这两个子网都在 Trust 区段中。这两个子网为：

- 工程 （定义地址为 “Engineering”）
- 公司的其余部分 （定义地址为 “Office”）。

其 Web 和邮件服务器也有一个 DMZ 区段。

下例介绍了对以下用户的一组典型策略：

- “Engineering”可使用用于出站信息流的所有服务， FTP-Put、 IMAP、 MAIL 和 POP3 除外。
- “Office”可使用电子邮件和访问 “互联网”，只要它们通过 WebAuth 认证自己。（有关 WebAuth 用户认证的信息，请参阅第 274 页上的 “Auth 用户和用户组”。）
- 来自 Trust 和 Untrust 区段的任何用户，都可访问 DMZ 区段中的 Web 和邮件服务器。
- 也有一组系统管理员（定义地址为“Sys-admins”），对 DMZ 区段中的服务器具有全部用户和管理访问权限。



注意： *下例使用服务组。有关创建此类组的信息，请参阅第 206 页上的 “服务组”。*

从区段 （源地址）	到区段 （目的地址）	服务	动作
Trust - Any	Untrust - Any	Com （服务组：FTP-Put、 IMAP、 MAIL、 POP3）	Deny
Trust - Engineering	Untrust - Any	Any	Permit
Trust - Office	Untrust - Any	Internet （服务组：FTP-Get、 HTTP、 HTTPS）	Permit (+ WebAuth)

从区段 （源地址）	到区段 （目的地址）	服务	动作
Untrust - Any	DMZ - mail.abc.com	MAIL	Permit
Untrust - Any	DMZ - www.abc.com	Web （服务组：HTTP、 HTTPS）	Permit

从区段 （源地址）	到区段 （目的地址）	服务	动作
Trust - Any	DMZ - mail.abc.com	e-mail （服务组：IMAP、 MAIL、 POP3）	Permit
Trust - Any	DMZ - www.abc.com	Internet （服务组：FTP-Get、 HTTP、 HTTPS）	Permit
Trust - Sys-admins	DMZ - Any	Any	Permit

从区段 （源地址）	到区段 （目的地址）	服务	动作
DMZ - mail.abc.com	Untrust - Any	MAIL	Permit

注意： *缺省策略为全部拒绝。*

WebUI

从信任，到 Untrust

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

   Source Address:

   Address Book: （选择） , Engineering

   Destination Address:

   Address Book: （选择） , Any

   Service: ANY

   Action: Permit

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

   Source Address:

   Address Book: （选择） , Office

   Destination Address:

   Address Book: （选择） , Any

   Service: Internet[5]

   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）

5. “Internet”是具有以下成员的服务组：FTP-Get、 HTTP 和 HTTPS。

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , Any

Service: Com[6]

Action: Deny

Position at Top: （选择）

注意：*对于从 Untrust 区段到 Trust 区段的信息流，缺省的拒绝策略拒绝所有信息流。*

从 Untrust，到 DMZ

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , mail.abc.com

Service: MAIL

Action: Permit

6. “Com”是具有以下成员的服务组：FTP-Put、 MAIL、 IMAP 和 POP3。

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

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （选择） , www.abc.com

   Service: Web[7]

   Action: Permit

从 Trust，到 DMZ

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

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （选择） , mail.abc.com

   Service: e-mail[8]

   Action: Permit

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

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （选择） , www.abc.com

   Service: Internet

   Action: Permit

7. “Web”是具有以下成员的服务组：HTTP 和 HTTPS。

8. “e-mail”是具有以下成员的服务组：MAIL、 IMAP 和 POP3。

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

Source Address:

Address Book: （选择）, Sys-admins

Destination Address:

Address Book: （选择）, Any

Service: ANY

Action: Permit

从 DMZ，到 Untrust

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

Source Address:

Address Book: （选择）, mail.abc.com

Destination Address:

Address Book: （选择）, Any

Service: MAIL

Action: Permit

CLI

从 Trust，到 Untrust

1. set policy from trust to untrust engineering any any permit
2. set policy from trust to untrust office any Internet[9] permit auth webauth
3. set policy top from trust to untrust any any Com[10] deny

从 Untrust，到 DMZ

4. set policy from untrust to dmz any mail.abc.com mail permit
5. set policy from untrust to dmz any www.abc.com Web[11] permit

从 Trust，到 DMZ

6. set policy from trust to dmz any mail.abc.com e-mail[12] permit
7. set policy from trust to dmz any www.abc.com Internet[9] permit
8. set policy from trust to dmz sys-admins any any permit

从 DMZ，到 Untrust

9. set policy from dmz to untrust mail.abc.com any mail permit
10. save

9. “Internet”是具有以下成员的服务组：FTP-Get、 HTTP 和 HTTPS。
10. “Com”是具有以下成员的服务组：FTP-Put、 MAIL、 IMAP 和 POP3。
11. “Web”是具有以下成员的服务组：HTTP 和 HTTPS。
12. “e-mail”是具有以下成员的服务组：MAIL、 IMAP 和 POP3。

范例：区段内部策略

在本例中，创建内部区段策略，允许一组帐户访问 Trust 区段中企业 LAN 上的机密服务器。首先将 ethernet1 绑定到 Trust 区段，并给定 IP 地址为 10.1.1.1/24。然后将 ethernet2 绑定到 Trust 区段，并指派 IP 地址为 10.1.5.1/24。启用 Trust 区段中的区段内部阻塞。接着，定义两个地址，一个作为公司存储财务记录的服务器地址，另一个作为会计部门主机所在位置的子网地址。然后创建区段内部策略，允许从这些主机访问服务器。

WebUI

Trust 区段 – 接口和阻塞

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.5.1/24
3. Network > Zones > Edit（对于 Trust）：输入以下内容，然后单击 **OK**：
   Block Intra-Zone Traffic: （选择）

地址

4. 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

5. 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

策略

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

   Source Address:

   Address Book: （选择）, accounting

   Destination Address:

   Address Book: （选择）, Hamilton

   Service: Any

   Action: Permit

CLI

Trust 区段 – 接口和阻塞

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet2 zone trust
4. set interface ethernet2 ip 10.1.5.1/24
5. set zone trust block

地址

6. set address trust Hamilton 10.1.1.100/32
7. set address trust accounting 10.1.5.0/24

策略

8. set policy from trust to trust accounting Hamilton any permit
9. save

范例：全局策略

在本例中，将创建一个全局策略，使每个区段中的每台主机都可以访问公司的 Web 网站，网址为 www.netscreen.com[13]。在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* 个区段间策略所实现的任务（其中 *n* = 区段数）。

WebUI

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

   Address Name: server1

   IP Address/Domain Name:

   Domain Name:（选择）, www.netscreen.com

   Zone: Global

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, server1

   Service: HTTP

   Action: Permit

CLI

1. set address global server1 www.netscreen.com
2. set policy global any server1 http permit
3. save

13. 要用域名而非 IP 地址，应确保在 NetScreen 设备上配置 DNS 服务。

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，单击要更改的策略的 Configure 栏中的 **Edit** 链接。在该策略出现的 Policy configuration 页面中进行更改，然后单击 **OK**。在 CLI 中，使用 **set policy** 命令。

ScreenOS 也提供启用和禁用策略的方法。

缺省情况下，策略被启用。要禁用策略，请执行以下操作：

WebUI

策略：从要禁用的策略的 Configure 栏中，清除 **Enable** 复选框。

被禁用策略的文本行以灰色显示。

CLI

1. set policy id *id_num* disable
2. save

注意：*要再次启用策略，请在要启用的策略 Configure 栏中选择* ***Enable*** *(WebUI)，或键入* ***unset policy id*** *id_num* ***disable*** *(CLI)。*

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 219 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。）

缺省情况下，最近创建的策略出现在策略组列表的底部。有一个选项允许将新配置的策略定位在列表的顶部。在 WebUI 的 Policy configuration 页面中，选择 **Position at Top** 复选框。在 CLI 中，将关键字 **top** 添加到 **set policy** 命令中：**set policy top** ...

要将策略移动到列表中的不同位置，请执行以下操作之一：

WebUI

在 WebUI 中有两种方法重新排序策略：在要移动的策略的 Configure 栏中，单击圆形箭头或单击单箭头。

如果单击圆形箭头：

出现 User Prompt 对话框。

要将策略移到列表的最底端，请输入 <-1>。要将策略向上移动，输入要移动到其前的策略的 ID 号。

单击 **OK**，执行移动。

如果单击单箭头：

出现 Policy Move 页面，显示要移动的策略以及显示其它策略的表格。

在显示其它策略的表格中，第一栏（Move Location）包含指向不同位置的箭头，可将策略移动这些位置。单击指向策略要移动到的列表中位置的箭头。

出现 Policy List 页面，移动的策略出现在新位置。

CLI

1. set policy move *id_num* { before | after } *number*
2. save

移除策略

除修改和重新排序策略外，还可以删除策略。在 WebUI 中，在要移除的策略的 Configure 栏中单击 **Remove**。当系统消息提示是否继续删除时，单击 **Yes**。在 CLI 中，使用 **unset policy** *id_num* 命令。

8

用户认证

本章重点介绍进行用户认证的几种方法。首先研究不同类型的认证服务器 — 内置于各 NetScreen 设备中的本地数据库以及外部 RADIUS、 SecurID 和 LDAP 认证服务器。然后，介绍如何定义不同的用户帐户（或“配置文件”）、如何创建用户组、如何在策略、“自动密钥 IKE”网关、“手动密钥 VPN”通道和 L2TP 通道中引用用户和用户组。本章最后一节介绍如何自定义 HTTP、 FTP、 L2TP、 Telnet 和 XAuth 登录提示中出现的标题。本章包括以下部分：

认证服务器

可对 NetScreen 设备进行配置，以便使用本地数据库或者一个或多个外部认证服务器验证以下类型用户的身份：

- Auth 用户
- IKE 用户
- 手动密钥用户
- L2TP 用户
- XAuth 用户
- Admin 用户

> ***注意：****IKE 和 “手动密钥” 用户帐户必须存储在本地数据库上。 RADIUS 是唯一支持 L2TP 和 XAuth 远程设置指派和管理权限指派的外部服务器。*

除其本地数据库外，NetScreen 设备还支持外部 RADIUS、SecurID 和 LDAP 服务器。可使用各种类型的认证服务器对 auth 用户、L2TP 用户、XAuth 用户和 admin 用户进行认证。此外，NetScreen 还支持 WebAuth，这是面向 auth 用户的一种可选认证方案。（有关 WebAuth 的范例，请参阅第 298 页上的 “范例：WebAuth + SSL （外部用户组）”。）所有包含 auth 用户帐户类型的 auth 服务器都可以作为缺省的 WebAuth auth 服务器。下表对服务器与用户类型及认证功能之间的对应支持关系加以总结：

服务器类型	支持的用户类型和功能										
	Auth 用户	IKE 用户	手动密钥用户	L2TP 用户		XAuth 用户		Admin 用户		用户组	组表达式
				Auth	远程设置	Auth	远程设置	Auth	权限		
本地	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
RADIUS	✓			✓	✓	✓	✓	✓	✓	✓	✓
SecurID	✓			✓		✓		✓			
LDAP	✓			✓		✓		✓			

在大多数 NetScreen 设备上，可对每个系统 — 根系统和虚拟系统 — 以任意组合形式使用最多 10 个主认证服务器。这一数字包括本地数据库，但不包括备份认证服务器。一个 RADIUS 或 LDAP 服务器支持两个备份服务器，一个 SecurID 服务器支持一个备份服务器；例如，您可使用本数据库和 9 个不同的主 RADIUS 服务器，每个 RADIUS 服务器分配有两个备份服务器。

多个认证服务器同时运行

各连接请求的颜色与认证检查的匹配颜色相关：

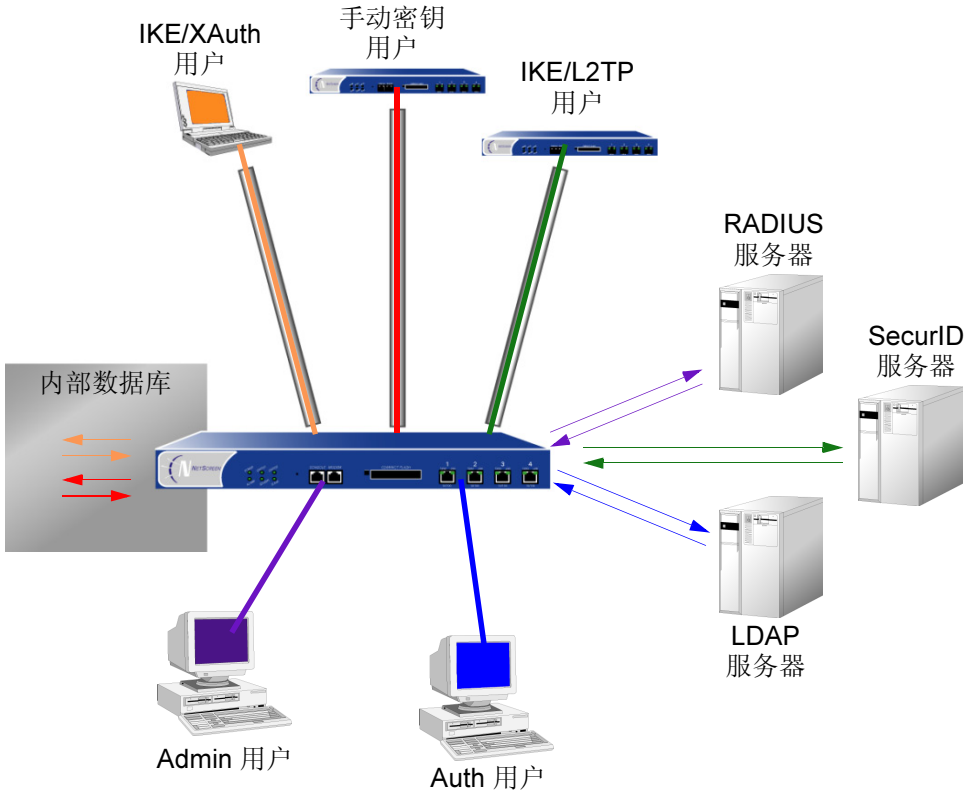
IKE/XAuth 用户 （橙色） –> 本地数据库

手动密钥用户 （红色） –> 本地数据库

IKE/L2TP 用户 （绿色） –> SecurID 服务器

Admin 用户 （紫色） –> RADIUS 服务器

Auth 用户 （蓝色） –> LDAP 服务器

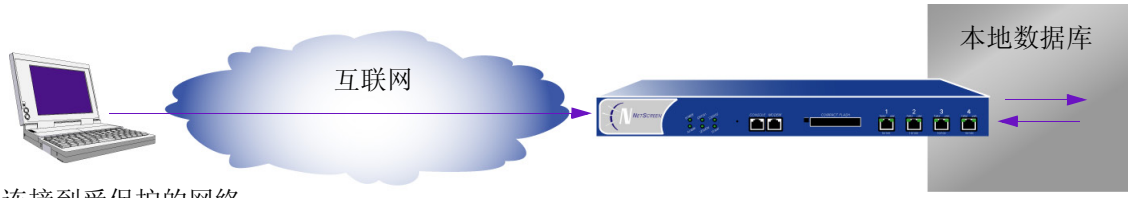


注意：*可使用一个认证服务器完成多种类型的用户认证。例如，* RADIUS *服务器可存储* admin*、*auth*、* IKE*、* L2TP*、手动密钥和* XAuth *用户。*

以下部分进一步详细研究本地数据库以及各种认证服务器。

本地数据库

所有 NetScreen 设备都支持使用内置用户数据库进行认证。在 NetScreen 设备上定义用户时， NetScreen 设备将用户名和密码输入到其本地数据库中。



认证用户请求连接到受保护的网络。

NetScreen 设备在批准连接请求之前，会查阅其内部数据库，对认证用户进行身份认证。

支持的用户类型和功能

本地数据库支持以下类型的用户和认证功能：

- Auth 用户
- IKE 用户
- L2TP 用户
- XAuth 用户
- 手动密钥用户
- Admin 用户
- Admin 权限
- WebAuth
- 用户组
- 组表达式*

* 在 NetScreen 设备上定义组表达式，但用户和用户组必须存储在外部 RADIUS auth 服务器上。有关组表达式的详细信息，请参阅第 343 页上的 “组表达式”。

对于所有类型的认证而言，本地数据库是缺省的认证服务器 （auth 服务器）。有关如何通过 WebUI 和 CLI 向本地数据库添加用户和用户组的说明，请参阅第 273 页上的 “认证类型及应用”。

范例：设置本地数据库超时

缺省情况下，admin 和 auth 用户的本地数据库认证超时时限为 10 分钟。在本例中，将 admin 用户的此项设置更改为永不超时，而将 auth 用户的此项设置更改为 30 分钟后超时。

WebUI

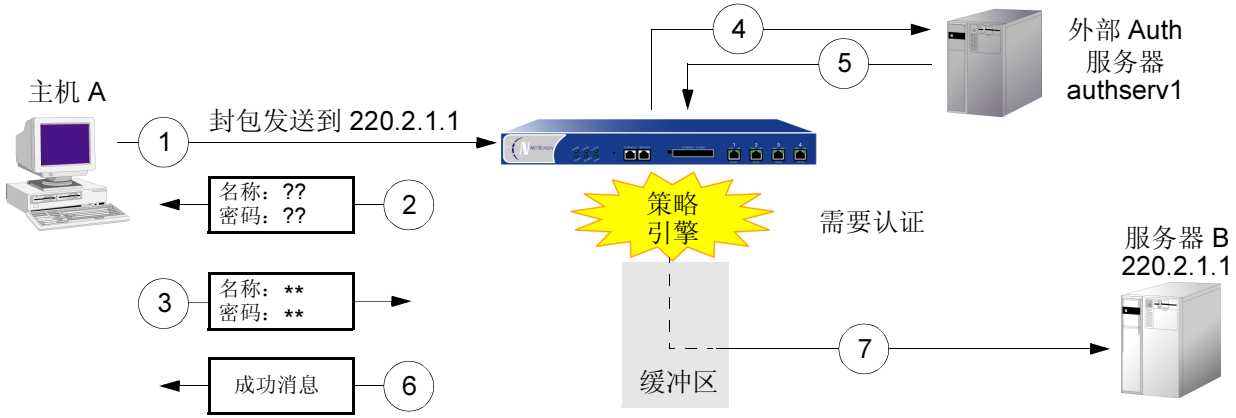
1. Configuration > Management：在 Enable Web Management Idle Timeout 字段中输入 **0**，然后单击 **Apply**。
2. Lists > Auth Servers > Edit（对于 Local）：在 Timeout 字段中输入 **30**，然后单击 **Apply**。

CLI

1. set admin auth timeout 0
2. set auth-server Local timeout 30
3. save

外部 AUTH 服务器

NetScreen 设备可与存储用户帐户的一个或多个外部认证服务器或“auth 服务器”相连。NetScreen 设备在接收到要求进行认证验证的连接请求后，会请求策略、L2TP 通道配置或 IKE 网关配置中所指定的 auth 外部服务器进行认证检查。然后，NetScreen 充当用户请求认证与 auth 服务器批准认证之间的中继器。成功的外部 auth 服务器认证检查的过程如下：

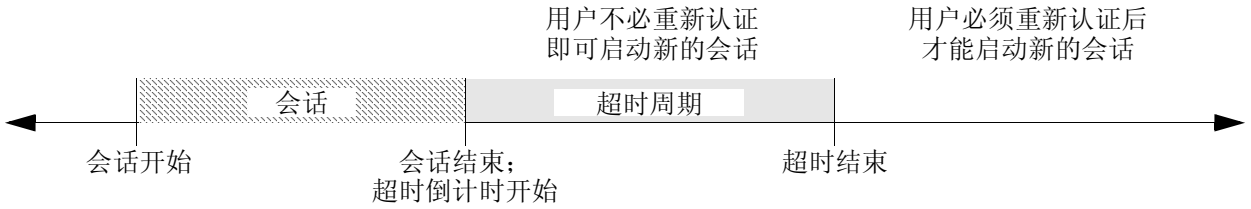


1. 主机 A 将 FTP、HTTP 或 Telnet TCP SYN 封包发送到 220.2.1.1。
2. NetScreen 设备截取封包、记录其相应策略要求从 authserv1 获得认证、将封包放入缓冲区，并提示用户输入用户名和密码。
3. 用户以用户名和密码回复。
4. NetScreen 设备将登录信息转发到 authserv1。
5. Authserv1 将成功通知发送回 NetScreen 设备。
6. NetScreen 设备通知 auth 用户成功通过认证。
7. 然后，NetScreen 设备将封包从其缓冲区转发到其目的地 220.2.1.1。

Auth 服务器对象属性

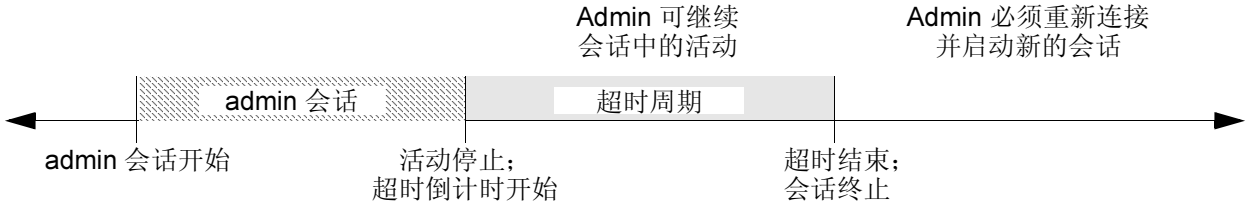
NetScreen 设备将每个 auth 服务器视为可在策略、IKE 网关和 L2TP 通道中引用的一个对象。以下属性定义并唯一标识 auth 服务器对象：

- 对象名：名称字符串，如 “authserv1”（唯一的预定义 auth 服务器为 “Local”）。
- ID 号：可手动设置 ID 号，也可让 NetScreen 设备自动对其进行设置。如果设置 ID 号，则必须选择未使用的号码。
- 类型：RADIUS、 SecurID、 LDAP。
- 服务器名称：服务器的 IP 地址或域名
- 备份服务器 1：主服务器的 IP 地址或域名
- 备份服务器 2：（RADIUS 和 LDAP）辅助备份服务器的 IP 地址或域名
- 帐户类型：以下一种或多种用户类型：Auth、 L2TP、 Xauth ； 或仅 Admin。
- 超时值：对于不同的用户 （auth 用户或 admin 用户），超时值具有不同的意义。
  - Auth 用户：第一个认证会话完成后开始超时倒计时。如果用户在倒计时达到超时临界值前发起新的会话，则不必重新认证，超时倒计时功能会自动重置。缺省超时值为 10 分钟，最大值为 255 分钟。也可将超时值设置为 0，此时认证周期将永远不会超时。



注意：*用户认证超时与会话空闲超时不同。如果在预定的时间长度内，某会话中未发生任何活动，NetScreen 设备会自动将该会话从其会话表中移除。*

– Admin 用户：如果空闲时间长度达到超时临界值， NetScreen 设备将终止 admin 会话。要继续管理 NetScreen 设备，admin 必须重新连接到该设备并重新认证。缺省超时值为 10 分钟，最大值为 1000 分钟。也可将超时值设置为 0，此时 admin 会话将永远不会超时。



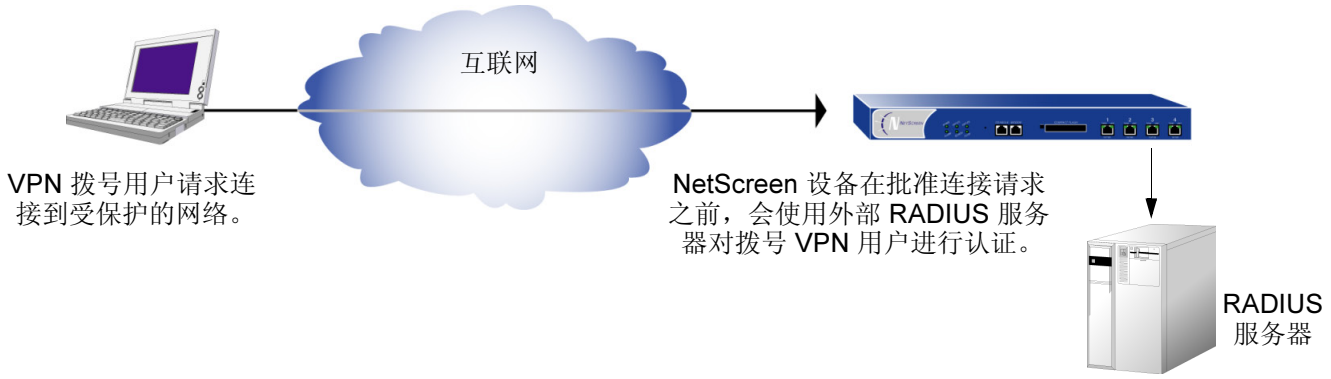
除上述适用于所有 auth 服务器对象的属性外，每个服务器还具有一些自己专有的属性。这些内容将在后续的 RADIUS、 SecurID 和 LDAP auth 服务器属性部分中加以说明。

Auth 服务器类型

除内部数据库外， NetScreen 还支持三种类型的外部 auth 服务器：RADIUS、 SecurID 和 LDAP。

RADIUS

远程认证拨号的用户服务 (RADIUS) 是一个用于认证服务器的协议，它最多可支持几万个用户。



RADIUS 客户端 （即 NetScreen 设备）通过客户端与服务器之间的一系列通信对用户进行认证。通常， RADIUS 会要求登录人员输入其用户名和密码。然后，它将这些值与其数据库中的对应值比较，用户通过认证后，客户端即允许其访问相应的网络服务。

要针对 RADIUS 配置 NetScreen 设备，必须指定 RADIUS 服务器的 IP 地址并定义共享机密 — 与 RADIUS 服务器上的定义相同。共享机密是一个密码， RADIUS 服务器用它来生成密钥，以便对 NetScreen 和 RADIUS 设备之间的信息流进行加密。

RADIUS Auth 服务器对象属性

除第 255 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， RADIUS 服务器还使用以下属性：

- **Shared Secret （共享机密）**：NetScreen 设备与 RADIUS 服务器之间共享的机密 （密码）。设备利用此机密将其向 RADIUS 服务器发送的用户密码进行加密。
- **RADIUS Port （RADIUS 端口）**：RADIUS 服务器上的端口号， NetScreen 设备向此处发送认证请求。缺省端口号为 1645。

支持的用户类型和功能

RADIUS 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 （认证和远程设置）
- XAuth 用户 （认证和远程设置）
- Admin 用户 （认证和权限指派）
- 用户组

RADIUS 服务器可支持本地数据库所支持的所有用户类型和功能。在三种类型的外部 auth 服务器中， RADIUS 是目前唯一能支持如此众多对象的服务器。为了使 RADIUS 服务器能够支持管理权限、用户组及远程 L2TP 和 XAuth IP 地址[1]、 DNS 和 WINS 服务器地址分配等 NetScreen 专用属性，必须在 RADIUS 服务器上加载定义上述属性的 NetScreen 词典文件。

1. NetScreen 使用标准 RADIUS 属性进行 IP 地址分配。如果只想用 RADIUS 进行 IP 地址分配，则不必加载 NetScreen 供应商专用属性 (VSA)。

NetScreen 词典文件

词典文件用于定义可加载到 RADIUS 服务器上的供应商专用属性 (VSA)。定义上述 VSA 的值后，NetScreen 可以在用户登录 NetScreen 设备时查询这些属性。NetScreen VSA 包括管理权限、用户组及远程 L2TP 和 XAuth IP 地址、DNS 和 WINS 服务器地址分配。NetScreen 词典文件共有三个，每个文件对应于下列三种 RADIUS 服务器类型之一：Microsoft、Cisco 和 Funk Software。

每个 NetScreen 词典文件都包含以下具体信息：

- **Vendor ID （供应商 ID）**：NetScreen 供应商 ID （VID；也称 “IETF 编号”）为 3224。 VID 用于识别特殊属性的具体供应商。某些类型的 RADIUS 服务器要求为每个属性条目输入 VID，而其它类型则只要求输入一次，然后即可全局应用。有关详细信息，请参阅 RADIUS 服务器文档。
- **Attribute Name （属性名）**：属性名用于描述各 NetScreen 专用属性，例如 NS-Admin-Privilege、NS-User-Group、 NS-Primary-DNS-Server 等等。
- **Attribute Number （属性编号）**：属性编号用于识别各供应商专用属性。 NetScreen 专用属性编号分为两个范围：
  - NetScreen ScreenOS：1 – 199
  - NetScreen-Global PRO：200 以上

  例如，用户组的 ScreenOS 属性编号为 3。用户组的 NetScreen-Global PRO 属性编号为 200。
- **Attribute Type（属性类型）**：属性类型用于确定属性数据（或“值”）的显示形式 — 字符串、IP 地址或整数。

向 RADIUS 服务器加载 NetScreen 词典文件时，服务器会自动接收上述信息。要输入新数据，必须以属性类型所指定的形式手动输入所需值。例如，为读写 admin 输入如下条目：

VID	属性名	属性编号	属性类型	值
3224	NS-Admin-Privileges	1	data=int4 （即整数）	2 （2 = 全部权限）

可从 www.netscreen.com/support/ 下载词典文件。

SecurID

SecurID 结合两种因素来创建动态变化的密码，而不使用固定密码。 SecurID 具有一个信用卡大小的设备，称为认证器，它拥有一个用于显示随机生成的数字字符串的 LCD 窗口，这种数字字符串称为令牌代码，每分钟变化一次。用户还拥有个人识别号码 (PIN)。用户登录时，需要输入用户名、其 PIN 以及当前令牌代码。

认证器执行只有 RSA 了解的算法，创建 LCD 窗口中出现的值。被认证的用户输入其 PIN 及卡上的号码时，执行相同算法的 ACE 服务器将接收到的值与其数据库中的值进行比较。如果它们匹配，则认证成功。

NetScreen 设备和 RSA SecurID ACE 服务器之间的关系与 NetScreen 设备和 RADIUS 服务器之间的关系相似。即，NetScreen 设备充当客户端，将认证请求转发到外部服务器申请批准，并在用户和服务器之间传递登录信息。SecurID 与 RADIUS 的不同之处在于用户 “密码”中包括不断变化的令牌代码。

SecurID Auth 服务器对象属性

除第 255 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， SecurID 服务器还使用以下属性：

- **Authentication Port（认证端口）**：SecurID ACE 服务器上的端口号，NetScreen 设备向此处发送认证请求。缺省端口号为 5500。
- **Encryption Type （加密类型）**：用于对 NetScreen 设备与 SecurID ACE 服务器之间的通信进行加密的算法 - SDI 或 DES。
- **Client Retries （客户端重试次数）**：放弃尝试之前， SecurID 客户端 （即 NetScreen 设备）尝试建立与 SecurID ACE 服务器的通信的次数。
- **Client Timeout （客户端超时）**：两次认证重试操作之间 NetScreen 设备等待的时间长度 （秒）。
- **Use Duress （使用强迫）**：禁止或允许使用不同 PIN 号码的选项。如果启用此选项，用户输入先前确定的强迫 PIN 号码时，NetScreen 设备会向 SecurID ACE 服务器发送一个信号，指示用户正在违背自己的意愿进行登录；即处于强迫之下。 SecurID ACE 服务器会允许访问一次，之后，它会拒绝该用户的所有进一步登录尝试，直至他 / 她与 SecurID 管理员联系。只有 SecurID ACE 服务器支持此选项时，才可使用强迫模式。

支持的用户类型和功能

SecurID ACE 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 （用户认证； L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置）
- XAuth 用户 （用户认证；不支持远程设置指派）
- Admin 用户 （用户认证； admin 用户接收只读的缺省权限指派）

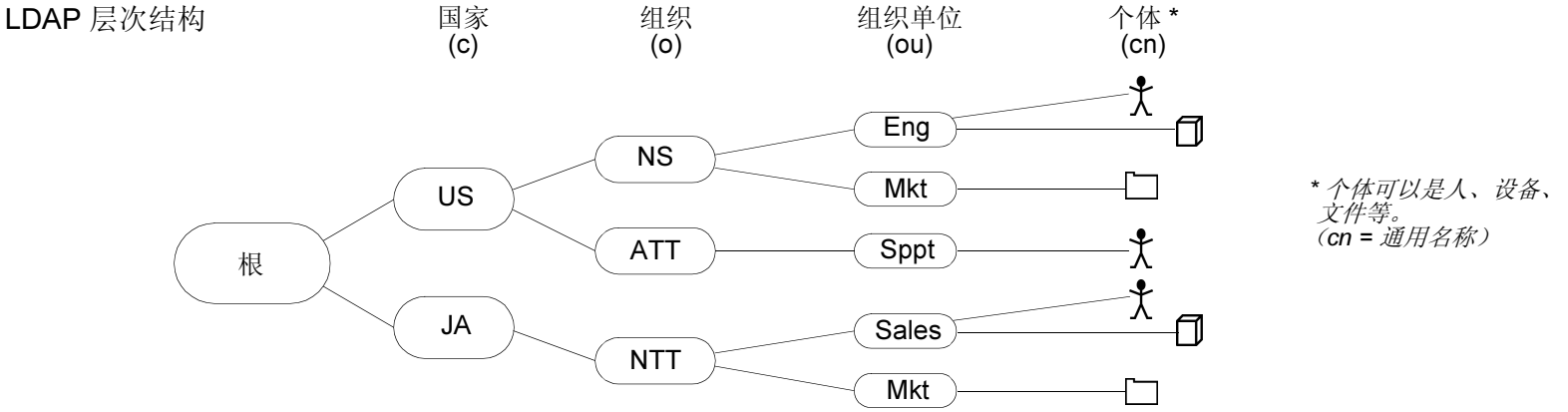
目前，尽管可使用 SecurID 服务器存储 L2TP、 XAuth 和 admin 用户帐户进行认证，但 SecurID ACE 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 SecurID 配套使用时， NetScreen 不支持用户组。

LDAP

轻量目录访问协议 (LDAP) 是密歇根大学在 1996 年开发出来的目录服务器标准。 LDAP 是一个用于以类似分支树的层次结构组织并访问信息的协议。其用途包括两部分：

- 确定资源位置，如网络上的组织、个体和文件等
- 帮助认证用户尝试连接由目录服务器控制的网络

LDAP 的基本结构分支至上而下依次为国家、组织、组织单位、个体。其中间还可包含其它分支层，如“州”和“县”等。下图为 LDAP 分支组织结构的一个范例。



***注意：** 有关 LDAP 的信息，请参阅 RFC-1777 “轻量目录访问协议”。*

可对 NetScreen 设备进行配置，以便链接到“轻量目录访问协议”(LDAP) 服务器。此服务器使用 LDAP 分层式语法来唯一识别每位用户。

LDAP Auth 服务器对象属性

除第 255 页上的 “Auth 服务器对象属性”中列出的通用 auth 服务器属性外， LDAP 服务器还使用以下属性：

- **LDAP Server Port（LDAP 服务器端口）**：LDAP 服务器上的端口号，NetScreen 设备向此处发送认证请求。缺省端口号为 389。

  ***注意：**如果更改 NetScreen 设备上的 LDAP 端口号，同时也应在 LDAP 服务器上进行更改。*

- **Common Name Identifier（通用名称标识符）**：LDAP 服务器用来识别在 LDAP 服务器中输入的个体的标识符。例如，“uid”表示 “用户 ID”，“cn”表示 “通用名称”。
- **Distinguished Name (dn) （识别名称）**：LDAP 服务器在使用通用名称标识符搜索具体条目前使用的路径。（例如 c=us;o=netscreen，其中 “c”代表 “县”，“o”代表 “组织”。）

支持的用户类型和功能

LDAP 服务器支持以下类型的用户和认证功能：

- Auth 用户
- L2TP 用户 （用户认证； L2TP 用户从 NetScreen 设备接收缺省 L2TP 设置）
- XAuth 用户 （用户认证；不支持远程设置指派）
- Admin 用户 （用户认证； admin 用户接收只读的缺省权限指派）

目前，尽管可使用 LDAP 服务器存储 L2TP、 XAuth 和 admin 用户帐户进行认证，但 LDAP 服务器仍不能指派 L2TP 或 XAuth 远程设置或 NetScreen 管理权限。此外，与 LDAP 配套使用时， NetScreen 不支持用户组。

定义 Auth 服务器对象

要在策略、 IKE 网关和 L2TP 通道中引用外部认证服务器 （auth 服务器），必须首先定义 auth 服务器对象。以下示例说明如何为 RADIUS 服务器、 SecurID 服务器和 LDAP 服务器定义 auth 服务器对象。

范例：为 RADIUS 定义 Auth 服务器对象

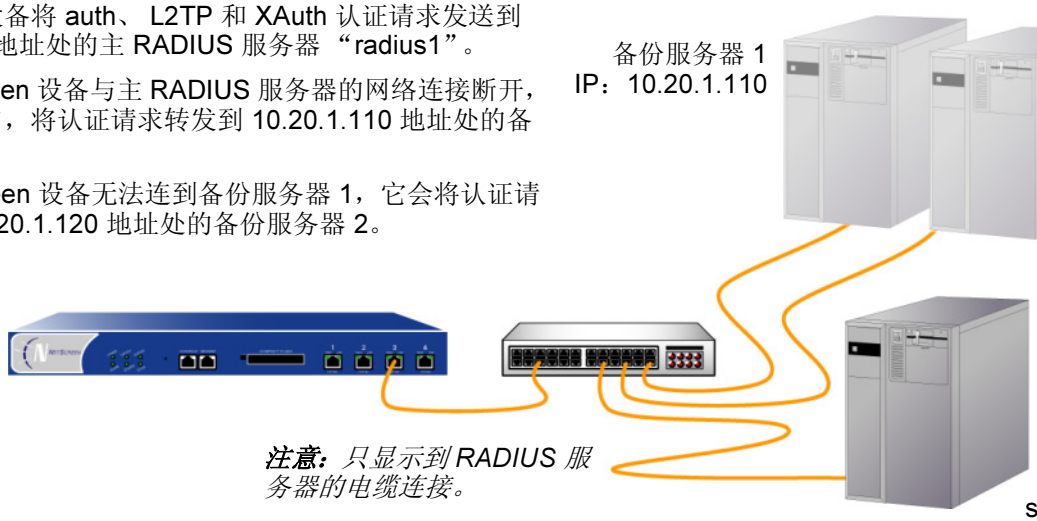
在下例中，将为 RADIUS 服务器定义 auth 服务器对象。将其用户帐户类型指定为 auth、L2TP 和 XAuth。将 RADIUS 服务器命名为“radius1”，并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.1.100 ；将其端口号由缺省值 (1645) 更改为 4500。将其共享机密定义为 “A56htYY97kl”。将超时值由缺省值 （10 分钟）更改为 30 分钟。同时将两个备份服务器的 IP 地址分别指定为 10.20.1.110 和 10.20.1.120。

此外，还要将 NetScreen 词典文件加载到 RADIUS 服务器上，使其能支持下列供应商专用属性 (VSA) 的查询：用户组、管理权限、远程 L2TP 和 XAuth 设置。

NetScreen 设备将 auth、 L2TP 和 XAuth 认证请求发送到 10.20.1.100 地址处的主 RADIUS 服务器 “radius1”。

如果 NetScreen 设备与主 RADIUS 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.1.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1，它会将认证请求转发到 10.20.1.120 地址处的备份服务器 2。



WebUI

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth、L2TP、XAuth

   RADIUS:（选择）

   RADIUS Port: 4500

   Shared Secret: A56htYY97kl

2. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意：*有关 NetScreen 词典文件的详细信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。*

CLI

1. set auth-server radius1 type radius
2. set auth-server radius1 account-type auth l2tp xauth[2]
3. set auth-server radius1 server-name 10.20.1.100
4. set auth-server radius1 backup1 10.20.1.110
5. set auth-server radius1 backup2 10.20.1.120
6. set auth-server radius1 radius-port 4500[3]
7. set auth-server radius1 timeout 30
8. set auth-server radius1 secret A56htYY97kl
9. save
10. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

注意：*有关 NetScreen 词典文件的详细信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关如何将词典文件加载到 RADIUS 服务器的说明，请参阅具体服务器的文档。*

2. 帐户类型的输入顺序非常重要。例如，如果首先键入 **set auth-server radius1 account-type l2tp**，则随后只能选择 **xauth**；不能在 **l2tp** 后键入 **auth**。正确顺序非常容易记住，因为它是按字母顺序排列的。
3. 更改端口号有助于防止可能有针对缺省 RADIUS 端口号 (1645) 展开的攻击。

范例：为 SecurID 定义 Auth 服务器对象

在下例中，将为 SecurID ACE 服务器定义 auth 服务器对象。将其用户帐户类型指定为 admin。将服务器命名为“securid1”，并接受 NetScreen 设备自动指派的 ID 号。输入主服务器的 IP 地址 10.20.2.100，及备份服务器的 IP 地址：10.20.2.110。将其端口号由缺省值 (5500) 更改为 15000。 NetScreen 设备和 SecurID ACE 服务器使用 DES 加密法保护认证信息。允许重试三次，客户端超时值为 10 秒[4]。将空闲超时值由缺省值（10 分钟）更改为 60 分钟[5]。禁用 **Use Duress** 设置。

NetScreen 设备将 admin 认证请求发送到 10.20.2.100 地址处的主 SecurID 服务器 “securid1”。

如果 NetScreen 设备与主 SecurID 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.2.110 地址处的备份服务器 1。

注意：*NetScreen 针对 SecurID 只支持一个备份服务器。*

注意：*只显示了到 SecurID 服务器的电缆连接。*

4. 客户端超时值是指两次认证重试操作之间 SecurID 客户端 （即 NetScreen 设备）等待的时间长度 （秒）。
5. 空闲超时值是指 NetScreen 设备在自动终止非活动 admin 会话前等待的空闲时间长度 （分钟）。（有关应用于 admin 用户和其它用户类型的超时值比较信息，请参阅第 255 页上的 “Auth 服务器对象属性”。）

WebUI

Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

Name: securid1
IP/Domain Name: 10.20.2.100
Backup1: 10.20.2.110
Timeout: 60
Account Type: Admin
SecurID Server:（选择）
Client Retries: 3
Client Timeout: 10 seconds
Authentication Port: 15000
Encryption Type: DES
User Duress: No

CLI

1. set auth-server securid1 type securid
2. set auth-server securid1 server-name 10.20.2.100
3. set auth-server securid1 backup1 10.20.2.110
4. set auth-server securid1 timeout 60
5. set auth-server securid1 account-type admin
6. set auth-server securid1 securid retries 3
7. set auth-server securid1 securid timeout 10
8. set auth-server securid1 securid auth-port 15000
9. set auth-server securid1 securid encr 1
10. set auth-server securid1 securid duress 0
11. save

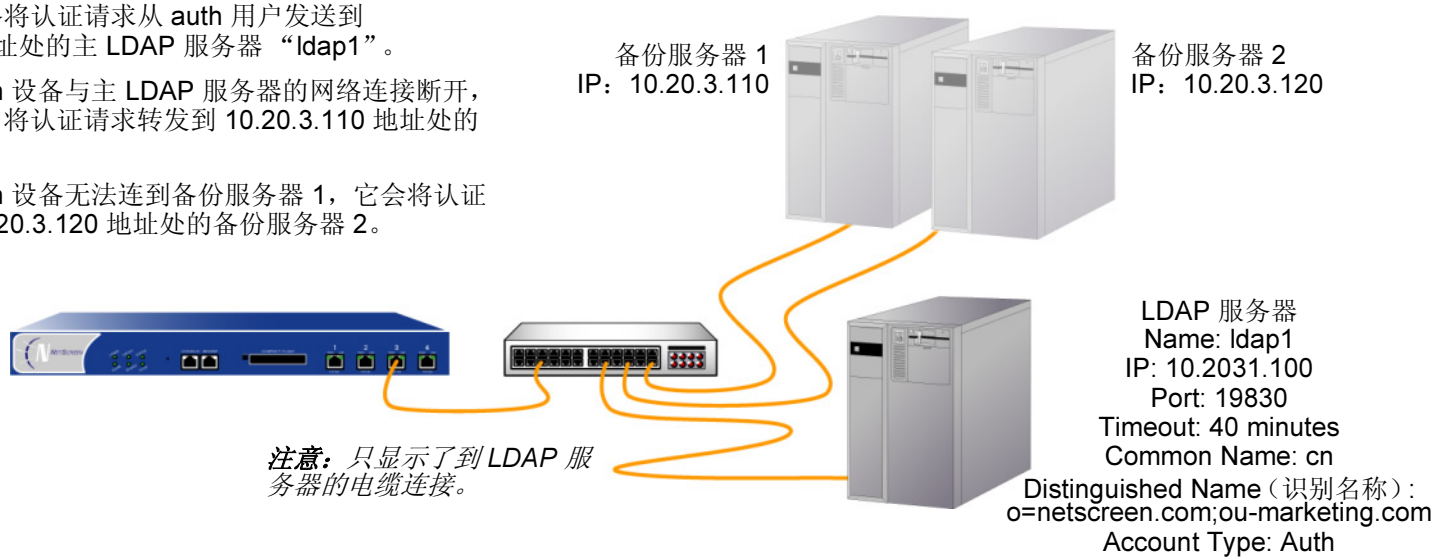
范例：为 LDAP 定义 Auth 服务器对象

在下例中，将为 LDAP 服务器配置 auth 服务器对象。将用户帐户类型指定为 auth。将 LDAP 服务器命名为“ldap1”，并接受 NetScreen 设备自动指派的 ID 号。输入其 IP 地址 10.20.3.100；将其端口号由缺省值 (389) 更改为 19830。将超时值由缺省值（10 分钟）更改为 40 分钟。同时将两个备份服务器的 IP 地址分别指定为 10.20.3.110 和 10.20.3.120。LDAP 通用名称标识符为 cn，Distinguished Name（识别名称）为 c=us;o=netscreen;ou=marketing。

NetScreen 设备将认证请求从 auth 用户发送到 10.20.3.100 地址处的主 LDAP 服务器 “ldap1”。

如果 NetScreen 设备与主 LDAP 服务器的网络连接断开，它会重新定向，将认证请求转发到 10.20.3.110 地址处的备份服务器 1。

如果 NetScreen 设备无法连到备份服务器 1，它会将认证请求转发到 10.20.3.120 地址处的备份服务器 2。



WebUI

Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

Name: ldap1
IP/Domain Name: 10.20.3.100
Backup1: 10.20.3.110
Backup2: 10.20.3.120
Timeout: 40
Account Type: Auth
LDAP:（选择）
LDAP Port: 4500
Common Name Identifier: cn
Distinguished Name (dn): c=us;o=netscreen;ou=marketing

CLI

1. set auth-server ldap1 type ldap
2. set auth-server ldap1 account-type auth
3. set auth-server ldap1 server-name 10.20.3.100
4. set auth-server ldap1 backup1 10.20.3.110
5. set auth-server ldap1 backup2 10.20.3.120
6. set auth-server ldap1 timeout 40
7. set auth-server ldap1 ldap port 15000
8. set auth-server ldap1 ldap cn cn
9. set auth-server ldap1 ldap dn c=us;o=netscreen;ou=marketing cn
10. save

定义缺省 Auth 服务器

缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。您可针对下列一种或多种用户类型，指定外部 auth 服务器作为缺省 auth 服务器：

- Admin
- Auth
- L2TP
- XAuth

这样，在策略、L2TP 通道、或 IKE 网关中配置认证时，如果希望对具体用户类型使用缺省 auth 服务器，则不必在每个配置中都指定 auth 服务器。 NetScreen 设备会引用先前已指定为缺省服务器的相应 auth 服务器。

范例：更改缺省 Auth 服务器

在本例中，将使用先前范例中创建的 RADIUS、 SecurID 和 LDAP auth 服务器对象：

- radius1 （第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”）
- securid1 （第 267 页上的 “范例：为 SecurID 定义 Auth 服务器对象”）
- ldap1 （第 269 页上的 “范例：为 LDAP 定义 Auth 服务器对象”）

然后，指定本地数据库、 radius1、 securid1 和 ldap1 作为下列用户类型的缺省服务器：

- radius1：admin 用户的缺省 auth 服务器
- securid1：L2TP 用户的缺省 auth 服务器
- ldap1：auth 用户的缺省 auth 服务器
- Local：XAuth 用户的缺省 auth 服务器[6]

6. 缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。因此，除非先前已为 XAuth 用户指定外部 auth 服务器作为缺省服务器，否则不必进行此配置。

WebUI

1. Configuration > Admin > Administrators：从 Admin Auth Server 下拉列表中选择 **Local/radius1**，然后单击 **Apply**。
2. VPNs > AutoKey Advanced > XAUTH Settings：从 Default Authentication Server 下拉列表中选择 **Local**，然后单击 **Apply**[7]。

注意：*对于策略中的 auth 用户认证或 IKE 网关中的 XAuth 用户认证，不能在 WebUI 中设置和引用缺省 auth 服务器。必须在要应用用户认证的每个策略和每个 IKE 网关配置中，从下拉列表选择一个 auth 服务器。*

CLI

1. set admin auth server radius1
2. set auth default auth server ldap1
3. set l2tp default auth server securid1
4. set xauth default auth server Local[7]
5. save

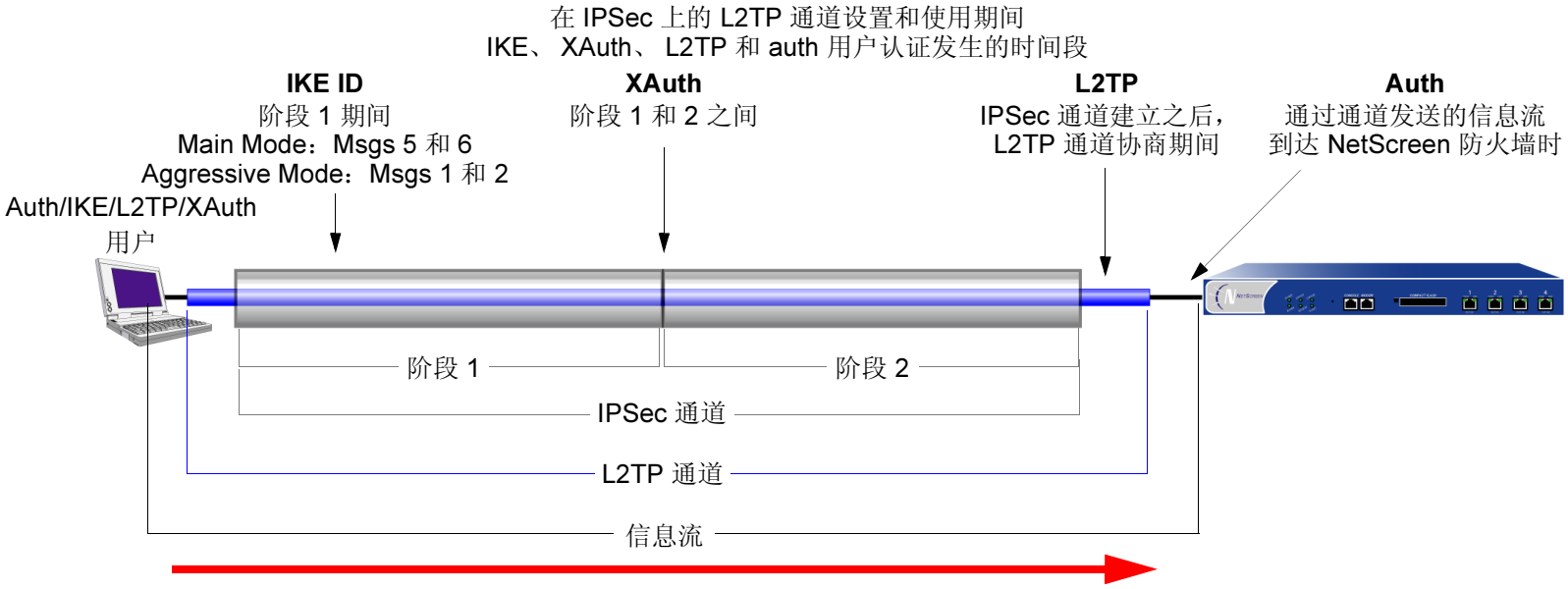
7. 缺省情况下，本地数据库是所有用户类型的缺省 auth 服务器。因此，除非先前已为 XAuth 用户指定外部 auth 服务器作为缺省服务器，否则不必进行此配置。

认证类型及应用

以下部分介绍可以创建的不同类型用户组和用户，以及在配置策略、 IKE 网关、“手动密钥”通道和 L2TP 通道时如何使用它们：

- 第 274 页上的 “Auth 用户和用户组”
- 第 303 页上的 “IKE 用户和用户组”
- 第 308 页上的 “XAuth 用户和用户组”
- 第 328 页上的 “手动密钥用户和用户组”
- 第 335 页上的 “L2TP 用户和用户组”
- 第 340 页上的 “Admin 用户”

NetScreen 设备在连接过程的不同阶段对不同类型的用户进行认证。有关在创建 IPSec 上的 L2TP VPN 通道期间 IKE、 XAuth、 L2TP 和 auth 认证技术运行的时间，请参阅下图：



注意：因为 XAuth 和 L2TP 都提供用户认证和地址分配，故通常它们不同时使用。此处将两者同时显示，只是为了说明 VPN 通道创建期间各种认证类型发生的时间。

Auth 用户和用户组

auth 用户是一个网络用户，启动通过防火墙的连接时，他 / 她必须提供用户名和密码进行认证。可将 auth 用户帐户存储在本地数据库或外部 RADIUS、 SecurID 或 LDAP 服务器上。

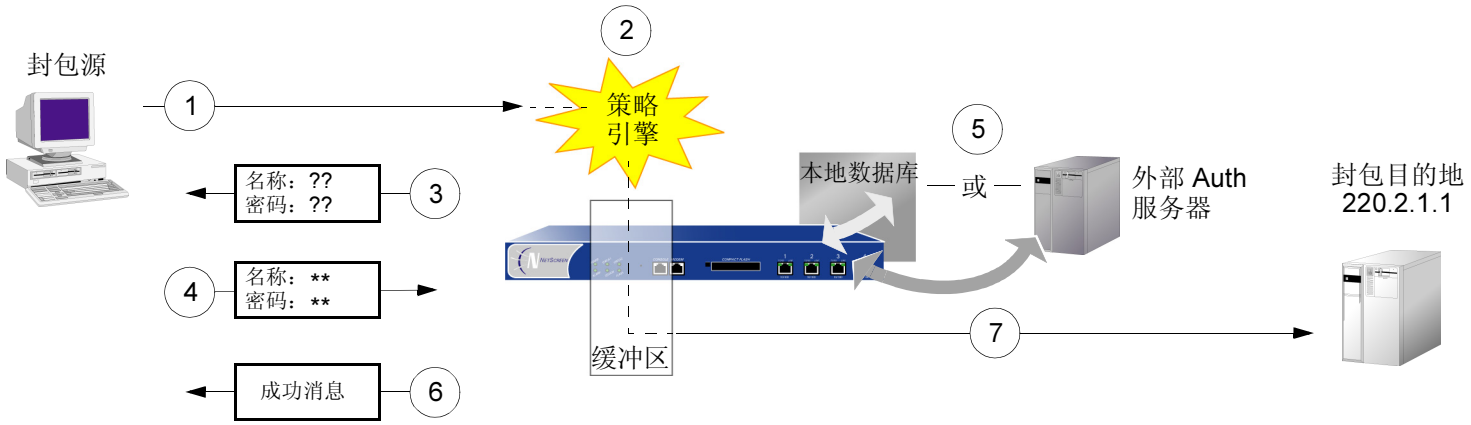
可将多个 auth 用户帐户集合到一起组成 auth 用户组，用户组可以存储在本地数据库或 RADIUS 服务器上。如果在 RADIUS 服务器上创建外部用户组，也必须在 NetScreen 设备上创建一个相同 （但空白）的用户组。例如，如果在名为“rs1”的 RADIUS 服务器上定义一个名为“au_grp1”的 auth 用户组，并在组中添加 10 个成员，则在 NetScreen 设备上必须也定义一个名为 “au_grp1” 的 auth 用户组，将其标识为外部用户组，但不能在其中添加成员。如果在策略中引用外部 auth 用户组 “au_grp1” 和 auth 服务器 “rs1” ，则当与该策略匹配的信息流引发认证检查时，NetScreen 设备可以正确查询指定的 RADIUS 服务器。

在策略中引用 Auth 用户

定义 auth 用户后，可创建一个要求用户通过两种认证方案之一进行认证的策略。第一种方案在与要求认证的策略匹配的 FTP、 HTTP 或 Telnet 信息流到达 NetScreen 设备时，对用户进行认证。在第二种方案中，用户在发送应用要求用户认证的策略的信息流 （任何类型，不局限于 FTP、 HTTP 或 Telnet）之前进行认证。

运行时认证

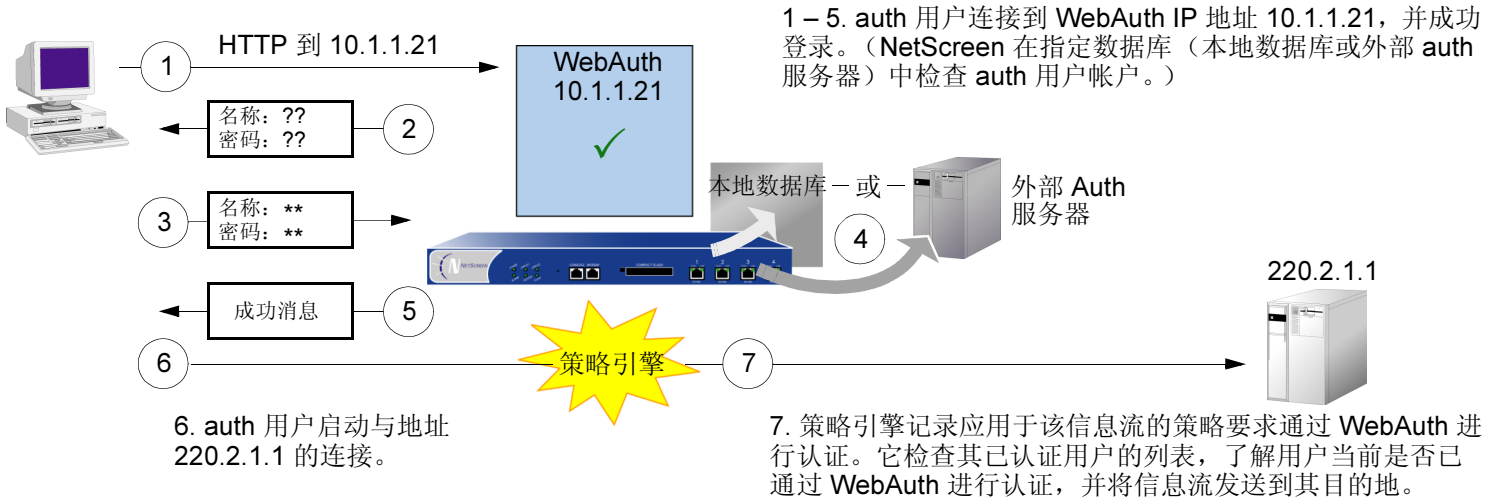
用户尝试启动（应用要求进行认证的策略的）HTTP、FTP 或 Telnet 连接请求时，NetScreen 设备会截取该请求，并提示用户输入名称和密码（请参阅第 225 页上的“用户认证”）。在批准请求之前，NetScreen 设备会将用户名和密码与本地数据库或外部 auth 服务器上的用户名和密码进行比较，以确认其有效性。



1. auth 用户将 FTP、HTTP 或 Telnet 封包发送到 220.2.1.1。
2. NetScreen 设备截取封包，记录其策略要求从本地数据库或 auth 服务器获得认证，并将封包放入缓冲区。
3. NetScreen 设备提示用户通过 FTP、HTTP 或 Telnet 输入登录信息。
4. 用户以用户名和密码回复。
5. NetScreen 设备在其本地数据库上检查 auth 用户帐户，或将登录信息发送到策略中指定的外部 auth 服务器。
6. 找到有效匹配项（或从外部 auth 服务器接收到有效匹配的通告）后，NetScreen 设备会通知用户登录成功。
7. NetScreen 设备将封包从其缓冲区转发到其目的地 220.2.1.1。

策略前检查认证 (WebAuth)

将信息流发送到预定目的地之前，auth 用户启动面向此 IP 地址的 HTTP 会话（将 WebAuth 功能交由 NetScreen 设备托管），并对自己进行认证。NetScreen 设备对用户进行认证后，用户可根据要求通过 WebAuth 进行认证的策略的许可，将信息流发送目的地。（有关详细信息，请参阅第 274 页上的 “Auth 用户和用户组”。）



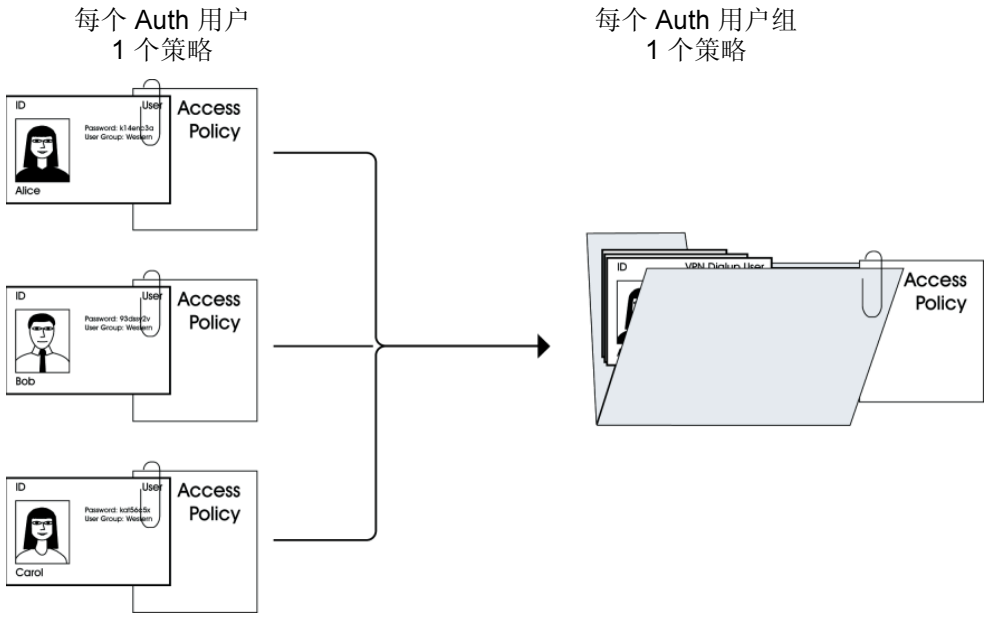
有关 WebAuth 的一些详细说明：

- 可保留本地数据库作为缺省 WebAuth auth 服务器，也可为之选择外部 auth 服务器。符合 WebAuth auth 服务器条件的主要要求是：auth 服务器必须具有 auth 用户帐户类型。
- WebAuth 地址必须与要用来托管该地址的接口处于相同的子网内。例如，如果希望 auth 用户通过 ethernet3（IP 地址为 210.1.1.1/24）与 WebAuth 相连，则应将 WebAuth 的 IP 地址指定在 210.1.1.0/24 子网内。
- 可将 WebAuth 地址设置在与任意物理接口、子接口或虚拟安全接口 (VSI) 相同的子网内。（有关不同类型接口的信息，请参阅第 81 页上的 “接口”。）

- 如果要在透明模式中使用 WebAuth，可将 WebAuth 地址设置在与 VLAN1 IP 地址相同的子网内。
- 可将 WebAuth 地址设置于多个接口上。
- 如果在同一安全区段绑定多个接口，则可将 WebAuth 地址设置于某个接口上，来自同一区段但使用不同接口的信息流仍可到达该处。

在策略中引用 Auth 用户组

要管理多个 auth 用户，可创建 auth 用户组，并将其存储在本地 NetScreen 设备或外部 RADIUS 服务器上。您可将用户集合成组，使对此组实施的任何更改应用于所有的组成员，而不必分别管理每个用户。



范例：运行时认证 （本地用户）

在本例中，将定义一个名为 louis 的本地 auth 用户，其密码为 iDa84rNk，在Trust 区段通讯簿中的地址名为“host1”。然后配置两个外向策略：一个拒绝所有出站信息流，另一个来自 host1，要求 louis 进行认证。（Louis 必须启动所有来自 host1 的出站信息流。）NetScreen 设备会拒绝来自其它所有地址的出站访问请求以及来自“host1”的未经认证信息流。

WebUI

本地 Auth 用户和地址

1. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：

   User Name: louis

   Status: Enable

   Authentication User:（选择）

   Password: iDa84rNk

   Confirm Password: iDa84rNk

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

   Address Name: host1

   IP Address/Domain Name:

   IP/Netmask:（选择）, 10.1.4.1/32

   Zone: Trust

策略

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, Any

   Service: ANY

   Action: Deny

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

   Source Address:

   Address Book:（选择）, host1

   Destination Address:

   Address Book:（选择）, Any

   Service: ANY

   Action: Permit

   Position at Top:（选择）

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

   Authentication:（选择）

   Auth Server:（选择）, Local

   User:（选择）, Local Auth User - louis

CLI

本地用户和地址

1. set user louis password iDa84rNk[8]
2. set address trust host1 10.1.1.4/32

策略

3. set policy from trust to untrust any any any deny
4. set policy top from trust to untrust host1 any any permit auth user louis
5. save

8. 缺省情况下，要为之指定密码的用户被归类为 auth 用户。

范例：运行时认证 （本地用户组）

在本例中，将定义一个名为 auth_grp1 的本地用户组。将先前创建的 auth 用户 louis 和 lara 添加到该组中[9]。然后配置一个引用 auth_grp1 的策略。此策略为 auth_grp1 提供 FTP 取放权限，令其以 Trust 区段中 “auth_grp1” 地址名（IP 地址 10.1.8.0/24）访问 DMZ 区段中名为 “ftp1”（IP 地址 220.1.1.3/32）的 FTP 服务器。

WebUI

本地用户组和成员

1. Objects > User Groups > Local > New：在 Group Name 字段中键入 **auth_grp1**，执行以下操作，然后单击 **OK**：

   选择 **louis**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

   选择 **lara**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

地址

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

   Address Name: auth_grp1

   IP Address/Domain Name:

   IP/Netmask:（选择）, 10.1.8.0/24

   Zone: Trust

9. 在本地数据库中创建用户组时，在向组中添加用户之前，用户组的用户类型不会定义。而添加用户后，用户组会获得与添加于其中的用户相同的类型。通过添加 auth、 IKE、 L2TP 和 XAuth 用户类型可创建多类型用户组。不能将 “手动密钥” 用户和 Admin 用户与其它任意用户类型组合。

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

   Address Name: ftp1

   IP Address/Domain Name:

   IP/Netmask:（选择）, 220.1.1.3/32

   Zone: DMZ

策略

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

   Source Address:

   Address Book:（选择）, auth_grp1

   Destination Address:

   Address Book:（选择）, ftp1

   Service: FTP

   Action: Permit

   Position at Top:（选择）

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

   Authentication:（选择）

   Auth Server:（选择）, Local

   User Group:（选择）, Local Auth Group - auth_grp1

CLI

本地用户组和成员

1. set user-group auth_grp1 location local
2. set user-group auth_grp1 user louis
3. set user-group auth_grp1 user lara

地址

4. set address trust auth_grp1 10.1.8.0/24
5. set address dmz ftp1 220.1.1.3/32

策略

6. set policy top from trust to dmz auth_grp1 ftp1 ftp permit auth user-group auth_grp1
7. save

范例：运行时认证 （外部用户）

在本例中，将定义名为 “x_srv1”的外部 LDAP auth 服务器，其属性如下：

- Account type: auth
- IP address: 10.1.1.100
- Backup1 IP address: 10.1.1.110
- Backup2 IP address: 10.1.1.120
- Authentication timeout: 60 minutes
- LDAP port number: 14500
- Common name identifier: cn
- Distinguished name: c=us;o=netscreen

以密码 eTcS114u 将 auth 用户 “euclid”加载到外部 auth 服务器上。然后，为外部用户 euclid 配置要求在 auth 服务器 x_srv1 上进行认证的外向策略。

WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: x_srv1

   IP/Domain Name: 10.1.1.100

   Backup1: 10.1.1.110

   Backup2: 10.1.1.120

   Timeout: 60

   Account Type: Auth

   LDAP:（选择）

   LDAP Port: 14500

   Common Name Identifier: cn

   Distinguished Name (dn): c=us;o=netscreen

外部用户

2. 在外部 LDAP auth 服务器 x_serv1 上定义 auth 用户“euclid”，密码为 eTcS114u。

地址

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

   Address Name: euc_host

   IP/Netmask:（选择）, 10.1.1.20/32

   Zone: Trust

策略

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, Any

   Service: ANY

   Action: Permit

   Position at Top:（选择）

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

   Authentication:（选择）

   Auth Server:（选择）, x_srv1

   User:（选择）, External User

   External User: euclid

CLI

Auth 服务器

1. set auth-server x_srv1
2. set auth-server x-srv1 type ldap
3. set auth-server xsrv1 account-type auth
4. set auth-server x_srv1 server-name 10.1.1.100
5. set auth-server lx_srv1 backup1 10.1.1.110
6. set auth-server x_srv1 backup2 10.1.1.120
7. set auth-server x_srv1 timeout 60
8. set auth-server x_srv1 ldap port 14500
9. set auth-server x_srv1 ldap cn cn
10. set auth-server x_srv1 ldap dn c=us;o=netscreen

外部用户

11. 在外部 LDAP auth 服务器 x_serv1 上定义 auth 用户“euclid”，密码为 eTcS114u。

地址

12. set address trust euc_host 10.1.1.20/32

策略

13. set policy top from trust to untrust euc_host any any auth server x_srv1 user euclid
14. save

范例：运行时认证 （外部用户组）

在本例中，将配置名为 “radius1”[10] 的外部 RADIUS auth 服务器，定义名为 “auth_grp2” 的外部 auth 用户组。在下列两个位置定义外部 auth 用户组 auth_grp2：

1. 外部 RADIUS auth 服务器“radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 auth 用户装入 auth 用户组 “auth_grp2” 中，而将 NetScreen 设备上的组保留为空白。此组中的成员是要求独占访问 IP 地址 10.1.1.80 处服务器的帐户用户。为该服务器创建一个通讯簿条目，并将地址命名为 “midas”。然后配置一个内部区段策略，只允许已经认证的信息流从 auth_grp2 流向 midas，这两者均位于 Trust 区段中。（有关内部区段策略的详细信息，请参阅第 7 章 “策略”。）

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意：*有关 NetScreen 词典文件的信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 RADIUS 服务器上定义 auth 用户帐户后，使用 NetScreen 用户组 VSA 创建用户组“auth_grp2”，并将其应用于要添加到该组中的 auth 用户帐户。

10. RADIUS auth 服务器的配置与第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”中大致相同，但本例中仅指定 “auth”作为用户帐户类型。

WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：
   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: Auth
   RADIUS:（选择）
   RADIUS Port: 4500
   Shared Secret: A56htYY97kl

外部用户组

2. Objects > User Groups > External > New：输入以下内容，然后单击 **OK**：
   Group Name: auth_grp2
   Group Type: Auth

地址

3. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: midas
   IP Address/Domain Name:
   IP/Netmask:（选择）, 10.1.1.80/32
   Zone: Trust

策略

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, midas

   Service: ANY

   Action: Permit

   Position at Top:（选择）

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

   Authentication: （选择）

   Auth Server: （选择）, radius1

   User Group: （选择）, External Auth Group - auth_grp2

CLI

Auth 服务器

1. set auth-server radius1 type radius
2. set auth-server radius1 account-type auth
3. set auth-server radius1 server-name 10.20.1.100
4. set auth-server radius1 backup1 10.20.1.110
5. set auth-server radius1 backup2 10.20.1.120
6. set auth-server radius1 radius-port 4500
7. set auth-server radius1 timeout 30
8. set auth-server radius1 secret A56htYY97kl

外部用户组

9. set user-group auth_grp2 location external
10. set user-group auth_grp2 type auth

地址

11. set address trust midas 10.1.1.80/32

策略

12. set policy top from trust to trust any midas any permit auth server radius1 user-group auth_grp2
13. save

范例：WebAuth （本地用户组）

本例中，在启动流向互联网的出站信息流之前，要求用户通过 WebAuth 方式进行预认证。在 NetScreen 设备上的本地数据库中创建名为 “auth_grp3”的用户组。然后，为 Trust 区段中的每个对象创建 auth 用户帐户，并将其添加到“auth_grp3”中。

Trust 区段接口使用 ethernet1，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 WebAuth IP 地址，并保留本地数据库作为缺省的 WebAuth 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 10.1.1.50，并以用户名和密码登录。然后，NetScreen 设备将该用户名和密码与其数据库中的内容进行比较，以批准或拒绝认证请求。如果它批准该请求，被认证的用户将有 60 分钟的时间启动流向互联网的信息流。终止该启动会话后，在 NetScreen 设备要求用户重新认证之前，用户又有 60 分钟的时间启动另一会话。

WebUI

WebAuth

1. Configuration > Auth > WebAuth：从 WebAuth Server 下拉列表中选择 **Local**，然后单击 **Apply**。
2. Network > Interfaces > Edit（对于 ethernet1）：选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.1.1.50**。
3. Configuration > Auth > Auth Servers > Edit（对于 Local）：在 Timeout 字段中输入 **30**，然后单击 **Apply**。

用户组

4. Objects > User Groups > Local > New：在 Group Name 字段中键入 **auth_grp3**，执行以下操作，然后单击 **OK**：

   选择 ***user name***，使用 **<<** 按钮将该用户从 Available Members 栏移动到 Group Members 栏中。

   重复选择过程，添加 auth 用户，直到该组完成为止。

策略

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

Source Address:

Address Book:（选择）, Any

Destination Address:

Address Book:（选择）, Any

Service: ANY

Action: Permit

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

Authentication:（选择）

WebAuth:（选择）

User Group:（选择）, Local Auth Group - auth_grp3

CLI

WebAuth

1. set webauth auth-server Local
2. set interface ethernet1 webauth-ip 10.1.1.50
3. set interface ethernet1 webauth
4. set auth-server Local timeout 30

用户组

5. set user-group auth_grp3 location local

> ***注意：****NetScreen 设备根据添加于本地用户组中的成员类型来确定组的类型。要使 auth_grp3 成为 auth 用户组，应在组中添加一个 auth 用户。*

6. 使用以下命令将 auth 用户添加到刚刚创建的用户组中：
   set user-group auth_grp3 user *name_str*

策略

7. set policy top from trust to untrust any any any permit webauth user-group auth_grp3
8. save

范例：WebAuth （外部用户组）

WebAuth 是一种用于在用户启动通过防火墙的信息流之前进行预认证的方法。在本例中，将创建一个要求对所有外向信息流通过 WebAuth 方法进行认证的策略。

在 RADIUS 服务器“radius1”和 NetScreen 设备上创建名为“auth_grp4”的 auth 用户组。在 RADIUS 服务器上，为 Trust 区段中的每个对象创建用户帐户，并将其添加到 “auth_grp4”中。

注意：*此处使用的 RADIUS 服务器设置与第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”中大致相同，但本例中仅指定 “auth”作为用户帐户类型。*

Trust 区段接口使用 ethernet1，其 IP 地址为 10.1.1.1/24。指定 10.1.1.50 作为 WebAuth IP 地址，并使用外部 RADIUS auth 服务器“radius1”作为缺省的 WebAuth 服务器。因此，用户在启动流向互联网的信息流之前，必须首先以 HTTP 方式连接到 10.1.1.50，并以用户名和密码登录。然后， NetScreen 设备在“radius1”和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意：*有关 NetScreen 词典文件的信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 auth 服务器“radius1”上输入用户组“auth_grp4”，然后在其中装入 auth 用户帐户。

WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: radius1

   IP/Domain Name: 10.20.1.100

   Backup1: 10.20.1.110

   Backup2: 10.20.1.120

   Timeout: 30

   Account Type: Auth

   RADIUS:（选择）

   RADIUS Port: 4500

   Shared Secret: A56htYY97k

WebAuth

2. Configuration > Auth > WebAuth：从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。
3. Network > Interfaces > Edit（对于 ethernet1）：选择 **WebAuth**，在 WebAuth IP 字段中输入 **10.10.1.50**，然后单击 **OK**。

用户组

4. Objects > User Groups > External > New：输入以下内容，然后单击 **OK**：

   Group Name: auth_grp4

   Group Type: Auth

策略

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

Source Address:

Address Book:（选择）, Any

Destination Address:

Address Book:（选择）, Any

Service: ANY

Action: Permit

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

Authentication:（选择）

WebAuth:（选择）

User Group:（选择）, External Auth Group - auth_grp4

CLI

Auth 服务器

1. set auth-server radius1 type radius
2. set auth-server radius1 account-type auth
3. set auth-server radius1 server-name 10.20.1.100
4. set auth-server radius1 backup1 10.20.1.110
5. set auth-server radius1 backup2 10.20.1.120
6. set auth-server radius1 radius-port 4500
7. set auth-server radius1 timeout 30
8. set auth-server radius1 secret A56htYY97kl

WebAuth

9. set webauth auth-server radius1
10. set interface ethernet1 webauth-ip 10.1.1.50
11. set interface ethernet1 webauth

用户组

12. set user-group auth_grp4 location external
13. set user-group auth_grp4 type auth

策略

14. set policy top from trust to untrust any any any permit webauth user-group auth_grp4
15. save

范例：WebAuth + SSL （外部用户组）

在本例中，将 WebAuth 与“安全套接字层”(SSL) 技术组合，来保护用户登录时发送的用户名和密码。WebAuth 利用相同的证书来保护流向 NetScreen 设备的管理信息流 （以通过 WebUI 进行管理）。（有关 SSL 的详细信息，请参阅第 **3**-9 页上的 “安全套接字层”。）

WebAuth + SSL 的配置包括以下四个步骤：

1. 定义外部 RADIUS auth 服务器“radius1”，在 RADIUS 服务器和 NetScreen 设备上创建名为“auth_grp5”的 auth 用户组。在 RADIUS 服务器上，为 Untrust 区段中的所有 auth 用户创建用户帐户，并将其添加到“auth_grp5”中。

   注意：*此处使用的 RADIUS 服务器设置与第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”中大致相同，但本例中仅指定 “auth” 作为用户帐户类型。*

2. Untrust 区段接口使用 ethernet3，其 IP 地址为 210.1.1.1/24。指定 210.1.1.50 作为 WebAuth IP 地址，并使用外部 RADIUS auth 服务器“radius1”作为缺省的 WebAuth 服务器。
3. 针对 NetScreen SSL 设置，指定先前加载到 NetScreen 设备上的证书[11] 的 IDX 号（本例中为 1）、DES_SHA-1 密码和 SSL 端口号 2020。此外，还必须在 ethernet3 上启用 SSL 可管理性，以便 ethernet3 不会拒绝面向该接口的 SSL 连接尝试。
4. 然后，配置一个要求对从 Untrust 区段到 Trust 区段的所有信息流通过 WebAuth + SSL 方法进行认证的内向策略。

因此，用户在启动流向因特网的信息流之前，必须首先以 HTTP 方式连接到 https://210.1.1.50:2020，并以用户名和密码登录。然后， NetScreen 设备在 “radius1” 和尝试登录的用户之间中继所有 WebAuth 用户认证请求及响应。

11. 有关如何获取数字证书并将其加载到 NetScreen 设备的信息，请参阅第 4 卷 “VPN”。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   ***注意：**有关 NetScreen 词典文件的信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在 auth 服务器“radius1”上输入用户组“auth_grp5”，然后在其中装入 auth 用户帐户。

WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: Auth
   RADIUS:（选择）
   RADIUS Port: 4500
   Shared Secret: A56htYY97k

WebAuth

2. Configuration > Auth > WebAuth：从 WebAuth Server 下拉列表中选择 **radius1**，然后单击 **Apply**。
3. Network > Interfaces > Edit（对于 ethernet3）：选择 **WebAuth**，在 WebAuth IP 字段中输入 **210.1.1.50**，然后单击 **OK**。

SSL

4. Configuration > Admin > Management：输入以下内容，然后单击 **OK**：

   HTTPS (SSL) Port: 2020

   Certificate:（选择先前加载的证书）

   Cipher: DES_SHA-1

5. Network > Interfaces > Edit（对于 ethernet3）：在 Management Services 区域中选择 **SSL**，然后单击 **OK**。

用户组

6. Objects > User Groups > External > New：输入以下内容，然后单击 **OK**：

   Group Name: auth_grp5

   Group Type: Auth

策略

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

   Source Address:

   Address Book:（选择）, Any

   Destination Address:

   Address Book:（选择）, Any

   Service: ANY

   Action: Permit

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

   Authentication: （选择）

   WebAuth: （选择）

   User Group: （选择）, External Auth Group - auth_grp5

CLI

Auth 服务器

1. set auth-server radius1 type radius
2. set auth-server radius1 account-type auth
3. set auth-server radius1 server-name 10.20.1.100
4. set auth-server radius1 backup1 10.20.1.110
5. set auth-server radius1 backup2 10.20.1.120
6. set auth-server radius1 radius-port 4500
7. set auth-server radius1 timeout 30
8. set auth-server radius1 secret A56htYY97kl
9. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

> ***注意：****有关 NetScreen 词典文件的信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

WebAuth

10. set webauth auth-server radius1
11. set interface ethernet3 webauth-ip 210.1.1.50
12. set interface ethernet3 webauth

SSL

13. set ssl port 2020
14. set ssl port cert 1
15. set ssl encrypt des sha-1
16. set ssl enable

用户组

17. set user-group auth_grp5 location external
18. set user-group auth_grp5 type auth

策略

19. set policy top from untrust to trust any any any permit webauth user-group auth_grp5
20. save

IKE 用户和用户组

IKE 用户是具有动态分配 IP 地址的远程 VPN 用户。用户（实际上是用户的设备）在“阶段 1”与 NetScreen 设备协商期间，通过发送 IKE ID 及证书或预共享密钥，来对自身进行认证。

IKE ID 可以是电子邮件地址、IP 地址、域名或 ASN1-DN 字符串[12]。如果某 IKE 用户发送以下内容，NetScreen 设备将认证此 IKE 用户：

- **证书**，其中 Distinguished name (DN)（识别名称）字段或 SubAltName 字段中的一个或多个值与 NetScreen 设备上配置的用户 IKE ID 相同。
- **预共享密钥**和 **IKE ID**， NetScreen 设备可从接收的 IKE ID 及其上存储的预共享密钥种子值成功生成相同的预共享密钥

在“自动密钥”IKE 网关配置中引用 IKE 用户或用户组。将需要相同网关和通道配置的 IKE 用户集合到一个组中后，只需定义一个引用该组的网关（和一个引用该网关的 VPN 通道），而不必为每个 IKE 用户定义一个网关和通道。

通常，为每个主机创建独立的用户帐户是不可能的。这种情况下，可创建只具有一个成员的 IKE 用户组，作为一个组 IKE ID 用户。该用户的 IKE ID 包含一组必须出现在拨号 IKE 用户的 IKE ID 定义中的值。如果远程拨号 IKE 用户的 IKE ID 与组 IKE ID 用户的 IKE ID 相匹配， NetScreen 将认证该远程用户。有关详细信息，请参阅*第 4-180 页上的“组 IKE ID”*。

注意：*IKE 用户和 IKE 用户组帐户只能存储在本地数据库上。*

12. 使用“抽象语法表示法”版本 1 的一个 IKE ID 示例，识别名称 (ASN1-DN) 格式为：CN=joe,OU=it,O=netscreen,L=sunnyvale,ST=ca,C=us,E=joe@ns.com。

范例：定义 IKE 用户

在本例中，将定义四个 IKE 用户， Amy、 Basil、 Clara 和 Desmond，每个用户具有不同的 IKE ID 类型。

- Amy – 电子邮件地址 （用户完全合格的域名或 U-FQDN）：amy@ns.com
- Basil – IP 地址：211.13.1.1
- Clara – 完全合格的域名 (FQDN)：www.netscreen.com
- Desmond – ASN1-DN 字符串：CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com

WebUI

1. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：
   User Name: Amy
   Status: Enable
   IKE User:（选择）
   Simple Identity:（选择）
   IKE Identity : amy@ns.com
2. Lists > Users > Local > New：输入以下内容，然后单击 **OK**：
   User Name: Basil
   Status: Enable
   IKE User:（选择）
   Simple Identity:（选择）
   IKE Identity : 211.13.1.1

3. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：
   User Name: Clara
   Status: Enable
   IKE User:（选择）
   Simple Identity:（选择）
   IKE Identity : www.netscreen.com
4. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：
   User Name: Desmond
   Status: Enable
   IKE User:（选择）
   Use Distinguished Name for ID:（选择）
   CN : des
   OU: art
   Organization: netscreen
   Location: sunnyvale
   State: ca
   Country: us
   E-mail: des@ns.com

CLI

1. set user Amy ike-id u-fqdn amy@ns.com
2. set user Basil ike-id ip 211.13.1.1
3. set user Clara ike-id fqdn www.netscreen.com
4. set user Desmond ike-id wildcard CN=des,OU=art,O=netscreen,L=sunnyvale,ST=ca,C=us,E=des@ns.com
5. save

范例：创建 IKE 用户组

在本例中，将创建一个名为 ike_grp1 的用户组。向其中添加 IKE 用户 Amy 时，它即成为 IKE 用户组。然后添加上例第 304 页上的 “范例：定义 IKE 用户”中定义的其它三个 IKE 用户。

WebUI

Objects > User Groups > Local > New：在 Group Name 字段中键入 **ike_grp1**，执行以下操作，然后单击 **OK**：

选择 **Amy**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Basil**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Clara**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Desmond**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

CLI

1. set user-group ike_grp1 location local
2. set user-group ike_grp1 user amy
3. set user-group ike_grp1 user basil
4. set user-group ike_grp1 user clara
5. set user-group ike_grp1 user desmond
6. save

在网关中引用 IKE 用户

定义 IKE 用户或 IKE 用户组后，当远程 IKE 网关是一个拨号用户或拨号用户组时，可在 IKE 网关配置中引用它。以下为在网关配置中引用 IKE 用户的范例：

- 第 **4**-163 页上的 “范例：基于策略的拨号到 LAN 的 VPN，自动密钥 IKE”
- 第 **4**-186 页上的 “范例：组 IKE ID （证书）”
- 第 **4**-195 页上的 “范例：组 IKE ID （预共享密钥）”

XAuth 用户和用户组

XAuth 是一个远程用户，它通过 “自动密钥” IKE VPN 通道与 NetScreen 设备相连。 XAuth 包括两个部分：用户认证和 TCP/IP 地址分配。 NetScreen 支持其中一项或两项同时应用。

IKE 用户认证实际是对个体的设备的认证，而 XAuth 用户的认证则是对个体自身的认证。

远程 TCP/IP 设置的分配可为远程用户提供一个虚拟适配器[13]，用户在发送 VPN 信息流时可使用此虚拟适配器，而对于非 VPN 信息流则使用 ISP 或网络管理员提供的 TCP/IP 网络适配器设置。通过为远程用户分配已知的 IP 地址，可定义通过特定通道接口到达此地址的路由。然后，NetScreen 设备可以确保返回路由通过 VPN 通道而非缺省网关，到达远程用户的 IP 地址。地址分配还允许下游防火墙在创建策略时引用这些地址。

在网关中引用 XAuth 用户

NetScreen 支持 XAuth 版本 6 (v6)。为确保 “阶段 1” IKE 协商中的双方都支持 XAuth v6，它们在前两个 “阶段 1” 消息中都向对方发送以下供应商 ID：0x09002689DFD6B712。此供应商 ID 号在 XAuth 互联网草案 draft-beaulieu-ike-xauth-02.txt 中指定。

“阶段 1” 协商完成后，NetScreen 设备向远程站点的 XAuth 用户发送登录提示。如果 XAuth 用户使用正确的用户名和密码成功登录， NetScreen 设备将为该用户分配 TCP/IP 设置，双方继续进行 “阶段 2” 协商。

13. 虚拟适配器是 TCP/IP 设置 （IP 地址、 DNS 服务器地址、 WINS 服务器地址），它由 NetScreen 设备分配给远程用户，以在 VPN 通道连接期间使用。

XAuth 分配的 IP 地址在指定的 XAuth 地址超时期间属于某用户。到达超时时限后，用户会接收新的 IP 地址，它可能与先前分配的地址[14] 相同，也可能不同。可将 XAuth 超时值定义为大于 IKE “阶段 1”生存期时间的值，以避免在会话期间 IP 地址意外更改。

到达 IKE “阶段 1”生存期后， IKE 会商定一个 “阶段 1”重定密钥，然后在 “阶段 2”协商开始前再次提示 XAuth 用户登录。如果尚未达到 XAuth 地址超时期限， XAuth 用户将在成功登录后再次接收到相同的 IP 地址。 IKE “阶段 1”协商结束后，开始进行 XAuth 用户认证。XAuth 地址分配最初在用户登录成功后进行，而在 XAuth 地址超时时间到期时再次开始。这两次操作彼此独立。

NetScreen 设备可以向 XAuth 用户随机分配 IP 地址、DNS 服务器地址和 WINS 服务器地址。NetScreen 支持 XAuth 的以下方面：

- 本地 XAuth 用户和外部 XAuth 用户的认证
- 本地 XAuth 用户组和外部 XAuth 用户组的认证 （如果存储在 RADIUS auth 服务器上）
- 从 IP 地址池为本地 XAuth 用户和 RADIUS auth 服务器上存储的外部 XAuth 用户分配 IP、 DNS 服务器和 WINS 服务器地址

14. 如果必须为某个用户始终分配相同的 IP 地址，则可在用户配置中指定地址。此 NetScreen 设备会分配此地址，而不是从 IP 池中随机分配一个地址。请注意，这样的地址不能在 IP 池中，否则，它可能会被分配给其它用户，而在需要时无法使用。

范例：XAuth 认证 （本地用户）

在本例中，将在本地数据库上定义名为 x1、密码为 aGgb80L0ws 的 XAuth 用户。

然后，在 IKE 网关配置中对 IP 220.2.2.1 处的对等方引用该用户。将远程网关命名为 “gw1”，为 “阶段 1” 协商指定 Main mode（主模式）和方案 pre-g2-3des-sha，并使用预共享密钥 “netscreen1”。将 VPN 通道命名为 “vpn1”，为 “阶段 2” 协商指定方案 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为外向接口。

WebUI

1. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：

   User Name: x1

   Status: Enable

   XAuth User:（选择）

   Password: iDa84rNk

   Confirm Password: iDa84rNk

VPN

2. VPNs > AutoKey Advanced > Gateway > New：输入以下内容，然后单击 **OK**：

   Gateway Name: gw1

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address:（选择）

   IP Address: 220.2.2.1

   Preshared Key: netscreen1

   Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 Return，返回基本“网关”配置页：

Security Level: Custom: （选择）

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

Enable XAUTH: （选择）

Local Authentication: （选择）

User: （选择）

Name: x1

3. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：

VPN Name: vpn1

Security Level: Compatible

Remote Gateway Tunnel: gw1

CLI

XAuth 用户

1. set user x1 password aGgb80L0ws
2. unset user x1 type auth[15]

VPN

3. set ike gate gw1 ip 220.2.2.1 main outgoing-interface ethernet3 preshare netscreen1 proposal pre-g2-3des-sha
4. set ike gateway gw1 xauth server Local user x1

15. CLI 命令 **set user** *name_str* **password** *pswd_str* 将创建一个用户类型为 auth 和 xauth 的用户。要创建仅为 xauth 类型的用户，必须随后输入命令 **unset user** *name_str* **type auth**。

5. set vpn vpn1 gateway gw1 sec-level compatible
6. save

范例：XAuth 认证 （本地用户组）

本例中，将在本地数据库上创建一个名为 xa-grp1 的用户组，并添加上例第 310 页上的 “范例：XAuth 认证 （本地用户）”中创建的 XAuth 用户 “x1”。将该用户添加到组中时，它自动成为 XAuth 用户组。

然后，在 IKE 网关配置中对 IP 220.2.2.2 处的对等方引用该组。将远程网关命名为 “gw2”，为 “阶段 1”协商指定 Main mode （主模式）和方案 pre-g2-3des-sha，并使用预共享密钥 “netscreen2”。将 VPN 通道命名为 “vpn2”，为 “阶段 2”协商指定方案 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为外向接口。

WebUI

XAuth 用户组

1. Lists > User Groups > Local > New：在 Group Name 字段中键入 **xa-grp1**，执行以下操作，然后单击 **OK**：

   选择 **x1**，使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

VPN

2. VPNs > AutoKey Advanced > Gateway > New：输入以下内容，然后单击 **OK**：

   Gateway Name: gw2

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address:（选择）

   IP Address: 220.2.2.2

   Preshared Key: netscreen2

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本“网关”配置页：

Phase 1 Proposal: pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

Enable XAUTH: （选择）

Local Authentication: （选择）

User Group: （选择）

Name: xa-grp1

3. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：

VPN Name: vpn2

Security Level: Compatible

Remote Gateway Tunnel: gw2

CLI

XAuth 用户组

1. set user-group xa-grp1 location local
2. set user-group xa-grp1 user x1

VPN

3. set ike gate gw2 ip 220.2.2.2 main outgoing-interface ethernet3 preshare netscreen2 proposal pre-g2-3des-sha
4. set ike gateway gw2 xauth server Local user-group xa-grp1
5. set vpn vpn2 gateway gw2 sec-level compatible
6. save

范例：XAuth 认证 （外部用户）

在本例中，将引用先前加载到外部 SecurID auth 服务器上的 XAuth 用户，用户名为“xa-1”，密码为 iNWw10bd01。本例使用的 SecurID auth 服务器配置与第 267 页上的 “范例：为 SecurID 定义 Auth 服务器对象”中定义的大致相同，但此处将帐户类型定义为 XAuth。

在远程 IKE 网关配置中对 IP 220.2.2.3 处的对等方引用 XAuth 用户 xa-1。将远程网关命名为“gw3”，为“阶段 1”协商指定 Main mode （主模式）和方案 pre-g2-3des-sha，并使用预共享密钥 “netscreen3”。将 VPN 通道命名为“vpn3”，为 “阶段 2”协商指定方案 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为外向接口。

WebUI

外部 SecurID Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: securid1

   IP/Domain Name: 10.20.2.100

   Backup1: 10.20.2.110

   Timeout: 60

   Account Type: XAuth

   SecurID Server:（选择）

   Client Retries: 3

   Client Timeout: 10 seconds

   Authentication Port: 15000

   Encryption Type: DES

   User Duress: No

XAuth 用户

2. 在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户“xa-1”。

VPN

3. VPNs > AutoKey Advanced > Gateway > New：输入以下内容，然后单击 **OK**：

   Gateway Name: gw3

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address:（选择）

   IP Address: 220.2.2.3

   Preshared Key: netscreen3

   Outgoing Interface: ethernet3

   > Advanced: 输入以下高级设置，然后单击 **Return**，返回基本“网关”配置页：

   Phase 1 Proposal: pre-g2-3des-sha

   Mode (Initiator): Main (ID Protection)

   Enable XAUTH:（选择）

   External Authentication:（选择）, securid1

   User:（选择）

   Name: xa-1

4. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：

   VPN Name: vpn3

   Security Level: Compatible

   Remote Gateway Tunnel: gw3

CLI

外部 SecurID Auth 服务器

1. set auth-server securid1 type securid
2. set auth-server securid1 server-name 10.20.2.100
3. set auth-server securid1 backup1 10.20.2.110
4. set auth-server securid1 timeout 60
5. set auth-server securid1 account-type xauth
6. set auth-server securid1 securid retries 3
7. set auth-server securid1 securid timeout 10
8. set auth-server securid1 securid auth-port 15000
9. set auth-server securid1 securid encr 1
10. set auth-server securid1 securid duress 0

XAuth 用户

11. 在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户“xa-1”。

VPN

12. set ike gate gw3 ip 220.2.2.3 main outgoing-interface ethernet3 preshare netscreen3 proposal pre-g2-3des-sha
13. set ike gateway gw3 xauth server securid1 user xa-1
14. set vpn vpn3 gateway gw3 sec-level compatible
15. save

范例：XAuth 认证 （外部用户组）

在本例中，将配置名为 “radius1”[16] 的外部 RADIUS auth 服务器，定义名为 “xa-grp2” 的外部 auth 用户组。在下列两个位置定义外部 XAuth 用户组 xa-grp2：

1. 外部 RADIUS auth 服务器“radius1”
2. NetScreen 设备

只在 RADIUS 服务器上将 XAuth 用户装入 XAuth 用户组 “xa-grp2” 中，而将 NetScreen 设备上的组保留为空白。该组中的成员为远程站点处的分销商，需要在企业 LAN 中访问 FTP 服务器。在 Untrust 区段通讯簿中，为具有 IP 地址 192.168.1.0/24、名为 “reseller1” 的远程站点添加一个条目。也可在 Trust 区段通讯簿中，为 IP 地址 10.100.2.11/32 的 FTP 服务器 “rsl-srv1” 输入一个地址。

将 VPN 通道配置为 211.1.1.1，以便对用户组 xa-grp2 中的 XAuth 用户进行认证。将远程网关命名为 “gw4” ，为 “阶段 1” 协商指定 Main mode （主模式）和方案 pre-g2-3des-sha，并使用预共享密钥 “netscreen4”。将 VPN 通道命名为 “vpn4”，为 “阶段 2” 协商指定方案 g2-esp-3des-sha。选择 Untrust 区段接口 ethernet3 作为外向接口。

最后，创建一个策略，允许 FTP 信息流从 Untrust 区段中的 reseller1 通过 vpn4 流向 Trust 区段中的 rsl-svr1。

RADIUS 服务器

1. 将 NetScreen 词典文件加载到 RADIUS 服务器上。

   注意：*有关 NetScreen 词典文件的信息，请参阅第 259 页上的 “NetScreen 词典文件”。有关将词典文件加载到 RADIUS 服务器的说明，请参阅 RADIUS 服务器文档。*

2. 在外部 auth 服务器“radius1”上输入 auth 用户组“xa-grp2”，然后在其中装入 XAuth 用户帐户。

16. RADIUS auth 服务器的配置与第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”中大致相同，但本例中仅指定 “xauth” 作为用户帐户类型。

WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：
   Name: radius1
   IP/Domain Name: 10.20.1.100
   Backup1: 10.20.1.110
   Backup2: 10.20.1.120
   Timeout: 30
   Account Type: XAuth
   RADIUS:（选择）
   RADIUS Port: 4500
   Shared Secret: A56htYY97kl

外部用户组

2. Objects > User Groups > External > New：输入以下内容，然后单击 **OK**：
   Group Name: xa-grp2
   Group Type: XAuth

地址

3. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: reseller1
   IP/Netmask:（选择）, 192.168.1.0/24
   Zone: Untrust

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

   Address Name: rsl-svr1

   IP/Netmask:（选择）, 10.100.2.11/32

   Zone: Trust

XAuth 用户

5. 在外部 SecurID auth 服务器 securid1 上定义密码为 iNWw10bd01 的 auth 用户“xa-1”。

VPN

6. VPNs > AutoKey Advanced > Gateway > New：输入以下内容，然后单击 **OK**：

   Gateway Name: gw4

   Security Level: Custom

   Remote Gateway Type:

   Static IP Address:（选择）

   IP Address: 211.1.1.1

   Preshared Key: netscreen4

   Outgoing Interface: ethernet3

   > Advanced: 输入以下高级设置，然后单击 **Return**，返回基本“网关”配置页：

   Phase 1 Proposal: pre-g2-3des-sha

   Mode (Initiator): Main (ID Protection)

   Enable XAUTH:（选择）

   External Authentication:（选择）, securid1

   User Group:（选择）

   Name: xa-grp2

7. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：
   VPN Name: vpn4
   Security Level: Compatible
   Remote Gateway Tunnel: gw4

策略

8. Policies > (From: Untrust, To: Trust) New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, reseller1
   Destination Address:
   Address Book:（选择）, rsl-svr1
   Service: FTP-Get
   Action: Tunnel
   Tunnel VPN: vpn4
   Modify matching outgoing VPN policy:（清除）
   Position at Top:（选择）

CLI

Auth 服务器

1. set auth-server radius1 type radius
2. set auth-server radius1 account-type xauth
3. set auth-server radius1 server-name 10.20.1.100
4. set auth-server radius1 backup1 10.20.1.110
5. set auth-server radius1 backup2 10.20.1.120
6. set auth-server radius1 radius-port 4500
7. set auth-server radius1 timeout 30
8. set auth-server radius1 secret A56htYY97kl

外部用户组

9. set user-group xa-grp2 location external
10. set user-group xa-grp2 type xauth

地址

11. set address untrust reseller1 192.168.1.0/24
12. set address trust rsl-svr1 10.100.2.11/32

VPN

13. set ike gate gw4 ip 211.1.1.1 main outgoing-interface ethernet3 preshare netscreen4 proposal pre-g2-3des-sha
14. set ike gateway gw4 xauth server radius1 user-group xa-grp2
15. set vpn vpn4 gateway gw4 sec-level compatible

策略

16. set policy top from untrust to trust reseller1 rsl-svr1 ftp-get tunnel vpn vpn4
17. save

范例：XAuth 认证和地址分配 （本地用户组）

在本例中，为本地数据库上存储的 IKE/XAuth 用户组建立认证和 IP、 DNS 服务器及 WINS 服务器 IP 地址分配[17]。IKE/XAuth 用户以拨号 VPN 连接方式尝试连接 NetScreen 设备时，NetScreen 设备会在“阶段 1”协商期间使用 IKE ID 和 RSA 证书对用户 （即客户端设备）进行认证。然后， NetScreen 设备使用用户名和密码对 XAuth 用户 （即使用设备的个体）进行认证，并在 “阶段 1”和 “阶段 2”协商之间分配 IP、 DNS 服务器和 WINS 服务器 IP 地址。

创建本地用户组 ixa-grp1。然后定义两个分别名为 “ixa-u1”（密码：ccF1m84s）和 “ixa-u2”（密码：C113g1tw）的 IKE/XAuth 用户，将它们添加到组中，从而将组类型定义为 IKE/XAuth。（本例中将不向组中另外添加其它 IKE/XAuth 用户。）

创建名为 xa-pool1 的 DIP 池，地址范围从 10.2.2.1 到 10.2.2.100。NetScreen 设备为 XAuth 用户分配 IP 地址时，即从此地址池中提取地址。

注意：*DIP 池与 XAuth 用户发送信息流的目标区段必须具有不同的地址空间，以避免出现路由选择问题和地址分配重复。*

17. 也可使用外部 RADIUS auth 服务器对 XAuth 用户进行认证和地址分配。但外部 SecurID 或 LDAP auth 服务器只能用于 XAuth 认证（不能进行地址分配）。对于 IKE 用户认证，只能使用本地数据库。

配置以下 XAuth 缺省设置：

- 将 XAUTH 地址超时设置为 480 分钟。
- 选择本地数据库作为缺省 auth 服务器。
- 启用 CHAP （质询握手认证协议）， NetScreen 设备根据此协议向远程客户端发送一个质询 （加密密钥），该客户端用户使用此密钥对其登录名和密码进行加密。
- 选择 xa-pool1 作为缺省 DIP 池。
- 将主、辅 DNS 服务器 IP 地址分别定义为 10.1.1.150 和 10.1.1.151。
- 将主、辅 WINS 服务器 IP 地址分别定义为 10.1.1.160 和 10.1.1.161。

引用用户组 ixa-grp1 并使用缺省 XAuth auth 服务器设置，配置名为 “ixa-gw1” 的 IKE 网关。然后，配置名为 “ixa-tun1” 的 VPN 通道和允许信息流通过 VPN 通道 ixa-tun1 从 ixa-grp1 流向 Trust 区段的策略。

WebUI

IKE/XAuth 用户和用户组

1. Objects > User Groups > Local > New：在 Group Name 字段中键入 **ixa-grp1**，然后单击 **OK**。
2. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：

User Name: ixa-u1

User Group: ixa-grp1

Status: Enable

IKE User:（选择）

Simple Identity:（选择）

IKE ID Type: Auto

IKE Identity: u1@ns.com

XAuth User:（选择）

Password: ccF1m84s

Confirm Password: ccF1m84s

3. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：

User Name: ixa-u2
User Group: ixa-grp1
Status: Enable
IKE User:（选择）
Simple Identity:（选择）
IKE ID Type: Auto
IKE Identity: u2@ns.com
XAuth User:（选择）
Password: C113g1tw
Confirm Password: C113g1tw

IP 池

4. Objects > IP Pools > New：输入以下内容，然后单击 **OK**：

IP Pool Name: xa-pool1
Start IP: 10.2.2.1
End IP: 10.2.2.100

缺省 XAuth Auth 服务器

5. VPNs > AutoKey Advanced > XAuth Settings：输入以下内容，然后单击 **Apply**：

Reserve Private IP for XAuth User: 480
Default Authentication Server: Local
Query Client Settings on Default Server:（清除）
CHAP:（选择）
IP Pool Name: xa-pool1
DNS Primary Server IP: 10.1.1.150

DNS Secondary Server IP: 10.1.1.151

WINS Primary Server IP: 10.1.1.160

WINS Secondary Server IP : 10.1.1.161

VPN

6. VPNs > AutoKey Advanced > Gateway > New：输入以下内容，然后单击 **OK**：

   Gateway Name: ixa-gw1

   Security Level: Custom

   Remote Gateway Type:

   Dialup User Group:（选择）

   Group: ixa-grp1

   > Advanced: 输入以下高级设置，然后单击 **Return**，返回基本“网关”配置页：

   Phase 1 Proposal: rsa-g2-3des-sha

   Mode (Initiator): Aggressive

   Outgoing Interface: ethernet3

   Enable XAUTH:（选择）

   Use Default:（选择）

   User Group:（选择）

   Name: ixa-grp1

7. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：

   VPN Name: ixa-vpn1

   Security Level: Compatible

   Remote Gateway Tunnel: ixa-gw1

策略

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

Source Address:

Address Book:（选择）, Dial-Up VPN

Destination Address:

Address Book:（选择）, Any

Service: ANY

Action: Tunnel

Tunnel VPN: ixa-vpn1

Modify matching outgoing VPN policy:（清除）

Position at Top:（选择）

CLI

IKE/XAuth 用户和用户组

1. set user-group ixa-grp1 location local
2. set user ixa-u1 type ike xauth
3. set user ixa-u1 ike-id u-fqdn u1@ns.com
4. set user ixa-u1 password ccF1m84s
5. unset user ixa-u1 type auth
6. set user ixa-u2 type ike xauth
7. set user ixa-u2 ike-id u-fqdn u2@ns.com
8. set user ixa-u2 password C113g1tw
9. unset user ixa-u2 type auth

IP 池

10. set ippool xa-pool1 10.2.2.1 10.2.2.100

缺省 XAuth Auth 服务器

11. set xauth lifetime 480
12. set xauth default auth server Local chap
13. set xauth default ippool xa-pool1
14. set xauth default dns1 10.1.1.150
15. set xauth default dns2 10.1.1.151
16. set xauth default wins1 10.1.1.160
17. set xauth default wins210.1.1.161

VPN

18. set ike gateway ixa-gw1 dialup ixa-grp1 aggressive outgoing-interface ethernet3 proposal rsa-g2-3des-sha
19. set ike gateway ixa-gw1 xauth server Local user-group ixa-grp1
20. set vpn ixa-vpn1 gateway ixa-gw1 sec-level compatible

策略

21. set policy top from untrust to trust “Dial-Up VPN” any any tunnel vpn ixa-vpn1
22. save

手动密钥用户和用户组

“手动密钥”用户是具有动态分配 IP 地址的远程 VPN 用户。与此类用户相关联的 VPN 通道采用 “手动密钥”方法进行加密和 / 或 IPSec 认证。与必须在“自动密钥” IKE 网关配置中引用的 IKE 用户不同，“手动密钥”用户的配置包括设置“手动密钥”VPN 通道所必需的所有参数。“手动密钥”用户与 IKE 用户的相似之处在于，此两种类型的用户都只能存储在本地数据库上。

定义“手动密钥”用户或将多个用户组合在一起后，即可在策略中引用该用户或用户组。将“手动密钥”用户集合成组的好处在于：只需创建一个引用该组的策略即可，而不必为每个 “手动密钥”用户都创建一个策略。

注意：*有关 “手动密钥” VPN 通道的详细信息，请参阅第 4 卷 “VPN”。有关范例，请参阅第* ***4*** *-157 页上的“范例：基于策略的拨号到 LAN 的 VPN，手动密钥”。*

范例：手动密钥用户

在本例中，将定义名为 mk-u1 的 “手动密钥” 用户，它具有以下元素：

- 安全参数索引 (SPI)：1000 （本地）， 1001 （远程）
- 外向接口：ethernet3 （Untrust 区段接口）
- 使用 DES-CBC 作为加密算法 （密码：W1goAciM32）、 MD5 作为认证算法 （密码：TmoR104iVs）的 “封装安全性负荷” (ESP)

然后，在允许访问 Trust 区段 FTP 服务器 （名称：ftp-svr1 ； IP 地址：10.1.1.55/32）的内向策略中引用 mk-u1。

WebUI

手动密钥用户

1. Objects > Users > Manual Key > New：输入以下内容，然后单击 **OK**：

   User Name: mk-u1
   User Group: None
   Security Index: 1000 (Local); 1001 (Remote)
   Outgoing Interface: ethernet3
   ESP:（选择）
   ESP-Encryption-Algorithm: 3DES-CBC
   Generate Key by Password: W1goAciM32
   Authentication Algorithm: MD5
   Generate Key by Password: TmoR104iVs

地址

2. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: ftp-svr1
   IP Address/Domain Name:
   IP/Netmask:（选择）, 10.1.1.55/32
   Zone: Trust

策略

3. Policies > (From: Untrust; To: Trust) > New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book:（选择）, Dial-Up VPN
   Destination Address:
   Address Book:（选择）, ftp-svr1
   Service: FTP-Get
   Action: Tunnel
   Tunnel VPN: Dialup User - mk-u1
   Modify matching outgoing VPN policy:（清除）
   Position at Top:（选择）

CLI

手动密钥用户

1. set user mk-u1 dialup 1000 1001 outgoing-interface ethernet3 esp des password W1goAciM32 auth md5 password TmoR104iVs

地址

2. set address trust ftp-svr1 10.1.1.555/32

策略

3. set policy top from untrust to trust “Dial-Up VPN” ftp-svr1 ftp-get tunnel mk-u1
4. save

范例：手动密钥用户组

在本例中，将创建一个名为 “mk-grp1” 的用户组。然后，将名为 mk-u2 的 “手动密钥” 用户添加到该组，从而确定组类型为 “手动密钥”。用户 mk-u2 具有以下元素：

- 安全参数索引 (SPI)：1100 （本地）， 1101 （远程）
- 外向接口：ethernet3 （Untrust 区段接口）
- 使用 DES-CBC 作为加密算法（密码：1L2hCr89）、MD5 作为认证算法（密码：Ukpb8p13）的 “封装安全性负荷” (ESP)

（本例中将不向组中另外添加其它 “手动密钥” 用户。）

然后，在允许访问 Trust 区段 FTP 服务器 （名称：ftp-svr1 ； IP 地址：10.1.1.55/32）的内向策略中引用 mk-grp1。

WebUI

手动密钥组和用户

1. Objects > User Groups > Manual Key > New：在 Group Name 字段中键入 **mk-grp1**，然后单击 **OK**。
2. Objects > Users > Manual Key > New：输入以下内容，然后单击 **OK**：

   User Name: mk-u2
   User Group: None
   Security Index: 1100 (Local); 1101 (Remote)
   Outgoing Interface: ethernet3
   ESP:（选择）
   ESP-Encryption-Algorithm: 3DES-CBC
   Generate Key by Password: 1L2hCr89
   Authentication Algorithm: MD5
   Generate Key by Password: Ukpb8p13

地址

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

   Address Name: ftp-svr1

   IP Address/Domain Name:

   IP/Netmask:（选择）, 10.1.1.55/32

   Zone: Trust

策略

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

   Source Address:

   Address Book:（选择）, Dial-Up VPN

   Destination Address:

   Address Book:（选择）, ftp-svr1

   Service: FTP-Get

   Action: Tunnel

   Tunnel VPN: Dialup User Group - mk-grp1

   Modify matching outgoing VPN policy:（清除）

   Position at Top:（选择）

CLI

手动密钥用户

1. set user mk-u2 dialup 1100 1101 outgoing-interface ethernet3 esp des password 1L2hCr89 auth md5 password Ukpb8p13
2. set dialup-group mk-grp1 + mk-u2

地址

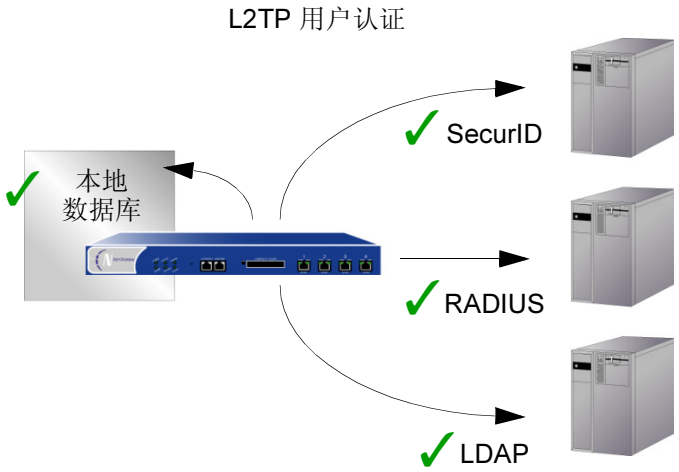
3. set address trust ftp-svr1 10.1.1.555/32

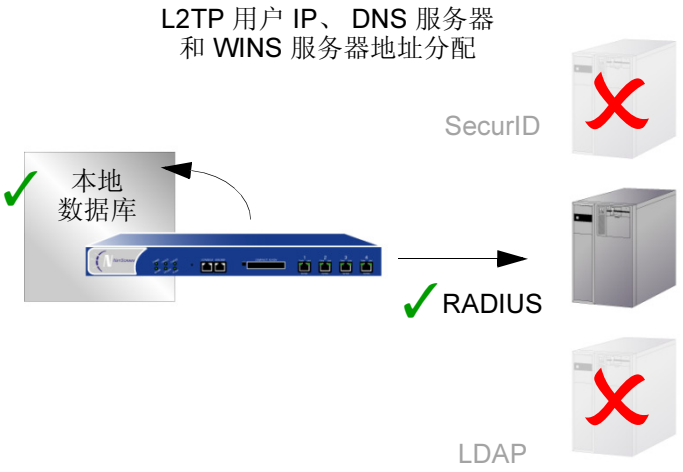
策略

4. set policy top from untrust to trust “Dial-Up VPN” ftp-svr1 ftp-get tunnel mk-grp1
5. save

L2TP 用户和用户组

“第 2 层通道协议” (L2TP) 提供一种认证远程用户和分配 IP、DNS 服务器与 WINS 服务器地址的方法。可对 NetScreen 设备进行配置，以便使用本地数据库或外部 auth 服务器认证 L2TP 用户。要对 IP、DNS 服务器及 WINS 服务器地址进行分配，可相应配置 NetScreen 设备，以使用本地数据库或 RADIUS 服务器（加载有 NetScreen 词典文件 — 请参阅第 259 页上的 “NetScreen 词典文件”）。





甚至可使用 auth 服务器的组合，不同服务器分别对应 L2TP 两个方面之一。例如，可使用 SecurID 服务器对 L2TP 用户进行认证，但从本地数据库进行地址分配。下例说明如何应用两个 auth 服务器分别处理 L2TP 的两方面需求。有关其它范例以及 L2TP 的详细解释，请参阅第 **4**-233 页上的“L2TP（Layer 2 Tunneling Protocol，第 2 层通道协议）”。

范例：本地和外部 L2TP Auth 服务器

在本例中，将设置外部 SecurID auth 服务器对 L2TP 用户进行认证，并使用本地数据库为 L2TP 用户分配 IP、 DNS 服务器和 WINS 服务器地址。

外部 SecurID auth 服务器为 securid1。 Auth 服务器的配置与第 267 页上的 “范例：为 SecurID 定义 Auth 服务器对象”中基本相同，只是此处帐户类型为 L2TP。 SecurID auth 服务器参数如下：

- Name: securid1
- IP Address: 10.20.2.100
- Backup1 IP Address: 10.20.2.110
- Port: 15000
- Encryption: DES
- Client Retries: 3
- Client Timeout: 10 seconds
- Idle Timeout: 60 minutes
- Account Type: L2TP

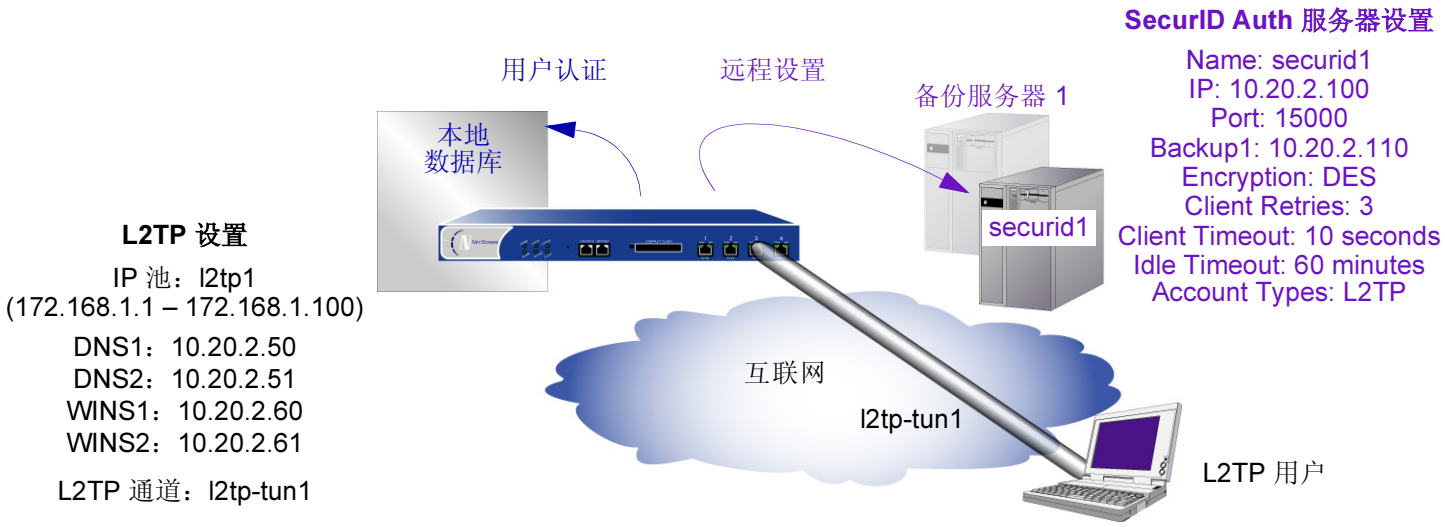
L2TP 缺省设置如下：

- IP Pool: l2tp1 (172.168.1.1 - 172.168.1.100)
- DNS Primary Server IP: 10.20.2.50
- DNS Secondary Server IP: 10.20.2.51
- PPP Authentication: CHAP
- WINS Primary Server IP: 10.20.2.60
- WINS Primary Server IP: 10.20.2.61

以上述设置对 NetScreen 设备进行配置后，创建名为 “l2tp-tun1” 的 L2TP 通道，它引用 securid1 进行认证，并使用缺省设置进行地址分配。

此外，还必须如上所示设置 SecurID 服务器，并在其中装入 L2TP 用户。

注意： *仅 L2TP 配置是不安全的。为了对 L2TP 通道进行保护，建议将其与 IPSec 通道 （必须处于 Transport 模式）结合使用，如第* ***4*** *-250 页上的 “范例：配置 IPSec 上的 L2TP” 中所示。*



WebUI

Auth 服务器

1. Configuration > Auth > Auth Servers > New：输入以下内容，然后单击 **OK**：

   Name: securid1
   IP/Domain Name: 10.20.2.100
   Backup1: 10.20.2.110
   Timeout: 60
   Account Type: L2TP
   SecurID Server:（选择）
   Client Retries: 3
   Client Timeout: 10 seconds
   Authentication Port: 15000
   Encryption Type: DES
   User Duress: No

IP 池

2. Objects > IP Pools > New：输入以下内容，然后单击 **OK**：

   IP Pool Name: l2tp1

   Start IP: 172.168.1.1

   End IP: 172.168.1.100

L2TP 缺省设置

3. VPNs > L2TP > Default Settings：输入以下内容，然后单击 **Apply**：

   IP Pool Name: l2tp1

   PPP Authentication: CHAP

   DNS Primary Server IP: 10.20.2.50

   DNS Secondary Server IP: 10.20.2.51

   WINS Primary Server IP: 10.20.2.60

   WINS Secondary Server IP: 10.20.2.61

L2TP 通道

4. VPNs > L2TP > Tunnel > New：输入以下内容，然后单击 **OK**：

   Name: l2tp-tun1

   Dialup User: all-l2tp-users

   Authentication Server: securid1

   Query Remote Settings:（清除）

CLI

Auth 服务器

1. set auth-server securid1 type securid
2. set auth-server securid1 server-name 10.20.2.100
3. set auth-server securid1 backup1 10.20.2.110
4. set auth-server securid1 timeout 60
5. set auth-server securid1 account-type l2tp
6. set auth-server securid1 securid retries 3
7. set auth-server securid1 securid timeout 10
8. set auth-server securid1 securid auth-port 15000
9. set auth-server securid1 securid encr 1
10. set auth-server securid1 securid duress 0

IP 池

11. set ippool l2tp1 172.168.1.1 172.168.1.100

L2TP 缺省设置

12. set l2tp default auth server securid1
13. set l2tp default ippool l2tp1
14. set l2tp def ppp-auth chap
15. set l2tp dns1 10.20.2.50
16. set l2tp dns1 10.20.2.51
17. set l2tp wins1 10.20.2.60
18. set l2tp wins2 10.20.2.61

L2TP 通道

19. set l2tp l2tp-tun1
20. set l2tp l2tp-tun1 auth server securid1
21. save

Admin 用户

Admin 用户是 NetScreen 设备的管理员。共有五种 admin 用户：

- 根 admin
- 根级读 / 写 admin
- 根级只读 admin
- Vsys admin
- Vsys 只读 admin

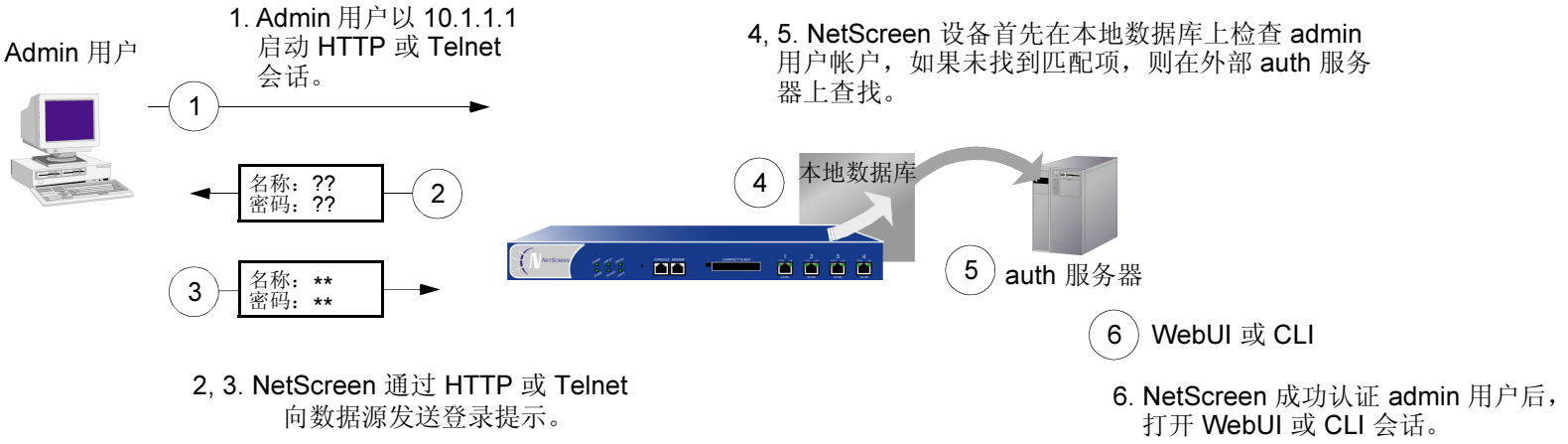
> ***注意：****有关各类型 admin 用户权限的信息，以及创建、修改和删除 admin 用户的范例，请参阅第* ***3*** *-1 页上的 “管理”。*

尽管 NetScreen 设备根用户的配置文件必须存储在本地数据库中，但可将具有读 / 写和只读权限的 vsys 用户和根级 admin 用户存储在本地数据库或外部 auth 服务器中。

如果将 admin 用户帐户存储在外部 RADIUS auth 服务器上，并在 auth 服务器上加载 NetScreen 词典文件（请参阅第 259 页上的 “NetScreen 词典文件”），则可选择查询服务器上定义的 admin 权限。此外，您也可以指定某权限级别，以全局方式应用于该 auth 服务器上存储的所有 admin 用户。可指定读 / 写或只读权限。如果将 admin 用户存储在外部 SecurID 或 LDAP auth 服务器或者未加载 NetScreen 词典文件的 RADIUS 服务器上，则不能在 auth 服务器上定义它们的权限属性。因此，必须在 NetScreen 设备上为它们指定权限级别。

如果在 NetScreen 设备上设置：	且 RADIUS 服务器已加载 NetScreen 词典文件，则：	且 SecurID、 LDAP 或 RADIUS 服务器未加载 NetScreen 词典文件，则：
从 RADIUS 服务器获取权限	指定适当权限	根级或 vsys 级 admin 登录失败
为外部 admin 指定读 / 写权限	指定根级或 vsys 级读 / 写权限	指定根级读 / 写权限 Vsys admin 登录失败
为外部 admin 指定只读权限	指定根级或 vsys 级只读权限	指定根级只读权限 Vsys admin 登录失败

admin 认证过程如下图所示：



多类型用户

可将 auth、 IKE、 L2TP、 XAuth 用户组合在一起，创建下列组合对象并存储在本地数据库上：

- Auth/IKE 用户
- Auth/L2TP 用户
- Auth/IKE/L2TP 用户
- IKE/L2TP 用户
- Auth/XAuth 用户
- Auth/IKE/XAuth 用户
- IKE/XAuth 用户
- L2TP/XAuth 用户
- IKE/L2TP/XAuth 用户
- Auth/IKE/L2TP/XAuth 用户

尽管在本地数据库上定义多类型用户帐户时，可以创建上述所有组合形式，但在创建之前仍须考虑以下事项：

- 将 IKE 用户类型与其它任何用户类型组合后，会限制其扩展的潜在能力。与“手动密钥”用户帐户相同，IKE 用户帐户必须存储在本地数据库上。如果创建 auth/IKE、IKE/L2TP 和 IKE/XAuth 用户帐户，而之后用户数超出本地数据库容量时，您就无法将这些帐户重新置于外部 auth 服务器中。如果将 IKE 用户帐户与其它类型帐户分离，则在必要时，您可以灵活地将非 IKE 用户帐户移动到外部 auth 服务器中。
- L2TP 和 XAuth 提供相同的服务：远程用户认证以及 IP、DNS 服务器与 WINS 服务器地址分配。建议不要对 IPSec 上的 L2TP 通道同时使用 L2TP 和 XAuth。不仅因为这两种协议的作用相同，而且在“阶段 2”IKE 协商完成、 L2TP 协商开始后， L2TP 地址分配会将覆盖 XAuth 地址分配。
- 如果将 auth/L2TP 或 auth/XAuth 组合在一起，在本地数据库上创建多类型用户帐户，则两种类型用户登录时必须使用相同的用户名和密码。

  尽管创建一个多类型用户帐户较之将用户类型分为两个单独帐户而言操作起来更为方便，但后者却可以为您带来更高的安全性。例如，可将 auth 用户帐户存储在外部 auth 服务器上，将 XAuth 用户帐户存储在本地数据库上。然后，可以为每个帐户指定不同的登录用户名和密码，并在 IKE 网关配置中引用 XAuth 用户，而在策略配置中引用 auth 用户。拨号 VPN 用户必须经过两次认证，认证时可以使用两个完全不同的用户名和密码。

组表达式

组表达式是可以在策略中用来使认证要求实现条件化的语句。组表达式可以将用户、用户组或其它组表达式作为认证的可选条件 (“a” OR “b”) 或者作为认证的必需条件 (“a” AND “b”) 组合起来，也可以将某个用户、用户组或另一组表达式排除在外 (NOT “c”)。

注意：*虽然您在 NetScreen 设备上定义组表达式（并存储在本地数据库上），但组表达式中引用的用户和用户组必须存储在外部 RADIUS 服务器上。 RADIUS 服务器允许一个用户属于多个用户组。但本地数据库不允许这样。*

组表达式使用三个运算符 OR、AND 和 NOT。表达式中用 OR、AND 和 NOT 关联起来的对象可以是一个 auth 用户、auth 用户组或先前定义的组表达式。

用户

OR – 如果策略的认证情况指定用户为 “a” OR “b”，则当用户属于这两者之一时，NetScreen 设备会认证他 / 她。

AND – 组表达式中使用 AND 运算符时，要求两个表达式对象中至少有一个是用户组或组表达式。（要求某个用户为用户 “a” AND 用户 “b” 是不符合逻辑的。）如果策略的认证情况要求用户为为 “a” AND 组 “b” 中的成员，则只有当满足这两个条件时，NetScreen 设备才会认证该用户。

NOT – 如果策略的认证情况指定用户为除用户 “c” 外的任何其它用户 (NOT “c”)，则只要用户不是 “c”，NetScreen 设备就会认证他 / 她。

用户组

OR – 如果策略的认证情况指定用户属于组 “a” OR 组 “b”，则当该用户属于其中任一组时，NetScreen 设备认证他 / 她。

AND – 如果策略的认证情况要求用户属于组 “a” AND 组 “b”，则只有当用户同时属于两组时，NetScreen 设备才会认证他 / 她。

NOT – 如果策略的认证情况指定用户属于除组 “c” 外的任意组 (NOT “c”)，则当用户不属于此组时，NetScreen 设备认证他 / 她。

组表达式

OR – 如果策略的认证情况指定用户符合组表达式 “a” OR 组表达式 “b” 的描述，则只有当其中某一组表达式适用于该用户时，NetScreen 设备才会认证他 / 她。

AND – 如果策略的认证情况指定用户应符合组表达式 “a” AND 组表达式 “b” 的描述，则只有当两个表达式都适用于该用户时，NetScreen 设备才会认证他 / 她。

NOT – 如果策略的认证情况指定用户应不符合组表达式 “c” 的描述 (NOT “c”)，则只有当该用户不符合此组表达式时，NetScreen 设备才会认证他 / 她。

范例：组表达式 (AND)

在本例中，将创建一个表述为 “sales AND marketing” 的组表达式 “s+m” 。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建了 auth 用户组 “sales” 和 “marketing” ，并在其中留置了用户。（有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”。）然后，在内部区段策略[18] 中使用该组表达式，策略中的认证部分要求用户必须是这两个用户组的成员，才能访问名 “project1” 的服务器 (10.1.1.70) 上的机密内容。

WebUI

1. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: project1
   IP Address/Domain Name
   IP/Netmask: 10.1.1.70/32
   Zone: Trust
2. Objects > Group Expressions > New：输入以下内容，然后单击 **OK**：
   Group Expression: s+m
   AND:（选择）, sales AND marketing

18. 要使内部区段策略正常工作，源地址和目标地址必须位于不同的子网中，这些子网通过绑定到同一区段的接口连接到 NetScreen 设备。除 NetScreen 设备外，其它任何路由设备都不能在两个地址间转发信息流。有关内部区段策略的详细信息，请参阅第 215 页上的 “策略”。

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

   Source Address

   Address Book: Any

   Destination Address

   Address Book: project1

   Service: ANY

   Action: Permit

   Position at Top:（选择）

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

   Authentication:（选择）

   Auth Server:（选择）, radius1

   Group Expression:（选择）, External Group Expression - s+m

CLI

1. set address trust project1 10.1.1.70/32
2. set group-expression s+m sales and marketing
3. set policy top from trust to trust any project1 any permit auth server radius1 group-expression s+m
4. save

范例：组表达式 (OR)

在本例中，将创建一个表述为 “amy OR basil” 的组表达式 “a/b” 。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建了 auth 用户帐户 “amy” 和 “basil”。（有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”。）然后在从 Trust 区段到 DMZ 的策略中使用该组表达式。策略的认证部分要求用户必须为 amy 或 basil，才能访问 210.1.1.70 处名为 “web1” 的 Web 服务器。

WebUI

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

   Address Name: web1

   IP Address/Domain Name

   IP/Netmask: 210.1.1.70/32

   Zone: DMZ

2. Objects > Group Expressions > New：输入以下内容，然后单击 **OK**：

   Group Expression: a/b

   OR:（选择）, amy OR basil

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

   Source Address

   Address Book: Any

   Destination Address

   Address Book: web1

   Service: ANY

   Action: Permit

   Position at Top:（选择）

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

   Authentication:（选择）

   Auth Server:（选择）, radius1

   Group Expression:（选择）, External Group Expression - a/b

CLI

1. set address trust project1 210.1.1.70/32
2. set group-expression a/b amy or basil
3. set policy top from trust to dmz any web1 any permit auth server radius1 group-expression a/b
4. save

范例：组表达式 (NOT)

在本例中，将创建一个表述为 “NOT temp” 的组表达式 “-temp” 。您先前已在名为 “radius1” 的外部 RADIUS auth 服务器上创建本地 auth 用户组 “temp”。（有关如何配置外部 RADIUS auth 服务器的范例，请参阅第 264 页上的 “范例：为 RADIUS 定义 Auth 服务器对象”。）然后，在从 Trust 区段到 Untrust 区段的策略中使用该组表达式，该策略允许除临时合同工以外的所有专职雇员访问互联网。策略的认证部分要求使 Trust 区段中除 “temp” 中的用户而外的所有人员通过认证，拒绝 “temp” 中的用户访问 Untrust 区段。

WebUI

1. Objects > Group Expressions > New：输入以下内容，然后单击 **OK**：

   Group Expression: -temp

   OR:（选择）, NOT temp

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

   Source Address:

   Address Book: Any

   Destination Address:

   Address Book: Any

   Service: HTTP

   Action: Permit

   Position at Top:（选择）

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

   Authentication: （选择）

   Auth Server: （选择）, Local

   Group Expression:（选择）, External Group Expression - -temp

CLI

1. set group-expression -temp not temp
2. set policy top from trust to untrust any any any permit auth server radius1 group-expression -temp
3. save

标题自定义

标题是指在以下类型登录期间在屏幕的下列位置出现的消息：

- Admin 用户连接登录到 NetScreen 设备时，在 Telnet 或控制台显示器的顶部显示
- Auth 用户成功登录到 WebAuth 地址后，在 Web 浏览器屏幕的顶部显示
- 对于 auth 用户，在 Telnet、 FTP 或 HTTP 的登录提示、成功消息和失败消息上显示

除控制台登录标题外，所有标题都具有缺省消息。您可以自定义出现在标题上的消息，使其更适合使用 NetScreen 设备的网络环境。

范例：自定义 WebAuth 成功消息

在本例中，将更改通过 WebAuth 成功登录后出现在 Web 浏览器中的消息，用以指示 auth 用户已成功通过认证。新消息为 “Authentication approved”。

WebUI

Configuration > Banners > WebAuth：在 Success Banner 字段中，键入 **Authentication approved**，然后单击 **Apply**。

CLI

1. set webauth banner success “Authentication approved”
2. save

9

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) 的前提下具成本效益的载流容量。通过创建策略并将适当的速率控制应用到流经 NetScreen 设备的每一种信息流类别，您可使用 NetScreen 设备对信息流进行整形。

注意：*只有那些目的区段有单个接口绑定到其中的策略才可以应用信息流整形。*

在策略级管理带宽

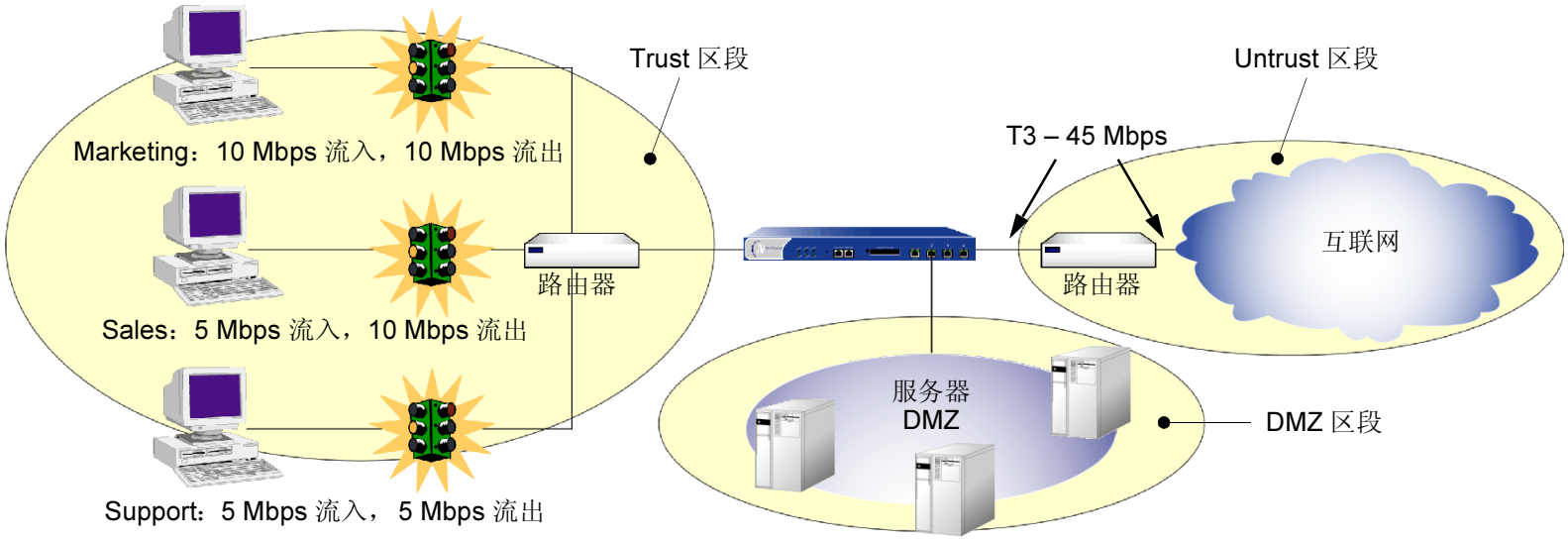
要将信息流分类，可创建一个指定每类信息流的保障带宽数量、最大带宽及优先级等内容的策略。每一接口的物理带宽都分配给所有策略的保障带宽参数。如果有带宽剩余，可由其它信息流共享。换句话说，每个策略可得到其保障带宽并基于其优先级共享剩余的带宽 （直至达到其最大带宽规格的限制）。

信息流整形功能适用于所有策略的信息流。如果您关闭某一策略的信息流整形但其它策略的信息流整形仍然开启，那么系统将对此策略应用缺省信息流整形策略策略，即保障带宽为 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 228 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. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：

   信息流带宽：45000[2]

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

   信息流带宽：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。

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

   Name: Marketing Traffic Shaping Policy

   Source Address:

   Address Book: （选择） , Marketing

   Destination Address:

   Address Book: （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

4. 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: （选择） , Sales

   Destination Address:

   Address Book: （选择） , Any

   Service: Any

   Action: Permit

3. 您也可在参考 VPN 通道的策略中启用信息流整形。

> 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

5. 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: （选择）, Support

Destination Address:

Address Book: （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

6. 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: （选择）, Any

Destination Address:

Address Book: （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

7. 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: （选择）, Any

Destination Address:

Address Book: （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

8. 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: （选择）, Any

   Destination Address:

   Address Book: （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. set interface ethernet1 bandwidth 45000[4]
2. set interface ethernet3 bandwidth 45000
3. set policy name “Marketing Traffic Shaping Policy” from trust to untrust marketing any any permit traffic gbw 10000 priority 0 mbw 15000
4. set policy name “Sales Traffic Shaping Policy” from trust to untrust sales any any permit traffic gbw 10000 priority 0 mbw 10000
5. set policy name “Support Traffic Shaping Policy” from trust to untrust support any any permit traffic gbw 5000 priority 0 mbw 10000
6. set policy name “Allow Incoming Access to Marketing” from untrust to trust marketing any any permit traffic gbw 10000 priority 0 mbw 10000
7. set policy name “Allow Incoming Access to Sales” from untrust to trust sales any any permit traffic gbw 5000 priority 0 mbw 10000
8. set policy name “Allow Incoming Access to Support” from untrust to trust support any any permit traffic gbw 5000 priority 0 mbw 5000
9. save

或者，要在接口级启用信息流整形，请执行以下操作：

1. set interface ethernet1 bandwidth 45000
2. set interface ethernet3 bandwidth 45000
3. set traffic-shaping mode auto
4. 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 设备支持的信息流整形功能，您可对未分配给保障带宽的或已保证但未使用的带宽执行优先级排列。优先级排列功能允许所有用户和应用程序在需要时都能够访问可用带宽，同时又确保重要的信息流可以通过，必要时能够以牺牲次重要信息流的带宽为代价。通过排列功能， NetScreen 能够以八种不同的优先级排列对信息流进行缓冲。这八种排列为：

- High priority （高优先级）
- 2nd priority （第 2 优先级）
- 3rd priority （第 3 优先级）
- 4th priority （第 4 优先级）
- 5th priority （第 5 优先级）
- 6th priority （第 6 优先级）
- 7th priority （第 7 优先级）
- Low priority (default) （低优先级 （缺省））

策略的优先级设置意味着未分配给其它策略的带宽基于高优先级在前和低优先级在后的原则进行了排列。具有相同优先级设置的策略将以轮询方式竞争带宽。NetScreen 设备首先处理具有较高优先级策略的所有信息流，然后再处理具有次优先级设置策略的信息流，依此类推，直至处理完所有的信息流请求。如果信息流请求超过可用带宽，则将丢弃优先级最低的信息流。

小心：*应注意不要分配给接口超过其支持能力的带宽。策略配置过程本身不能避免创建不支持的策略配置。如果竞争策略的保障带宽超过接口上设置的信息流带宽，将有可能丢失数据。*

如果您未分配任何保障带宽，则可使用优先级排列来管理网络的所有信息流。也就是说，必须在发送完全部高优先级信息流之后，才能发送 2nd priority（第 2 优先级）信息流，依此类推。只有在处理完其它所有信息流之后，NetScreen 设备才处理低优先级信息流。

范例：优先级排列

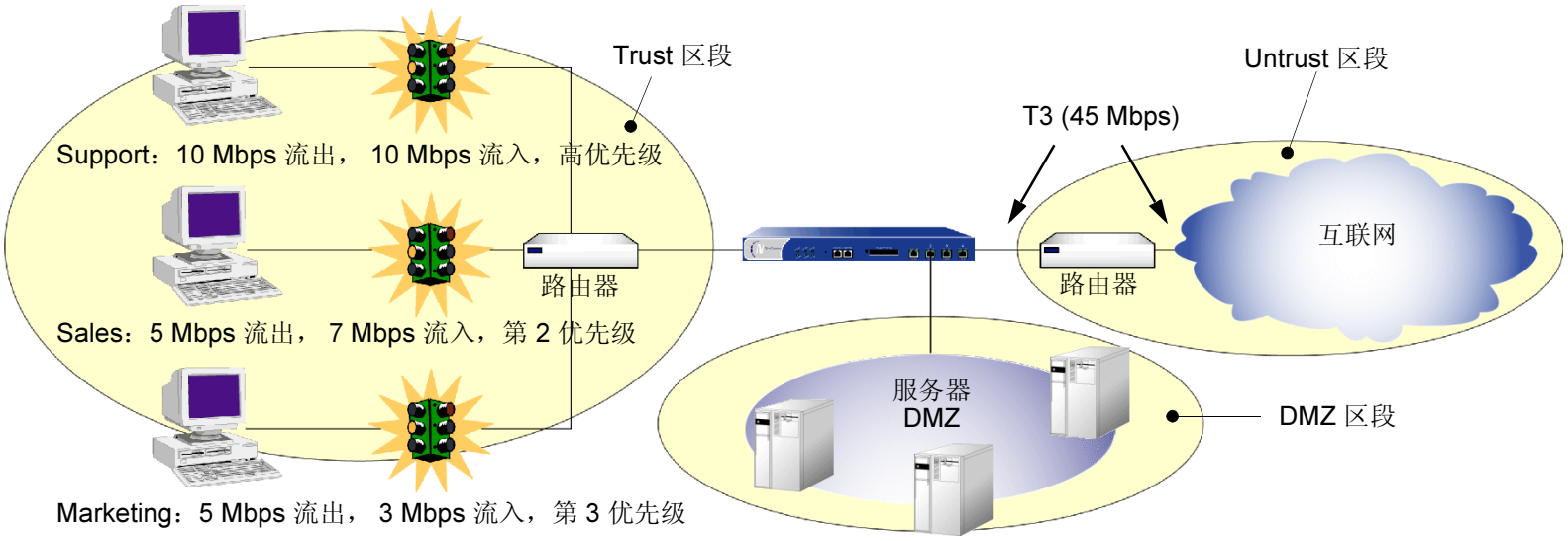
在本例中，您需要为三个部门（Support、 Sales 和 Marketing）配置保障带宽和最大带宽，如下所示：

	出站保证的最大值	入站保证的最大值	组合的保证的最大值	优先级
Support	10*	10	20	高
Sales	5	7	12	2
Marketing	5	3	8	3
总计	20	20	40	

* 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 40 Mbps 的带宽以满足保证的策略要求。余下 5 Mbps 可用带宽，其中的 3 Mbps 将分配给 Sales 以满足其最大带宽分配要求。Marketing 信息流的优先级最低，它将使用 8 Mbps 保障信息流，同时还会得到剩余的最后 2 Mbps 带宽来尽量满足其最大带宽分配要求。

ethernet1 接口被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。



Web UI

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

   信息流带宽：40000

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

   Traffic Bandwidth: 40000

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

   Name: Sup-out

   Source Address:

   Address Book: （选择）, Support

Destination Address:

Address Book: （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: 10000

Maximum Bandwidth: 10000

Traffic Priority: High priority

DiffServ Codepoint Marking[5] : （选择）

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

Name: Sal-out

Source Address:

Address Book: （选择） , Sales

Destination Address:

Address Book: （选择） , Any

Service: Any

Action: Permit

5. 差异服务 (DS) 是在优先级层次结构中的某一位置标记（或“做记号”）信息流的系统。DS 码点标记将 NetScreen 的策略优先级映射到 IP 封包包头 DS 字段中码点的前三位。有关“DS 码点标记”的详细信息，请参阅第 228 页上的 “信息流整形”。

> 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

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: Enable

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

Name: Mar-out

Source Address:

Address Book: （选择）, Marketing

Destination Address:

Address Book: （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: 5000

Traffic Priority: 3rd Priority

DiffServ Codepoint Marking: （选择）

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

   Name: Sup-in

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （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: 10000

   Maximum Bandwidth: 10000

   Traffic Priority: High priority

   DiffServ Codepoint Marking: （选择）

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

   Name: Sal-in

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （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: 7000

Maximum Bandwidth: 1000

Traffic Priority: 2nd priority

DiffServ Codepoint Marking: （选择）

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

Name: Mar-in

Source Address:

Address Book: （选择）, Any

Destination Address:

Address Book: （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: 3000

Maximum Bandwidth: 5000

Traffic Priority: 3rd priority

DiffServ Codepoint Marking: （选择）

CLI

1. set interface ethernet1 bandwidth 40000
2. set interface ethernet3 bandwidth 40000
3. set policy name sup-out from trust to untrust support any any permit traffic gbw 10000 priority 0 mbw 10000 dscp enable
4. set policy name sal-out from trust to untrust sales any any permit traffic gbw 5000 priority 2 mbw 5000 dscp enable
5. set policy name mar-out from trust to untrust marketing any any permit traffic gbw 5000 priority 3 mbw 5000 dscp enable
6. set policy name sup-in from untrust to trust any support any permit traffic gbw 10000 priority 0 mbw 10000 dscp enable
7. set policy name sal-in from untrust to trust any sales any permit traffic gbw 7000 priority 2 mbw 10000 dscp enable
8. set policy name mar-in from untrust to trust any marketing any permit traffic gbw 3000 priority 3 mbw 5000 dscp enable
9. save

10

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.netscreen.com 对应的 IP 地址是 209.125.148.135）来引用位置以外，还可以通过 DNS 用域名 （如 www.netscreen.com）来引用位置。下列所有程序均支持 DNS 转换：

- 地址簿
- 系统日志
- 电子邮件
- WebTrends
- Websense
- LDAP
- SecurID
- RADIUS
- NetScreen-Global PRO

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 374 页上的 “DHCP”）时，还必须在 WebUI 的 DHCP 页中输入 DNS 服务器的 IP 地址，也可以使用 CLI 中的* ***set interface*** *interface* ***dhcp*** *命令。*

DNS 查找

当 NetScreen 设备与 DNS 服务器连接以解析域名 / 地址映射时，会将该条目存储在其 DNS 状态表中。下面的列表包含 DNS 查找涉及到的一些具体内容：

- 在 WebUI 中，一旦在支持 DNS 的页面中按下 **Apply** 或 **OK** 就会执行 DNS 查找。在 CLI 中，输入支持 DNS 的命令后，将会执行 DNS 查找。
- 当 DNS 查找返回多个条目时，通讯簿会接受所有条目。上面所列的其它程序只接受第一个条目。
- 当使用 WebUI 中的 **Refresh** 按钮或输入 **exec dns refresh** CLI 命令刷新查找时，如果 NetScreen 设备发现域名表中有内容发生了变化，将重新安装所有策略。
- 如果 DNS 服务器发生故障， NetScreen 设备会重新查找所有内容。
- 如果查找失败， NetScreen 设备将从高速缓存表中将其删除。
- 如果在向通讯簿添加地址时域名查找失败， NetScreen 设备会显示一条错误信息，声明已成功添加地址，但是 DNS 名查找失败。

NetScreen 设备必须每天进行一次新的查找，您可以安排 NetScreen 设备在指定时间进行查找：

WebUI

Network > DNS：输入以下内容，然后单击 **Apply**：

DNS refresh every day at：选中复选框而后输入时间 <hh:mm>

CLI

1. set dns host schedule *time_str*
2. 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

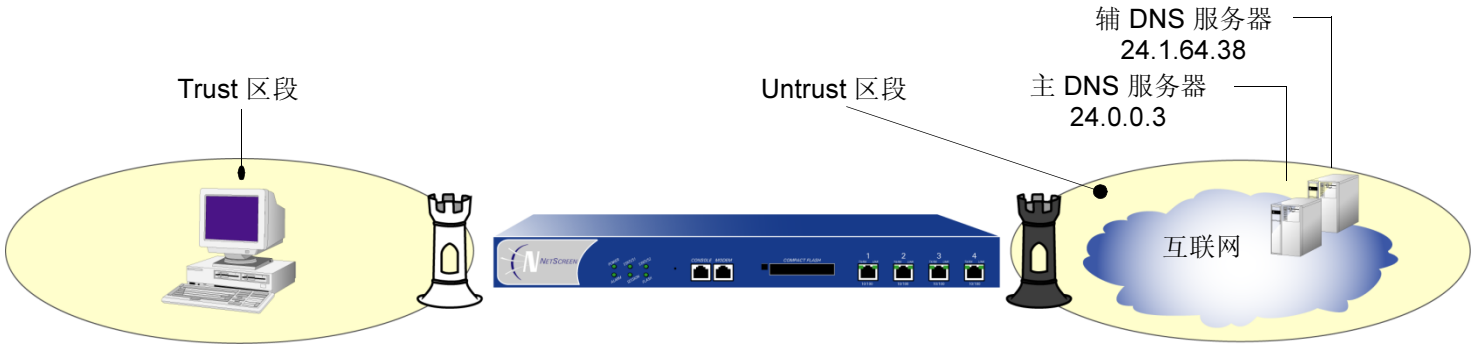
Network > DNS > Show DNS Table

CLI

get dns host report

范例：定义 DNS 服务器地址并安排查找计划

要实现 DNS 功能，在 NetScreen 设备中为 24.1.64.38 和 24.0.0.3 上的 DNS 服务器输入 IP 地址，保护总公司仅有的一台主机。将 NetScreen 设备安排为在每天晚上 11:00 时刷新存储在 DNS 状态表中的 DNS 设置。



WebUI

Network > DNS：输入以下内容，然后单击 **Apply**：

Primary DNS Server: 24.0.0.3

Secondary DNS Server: 24.1.64.38

DNS refresh every day at: （选择）, 23:00

CLI

1. set dns host dns1 24.0.0.3
2. set dns host dns2 24.1.64.38
3. set dns host schedule 23:00
4. save

DHCP

“动态主机配置协议” (DHCP) 的设计目的是通过自动为网络中的主机分配 TCP/IP 设置，来减少对网络管理员的需求。 DHCP 会代替管理员自动为网络中的每台机器分配、配置、跟踪和更改 （必要时）所有 TCP/IP 设置。此外，DHCP 还可以确保不使用重复地址、重新分配未使用的地址，并且可以自动为主机连接的子网分配适当的 IP 地址。

不同的 NetScreen 设支持不同的 DHCP 角色：

- **DHCP 客户端：**有些 NetScreen 设备可以作为 DHCP 客户端，从 ISP 处接收为 Untrust 区段接口动态指定的 IP 地址。
- **DHCP 服务器：**有些 NetScreen 设备也可以作为 DHCP 服务器，为 Trust 区段内的主机 （作为 DHCP 客户端）分配动态 IP 地址。 .

  注意：*在使用 DHCP 为 Trust 区段内的主机 （如工作站和打印机）分配地址时，您仍然可以对其它机器（如邮件服务器和 WINS 服务器）使用固定 IP 地址。*

- **DHCP 转接代理：**某些 NetScreen 设备还可以充当 DHCP 中继代理，接收来自 DHCP 服务器的 DHCP 信息，并将该信息转递给 Trust 区段内的主机。
- **DHCP 客户端 / 服务器：**最后，NetScreen 设备可以同时作为 DHCP 客户端和 DHCP 服务器。此外，您也可以配置 DHCP 客户端模块将接收到的 TCP/IP 设置转发到 DHCP 服务器模块，向 Trust 区段提供 TCP 设置作为 DHCP 客户端的主机时使用。

DHCP 由两部分组成：用于传送与主机有关的 TCP/IP 配置设置的协议和用于分配 IP 地址的机制。当 NetScreen 设备充当 DHCP 服务器时，它会在每一主机启动时为其提供下面的 TCP/IP 设置：

- 缺省网关 IP 地址和网络掩码。如果您将这些设置保留为 0.0.0.0/0，DHCP 服务器模块会自动使用缺省 Trust 区段接口的 IP 地址和网络掩码。[1]
- 下列服务器的 IP 地址：
  - WINS 服务器 (2)：[2] “Windows 互联网命名服务” (WINS) 服务器将 Windows NT 网络环境使用的 NetBIOS 名称映射为基于 IP 的网络中使用的 IP 地址。
  - NetInfo 服务器 (2)：NetInfo 是一种 Apple 网络服务，用于在 LAN 内分发管理数据。
  - NetInfo 标记 (1)：Apple NetInfo 数据库使用的识别标记。
  - DNS 服务器 (3)：“域名系统” (DNS) 服务器可将统一资源定位器 (URL) 映射为 IP 地址。
  - SMTP 服务器 (1)：“简单邮件传输协议” (SMTP) 服务器可向存储收到邮件的邮件服务器（如 POP3 服务器）传送 SMTP 消息。
  - POP3 服务器 (1)：“邮局协议版本 3” (POP3) 服务器可存储收到的邮件。 POP3 服务器必须与 SMTP 服务器联合使用。
  - 新闻服务器 (1)：新闻服务器接收并存储新闻组的寄来的信息。

注意：*当 NetScreen 设备向某一 DHCP 客户端传递上述参数时，如果该客户端有指定的 IP 地址，该地址将忽略从 DHCP 服务器接收到的所有动态信息。*

1. 在可以于 Trust 区段绑定多个接口的装置上，缺省接口是第一个绑定到该区段并指定 IP 地址的接口。
2. 括号中的数字表示支持的服务器数量。

DHCP 服务器

NetScreen 设备在绑定到 Trust 区段的一个或多个接口上最多能支持八台 DHCP 服务器。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 设备会为充当 DHCP 客户端的主机从地址池[3] 中分配（或“租借”）一个 IP 地址。可在一定时间内租用该 IP 地址，也可无限期租用，直到客户端放弃该 IP 地址为止。（要定义无限租用期，请输入 0。）
- 在“保留”模式下，特定客户端每次联机时， NetScreen 设备都会从地址池中专门为其分配一个指定的 IP 地址。

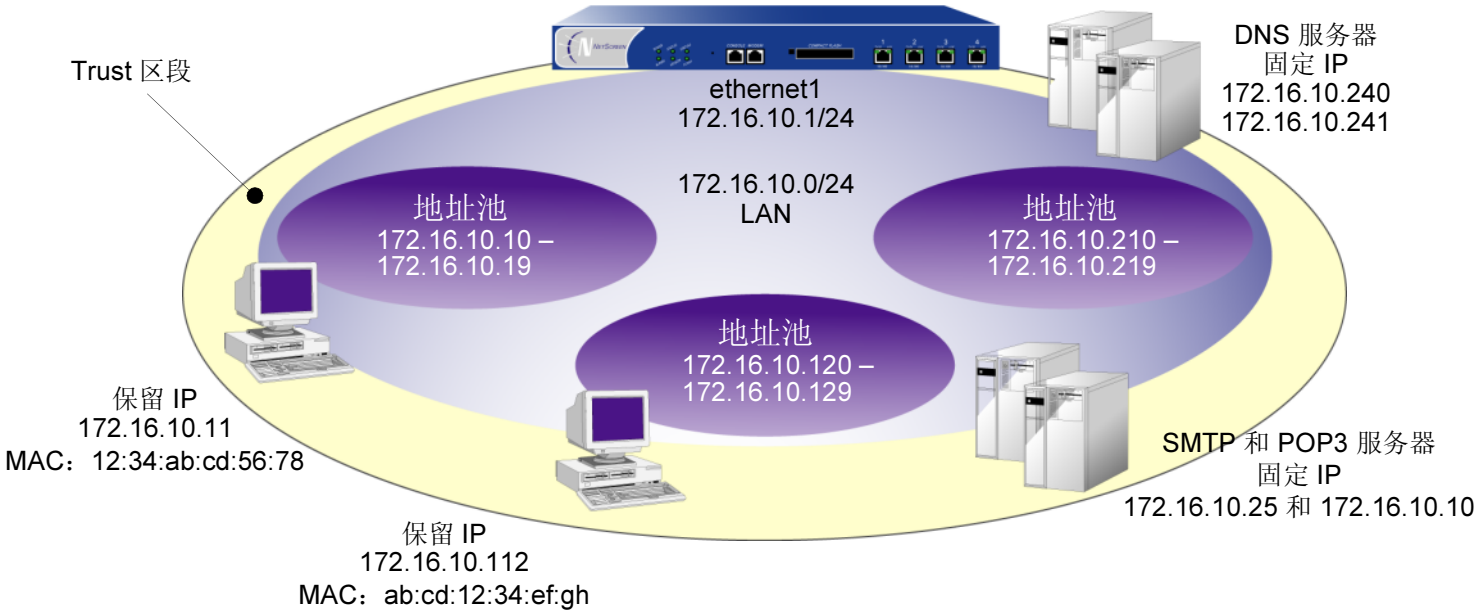
注意：*NetScreen 设备在快速存储器中保存通过 DHCP 分配的每个 IP 地址。因此，重新启动 NetScreen 设备不影响地址分配。*

当冗余 NSRP 集群中的主单元行使 DHCP 服务器的功能时，集群中的所有成员都会保留全部的 DHCP 配置以及 IP 地址分配信息。一旦发生故障切换，新的主单元将负责维护所有 DHCP 分配。但是，如果 HA 通信暂时不可用，可以对集群中的两个单元同时使用下面的 CLI 命令，使集群成员中的 DHCP 分配重新同步：**set nsrp rto-mirror sync**。

3. 地址池是指同一子网内的 IP 地址的定义范围， NetScreen 设备可以从中提取 DHCP 地址进行分配。最多可以编组 255 个 IP 地址。

范例：NetScreen 设备作为 DHCP 服务器

用 DHCP 将 Trust 区段内的 172.16.10.0/24 网络分成三个 IP 地址池。除了使用保留 IP 地址的两个工作站和具有静态 IP 地址的四个服务器以外，所有的 IP 地址均为动态分配。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。



WebUI

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

   Address Name: DNS#1

   IP Address/Domain Name: IP/Netmask: 172.16.10.240/32

   Comment: Primary DNS Server

   Zone: Trust

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

   Address Name: DNS#2

   IP Address/Domain Name: IP/Netmask: 172.16.10.241/32

   Comment: Secondary DNS Server

   Zone: Trust

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

   Address Name: SMTP

   IP Address/Domain Name: IP/Netmask: 172.16.10.25/32

   Comment: SMTP Server

   Zone: Trust

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

   Address Name: POP3

   IP Address/Domain Name: IP/Netmask: 172.16.10.110/32

   Comment: POP3 Server

   Zone: Trust

5. Network > Interfaces > Edit （对于 ethernet1） > DHCP：选择 **DHCP Server**，然后单击 **Apply**。[4]

4. 如果您将 Gateway 和 Netmask 字段保留为 0.0.0.0， DHCP 服务器模块会发送 ethernet1 的 IP 地址和网络掩码组到其客户端 （本范例为 172.16.10.1 和 255.255.255.0）。然而，如果您启用 DHCP 客户端模块以转发 TCP/IP 设置到 DHCP 服务器模块（请参阅第 389 页上的 “TCP/IP 设置传播”），则必须手动在 Gateway 和 Netmask 字段中输入 172.16.10.1 和 255.255.255.0。

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

   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

7. Interfaces > Edit（对于 ethernet1）> DHCP > New Address：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

8. Interfaces > Edit（对于 ethernet1）> DHCP > New Address：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

9. Interfaces > Edit（对于 ethernet1）> DHCP > New Address：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

10. Interfaces > Edit（对于 ethernet1）> DHCP > New Address：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

11. Interfaces > Edit（对于 ethernet1）> DHCP > New Address：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. set address trust dns1 172.16.10.240 255.255.255.255 “primary dns server”
2. set address trust dns2 172.16.10.241 255.255.255.255 “secondary dns server”
3. set address trust snmp 172.16.10.25 255.255.255.255 “snmp server”
4. set address trust pop3 172.16.10.110 255.255.255.255 “pop3 server”
5. set interface ethernet1 dhcp server option domainname dynamic.com[5]
6. set interface ethernet1 dhcp server option lease 0
7. set interface ethernet1 dhcp server option dns1 172.16.10.240
8. set interface ethernet1 dhcp server option dns2 172.16.10.241
9. set interface ethernet1 dhcp server option smtp 172.16.10.25
10. set interface ethernet1 dhcp server option pop3 172.16.10.110
11. set interface ethernet1 dhcp server ip 172.16.10.10 to 172.16.10.19
12. set interface ethernet1 dhcp server ip 172.16.10.120 to 172.16.10.129
13. set interface ethernet1 dhcp server ip 172.16.10.210 to 172.16.10.219
14. set interface ethernet1 dhcp server ip 172.16.10.11 mac 1234abcd5678
15. set interface ethernet1 dhcp server ip 172.16.10.112 mac abcd1234efgh
16. set interface ethernet1 dhcp server service
17. save

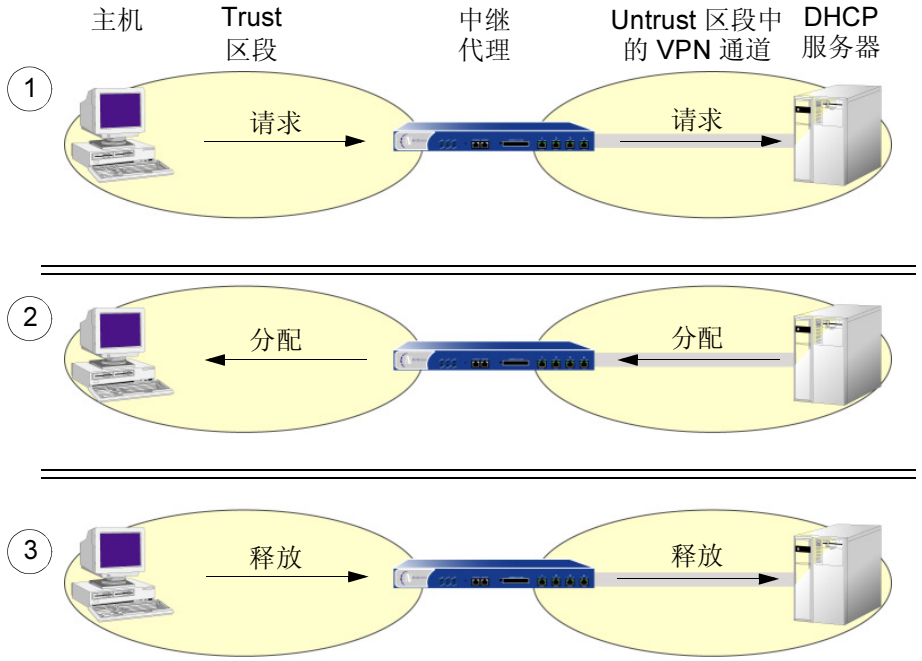
5. 如果您不设定网关的 IP 地址或网络掩码， DHCP 服务器模块会发送 ethernet1 的 IP 地址和网络掩码给其客户端 （本范例为 172.16.10.1 和 255.255.255.0）。然而，如果您启用 DHCP 客户端模块以转发 TCP/IP 设置到 DHCP 服务器模块 （请参阅第 389 页上的 “TCP/IP 设置传播”），则必须手动输入这些选项：**set interface ethernet1 dhcp server option gateway 172.16.10.1** 和 **set interface ethernet1 dhcp server option netmask 255.255.255.0**.

DHCP 中继代理

充当 DHCP 中继代理时，NetScreen 设备在 Trust 区段内的主机与 Untrust 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。

注意： *当 NetScreen 设备充当 DHCP 中继代理时，由于远程 DHCP 服务器控制着所有 IP 地址分配，所以 NetScreen 设备不会生成 DHCP 分配状态报告。*

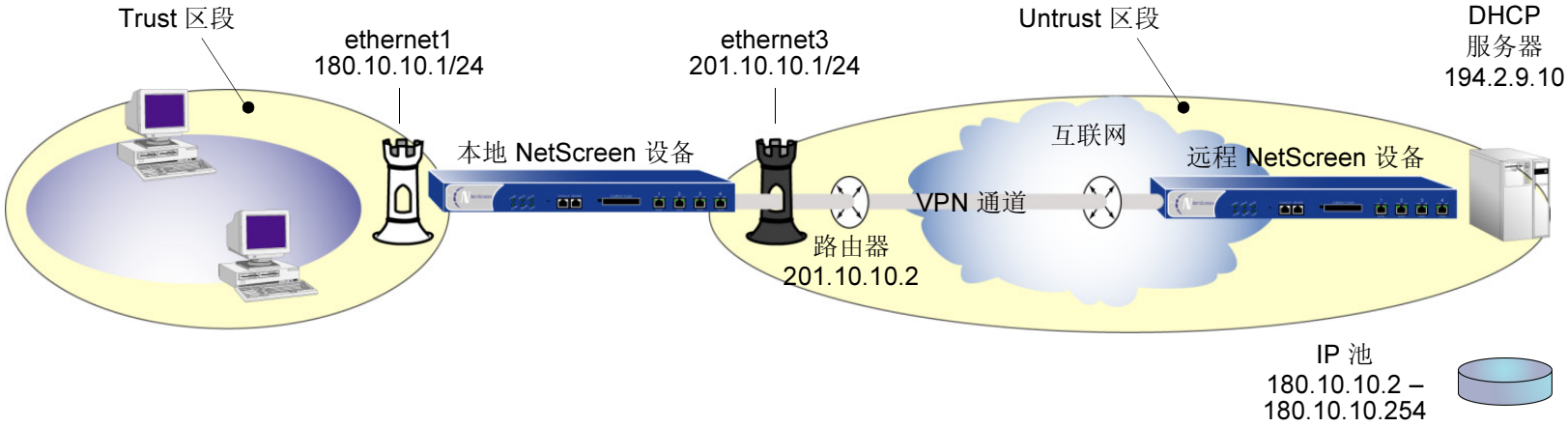
下面的简化示意图展示了使用 NetScreen 设备作为 DHCP 中继代理时的有关过程。请注意，当 DHCP 消息在不可信网络中传送时，为确保安全，这些消息将通过 VPN 通道进行传递。



注意： *当 NetScreen 设备用作 DHCP 中继代理时，其接口必须处于路由模式或透明模式。*

范例：NetScreen 设备作为 DHCP 中继代理

在本例中，NetScreen 设备从 IP 地址为 194.2.9.10 的 DHCP 服务器中接收 DHCP 信息，而后将其转递给 Trust 区段中的主机。主机从 DHCP 服务器上定义的 IP 池中接收 IP 地址。地址范围是 180.10.10.2 — 180.10.10.254。在本地 NetScreen 设备和 DHCP 服务器之间通过 VPN 通道传递 DHCP 消息，该 DHCP 服务器位于第二个 NetScreen 设备之后。接口 ethernet1 绑定到 Trust 区段，其 IP 地址为 180.10.10.1/24，并且处于路由模式。接口 ethernet3 绑定到 Untrust 区段，其 IP 地址为 201.10.10.1/24。所有安全区段都在 trust-vr 路由选择域中。



WebUI

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

   Zone: Trust

   IP Address/Netmask: 180.10.10.1/24

   输入以下内容，然后单击 **OK**：

   Interface Mode: Route

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

   Zone: Untrust

   IP Address/Netmask: 201.10.10.1/24

3. Network > Routing > Routing Table > 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: 201.10.10.2[6]

4. 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: 194.2.9.10/32

   Zone: Untrust

5. 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 Address: 194.2.9.1

   Outgoing Interface: ethernet3

6. 设置到指定为缺省网关的外部路由器的路由，这对于出站 VPN 和网络信息流来说都是必须的。在本例中， NetScreen 设备将向这个路由器发送经过封装的 VPN 信息流，因为该路由器是路由上到远程 NetScreen 设备的首个跳跃。在本例的示意图中，通过描述经过路由器的通道，说明了上述概念。

> 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：

Security Level:

User Defined: Custom （选择）

Phase1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

6. 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 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：

Bind to: None

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

DHCP Relay Agent: （选择）

Relay Agent Server IP or Domain Name: 194.2.9.10

Use Trust Zone Interface as Source IP for VPN: （选择）

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

Source Address:

Address Book: （选择） , Any

Destination Address:

Address Book: （选择） , DHCP Server

Service: DHCP-Relay

Action: Tunnel

Tunnel VPN: to_dhcp

Modify matching outgoing VPN policy: （选择）

CLI

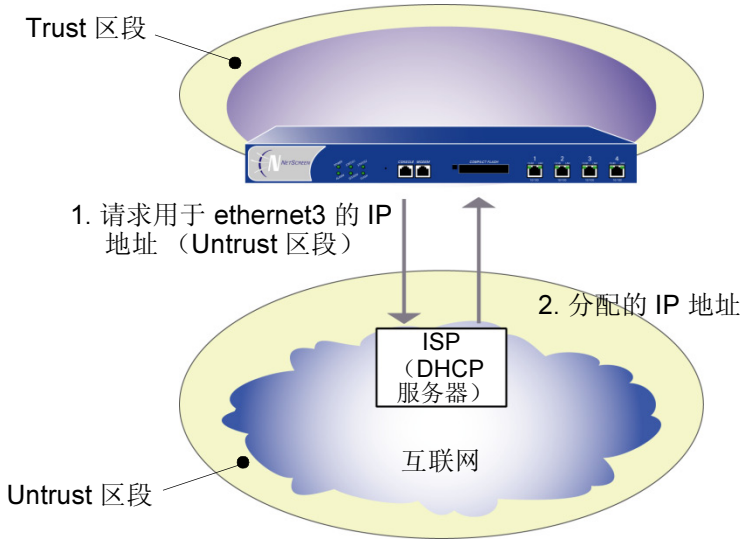
1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 180.10.10.1/24
3. set interface ethernet1 route
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 201.10.10.1/24
6. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.10.10.2
7. set address untrust dhcp_server 194.2.9.10/32
8. set ike gateway “dhcp server” ip 194.2.9.1 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
9. set vpn to_dhcp gateway “dhcp server” proposal g2-esp-3des-sha
10. set interface ethernet1 dhcp relay server-name 194.2.9.10
11. set interface ethernet1 dhcp relay vpn
12. set policy from trust to untrust any dhcp_server dhcp-relay tunnel vpn to_dhcp
13. set policy from untrust to trust dhcp_server any dhcp-relay tunnel vpn to_dhcp
14. save

DHCP 客户端

充当 DHCP 客户端时， NetScreen 设备将从 DHCP 服务器中动态接收绑定到 Untrust 区段的接口的 IP 地址。

范例：NetScreen 设备作为 DHCP 客户端

绑定到 Untrust 区段的接口具有动态分配的 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 地址是 222.33.44.55。



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**[7]，然后单击 **OK**。

CLI

1. set interface ethernet3 dhcp
2. set interface ethernet3 dhcp settings server 222.33.44.55
3. save

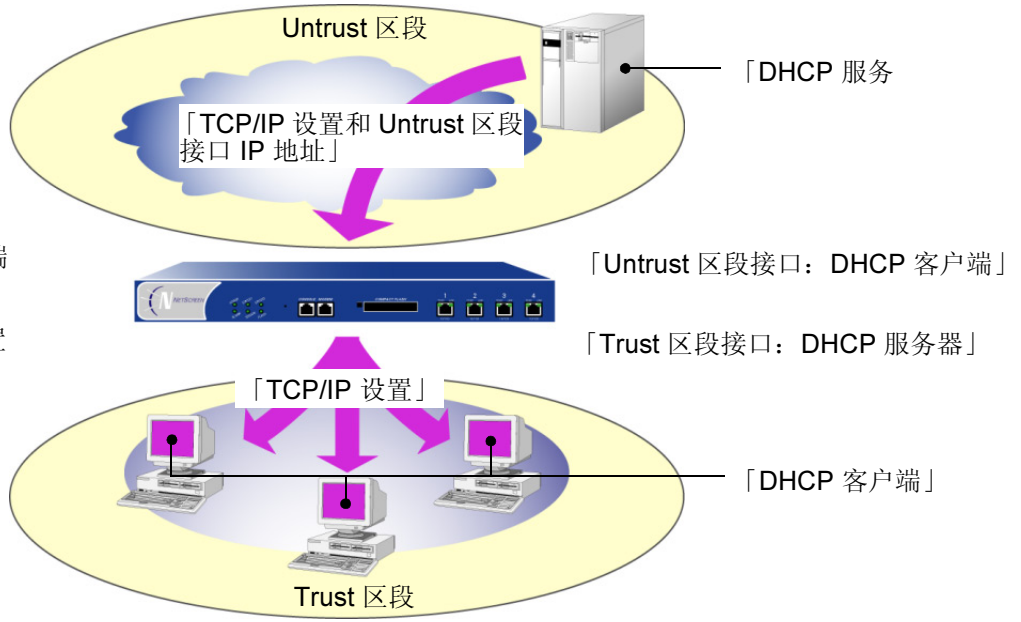
7. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址；但是，可以通过 CLI 指定。

TCP/IP 设置传播

有些 NetScreen 设备可以作为「动态主机配置协议」(DHCP) 客户端，从外部 DHCP 服务器接收 Untrust 区段接口的 TCP/IP 设置和 IP 地址。有些 NetScreen 设备可以作为 DHCP 服务器，向 Trust 区段中的客户端提供 TCP/IP 设置和 IP 地址。当 NetScreen 设备同时作为 DHCP 客户端和 DHCP 服务器时，可以将通过 DHCP 客户端模块获知的 TCP/IP 设置传输到 DHCP 服务器模块。 TCP/IP 设置包括缺省网关的 IP 地址和子网掩码，和用于任何或所有下列服务器的 IP 地址：

- DNS (3)
- WINS (2)
- NetInfo (2)
- SMTP (1)
- POP3 (1)
- News (1)

「NetScreen 设备同时是 Untrust 区段中 DHCP 服务器的客户端和 Trust 区段中客户端的 DHCP 服务器。」
「采用自己作为 DHCP 客户端时接收的 TCP/IP 设置，然后作为 DHCP 服务器将设置转发到 Trust 区段中的客户端。」



您可以配置 DHCP 服务器模块，使用 **set interface untrust dhcp-client settings update-dhcpserver** 命令传播从 DHCP 客户端模块接收的所有 TCP/IP 设置。您也可以用不同设置覆盖任何设置。

范例：转发 TCP/IP 设置

在本范例中，您配置 NetScreen 设备以同时作为 Untrust 接口上的 DHCP 客户端和 Trust 接口上的 DHCP 服务器。

作为 DHCP 客户端时， NetScreen 设备会从在 211.3.1.6 的外部 DHCP 服务器接收 Untrust 接口的 IP 地址和其 TCP/IP 设置。您启用 NetScreen 设备中的 DHCP 客户端模块以将其接收到的 TCP/IP 设置传输到 DHCP 服务器模块。

您配置 NetScreen 设备 DHCP 服务器模块对其从 DHCP 客户端模块接收到的 TCP/IP 设置进行下列工作：

- 转发 DNS IP 地址到其在 Trust 区段中的 DHCP 客户端。
- 以下列内容覆盖缺省网关[8]、网络掩码和 SMTP 服务器及 POP3 服务器 IP 地址：
  - 10.1.1.1 （这是 Trust 接口的 IP 地址）
  - 255.255.255.0 （这是 Trust 接口的网络掩码）
  - SMTP: 211.1.8.150
  - POP3: 211.1.8.172

您也会配置 DHCP 服务器模块以发送下列未从 DHCP 客户端模块接收到的 TCP/IP 设置：

- 主要 WINS 服务器：10.1.2.42
- 次要 WINS 服务器：10.1.5.90

最后，您配置 DHCP 服务器模块以从下列 IP 池将 IP 地址指定给在 Trust 区段中作为 DHCP 客户端的主机：10.1.1.50 – 10.1.1.200.

8. 如果 DHCP 服务器已在 Trust 接口上启用并有已定义的 IP 地址池（这是有些 NetScreen 设备上的缺省行为），您必须先删除 IP 地址池，然后才能更改缺省网关和网络掩码。

WebUI

注意：在 ScreenOS 4.0.0 中，您只能通过 CLI 设定这项功能。

CLI

1. set interface untrust dhcp-client settings server 211.3.1.6
2. set interface untrust dhcp-client settings update-dhcpserver
3. set interface untrust dhcp-client settings autoconfig
4. set interface untrust dhcp-client enable
5. set interface trust dhcp server option gateway 10.1.1.1
6. set interface trust dhcp server option netmask 255.255.255.0
7. set interface trust dhcp server option wins1 10.1.2.42
8. set interface trust dhcp server option wins2 10.1.5.90
9. set interface trust dhcp server option pop3 211.1.8.172
10. set interface trust dhcp server option smtp 211.1.8.150
11. set interface trust dhcp server ip 10.1.1.50 to 10.1.1.200
12. set interface trust dhcp server 222.33.44.55service
13. save

PPPoE

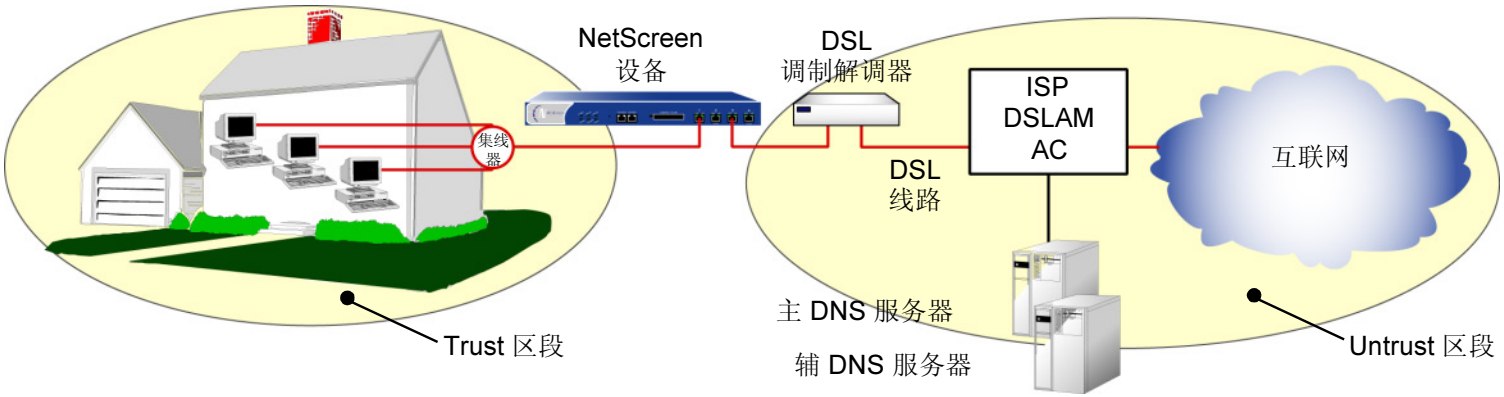
“以太网点对点传输协议”(PPPoE) 允许以太网 LAN 成员通过将 IP 包封装在 PPP 负荷（它封装在 PPPoE 负荷内）中的方式与其 ISP 单独建立 PPP 连接。

某些 NetScreen 设备支持 PPPoE，允许它们将 PPPoE 用于其客户端的互联网访问，以兼容方式在 ISP 管理的 DSL、Ethernet Direct 和电缆网络上运行。

范例：设置 PPPoE

下例讲解如何为 PPPoE 连接定义 NetScreen 设备的不可信接口，以及如何开始 PPPoE 服务。

在本例中，NetScreen 设备从该 ISP 处接收为其 Untrust 区段接口 (ethernet3) 动态分配的 IP 地址，并且该 NetScreen 设备还会为其 Trust 区段内的三台主机动态分配 IP 地址。此时，该 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，该接口处于 NAT 模式。



在为 PPPoE 服务设立本例中的站点之前，您必须得有以下设备：

- 数字用户线 (DSL) 调制解调器和线缆
- ISP 帐户
- 用户名及密码 （ISP 提供）

WebUI

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   IP Address/Netmask: 172.16.30.10/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Obtain IP using PPPoE: （选择）
   User Name/Password: < 名称 >/< 密码 >
3. Network > Interfaces > Edit（对于 ethernet3）：要测试 PPPoE 连接，请单击 **Connect**。

   注意：*建立起 PPPoE 连接后， ISP 会自动为不可信接口和 “域名服务” (DNS) 服务器提供 IP 地址。*

   如果不可信接口使用静态 IP 地址，则必须先获得 DNS 服务器的 IP 地址，然后将其手动输入 NetScreen 设备和信任主机。
4. Network > Interfaces > Edit（对于 ethernet1）> DHCP：选择 **DHCP Server**，然后单击 **Apply**。
5. 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 Options：输入以下内容，然后单击 **Return**：

DNS#2: 0.0.0.0

Domain Name: （保留空白）

6. 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

7. 关闭 DSL 调制解调器、NetScreen 设备和三台工作站的电源。
8. 打开 DSL 调制解调器。
9. 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。

10. 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：*在使用 DHCP 为信任方的主机分配 IP 地址时， NetScreen 设备自动将从 ISP 接收的 DNS 服务器的 IP 地址转发给信任主机。*

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. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.16.30.10/24
3. set interface ethernet3 zone untrust
4. set pppoe interface ethernet3
5. set pppoe username *name_str* password *pswd_str*
6. 要测试 PPPoE 连接：

   exec pppoe connect

   get pppoe
7. set interface ethernet1 dhcp server service
8. set interface ethernet1 dhcp server ip 172.16.30.2 to 172.16.30.5
9. set interface ethernet1 dhcp server option lease 60
10. save
11. 关闭 DSL 调制解调器、NetScreen 设备和三台工作站的电源。
12. 打开 DSL 调制解调器。
13. 打开 NetScreen 设备。
14. 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。

URL 过滤配置

NetScreen 利用 Websense Enterprise Engine 支持 URL 过滤，根据站点的 URL、域名和 IP 地址， Websense Enterprise Engine 可以阻止或允许访问不同的站点。使用直接嵌入在 NetScreen 防火墙中的 Websense API，NetScreen 设备可以与 Websense URL-blocking 服务器建立直接链接。

利用 Websense 管理器， NetScreen 管理员可以执行下列操作：

- 修改 URL-blocking 数据库，以阻止或允许访问所选的任何站点
- 为一天中的不同时间安排不同的 URL 过滤配置文件
- 下载被封锁或查看的 URL 的 Websense Reporter 日志

***注意：** 有关 Websense 的详细信息，请访问 www.websense.com。*

要指定 URL 过滤选项：

WebUI

Configuration > URL Filtering：输入以下内容，然后单击 **Apply**：

Enable URL Filtering via Websense Server: （选择）

Websense Server Name：运行 Websense 服务器的计算机的 IP 地址。

Websense Server Port：Websense 的缺省端口是 15868。如果更改了 Websense 服务器的缺省端口，还必须得更改 NetScreen 设备上的端口。有关完整信息，请参阅 Websense 文档。

Communication Timeout：NetScreen 设备等待 Websense 过滤器响应的时间间隔（以秒为单位）。如果 Websense 在该时间间隔内没有响应，您可以选择让 NetScreen 设备阻止或允许该请求 （参见下文）。

Current Server Status：NetScreen 设备报告 Websense 服务器的状态。要更新状态报告，请单击 Server Status 图标。

If connectivity to the Websense server is lost：如果 NetScreen 设备与 Websense 服务器失去联系，您可以指定 **Block** 或 **Permit** 所有 HTTP 请求。

Blocked URL Message Type：当 Websense 封锁某站点时，用户接收的消息源。如果选择 **Websense**， Websense 服务器将会发送该消息。如果选择 **NetScreen**， NetScreen 设备将会发送该消息，该消息是在 NetScreen Blocked URL Message 字段内输入的。

> ***注意：*** *如果选择* ***NetScreen****， Websense 提供的一些功能将被禁止，如重定向功能。*

NetScreen Blocked URL Message：此处为封锁某站点后 NetScreen 设备返回给用户的消息。您可以使用从 Websense 发来的消息，也可以创建一条要从 NetScreen 设备发送的消息（最多 220 个字符）。

CLI

1. set url config { enable | disable }
2. set url message *“string”*
3. set url msg-type {0 | 1}
4. set url server { *dom_name* | *ip_addr* } *port_num number*
5. set url fail-mode { block | permit }

> ***注意：*** *有关* ***set url*** *命令参数的解释，以及示例和相关命令，请参阅 NetScreen CLI Reference Guide。*

下载 / 上传设置和软件

可以向 NetScreen 设备上传和从中下载配置设置和软件。上传和下载的位置种类取决于您是使用 WebUI 还是使用 CLI 来执行该操作。如果使用 WebUI 和 Web 浏览器支持，您可以从任何本地目录上传或下载配置设置以及上传 ScreenOS 软件。如果是通过 CLI，您可以向 TFTP 服务器或 PC 卡上传和从中下载设置及软件。

保存和导入设置

在每次做出重要改动后备份设置是一种很好的习惯。通过 WebUI，您可以将配置下载至任何本地目录，做为预防备份。对于某些 NetScreen 设备，可以使用 CLI 将配置下载至 TFTP 服务器或 PC 卡中。一旦需要保存的备份配置，只需将其上传到 NetScreen 设备即可。

上传和下载配置的功能还提供了大量分发配置模板的方法。

要下载配置：

WebUI

1. Configuration > Update > Config File：单击 **Save to File**。

   会出现一条系统消息，提示您打开该文件或将其保存到计算机上。
2. 单击 **Save**。
3. 找到要保存配置文件的位置，然后单击 **Save**。

CLI

save config from flash to { tftp *ip_addr* | slot } *filename* [from *interface*]

注意：*在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。*

要上传配置：

WebUI

Configuration > Update > Config File：输入以下内容，然后单击 **Apply**：

如果要将新配置和当前配置合并在一起，请选择 **Merge to Current Configuration**；如果要用新配置覆盖当前配置，请选择 **Replace Current Configuration**。

> New Configuration File：输入配置文件位置或单击 **Browse** 找到文件位置，选择该文件，然后单击 **Open**。

CLI

save config from { tftp *ip_addr* | slot } *filename* to flash [merge [from *interface*]]

注意：*在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。*

上传和下载软件

当 NetScreen ScreenOS 操作系统进行了更新时，客户可以购买并将其上传至自己的 NetScreen 设备中。对于某些 NetScreen 设备，可以使用 WebUI 从本地目录上传软件。通过 CLI，可以从 TFTP 服务器或 PC 卡上传软件，并且可以将软件下载至 TFTP 服务器。

注意： *软件升级后，请重新启动 NetScreen 设备。此过程需要几分钟时间。*

WebUI

Configuration > Update > ScreenOS/Keys：输入以下内容，然后单击 **Apply**：

Select what you want to update: Firmware、 Image Key 或 License File。

> Load File：输入要更新的文件的位置或单击 **Browse** 找到文件位置，选择该文件，然后单击 **Open**。

CLI

save software from { tftp *ip_addr* | slot } *filename* to flash

注意： *在某些 NetScreen 设备中，必须指定 slot 1 或 slot 2。*

您还可以通过 CLI 将软件下载至 TFTP 服务器，使用以下 **save** 命令：

save software from flash to tftp *ip_addr filename* [from *interface*]

许可密钥

利用许可密钥功能，无需将 NetScreen 设备升级为不同的设备或系统映像，即可对其能力进行扩展。您可以购买一个密钥来解锁软件中已加载的指定功能，比如下面的这些功能：

- 用户容量
- 虚拟系统、区段和虚拟路由器
- HA

每台 NetScreen 设备出厂时都已启用了标准功能集，而且可能会支持激活可选功能或提高现有功能的能力。要了解当前都有哪些功能可以进行升级，请参阅 NetScreen 的最新市场文献。

获得并应用许可密钥的过程如下：

1. 与向您销售 NetScreen 设备的增值转售商 (VAR) 联系，或者直接与 NetScreen Technologies 联系。
2. 提供您设备的序列号并说明您想要的功能选项。

   生成许可密钥，而后通过电子邮件将其发送给您。
3. 通过 WebUI 或 CLI 输入该密钥。（参见以下示例。）

范例：扩大用户容量

某家小公司使用了单台 NetScreen 设备，该设备只具有数量为 10 位用户的许可，随着公司的发展，它现在需要一种用户数不受限制的许可。此时， NetScreen 管理员只要获得一个不限制用户数目的软件密钥，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 File Update: （选择）

Load File: C:\netscreen\keys\A2010002.txt

或者

单击 **Browse** 找到 C:\netscreen\keys，选择 A2010002.txt，然后单击 **Open**。

CLI

1. exec license-key capacity 6a48e726ca050192
2. reset

系统时钟

每台 NetScreen 设备有一个系统时钟，可将其设置为您当地的时区。可以使用 WebUI 或 CLI 来配置当前的时钟设置。

NetScreen 设备可以使用 “网络时间协议” (NTP) 使系统时钟与 NTP 服务器时钟同步。这样，设备可以通过互联网以指定的时间间隔保持系统时钟同步。设置时区时，要指定 NetScreen 设备当地时间早于或晚于 “格林威治标准时间” (GMT) 的小时数。例如，如果 NetScreen 设备的当地时区是 “太平洋标准时间”，则它要比 GMT 时间晚 8 小时。从 Set Offset 下拉列表中选择 **-8**。

还可以通过 WebUI 使系统时钟与计算机时钟同步：

1. Configuration > Date/Time：选择 **Sync Clock with Client** 选项。

   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** 启用自动时钟同步，或单击 **No** 取消操作。

范例：设置系统时钟

在下面的例子中，您要将系统时钟设置为 “太平洋标准时间”，并且将 NetScreen 设备配置为通过 IP 地址为 211.1.10.10 的 NTP 服务器，每隔 5 分钟更新一次时钟。

WebUI

Configuration > Date/Time：输入以下内容，然后单击 **Apply**：

Set Offset hours minutes from GMT: (hours) -8， (minutes) 0

Automatically synchronize with an Internet time server (NTP)：（选择）

Server IP/Name: 211.1.10.10

Update system clock every minutes: 5

CLI

1. set clock ntp
2. set ntp timezone -8 0
3. set ntp server 211.1.10.10
4. set ntp interval 5
5. save

索引

D

E

F

G

H

I

J

K

L

M

N

P

Q

R

V

W

X

Y

Z