NetScreen 概念与范例

ScreenOS 参考指南

第 6 卷：路由

ScreenOS 5.1.0

编号 093-1371-000-SC

修订本 B

Copyright Notice

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, 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:

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave.

Sunnyvale, CA 94089-1206

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

路由选择是 NetScreen 设备和系统等安全设备的基本部分。通过动态路由选择， NetScreen 设备可使用通用协议与路由器及其它网络设备交换路由选择信息，并自动建立及更新路由表。由于动态路由协议使调整自动进行，因此大大缩短了更改网络拓扑结构与调整路由表之间的时间延迟。组播路由提供了一种将信息流转发到多个主机的有效方法。企业使用组播路由将信息流 (例如数据流或视频流) 从一个源同时传送到一组接收方。

第 6 卷，“路由”将介绍以下内容 :

- 路由基础，包括路由表以及如何为基于目标的路由或基于源的路由配置静态路由
- 如何在 NetScreen 设备上配置虚拟路由器以及如何在协议间或虚拟路由器间重新分配路由表条目
- 如何在 NetScreen 设备上配置下列动态路由协议 : 开放式最短路径优先 (OSPF)、路由信息协议 (RIP) 及边界网关协议 (BGP)
- 组播路由基础，包括如何配置静态组播路由
- 如何配置下列组播协议 : 互联网组管理协议 (IGMP)、协议无关组播 - 稀疏模式 (PIM-SM) 以及协议无关组播 - 源特定组播 (PIM-SSM)

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

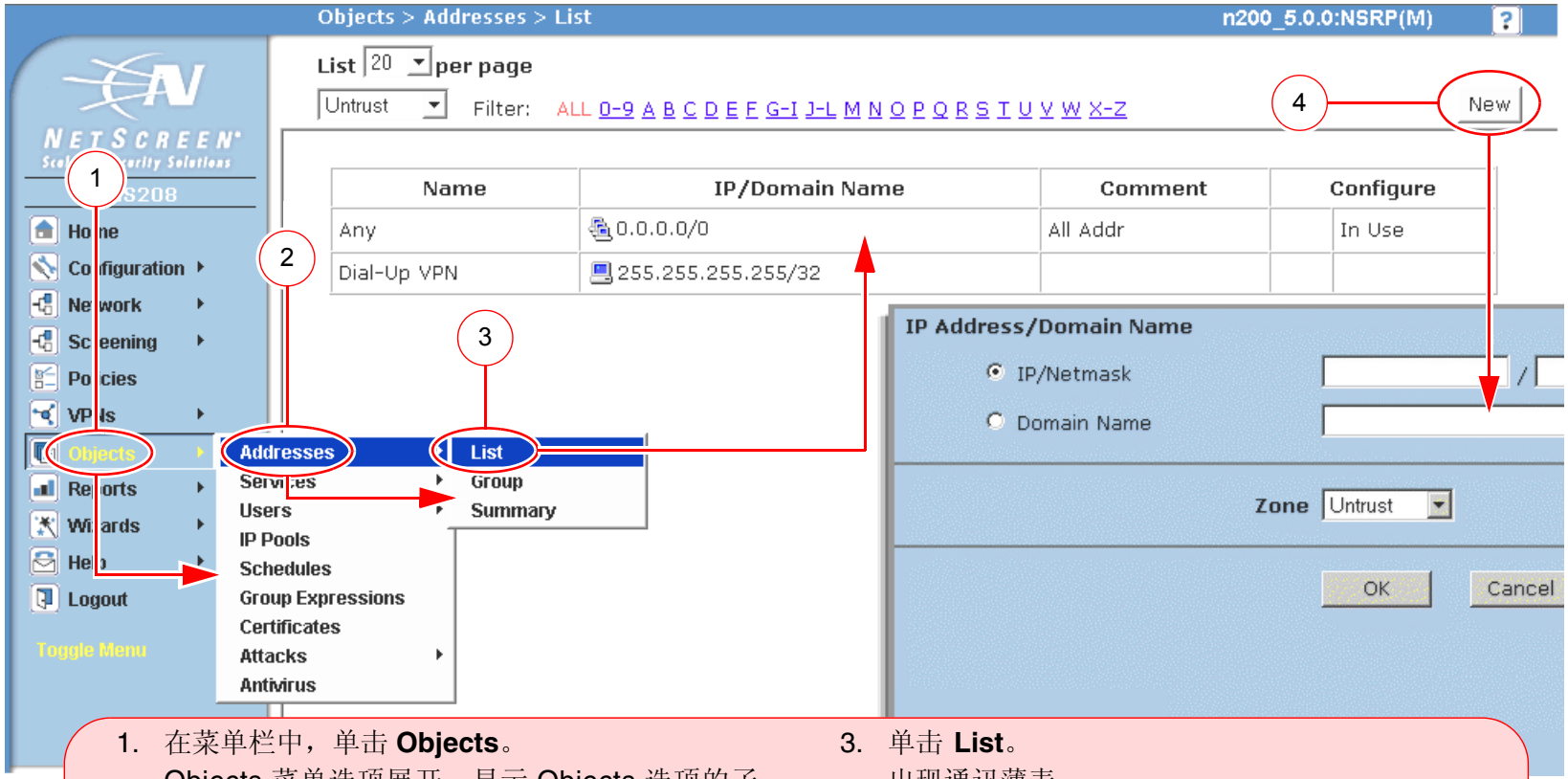
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

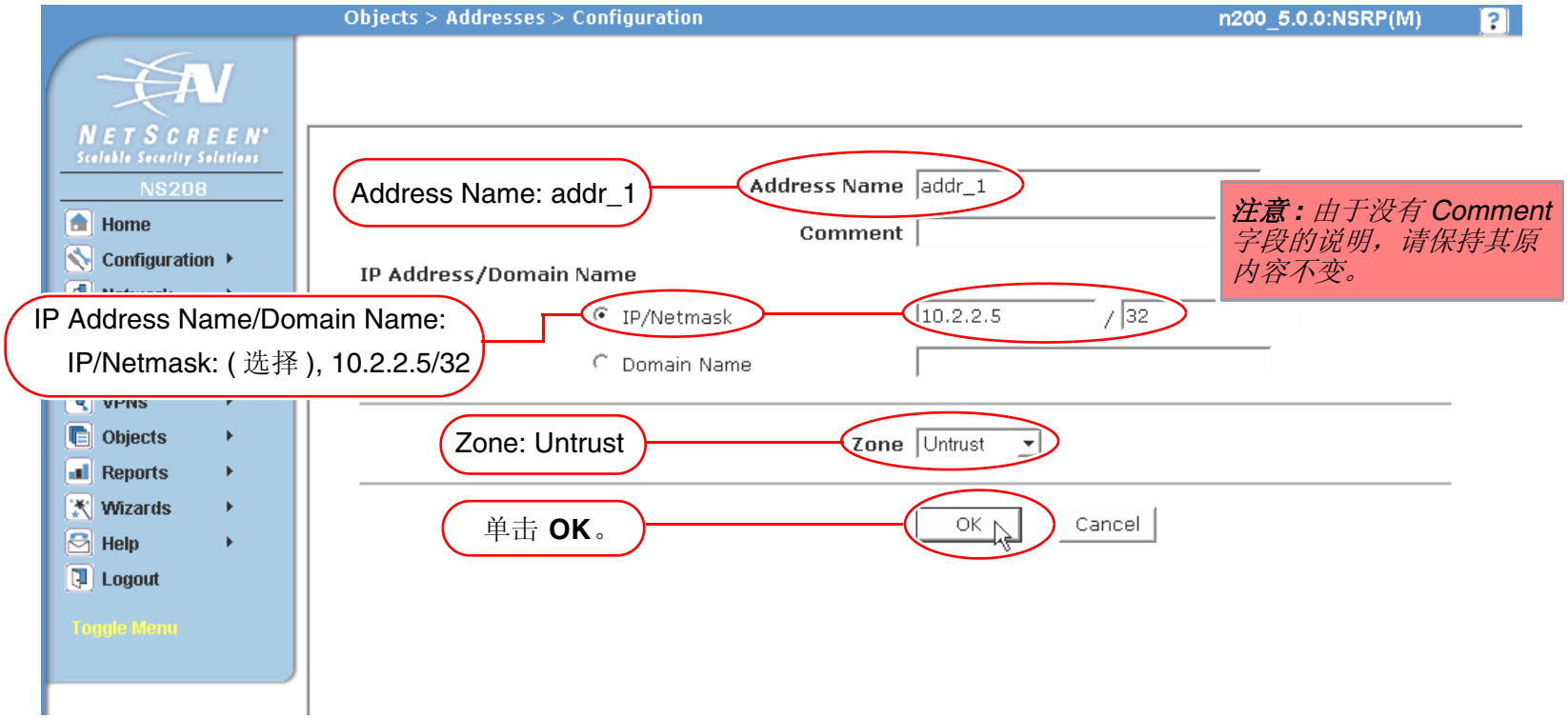
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

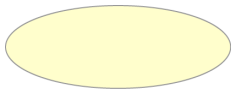


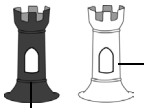
插图约定

下列图形构成了贯穿本书的插图所用的基本图像集：


通用 NetScreen 设备


虚拟路由选择域

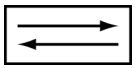

安全区段


安全区段接口
白色 = 受保护区段接口
（例如：Trust 区段）
黑色 = 区段外接口
（例如：Untrust 区段）


通道接口

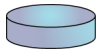

VPN 通道


路由器图标


交换机图标


包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）


互联网


动态 IP (DIP) 池


台式计算机


便携式计算机


通用网络设备
（例如：NAT 服务器，
接入集中器）


服务器

命名约定和字符类型

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

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

ScreenOS 支持以下字符类型 :

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

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

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

JUNIPER NETWORKS NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

路由表和静态路由

为使 NetScreen 设备将数据包从一个网络转发到另一个网络，ScreenOS 维护包含所有已知网络地址条目的*路由表*。路由表通常包含一个或多个*静态路由*，静态路由是手动输入的配置信息，用于定义指向特定目的地址的路径。另外，NetScreen 设备还为组播路由维护单独的路由表。有关组播路由的信息，请参阅第 196 页上的 “NetScreen 设备上的组播路由”。

本章介绍 ScreenOS 路由表、 NetScreen 设备上的基本路由选择过程以及在 NetScreen 设备上配置静态路由的方法。本章包括以下部分：

路由选择基本原理

路由选择是将数据包从一个网络转发到指向最终目的地址的另一个网络的过程。路由器是一个网络与另一个网络之间的汇合点。NetScreen 安全设备提供集成的路由选择功能，让 ScreenOS 将受保护的信息流有效地转发到目的地址。

路由选择方法

在 NetScreen 设备上，可以配置三种路由选择类型：静态、动态和组播。网络使用静态路由时，管理员必须手动配置路由并维护路由器上的路由表。如果网络与许多其它网络相连，或者经常更改内部网络的连接，则应使用动态路由协议自动更新路由表。动态路由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。组播协议使路由器可以从一个源同时向多个接收方转发信息流。

静态路由选择

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

1. 下一跳目的地址是一个路由器。

动态路由选择

动态路由选择涉及路由器交换网络与子网可到达性的信息，以及路由器通过分析内向路由更新消息调整路由表。这些消息在网络中传播，用来引导路由器重新计算路由，并对路由表做出相应更改。

有关“开放式最短路径优先” (OSPF) 的详细信息，请参阅第 3 章，“开放式最短路径优先 (OSPF)”。

有关“路由选择信息协议” (RIP) 的信息，请参阅第 4 章，“路由选择信息协议 (RIP)”。

有关“边界网关协议” (BGP) 的信息，请参阅第 5 章，“边界网关协议 (BGP)”。

组播路由选择

企业使用组播路由选择将信息流 (如数据流或视频流) 从一个源同时传输到一组接收方。任意主机都可以成为源，接收方可以位于互联网上的任意位置。

由于启用组播的路由器仅对要接收信息流的主机传输组播信息流，因此 IP 组播路由选择为将信息流转发到多个主机提供了有效方法。主机必须表示要接收组播数据，而且必须加入组播组才能接收该类数据。启用了组播的路由器仅将组播信息流转发到有意接收该信息流的接收方。

有关组播路由选择的信息，请参阅第 6 章，“组播路由”。

路由表

路由器通常与多个网络相连，负责引导信息流通过这些网络。每个路由器维护一个路由表，该表由已知的网络构成，并且还指明如何到达这些网络。在 NetScreen 设备上处理内向数据包时， ScreenOS 会执行路由表查找，以找出通向目的地址的相应接口。有关 ScreenOS 中数据包的转发流程的详细信息，请参阅第 2 卷，“基本原理”。路由器还为组播路由维护一个路由表。有关组播路由的信息，请参阅第 196 页上的 “组播路由表”。

路由表中的每个条目 (称为*路由条目*或简称为*路由*) 可由信息流所转发到的目标网络识别。目标网络以 IP 地址和网络掩码的形式给出，可以是 IP 网络、子网、超级网或主机。 ScreenOS 路由表条目可能有以下几种来源 :

- 直接连接的网络 (目标网络为分配给 “路由”模式接口的 IP 地址)[2]
- 动态路由协议，如 OSPF、 BGP 或 RIP
- 从其它路由器或虚拟路由器导入的路由
- 静态配置的路由

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

下面是一个 ScreenOS 路由表的范例：

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

Total 8 entries

     ID  IP-Prefix       Interface     Gateway       P      Pref     Mtr   Vsys
--------------------------------------------------------------------------------
*     9  0.0.0.0/0          eth3        10.31.1.1     eB      40      100   root
*    11  192.168.1.100/32   eth2        10.3.3.100    iB      250     0     root
*    10  1.1.0.0/16         eth3        10.31.1.1     eB      40      100   root
*     4  10.1.1.1/32        eth3        10.2.2.250    S       20      1     root
*     1  192.168.1.1/32     eth1        0.0.0.0       C       0       0     root
*     5  2.2.0.0/16         eth3        10.2.2.250    S       20      1     root
*     2  10.3.3.0/24        eth2        0.0.0.0       C       0       0     root
*     3  10.2.2.0/24        eth3        0.0.0.0       C       0       0     root
```

缺省路由

目标网络　转发数据的接口　下一跳　协议　优先级　度量　Vsys

对于每个目标网络，路由表包含以下信息：

- NetScreen 设备上的接口，用于转发流向目标网络的信息流。
- 下一跳，既可以是 NetScreen 设备上的另一个虚拟路由器，也可以是网关的 IP 地址 (通常为路由器的地址)。
- 产生该路由的协议。
- *优先级*，当存在多个路由指向同一目标网络时，可使用优先级来选择要使用的路由。该值由协议或路由的来源决定。路由的优先级值越低，越有可能被选择为活动路由。

  可以为每个虚拟路由器修改各项协议或路由来源的优先级值。有关详细信息，请参阅第 6 卷中的 “虚拟路由器”一章。

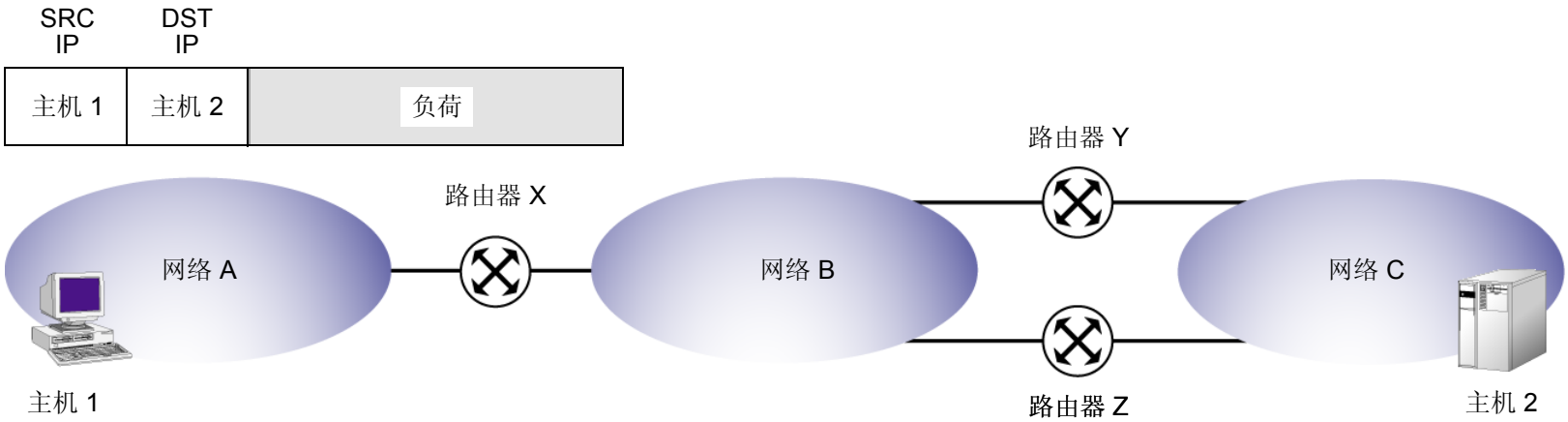
- *度量*，当存在多个路由指向同一目标网络且优先级相同时，还可以使用度量来选择要使用的路由。直连的路由的度量值始终为 0。静态路由的缺省度量值为 1，但可以在定义静态路由时指定其它值。
- 此路由所属的虚拟系统 (vsys)。有关虚拟路由器和 vsys 的详细信息，请参阅第 27 页上的 “虚拟路由器和虚拟系统”。

大多数路由表都包含一个*缺省路由*（网络地址为 0.0.0.0/0），对于发往路由表中定义的网络之外的网络的数据包。

使用静态路由进行路由选择

当某一主机向位于不同网络的另一台主机发送数据包时，每个数据包包头都含有目标主机的地址。当路由器收到数据包时，会将该目的地址与其路由表中的所有地址进行比较。路由器先在路由表中选择一个最明确的[3]指向目的地址的路由，再根据选定的路由条目决定转发数据包的下一跳。

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



3. 确定最明确路由的方法是，先对路由表中每个条目的目的地址和网络掩码执行位逻辑 AND 运算。例如，IP 地址 10.1.1.1 与子网掩码 255.255.255.0 进行位逻辑 AND 运算的结果为 10.1.1.0。最明确的路由就是子网掩码中设置为 1 的位最多的路由（也称作 “最长匹配路由”）。

以下说明每个路由器上的路由表。

路由表

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

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

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

在上例中，路由器 X 有一个为网络 C 配置的静态路由，相应网关 (下一跳) 为路由器 Y。当路由器 X 收到发往网络 C 中主机 2 的数据包时，先将数据包中的目的地址与其路由表进行比较，然后会发现表中的最后一个路由条目是指向目的地址的最明确的路由。最后一条路由条目指定将发往网络 C 的信息流发送到路由器 Y 进行传送。路由器 Y 接收数据包，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数据包。

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

NETSCREEN 设备上的虚拟路由器

ScreenOS 可以将其路由选择组件分成两个或多个虚拟路由器。虚拟路由器支持静态路由协议、动态路由协议和组播协议，可以在一个虚拟路由器上同时启用这些协议。 NetScreen 设备上预先定义了两个虚拟路由器：

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

一些 NetScreen 设备还允许创建其它的定制虚拟路由器。通过将路由选择信息分给两个 (或多个) 虚拟路由器，可以控制给定路由选择域中对其它路由选择域可见的信息。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。也就是说，从一个虚拟路由器的区段发出的信息流*不能*自动转发到另一个虚拟路由器中的区段，即使存在允许转发信息流的策略。如果希望信息流在虚拟路由器之间传递，则需要导出 VR 之间的路由，或在一个 VR 中配置静态路由，将另一 VR 定义为下一跳。

本章不包括有关创建定制虚拟路由器、使用两个或多个虚拟路由器以及导出 VR 之间的路由的信息。有关虚拟路由器的详细信息，请参阅第 19 页上的 “虚拟路由器”。

配置静态路由的时机

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

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

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

- 对于出站 VPN 信息流，如果有多个出接口指向目的地址，则需要设置路由，让出站信息流通过所需接口发送到外部路由器。
- 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，并且该路由将 trust-vr 作为网关。
- 在缺省情况下， NetScreen 设备使用目的 IP 地址来查找转发数据包的最佳路由。也可以在虚拟路由器上启用基于源或基于源接口的路由表。基于源和基于源接口的路由表都包含在虚拟路由器上配置的静态路由。

配置静态路由

要配置静态路由，需要定义以下内容：

- 从中添加路由的虚拟路由器。
- 目标网络的 IP 地址和网络掩码。
- 路由的下一跳，既可以是 NetScreen 设备上的另一个虚拟路由器，也可以是网关 (路由器) 的 IP 地址。如果要指定另一个虚拟路由器，请确保该虚拟路由器的路由表中存在目标网络条目。
- 转发被路由的信息流的接口。接口可以是 ScreenOS 支持的任何接口，如物理接口 (例如 ethernet1/2) 或通道接口。也可对某些应用程序指定 Null 接口 — 请参阅第 17 页上的 “将信息流转发到 Null 接口”。
- (可选) 当存在多个路由指向同一目标网路且优先级相同时，使用路由度量来选择活动路由。静态路由的缺省度量值为 1。
- (可选) 路由标记是在重新分配路由时可用作过滤器的值。例如，可以选择只将包含特定标记值的那些路由导入到虚拟路由器中。
- (可选) 路由的优先级值。缺省情况下，所有静态路由具有相同的优先级值，该值在虚拟路由器中设置。
- (可选) 是否保持路由为活动状态，即使转发接口中断或 IP 地址从接口中被删除。请参阅第 18 页上的 “永久活动路由”。

范例：静态路由

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

Trust-vr 和 untrust-vr 路由表必须包含指向以下目的地址的路由 (以下数字对应第 12 页上的图示):

untrust-vr

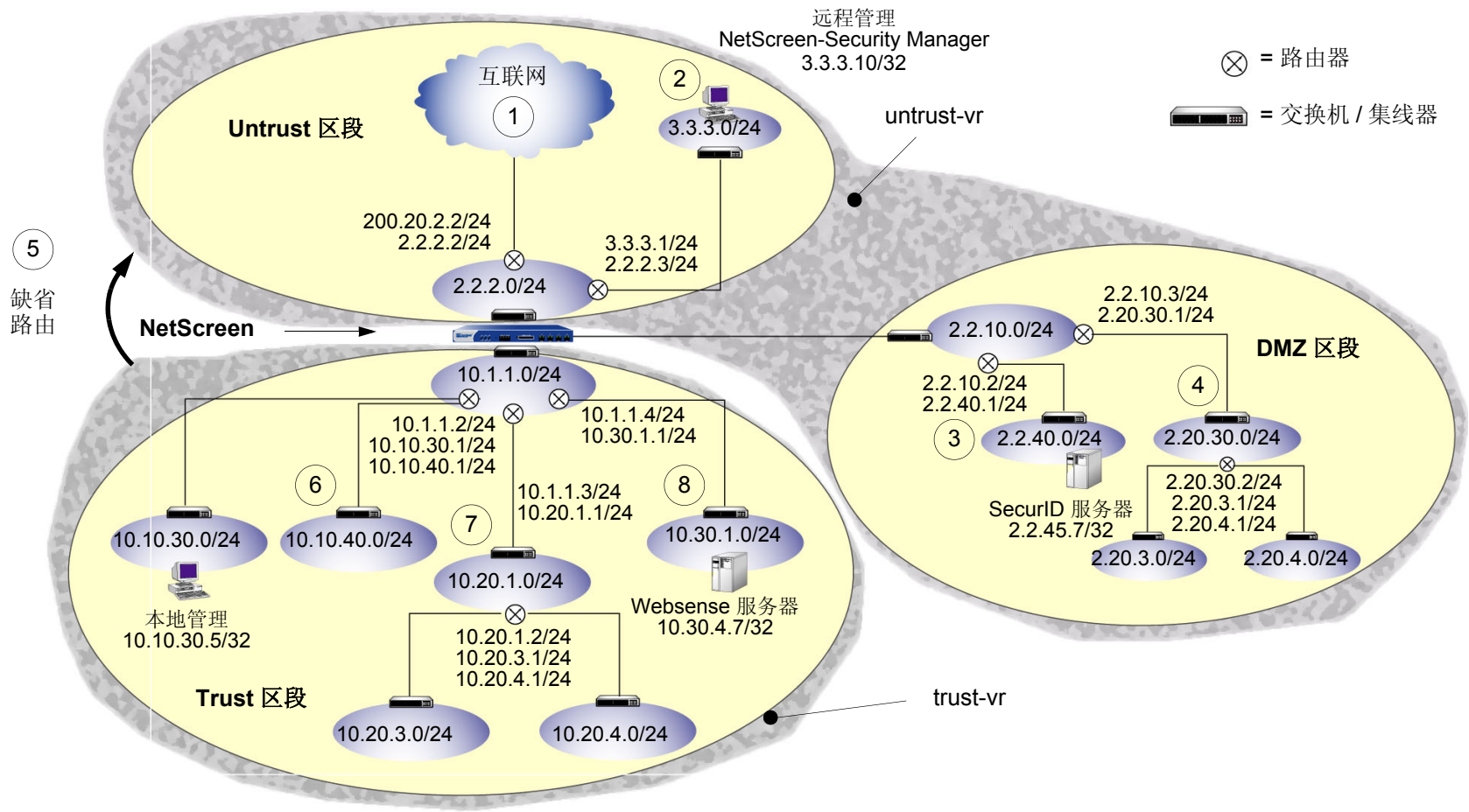
1. 连接到互联网的缺省网关 (这是虚拟路由器的缺省路由)
2. 3.3.3.0/24 子网中的远程管理员
3. DMZ 区段中的 2.2.40.0/24 子网
4. DMZ 区段中的 2.20.0.0/16 子网

trust-vr

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

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

静态路由配置


远程管理
NetScreen-Security Manager
3.3.3.10/32
= 路由器
= 交换机 / 集线器
互联网
1
2
3.3.3.0/24
Untrust 区段
untrust-vr
200.20.2.2/24
2.2.2.2/24
3.3.3.1/24
2.2.2.3/24
2.2.2.0/24
5
缺省
路由
NetScreen
2.2.10.3/24
2.20.30.1/24
2.2.10.0/24
DMZ 区段
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
6
8
7
10.1.1.3/24
10.20.1.1/24
10.10.30.0/24
10.10.40.0/24
10.30.1.0/24
10.20.1.0/24
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 区段
trust-vr
10.20.3.0/24
10.20.4.0/24

WebUI

1. untrust-vr

Network > Routing > Routing Entries > untrust-vr New: 输入以下内容以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

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

Network Address/Netmask: 3.3.3.0/24

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.3

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

Network Address/Netmask: 2.2.40.0/24

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 2.2.10.2

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

Network Address/Netmask: 2.20.0.0/16

Gateway: (选择)

Interface: ethernet2

Gateway IP Address: 2.2.10.3

2. trust-vr

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

Network Address/Netmask: 0.0.0.0/0

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

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

Network Address/Netmask: 10.10.0.0/16

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.2

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

Network Address/Netmask: 10.20.0.0/16

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.3

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

Network Address/Netmask: 10.30.1.0/32

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 10.1.1.4

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

CLI

1. untrust-vr

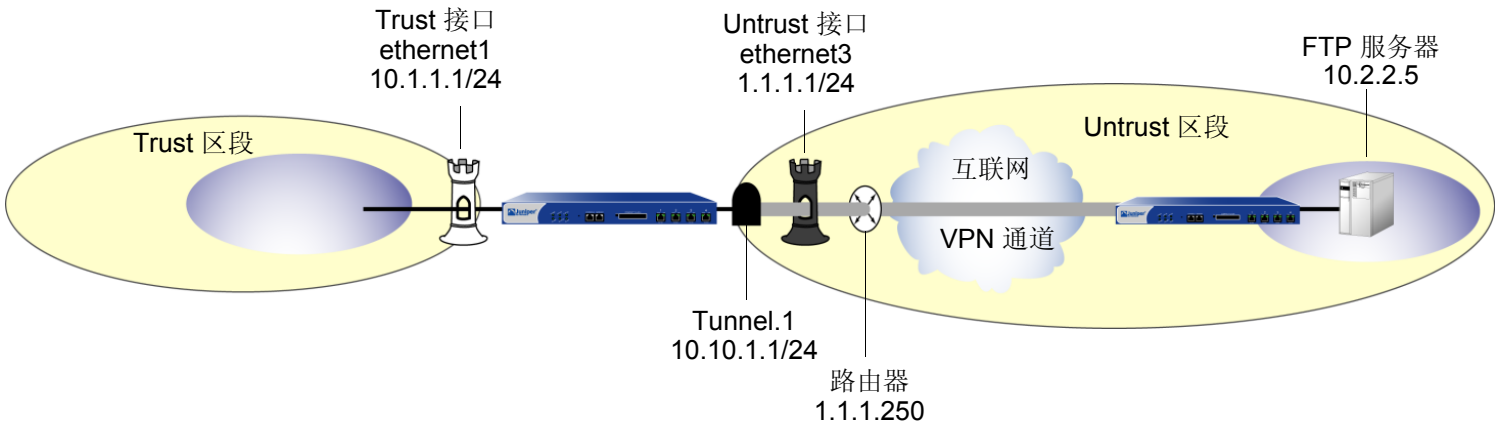
```
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
set vrouter untrust-vr route 3.3.3.0/24 interface ethernet3 gateway 2.2.2.3
set vrouter untrust-vr route 2.2.40.0/24 interface ethernet2 gateway 2.2.10.2
set vrouter untrust-vr route 2.20.0.0/16 interface ethernet2 gateway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

2. trust-vr

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

范例：用于通道接口的路由

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



WebUI

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

Network Address/Netmask: 10.2.2.5/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

CLI

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

将信息流转发到 Null 接口

可以用 Null 接口做为出接口来配置静态路由。因为 Null 接口总被认为是活动的，所以定义到 Null 接口的信息流将被丢弃。要使到 Null 接口的路由成为 “最终”路由，应使用高于其它路由的度量值定义该路由。对于将 Null 接口做为转发信息流的接口的静态路由，有三种应用：

- 防止在其它路由表中进行路由查找

  如果启用基于源接口的路由，则缺省情况下 NetScreen 设备在基于源接口的路由表中执行路由查找。(有关配置基于源接口的路由选择的信息，请参阅第 42 页上的 “基于源接口的路由选择”。) 如果在基于源接口路由表中没有找到相应路由，并且已启用基于源的路由，则 NetScreen 设备在基于源的路由表中执行路由查找。如果在基于源的路由表中没有找到相应路由，则 NetScreen 设备在基于目标的路由表中执行路由查找。如果要防止在基于源的路由表或基于目标的路由表中进行路由查找，则可以将 Null 接口做为出接口，在基于源接口的路由表中创建一个缺省路由。使用高于其它路由的度量值，以确保仅当不存在其它与路由匹配的基于源接口的路由时，才使用此路由。

- 防止在非通道接口上发送通道信息流

  可以使用具有外向通道接口的静态或动态路由，以加密发往指定目的地址的信息流。如果通道接口处于非活动状态，则定义在接口上的所有路由都处于非活动状态。如果在非通道接口上存在备用路由，则发送的信息流将不加密。要防止要加密的信息流在非通道接口上发出，则应以 Null 接口做为出接口，定义一个与通道信息流具有相同目的地址的静态路由。为此接口分配高于通道接口路由的度量值，以确保仅当通道接口路由不可用时，该路由才处于活动状态。当通道接口变为非活动状态时，具有 Null 接口的路由将变为活动状态，并且发往通道目的地址的信息流将被丢弃。

- 防止出现信息流回路

  当 NetScreen 设备通告汇总的路由时，设备可能会接收具有不在其路由表中的前缀的信息流。然后，它可能基于其缺省的路由转发信息流。这样汇总的路由通告就可能导致接收路由器将信息流发回 NetScreen 设备。要避免出现此类回路，可以对汇总路由前缀定义一个静态路由，此静态路由用 Null 接口做为出接口并有较高路由度量值。如果 NetScreen 设备接收的信息流的前缀在其汇总路由通告中，而不是在其路由表中，则信息流将被丢弃。

永久活动路由

在某些情况下，即使与路由关联的物理接口中断或没有被分配的 IP 地址，仍希望路由在路由表中维持其活动状态。例如，无论何时有信息流需要发送到 XAuth 服务器上时，该服务器都会为 NetScreen 设备上的某个接口分配 IP 地址。即使没有任何 IP 地址分配到接口上，通向 XAuth 服务器的路由也需要保持活动状态，从而保证发往 XAuth 服务器的信息流不会被丢弃。

对于在配置 IP 跟踪的接口间保持路由处于活动状态，这也非常有用。如果通过初始接口不能到达目的 IP 地址，则 IP 跟踪允许 NetScreen 设备通过不同的接口重新路由外向信息流。即使 NetScreen 设备将信息流重新路由到另一接口，它仍需要能够在初始接口上发送 ping 请求，以确定目的地址是否又可以到达。

2

虚拟路由器

路由选择是 NetScreen 设备和系统等安全设备的基本部分。如果没有路由选择，安全设备就不能将安全的信息流有效地转发到目的地址位置。可以将 NetScreen 设备配置为只使用静态路由，但网络一旦发生变化，必须手动添加、删除或修改路由表条目。(有关配置静态路由的详细信息，请参阅第 1 页上的 “路由表和静态路由”。) 通过动态路由选择，NetScreen 设备可使用通用协议与路由器及其它网络设备交换路由选择信息，并自动建立及更新路由表。由于动态路由协议使调整自动进行，因此大大缩短了更改网络拓扑结构与调整路由表之间的时间延迟。有关组播路由表的详细信息，请参阅第 196 页上的 “组播路由表”。

本章介绍如何在 NetScreen 设备上配置虚拟路由器 (VR) 以及如何在协议或 VR 之间重新分配路由表条目。本章包括以下部分：

NETSCREEN 设备上的虚拟路由器

ScreenOS 可以将其路由选择组件分成两个或多个虚拟路由器。虚拟路由器 (VR) 支持静态路由协议、动态路由协议和组播路由协议，可以在一个 VR 上同时启用这些协议。 Juniper Networks NetScreen 设备上有两个预定义的 VR:

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

不能删除 trust-vr 或 untrust-vr VR。但是在某些 NetScreen 设备上，可以创建及配置其它 VR (有关创建自定义 VR 的详细信息，请参阅第 25 页上的 “定制虚拟路由器”)。可以为预定义和自定义 VR 配置某些参数 (请参阅第 31 页上的 “修改虚拟路由器”)。

可以存在多个 VR，但是 *trust-vr* 是缺省的 VR。在 VR 表中，星号 (*) 指示 trust-vr 为命令行界面 (CLI) 中的缺省 VR。可以使用 **get vrouter** CLI 命令来查看 VR 表。要在其它的 VR 内配置区段和接口，必须按名称指定 VR，例如 untrust-vr。

使用两个虚拟路由器

通过将路由信息划分给两个虚拟路由器 (VR)，可以控制给定路由选择域中对其它路由选择域可见的信息。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缺省预定义的 VR 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 VR untrust-vr 中。由于一个 VR 的路由表中的信息对于其它 VR 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。

在虚拟路由器间转发信息流

NetScreen 设备上存在两个虚拟路由器 (VR) 时，即使存在允许信息流的策略，也不能在位于不同 VR 的区段之间自动转发信息流。要使信息流能从一个 VR 流向另一个，要确保路由表中存在相应的条目。要进行此操作，可以：

- 在一个 VR 上配置一个静态路由，该路由将另一个 VR 定义为下一跳。此路由甚至可以是该 VR 的缺省路由。例如，可以为 trust-vr 配置一个缺省路由，并将 untrust-vr 作为下一跳。如果出站数据包中的目的地址不与 trust-vr 路由表中的其它任何条目匹配，则将该数据包转发到 untrust-vr。有关配置静态路由的详细信息，请参阅第 1 页上的 “路由表和静态路由”。
- 将一个 VR 的路由表中的路由导出到另一个 VR 的路由表中。可以导出和导入特定路由。还可以将 trust-vr 路由表中的所有路由导出到 untrust-vr 的路由表中。这样可以将 untrust-vr 中收到的数据包转发到 trust-vr 中的目的地址。有关详细信息，请参阅第 60 页上的 “在虚拟路由器之间导出和导入路由”。

配置两个虚拟路由器

如上文所述，可在 NetScreen 设备上配置多个虚拟路由器 (VR)，让每个 VR 维护各自的路由表。在缺省情况下，所有预定义和用户定义的安全区段均绑定到 trust-vr。也就是说，绑定到上述安全区段的所有接口也属于 trust-vr。本节介绍如何将安全区段 (及其接口) 绑定到 untrust-vr VR。

可以将安全区段只绑定到一个 VR 上。当多个安全区段之间不存在地址重叠时，可以将它们绑定到一个 VR。也就是说，这些区段中的所有接口必须处于路由模式。将某一区段绑定到某一 VR 后，该区段中的所有接口都属于该 VR。可以更改安全区段的绑定对象，将绑定到一个虚拟路由器的安全区段重新绑定到另一个虚拟路由器，但必须先删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接口绑定的详细信息，请参阅第 2 卷，“基本原理”中 “接口”一章。)

下面是将安全区段绑定到 untrust-vr VR 的基本步骤：

1. 删除要绑定到 untrust-vr 的区段的所有接口。如果存在分配给该区段的接口，则不能修改从区段到 VR 的绑定。如果已经为接口分配了 IP 地址，则需要先删除分配的地址，然后才能删除该区段的接口。
2. 将区段分配给 untrust-vr VR。
3. 将接口重新分配给区段。

范例 : 将区段绑定到 untrust-vr

在以下范例中，缺省情况下 Untrust 安全区段被绑定到 trust-vr，ethernet3 接口被绑定到 Untrust 安全区段。(Untrust 安全区段没有绑定其它接口。) 必须先将接口 ethernet3 的 IP 地址和网络掩码设置成 0.0.0.0，然后才能更改绑定信息，将 Untrust 安全区段绑定到 untrust-vr。

WebUI

1. 解除接口到 Untrust 区段的绑定

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

   Zone Name: Null

   IP Address/Netmask: 0.0.0.0/0

2. 将 Untrust 区段绑定到 untrust-vr

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

3. 将接口绑定到 Untrust 区段

   Network > Interfaces (ethernet3) > Edit: 从 Zone Name 下拉列表中选择 **Untrust**，然后单击 **OK**。

CLI

1. 解除接口到 Untrust 区段的绑定

```
set interface ethernet3 0.0.0.0/0
unset interface ethernet3 zone
```

2. 将 Untrust 区段绑定到 untrust-vr

```
set zone untrust vr untrust-vr
```

3. 将接口绑定到 Untrust 区段

```
set interface eth3 zone untrust
save
```

在下表中，左侧 **get zone** 的输出内容显示了在缺省情况下接口、区段和虚拟路由器 (VR) 之间的绑定情况。在缺省绑定中， Untrust 区段被绑定到 trust-vr。右侧 **get zone** 的输出内容显示了重新配置绑定信息后，接口、区段和 VR 之间的绑定；此时， Untrust 区段被绑定到 untrust-vr。

Untrust 区段绑定到 trust-vr (缺省绑定)

```
ns-> get zone
Total of 12 zones in vsys root. 7 policy configurable zone(s)
--------------------------------------------------------------------
  ID Name          Type     Attr     VR           Default-IF    VSYS
   0 Null          Null     Shared untrust-vr     null          Root
   1 Untrust       Sec(L3)  Shared trust-vr       ethernet3     Root
   2 Trust         Sec(L3)         trust-vr       ethernet1     Root
   3 DMZ           Sec(L3)         trust-vr       ethernet2     Root
   4 Self          Func            trust-vr       self          Root
   5 MGT           Func            trust-vr       vlan1         Root
   6 HA            Func            trust-vr       null          Root
  10 Global        Sec(L3)         trust-vr       null          Root
  11 V1-Untrust    Sec(L2)         trust-vr       v1-untrust    Root
  12 V1-Trust      Sec(L2)         trust-vr       v1-trust      Root
  13 V1-DMZ        Sec(L2)         trust-vr       v1-dmz        Root
  16 Untrust-Tun Tun               trust-vr       null          Root
```

Untrust 区段绑定到 untrust-vr

```
ns-> get zone
Total of 12 zones in vsys root. 7 policy configurable zone(s)
--------------------------------------------------------------------
  ID Name          Type     Attr     VR           Default-IF    VSYS
   0 Null          Null     Shared untrust-vr     null          Root
   1 Untrust       Sec(L3)  Shared untrust-vr     ethernet3     Root
   2 Trust         Sec(L3)         trust-vr       ethernet1     Root
   3 DMZ           Sec(L3)         trust-vr       ethernet2     Root
   4 Self          Func            trust-vr       self          Root
   5 MGT           Func            trust-vr       vlan1         Root
   6 HA            Func            trust-vr       null          Root
  10 Global        Sec(L3)         trust-vr       null          Root
  11 V1-Untrust    Sec(L2)         trust-vr       v1-untrust    Root
  12 V1-Trust      Sec(L2)         trust-vr       v1-trust      Root
  13 V1-DMZ        Sec(L2)         trust-vr       v1-dmz        Root
  16 Untrust-Tun Tun               trust-vr       null          Root
--------------------------------------------------------------------
```

定制虚拟路由器

某些 NetScreen 设备[1] 允许您除了使用两个预定义的 VR 外，还可以创建定制虚拟路由器 (VR)。可以全面修改用户定义的 VR，包括 VR ID、路由表允许的最大条目数以及特定协议生成的路由的优先级值。

范例：创建定制虚拟路由器

在本例中，将创建一个名为 trust2-vr 的定制 VR，随后将 trust2-vr VR 的路由自动导出到 untrust-vr 中。

WebUI

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

Virtual Router Name: trust2-vr

Auto Export Route to Untrust-VR: (选择)

CLI

```
set vrouter name trust2-vr
set vrouter trust2-vr auto-route-export
save
```

1. 只有某些 NetScreen 设备支持定制 VR。要创建定制 VR，需要有软件许可密钥。

范例：删除定制虚拟路由器

在本例中，您要删除一个名为 trust2-vr 的现有用户定义的虚拟路由器 (VR)。

WebUI

Network > Routing > Virtual Routers: 对于 trust2-vr，单击 **Remove**。

当出现提示，请求您确认删除操作时，单击 **OK**。

CLI

```
unset vrouter trust2-vr
```

当出现提示，请求确认删除操作时 (vrouter unset, are you sure? y/[n])，请输入 **Y**。

```
save
```

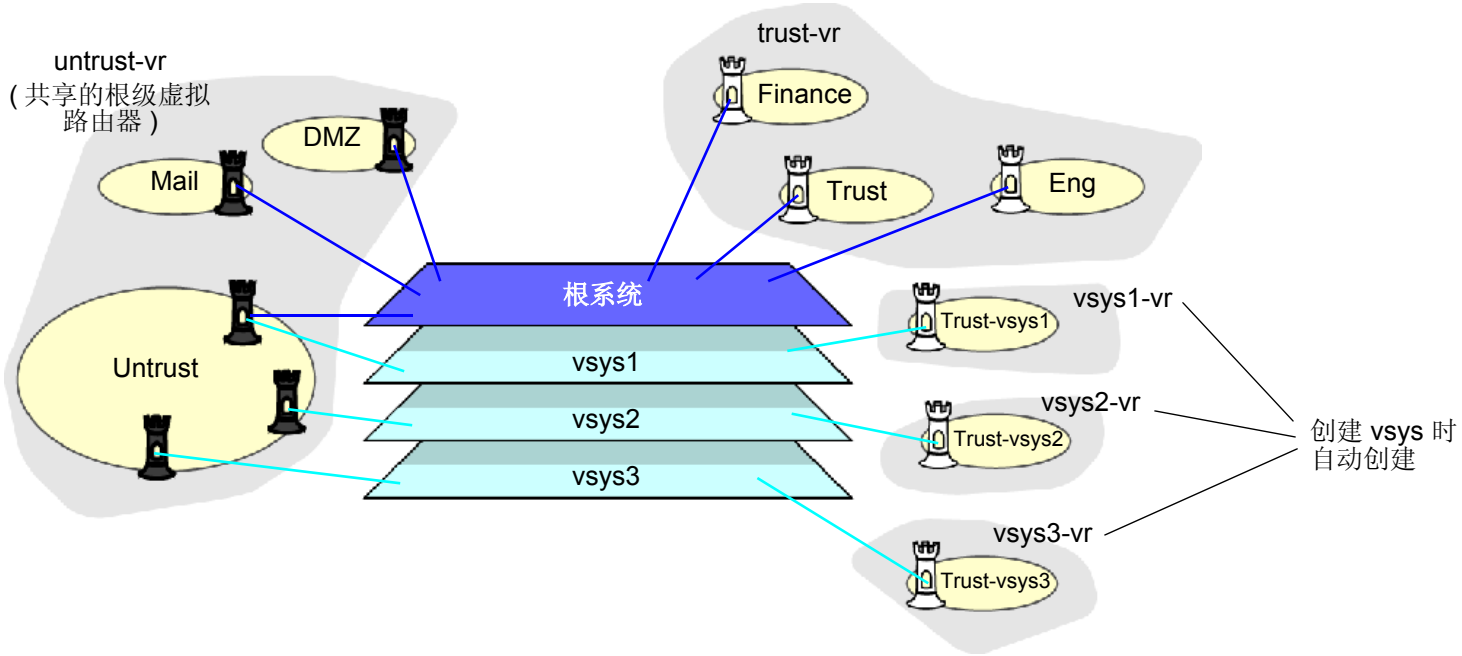
注意：*不能删除预定义的 untrust-vr 和 trust-vr 虚拟路由器 (VR)，但可以删除任何用户定义的 VR。要修改用户定义 VR 的名称或更改 VR ID，必须先删除该 VR，然后用新的名称或 VR ID 重新创建它。*

虚拟路由器和虚拟系统

根级管理员在启用虚拟系统[2] 的系统上创建 vsys 后， vsys 将自动使用以下虚拟路由器 (VR):

- 已定义为共享的任何根级 VR。在缺省情况下， untrust-vr 是一个共享的 VR，可被任何 vsys 访问。还可将其它根级 VR 配置为共享。
- Vsys 级 VR。创建 vsys 后，会自动创建一个 vsys 级 VR，负责维护 Trust-*vsysname* 区段的路由表。可以选择将该 VR 命名为 *vsysname*-vr 或用户定义的名称。 Vsys 级的 VR 不能被其它 vsys 共享。

可以为 vsys 定义一个或多个定制 VR。有关虚拟系统的详细信息，请参阅第 9 卷，“虚拟系统”。在下图中，三个 vsys 各有两个与之相关的 VR: 名为 *vsysname*-vr 的 vsys 级 VR 以及 untrust-vr。



2. 只有 NetScreen 系统 (NetScreen-500、 -5200、 -5400) 支持虚拟系统。要创建 vsys 对象，需要有软件许可密钥。

范例：在 Vsys 中创建虚拟路由器

在本例中，将为 vsys my-vsys1 定义一个定制虚拟路由器 (VR) vr-1a，路由器 ID 为 10.1.1.9。

WebUI

Vsys > Enter (对于 my-vsys1) > Network > Routing > Virtual Routers > New: 输入以下内容，然后单击 **Apply**:

Virtual Router Name: vr-1a

Virtual Router ID: Custom (选择)

在文本框中输入 10.1.1.9

CLI

```
set vsys my-vsys1
(my-vsys1) set vrouter name vr-1a
(my-vsys1/vr-1a) set router-id 10.1.1.9
(my-vsys1/vr-1a) exit
(my-vsys1) exit
```

在以下提示后输入 **Y**:

```
Configuration modified, save? [y]/n
```

在创建 vsys 时创建的 vsys 级 VR 是 vsys 的缺省 VR。可以将 vsys 的缺省 VR 更改为定制 VR。例如，可以将本例中先前创建的定制 VR vr-1a 设置成 vsys my-vsys1 的缺省 VR:

WebUI

Vsys > Enter (对于 my-vsys1) > Network > Routing > Virtual Routers > Edit (对于 vr-1a): 选择 Make This Vrouter Default-Vrouter for the System，然后单击 **Apply**。

CLI

```
set vsys my-vsys1
(my-vsys1) set vrouter vr-1a
(my-vsys1/vr-1a) set default-vrouter
(my-vsys1/vr-1a) exit
(my-vsys1) exit
```

在以下提示后键入 **Y**:

```
Configuration modified, save? [y]/n
```

在缺省情况下，预定义安全区段 Trust-*vsysname* 被绑定到创建 vsys 时创建的 vsys 级 VR。当然，可以将预定义安全区段 Trust-*vsysname* 及任何用户定义的 vsys 级安全区段绑定到可供 vsys 使用的任意 VR 上。

在缺省情况下， untrust-vr 可被所有 vsys 共享。虽然不能共享 vsys 级的 VR，但可以定义任何根级 VR 供 vsys 共享。这样，即可在 vsys 级的 VR 中定义将共享的根级 VR 作为下一跳的路由。还可以在 vsys 级 VR 和共享的根级 VR 之间配置路由的重新分配。

范例：在虚拟路由器间共享路由

在本例中，根级虚拟路由器 (VR) my-router 包含指向网络 4.0.0.0/8 的路由表条目。如果将根级 VR my-router 配置为可由 vsys 共享，则可以在 vsys 级 VR 中定义指向目的地址 4.0.0.0/8 的路由，并将 my-router 作为下一跳。在本例中， vsys 是 my-vsys1， vsys 级 VR 是 my-vsys1-vr。

WebUI

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

Virtual Router Name: my-router

Shared and accessible by other vsys (选择)

Vsys > Enter (对于 my-vsys1) > Network > Routing > Routing Entries > New (对于 my-vsys1-vr): 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 40.0.0.0 255.0.0.0

Next Hop Virtual Router Name: (选择) my-router

CLI

```
set vrouter name my-router sharable
set vsys my-vsys1
(my-vsys1) set vrouter my-vsys1-vr route 40.0.0.0/8 vrouter my-router
(my-vsys1) exit
```

在以下提示后输入 **Y**:

```
Configuration modified, save? [y]/n
```

修改虚拟路由器

可通过 WebUI 或 CLI 修改预定义或定制虚拟路由器 (VR)。例如，修改 trust-vr VR:

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit

CLI

```
set vrouter trust-vr
```

可以修改 VR 的下列参数 :

- 虚拟路由器 ID (有关详细信息，请参阅第 32 页上的 “虚拟路由器 ID”)
- 路由表中允许的最大条目数 (有关详细信息，请参阅第 34 页上的 “最大路由表条目数”)
- 基于协议的路由优先级值 (有关详细信息，请参阅第 35 页上的 “路由优先级”)
- 指示 VR 根据数据包的源 IP 地址转发信息流 (在缺省情况下，VR 根据数据包的目的 IP 地址转发信息流。有关详细信息，请参阅第 38 页上的 “基于源的路由选择”。)
- (仅限于 trust-vr) 对于配置为 “路由”模式的接口，启用或禁用将路由自动导出到 untrust-vr
- (仅限于 trust-vr) 添加一个缺省路由，该路由将另一个虚拟路由器作为下一跳
- (仅限于缺省的根级 VR) 让动态路由选择 MIB 的 SNMP 陷阱变成私有
- 允许考虑通告非活动接口上的路由 (在缺省情况下，只有活动接口上定义的活动路由可重新分配给其它协议或导出到其它 VR。)
- 指示 VR 忽略接口子网地址的重叠 (在缺省情况下，不能为同一 VR 中的接口配置重叠的子网 IP 地址。)
- 允许 VR 与其 NetScreen 冗余协议 (NSRP) 对等方的虚拟路由器的配置保持同步

虚拟路由器 ID

通过动态路由协议，每个路由设备都能使用*唯一的*路由器标识符与其它路由设备进行通信。标识符可以采取点分十进制表示法 (类似于 IP 地址) 或整数值的形式。启用动态路由协议之前如果没有定义特定的虚拟路由器 ID，ScreenOS 会自动选择虚拟路由器 (VR) 中活动接口的最高 IP 地址作为路由器标识符。

在缺省情况下，所有 NetScreen 设备都将 IP 地址 192.168.1.1 分配给 VLAN1 接口。在 NetScreen 设备上启用动态路由协议之前如果没有指定路由器 ID，设备很可能将缺省 IP 地址 192.168.1.1 选择为路由器 ID。由于一个路由域中不能有多个 NetScreen VR 使用同一个 VR ID，因此上述做法可能导致路由选择产生问题。因此， Juniper Networks 建议您始终明确分配 VR ID，该 VR ID 在网络中应是唯一的。可以将 VR ID 设置成回传接口的地址，前提是该回传接口不是 “NetScreen 冗余协议” (NSRP) 集群中的 “虚拟安全接口” (VSI)。 (有关配置 NSRP 集群的详细信息，请参阅第 10 卷，“高可用性”。)

范例 : 分配虚拟路由器 ID

在本例中，将为 trust-vr 分配路由器 ID 0.0.0.10。

注意 : *在 WebUI 中，必须使用点分十进制表示法输入路由器 ID。在 CLI 中，既可使用点分十进制表示法 (0.0.0.10) 输入路由器 ID，也可以只输入 10 (CLI 会将该数字转换成 0.0.0.10)。*

WebUI

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

Virtual Router ID: Custom (选择)

在文本框中输入 0.0.0.10

CLI

```
set vrouter trust-vr router-id 10
save
```

注意 : *如果已在虚拟路由器 (VR) 中启用动态路由协议，则不能分配或更改路由器 ID。如需更改路由器 ID，必须先在 VR 中禁用动态路由协议。有关在 VR 中禁用动态路由协议的信息，请参阅本卷的相应章节。*

最大路由表条目数

每个虚拟路由器 (VR) 都从一个系统范围的池中分配到所需的路由表条目。最大可用条目数取决于 NetScreen 设备[3] 及设备上配置的 VR 的数目。可以限制可为特定 VR 分配的最大路由表条目数。这样有利于防止某 VR 用完系统中的所有条目。

范例：限制路由表条目数

在本例中，将 trust-vr 的最大路由表条目数设置为 20。

WebUI

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

Maximum Route Entry:

Set limit at: (选择), 20

CLI

```
set vrouter trust-vr max-routes 20
save
```

3. 请参阅相关的产品数据页，以决定您的 NetScreen 设备上可以使用的最大路由表条目数。

路由选择

路由表中可以存在多个使用同一前缀 (IP 地址和掩码) 的路由。如果路由表中包含多个指向同一目的地址的路由，设备会比较每个路由器的优先级值。设备会选择优先级值最低的路由。如果优先级值相同，随后会比较度量值。设备会选择度量值最低的路由。[4]

路由优先级

路由优先级是加给路由的权值，它会影响信息流到达目的地址的最佳路径的确定。将路由导入或加入路由表时，虚拟路由器 (VR) 会根据获知该路由的协议为该路由添加一个优先级值。低优先级值 (接近 0 的数) 优先于高优先级值 (远离 0 的数)。

在 VR 中，可根据协议设置路由的优先级值。下表显示了每个协议的路由的缺省优先级值。

协议	缺省优先级
Connected	0
Static	20
Auto-Exported	30
EBGP	40
OSPF	60
RIP	100
Imported	140
OSPF External Type 2	200
IBGP	250

4. 如果存在多个路由指向同一目的地址，且优先级值和度量值均*相同*，设备会从中任选一个路由。在这种情况下，无法确保或预测设备会选择哪个特定路由。

您还可以调整路由优先级值，将信息流沿着首选路径传送。

***注意：**如果某类型路由 (例如， OSPF 类型 1 路由) 的优先级发生了变化，新的优先级将显示在路由表中。但要等到重新获知该路由 (通过先禁用、再启用动态路由协议来实现) 后，新的优先级才能生效，为使静态路由的新优先级生效，必须先删除、再添加静态路由。*

范例：设置路由优先级

在本例中，您将为已被添加到 untrust-vr 的路由表中的任何 “直连[5]” 路由将优先级值指定为 4。

WebUI

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

Route Preference:

Connected: 4

CLI

```
set vrouter untrust-vr preference connected 4
save
```

5. 当路由器的一个接口具有目标网络中的 IP 地址时，就会连接一条路由。

路由度量

路由度量用于确定数据包到达给定目的地址采取的最佳路径。路由器使用路由度量来权衡指向同一目的地址的两个路由，并确定选择使用哪个路由。如果存在多个路由指向同一目标网络，则度量值最小的路由优先。

路由度量可以根据数据包到达目的地址必须经过的路由器数量、路径的相对速度和带宽、该路径总的链路权值的和，也可以将这些因素 (和其它因素) 综合在一起来确定。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。已连接路由的缺省度量值始终为 0。静态路由的缺省度量值为 1，但可以在配置静态路由时指定不同的度量值。

路由表

NetScreen 虚拟路由器 (VR) 支持三种类型的路由表 :

- 基于目标的路由表，它允许 NetScreen 设备基于内向数据包的目的 IP 地址执行路由查找。在缺省情况下，NetScreen 设备仅使用目的 IP 地址来查找转发数据包的最佳路由。
- 基于源的路由表，它允许 NetScreen 设备基于内向数据包的源 IP 地址执行路由查找。要向基于源的路由表添加条目，必须为在其上 NetScreen 设备可以执行路由查找的特定源地址配置静态路由。在缺省情况下禁用此路由表。请参阅下文中的 “基于源的路由选择”。
- 基于源接口的路由选择 (SIBR) 表，它允许 NetScreen 设备基于数据包到达的设备上的接口执行路由查找。要将条目添加到 SIBR 表中，必须为在其上 VR 执行路由查找的特定接口配置静态路由。在缺省情况下禁用此路由表。请参阅第 42 页上的 “基于源接口的路由选择”。

基于目标的路由表总是存在于 VR 中。在 VR 中，可以启用一个基于源或基于源接口的路由表，或两个都启用。

基于源的路由选择

可以引导 NetScreen 设备基于数据包的源 IP 地址而不是目的 IP 地址转发信息流。例如，通过此功能，可以在一条路径上转发特定子网的用户发出的信息流，而在另一条路径上转发另一子网的用户发出的信息流。在虚拟路由器 (VR) 上启用基于源的路由选择后， NetScreen 设备会在基于源的路由表中根据数据包的源 IP 地址执行路由表查找。如果 NetScreen 设备在基于源的路由表中没有找到针对源 IP 地址的路由，那么该设备在基于目标的路由表中使用数据包的目的 IP 地址进行路由查找。

在指定的 VR 上将基于源的路由定义为静态配置的路由。 VR 必须先配置基于源的路由，然后才能应用它们。例如，不能将其它 VR 指定为基于源的路由的下一跳。也不能将基于源的路由重新分配给其它 VR 或路由协议。

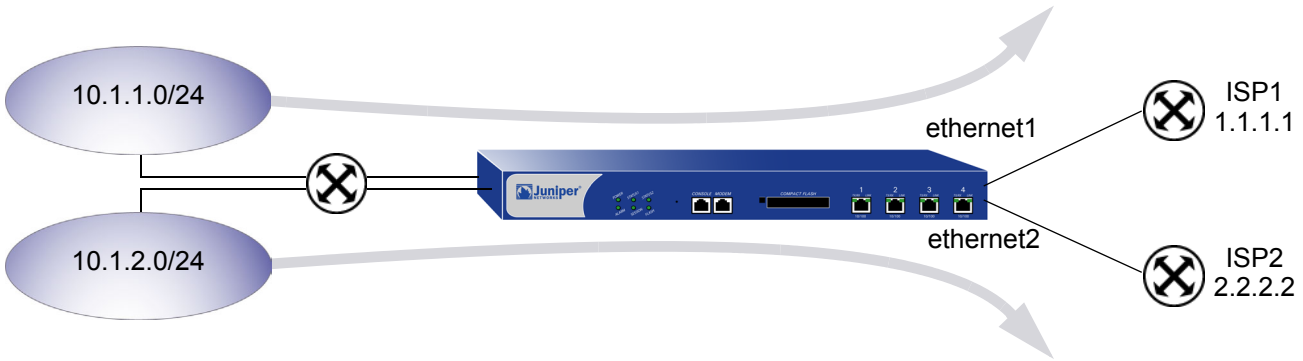
使用此功能 :

1. 通过指定下列信息来创建一个或多个基于源的路由 :
   - 应用基于源的路由选择的 VR 名称
   - NetScreen 设备执行路由表查找依据的源 IP 地址 (此地址作为基于源的路由表中的条目出现。)
   - 转发数据包的出接口的名称
   - 基于源的路由的下一跳 (注意，如果已使用 CLI 命令 **set interface** *interface* **gateway** *ip_addr* 为接口指定了缺省网关，则不必指定网关参数 ; 该接口的缺省网关将被用作基于源的路由的下一跳。不能指定另一个 VR 作为基于源的路由的下一跳。)
   - 基于源的路由的度量值 (如果有多个基于源的路由使用同一前缀，设备只使用度量值最低的路由执行路由查找，并将使用同一前缀的其它路由标上 “inactive” 字样。)
2. 为 VR 启用基于源的路由选择。NetScreen 设备使用数据包的源 IP 在基于源的路由表中进行路由查找。如果找不到与源 IP 地址匹配的路由，将使用目的 IP 地址查找路由表。

范例：基于源的路由选择

在下例中，从 10.1.1.0/24 子网中的用户发出的信息流将被转发到 ISP 1，从 10.1.2.0/24 子网中的用户发出的信息流将被转发到 ISP 2。需要在 trust-vr 虚拟路由器的缺省路由表中配置两个条目，并启用基于源的路由选择：

- 子网 10.1.1.0/24，转发接口为 ethernet3，下一跳为 ISP 1 的路由器 (1.1.1.1)
- 子网 10.1.2.0/24，转发接口为 ethernet4，下一跳为 ISP 2 的路由器 (2.2.2.2)



WebUI

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

Network Address / Netmask: 10.1.1.0 255.255.255.0

Interface: ethernet3 (选择)

Gateway IP Address: 1.1.1.1

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

Network Address/Netmask: 10.1.2.0 255.255.255.0

Interface: ethernet4 (选择)

Gateway IP Address: 2.2.2.2

注意：*在 WebUI 中，缺省优先级和度量值为 1。*

Network > Routing > Virtual Routers > Edit (对于 trust-vr): 选择 **Enable Source Based Routing**，然后单击 **OK**。

CLI

```
set vrouter trust-vr route source 10.1.1.0/24 interface ethernet3 gateway
    1.1.1.1 metric 1
set vrouter trust-vr route source 10.1.2.0/24 interface ethernet4 gateway
    2.2.2.2 metric 1
set vrouter trust-vr source-routing enable
save
```

基于源接口的路由选择

基于源接口路由选择 (称为 “SIBR”) 允许 NetScreen 设备基于源接口 (数据包到达 NetScreen 设备的接口) 转发信息流。在虚拟路由器 (VR) 上启用 SIBR 后， NetScreen 设备会在 SIBR 路由表中执行路由查找。如果 NetScreen 设备在 SIBR 路由表中没有找到针对源接口的路由条目，它可以在基于源的路由表或基于目标的路由表中执行路由查找 (如果在 VR 中启用了基于源的路由选择)。

对于特定的源接口，可以将基于源接口的路由定义为静态路由。将源接口的路由在某个 VR 中进行配置，则该源接口路由只能应用到该 VR 中。例如，不能将其它 VR 指定为基于源接口的路由的下一跳。也不能将基于源接口的路由导出到其它 VR，或将它们重新分配给路由协议。

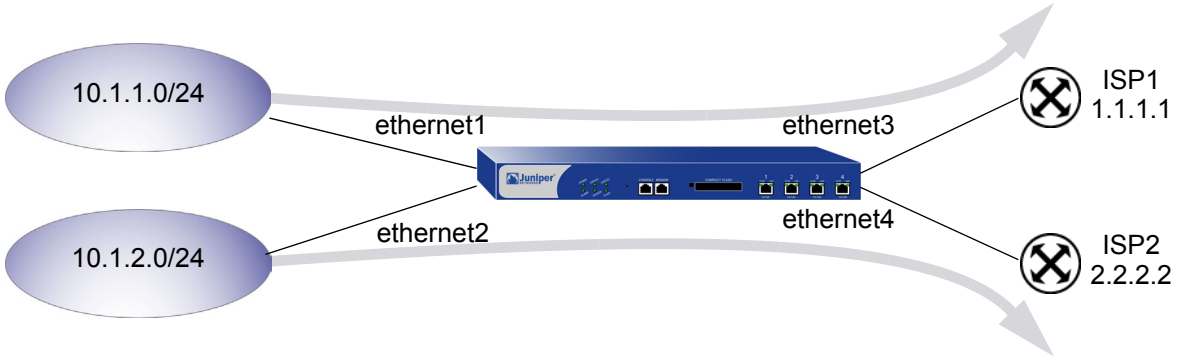
使用此功能 :

1. 通过指定下列信息来创建一个或多个基于源接口的路由 :
   - 应用基于源接口的路由选择的 VR 的名称
   - NetScreen 设备在其上于 SIBR 表中执行查找的源接口 (此接口作为路由表中的条目出现。)
   - 用于路由的 IP 地址和网络掩码前缀
   - 转发数据包的出接口的名称
   - 基于源接口的路由的下一跳 (注意，如果已使用 CLI 命令 **set interface** *interface* **gateway** *ip_addr* 为接口指定了缺省网关，则不必指定网关参数 ; 该接口的缺省网关将被用作基于源接口的路由的下一跳。不能指定另一个 VR 作为基于源接口的路由的下一跳。)
   - 基于源接口的路由的度量值 (如果有多个基于源接口的路由使用同一前缀，设备只使用度量值最低的路由执行路由查找，并将使用同一前缀的其它路由标上 “inactive” 字样。)
2. 为 VR 启用基于源接口的路由选择。 NetScreen 设备使用数据包的源接口在基于源接口的路由表中进行路由查找。

范例：基于源接口的路由选择

在下例中，从 10.1.1.0/24 子网中的用户发出的信息流到达 NetScreen 设备的 ethernet1 接口并被转发到 ISP 1，而从 10.1.2.0/24 子网中的用户发出的信息流到达设备的 ethernet2 接口并被转发到 ISP 2。需要在 trust-vr VR 的缺省路由表中配置两个条目，并启用 SIBR:

- 子网 10.1.1.0/24，源接口为 ethernet1，转发接口为 ethernet3，下一跳为 ISP 1 的路由器 (1.1.1.1)
- 子网 10.1.2.0/24，源接口为 ethernet2，转发接口为 ethernet4，下一跳为 ISP 2 的路由器 (2.2.2.2)



WebUI

Network > Routing > Source Interface Routing > New (对于 ethernet1): 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.1.1.0 255.255.255.0

Interface: ethernet3 (选择)

Gateway IP Address: 1.1.1.1

Network > Routing > Source Interface Routing > New (对于 ethernet2): 输入以下内容，然后单击 **OK**:

Network Address/Netmask: 10.1.2.0 255.255.255.0

Interface: ethernet4 (选择)

Gateway IP Address: 2.2.2.2

***注意：**在 WebUI 中，缺省优先级和度量值为 1。*

Network > Routing > Virtual Routers > Edit (对于 trust-vr): 选择 **Enable Source Interface Based Routing**，然后单击 **OK**。

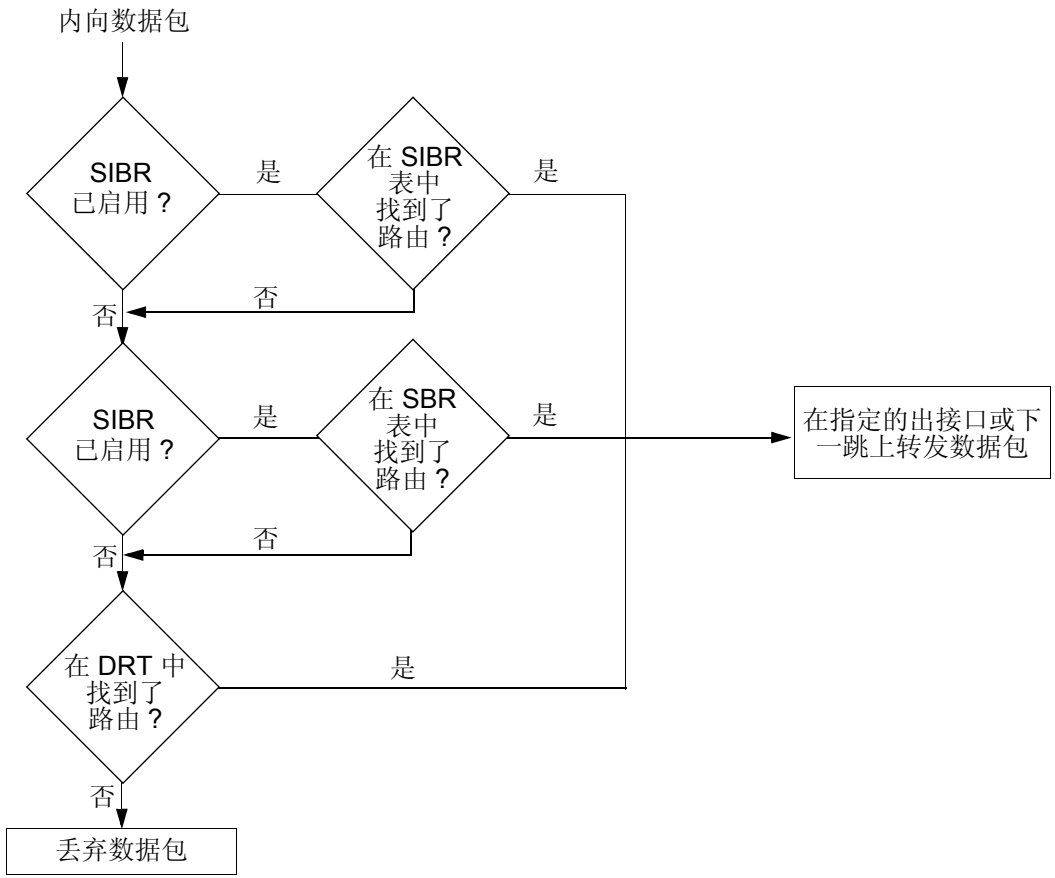
CLI

```
set vrouter trust-vr route source in-interface ethernet1 10.1.1.0/24 interface
    ethernet3 gateway 1.1.1.1 metric 1
set vrouter trust-vr route source in-interface ethernet2 10.1.2.0/24 interface
    ethernet4 gateway 2.2.2.2 metric 1
set vrouter trust-vr sibr-routing enable
save
```

路由查找顺序

如果在虚拟路由器 (VR) 中启用了基于源的路由和 SIBR，则 VR 通过以特定的顺序对照路由表检查内向数据包来执行路由查找。本节介绍缺省路由查找顺序，以及通过为每个路由表配置优先级值来更改此顺序的方法。

请参阅第 **2**-12 页上的“数据包流序列”。如果一个内向数据包与现有会话不匹配， NetScreen 设备会执行“首包处理”，该过程包括路由查找。下图显示了缺省的路由查找顺序。



1. 如果在 VR 中启用了 SIBR，则 NetScreen 设备首先在 SIBR 路由表中检查是否有与数据包到达的接口相匹配的路由条目。如果 NetScreen 设备在 SIBR 路由表中找到了针对源接口的路由条目，则它按照此匹配的路由选择条目的指定转发数据包。如果 NetScreen 设备在 SIBR 路由表中没有找到针对源 IP 地址的路由条目，则该设备将查看 VR 中基于源的路由 (SBR) 是否启用。

2. 如果在 VR 中启用了 SBR，则 NetScreen 设备在 SBR 路由表中检查是否有与数据包的源 IP 地址相匹配的路由条目。如果 NetScreen 设备找到了针对源 IP 地址的匹配路由条目，它将按照此条目的指定转发数据包。如果 NetScreen 设备在 SBR 路由表中没有找到针对源 IP 地址的路由条目，则该设备检查基于目标的路由表 (DRT)。
3. NetScreen 设备在基于目标的路由表中检查是否有与数据包的目的 IP 地址相匹配的路由条目。如果 NetScreen 设备找到了针对目的 IP 地址的匹配路由条目，它将按照此条目的指定转发数据包。如果设备没有找到与目的 IP 地址准确匹配的路由条目，但存在为 VR 配置的缺省路由，则设备将按照该缺省路由的指定转发数据包。如果 NetScreen 设备没有找到针对目的 IP 地址的路由条目，并且不存在为 VR 配置的缺省路由，则丢弃该数据包。

NetScreen 设备检查路由表是否有匹配的路由的顺序，由分配给每个路由表的优先级值来确定。设置首先检查有最高优先级值的路由表，最后检查有最低优先级值的路由表。缺省情况下， SIBR 路由表有最高的优先级值 (3)， SBR 有次高的优先级值 (2)，基于目标的路由表有最低的优先级值 (1)。

可以对路由表重新分配新的优先级值，以更改 NetScreen 设备在 VR 中执行路由查找的顺序。请记住，设备按从最高优先级值到最低优先级值的顺序检查路由表。

范例：更改路由查找顺序

在下例中，将在 trust-vr 中启用 SIBR 和基于源的路由选择。您需要 NetScreen 设备按下列顺序在路由表中执行路由查找：首先是基于源的路由选择，其次是 SIBR，然后是基于目标的路由选择。要配置此路由表查找的顺序，需要用高于 SIBR 的优先级值来配置基于源的路由选择 — 本例中，将优先值 4 分配给基于源的路由。

WebUI

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

Route Lookup Preference (1-255): (选择)

For Source Based Routing: 4

Enable Source Based Routing: (选择)

Enable Source Interface Based Routing: (选择)

CLI

```
set vrouter trust-vr sibr-routing enable
set vrouter trust-vr source-routing enable
set vrouter trust-vr route-lookup preference source-routing 4
save
```

在多个虚拟路由器中的路由查找

可以只为基于目标的路由条目，而不为基于源或基于源接口的路由条目指定其它的虚拟路由器 (VR) 作为下一跳。例如，基于目标的路由表中的缺省路由可以指定 untrust-vr 作为下一跳。如果一个 VR 中的路由查找会导致另一 VR 中的路由查找， NetScreen 设备总是在基于目标的路由表中执行第二个路由查找。下例说明了此行为。

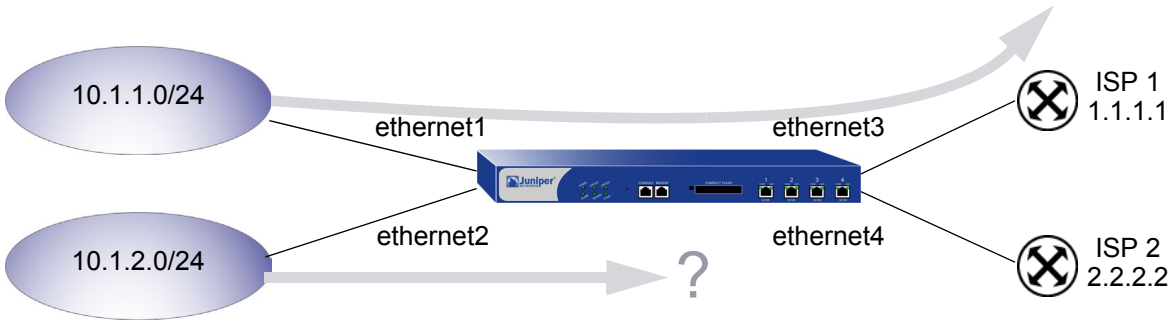
在下例中，将在 trust-vr 和 untrust-vr 路由表中都启用基于源的路由选择。 trust-vr 有下列路由选择条目：

- 针对子网 10.1.1.0/24 的基于源的路由选择条目，转发接口为 ethernet3，下一跳为路由器 1.1.1.1
- 缺省路由，下一跳为 untrust-vr

untrust-vr 有下列路由选择条目：

- 针对子网 10.1.2.0/24 的基于源的路由选择条目，转发接口为 ethernet4，下一跳为路由器 2.2.2.2
- 默认路由，转发接口为 ethernet3，下一跳为路由器 1.1.1.1

子网 10.1.2.0/24 发出的信息流总是在 ethernet3 上被转发到路由器 1.1.1.1，如下图所示。



Trust-VR
基于源的路由表

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	1	10.1.1.0/24	eth3	2.2.2.250	S	20	1	Root

基于目标的路由表

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	1	0.0.0.0/24	n/a	untrust-vr	S	20	0	Root

从子网 10.1.2.0/24 发出的信息流到达 NetScreen 设备的 ethernet2。因为不存在匹配的基于源的路由条目，所以 NetScreen 设备在基于目标的路由表中执行路由查找。基于目标的路由表中的缺省路由指定 untrust-vr 作为下一跳。

Untrust-VR
基于源的路由表

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	1	10.1.2.0/24	eth4	2.2.2.250	S	20	1	Root

基于目标的路由表

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	1	0.0.0.0/24	eth3	1.1.1.150	S	20	0	Root

在 untrust-vr 中， NetScreen 设备只在基于目标的路由表中执行路由查找，即使 untrust-vr 中的基于源的路由表包含与信息流匹配的条目。请注意，基于目标的路由表中的匹配路由 (缺省路由) 在接口 ethernet3 上转发信息流。

等值路由

NetScreen 设备在每会话基础上支持等开销多路径 (ECMP) 路由。等开销的路由具有相同的优先级和度量值。NetScreen 设备将某个会话与某个路由相关联后，NetScreen 设备就使用该路由，直到获知了更好的路由或当前的路由不可用为止。符合条件的路由必须有属于同一区段的出接口。

***注意：**如果出接口不属于同一区段，并且返回的数据包被转到了一个非预期的区段，则不能发生会话匹配，并且信息流不能通过。*

ECMP 帮助实现对相同目的地址的两个到四个路由中的负载均衡，或在两个或更多目的地址中增加有效的带宽使用。当 ECMP 启用时， NetScreen 设备将通过路由协议使用到相同目的地址的静态定义的路由或动态获知的多个路由。NetScreen 设备以轮询方式使用等值路由。 ECMP 与只创建一个会话的应用程序配合使用效果最好，例如 Telnet 和 SSH。如果出接口不同并处于 NAT 模式，那么由于每个会话携带不同转换的源 IP 地址，所以创建多个会话的应用程序 (如 HTTP) 不能正常工作。

如果没有 ECMP，则 NetScreen 设备只使用首先学到的或事先定义好的路由。其它等开销的路由保持不使用，直到当前活动的路由不再活动为止。

注意：**当使用 ECMP 时，如果有两台 NetScreen 设备具有邻接关系，并且发现有数据包损失以及负载均衡不正常，请检查邻接设备的“地址解析协议”(ARP) 配置，以确保* ***arp always-on-dest *功能已禁用 (缺省)。有关与 ARP 相关的命令的详细信息，请参阅“基本原理”卷中的第* ***2*** *-95 页上的“非活动接口和信息流”。*

例如，考虑出现在 trust-vr 的基于目标的路由表中的下列两个路由 :

```
     ID          IP-Prefix       Interface          Gateway    P Pref     Mtr      Vsys
*    8           0.0.0.0/0       ethernet3        1.1.1.250    C    0       1      Root
     9           0.0.0.0/0       ethernet2        2.2.2.250    S   20       1      Root
```

本例中，存在两个缺省路由来提供到两个不同的 ISP 的连接，目的是结合 ECMP 使用两个缺省路由。

这两个路由有相同的度量值，但第一个路由是一个已连接的路由 (C 具有优先级 0)。 NetScreen 设备通过 DHCP 或 PPP 获取第一个路由，并且此设备通过手动配置获取缺省路由。第二个路由是手动配置的静态路由 (S 具有自动优先级 20)。禁用 ECMP 后， NetScreen 设备在 ethernet3 上将所有信息流转发到已连接的路由。

要实现这两个路由的负载均衡，可将静态路由的路由优先级更改为零 (0) 来匹配已连接的路由，方法是输入命令 **set vrouter** *trust-vr* **preference static 0**，然后启用 ECMP。启用 ECMP 后， NetScreen 设备负载通过在两个符合条件的 ECMP 路由之间进行选择来实现均衡。以下显示了更新后的路由表。

```
   ID          IP-Prefix       Interface          Gateway    P Pref     Mtr      Vsys
*   8         0.0.0.0/0        ethernet3        1.1.1.250     C    0       1      Root
*   9         0.0.0.0/0        ethernet2        2.2.2.250     S    0       1      Root
```

如果启用了 ECMP，并且 NetScreen 设备在路由表中找到了多个等开销的匹配路由，则此设备为每个路由查找选择一个不同的等开销路由。按照以上显示的路由， NetScreen 设备在 ethernet3 和 ethernet2 之间进行选择以将信息流转发到网络 0.0.0.0/0。

如果对该网络的等开销路由多于两个，则 NetScreen 设备按轮换 (轮询) 顺序选择路由，一直达到配置的最大数，以便设备为每个路由查找选择不同的 ECMP 路由。

启用等值路由

缺省情况下禁用 ECMP (最大路由数 = 1)。要启用 ECMP 路由选择，需要基于每个虚拟路由器指定等开销路由的最大数量。最多可以指定四个路由。设置路由的最大数量后，即使获知了更多的路由， NetScreen 设备也不会添加或更改路由。

范例 : 配置 ECMP 路由的最大数

在下例中，将 trust-vr 的 ECMP 路由的最大数设置为两个。即使在相同区段内及在路由表中可能存在三个或四个等开销路由， NetScreen 设备也只在配置的符合条件的路由数之间进行选择。在此情况下，数据只沿着两条指定的 ECMP 路径转发。

WebUI

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

Maximum ECMP Routes:

Set Limit at: (选择), 2

CLI

```
set vrouter trust-vr max-ecmp-routes 2
save
```

路由重新分配

虚拟路由器 (VR) 中的路由表包含以下路由：VR 中运行的所有动态路由协议收集的路由、静态路由以及直接连接的路由。在缺省情况下，动态路由协议 (如 OSPF、 RIP 或 BGP) 只将满足以下条件的路由通告给其邻居或对等方：

- 路由表中的活动路由。
- 通过动态路由协议获知的路由[6]。

为使动态路由协议能够通告其它协议获知的路由 (含静态配置的路由)，需要将源协议获知的路由*重新分配*给通告协议。

可以将某路由协议获知的路由 (含静态配置的路由) 重新分配给同一 VR 中的不同路由协议。这样，接收方路由协议就有能力通告重新分配的路由。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，如果某路由域使用 OSPF 协议且连接到一个使用 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 OSPF 邻居如何到达 BGP 域中的设备。

设备根据系统或网络管理员定义的*重新分配规则*[7]，在协议之间重新分配路由。将路由添加到 VR 的路由表时，设备会逐一应用 VR 中定义的所有重新分配规则，决定是否重新分配该路由。从路由表中删除路由时，设备会逐一应用 VR 中定义的所有重新分配规则，决定是否将该路由从 VR 的其它路由协议中删除。注意，添加或删除路由时，将应用所有的重新分配规则。在重新分配规则中，不存在规则顺序或 “最先匹配规则” 的概念。

在 NetScreen 设备上，可以配置*路由映射*，指定要重新分配的路由以及重新分配的路由的属性。

6. OSPF、 RIP 和 BGP 还会通告启用这些协议的 ScreenOS 接口的连接路由。
7. 在任意两个协议之间，只能定义一条重新分配规则。

配置路由映射

*路由映射*由一组语句构成，设备按先后顺序在路由上应用这些语句。路由映射中的每条语句定义了一个作为该路由比较依据的条件。设备将指定的路由映射中每个语句按序列号递增的顺序与路由加以比较，直到找到匹配的语句，随后将应用该语句指定的操作。如果路由与路由映射语句中的条件匹配，该路由不是允许就是被拒绝。路由映射语句还能修改匹配路由的特定属性。每次比较到路由映射结尾，都意味着隐式的拒绝；换言之，如果某路由不与任何路由映射条目匹配，则该路由被拒绝。

下面是可在路由映射语句中配置的匹配条件：

匹配条件	说明
BGP AS Path	用于匹配指定的 AS 路径访问列表。请参阅第 56 页上的 “路由过滤”。
BGP Community	用于匹配指定的 Community 属性列表。请参阅第 56 页上的 “路由过滤”。
OSPF route type	用于匹配 OSPF 内部类型 1、外部类型 1 或外部类型 2 其中之一。
Interface	用于匹配指定接口。
IP address	用于匹配指定的访问列表。请参阅第 56 页上的 “路由过滤”。
Metric	用于匹配指定的路由度量值。
Next-hop	用于匹配指定的访问列表。请参阅第 56 页上的 “路由过滤”。
Tag	用于匹配指定的路由标记值或 IP 地址。

对于每个匹配条件，可以指定接受 (允许) 还是拒绝 (不允许) 与该条件匹配的路由。如果某路由与条件匹配且被允许，则可选择性地设置该路由的属性值。可以在路由映射语句中设置以下属性 :

设置属性	说明
BGP AS Path	将匹配路由的路径列表属性预先设置成指定的 AS 路径访问列表。
BGP Community	将匹配路由的公共组属性设置到指定的公共组列表。
BGP local preference	将匹配路由的 local-pref 属性设置成指定值。
BGP weight	设置匹配路由的权值。
Offset metric	按指定的数字递增匹配路由的度量。这会在期望值较低的路径上增加度量。对于 RIP 路由，可以将此递增应用到通告的路由 (路由映射流出) 或获知的路由 (路由映射流入)。对于其它路由，可以将此递增应用到被导出到其它虚拟路由器 (VR) 的路由。
OSPF metric type	将匹配路由的 OSPF 度量类型设置成外部类型 1 或外部类型 2。
Metric	将匹配路由的度量设置成指定值。
Next-hop of route	将匹配路由的下一跳设置成指定 IP 地址。
Preserve metric	保护被导出到其它 VR 中的匹配路由的度量。
Preserve preference	保护被导出到其它 VR 中的匹配路由的优先级值。
Tag	将匹配路由的标记设置成指定标记值或 IP 地址。

路由过滤

通过过滤路由，可以控制允许哪些路由进入虚拟路由器 (VR)、将哪些路由通告给对等方以及将哪些路由从一个路由协议重新分配给另一个路由协议。可以对两类路由应用过滤器：从路由选择对等方发出的内向路由；从 NetScreen VR 发出、指向对等路由器的外向路由。可使用以下过滤机制：

- 访问列表 — 访问列表是一组指定的 IP 地址前缀。使用访问列表，可以根据网络前缀过滤路由。有关配置访问列表的信息，请参阅访问列表。
- BGP AS 路径访问列表 — AS 路径属性是传送路由通告时经过的自治系统的列表，该列表是路由信息的一部分。 AS 路径访问列表是代表特定 AS 的一组规则表达式。使用 AS 路径访问列表，可根据路由经过的 AS 对路由进行过滤。有关配置 AS 路径访问列表的信息，请参阅第 174 页上的 “AS 路径访问列表”。
- BGP 公共组列表 — 公共组属性，包含 BGP 路由所属公共组的标识符。 BGP 公共组列表是一组 BGP 公共组，用于根据路由所属的公共组对路由进行过滤。有关配置 BGP 公共组列表的信息，请参阅第 186 页上的 “BGP 公共组”。

访问列表

访问列表是有先后顺序的语句列表，其语句用作路由的比较依据。每条语句指定网络前缀的 IP 地址 / 网络掩码以及转发状态 (允许或拒绝路由)。例如，访问列表中的一条语句可以允许子网 1.1.1.0/24 的路由。同一访问列表中的另一条语句可以拒绝子网 2.2.2.0/24 的路由。如果路由与访问列表中的语句匹配，则会应用指定的转发状态。

注意，路由先与访问列表中的第一条语句加以比较，接着比较下一条，直到找到匹配的语句。因此，访问列表中的语句顺序非常重要。如果存在匹配语句，访问列表中的所有后续语句都将被忽略。因此，应将较明确的语句置于不太明确的语句之前。例如，将拒绝 1.1.1.1/30 子网的路由的语句放在允许 1.1.1.0/24 子网的路由的语句之前。

也可以使用访问列表来控制组播信息流的流动。有关信息，请参阅第 199 页上的 “访问列表”。

范例 : 配置访问列表

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 :

- Identifier: 2 (配置访问列表时，必须指定访问列表标识符)
- Forwarding Status: 允许
- IP Address / Netmask Filtering: 1.1.1.1/24
- Sequence Number: 10 (访问列表中该语句相对其它语句的位置)

WebUI

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

Access List ID: 2

Sequence No: 10

IP/Netmask: 1.1.1.1/24

Action: Permit

CLI

```
set vrouter trust-vr access-list 2 permit ip 1.1.1.1/24 10
save
```

范例：将路由重新分配到 OSPF

在本例中，将重新分配已通过自治系统 65000 进入 OSPF 的指定 BGP 路由。首先配置 AS 路径访问列表，允许已经过 AS 65000 的路由。（有关配置 AS 路径访问列表的详细信息，请参阅第 174 页上的 “AS 路径访问列表”。）然后，将配置路由映射 “rtmap1”，以便匹配 AS 路径访问列表中的路由。最后，在 OSPF 中指定使用路由映射 “rtmap1” 的重新分配规则，并将 BGP 指定为路由的源协议。

WebUI

1. BGP AS 路径访问列表

   Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > AS Path: 输入以下内容，然后单击 **Add**:

   AS Path Access List ID: 1

   Permit: (选择)

   AS Path String: _65000_

2. 路由映射

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

   Map Name: rtmap1

   Sequence No.: 10

   Action: permit (选择)

   Match Properties:

   AS Path: (选择), 1

3. 重新分配规则

Network > Routing > Virtual Router > Edit (对于 trust-vr) > Edit OSPF Instance > Redistributable Rules: 选择以下内容，然后单击 **Add**:

Route Map: rtmap1

Protocol: BGP

CLI

1. BGP AS 路径访问列表

```
set vrouter trust-vr protocol bgp as-path-access-list 1 permit _65000_
```

2. 路由映射

```
set vrouter trust-vr
ns(trust-vr)-> set route-map name rtmap1 permit 10
ns(trust-vr/rtmap1-10)-> set match as-path 1
ns(trust-vr/rtmap1-10)-> exit
ns(trust-vr)-> exit
```

3. 重新分配规则

```
set vrouter trust-vr protocol ospf redistribute route-map rtmap1 protocol bgp
save
```

在虚拟路由器之间导出和导入路由

如果在 NetScreen 设备上配置了两个虚拟路由器 (VR)，则可以允许一个 VR 获知另一个 VR 上的指定路由。要进行此操作，必须在要将路由导出到目标 VR 中的源 VR 上定义*导出规则*。导出路由时， VR 允许其它 VR 获知其网络。在目标 VR 上，可根据需要配置*导入规则*，以控制允许从源 VR 导入的路由。如果目标 VR 上没有导入规则，它会接受导出的全部路由。

在 VR 之间导出和导入路由：

1. 在源 VR 上，定义导出规则。
2. (可选) 在目标 VR 上，定义导入规则。虽然此步骤为可选步骤，但是通过导入规则，可以进一步控制目标 VR 从源 VR 接受的路由。

在 NetScreen 设备上，可通过指定以下信息配置导出或导入规则：

- 目标 VR (对于导出规则) 或源 VR (对于导入规则)
- 导出 / 导入的路由的协议
- 导出 / 导入哪些路由
- (可选) 导出 / 导入的路由的新属性或已修改的属性

配置导出或导入规则与配置重新分配规则类似。可以配置*路由映射*，指定要导出 / 导入的路由以及这些路由的属性。

可配置 trust-vr 将所有路由表条目自动导出到 untrust-vr 中。还可以配置一个用户定义的 VR，以自动向其它 VR 导出路由。不能导出网络中与 NAT 模式的接口直接相连的路由。

范例：配置导出规则

在本例中， trust-vr 中指向网络 1.1.1.1/24 的 OSPF 路由将被导出到 untrust-vr 路由选择域中。首先要为网络前缀 1.1.1.1/24 创建一个访问列表，随后将在路由映射 “rtmap1” 中使用该列表，以过滤指向网络 1.1.1.1/24 的匹配路由。随后，还要创建路由导出规则，将 trust-vr 中匹配的 OSPF 路由导出到 untrust-vr 中。

WebUI

trust-vr

1. 访问列表

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

   Access List ID: 2

   Sequence No: 10

   IP/Netmask: 1.1.1.1/24

   Action: Permit

2. 路由映射

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

   Map Name: rtmap1

   Sequence No.: 10

   Action: permit (选择)

   Match Properties:

   Access List: (选择), 2

3. 导出规则

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

Destination Virtual Router: untrust-vr

Route Map: rtmap1

Protocol: OSPF

CLI

trust-vr

1. 访问列表

```
set vrouter trust-vr
ns(trust-vr)-> set access-list 2 permit ip 1.1.1.1/24 10
```

2. 路由映射

```
ns(trust-vr)-> set route-map name rtmap1 permit 10
ns(trust-vr/rtmap1-10)-> set match ip 2
ns(trust-vr/rtmap1-10)-> exit
```

3. 导出规则

```
ns(trust-vr)-> set export-to vrouter untrust-vr route-map rtmap1 protocol ospf
ns(trust-vr)-> exit
save
```

范例：配置自动导出

可以配置 trust-vr，将其所有路由自动导出到 untrust-vr 中。但是，这并不一定表示 untrust-vr 会导入 trust-vr 导出的所有路由。如果为 untrust-vr 定义了导入规则，则只导入符合导入规则的路由。在本例中， trust-vr 自动将所有路由导出到 untrust-vr 中，但 untrust-vr 上的导入规则只允许导入内部 OSPF 路由。

WebUI

trust-vr

Network > Routing > Virtual Router > Edit (对于 trust-vr): 选择 **Auto Export Route to Untrust-VR**，然后单击 **OK**。

untrust-vr

Network > Routing > Virtual Router > Route Map (对于 untrust-vr) > New: 输入以下内容，然后单击 **OK**:

Map Name: from-ospf-trust

Sequence No.: 10

Action: permit (选择)

Route Type: internal-ospf (选择)

CLI

trust-vr

```
set vrouter trust-vr auto-route-export
```

untrust-vr

```
set vrouter untrust-vr
ns(untrust-vr)-> set route-map name from-ospf-trust permit 10
ns(untrust-vr/from-ospf-trust-10)-> set match route-type internal-ospf
ns(untrust-vr/from-ospf-trust-10)-> exit
ns(untrust-vr)-> set import-from vrouter trust-vr route-map from-ospf-trust
    protocol ospf
ns(untrust-vr)-> exit
save
```

3

开放式最短路径优先 (OSPF)

本章介绍 NetScreen 设备上的 “开放式最短路径优先” (OSPF) 路由协议。其中包括以下主题：

OSPF 概述

“开放式最短路径优先”(OSPF) 路由协议是专门在单个“自治系统”(AS) 内运行的“内部网关协议”(IGP)。运行 OSPF 的路由器通过在整个 AS 内定期发布*链接状态通告* (LSA)，来发布其状态信息 (例如，可用接口和邻居可到达性)。

每个 OSPF 路由器都使用邻接路由器发出的 LSA 来维护*链接状态数据库*。链接状态数据库是周围网络的拓扑结构和状态信息的列表。遍及整个路由选择域的 LSA 持续发布使得 AS 内的所有路由器都维护相同的链接状态数据库。

OSPF 使用链接状态数据库来确定到达 AS 中任意网络的最佳路径。这通过生成*最短路径树*完成，最短路径树是到达 AS 中任意网络的最短路径的图形化表示。虽然所有路由器都具有相同的链接状态数据库，但它们都具有唯一的最短路径树，因为路由器在生成该树时，始终将其自身置于树的顶端。

区域

在缺省情况下，所有路由器均被分组到名为 area 0 (通常表示为 area 0.0.0.0) 的单个 “中枢”区域中。但是地理上分布较广的网络通常会被分割成多个区域。随着网络的扩展，链接状态数据库也会不断增大，将链接状态数据库分隔成多个较小的组可使其更易扩展。

区域可以减少网络内流通的路由选择信息量，因为路由器只维护其所在区域的链接状态数据库。而不维护该区域外的网络或路由器的链接状态信息。连接到多个区域的路由器负责维护所连接的每个区域的链接状态数据库。所有区域都必须直接与 area 0 相连，只有一种例外情况 (随后将对其进行介绍)。

AS 外部通告对指向其它 AS 中目的地址的路由进行描述，这些外部通告遍及整个 AS。可以将某些 OSPF 区域配置为*剩余区域*; AS 外部通告不会遍及这些区域。 OSPF 中使用两类常见的区域 :

- **Stub 区域** - 这样一个区域 : 对于通过非 OSPF 源 (例如 BGP) 获知的路由，它从中枢区域接收路由汇总，而不从其它区域接收链接状态通告。如果剩余区域中不允许汇总路由，可将其视为*完全剩余区域*。
- **Not So Stubby 区域 (NSSA)** - 与常规剩余区域相同， NSSA 不能从当前区域之外的非 OSPF 源接收路由。但是，仍可获知区域内所获知的外部路由，并可将其传送到其它区域。

路由器分类

依据参与 OSPF 路由的路由器在网络中的功能或位置对其进行分类 :

- **内部路由器** - 所有接口均属于同一区域的路由器。
- **中枢路由器** - 有一个接口位于中枢区域内的路由器。
- **区域边界路由器** - 与多个区域相连的路由器称为区域边界路由器 (ABR)。 ABR 汇总来自非中枢区域的路由，以便将其发布到中枢区域。在缺省情况下，运行 OSPF 的 NetScreen 设备上将创建一个中枢区域。如果您在虚拟路由器上又创建了一个区域，则该设备将充当 ABR。
- **AS 边界路由器** - 当某个 OSPF 区域与另一 AS 相接时，这两个自治系统间的路由器被称为自治系统边界路由器 (ASBR)。 ASBR 负责在 AS 内通告外部 AS 路由选择信息。

Hello 协议

接口位于同一子网中的两个路由器称为*邻居*。路由器使用 Hello 协议建立并维护此邻接关系。当两个路由器建立双向通信时，即认为其已建立*邻接关系*。如果两个路由器之间未建立邻接关系，则它们将无法交换路由选择信息。

如果某个网络上具有多个路由器，则必须将其中的一个路由器作为*指定路由器* (DR)，而将另外一个路由器作为*备份指定路由器* (BDR)。 DR 负责将 LSA 大量发向网络， LSA 中包含一个列表，列出了所有连接到网络且启用了 OSPF 的路由器。 DR 是唯一能与网络中的其它路由器构成邻接关系的路由器。因此， DR 是网络上唯一能为其它路由器提供路由选择信息的路由器。如果 DR 出现故障， BDR 将成为指定路由器。

网络类型

NetScreen 设备支持以下 OSPF 网络类型：

- 广播网络
- 点对点网络
- 点对多点网络

广播网络

*广播网络*是连接多个路由器的网络，它可将单个物理消息发送或广播到所有相连的路由器。假定广播网络上的路由器对之间可相互通信。以太网即为广播网络的一个范例。

在广播网络上， OSPF 路由器将 hello 数据包发送到组播地址 224.0.0.5，动态检测其邻接路由器。对于广播网络，Hello 协议负责为网络选定 “指定路由器” 和 “备份指定路由器”。

*非广播网络*是虽连接了多个路由器，但却不能将消息广播到各个相连路由器的网络。在非广播网络上，需要将以往组播的 OSPF 协议数据包发送到每一个邻接路由器。NetScreen 设备不支持非广播网络中的 OSPF。

点对点网络

*点对点*网络一般通过 “广域网” (WAN) 连接两个路由器。两台通过 IPSec VPN 通道相连的 NetScreen 设备即为一个点对点网络。在点对点网络上， OSPF 路由器将 hello 数据包发送到组播地址 224.0.0.5，动态检测邻接路由器。

点对多点网络

*点对多点*网络是一种非广播网络，在该网络中，OSPF 将路由器间的连接视为点对点链接。无需为该网络选择指定路由器或大量发送 LSA。点对多点网络中的路由器将 hello 数据包发送到可与之直接通信的所有邻居。

***注意：**在 NetScreen 设备上，仅在通道接口上支持 OSPF 点对多点配置，必须禁用路由拒绝以使网络正常运行。不能在物理以太网接口上配置点对多点连接。有关详细信息，请参阅第 103 页上的 “点对多点通道接口”。*

链接状态通告

每个 OSPF 路由器都将向外发送定义路由器本地状态信息的 LSA。另外，路由器还可向外发送其它类型的 LSA，这取决于路由器的 OSPF 功能。下表对 LSA 类型进行了归纳：

LSA 类型	发送者	发送范围	LSA 中发送的信息
路由器 LSA	所有 OSPF 路由器	区域	描述整个区域内所有路由器接口的状态。
网络 LSA	广播网络和 NBMA 网络上的 “指定路由器”	区域	包含与网络相连的所有路由器的列表。
汇总 LSA	区域边界路由器	区域	描述可到达位于区域外但仍处于 AS 内的某一目的地址的路由。有两种类型： 类型 3 汇总 LSA 描述到达网络的路由。 类型 4 汇总 LSA 描述到达 AS 边界路由器的路由。
AS 外部	自治系统边界路由器	自治系统	指向另一 AS 中的网络的路由。通常为缺省路由 (0.0.0.0/0)。

基本 OSPF 配置

可在 NetScreen 设备上为每个虚拟路由器创建 OSPF。如果系统中存在多个虚拟路由器 (VR)，则可启用多个 OSPF 实例，每个实例代表一个 VR。

***注意：**在 NetScreen 设备上配置动态路由协议之前，应先分配 VR ID，如第 2 章，“虚拟路由器”中所述。*

本节介绍在 NetScreen 设备上的 VR 中配置 OSPF 的基本步骤：

1. 在 VR 中创建并启用 OSPF 路由选择实例。此步骤还会自动创建一个 OSPF 中枢区域 (区域 ID 为 0.0.0.0)，该区域不能被删除。
2. (可选) 除非所有 OSPF 接口都连接到中枢区域，否则需要用自身的区域 ID 定义新的 OSPF 区域。例如，如果 NetScreen 设备要充当 ABR，则除了中枢区域外，还需创建一个新的 OSPF 区域。可将新区域配置为常规、剩余或不完全剩余区域。
3. 为每个 OSPF 区域分配一个或多个接口。必须将接口明确添加到 OSPF 区域 (包括中枢区域)。
4. 在每个接口上启用 OSPF。
5. 验证 OSPF 配置是否正确以及运行是否正常。

本节介绍如何使用 CLI 或 WebUI 来执行下图所示范例的每一项任务。本例中，将配置 NetScreen 设备充当 ABR，使其通过接口 ethernet3 连接到 area 0，并通过接口 ethernet1 连接到 area 10。

还可以配置其它可选 OSPF 参数，例如：

- 全局参数，例如根据 OSPF 协议在 VR 级别上设置的虚拟链接 (请参阅第 86 页上的 “全局 OSPF 参数”)
- 接口参数，例如根据 OSPF 协议在每个接口上设置的认证 (请参阅第 92 页上的 “OSPF 接口参数”)
- 与安全相关的 OSPF 参数，既可以在 VR 级别上设置，也可以在每个接口上设置 (请参阅第 95 页上的 “安全配置”)

创建 OSPF 路由选择实例

可在 NetScreen 设备的特定 VR 上创建并启用 OSPF 路由选择实例。创建 OSPF 路由选择实例时还将自动创建一个 OSPF 中枢区域。在 VR 上创建并启用 OSPF 路由选择实例后， OSPF 将在 VR 中所有启用 OSPF 的接口上传送和接收数据包。

范例：创建 OSPF 实例

在下例中，将首先为 trust-vr 分配路由器 ID 0.0.0.10。然后在 trust-vr 上创建一个 OSPF 路由选择实例。(有关 VR 以及在 NetScreen 设备上配置 VR 的详细信息，请参阅第 2 章，“虚拟路由器”。)

WebUI

1. 路由器 ID

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

Virtual Router ID: Custom (选择)

在文本框中输入 0.0.0.10

2. OSPF 路由选择实例

Network > Routing > Virtual Router (trust-vr) > Edit > Create OSPF Instance: 选择 **OSPF Enabled**，然后单击 **OK**。

CLI

1. 路由器 ID

```
set vrouter trust-vr router-id 10
```

2. OSPF 路由选择实例

```
set vrouter trust-vr protocol ospf
set vrouter trust-vr protocol ospf enable
save
```

***注意：**在 CLI 中，必须首先创建 OSPF 路由选择实例，之后才能启用它。因此，必须发出两个独立的 CLI 命令，以启用 OSPF 路由选择实例。*

范例：移除 OSPF 实例

本例中，将禁用 trust-vr 中的 OSPF 路由选择实例。OSPF 会禁止 trust-vr 中所有启用 OSPF 的接口传送和处理数据包。

WebUI

Network > Routing > Virtual Routers (trust-vr) > Edit > Edit OSPF Instance: 取消选择 OSPF Enabled，然后单击 **OK**。

Network > Routing > Virtual Routers (trust-vr) > Edit > Delete OSPF Instance，然后在出现确认提示时单击 **OK**。

CLI

```
unset vrouter trust-vr protocol ospf enable
unset vrouter trust-vr protocol ospf
save
```

***注意：**在 CLI 中，必须先禁用 OSPF 路由选择实例，然后才能删除它。因此，必须发出两个独立的 CLI 命令，以删除 OSPF 路由选择实例。*

定义 OSPF 区域

区域可以减少需要经由网络进行流通的路由选择信息量，因为 OSPF 路由器只维护其所在区域的链接状态数据库。而不维护该区域外的网络或路由器的链接状态信息。

所有区域必须连接到区域 0，该区域是在虚拟路由器上配置 OSPF 路由选择实例时创建的。如需创建其它 OSPF 区域，可根据需要将其定义为剩余区域或不完全剩余区域。有关这些类型区域的详细信息，请参阅第 67 页上的 “区域”。

可配置下列可选区域参数：

区域参数	说明	缺省值
Metric for default route	(仅限于 NSSA 和剩余区域) 指定缺省路由通告的度量值。	1
Metric type for the default route.	(仅限于 NSSA 区域) 指定缺省路由的外部度量类型 (1 或 2)。	1
No summary	(仅限于 NSSA 和剩余区域) 指定*不*将汇总 LSA 通告给区域。	将汇总 LSA 通告给区域
Range	(所有区域) 指定要在汇总 LSA 中通告的 IP 地址范围以及是否通告它们。	—

范例 : 创建 OSPF 区域

在下例中，将创建一个区域 ID 为 10 的 OSPF 区域。

WebUI

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

Area ID: 10

Type: normal (选择)

Action: Add

CLI

```
set vrouter trust-vr protocol ospf area 10
save
```

为 OSPF 区域分配接口

创建接口后，即可使用 WebUI 或 CLI 的 **set interface** 命令为该区域分配一个或多个接口。

范例 : 为区域分配接口

在下例中，将为 OSPF area 10 分配 ethernet1 接口，为 OSPF area 0 分配 ethernet3 接口。

WebUI

Network > Routing > Virtual Routers > Edit (trust-vr) > Edit OSPF Instance > Area > Configure (Area 10): 使用 **Add** 按钮，将 ethernet1 接口从 Available Interface(s) 栏移动到 Selected Interfaces 栏中。单击 **OK**。

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance > Area > Configure (Area 0): 使用 **Add** 按钮，将 ethernet3 接口从 Available Interface(s) 栏移动到 Selected Interfaces 栏中。单击 **OK**。

CLI

```
set interface ethernet1 protocol ospf area 10
set interface ethernet3 protocol ospf area 0
save
```

范例 : 配置区域范围

在缺省情况下， ABR 不汇总从一个区域发送到另一个区域的路由。通过配置区域范围，可将某区域内的一组子网合并为单个网络地址，以便在发往其它区域的单个汇总链接通告中通告该地址。配置区域范围时，可以指定通告还是保留通告中定义的区域范围。

在下例中，将为 area 10 定义以下区域范围 :

- 要进行通告的 10.1.1.0/24
- 不进行通告的 10.1.2.0/24

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance > Area > Configure (0.0.0.10): 在 Area Range 区域中输入以下内容，然后单击 **Add**:

IP / Netmask: 10.1.1.0/24

Type: (选择) Advertise

在 Area Range 区域中输入以下内容，然后单击 **Add**:

IP / Netmask: 10.1.2.0/24

Type: (选择) No Advertise

CLI

```
set vrouter trust-vr protocol ospf area 10 range 10.1.1.0/24 advertise
set vrouter trust-vr protocol ospf area 10 range 10.1.2.0/24 no-advertise
save
```

在接口上启用 OSPF

在缺省情况下，虚拟路由器 (VR) 的接口上一律禁用 OSPF。将接口分配给区域后，必须在该接口上明确启用 OSPF。在接口上禁用 OSPF 后， OSPF 不会在指定接口上传送或接收数据包，但接口配置参数仍将保留。

***注意：** 如果禁用了 VR 中的 OSPF 路由选择实例 (请参阅第 73 页上的 “范例 : 移除 OSPF 实例”)， OSPF 会禁止在 VR 中所有启用 OSPF 的接口上传送和处理数据包。*

范例 : 在接口上启用 OSPF

本例中，将在接口 ethernet1 (先前已分配给 area 10) 和接口 ethernet3 (先前已分配给 area 0) 上启用 OSPF 路由选择实例。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > OSPF: 选择 **Enable Protocol OSPF**，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet3) > OSPF: 选择 **Enable Protocol OSPF**，然后单击 **Apply**。

CLI

```
set interface ethernet1 protocol ospf enable
set interface ethernet3 protocol ospf enable
save
```

范例：在接口上禁用 OSPF

本例中，只禁用 ethernet1 接口上的 OSPF 路由选择实例。仍然可以在 trust-vr 虚拟路由器 (VR) 中启用了 OSPF 的其它任何接口上传送和处理 OSPF 数据包。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > OSPF: 选择 **Enable Protocol OSPF**，然后单击 **Apply**。

CLI

```
unset interface ethernet1 protocol ospf enable
save
```

注意：*如果禁用了 VR 中的 OSPF 路由选择实例 (请参阅第 73 页上的“范例：移除 OSPF 实例”)，OSPF 会禁止在 VR 中所有启用了 OSPF 的接口上传送和处理数据包。*

检验配置

可通过在命令提示符下执行下面的 CLI 命令来查看为 trust-vr 输入的配置 :

```
ns-> get vrouter trust-vr protocol ospf config
VR: trust-vr RouterId: 10.1.1.250
----------------------------------
set protocol ospf
set enable
set area 0.0.0.10 range 10.1.1.0 255.255.255.0 advertise
set area 0.0.0.10 range 10.1.2.0 255.255.255.0 no-advertise
set area 0.0.0.10
set vlink area-id 0.0.0.10 router-id 10.1.1.250
exit
set interface ethernet1 protocol ospf area 0.0.0.10
set interface ethernet1 protocol ospf enable
set interface ethernet3 protocol ospf area 0.0.0.0
set interface ethernet3 protocol ospf enable
```

可通过 **get vrouter trust-vr protocol ospf** 命令来验证虚拟路由器上是否运行了 OSPF。

```
ns-> get vrouter trust-vr protocol ospf
VR: trust-vr RouterId: 10.1.1.250
---------------------------------
OSPF enabled
Supports only single TOS(TOS0) route
Internal Router
Automatic vlink creation is disabled
Numbers of areas is 2
Number of external LSA(s) is 0
SPF Suspend Count is 10 nodes
Hold time between SPFs is 3 second(s)
Advertising default-route lsa is off
Default-route discovered by ospf will be added to the routing table
RFC 1583 compatibility is disabled.
Hello packet flooding protection is not enabled
LSA flooding protection is not enabled
Area 0.0.0.0
        Total number of interfaces is 1, Active number of interfaces is 1
        SPF algorithm executed 2 times
        Number of LSA(s) is 1
Area 0.0.0.10
        Total number of interfaces is 1, Active number of interfaces is 1
        SPF algorithm executed 2 times
        Number of LSA(s) is 0
```

突出显示的区域表示正在运行 OSPF，并对每个 OSPF 区域中的活动 OSPF 区域和活动接口进行验证。

注意：*建议您始终明确分配路由器 ID，最好不要使用缺省值。有关设置路由器 ID 的信息，请参阅第 2 章，“虚拟路由器”。*

可通过 **get vrouter trust-vr protocol ospf interface** 命令来验证接口上是否启用了 OSPF，并可查看接口状态。

```
ns-> get vrouter trust-vr protocol ospf interface
VR: trust-vr RouterId: 10.1.1.250
---------------------------------
Interface    IpAddr        NetMask       AreaId        Status    State
-------------------------------------------------------------------------------

ethernet3    2.2.2.2       255.255.255.0 0.0.0.0       enabled Designated Router

ethernet1    10.1.1.1      255.255.255.0 0.0.0.10      enabled Up
```

可为要将其选作“指定路由器”(DR) 或“备份指定路由器”(BDR) 的虚拟路由器配置优先级。上例中，“State”栏中列出了虚拟路由器的优先级。

可通过 **get vrouter trust-vr protocol ospf neighbor** 命令来验证 NetScreen 设备上的 OSPF 路由选择实例是否已与 OSPF 邻居建立了邻接关系。

```
ns-> get vrouter trust-vr protocol ospf neighbor
VR: trust-vr RouterId: 10.1.1.250
---------------------------------
                Neighbor(s) on interface ethernet3 (Area 0.0.0.0)
IpAddr/If Index RouterId        Priority State    Options
-------------------------------------------------------------------------------
2.2.2.2         2.2.2.250              1 Full     E

                Neighbor(s) on interface ethernet1 (Area 0.0.0.10)
IpAddr/If Index RouterId        Priority State    Options
-------------------------------------------------------------------------------
10.1.1.1        10.1.1.252             1 Full     E
```

上例 “State”栏中的 “Full”表示与邻居已建立了完全的 OSPF 邻接关系。

重新分配路由

路由重新分配是指在路由协议之间交换路由信息。例如，可以将以下类型的路由重新分配到同一虚拟路由器中的 OSPF 路由选择实例中：

- 从 BGP 或 RIP 获知的路由
- 直接连接的路由
- 导入的路由
- 静态配置的路由

配置重新分配路由时，必须先指定一个路由映射，以过滤重新分配的路由。有关为重新分配路由创建路由映射的详细信息，请参阅第 2 章，“虚拟路由器”。

范例：将路由重新分配给 OSPF

下例中，将源自 BGP 路由选择域的路由重新分配到当前 OSPF 路由选择域中。 CLI 和 WebUI 范例都假设先前已创建了一个名为 add-bgp 的路由映射。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance > Redistributable Rules: 输入以下内容，然后单击 **Add**:

Route Map: add-bgp

Protocol: BGP

CLI

```
set vrouter trust-vr protocol ospf redistribute route-map add-bgp protocol bgp
save
```

汇总重新分配的路由

在大型网络中，可能存在成百上千的网络地址，某些路由器可能拥挤着过多的路由信息。将一系列路由从外部协议重新分配到当前 OSPF 路由选择实例后，可将这些路由捆绑成一个广义或汇总网络路由。通过汇总多个地址，可将一系列路由视为一个路由，以简化查找过程。

在复杂的大型网络中使用路由汇总的一个优点是：可以将拓扑更改与其它路由器相分离。例如，如果给定域中的特定链接间断性地失效，汇总路由将不会更改，这样该域外部的路由器不必因为链接失败而不断地修改其路由表。

除了会在中枢路由器上的路由表中创建较少的条目外，当某个汇总网络中断或恢复连接时，路由汇总还可避免 LSA 传播到其它区域。也可汇总区域间路由或外部路由。

有时汇总的路由可能会导致出现回路。可以配置到 Null 接口的路由以避免回路的产生。本节之后将给出一个创建汇总路由的范例，然后再给出一个设置 Null 接口的范例。

范例：汇总重新分配的路由

本例中，将把 BGP 路由重新分配到当前的 OSPF 路由选择实例中。随后将一组导入的路由汇总到网络地址 2.1.1.0/24 下。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance > Redistributable Rules: 输入以下内容，然后单击 **Add**:

Route Map: add-bgp

Protocol: BGP

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance > Summary Import: 输入以下内容，然后单击 **Add**:

IP / Netmask: 2.1.1.0/24

CLI

```
set vrouter trust-vr protocol ospf redistribute route-map add-bgp protocol bgp
set vrouter trust-vr protocol ospf summary-import ip 2.1.1.0/24
save
```

范例：避免由汇总路由所创建的回路

本例中，将为在前例中创建的到网络 2.1.1.0/24 的汇总路由设置 Null 接口。网络 2.1.1.0/24 中存在主机 2.1.1.2、2.1.1.3 和 2.1.1.4。发往地址 2.1.1.10 的所有数据包均属汇总路由的范围。NetScreen 设备将接受这些数据包，不过除了可将其发送回原地址外，无法将其转发到任何其它位置，这样便形成了一个网络回路。为避免出现网络回路，将为此路由设置 Null 接口。设置 Null 接口时，设置高优先级值和度量值十分重要。

WebUI

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

Network Address/Netmask: 2.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Preference: 255

Metric: 65535

CLI

```
set vrouter trust-vr route 2.1.1.0/24 interface null preference 255 metric
    65535
save
```

全局 OSPF 参数

本节介绍可以在虚拟路由器 (VR) 级别配置的可选 OSPF 全局参数。在 VR 级别上配置 OSPF 参数后，该参数设置会影响所有启用了 OSPF 的接口上的操作。通过 CLI 中的 OSPF 路由协议环境或 WebUI，可以修改全局参数的设置。

下表介绍了 OSPF 全局参数及其缺省值。

OSPF 全局参数	说明	缺省值
Advertise default route	指定将 VR 路由表中的活动缺省路由 (0.0.0.0/0) 通告给所有 OSPF 区域。还可指定度量值 (或者是否保留路由的初始度量) 和度量类型 (ASE 类型 1 或类型 2)。还可指定始终通告缺省路由。	不通告缺省路由。
Reject default route	指定不将从 OSPF 中获知的任何缺省路由添加到路由表中。	将从 OSPF 中获知的缺省路由添加到路由表中。
Automatic virtual link	指定 VR 在无法到达 OSPF 中枢时自动创建虚拟链接。	禁用
Maximum hello packets	指定 VR 在一个 hello 接口上所能接收到的最大 OSPF hello 数据包数。	10
Maximum LSA packets	指定 VR 在指定的时间 (几秒钟) 内所能接收到的最大 OSPF LSA 数据包数。	无缺省值
RFC 1583 compatibility	指定 OSPF 路由选择实例与早期 OSPF 版本 RFC 1583 兼容。	如 RFC 2328 所定义，NetScreen 设备支持 OSPF 版本 2。
Equal cost multipath routing (ECMP)	指定负载均衡 (目的地址具有多个等开销路径) 所使用的最大路径数 (1-4)。请参阅第 50 页上的 “等值路由”。	禁用 (1)
Virtual link configuration	为虚拟链接配置 OSPF 区域和路由器 ID。根据需要，可以为虚拟链接配置认证方法、 hello 间隔、重新传输间隔、传输延迟或邻居不工作间隔。	不配置虚拟链接。

范例：通告缺省路由

缺省路由 0.0.0.0/0 与路由表中每一个目标网络均匹配，尽管可使用具体的前缀来覆盖该缺省路由。

本例中，将通告当前 OSPF 路由选择实例的缺省路由。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance: 选择 **Advertising Default Route Enable**，然后单击 **OK**。

注意：*在 WebUI 中，缺省度量为 1，缺省度量类型为 ASE 类型 1。*

CLI

```
set vrouter trust-vr protocol ospf advertise-default-route metric 1 metric-type 1
save
```

虚拟链接

OSPF 互连网络中的所有区域都必须直接连接到中枢区域。有时，需要创建一个不能实际连接到中枢区域的新区域。为解决此问题，可配置一个虚拟链接。虚拟链接提供一个远程区域，它使用逻辑路径通过另一区域与中枢区域相连。

必须在链接两端的路由器上配置虚拟链接。要在 NetScreen 设备上配置虚拟链接，需要定义以下内容：

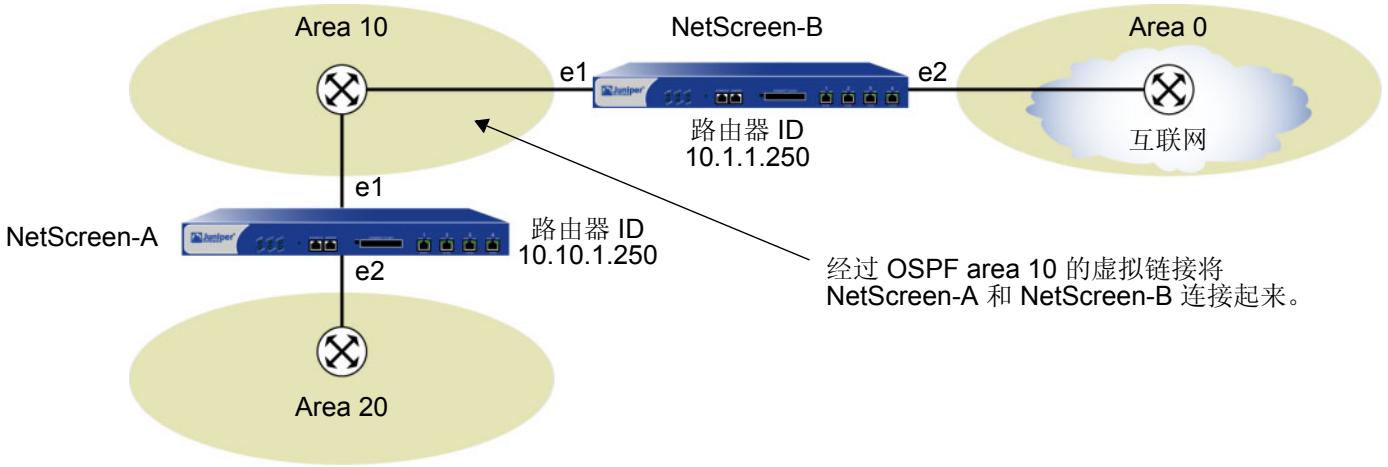
- 虚拟链接经过的 OSPF 区域的 ID。不能创建经过中枢区域或剩余区域的虚拟链接。
- 虚拟链接另一端路由器的 ID。

可以为虚拟链接配置以下可选参数：

虚拟链接参数	说明	缺省值
Authentication	指定明文密码或 MD5 认证。	不使用认证。
Dead interval	指定自收不到 OSPF 邻居的响应算起，经过多少秒后认为该邻居未运行。	40 seconds
Hello interval	指定发送 OSPF hello 数据包的时间间隔 (单位为秒)。	10 seconds
Retransmit interval	指定经过多少秒后，接口向不响应初始 LSA 的邻居重新发送 LSA。	5 seconds
Transmit delay	指定传输接口上发送的链接状态更新数据包间隔的秒数。	1 seconds

范例：创建虚拟链接

下例中，将创建一个通过 OSPF area 10 的虚拟链接，一端连接到 NetScreen-A (其路由器 ID 为 10.10.1.250)，另一端连接到 NetScreen-B (其路由器 ID 为 10.1.1.250)。(有关如何在 NetScreen 设备上配置路由器 ID 的信息，请参阅第 2 章，“虚拟路由器”。) 还要将虚拟链接的传输延迟配置成 10 秒。并需要在每台 NetScreen 设备上标识虚拟链接另一端设备的路由器 ID。



***注意：**在激活虚拟链接之前，必须在每台设备的两个接口上均启用 OSPF，并确保在设备 A 和 B 的接口上运行 OSPF。*

WebUI (NetScreen-A)

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

Area ID: 10 (选择)

Router ID: 10.1.1.250

> Configure: 在 Transmit Delay 字段中，键入 **10**，然后单击 **OK**。

CLI (NetScreen-A)

```
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.1.1.250
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.1.1.250
    transit-delay 10
save
```

***注意：**在 CLI 中，必须先创建虚拟链接，之后才能为虚拟链接配置可选参数。因此，在上述 CLI 范例中，必须发出两个独立的命令，先创建虚拟链接，再对其进行配置。*

WebUI (NetScreen-B)

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

Area ID: 10

Router ID: 10.10.1.250

> Configure: 在 Transmit Delay 字段中，键入 **10**，然后单击 **OK**。

CLI (NetScreen-B)

```
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.10.1.250
set vrouter trust-vr protocol ospf vlink area-id 10 router-id 10.10.1.250
    transit-delay 10
save
```

范例 : 创建自动虚拟链接

当虚拟路由器 (VR) 无法到达网络中枢时，可引导它自动为实例创建虚拟链接。让 VR 自动创建虚拟链接，可以取代手动创建每个虚拟链接的耗时过程。下例中，将配置自动创建虚拟链接。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance: 选择 **Automatically Generate Virtual Links**，然后单击 **OK**。

CLI

```
set vrouter trust-vr protocol ospf auto-vlink
save
```

OSPF 接口参数

本节介绍可在接口级别上配置的 OSPF 参数。在接口级别上配置 OSPF 参数后，该参数设置会影响特定接口上的 OSPF 操作。使用 CLI 中的 **interface** 命令或 WebUI，可以修改接口参数的设置。

下表介绍了可选的 OSPF 接口参数及其缺省值。

OSPF 接口参数	说明	缺省值
Authentication	指定明文密码或消息整理 5 (MD5) 认证，以验证接口上的 OSPF 通信。明文密码要求密码字符串最长为 8 位， MD5 认证密码要求密码字符串最长为 16 位。 MD5 密码还要求配置密钥字符串。	不使用认证
Cost	指定接口的度量。与接口相关的开销取决于与该接口相连的链接的带宽。带宽越高，开销值就越低 (越能满足需求)。	1 代表大于等于 100MB 的链接 10 代表 10MB 的链接 100 代表 1MB 的链接
Dead interval	指定自收不到 OSPF 邻居的响应算起，经过多少秒后 OSPF 即认定该邻居未运行。	40 seconds
Hello interval	指定 OSPF 向网络发送 hello 数据包的时间间隔，以秒为单位。	10 seconds
Link type	将通道接口指定为点对点链接或点对多点链接。请参阅第 103 页上的“点对多点通道接口”。	将以太网接口视为广播接口。 在缺省情况下，绑定到 OSPF 区域的通道接口为点对点链接。
Neighbor list	以访问列表的形式指定有资格构成邻接关系的 OSPF 邻居所在的子网。	无 (与接口上的所有邻居均构成邻接关系)
Passive Interface	指定作为 OSPF 路由 (而非外部路由) 被通告给 OSPF 域的接口 IP 地址，但该接口不传送或接收 OSPF 数据包。当接口上同时启用了 BGP 时此选项非常有用。	启用 OSPF 的接口传送并接收 OSPF 数据包

OSPF 接口参数	说明	缺省值
Priority	指定要将其选作 “指定路由器”或 “备份指定路由器”的虚拟路由器的优先级。路由器的优先级值越大，越有可能 (但不一定) 被选中。	1
Retransmit interval	指定经过多少秒后，接口向不响应初始 LSA 的邻居重新发送 LSA。	5 seconds
Transit delay	指定传输接口上发送的链接状态更新数据包间隔的秒数。	1 seconds
Demand circuit	(仅限通道接口) 根据 RFC 1793 将通道接口配置为按需电路。请参阅第 101 页上的 “通道接口上的按需电路”。	禁用
Reduce flooding	指定减少按需电路上的 LSA 泛滥。	禁用
Ignore MTU	指定忽略 OSPF 数据库协商期间查找到的本地和远程接口间的最大传输单位 (MTU) 值中的任何不匹配项。仅当本地接口上的 MTU 低于远程接口上的 MTU 时才应使用此选项。	禁用

注意：*要构成邻接关系，同一区域内的所有 OSPF 路由器必须使用同一 hello 间隔、不工作间隔和重新传输间隔值。*

范例 : 设置 OSPF 接口参数

本例中，将为 ethernet1 接口配置以下 OSPF 参数 :

- 将 OSPF hello 消息之间的时间间隔增加到 15 秒。
- 将 OSPF 重新传输之间的时间间隔增加到 7 秒。
- 将 LSA 传输之间的时间间隔增加到 2 秒。

WebUI

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

Hello Interval: 15

Retransmit Interval: 7

Transit Delay: 2

CLI

```
set interface ethernet1 protocol ospf hello-interval 15
set interface ethernet1 protocol ospf retransmit-interval 7
set interface ethernet1 protocol ospf transit-delay 2
save
```

安全配置

本节介绍 OSPF 路由选择域中可能出现的安全问题以及预防攻击的方法。

***注意：**为使 OSPF 更加安全，应将 OSPF 域中的所有路由器配置为处于同一安全级别。否则，只要有一个 OSPF 路由器遭到了破坏，则整个 OSPF 路由选择域都有可能会瘫痪。*

邻居认证

由于 LSA 没有被加密且绝大多数协议分析器都可对 OSPF 数据包进行解封，因此 OSPF 路由器很容易被欺骗。认证 OSPF 邻居是防止这类攻击的最佳方法。

OSPF 提供了简单的密码和 MD5 认证这两种方法，验证从邻居接收的 OSPF 数据包。接口上收到的所有未经验证的 OSPF 数据包都会被丢弃。在缺省情况下， OSPF 接口一律不启用认证。

MD5 认证要求发送方和接收方 OSPF 路由器使用同一密钥。可以在 NetScreen 设备上指定多个 MD5 密钥，每个密钥都有一个与之配套的密钥标识符。如果在 NetScreen 设备上配置了多个 MD5 密钥，则可以选择认证该设备与邻接路由器通信所使用的密钥的密钥标识符。这样就能在尽量不丢弃数据包的情况下，定期更改一对路由器上的 MD5 密钥。

范例：配置明文密码

本例中，将在 ethernet1 接口上为 OSPF 设置明文密码 12345678。

WebUI

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

Password: (选择), 12345678

CLI

```
set interface ethernet1 protocol ospf authentication password 12345678
save
```

范例 : 配置 MD5 密码

在下例中，将在接口 ethernet1 上设置两个不同的 MD5 密钥，并将其中的一个选择为活动密钥。缺省密钥 ID 为 0，因此不必为所输入的第一个 MD5 密钥指定密钥 ID。

WebUI

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

Authentication:

MD5 Keys: (选择)

1234567890123456

9876543210987654

5022313610981757

Key ID: 1

Preferred: (选择)

CLI

```
set interface ethernet1 protocol ospf authentication md5 1234567890123456
set interface ethernet1 protocol ospf authentication md5 9876543210987654
    key-id 1
set interface ethernet1 protocol ospf authentication md5 5022313610981757
    key-id 2
set interface ethernet1 protocol ospf authentication md5 active-md5-key-id 1
save
```

过滤 OSPF 邻居

通过多路访问环境，可以相对轻松地将设备 (包括路由器) 连接到网络中。如果连接的设备不可靠，则可能会产生稳定性或性能问题。

在缺省情况下，NetScreen 虚拟路由器 (VR) 上的 OSPF 路由选择实例与启用 OSPF 的接口上正在通信的所有 OSPF 邻居建立邻接关系。通过定义包含符合条件的 OSPF 邻居的子网列表，可以对与 OSPF 路由选择实例构成邻接关系的接口上的设备进行限制。只有指定子网内的主机或路由器才可以与 OSPF 路由选择实例构成邻接关系。要指定包含符合条件的 OSPF 邻居的子网，需要在 VR 级别上定义子网的访问列表。

范例 : 配置邻居列表

本例中，将配置一个访问列表，该列表允许子网 10.10.10.130/27 中的主机。随后将指定用该访问列表来配置符合条件的 OSPF 邻居。

WebUI

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

Access List ID: 4

Sequence No.: 10

IP/Netmask: 10.10.10.130/27

Action: Permit (选择)

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

Neighbor List: 4

CLI

```
set vrouter trust-vr access-list 4
set vrouter trust-vr access-list 4 permit ip 10.10.10.130/27 10
set interface ethernet1 protocol ospf neighbor-list 4
save
```

拒绝缺省路由

在 “路由迂回攻击” 中，路由器将缺省路由 (0.0.0.0/0) 加入路由选择域中，以便将数据包返回给自己。随后，该路由器既可以丢弃数据包，从而导致服务中断，也可以在转发数据包之前获得数据包中的机密信息。在 NetScreen 设备上，在缺省情况下 OSPF 将接受在 OSPF 中获知的所有缺省路由，并将缺省路由添加到路由表中。

范例 : 删除缺省路由

在下例中，将指定不从 OSPF 获知缺省路由。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit OSPF Instance: 选中 **Do Not Add Default-route Learned in OSPF** 复选框，然后单击 **OK**。

CLI

```
set vrouter trust-vr protocol ospf reject-default-route
save
```

防止泛滥

出现故障或遭受破坏的路由器可以向其邻居大量发送 OSPF hello 数据包或 LSA。每个路由器都从网络上其它路由器所发送的 LSA 中检索信息，为路由表提取路径信息。通过使用 LSA 泛滥保护，可对进入虚拟路由器 (VR) 的 LSA 的数量进行管理。如果 VR 接收的 LSA 过多，路由器将由于 LSA 泛滥而出现故障。如果短时间内路由器生成了过量的 LSA，则会发生 LSA 攻击，从而导致网络中的其它 OSPF 路由器频繁运行 SPF 算法。

在 NetScreen VR 上，可以配置每个 hello 间隔内接收到的最大 hello 数据包数以及某时间间隔内在 OSPF 接口上接收到的最大 LSA 数。超过配置的临界值的数据包将被丢弃。在缺省情况下， OSPF hello 数据包的临界值为每个 hello 间隔 10 个数据包 (OSPF 接口的缺省 hello 间隔为 10 秒)。没有缺省的 LSA 临界值，如果不设置 LSA 临界值，将接收所有 LSA。

范例 : 配置 Hello 临界值

在下例中，要将临界值配置为每个 hello 间隔 20 个数据包。 Hello 间隔 (可以在每个 OSPF 接口上配置该间隔) 保持其缺省值 10 秒不变。

WebUI

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

Prevent Hello Packet Flooding Attack: On

Max Hello Packet: 20

CLI

```
set vrouter trust-vr protocol ospf hello-threshold 20
save
```

范例：配置 LSA 临界值

本例中，将创建每 20 秒钟 10 个数据包的 OSPF LSA 泛滥攻击临界值。

WebUI

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

LSA Packet Threshold Time: 20

Maximum LSAs: 10

CLI

```
set vrouter trust-vr protocol ospf lsa-threshold 20 10
save
```

通道接口上的按需电路

如 RFC 1793 中所定义，OSPF 按需电路是指连接时间或使用情况影响使用此类连接的开销的网段。在按需电路中，由 OSPF 产生的信息流需要被限定为网络拓扑结构的更改。在 NetScreen 设备上，点对点和串行通道接口均可成为按需电路，为了实现正常运行，必须手动将通道的两端配置为按需电路。

***注意：**不能将点对多点接口配置为具有 OSPF 的按需电路 (请参阅第 103 页上的 “点对多点通道接口”)。*

在配置为按需电路的通道接口上，NetScreen 设备将抑制 OSPF hello 数据包的发送及 LSA 泛滥的定期刷新以减少开销。OSPF 邻居达到 “Full” 状态 (Hello 数据包相匹配且路由器和网络 LSA 反映所有邻居) 后， NetScreen 设备将抑制定期刷新 hello 数据包和 LSA。NetScreen 设备仅大量发送其内容已被更改的 LSA。

范例 : 创建 OSPF 按需电路

在下例中，将 tunnel.1 接口配置为按需电路。

***注意：**需要将远程对等方的通道接口配置为按需电路。但不必在远程对等方上配置减少的 LSA 泛滥。*

WebUI

Network > Interface > Edit > OSPF: 输入以下内容，然后单击 **Apply**:

Demand Circuit: (选择)

CLI

```
set interface tunnel.1 protocol ospf demand-circuit
save
```

范例 : 启用减少的泛滥

如果不想配置按需电路，但需要抑制 LSA 泛滥，则可启用减少泛滥功能。在下例中，将启用定期 LSA 抑制，而不会影响 tunnel.1 接口的 hello 数据包流。

WebUI

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

Reduce Flooding: (选择)

CLI

```
set interface tunnel.1 protocol ospf reduce-flooding
save
```

点对多点通道接口

将通道接口绑定到 NetScreen 设备上的某个 OSPF 区域时，在缺省情况下，将创建一个点对点 OSPF 通道。点对点通道接口仅能与远程端的一个 OSPF 路由器建立邻接关系。如果要将本地通道接口绑定到多个通道，则必须将该本地通道接口配置为点对多点接口，并在该通道接口上*禁用*路由拒绝功能。

***注意：**在接口上启用 OSPF 前必须将通道接口配置为点对多点接口。将接口配置为点对多点接口后，不能再将其配置为按需电路 (请参阅第 101 页上的 “通道接口上的按需电路”)。但是，可为该接口配置减少的 LSA 泛滥。*

有关将多个通道绑定到某个通道接口的范例，请参阅 “VPN” 卷中 “高级 VPN 功能” 一章中 “每个通道接口多个通道” 一节中的 “自动路由表和 NHTB 表条目”。有关设置链接类型、设置路由拒绝功能以及配置具有点对多点通道接口的网络的范例，请阅读本节内容。

设置链接类型

如果要在多个通道上建立 OSPF 邻接关系，则需要将链接类型设置为 “点对多点” (p2mp)。

范例 : 设置 OSPF 链接类型

本例中，将 tunnel.1 的链接类型设置为 “点对多点” (p2mp) 以满足网络需要。

WebUI

Network > Interface > Edit > OSPF: 从 Link Type 单选按钮列表中选择 Point-to-Multipoint

CLI

```
set interface tunnel.1 protocol ospf link-type p2mp
save
```

范例：禁用路由拒绝限制

在缺省情况下，除非明确配置不在同一接口上发送和接收数据包，否则 NetScreen 设备很可能会在同一接口上发送和接收数据包。在点对多点情形下，可能希望如此。要配置 NetScreen 设备在同一接口上发送和接收数据包，必须禁用路由拒绝限制。本例中，将通过 CLI 在点对多点通道接口 tunnel.1 上禁用路由拒绝限制。

WebUI

> ***注意：****必须使用 CLI 来设置路由拒绝功能。*

CLI

```
unset interface tunnel.1 route-deny
save
```

范例：点对多点网络

本例中的网络是一个中型企业的网络，该企业的总部 (CO) 设在旧金山，并在芝加哥、洛杉矶、蒙特利尔和纽约设有远程站点。

每个办公室都有一台 NetScreen 设备，每个 NetScreen 设备后面的各个网络均可与其它远程设备后面的所有网络进行通信。名为 *vpn* 的定制区段允许这五台设备使用最少的策略配置来安全发送和接收信息流。所有设备的计时器值必须相符以建立邻接关系。

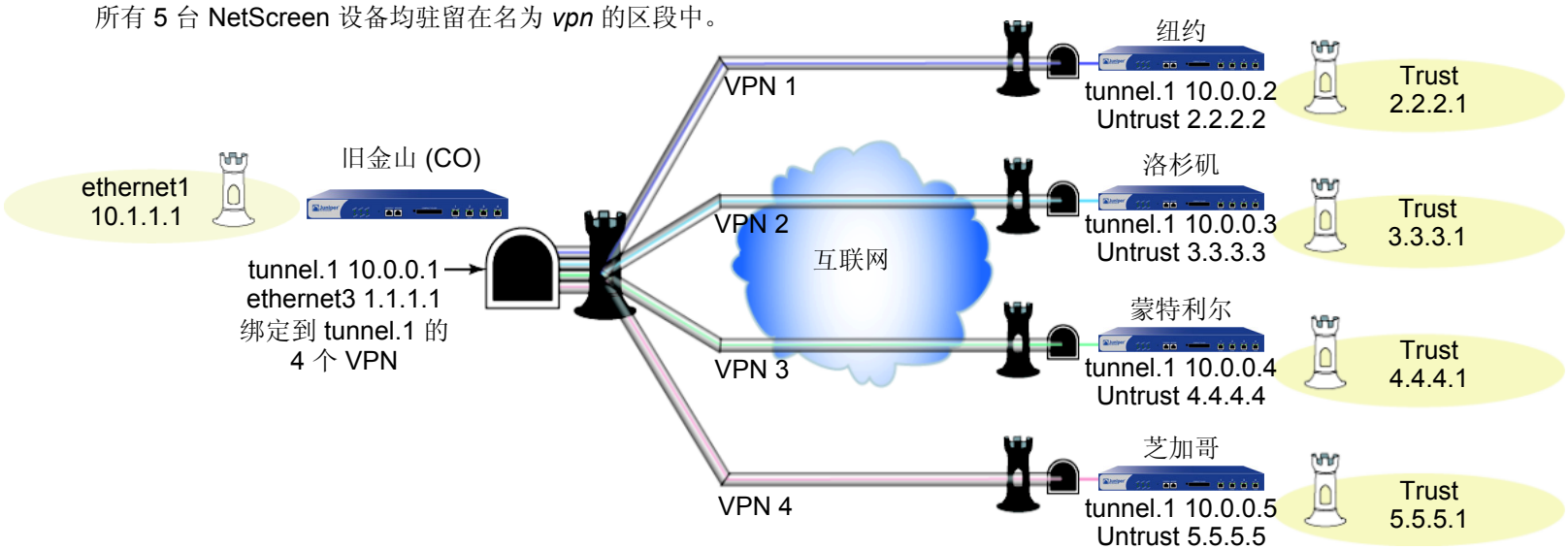
本例中，将在 CO NetScreen 设备上配置下列设置：

1. 安全区段和接口
2. 路由和 OSPF
3. VPN
4. 策略

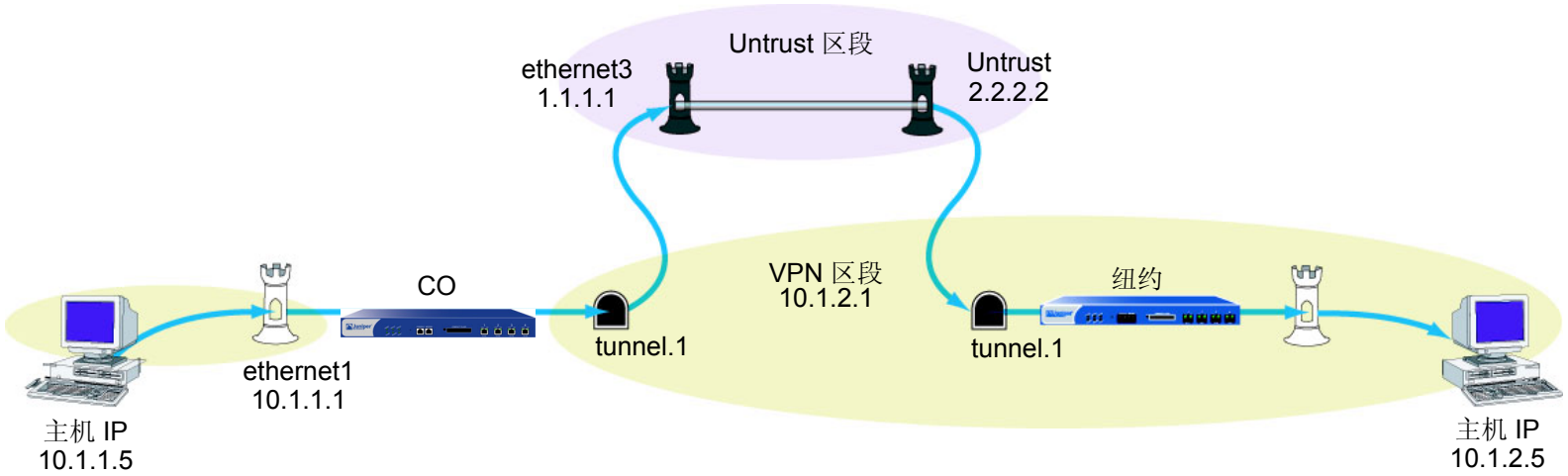
要完成网络配置，需要在四个远程办公室 NetScreen 设备中的每台设备上配置下列设置：

1. 安全区段和接口
2. OSPF
3. VPN
4. 策略

在此点对多点通道接口图中，四个 VPN 源自旧金山的 NetScreen 设备，并辐射到纽约、洛杉矶、蒙特利尔和芝加哥的远程办公室。



从 CO 的设备的角度来讲，从 CO 流向纽约的远程设备的信息流将按下图中所示的路径进行传送。



注意：*本例中，每个 WebUI 部分将仅列出通向配置设备所需页面的导航路径。要查看需要为所有 WebUI 部分设置的特定参数和值，请参阅其后面的 CLI 部分。*

WebUI (总部设备)

1. 安全区段和接口

   Network > Zones > New

   Network > Interfaces > New Tunnel IF

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interface > Edit (对于 tunnel.1) > OSPF

2. VPN

   VPNs > AutoKey Advanced > Gateway

3. 路由和 OSPF

   Network > Routing > Virtual Routers > Edit

CLI (总部设备)

1. 安全区段和接口

```
set zone name vpn tunnel untrust
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 10.0.0.1/24
save
```

2. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha

set ike gateway gw2 address 3.3.3.3 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha

set ike gateway gw3 address 4.4.4.4 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha

set ike gateway gw4 address 5.5.5.5 main outgoing-interface ethernet3 preshare
    ospfp2mp proposal pre-g2-3des-sha

set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn1 id 1 bind interface tunnel.1

set vpn vpn2 gateway gw2 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn2 monitor rekey
```

```
set vpn2 id 2 bind interface tunnel.1

set vpn vpn3 gateway gw3 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn3 monitor rekey
set vpn3 id 3 bind interface tunnel.1

set vpn vpn4 gateway gw4 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn4 monitor rekey
set vpn4 id 4 bind interface tunnel.1
save
```

3. 路由和 OSPF

```
set vrouter trust route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.10

set vrouter trust router-id 10
set vrouter trust protocol ospf
set vrouter trust protocol ospf enable

set interface tunnel.1 protocol ospf area 0
set interface tunnel.1 protocol ospf enable
set interface tunnel.1 protocol ospf link-type p2mp
unset interface tunnel.1 route-deny
save
```

注意：*在缺省情况下，禁用路由拒绝。不过，当在某些点上启用了路由拒绝功能后，为了实现点对多点通道接口的正常运行，需要禁用该功能。*

4. 策略 (按需配置)

```
set policy id 1 from trust to vpn any any any permit
set policy id 2 from vpn to trust any any any permit
save
```

可以按照这些步骤来配置远程办公室的 NetScreen 设备。NetScreen 设备通过 LSA 获知邻居。

要完成第 106 页上图中所示的配置，必须对每台远程设备重复执行以下部分所述内容，并更改 IP 地址、网关名称以及 VPN 名称，还要设置策略以满足网络需要。对于每个远程站点，名为 vpn 的区段将发生更改。

***注意：**对 WebUI 步骤进行了简化处理，但范例的 CLI 部分是完整的。可参阅前面相应的 CLI 部分以获取有关要使用的确切设置和值的信息。*

WebUI (远程办公室设备)

1. 安全区段和接口

   Network > Zones > New

   Network > Interfaces > New Tunnel IF

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interface > Edit (对于 tunnel.1) > OSPF

2. VPN

   VPNs > AutoKey Advanced > Gateway

3. 路由和 OSPF

   Network > Routing > Virtual Routers > Edit

CLI (远程办公室设备)

1. 安全区段和接口

```
set zone name vpn tunnel untrust
set interface ethernet3 zone untrust
set interface untrust ip 2.2.2.2/24
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 10.0.0.2/24
save
```

2. OSPF

```
set vrouter trust protocol ospf
set vrouter trust protocol ospf enable

set interface tunnel.1 protocol ospf area 0
set interface tunnel.1 protocol ospf enable
save
```

3. VPN

```
set ike gateway gw1 address 1.1.1.1/24 main outgoing-interface untrust preshare
    ospfp2mp proposal pre-g2-3des-sha
set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn vpn1 id 1 bind interface tunnel.1
save
```

4. 策略 (按需配置)

```
set policy id 1 from trust to vpn any any any permit
set policy id 2 from vpn to trust any any any permit
save
```

可以使用 **get vrouter** *vrouter* **protocol ospf config** 命令来查看新的更改。

4

路由选择信息协议 (RIP)

本章介绍 NetScreen 设备上的 “路由选择信息协议” (RIP) 版本 2 路由协议。其中包括以下主题：

RIP 概述

“路由选择信息协议” (RIP) 是一种距离向量协议，用作中等大小自治系统 (AS) 中的 “内部网关协议” (IGP)。ScreenOS 支持 RIP 版本 2 (RIPv2)，如 RFC 2453 中定义。 RIPv2 只支持简单密码 (纯文本) 认证， NetScreen 的 RIP 实现方案还支持 MD5 认证扩展，如 RFC 2082 的定义。

RIP 管理小型同构网络 (例如企业 LAN) 中的路由信息。RIP 网络中允许的最长路径为 15 个跳。度量值 16 表明目的地址无效或不可达 (由于该值大于 RIP 网络中允许的最大长度 15 个跳，因此又被称作 “无穷大”)。

RIP 不适于大型网络或基于实时参数 (例如测得的延迟、可靠性或负载) 选择路由的网络。 RIP 支持点对点网络 (与 VPN 一起使用) 以及广播 / 组播以太网。 RIP 支持通道接口 (具有或没有配置的按需电路) 上的 “点对多点” 连接。有关按需电路的详细信息，请参阅第 143 页上的 “通道接口的按需电路”。

RIP 每隔 30 秒将包含完整路由表的消息发送给每个邻接路由器。这些消息通常以组播形式从 RIP 端口发送到地址 224.0.0.9。

对于每个可通过 RIP 路由选择实例到达的目的地址，RIP 路由选择数据库都包含一个条目。RIP 路由选择数据库包括以下信息 :

- 目的地址的 IPv4 地址。注意 RIP 不区分网络与主机。
- 通向目的地址的路由上的第一个路由器的 IP 地址 (下一跳)。
- 到达第一个路由器所用的网络接口。
- 度量值，指出到达目的地址的距离或成本。多数 RIP 实现方案将 1 作为每个网络的度量值。
- 计时器，指出自上次更新数据库条目后经过的时间。

基本 RIP 配置

可以在 NetScreen 设备上的每个虚拟路由器创建 RIP。如果系统内存在多个虚拟路由器 (VR)，则可启用多个 RIP 实例，版本 1 或版本 2 的每个实例代表一个 VR。在缺省情况下， NetScreen 设备支持 RIP 版本 2。

注意：在 NetScreen 设备上配置动态路由协议之前，应先分配 VR ID，如第 2 章，“虚拟路由器”中所述。

本节介绍下列在 NetScreen 设备上配置 RIP 的基本步骤：

1. 在 VR 中创建 RIP 路由选择实例。
2. 启用 RIP 实例。
3. 在连接到其它 RIP 路由器的接口上启用 RIP。
4. 将通过不同路由协议 (例如 OSPF、 BGP 或静态配置的路由) 获知的路由重新分配给 RIP 实例。

本节将介绍如何使用 CLI 或 WebUI 执行上述任务。

可以配置可选的 RIP 参数，如下所示：

- 全局参数，例如计时器和可信任 RIP 邻居，在 VR 级上为 RIP 协议设置 (请参阅第 125 页上的 “全局 RIP 参数”)
- 接口参数，例如邻居认证，基于每个接口为 RIP 协议设置 (请参阅第 128 页上的 “RIP 接口参数”)
- 与安全相关的 RIP 参数，在 VR 级上或基于每个接口设置 (请参阅第 130 页上的 “安全配置”)

创建 RIP 实例

将在 NetScreen 设备的特定虚拟路由器上创建并启用 RIP 路由选择实例。在 VR 上创建并启用 RIP 路由选择实例后， RIP 可在 VR 中所有启用 RIP 的接口上传送和接收数据包。

在 VR 中删除 RIP 路由选择实例后， VR 中所有接口的相应 RIP 配置也会被删除。

关于 VR 和在 NetScreen 设备上配置 VR 的详细信息，请参阅第 2 章，“虚拟路由器”。

范例 : 创建 RIP 实例

在 *trust-vr* 上创建 RIP 路由选择实例，然后启用 RIP。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit: 选择 **Create RIP Instance**。

选择 Enable RIP，然后单击 **OK**。

CLI

1. 路由器 ID

```
set vrouter trust-vr router-id 10
```

2. RIP 路由选择实例

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable
save
```

注意 : *在 CLI 中，创建 RIP 路由选择实例的过程有两个步骤。创建 RIP 实例，然后启用 RIP。*

范例：删除 RIP 实例

在本例中，将禁用 trust-vr 中的 RIP 路由选择实例。在 trust-vr 中所有启用 RIP 的接口上， RIP 会停止传送及处理数据包。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance: Deselect Enable RIP 然后单击 **OK**。

Network > Routing > Virtual Router (trust-vr) > Edit > Delete RIP Instance，然后在出现确认提示时单击 **OK**。

CLI

```
unset vrouter trust-vr protocol rip enable
unset vrouter trust-vr protocol rip
save
```

在接口上启用 RIP

在缺省情况下，虚拟路由器 (VR) 中的所有接口都禁用 RIP，因此必须在接口上明确启用 RIP。在接口级上禁用 RIP 后， RIP 不会在指定接口上传输或接收数据包。在接口上禁用 RIP 后，设备仍保留接口配置参数。

***注意：** 如果在 VR 中禁用了 RIP 路由选择实例 (请参阅第 116 页上的 “范例 : 删除 RIP 实例”)，RIP 会禁止在 VR 中所有启用 RIP 的接口上传输及处理数据包。*

范例 : 在接口上启用 RIP

在本例中，将在 Trust 接口上启用 RIP。

WebUI

Network > Interface > Edit (对于 Trust) > RIP: 选择 Protocol RIP **Enable**，然后单击 **Apply**。

CLI

```
set interface trust protocol rip enable
save
```

范例：在接口上禁用 RIP

在本例中，将在 Trust 接口上禁用 RIP。要彻底删除 RIP 配置，在保存前输入第二个 CLI 命令。

WebUI

Network > Interface (对于 Trust) > RIP: 清除 Protocol RIP **Enable**，然后单击**Apply**。

CLI

```
unset interface trust protocol rip enable
unset interface trust protocol rip
save
```

重新分配路由

路由重新分配是指在路由协议之间交换路由信息。例如，可以将以下类型的路由重新分配给同一虚拟路由器 (VR) 中的 RIP 路由实例：

- 通过 BGP 获知的路由
- 通过 OSPF 获知的路由
- 直接连接的路由
- 导入的路由
- 静态配置的路由

需要配置一个路由映射过滤重新分配的路由。有关为路由重新分配创建路由映射的详细信息，请参阅第 2 章，“虚拟路由器”。

通过其它协议导入 RIP 的路由的缺省度量值为 10。可以更改缺省度量值 (请参阅第 125 页上的 “全局 RIP 参数”)。

范例 : 将路由重新分配给 RIP

在本例中，将子网 20.1.0.0/16 中的静态路由重新分配给 trust-vr 中的 RIP 邻居。要进行此操作，首先要创建一个访问列表，以允许 20.1.0.0/16 子网中的地址。随后，将配置路由映射，该路由映射允许与配置的访问列表相匹配的地址。使用路由映射，可以指定将静态路由重新分配给 RIP 路由实例。

WebUI

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

Access List ID: 20

Sequence No.: 1

IP/Netmask: 20.1.0.0/16

Action: Permit (选择)

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

Map Name: rtmap1

Sequence No.: 1

Action: Permit (选择)

Match Properties:

Access List: (选择), 20 (选择)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit RIP Instance > Redistributable Rules: 输入以下内容，然后单击 **Add**:

Route Map: rtmap1 (选择)

Protocol: Static (选择)

CLI

```
set vrouter trust-vr access-list 20 permit ip 20.1.0.0/16 1
set vrouter trust-vr route-map name rtmap1 permit 1
set vrouter trust-vr route-map rtmap1 1 match ip 20
set vrouter trust-vr protocol rip redistribute route-map rtmap1 protocol static
save
```

查看 RIP 信息

修改 RIP 参数后，可以查看下列类型的 RIP 详细信息：

- 数据库，它显示路由选择信息
- 协议，它给出虚拟路由器 (VR) 的 RIP 协议和接口的详细信息
- 邻居

查看 RIP 数据库

可以通过 CLI 验证 RIP 路由选择信息。可以选择查看包含所有 RIP 数据库条目的完整列表或单个条目。

范例：查看 RIP 数据库的详细信息

在本例中，将查看 RIP 数据库中的详细信息。通过附加所需 VR 的 IP 地址和网络掩码，可以选择查看所有数据库条目，还是将输出限制为单个数据库条目。

在此例中，指定 trust-vr 并附加前缀和 IP 地址 10.10.10.0/24，以只查看单个表条目。

WebUI

> ***注意：**必须使用 CLI 来查看 RIP 数据库。*

CLI

```
get vrouter trust-vr protocol rip database prefix 10.10.10.0/24
save
```

输入 CLI 命令后，可以查看 RIP 数据库条目。

```
ns-> get vrouter trust-vr protocol rip database 10.10.10.0/24
VR: trust-vr
------------------------------------------------------------------------------
Total database entry: 3
Flags: Added in Multipath - M, RIP - R, Redistributed - I,
       Default (advertised) - D, Permanent - P, Summary - S,
       Unreachable - U, Hold - H
DBID   Prefix               Nexthop        Ifp     Cost Flags   Source
    7  10.10.10.0/24        20.20.20.1     eth1       2 MR      20.20.20.1
------------------------------------------------------------------------------
```

RIP 数据库包含下列字段 :

- DBID，条目的数据库标识符
- Prefix， IP 地址和前缀
- Nexthop，下一跳 (路由器) 的地址
- Ifp，连接的类型 (以太网或通道)
- 分配的 Cost 度量值，用来指示到源的距离

Flags，可以是以下一项或多项 : Multipath (M)、 RIP (R)、 Redistributed (I)、 Advertised default (D)、 Permanent (P)、 Summary (S)、 Unreachable (U) 或 Hold (H)。

此例中，数据库标识符为 7， IP 地址和前缀为 10.10.10.0/24，下一跳为 20.20.20.1。这是一个具有开销为 2 的以太网连接。标志为 M 和 R，表示此路由为多路径并使用 RIP。

查看 RIP 协议详细信息

可以通过查看 RIP 协议详细信息来验证 RIP 配置与网络需求是否匹配。通过将 *interface* 附加到 CLI 命令，可以将输出限制为接口汇总表。

范例：查看 RIP 协议详细信息

可以查看全部的 RIP 协议信息来检查配置，或验证保存的更改是否处于活动状态。

WebUI

> ***注意：****必须使用 CLI 来查看 RIP 协议的详细信息。*

CLI

```
get vrouter trust-vr protocol rip
```

```
ns-> get vrouter trust-vr protocol rip
VR: trust-vr
------------------------------------------------------------------------------
State: enabled
Version: 2
Default metric for routes redistributed into RIP: 10
Maximum neighbors per interface: 16
Not validating neighbor in same subnet: disabled
RIP update transmission not scheduled
Maximum number of Alternate routes per prefix: 2
Advertising default route: disabled
Default routes learnt by RIP will not be accepted
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Update packet threshold is not configured
Total number of RIP interfaces created on vr(trust-vr): 1

Update| Invalid|   Flush| DC Retransmit| DC Poll| Hold Down (Timers in seconds)
-------------------------------------------------------
    30|     180|     120|             5|      40|      90

Flags: Split Horizon - S, Split Horizon with Poison Reverse - P, Passive - I
       Demand Circuit - D
Interface   IP-Prefix        Admin      State    Flags   NbrCnt Metric Ver-Rx/Tx

------------------------------------------------------------------------------
tun.1       122.1.2.114/8    enabled    disabled SD           1      1   v1v2/v1v
```

可以查看 RIP 协议设置、数据包详细信息、 RIP 计时器信息和汇总的接口表。

查看 RIP 邻居信息

可以查看有关虚拟路由器 (VR) 的 RIP 邻居的详细信息。可以检索有关所有邻居信息的列表，或通过附加所需邻居的 IP 地址来检索特定邻居的一个条目。从这些统计中，可以检查路由器的状态，以及验证邻居和 NetScreen 设备之间的连接。

范例 : 查看有关 RIP 邻居的详细信息

在下例中，将查看 trust-vr 的 RIP 邻居信息。

WebUI

> ***注意 :*** *必须使用 CLI 来查看 RIP 邻居信息。*

CLI

```
get vrouter trust-vr protocol rip neighbors
```

```
ns-> get vrouter trust-vr protocol rip neighbors
VR: trust-vr
------------------------------------------------------------------------------
Flags : Static - S, Demand Circuit - T, NHTB - N, Down - D, Up - U, Poll - P,
        Demand Circuit Init - I
Neighbors on interface tunnel.1
------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes Flags

------------------------------------------------------------------------------
10.10.10.1      v2       -            -                     0         0 TSD
```

除查看 IP 地址和 RIP 版本外，还可以查看下列 RIP 邻居信息 :

- 条目年龄
- 到期时间
- 坏数据包的数量
- 坏路由的数量
- 标志 : 静态 (S)、按需电路 (T)、 NHTB (N)、中断 (D)、连接 (U)、轮询 (P) 或按需电路初始化 (I)

查看接口的 RIP 协议详细信息

可以查看全部接口的所有有关的 RIP 协议信息，以及邻接路由器的详细信息汇总。可以选择附加特定邻居的 IP 地址来限制输出。

范例：查看特定接口的 RIP

在下例中，将为邻居查看有关 tunnel.1 接口的信息，该邻居驻留在 IP 地址 10.10.10.2。

WebUI

> ***注意：*** *必须使用 CLI 来查看 RIP 接口的详细信息。*

CLI

```
get interface tunnel.1 protocol rip neighbor 10.10.10.2
```

```
ns-> get interface tunnel.1 protocol rip
VR: trust-vr
------------------------------------------------------------------------------
Interface: tunnel.1, IP: 10.10.10.2/8, RIP: enabled, Router: enabled
Receive version v1v2, Send Version v1v2
State: Down, Passive: No
Metric: 1, Split Horizon: enabled, Poison Reverse: disabled
Demand Circuit: configured
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Authentication: none
Current neighbor count: 1
Update not scheduled
Transmit Updates: 0 (0 triggered), Receive Updates: 0
Update packets dropped because flooding: 0
Bad packets: 0, Bad routes: 0

Flags : Static - S, Demand Circuit - T, NHTB - N Down - D, Up - U, Poll - P
Neighbors on interface tunnel.1
------------------------------------------------------------------------------
IpAddress       Version  Age          Expires      BadPackets BadRoutes Flags

------------------------------------------------------------------------------
10.10.10.1      -        -            -                     0         0 TSD
```

从此信息汇总中，可以查看当前的坏数据包和坏路由的数量、验证 RIP 添加到此连接的任何开销以及查看认证设置。

全局 RIP 参数

本节介绍可以在虚拟路由器 (VR) 级上配置的 RIP 全局参数。在 VR 级上配置 RIP 参数后，该参数设置会影响所有启用 RIP 的接口上的操作。通过 CLI 中的 RIP 路由协议环境或 WebUI，可以修改全局参数的设置。

下表介绍 RIP 全局参数及其缺省值。

RIP 全局参数	说明	缺省值
Default metric	通过其它协议 (例 OSPF 和 BGP) 导入 RIP 的路由的缺省度量值。	10
Update timer	指定何时将 RIP 路由的更新发给邻居 (以秒为单位)。	30 seconds
Maximum packets per update	指定每次更新时接收的最大数据包数。	无最大值
Invalid timer	指定自邻居停止发送路由通告起，经过多久后该路由无效 (以秒为单位)。	180 seconds
Flush timer	指定自路由失效起，经过多久后被删除，以秒为单位。	120 seconds
Maximum neighbors	允许的最大 RIP 邻居数。	取决于平台
Trusted neighbors	指定定义 RIP 邻居的访问列表。如果不指定邻居，RIP 会通过组播或广播来检测接口上的邻居。请参阅第 132 页上的 “过滤 RIP 邻居”。	所有邻居都是可信任的
Allow neighbors on different subnet	指定允许 RIP 邻居在不同子网中。	禁用
Advertise default route	指定是否通告缺省路由 (0.0.0.0/0)。	禁用
Reject default route	指定 RIP 是否拒绝通过其它协议获知的缺省路由。请参阅第 133 页上的 “拒绝缺省路由”。	禁用
Incoming route map	为将由 RIP 获知的路由指定过滤器。	无
Outgoing route map	为将由 RIP 通告的路由指定过滤器。	无
Maximum alternate routes	指定可以添加到 RIP 路由数据库中的同一前缀的 RIP 路由的最大数。请参阅第 141 页上的 “备用路由”。	0
Summarize advertised routes	指定与汇总范围内的所有路由对应的汇总路由的通告。请参阅第 139 页上的 “前缀汇总”。	无

RIP 全局参数	说明	缺省值
RIP protocol version	指定 VR 使用的 RIP 协议的版本。可以基于每个接口覆盖此版本。请参阅第 137 页上的 “RIP 协议版本”。	版本 2
Hold-timer	防止对路由表产生路由翻动。可以在最小值 (更新计时器值的三倍) 和最大值 (更新计时器值和等待时间计时器值之和，不超过刷新计时器的值) 之间指定一个值。	90 seconds
Retransmit timer	指定按需电路上的触发响应的重新传输间隔。可以设置重新传输计时器，并分配一个与网络需求匹配的重试计数。	5 seconds 10 次重试次数
Poll-timer	检查按需电路的远程邻居，以查看此邻居是否处于连接状态。可以配置轮询时间计时器 (以分钟为单位) 并分配一个与网络需求匹配的重试计数。重试计数为零 (0) 意味着始终轮询。	180 seconds 0 次重试次数

通告缺省路由

可以更改 RIP 配置以包括缺省路由的通告，并更改与缺省路由关联的度量值。

范例：通告缺省路由

在缺省情况下，不将缺省路由 (0.0.0.0/0) 通告给 RIP 邻居。以下命令将缺省路由通告给 trust-vr VR 中的 RIP 邻居，度量值为 5 (必须输入一个度量值)。路由表中必须存在该缺省路由。

WebUI

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

Advertising Default Route: (选择)

Metric: 5

CLI

```
set vrouter trust-vr protocol rip adv-default-route metric number 5
save
```

注意：*有关 RIP 路由协议环境中可配置的全局参数的详细信息，请参阅* NetScreen CLI Reference Guide。

RIP 接口参数

本节介绍在接口级上配置的 RIP 参数。在接口级上配置 RIP 参数后，该参数设置只会影响特定接口上的 RIP 操作。使用 CLI 中的 **interface** 命令或 WebUI，可以修改接口参数的设置。

下表介绍 RIP 接口参数及其缺省值。

RIP 接口参数	说明	缺省值
Split-horizon	指定是否启用水平分割 (不在发送到某接口的更新中通告该接口获知的路由)。如果同时启用水平分割和毒性逆转，则会在发送到某接口的更新中通告该接口获知的路由 (度量值为 16)。	水平分割已启用。毒性逆转已禁用。
RIP metric	指定接口的 RIP 度量。	1
Authentication	指定明文密码或 MD5 认证。请参阅第 130 页上的 “邻居认证”。	不使用认证
Passive mode	指定接口只能接收 RIP 数据包，但不能传输数据包。	否
Incoming route map	为将由 RIP 获知的路由指定过滤器。	无
Outgoing route map	为将由 RIP 通告的路由指定过滤器。	无
RIP version for sending or receiving updates	指定接口上发送或接收更新的 RIP 协议版本。用于发送更新的接口的版本不必与用于接收更新的接口的版本相同。请参阅第 137 页上的 “RIP 协议版本”。	为虚拟路由器配置的版本
Route summarization	指定是否在接口上启用路由汇总。请参阅第 139 页上的 “前缀汇总”。	禁用
Demand-circuit	指定特定通道接口上的按需电路。仅当出现更改时， NetScreen 设备才发送消息。请参阅第 143 页上的 “通道接口的按需电路”。	无
Static neighbor IP	指定手动分配的 RIP 邻居的 IP 地址。	无

可以在虚拟路由器 (VR) 级或接口级上定义内向和外向路由映射。在接口级上定义的路由映射优先于在 VR 级上定义的路由映射。例如，如果在 VR 级上定义了一个内向路由映射，并在接口级上定义了另一个内向路由映射，则接口级上定义的内向路由映射优先。有关详细信息，请参阅第 54 页上的 “配置路由映射”。

范例 : 设置 RIP 接口参数

在本例中，将为 Trust 接口配置以下 RIP 参数 :

- 设置 MD5 认证，密钥为 1234567898765432，密钥 ID 为 215。
- 启用接口的水平分割和毒性逆转。

WebUI

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

Authentication: MD5 (选择)

Key: 1234567898765432

Key ID: 215

Split Horizon: Enabled with poison reverse (选择)

CLI

```
set interface trust protocol rip authentication md5 1234567898765432 key-id 215
set interface trust protocol rip split-horizon poison-reverse
save
```

安全配置

本节介绍 RIP 路由选择域中可能出现的安全问题，以及预防攻击的方法。

***注意：**为使 RIP 更加安全，应将 RIP 域中的所有路由器配置在同一安全级别上。否则，只要一个 RIP 路由器遭受破坏，整个 RIP 路由选择域都有可能瘫痪。*

邻居认证

由于 RIP 数据包没有加密且多数协议分析器都提供 RIP 数据包的解封机制，因此 RIP 路由器很容易被欺骗。 RIP 邻居认证是防止这类攻击的最佳方法。

RIP 提供简单密码和 MD5 认证这两种方法，验证从邻居接收的 RIP 数据包。接口上收到的所有未经验证的 RIP 数据包都会被丢弃。在缺省情况下， RIP 接口都不启用认证。

对于发送方和接收方 RIP 路由器， MD5 认证要求使用同一个密钥。可以在 NetScreen 设备上配置一个以上 MD5 密钥，每个密钥都有一个配套的密钥标识符。如果在 NetScreen 设备上配置多个 MD5 密钥，则可以选择认证该设备与邻接路由器通信的密钥的密钥标识符。这样就能在尽量不丢弃数据包的情况下，定期更改一对路由器上的 MD5 密钥。

范例 : 配置 MD5 密码

在下例中，将在接口 ethernet1 上设置两个不同的 MD5 密钥，并将其中的一个选择为活动密钥。缺省密钥 ID 为 0，因此不必为第一个输入的 MD5 密钥指定密钥 ID。

WebUI

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

MD5 Keys: (选择)

1234567890123456 (第一个密钥字段)

9876543210987654 (第二个密钥字段)

Key ID: 1

Preferred: (选择)

CLI

```
set interface ethernet1 protocol rip authentication md5 1234567890123456
set interface ethernet1 protocol rip authentication md5 9876543210987654 key-id 1
set interface ethernet1 protocol rip authentication md5 active-md5-key-id 1
save
```

过滤 RIP 邻居

通过多路访问环境，可以相对轻松地将设备 (包括路由器) 连接到网络中。如果连接的设备不可靠，则可能产生稳定性或性能问题。为防止出现这类问题，可使用访问列表过滤允许成为 RIP 邻居的设备。在缺省情况下， RIP 邻居只能是 NetScreen 虚拟路由器 (VR) 所在子网中的设备。

范例 : 配置可信任邻居

在本例中，将为 trust-vr 中运行的 RIP 路由选择实例配置以下全局参数 :

- 最大 RIP 邻居数为 1。
- 可信任邻居的 IP 地址为 10.1.1.1，该地址在访问列表中指定。

WebUI

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

Access List ID: 10

Sequence No.: 1

IP/Netmask: 10.1.1.1/32

Action: Permit (选择)

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

Trusted Neighbors: (选择), 10

Maximum Neighbors: 1

CLI

```
set vrouter trust-vr
ns(trust-vr)-> set access-list 10 permit ip 10.1.1.1/32 1
ns(trust-vr)-> set protocol rip
ns(trust-vr/rip)-> set max-neighbor-count 1
ns(trust-vr/rip)-> set trusted-neighbors 10
ns(trust-vr/rip)-> exit
ns(trust-vr)-> exit
save
```

拒绝缺省路由

在 “路由迂回攻击” 中，路由器将缺省路由 (0.0.0.0/0) 加入路由域中，以便将数据包返回给自己。随后，该路由器既可以丢弃数据包，引发服务中断，也可以在转发数据包之前获得数据包中的机密信息。在 NetScreen 设备上，在缺省情况下将接受在 RIP 中获知的任意缺省路由，并将缺省路由添加到路由表中。

范例 : 拒绝缺省路由

在本例中，将配置在 trust-vr 中运行的 RIP 路由选择实例，拒绝在 RIP 中获知的任意缺省路由。

WebUI

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

Reject Default Route Learnt by RIP: (选择)

CLI

```
set vrouter trust-vr protocol rip reject-default-route
save
```

防止泛滥

出现故障或遭受破坏的路由器可能向其邻居大量发送 RIP 路由选择更新数据包。在 NetScreen 虚拟路由器 (VR) 上，可以配置更新时间间隔内 RIP 接口上可以接收的最大更新数据包数，以避免更新数据包的泛滥。所有超过配置的更新临界值的数据包都将被丢弃。如果不设置更新临界值，将接收所有数据包。

如果邻居的路由表较大，进行快闪更新时给定期内的路由更新次数可能很多，因此配置更新临界值时要格外小心。超过临界值的更新数据包将被丢弃，因此有效路由可能无法被获知。

范例：配置更新临界值

在本例中，要将 RIP 在接口上接收的最大路由选择更新数据包数设置为 4。

WebUI

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

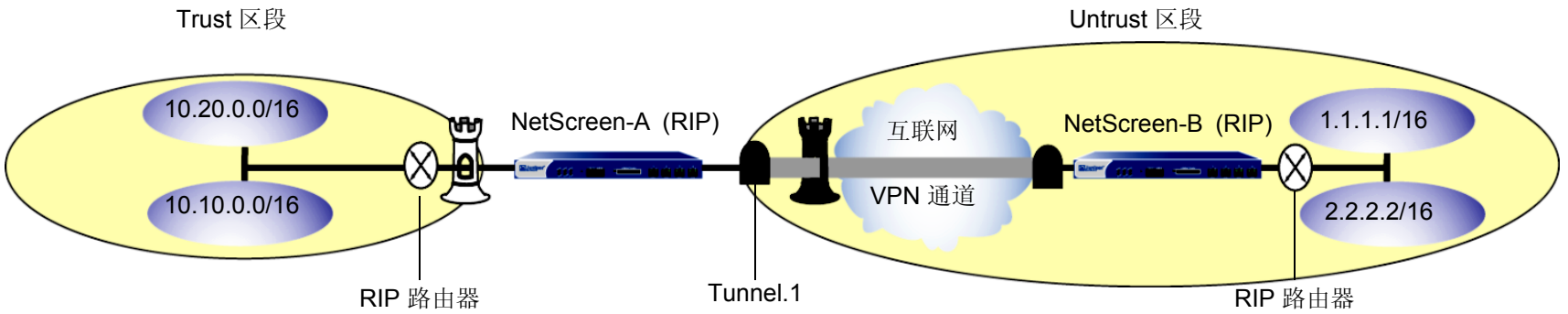
Maximum Number Packets per Update Time: (选择), 4

CLI

```
set vrouter trust-vr protocol rip threshold-update 4
save
```

范例：在通道接口上启用 RIP

在下例中，将在 NetScreen-A 设备的 trust-vr 中创建并启用 RIP 路由选择实例。在 VPN 通道接口和 Trust 区段接口上启用 RIP。只将子网 10.10.0.0/16 中的路由通告给 NetScreen-B 上的 RIP 邻居。要进行此操作，首先要配置访问列表只允许子网 10.10.0.0/16 中的地址，接着指定路由映射 *abcd*，以允许与访问列表匹配的路由。随后将指定路由映射，过滤通告给 RIP 邻居的路由。



WebUI

Network > Routing > Virtual Router > Edit (对于 trust-vr) > Create RIP Instance: 选择 **Enable RIP**，然后单击 **OK**。

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

Access List ID: 10

Sequence No.: 10

IP/Netmask: 10.10.0.0/16

Action: Permit

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

Map Name: abcd

Sequence No.: 10

Action: Permit

Match Properties:

Access List: (选择), 10

Network > Routing > Virtual Router > Edit (对于 trust-vr) > Edit RIP Instance: 选择以下内容，然后单击 **OK**:

Outgoing Route Map Filter: abcd

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

Enable RIP: (选择)

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

Enable RIP: (选择)

CLI

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable
set interface tunnel.1 protocol rip enable
set interface trust protocol rip enable
set vrouter trust-vr access-list 10 permit ip 10.10.0.0/16 10
set vrouter trust-vr route-map name abcd permit 10
set vrouter trust-vr route-map abcd 10 match ip 10
set vrouter trust-vr protocol rip route-map abcd out
save
```

可选 RIP 配置

本节将介绍可以配置的各种 RIP 功能。

RIP 协议版本

在 NetScreen 设备上，可以为虚拟路由器 (VR) 和每个发送和接收更新的 RIP 接口配置 RIP 协议版本。按照 RFC 2453， VR 可以运行一个与运行在特定接口上的 RIP 实例不同的 RIP 版本。也可以在 RIP 接口上为发送和接收更新配置不同的 RIP 协议版本。

在 VR 上，可以配置 RIP 版本 1 或 版本 2，缺省值是版本 2。对于在 RIP 接口上发送更新，可以配置 RIP 版本 1、版本 2 或与版本 1 兼容的模式 (如 RFC 2453 中所述)。对于在 RIP 接口上接收更新，可以配置 RIP 版本 1、版本 2 或版本 1 及版本 2。

注意： *不推荐版本 1 及版本 2 共同使用。在协议的版本 1 及版本 2 之间可能导致网络兼容性的问题。*

对于在 RIP 接口上的发送并接收更新，缺省 RIP 协议版本为 VR 配置的版本。

范例 : 设置 RIP 协议版本

在下例中，将在 trust-vr 中设置 RIP 协议版本 1。对于接口 ethernet3，将对发送更新和接收更新都设置 RIP 协议版本 2。

WebUI

Network > Routing > Virtual Router > Edit (对于 trust-vr) > Edit RIP Instance: 为 Version 选择 V1，然后单击 **Apply**。

Network > Interfaces > Edit (对于 ethernet3) > RIP: 在 Update Version 中为 Sending and Receiving 选择 V2，然后单击 **Apply**。

CLI

```
set vrouter trust-vr protocol rip version 1
set interface ethernet3 protocol rip receive-version v2
set interface ethernet3 protocol rip send-version v2
save
```

要验证 VR 和 RIP 接口中的 RIP 版本，可以输入 **get vrouter trust-vr protocol rip** 命令。

```
VR: trust-vr
---------------------------------
State: enabled
Version: 1
Default metric for routes redistributed into RIP: 10
Maximum neighbors per interface: 512
Not validating neighbor in same subnet: disabled
Next RIP update scheduled after: 14 sec
Advertising default route: disabled
Default routes learnt by RIP will be accepted
Incoming routes filter and offset-metric: not configured
Outgoing routes filter and offset-metric: not configured
Update packet threshold is not configured
Total number of RIP interfaces created on vr(trust-vr): 1

Update Invalid Flush (Timers in seconds)
-----------------------------------------------------------
    30     180   120
Flags: Split Horizon - S, Split Horizon with Poison Reverse - P, Passive - I
       Demand Circuit - D
Interface   IP-Prefix        Admin      State    Flags   NbrCnt Metric Ver-Rx/Tx
-------------------------------------------------------------------------------
ethernet3   20.20.1.2/24     enabled    enabled  S            0      1   2/2
```

在上例中，NetScreen 设备在 trust-vr 上运行 RIP 版本 1，但在发送和接收更新的 ethernet3 接口上运行 RIP 版本 2。

前缀汇总

可以配置汇总路由，其中包括一系列将由 RIP 通告的路由前缀。 NetScreen 设备然后仅通告与汇总范围对应的一个路由，而不是单独通告汇总范围内的每个路由。这就可以减少 RIP 更新中发送的路由条目数，并减少 RIP 邻居需要在其路由表中存储的条目数。可以在 RIP 接口 (设备由此发送) 上启用路由汇总。可以选择在一个接口上汇总路由，在另一接口上发送无汇总的路由。

注意：*不能选择性地对特定的汇总范围启用汇总，当在某个接口上启用汇总时，所有配置的汇总路由都出现在路由选择更新中。*

当配置汇总路由时，不能指定互相重叠的多个前缀范围，也不能指定包括默认路由的前缀范围。可以指定汇总路由的度量值。如果没有指定度量值，则使用汇总范围内的所有路由的最大度量值。

有时汇总的路由可以为出现回路创造机会。可以将路由配置到 Null 接口以避免回路。有关设置 Null 接口的详细信息，请参阅第 85 页上的 “范例：避免由汇总路由所创建的回路”。

范例：启用前缀汇总

在下例中，将配置汇总路由 10.1.0.0/16，它包含前缀 10.1.1.0/24 和 10.1.2.0/24。要允许 ethernet3 在 RIP 更新中发送汇总路由，需要在接口上启用汇总。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit RIP Instance > Summary IP: 输入以下内容，然后单击 **Add**:

Summary IP: 10.1.0.0

Netmask: 16

Metric: 1

Network > Interface > Edit (对于 ethernet3) > RIP: 选择汇总，然后单击 **Apply**。

CLI

```
set vrouter trust-vr protocol rip summary-ip 10.1.0.0/16
set interface ethernet3 protocol rip summary-enable
save
```

范例：禁用前缀汇总

在下例中，将在 trust-vr 上禁用 ethernet3 的前缀汇总路由。

WebUI

Network > Routing > Virtual Routers > Edit (对于 ethernet3) > Edit RIP Instance > Summary IP: 取消选择 Summarization，然后单击 **Apply**。

CLI

```
unset vrouter trust-vr protocol rip summary-ip 10.1.0.0/16
unset interface ethernet3 protocol rip summary-enable
save
```

备用路由

NetScreen 设备维护通过协议和重新分配给 RIP 的路由获知的路由的 RIP 数据库。在缺省情况下，只在数据库中维护给定前缀的最佳路由。可以指定在 RIP 数据库中，相同前缀可以有一个、两个或三个备用路由。如果在 RIP 数据库中允许前缀有备用路由，则具有不同的下一跳或 RIP 源，但前缀相同的路由将被添加到 RIP 数据库中。这将允许 RIP 支持按需电路和快速故障切换。

***注意：** Juniper Networks 推荐按需电路与备用路由配合使用。有关按需电路的详细信息，请参阅第 143 页上的 “通道接口的按需电路”。*

只有给定前缀在 RIP 数据库中的最佳路由添加到虚拟路由器 (VR) 的路由表中，并在 RIP 更新中被通告。如果从 VR 路由表中删除了最佳路由， RIP 从 RIP 数据库中添加相同前缀的次最佳路由。如果添加到 RIP 数据库的某个新路由优于 VR 路由表中的现有最佳路由，则 RIP 将更新以在路由表中使用新的更佳的路由，并停止使用旧路由。RIP 可能从 RIP 数据库中删除旧路由，也可能不删除，这取决于配置的备用路由限制。

通过发出此 CLI 命令可以查看 RIP 数据库 : **get vrouter** *vrouter* **protocol rip database**。下例中，RIP 数据库备用路由的数量设置为大于 0 的数字。 RIP 数据库为前缀 10.10.70.0/24 显示两个条目，一个开销为 2，另一个开销为 4。前缀的最佳路由 (具有最低开销的路由) 包括在 VR 的路由表中。

```
VR: trust-vr
------------------------------------------------------------------------------
Total database entry: 14
Flags : Added in Multipath - M, RIP - R, Redistributed - I
        Default (advertised) - D, Permanent - P, Summary - S
        Unreachable - U, Hold - H
DBID    Prefix                  Nexthop             Interface  Cost Flags Source
------------------------------------------------------------------------------
                                            .
                                            .
                                            .
  47    10.10.70.0/24           10.10.90.1          eth4          2 MR    10.10.90.1
  46    10.10.70.0/24           10.10.90.5          eth4          4 R     10.10.90.5
                                            .
                                            .
                                            .
```

如果启用了等开销多路径 (ECMP) 路由选择 (请参阅第 50 页上的 “等值路由”)，并且对于给定前缀 RIP 数据库中存在多个等开销路由，则 RIP 会将该前缀的多个路由添加到 VR 的路由表中，最多可达到 ECMP 限制。在某些情况下， RIP 路由数据库中的备用路由限制可导致 RIP 路由不能添加到 VR 的路由表中。如果 ECMP 限制小于或等于 RIP 数据库中的备用路由限制，则不能添加到 VR 路由表中的 RIP 路由仍保留在 RIP 数据库中 ; 只有先前添加的路由被删除或对于网络前缀而言不再是最佳的 RIP 路由时，这些路由才添加到 VR 路由表中。

例如，如果 ECMP 限制为 2，并且 RIP 数据库中备用路由限制为 3，则在 VR 的路由表中，对于同一前缀只能有两个具有相同开销的 RIP 路由。 RIP 数据库中可以存在其它的相同前缀 / 相同开销的路由，但只有两个路由添加到 VR 的路由表中。

范例 : 设置备用路由

下例中，在 trust-vr 中，将前缀在 RIP 数据库中的允许备用路由的数量设置为 1。对 VR 中 RIP 数据库的任何给定前缀，这将允许一个 “最佳” 路由和一个备用路由。

WebUI

Network > Routing > Edit (对于 trust-vr) > Edit RIP Instance: 在 Maximum Alternative Route 字段中输入 1，然后单击 **Apply**。

CLI

```
set vrouter trust-vr protocol rip alt-route 1
save
```

通道接口的按需电路

按需电路是两个通道接口之间的点对点连接。按需电路端点间的信息传递具有最小的网络开销。 RIP 的按需电路 (由广域网的 RFC 2091 定义) 在 NetScreen 设备的 VPN 通道上支持大量的 RIP 邻居。

RIP 的按需电路避免了 RIP 数据包在通道接口上的定期传输。为了节省开销， NetScreen 设备只在路由选择数据库中发生更改时才发送 RIP 信息。 NetScreen 设备也重新传输更新和请求，直到收到有效的确认为止。 NetScreen 设备通过静态邻居的配置获知 RIP 邻居，如果 VPN 通道中断，则 RIP 刷新由邻居的 IP 地址获知的路由。

因为按需电路处于恒定的状态，所以由按需电路获知的路由不随着 RIP 计时器老化。只能在下列情况下删除恒定状态的路由：

- 先前可达到的路由在收到的更新中更改为不可到达
- 由于过量的未确认重新传输导致 VPN 通道中断或按需电路中断

在 NetScreen 设备上，也可以将 “点对点” 或 “点对多点” 的通道接口配置为按需电路。在 “点对多点” 通道中必须禁用路由拒绝 (如果已配置)，以便所有路由可以到达远程站点。虽然不是必需的，但也可以在具有按需电路的 “点对多点” 接口上禁用水平分割。如果禁用水平分割，端点可以相互获知。

必须在 VPN 通道上使用重定密钥配置 VPN 监控才可获知通道状态。

在配置按需电路和静态邻居后，可以通过设置 RIP 重新传输计时器、轮询时间计时器和抑制时间计时器来符合网络需求。

本节之后是如何配置按需电路和静态邻居的范例。在 “点对多点” 通道接口上使用按需电路的 RIP 网络配置范例从第 146 页开始。

范例：配置按需电路

下例中，将 *tunnel.1* 接口配置为按需电路并保存该配置。

WebUI

Network > Interfaces > Edit > RIP: 选择 Demand Circuit，然后单击 **Apply**。

CLI

```
set interface tunnel.1 protocol rip demand-circuit
save
```

启用按需电路后，可以使用 **get vrouter** *vrouter* **protocol rip database** 命令检查其状态和定时器。根据按需电路的性能，可以更改计时器。

按需电路性能	建议
相对较慢	可以将传输计时器重新配置为较高值，以减少重新传输的数量。
无损失	可以将重新传输计时器重新配置为较低的重试计数。
拥塞和有损	可以将重新传输计时器重新配置到较高重试计数，以便在强迫静态邻居进入 POLL 状态之前留给其更多的响应时间。

配置静态邻居

运行 RIP 的 “点对多点” 接口需要静态配置的邻居。对于按需电路，手动配置是使 NetScreen 设备在 “点对多点” 接口上获知邻居地址的唯一方式。要配置 RIP 静态邻居，请输入 RIP 邻居的接口名称和 IP 地址。

范例 : 配置静态邻居

下例中，将以 tunnel.1 接口的 IP 地址 10.10.10.2 配置 RIP 邻居。

WebUI

Network > Interfaces > (编辑) RIP: 单击 **Static Neighbor IP** 按钮以前进到 Static Neighbor IP 表。输入静态邻居的 IP 地址，然后单击 **Add**。

CLI

```
set interface tunnel.1 protocol rip neighbor 10.10.10.2
unset interface tunnel.1 protocol rip neighbor 10.10.10.2
save
```

点对多点通道接口

在 RIP 版本 1 和版本 2 的编号的通道接口上支持 RIP 的 “点对多点”。

必须在使用或未使用按需电路配置的 “点对多点” 接口通道上禁用水平分割，以便消息可以到达所有远程站点。 RIP 动态获知邻居。 RIP 发送所有被传输的信息到组播地址 224.0.0.9，并根据需要将它们重新复制到所有通道。

如果要将 RIP 设置为具有按需电路的 “点对多点” 通道，则必须以集中星型配置设计网络。

范例 : 具有按需电路的点对多点

本例中的网络是一个中型企业的网络，它在旧金山有一个交换局 (CO) 并在芝加哥、洛杉矶、蒙特利尔和纽约有远程站点。每个办公室有一台 NetScreen 设备。

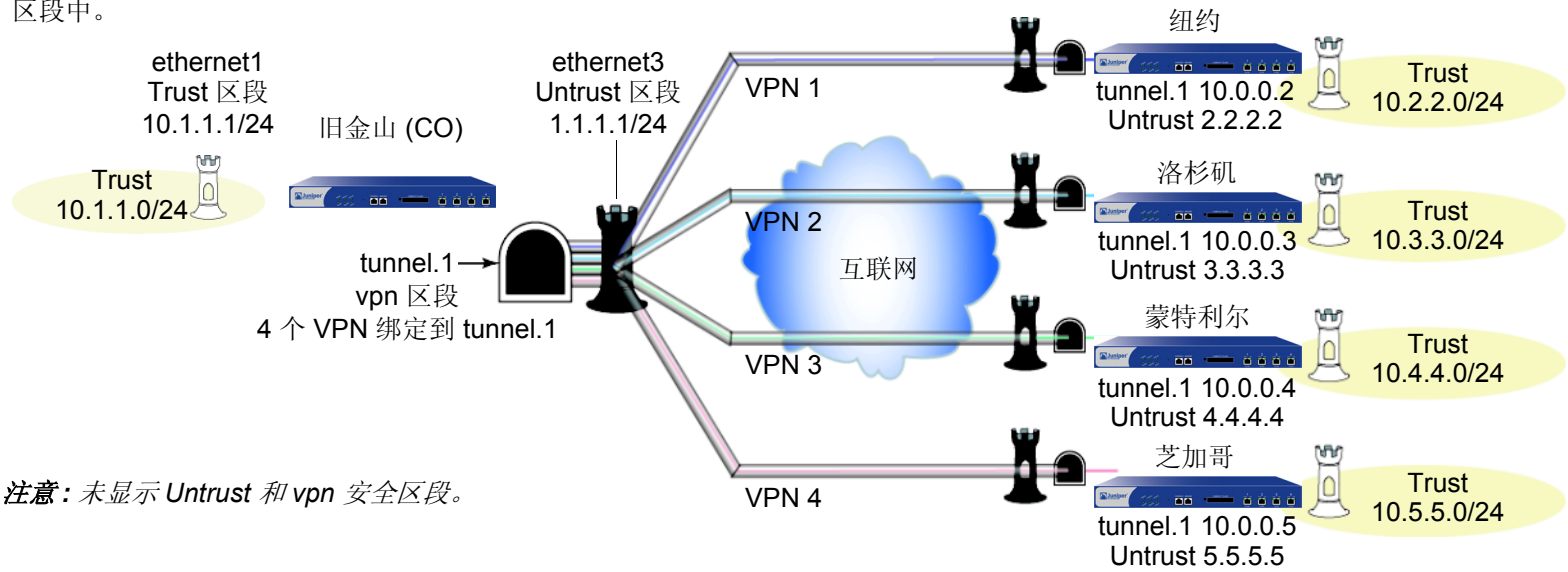
以下是 CO 的 NetScreen 设备特有的配置要求 :

1. 配置要运行 RIP 实例的 VR，启用 RIP，然后配置区段和 tunnel.1 接口。
2. 配置四个 VPN 并将它们绑定到 tunnel.1 接口。
3. 在 CO NetScreen 设备上配置 RIP 静态邻居。
4. 在本例中不要更改缺省计时器值。

以下是远程的 NetScreen 设备特有的配置需求 :

1. 配置要运行 RIP 实例的 VR，启用 RIP，然后配置区段和 tunnel.1 接口。
2. 配置 VPN 并将其绑定到 tunnel.1 接口。
3. 不要在远程办公室 NetScreen 设备上配置静态邻居。远程办公室设备只有一个将由初始的组播请求发现的邻接的设备。
4. 在本例中不要更改缺省计时器值。

从每个 NetScreen 设备的角度看，所有远程 NetScreen 设备都处于 Untrust 区段中。这些设备后面的所有 LAN 处于名为 *vpn* 的定制定义区段中。每个站点的 tunnel.1 接口也位于 vpn 安全区段中。



***注意：** 未显示 Untrust 和 vpn 安全区段。*

在网络图中，四个 VPN 通道从旧金山 NetScreen 设备始发，辐射到纽约、洛杉矶、蒙特利尔和芝加哥的远程办公室。从每个 NetScreen 设备的角度看，远程 NetScreen 设备都处于 Untrust 区段，但这些设备后面的 LAN 处于名为 *vpn* 的定制定义安全区段。每个站点的 tunnel.1 接口也位于 vpn 区段中。

在本例中，将在 CO NetScreen 设备上配置下列设置：

1. 安全区段和接口
2. VPN
3. 路由和 RIP
4. 静态邻居
5. 汇总路由
6. 策略

为了能够检查 CO 中设备上的电路状态，必须启用 VPN 监控。

要完成网络配置，在四个远程办公室 NetScreen 设备中的每个设备上配置下列设置：

1. 安全区段和接口
2. VPN
3. 路由和 RIP
4. 策略

注意：*在本例中，每个 WebUI 部分将仅列出通向设备配置页面的导航路径。要查看为任何 WebUI 部分所需设置的特定参数和值，请参阅其后的 CLI 部分。*

WebUI (交换局设备)

1. 安全区段和接口

Network > Zones > New

Network > Interfaces > New Tunnel IF

Network > Interfaces > Edit (对于 ethernet1、 ethernet3 和 tunnel.1)

2. VPN

VPNs > AutoKey Advanced > Gateway > New

VPNs > AutoKey IKE > New

3. 路由和 RIP

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create RIP Instance

Network > Interfaces > Edit (对于 tunnel.1) > RIP

4. 静态邻居

Network > Interfaces > Edit (对于 tunnel.1) > RIP > Static Neighbor IP

5. 汇总路由

   Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit RIP Instance > Summary IP

6. 策略 (按需配置)

   Policies > New

CLI (交换局设备)

1. 安全区段和接口

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

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

set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 10.0.0.1/24
```

2. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    ripvpn proposal pre-g2-3des-sha
set ike gateway gw2 address 3.3.3.3 main outgoing-interface ethernet3 preshare
    ripvpn proposal pre-g2-3des-sha
set ike gateway gw3 address 4.4.4.4 main outgoing-interface ethernet3 preshare
    ripvpn proposal pre-g2-3des-sha
set ike gateway gw4 address 5.5.5.5 main outgoing-interface ethernet3 preshare
    ripvpn proposal pre-g2-3des-sha

set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn1 id 1 bind interface tunnel.1
```

```
set vpn vpn2 gateway gw2 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn2 monitor rekey
set vpn1 id 2 bind interface tunnel.1

set vpn vpn3 gateway gw3 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn3 monitor rekey
set vpn1 id 3 bind interface tunnel.1

set vpn vpn4 gateway gw4 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn4 monitor rekey
set vpn1 id 4 bind interface tunnel.1
```

3. 路由和 RIP

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable
set vrouter trust-vr protocol rip summary-ip 100.10.0.0/16

set interface tunnel.1 protocol rip
set interface tunnel.1 protocol rip enable
set interface tunnel.1 protocol rip demand-circuit
```

4. 静态邻居

```
set interface tunnel.1 protocol rip neighbor 10.0.0.2
set interface tunnel.1 protocol rip neighbor 10.0.0.3
set interface tunnel.1 protocol rip neighbor 10.0.0.4
set interface tunnel.1 protocol rip neighbor 10.0.0.5
```

5. 汇总路由

```
set interface tunnel.1 protocol rip summary-enable
save
```

6. 策略 (按需配置)

```
set policy id 1 from trust to vpn any any any permit
set policy id 2 from vpn to trust any any any permit
save
```

可以按照以下步骤配置远程办公室 NetScreen 设备。当设置远程办公室时，不必配置静态邻居。在按需电路环境中，对于远程设备仅有一个邻居，远程设备在邻居启动时发送的组播消息中获知此邻居的信息。

要完成第 147 页的图中所示的配置，必须对每个远程设备重复本节的步骤，并更改 IP 地址、网关名称和 VPN 名称以匹配网络需求。对每个远程站点， trust 和 vpn 区段会变化。

注意：*在本例中，每个 WebUI 部分将仅列出通向设备配置页面的导航路径。要查看为任何 WebUI 部分所需设置的特定参数和值，请参阅其后的 CLI 部分。*

WebUI (交换局设备)

1. 安全区段和接口

   Network > Zones > New

   Network > Interfaces > New Tunnel IF

   Network > Interfaces > Edit (对于 ethernet1、 ethernet3 和 tunnel.1)

2. VPN

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > AutoKey IKE > New

3. 路由和 RIP

   Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create RIP Instance

   Network > Interfaces > Edit (对于 tunnel.1) > RIP

4. 策略 (按需配置)

   Policies > New

CLI (远程办公室设备)

1. 接口、路由协议和区段

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set zone name vpn
set interface tunnel.1 zone vpn
set interface tunnel.1 ip 10.0.0.2/24
```

2. VPN

```
set ike gateway gw1 address 1.1.1.1 main outgoing-interface ethernet3 preshare
    ripdc proposal pre-g2-3des-sha
set vpn vpn1 gateway gw1 no-replay tunnel idletime 0 proposal g2-esp-3des-sha
set vpn vpn1 monitor rekey
set vpn vpn1 id 1 bind interface tunnel.1
```

3. 路由和 RIP

```
set interface tunnel.1 protocol rip
set interface tunnel.1 protocol rip demand-circuit
set interface tunnel.1 protocol rip enable
```

4. 策略 (按需配置)

```
set policy id 1 from trust to vpn any any any permit
set policy id 2 from vpn to trust any any any permit
save
```

可以使用 **get vrouter** *vrouter* **protocol rip neighbors** 命令查看新的更改。按需电路的邻居出现在邻居表中，邻居信息不会老化或过期。可以使用 **get vrouter** *vrouter* **protocol rip database** 命令查看 RIP 数据库。在按需电路条目旁边会出现 *P*，它代表*恒定*。

5

边界网关协议 (BGP)

本章介绍 NetScreen 设备上的 “边界网关协议” (BGP)。其中包括以下主题：

BGP 概述

“边界网关协议”(BGP) 是一个路径向量协议，用于在“自治系统”[1] (AS) 之间传送路由信息。BGP 路由信息包括网络前缀 (路由) 经过的 AS 号的序列。这些与前缀相关的路径信息用于启用回路防护及强制执行路由策略。正如 RFC 1771 中所定义的那样， ScreenOS 支持 BGP 版本 4 (BGP-4)。

两个 *BGP 对等方*将建立一个 *BGP 会话*来交换路由信息。 BGP 路由器可以和不同的对等方一起参与 BGP 会话。必须先在 BGP 对等方之间建立 TCP 连接，然后才能打开 BGP 会话。形成初始连接时，对等方之间会交换整个路由表。路由表发生更改时， BGP 路由器将同对等方交换更新消息。BGP 路由器负责维护与其一同进行会话的所有对等方路由表的当前版本，并定期向对等方发送激活消息，以便对连接进行验证。

BGP 对等方只通告那些当前正在使用的路由。 BGP 对等方将路由通告给邻居时，还会包含描述该路由特征的路径属性。随后， BGP 路由器将比较路由属性和前缀，从指向给定目的地址的所有路径中挑选出最佳路由。

1. 自治系统是位于同一管理域中的一组路由器。

BGP 消息的类型

BGP 使用四种不同类型的消息与对等方进行通信 :

- **Open**: 消息用于互相标识 BGP 对等方以启动 BGP 会话。这类消息在对等方建立 TCP 会话后发送。交换公开消息时， BGP 对等方会指定其协议版本、 AS 号、等待时间以及 BGP 标识符。
- **Update**: 消息将路由通告给对等方，并取回先前通告的路由。
- **Notification**: 消息用于指出错误。 BGP 会话先终止，随后 TCP 会话关闭。

  注意 : *当交换公开消息时，如果对等方指出其支持不被 NetScreen 设备支持的协议功能，则 NetScreen 设备不会向该对等方发送 “通知” 消息。*

- **Keepalive**: 消息用于维护 BGP 会话。在缺省情况下，NetScreen 设备每隔 60 秒就向对等方发送一次激活消息。可对该时间间隔进行配置。

路径属性

BGP 路径属性是用来描述路由特征的一组参数。 BGP 将这些属性与其所描述的路由结合在一起，然后比较指向某一目的地址的所有路径，以选择要使用的可到达该目的地址的最佳路由。众所周知的必需路径属性 :

- **Origin**: 描述获知路由的来源，可以是 IGP、 EGP 或不完整。
- **AS-Path**: 包含传送路由通告时经过的自治系统的列表。
- **Next-Hop**: 是路由器的 IP 地址，路由的信息流将发往该地址。

可选路径属性 :

- **Multi-Exit Discriminator**: (MED) 是一个路径的度量，适用于 AS 之间存在多个链接的情况 (一个 AS 设置 MED，另一个 AS 用它来选择路径)。
- **Local-Pref**: 是一个度量，用于将路由的本地路由器的优先级通知给 BGP 对等方。
- **Atomic-Aggregate**: 通知 BGP 对等方 : 本地路由器在从对等方接收的一组重叠路由中选择了一个不太确切的路由。
- **Aggregator**: 指定执行路由聚合的 AS 和路由器。

- **Communities**: 指定此路由所属的一个或多个公共组。
- **Cluster List**: 包含路由经过的反射器集群的列表。

BGP 路由器将路由通告给对等方之前，可以选择添加或修改可选路径属性。

外部 BGP 和内部 BGP

外部 BGP (EBGP) 在不同的自治系统之间使用，例如，当将不同的 ISP 网络相互连接起来时，或者当企业网连接到 ISP 网络时。内部 BGP (IBGP) 在 AS 内使用，例如企业网内部。IBGP 的主要用途是将从 EBGP 获知的路由分配给 AS 中的路由器。因此， IBGP 路由器可将从其 EBGP 对等方获知的路由重新通告给其 IBGP 对等方，但不能将从 IBGP 对等方获知的路由通告给其它 IBGP 对等方。该限制条件使得网络中不存在路由通告回路，但同时也意味着 IBGP 网络必须是全网状结构 (即网络中的每一个 BGP 路由器必须与该网络中的其它所有路由器都建立了会话)。

某些路径属性只适用于 EBGP 或 IBGP。例如， MED 属性只在 EBGP 消息中使用，而 LOCAL-PREF 属性只出现在 IBGP 消息中。

基本 BGP 配置

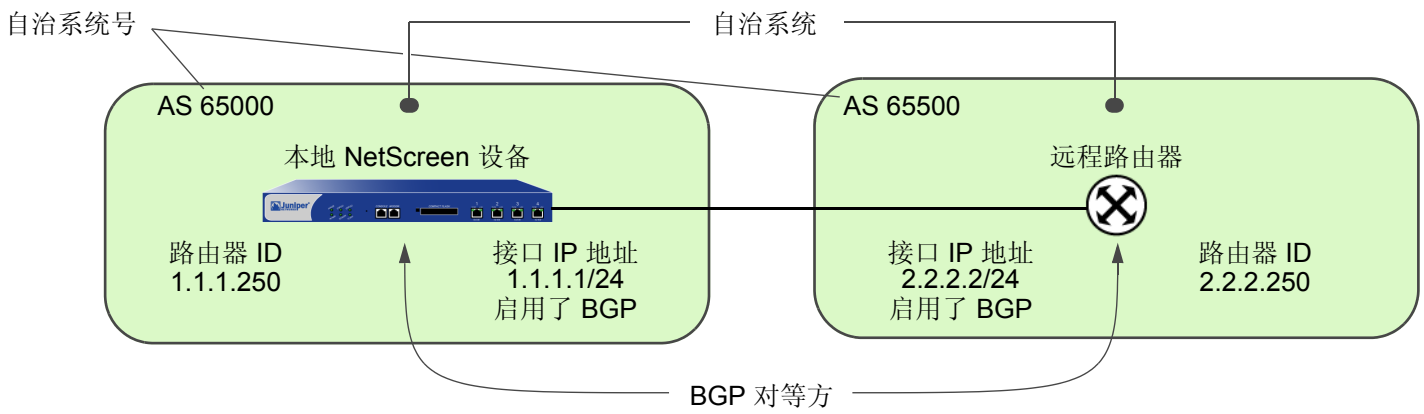
可以为 NetScreen 设备上的每个虚拟路由器 (VR) 创建 BGP 实例。如果设备上存在多个 VR，则可启用多个 BGP 实例，每个 VR 都具有一个实例。

***注意：**正如第 2 章 “虚拟路由器”中所述，在 NetScreen 设备上配置动态路由协议之前，应先分配虚拟路由器 ID。*

在 NetScreen 设备的 VR 中配置 BGP 的五个基本步骤：

1. 在 VR 中创建并启用 BGP 路由选择实例，方法是：首先为 BGP 实例分配一个自治系统号，然后再启用该实例。
2. 在连接到对等方的接口上启用 BGP。
3. 启用每个 BGP 对等方。
4. 配置一个或多个远程 BGP 对等方。
5. 检验 BGP 配置是否正确以及运行是否正常。

本节将介绍如何使用 CLI 或 WebUI 来执行下例中的各项任务。在本例中， NetScreen 设备是 AS 65000 中的 BGP 对等方。需要对 NetScreen 设备进行配置，以便它可以与 AS 65500 中的对等方建立一个 BGP 会话。



创建并启用 BGP 实例

将在 NetScreen 设备的特定虚拟路由器 (VR) 上创建并启用 BGP 路由选择实例。要创建 BGP 路由选择实例，需要先指定 VR 所在自治系统号[2]。如果 VR 是 IBGP 路由器，则其自治系统号必须与该网络中其它 IBGP 路由器的自治系统号相同。在 VR 上启用 BGP 路由选择实例后，该 BGP 路由选择实例即可同配置的 BGP 对等方进行联系并在二者之间建立会话。

范例 : 创建 BGP 路由选择实例

在下例中，将首先为 trust-vr 分配路由器 ID 0.0.0.10。随后将在 trust-vr 上创建并启用 BGP 路由选择实例，该 trust-vr 所在的 NetScreen 设备位于 AS 65000 中。 (有关虚拟路由器以及在 NetScreen 设备上配置虚拟路由器的详细信息，请参阅第 2 章 “虚拟路由器”。)

WebUI

1. 路由器 ID

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

Virtual Router ID: Custom (选择)

在文本框中输入 0.0.0.10

2. BGP 路由选择实例

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

AS Number (必需): 65000

BGP Enabled: (选择)

2. 自治系统 (AS) 号是全球唯一的编号，用于交换 EBGP 路由选择信息及标识 AS。AS 号由以下机构分配 : 美国 Internet 数字注册机构 (ARIN)、欧洲网络管理中心 (RIPE) 及亚太网络信息中心 (APNIC)。数字 64512 到 65535 具有专门用途，故不在全球互联网上通告。

CLI

1. 路由器 ID

```
set vrouter trust-vr router-id 10
```

2. BGP 路由选择实例

```
set vrouter trust-vr protocol bgp 65000
set vrouter trust-vr protocol bgp enable
save
```

范例 : 删除 BGP 实例

在本例中，将禁用并删除 trust-vr 中的 BGP 路由选择实例。 BGP 将终止与所有对等方之间的会话。

WebUI

Network > Routing > Virtual Routers (trust-vr) > Edit > Edit BGP Instance: 取消选择 BGP Enabled，然后单击 **OK**。

Network > Routing > Virtual Routers (trust-vr) > Edit: 选择 **Delete BGP Instance**，然后在出现确认提示信息时单击 **OK**。

CLI

```
unset vrouter trust-vr protocol bgp enable
unset vrouter trust-vr protocol bgp 65000
save
```

在接口上启用 BGP

必须在对等方所在的接口上启用 BGP。 (在缺省情况下， NetScreen 设备上的接口未绑定到任何路由协议。)

范例 : 在接口上启用 BGP

在本例中，将在接口 ethernet4 上启用 BGP。

WebUI

Network > Interfaces > Configure (对于 ethernet4): 选择 **Protocol BGP**，然后单击 **OK**。

CLI

```
set interface ethernet4 protocol bgp
save
```

范例 : 在接口上禁用 BGP

在本例中，将在接口 *ethernet4* 上禁用 BGP。已启用 BGP 的其它接口仍然可以传输并处理 BGP 数据包。

WebUI

Network > Interfaces > Configure (对于 ethernet4): 清除 **Protocol BGP**，然后单击 **OK**。

CLI

```
unset interface ethernet4 protocol bgp
save
```

配置 BGP 对等方

在两个 BGP 设备能够通信和交换路由之前，需要彼此确认对方身份，这样才能启动 BGP 会话。需要指定 BGP 对等方的 IP 地址，还可以配置一些用于建立并维护会话的参数。对等方既可以是内部 (IBGP) 对等方也可以是外部 (EBGP) 对等方。对于 EBGP 对等方，需要指定该对等方所在的自治系统。

通过检查对等方通告的 BGP 对等方标识符以及 AS 号，即可认证所有 BGP 对等方。如果与对等方连接成功，则会将该成功信息记入日志。如果与对等方连接出错，不是将 BGP 通知消息发送给对等方就是从对等方那里收到该消息，从而导致连接失败或关闭。

可以为单个对等方地址配置参数。还可以将对等方分配给*对等方组*，从而可为整个对等方组配置参数。

***注意：**不能将 IBGP 对等方与 EBGP 对等方分配给同一个对等方组。*

下表介绍可以为 BGP 对等方配置的参数及其缺省值。“对等方”列中的 “X”表示可以为单个对等方 IP 地址配置该参数，而 “对等方组”列中的 “X”则表示可以为对等方组配置该参数。

BGP 参数	对等方	对等方组	说明	缺省值
Advertise default route	X		将虚拟路由中的缺省路由通告给 BGP 对等方。	不通告缺省路由
EBGP multihop	X	X	本地 BGP 与邻居之间的节点数。	0 (禁用)
Force connect	X	X	促使 BGP 实例放弃与指定对等方之间的现有 BGP 连接，并接受新的连接。如果指向路由器的连接先中断后恢复，而重新建立对等连接又比较迅速，则可使用此参数尝试重新建立 BGP 对等连接。*	不适用
Hold time	X	X	在认为对等方中断之前持续收不到来自该对等方的消息的时间。	180 seconds
Keepalive	X	X	激活传输间隔的时间。	等待时间的 1/3
MD5 authentication	X	X	配置 MD-5 认证。	只检查对等方标识符和 AS 号
MED	X		配置 MED 属性值。	0

BGP 参数	对等方	对等方组	说明	缺省值
Next-hop self	X	X	对于发送到对等方的路由，下一跳路径属性被设置成本地虚拟路由器接口的 IP 地址。	不更改下一跳属性
Reflector client	X	X	将本地 BGP 设置成路由反射器后，对等方就是反射器的客户端。	无
Reject default route	X		忽略 BGP 对等方发出的缺省路由通告。	将对等方发出的缺省路由添加到路由表中
Retry time	X	X	自尝试建立会话失败起，至再次尝试建立 BGP 会话所经过的时间。	120 seconds
Send community	X	X	将公共组属性传送给对等方。	不将公共组属性传送给对等方
Weight	X	X	本地 BGP 与对等方之间路径的优先级。	100

* 注意：可以使用 **exec neighbor disconnect** 命令使 BGP 实例放弃与指定对等方之间的现有 BGP 连接，并接受新的连接。使用此 exec 命令不会更改 BGP 对等方的配置。例如，如需更改对等方应用的路由映射配置，可使用此 exec 命令。

某些参数可以在对等方级和协议级上同时配置 (请参阅第 172 页上的 “可选 BGP 配置”)。例如，假设将特定对等方的等待时间值配置为 210 秒，而协议级的缺省等待时间值为 180 秒，则对等方配置优先。可以在协议级和对等方级上设置不同的 MED 值，在对等方级上设置的 MED 值只能应用于通告给那些对等方的路由。

范例：配置 BGP 对等方

在下例中，将配置并启用 BGP 对等方。此对等方具有以下属性：

- IP 地址 1.1.1.250
- 位于 AS 65500 中

***注意：**必须启用配置的每一个对等方连接。*

WebUI

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

AS Number: 65500

Remote IP: 1.1.1.250

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors > Configure (对于刚刚添加的对等方): 选择 **Peer Enabled**，然后单击 **OK**。

CLI

```
set vrouter trust-vr protocol bgp neighbor 1.1.1.250 remote-as 65500
set vrouter trust-vr protocol bgp neighbor 1.1.1.250 enable
save
```

范例 : 配置 IBGP 对等方组

在下例中，将配置一个名为 **ibgp** 的 IBGP 对等方组，该对等方组包含以下 IP 地址 : 10.1.2.250 和 10.1.3.250。定义对等方组后，即可配置可应用于所有对等方组成员的参数 (例如 MD5 认证)。

注意：*必须启用配置的每一个对等方连接。如果将对等方配置为对等方组的一部分，仍需逐一启用对等方连接。*

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Peer Group: 输入 **ibgp** 作为 Group Name，然后单击 **Add**。

> Configure (对于 ibgp): 在 Peer authentication 字段中，输入 **verify03**，然后单击 **OK**。

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

AS Number: 65000

Remote IP: 10.1.2.250

Peer Group: ibgp (选择)

输入以下内容，然后单击 **Add**:

AS Number: 65000

Remote IP: 10.1.3.250

Peer Group: ibgp (选择)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors > Configure (对于 10.1.2.250): 选择 **Peer Enabled**，然后单击 **OK**。

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors > Configure (对于 10.1.3.250): 选择 **Peer Enabled**，然后单击 **OK**。

CLI

```
set vrouter trust-vr protocol bgp neighbor peer-group ibgp remote-as 65000
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 peer-group ibgp
set vrouter trust-vr protocol bgp neighbor 10.1.3.250 peer-group ibgp
set vrouter trust-vr protocol bgp neighbor 10.1.2.250 enable
set vrouter trust-vr protocol bgp neighbor 10.1.3.250 enable
set vrouter trust-vr protocol bgp neighbor peer-group ibgp md5-authentication
    verify03
save
```

验证 BGP 配置

使用命令 **get vrouter** *vrouter* **protocol bgp config** 可以查看通过 WebUI 或 CLI 输入的配置信息。

```
ns-> get vrouter trust-vr protocol bgp config
set protocol bgp 65000
set enable
unset synchronization
set neighbor 1.1.1.250 remote-as 65500
set neighbor 1.1.1.250 enable
exit
```

通过执行命令 **get vrouter** *vrouter* **protocol bgp**，可以验证虚拟路由器上是否正在运行 BGP。

```
ns-> get vrouter trust-vr protocol bgp
Admin State:            enable
Local Router ID:        10.1.1.250
Local AS number:        65000
Hold time:              180
Keepalive interval:     60 = 1/3 hold time, default
Local MED is:           0
Always compare MED:     disable
Local preference:       100
Route Flap Damping:     disable
IGP synchronization:    disable
Route reflector:        disable
Cluster ID:             not set (ID = 0)
Confederation based on RFC 1965
Confederation:          disable (confederation ID = 0)
Member AS:              none
Origin default route: disable
Ignore default route: disable
```

可以查看虚拟路由器 (VR) 和路由器 ID 的管理状态以及 BGP 特有的所有其它已配置参数。

***注意：** Juniper Networks 建议您应明确分配路由器 ID，最好不要使用缺省值。有关设置路由器 ID 的信息，请参阅 第 2 章 “虚拟路由器”。*

通过执行 **get vrouter** *vrouter* **protocol bgp neighbor** 命令，可以验证是否启用了 BGP 对等方或对等方组并可查看 BGP 会话的状态。

```
ns-> get vrouter trust-vr protocol bgp neighbor
Peer AS Remote IP       Local IP          Wt ConnID Status   State     Flag
 65500 1.1.1.250       0.0.0.0          100      0 Enabled ACTIVE    0000

total 1 BGP peers shown
```

本例中，可以确定已启用了 BGP 对等方，且会话处于活动状态。

可能的会话状态如下：

- **Idle** - 连接的最初状态
- **Connect** - BGP 正在等待 TCP 传输连接成功
- **Active** - BGP 正在启动传输连接[3]
- **OpenSent** - BGP 正在等待来自对等方的 OPEN 消息
- **OpenConfirm** - BGP 正在等待来自对等方的 KEEPALIVE 或 NOTIFICATION 消息
- **Established** - BGP 正在与对等方交换 UPDATE 数据包

3. 如果会话状态在 Active 和 Connect 之间不停地变化，则表明对等方之间的连接出现了问题。

安全配置

本节介绍 BGP 路由选择域中可能出现的安全问题以及预防攻击的方法。

***注意：**为使 BGP 更加安全，应将 BGP 域中的所有路由器配置为处于同一安全级别。否则，只要有一个 BGP 路由器遭到了破坏，则整个 BGP 路由选择域都有可能会瘫痪。*

邻居认证

由于 BGP 数据包没有加密且多数协议分析器都提供 BGP 数据包的解封机制，因此 BGP 路由器很容易被欺骗。对 BGP 对等方进行认证是防止这类攻击的最佳方法。

BGP 提供了 MD5 认证，以验证从对等方接收的 BGP 数据包。 MD5 认证要求发送方和接收方 BGP 路由器使用同一密钥。从指定对等方接收到的所有未经认证的 BGP 数据包都将被丢弃。在缺省情况下，只检查 BGP 对等方的对等方标识符和 AS 号。

范例 : 配置 MD5 认证

在下例中，首先将使用 AS 65500 中的远程 IP 地址 1.1.1.250 配置 BGP 对等方。接着将对对等方进行配置，使得可使用密钥 1234567890123456 进行 MD5 认证。

WebUI

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

AS Number: 65500

Remote IP: 1.1.1.250

> Configure (对于 Remote IP 1.1.1.250): 输入以下内容，然后单击 **OK**:

Peer Authentication: Enable (选择)

MD5 password: 1234567890123456

Peer Enabled: (选择)

CLI

```
set vrouter trust-vr
(trust-vr)-> set protocol bgp
(trust-vr/bgp)-> set neighbor 1.1.1.250 remote-as 65500
(trust-vr/bgp)-> set neighbor 1.1.1.250 md5-authentication 1234567890123456
(trust-vr/bgp)-> set neighbor 1.1.1.250 enable
(trust-vr/bgp)-> exit
(trust-vr)-> exit
save
```

拒绝缺省路由

在 “路由迂回攻击”中，路由器将缺省路由 (0.0.0.0/0) 加入路由选择域中，以便将数据包返回给自己。随后，该路由器既可以丢弃数据包，从而引发服务中断，也可以在转发数据包之前删除数据包中的机密信息。在 NetScreen 设备上，在缺省情况下 BGP 接受从 BGP 对等方发出的任意缺省路由，并将缺省路由添加到路由表中。

范例：拒绝缺省路由

在本例中，将配置在 trust-vr 中运行的 BGP 路由选择实例，忽略从 BGP 对等方发出的任意缺省路由。

WebUI

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

Ignore default route from peer: (选择)

CLI

```
set vrouter trust-vr protocol bgp reject-default-route
save
```

可选 BGP 配置

本节介绍可以为虚拟路由器中的 BGP 路由协议配置的参数。可以使用 CLI BGP 环境命令或 WebUI 配置这些参数。本节还将介绍某些比较复杂的参数配置。

下表介绍了 BGP 参数及其缺省值。

BGP 协议参数	说明	缺省值
Advertise default route	将虚拟路由器中的缺省路由通告给 BGP 对等方。	不通告缺省路由
Aggregate	创建聚合的路由。请参阅第 187 页上的 “路由聚合”。	禁用
Always compare MED	比较路由中的 MED 值。	禁用
AS path access list	创建 AS 路径访问列表，以允许或拒绝路由。	—
Community list	创建公共组列表。请参阅第 186 页上的 “BGP 公共组”。	—
AS confederation	创建联合。请参阅第 183 页上的 “联合”。	—
Equal cost multipath (ECMP)	可以添加等开销的多个路由，以提供负载均衡功能。请参阅第 50 页上的 “等值路由”。	禁用 (缺省值 = 1)
Flap damping	阻止路由的通告，直到它变稳定为止。	禁用
Hold time	在认为对等方中断之前持续收不到来自该对等方的消息的时间。	180 seconds
Keepalive	激活传输间隔的时间。	等待时间的 1/3
Local preference	配置 LOCAL_PREF 度量值。	100
MED	配置 MED 属性值。	0
Network	将静态网络和子网条目添加到 BGP 中。 BGP 将这些静态路由通告给所有 BGP 对等方。请参阅第 176 页上的 “将路由添加到 BGP”。	—
Route redistribution	将其它路由协议的路由导入 BGP。	—
Reflector	将本地 BGP 实例配置成客户端的路由反射器。请参阅第 180 页上的 “路由反射”。	禁用

BGP 协议参数	说明	缺省值
Reject default route	忽略 BGP 对等方发出的缺省路由通告。	将对等方发出的缺省路由添加到路由表中
Retry time	自与对等方之间建立 BGP 会话失败起，至再次尝试建立会话所经过的时间。	120 seconds
Synchronization	启用与 IGP (例如 OSPF 或 RIP) 之间的同步。	禁用

重新分配路由

路由重新分配是指在路由协议之间交换路由信息。例如，可以将以下类型的路由重新分配给同一虚拟路由器中的 BGP 路由选择实例：

- 通过 OSPF 或 RIP 获知的路由
- 直接连接的路由
- 导入的路由
- 静态配置的路由

配置重新分配路由时，必须先指定一个路由映射，以过滤重新分配的路由。有关为重新分配路由创建路由映射的详细信息，请参阅第 2 章，“虚拟路由器”。

范例 : 将路由重新分配给 BGP

在下例中，将来自 OSPF 路由选择域的路由重新分配到当前的 BGP 路由选择域中。CLI 和 WebUI 范例都假设先前已创建了名为 add-ospf 的路由映射。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Redist。Rules: 输入以下内容，然后单击 **Add**:

Route Map: add-ospf

Protocol: OSPF

CLI

```
set vrouter trust-vr protocol bgp redistribute route-map add-ospf protocol ospf
save
```

AS 路径访问列表

AS 路径属性包含路由经过的 AS 的列表。路由经过 AS 时，BGP 将 AS 路径属性预先设置成本地 AS 号。可使用 *AS 路径访问列表*来根据 AS 路径信息对路由进行过滤。 AS 路径访问列表包含一组定义 AS 路径信息的规则表达式，以及允许还是拒绝与这些信息匹配的路由。例如，可使用 AS 路径访问列表过滤经过特定 AS 的路由或来自特定 AS 的路由。

可使用规则表达式定义搜索，查找 AS 路径属性中的特定模式。可使用特殊符号和字符构建规则表达式。例如，要匹配经过 AS 65000 的路由，请使用规则表达式 **_65000_** (65000 前后的下划线用于匹配任意字符)。使用规则表达式 “65000$”，可以匹配来自 AS 65000 中的路由 (美元符号用于匹配 AS 路径属性的结尾，可能是该路由来自的 AS)。

范例：配置访问列表

下例将配置 trust-vr 的 AS 路径访问列表，允许经过 AS 65000 的路由，但不允许来自 AS 65000 的路由。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > AS Path: 输入以下内容，然后单击 **Add**:

AS Path Access List ID: 2

Deny: (选择)

AS Path String: 65000$

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > AS Path: 输入以下内容，然后单击 **Add**:

AS Path Access List ID: 2

Permit: (选择)

AS Path String: _65000_

CLI

```
set vrouter trust-vr protocol bgp as-path-access-list 2 deny 65000$
set vrouter trust-vr protocol bgp as-path-access-list 2 permit _65000_
save
```

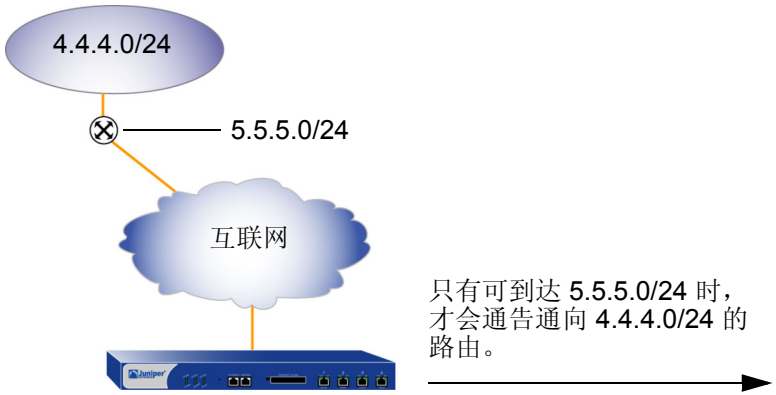
将路由添加到 BGP

要允许 BGP 通告网络路由，需要将源协议的路由重新分配给同一虚拟路由器 (VR) 中的通告协议 (BGP)。还可将静态路由直接添加到 BGP 中。如果可从 VR 到达网络前缀，则 BGP 将该路由通告给对等方，而无需将该路由重新分配到 BGP 中。当将网络前缀添加到 BGP 时，可以指定几个选项：

- 通过为 “检查可到达性” 选项选择 “Yes”，可以指定在 BGP 将路由通告给对等方之前是否一定可从 VR 到达*不同的*网络前缀。例如，如果必须通过特定的路由器接口到达需要 BGP 对其进行通告的前缀，则在 BGP 将网络通告给对等方之前，应确保可以到达该路由器接口。如果您指定的路由器接口是可到达的，则 BGP 会将该路由通告给其对等方。如果您指定的路由器接口是不可到达的，则不会将路由添加到 BGP，因此也不会将其通告给 BGP 对等方。如果您指定的路由器接口变为不可到达的，则 BGP 会从其对等方那里取回路由。
- 通过为 “检查可到达性” 选项选择 “No”，可以指定不管从 VR 能否到达，都始终通告网络前缀。缺省情况下，在 BGP 将路由通告给对等方之前，必须可从 VR 到达网络前缀。如果启用了检查可到达性，则可以连接路由。
- 可以将*权重*值分配给网络前缀。该权重值是您可以本地分配给路由的属性；不能将其通告给对等方。如果存在通向某个目的地址的多个路由，则将优先选择权重值最大的路由。
- 可以将路由的属性设置为路由映射中指定的属性（请参阅第 54 页上的 “配置路由映射”）。BGP 会通告具有路由映射中指定路由属性的路由。

范例：带条件的路由通告

在下例中，将静态路由添加到网络 4.4.4.0/24 中。指定必须可从虚拟路由器到达路由器接口 5.5.5.0/24，以便 BGP 可将 4.4.4.0/24 路由通告给对等方。如果 5.5.5.0/24 网络不可到达，则 BGP 不会通告 4.4.4.0/24 网络。



WebUI

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

IP/Netmask: 4.4.4.0/24

Check Reachability:

Yes: (选择), 5.5.5.0/24

CLI

```
set vrouter trust-vr protocol bgp network 4.4.4.0/24 check 5.5.5.0/24
save
```

范例：设置路由权重

在下例中，将路由 4.4.4.0/24 的权重值设置为 100。 (可以指定介于 0 和 65535 之间的权重值。)

WebUI

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

IP/Netmask: 4.4.4.0/24

Weight: 100

CLI

```
set vrouter trust-vr protocol bgp network 4.4.4.0/24 weight 100
save
```

范例：设置路由属性

在下例中，首先配置将路由的度量值设置为 100 的路由映射 *setattr*。然后在使用该路由映射 *setattr* 的 BGP 中配置一个静态路由。(不需要设置路由映射与路由条目的网络前缀匹配。)

WebUI

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

Map Name: setattr

Sequence No.: 1

Action: Permit (选择)

Set Properties:

Metric: (选择), 100

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

IP / Netmask: 4.4.4.0/24

Route Map: setattr (选择)

CLI

```
set vrouter trust-vr route-map name setattr permit 1
set vrouter trust-vr route-map setattr 1 metric 100
set vrouter trust-vr protocol bgp network 4.4.4.0/24 route-map setattr
save
```

路由反射

由于 IBGP 路由器不能将从一个 IBGP 对等方获知的路由重新通告给另一个 IBGP 对等方 (请参阅第 158 页上的“外部 BGP 和内部 BGP”)，因此需要配置*全网状*的 IBGP 会话，此时 BGP AS 中的每个路由器都是该 AS 中其它所有路由器的对等方。

注意：*拥有全网状会话并不意味着所有路由器相互之间直接相连，而是要求每个路由器与其它所有路由器之间能够建立并维护 IBGP 会话。*

全网状配置的 IBGP 会话不适于扩展。例如，在拥有 8 个路由器的 AS 中， 8 个路由器中的每一个路由器都需要与其它 7 个路由器构成对等关系，可以使用下面的公式对会话数进行计算：

$$x \cdot (x - 1)/2$$

对于包含 8 个路由器的 AS，全网状 IBGP 会话数应为 28。

路由反射是解决 IBGP 扩展问题的一种方法 (RFC 1966 中对其进行了介绍)。*路由反射器*是一种路由器，它可将 IBGP 获知的路由传送给指定的 IBGP 邻居 (*客户端*)，因而不再需要全网状会话。路由反射器与其客户端构成了一个*群集*，可使用群集 ID 进一步标识该群集。群集以外的路由器将整个群集看作一个实体，而不像全网状会话中那样要与 AS 中的每一个路由器构成对等关系。这种管理方法大大降低了开销。客户端同路由反射器交换路由，而路由反射器则在客户端之间反射路由。

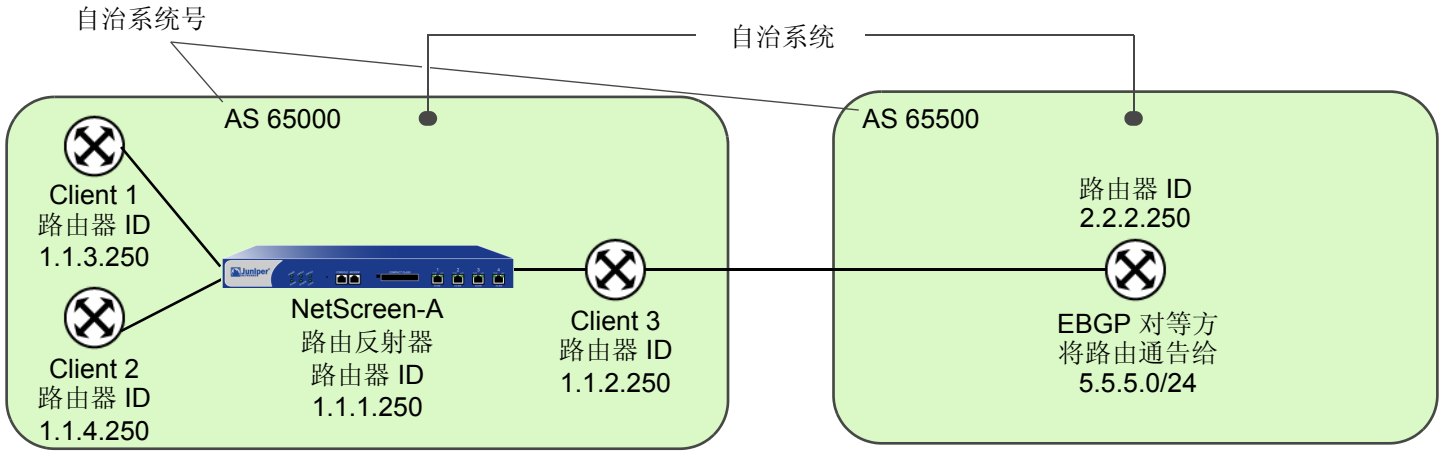
NetScreen 设备的本地虚拟路由器 (VR) 可以充当路由反射器，并且可以为其分配一个群集 ID。如果指定了群集 ID，则 BGP 路由选择实例会将该群集 ID 附加到路由的群集列表属性中。群集 ID 有利于防止路由回路的产生，因为本地 BGP 路由选择实例的群集 ID 出现在路由的群集列表中时，该实例会放弃该路由。

注意：*配置群集 ID 之前，必须先禁用 BGP 路由选择实例。*

在本地 VR 上设置路由反射器后，即可定义路由反射器的客户端。可以为客户端指定单个 IP 地址或对等方组。无需在客户端上配置其它信息。

范例：配置路由反射

在下例中， EBGP 路由器将 5.5.5.0/24 前缀通告给 Client 3。如果没有路由反射， Client 3 会将该路由通告给 NetScreen-A，但 NetScreen-A 不会将该路由重新通告给 Client 1 和 Client 2。如果将 NetScreen-A 配置成 Client 1、2 的路由反射器，并将 Client 3 配置成其客户端，则 NetScreen-A 会将从 Client 3 接收的路由重新通告给 Client 1 和 Client 2。



WebUI

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

Route reflector: Enable

Cluster ID: 99

> Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 65000

Remote IP: 1.1.2.250

输入以下内容，然后单击 **Add**:

AS Number: 65000

Remote IP: 1.1.3.250

输入以下内容，然后单击 **Add**:

AS Number: 65000

Remote IP: 1.1.4.250

> Configure (对于 Remote IP 1.1.2.250): 选择 **Reflector Client**，然后单击 **OK**。

> Configure (对于 Remote IP 1.1.3.250): 选择 **Reflector Client**，然后单击 **OK**。

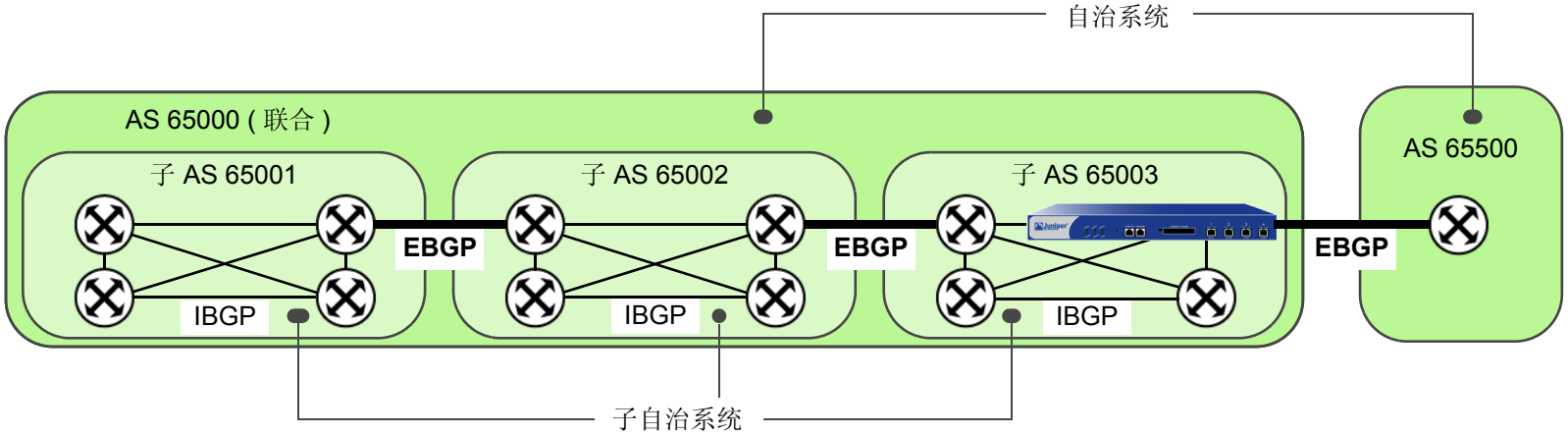
> Configure (对于 Remote IP 1.1.4.250): 选择 **Reflector Client**，然后单击 **OK**。

CLI

```
set vrouter trust-vr protocol bgp reflector
set vrouter trust-vr protocol bgp reflector cluster-id 99
set vrouter trust-vr protocol bgp neighbor 1.1.2.250 reflector-client
set vrouter trust-vr protocol bgp neighbor 1.1.3.250 reflector-client
set vrouter trust-vr protocol bgp neighbor 1.1.4.250 reflector-client
save
```

联合

类似路由反射 (请参阅第 180 页上的 “路由反射”)，*联合*是解决 IBGP 环境中全网状扩展问题的另一种方法，RFC 1965 中对其进行了介绍。联合将一个自治系统分隔成若干较小的 AS，每个子 AS 都是一个全网状的 IBGP 网络。联合以外的路由器将整个联合看作一个具有单个标识符的自治系统，子 AS 在联合以外不可见。如果建立会话的路由器位于同一联合的不同子 AS 中，该会话被称作 EIBGP 会话。它实质上是自治系统之间的 EBGP 会话，但路由器仍像 IBGP 对等方那样交换路由选择信息。



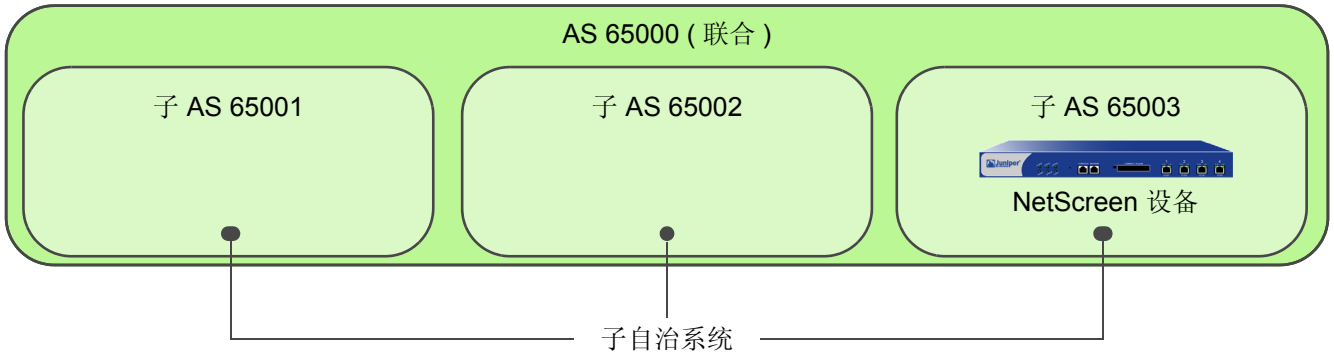
对于联合中的每一个路由器，需要指定以下信息：

- 子 AS 号 (创建 BGP 路由选择实例时指定的 AS 号)
- 子 AS 所属的联合 (此 AS 号对联合以外的 BGP 路由器可见)
- 联合中的对等方子 AS 号
- 联合是支持 RFC 1965 (缺省值) 还是支持 RFC 3065[4]

4. AS 路径属性 (请参阅第 157 页上的 “路径属性”) 通常由一个序列构成。路由更新经过的 AS。RFC 3065 允许在 AS 路径属性中加入路由更新经过的本地联合的成员 AS。

范例：配置联合

在本例中， NetScreen 设备是一个 BGP 路由器，位于联合 65000 的子 AS 65003 中。对等方子 AS 分别是联合 65000 中的 65002 和 65003。



WebUI

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

AS Number (必需): 65003
BGP Enabled: (选择)

> Confederation: 输入以下内容，然后单击 **Apply**:

Enable: (选择)
ID: 65000
Supported RFC: RFC 1965 (选择)

输入以下内容，然后单击 **Add**:
Peer member area ID: 65001

输入以下内容，然后单击 **Add**:
Peer member area ID: 65002

CLI

```
set vrouter trust-vr protocol bgp 65003
set vrouter trust-vr protocol bgp confederation id 65000
set vrouter trust-vr protocol bgp confederation peer 65001
set vrouter trust-vr protocol bgp confederation peer 65002
save
```

BGP 公共组

公共组路径属性提供了一种对目的地址进行分组 (称作公共组) 的方法，分组后， BGP 路由器即可使用公共组来控制其接受、优先选择或重新分配给对等方的路由。 BGP 路由器既可将公共组附加到路由中 (当路由没有公共组路径属性时)，也可以修改路由中的公共组 (当路由包含公共组路径属性时)。公共组路径属性提供了另外一种方法，可根据 IP 地址前缀或 AS 路径属性来分配路由信息。可以通过多种方式来使用公共组路径属性，但主要是为了简化复杂网络环境中的路由策略配置。

RFC 1997 介绍了 BGP 公共组的操作。AS 管理员可以将同一公共组分配给需要同一路由决定的一组路由，有时又被称作*路由着色*。例如，可以将一个公共组值分配给能访问互联网的路由，将另一个公共组值分配给不能访问互联网的路由。

公共组有两种形式 :

- *特定公共组*，由 AS 标识符和公共组标识符组成。公共组标识符由 AS 管理员定义。
- *众所周知的公共组*，表示要对包含这类公共组值的路由进行特殊处理。下面是可以为 NetScreen 设备上的 BGP 路由指定的众所周知的公共组值 :
  - **no-export**: 不能将具有此公共组路径属性的路由通告给 BGP 联合以外的路由器。
  - **no-advertise**: 不能将具有此公共组路径属性的路由通告给其它 BGP 对等方。
  - **no-export-subconfed**: 不能将具有此公共组路径属性的路由通告给 EBGP 对等方。

使用路由映射，可以过滤与指定公共组列表匹配的路由，删除或设置路由中的公共组路径属性，还可以向路由中添加公共组或从中删除公共组。

例如，如果 ISP 向客户提供了互联网连接功能，则可以为来自这些客户的所有路由分配特定的公共组号。随后，这些客户的路由将被通告给对等 ISP。由于来自其它 ISP 的路由被分配了不同的公共组号，因此不会被通告给对等 ISP。

路由聚合

聚合是这样一种技术：可将一定范围内的路由地址 (称为*起作用的路由*) 汇总为单个路由条目。配置聚合路由时，可以对多种可选参数进行设置。本节将举例介绍聚合路由配置。

范例：聚合具有不同 AS 路径的路由

配置聚合路由时，可以指定 BGP AS-Path 路径属性中的 AS-Set 字段包括所有起作用路由的 AS 路径。要指定此内容，请使用聚合路由配置中的 AS-Set 选项。

注意：*如果将 AS-Set 选项用于聚合路由，则起作用路由中的更改会导致聚合路由中的路径属性也随之发生更改。这会导致 BGP 重新通告其路径属性已发生更改的聚合路由。*

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Aggregate Address: 输入以下内容，然后单击 **Apply**:

Aggregate State: Enable (选择)

IP/Netmask: 1.0.0.0/8

AS-Set: (选择)

CLI

```
set vrouter trust protocol bgp
set vrouter trust protocol bgp aggregate
set vrouter trust protocol bgp aggregate 1.0.0.0/8 as-set
set vrouter trust protocol bgp enable
save
```

注意：*在启用 BGP 之前，必须首先启用 BGP 聚合。*

范例：在更新中过滤更具体的路由

配置聚合路由时，可以指定从路由更新中滤出更具体的路由。(BGP 对等方优先选择更具体的路由，如果将其通告到聚合路由。) 可以通过以下两种方法来过滤更具体的路由：

- 使用聚合路由配置中的 Summary-Only 选项来过滤所有更具体的路由。
- 使用聚合路由配置中的 Suppress-Map 选项来过滤路由映射所指定的路由。

在下例中， BGP 通告聚合路由 1.0.0.0/8，而从外向路由更新中滤出更具体的路由。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Aggregate Address: 输入以下内容，然后单击 **Apply**:

Aggregate State: Enable (选择)

IP/Netmask: 1.0.0.0/8

Suppress Option: Summary-Only (选择)

CLI

```
set vrouter trust protocol bgp aggregate 1.0.0.0/8 summary-only
save
```

在下例中，希望从包括聚合路由 1.0.0.0/8 的更新中滤出 1.2.3.0/24 范围内的路由。要实现这一目的，首先应对指定要过滤路由 (1.2.3.0/24) 的访问列表进行配置。然后，配置路由映射 ‘noadvert’ 允许路由 1.2.3.0/24。接下来配置聚合路由 1.0.0.0/8 并将路由映射 ‘noadvert’ 指定为外向更新的过滤选项。

WebUI

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

Access List ID: 1

Sequence No.: 777

IP/Netmask: 1.2.3.0/24

Action: Permit (选择)

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

Map Name: noadvert

Sequence No.: 2

Action: Permit (选择)

Match Properties:

Access List (选择), 1 (选择)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Aggregate Address: 输入以下内容，然后单击 **Apply**:

Aggregate State: Enable (选择)

IP/Netmask: 1.0.0.0/8

Suppress Option: Route-Map (选择), noadvert (选择)

CLI

```
set vrouter trust-vr access-list 1 permit ip 1.2.3.0/24 777
set vrouter trust-vr route-map name noadvert permit 2
set vrouter trust-vr route-map noadvert 2 match ip 1
set vrouter trust protocol bgp aggregate 1.0.0.0/8 suppress-map noadvert
save
```

范例：选择路径属性的路由

配置聚合路由时，可以指定应该使用哪些路由或不应该使用哪些路由来构建聚合路由的 BGP AS-Path 路径属性。使用聚合路由配置中的 Advertise-Map 选项来选择路由。可以将此选项与 AS-Set 选项一起使用，以选择使用 AS-Set 属性进行通告的路由。

在下例中，将配置要使用 AS-Set 属性进行通告的聚合路由 1.0.0.0/8。通告的 AS-Set 属性由位于前缀范围 1.5.0.0/16 内的所有更具体的路由组成，而并非由位于前缀范围 1.5.6.0/24 内的路由组成；配置路由映射“advertset”中将要包括和排除的前缀范围。

WebUI

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

Access List ID: 3

Sequence No.: 888

IP/Netmask: 1.5.6.0/24

Action: Deny (选择)

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

Access List ID: 3

Sequence No.: 999

IP/Netmask: 1.5.0.0/16

Action: Permit (选择)

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

Map Name: advertset

Sequence No.: 4

Action: Permit (选择)

Match Properties:

Access List (选择), 3 (选择)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Aggregate Address: 输入以下内容，然后单击 **Apply**:

Aggregate State: Enable (选择)

IP/Netmask: 1.0.0.0/8

Advertise Map: advertset (选择)

CLI

```
set vrouter trust-vr access-list 3 deny ip 1.5.6.0/24 888
set vrouter trust-vr access-list 3 permit ip 1.5.0.0/16 999
set vrouter trust-vr route-map name advertset permit 4
set vrouter trust-vr route-map advertset 4 match ip 3
set vrouter trust protocol bgp aggregate 1.0.0.0/8 as-set advertise-map
    advertset
save
```

范例：更改聚合路由的属性

配置聚合路由时，可根据指定的路由映射来设置聚合路由的属性。在下例中，将配置使用外向更新中的度量值 1111 进行通告的聚合路由 1.0.0.0/8。

WebUI

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

Map Name: aggmetric

Sequence No.: 5

Action: Permit (选择)

Set Properties: (选择)

Metric: 1111

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Aggregate Address: 输入以下内容，然后单击 **Apply**:

Aggregate State: Enable (选择)

IP/Netmask: 1.0.0.0/8

Attribute Map: aggmetric (选择)

CLI

```
set vrouter trust-vr route-map name aggmetric permit 5
set vrouter trust-vr route-map aggmetric 5 metric 1111
set vrouter trust protocol bgp aggregate 1.0.0.0/8 attribute-map aggmetric
save
```

6

组播路由

本章介绍基本的组播路由概念。本章包括以下几个部分：

组播路由概述

企业使用组播路由将信息流 (例如，数据流或视频流) 从一个源同时传输到一组接收方。可将任何主机作为源，而且接收方可以位于互联网的任意位置。

IP 组播路由提供了将信息流转发到多个主机的有效方法，因为启用组播的路由器仅将组播信息流传送到要接收该信息流的主机。为了能够接收数据，主机必须表示要接收组播数据，而且必须加入组播组。启用组播的路由器仅将组播信息流转发给有意接收该信息流的接收方。

要转发组播信息，组播路由环境需要具备以下内容 :

- 主机和路由器之间用于传送组播组成员关系信息的机制。 NetScreen 设备支持 IGMP (互联网组管理协议) 版本 1、2 和 3。路由器和主机仅使用 IGMP 来传送成员关系信息，而不转发或路由组播信息流 (有关 IGMP 的信息，请参阅第 205 页上的 “IGMP”。)
- 用来传送组播路由表以及将数据转发给网络中的各个主机的组播路由协议。 NetScreen 设备支持 PIM-SM (协议无关组播 – 稀疏模式) 和 PIM-SSM (协议无关组播 – 源特定模式)。 (有关 PIM-SM 和 PIM-SSM 的信息，请参阅第 247 页上的 “PIM”。)

  或者，还可使用 “IGMP 代理” 功能来转发组播信息流，而不占用运行组播路由协议的 CPU 开销。 (有关 “IGMP 代理” 的信息，请参阅第 219 页上的 “IGMP 代理”。)

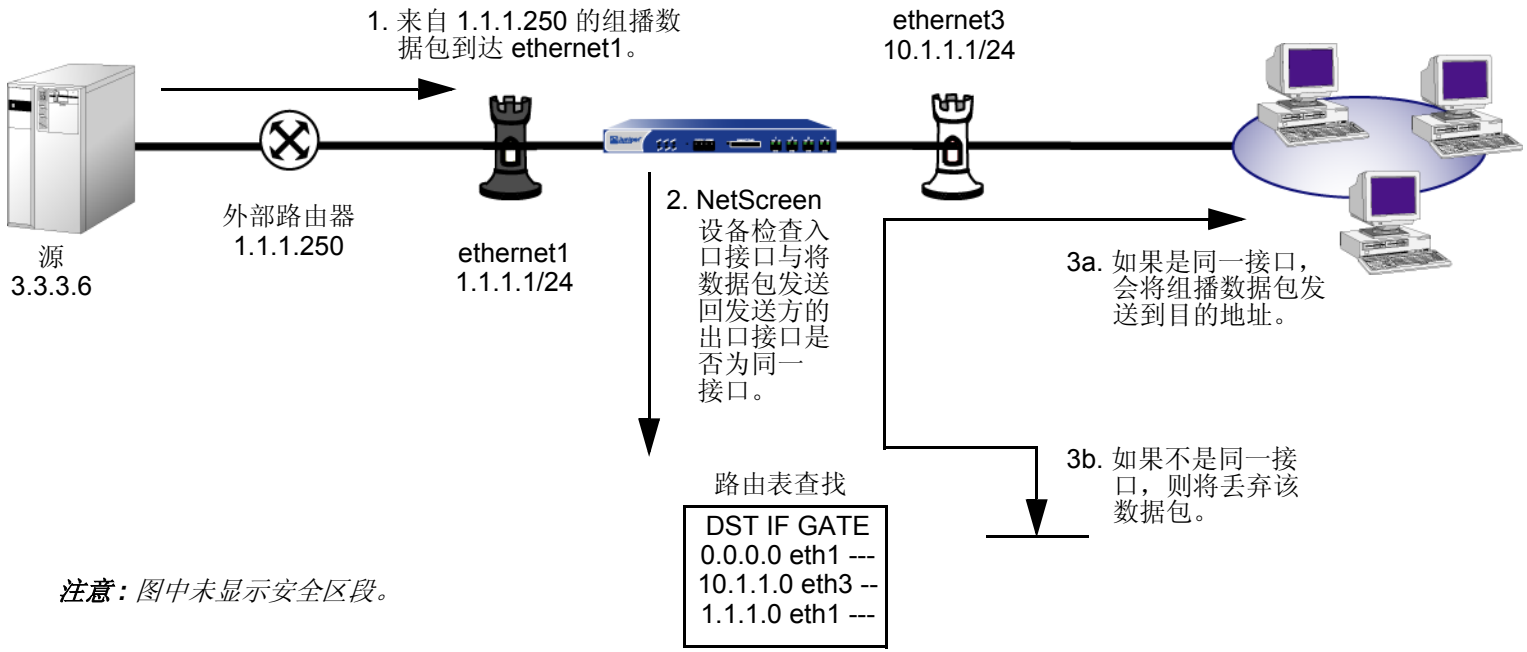
以下各节将介绍组播路由中所涉及到的基本概念。

组播地址

当源发送组播信息流时，目的地址即为组播组地址。组播组地址是其地址范围介于 224.0.0.0 和 239.255.255.255 之间的 “D 类” 地址。

反向路径转发

接收到组播数据包后，组播路由器将使用一个被称作反向路径转发 (RPF) 的过程来检查数据包的有效性。创建组播路由前，路由器将在单播路由表中执行路由查找以检查接收数据包的接口 (入口接口) 是否与将数据包发送回发送方时所必须使用的接口为同一接口。如果是同一接口，则路由器将创建组播路由条目，并将该数据包转发到下一跳路由器。如果不是同一接口，则路由器将丢弃该数据包。请注意，组播路由器不对静态路由执行此 RPF 检查。



注意：*图中未显示安全区段。*

NETSCREEN 设备上的组播路由

NetScreen 设备有两个预定义的虚拟路由器 (VR): trust-vr 和 untrust-vr。每个虚拟路由器均为具有其自身单播和组播路由表的单独路由选择组件。 (有关单播路由表的信息，请参阅第 1 页上的 “路由表和静态路由”。) 接收到内向组播数据包后， NetScreen 设备将使用组播路由表中的路由进行路由查找。

组播路由表

组播路由表由静态组播路由或通过组播路由协议学到的路由组成。NetScreen 设备使用组播路由表中的信息来转发组播信息流。 NetScreen 设备为虚拟路由器中的每个路由协议各提供了一个组播路由表。

组播路由表中含有路由协议的特定信息以及以下内容 :

- 以转发状态开头的各个条目。转发状态可采用下列格式之一 : (*, G) 或 (S, G)。 (*, G) 格式称为 “星号逗号 G” 条目，其中 * 表示任意源， G 为具体的组播组地址。(S, G) 格式称为 “S 逗号 G” 条目，其中 S 为源 IP 地址， G 为组播组地址。
- 上游和下游接口。
- 反向路径转发 (RPF) 邻居。

以下是 trust-vr 虚拟路由器中 PIM-SM 组播路由表的一个范例：

```
 trust-vr - PIM-SM routing table
---------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
---------------------------------------------------------------------------
Total PIM-SM mroutes: 2

(*, 236.1.1.1)  RP 20.20.20.10         00:06:24/-         Flags: LF
  Zone             : Untrust
  Upstream         : ethernet1/2         State          : Joined
  RPF Neighbor     : local               Expires        : -
  Downstream       :
  ethernet1/2  00:06:24/00:02:57  Join         0.0.0.0          FC

(20.20.20.200/24, 236.1.1.1)           00:06:24/00:00:36  Flags: TXLF  Register Prune
  Zone             : Untrust
  Proxy register   : (10.10.10.1, 238.1.1.1) of zone Trust
  Upstream         : ethernet1/1         State          : Joined
  RPF Neighbor     : local               Expires        : -
  Downstream       :
  ethernet1/2  00:06:24/-         Join         236.1.1.1          20.20.20.200 FC
```

静态组播路由

可定义从源到组播组的静态组播路由 (S, G)，或者将源和组播组中的其中一个用通配符来表示，也可两者都由通配符表示。静态组播路由通常用于传送组播数据，这些数据从 IGMP 路由器代理模式下的接口的主机转发到 IGMP 主机模式下的接口的上游路由器。 (有关 “IGMP 代理” 的信息，请参阅第 219 页上的 “IGMP 代理”。) 还可使用静态组播路由来支持区域间组播转发。可为具有任意输入和输出接口的 (S, G) 对创建静态路由。还可以创建一条静态组播路由，该路由的源或组播组或两者都通过通配符 0.0.0.0 来表示。配置静态路由时，入接口的组播组地址和出接口的组播组地址可以不同。

范例 : 配置静态组播路由

本例中，将配置一个从 IP 地址为 20.20.20.200 的源到组播组 238.1.1.1 的静态组播路由。对 NetScreen 设备进行配置，使其在出接口上可将组播组由 238.1.1.1 转换为 238.2.2.1。

WebUI

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

Source IP: 20.20.20.200

MGroup: 238.1.1.1

Incoming Interface: ethernet1 (选择)

Outgoing Interface: ethernet3 (选择)

Translated MGroup: 238.2.2.1

CLI

```
set vrouter trust-vr mroute mgroup 238.1.1.1 source 20.20.20.200 iif ethernet1
    oif ethernet3 out-group 238.2.2.1
save
```

访问列表

访问列表是有先后顺序的语句列表，当需要进行访问控制时，就将路由同该列表进行比较。每条语句指定网络前缀的 IP 地址 / 网络掩码以及转发状态 (允许或拒绝路由)。在组播路由中，语句还可包含组播组地址。在组播路由中，将创建访问列表来允许特定组播组或主机的组播信息流。因此，动作或转发状态始终为 “允许”。不能创建访问列表来拒绝某些组或主机。 (有关访问列表的其它信息，请参阅*第 56 页上的 “访问列表”*。)

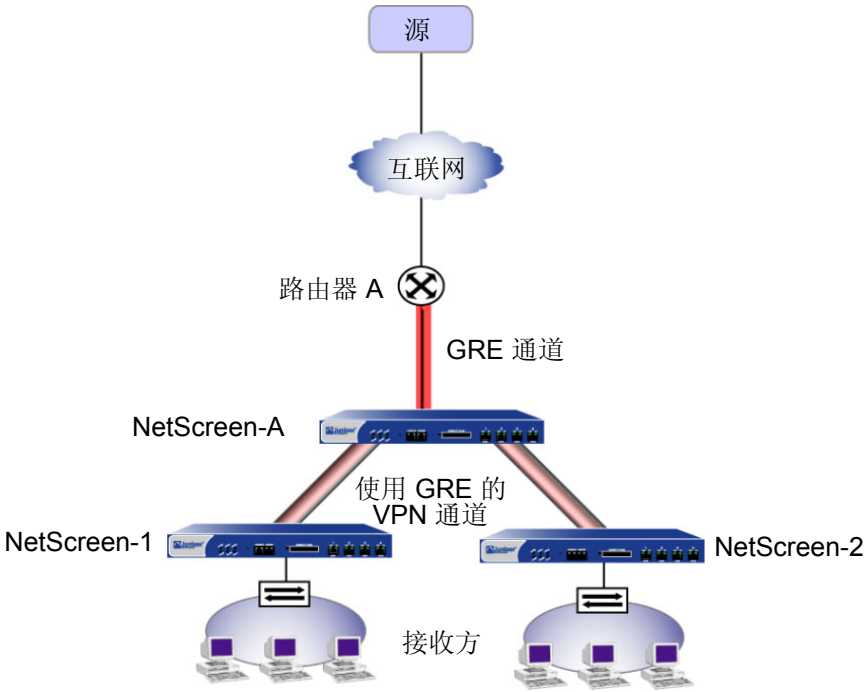
通用路由封装

在单播数据包中封装组播数据包是通过不支持组播的网络以及通过 IPSec 通道传送组播数据包所使用的常见方法。“通用路由封装” (GRE) 版本 1 是在 IPv4 单播数据包中封装任何类型数据包的一种机制。 NetScreen 设备支持在 IPv4 单播数据包中封装 IP 数据包的 GREv1。有关 GRE 的其它信息，请参阅 *RFC 1701, Generic Routing Encapsulation (GRE)*。

在 NetScreen 设备上，在通道接口上启用 GRE 封装。(请注意，只要回传接口与出接口位于同一区段中，即可在绑定到该回传接口的通道接口上启用 GRE。有关回传接口的信息，请参阅第 **2**-74 页上的 “回传接口”。) 在 NetScreen 设备和第三方设备或路由器间通过 IPSec VPN 通道传送组播数据包时，必须启用 GRE。

在 NetScreen 设备上，传送组播数据包所通过的出接口的数量受到具体平台的限制。在大型的星型 (hub-spoke)VPN 环境下，当 Netscreen 设备是做为中心 (Hub) 节点，可以通过在该 Netscreen 设备的上游路由器和末端 (Spoke) 处的 NetScreen 设备间创建一个 GRE 通道来避免此限制。

下图中，“路由器 A”为 NetScreen-A 的上游，“路由器 A”有两个终止于 NetScreen-1 和 NetScreen-2 的 GRE 通道。 NetScreen-A 通过 VPN 通道与 NetScreen-1 和 NetScreen-2 相连。“路由器 A”在传送组播数据包前，会先在 IPv4 单播数据包中对其进行封装。 NetScreen-A 将这些数据包作为单播数据包进行接收，然后通过 NetScreen-1 和 NetScreen-2 对其进行发送。



范例 : 配置 GRE 通道接口

在本例中，将在 NetScreen-1 上配置通道接口。将执行以下步骤 :

1. 创建 tunnel.1 接口并在 trust-vr 上将其绑定到 ethernet3 和 Untrust 区段。
2. 在 tunnel.1 上启用 GRE 封装。
3. 指定 GRE 通道的本地和远程端点。

本例仅介绍 NetScreen 设备的 GRE 配置。 (有关 VPN 的信息，请参阅第 5 卷，“VPN”。)

WebUI

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

Network > Interfaces > Tunnel (tunnel.1): 输入以下内容，然后单击 **Apply**:

Encap: GRE (选择)

Local Interface: ethernet3

Destination IP: 3.3.3.1

CLI

```
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.1 tunnel encap gre
set interface tunnel.1 tunnel local-if ethernet3 dst-ip 3.3.3.1
save
```

组播策略

在缺省情况下， NetScreen 设备不允许组播控制信息流 (如 IGMP 或 PIM 消息) 通过 NetScreen 设备。要允许组播控制信息流在区段间通过，必须配置一个指定以下内容的组播策略 :

- 源 – 信息流发起的区段
- 目的地址 – 信息流要发送到的区段
- 组播组 – NetScreen 设备将允许该组播组的控制信息通过防火墙。可指定以下内容之一 :
  - 组播组 IP 地址
  - 定义主机可加入的组播组的访问列表
  - 允许所有组播组的组播控制信息流的关键字 **any**
- 组播控制信息流 – 组播控制消息的类型 : IGMP 消息或 PIM 消息。 (有关 IGMP 的信息，请参阅第 205 页上的 “IGMP”。有关 PIM 的信息，请参阅第 247 页上的 “PIM”。)

此外，可指定以下内容 :

- 已转换的组播地址 – NetScreen 设备可在出口接口上将内部区段中的组播组地址转换为不同的地址。要转换组地址，必须在组播策略中指定初始组播地址和转换后的组播组地址。
- 双向 – 可创建双向策略以便将其应用到信息流的两个方向。

注意 : *组播策略仅控制组播控制信息流的流动。要允许 (单播和组播) 数据信息流在区段间通过，必须配置防火墙策略。 (有关策略的详细信息，请参阅第 2 卷，“基本原理”。)*

将不会象对防火墙策略进行排序那样对组播策略进行排序。因此，最新的组播策略不会覆盖先前的策略，以免出现冲突。相反， NetScreen 设备会进行最长匹配 (被其它路由协议使用) 来解决所有冲突。当查找到与请求相匹配的较小子网时，将使用该策略。

注意： *有关如何为 IGMP 消息配置组播策略的范例，请参阅第 225 页上的 “范例 : IGMP 的组播组策略”。有关如何为 PIM 消息配置组播策略的范例，请参阅第 262 页上的 “范例 : PIM-SM 的组播组策略”。*

7

IGMP

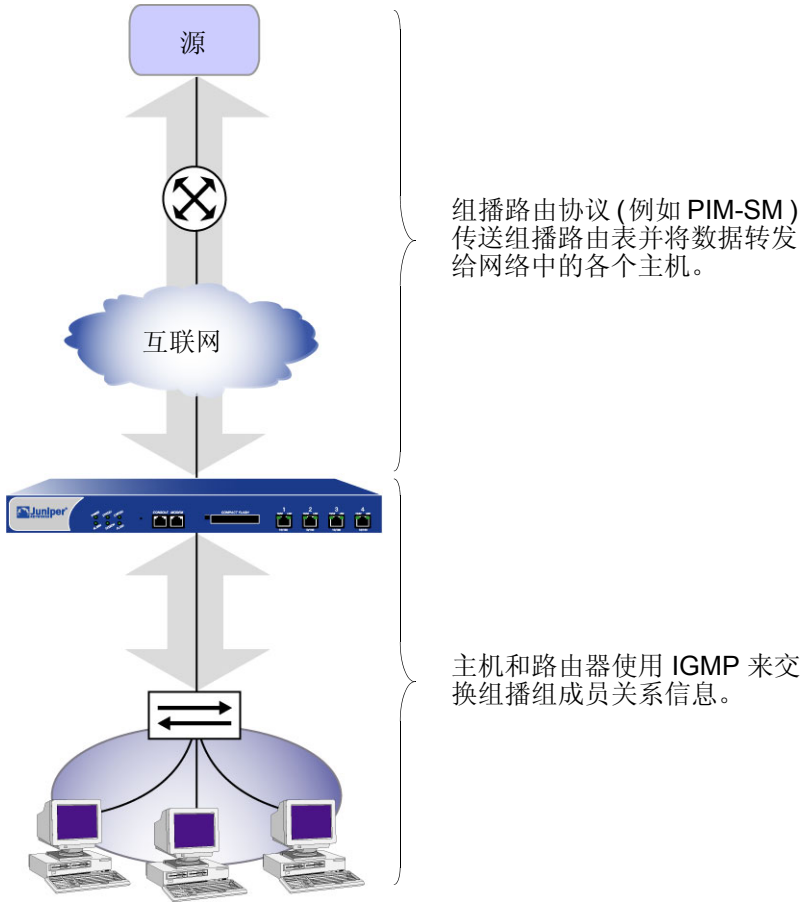
本章介绍 NetScreen 设备上的 “互联网组管理协议” (IGMP) 组播协议。本章包括以下几个部分：

IGMP 概述

通过在主机和路由器之间使用 “互联网组管理协议” (IGMP) 组播协议，可以在网络中建立并维护组播组成员关系。NetScreen 设备支持下列版本的 IGMP:

- 在 *RFC 1112, Host Extensions for IP Multicasting* 中定义的 IGMPv1，定义组播组成员关系的基本操作。
- 在 *RFC 2236, Internet Group Management Protocol, Version 2* 中定义的 IGMPv2，扩展了 IGMPv1 的功能。
- 在 *RFC 3376*, *Internet Group Management Protocol, Version 3* 中定义的 IGMPv3，添加了对源过滤的支持。运行 IGMPv3 的主机会指出它们要加入哪些组播组，以及它们要从哪里接收组播信息流的源。运行 “源特定组播中的协议无关组播” (PIM-SSM) 模式时， IGMPv3 是必需的。 (有关 PIM-SSM 的信息，请参阅第 302 页上的 “PIM-SSM”。)

IGMP 为主机和路由器维护组播组成员关系提供了一个机制。因而，组播路由协议 (例如 PIM) 处理来自 IGMP 的成员关系信息，在组播路由表中创建条目，并将组播信息流转发至网络上的各个主机。



以下各节将对不同类型的 IGMP 消息进行介绍，主机和路由器通过交换这些消息来维护网络上的组成员关系信息。运行较新 IGMP 版本的主机和路由器可以与运行较旧 IGMP 版本的主机和路由器一起使用。

主机

主机发送加入组播组的 IGMP 消息，并在这些组中维护它们的成员关系。路由器通过接听其本地网络上的这些 IGMP 消息来获知哪些主机是组播组的成员。下表对主机发送的 IGMP 消息进行了介绍。

IGMP 版本	IGMP 消息	目标
IGMPv1 和 v2	主机首次加入组播组时将发送成员关系报告，一旦其成为组成员后，则会定期发送成员关系报告。成员关系报告指出主机要加入哪个组播组。	主机所要加入的组播组的 IP 地址
IGMPv3	主机首次加入组播组时将发送成员关系报告，一旦其成为组成员后，则会定期发送成员关系报告。成员关系报告中含有组播组地址、过滤模式 (“包括”或“排除”) 以及源列表。如果过滤模式为“包括”，则会接受从源列表中的地址发出的数据包。如果过滤模式为 “排除”，则会接受从源列表中的源以外的源发出的数据包。	224.0.0.22
IGMPv2	当主机要离开组播组并将停止接收该组的数据时，它将发送 Leave Group 消息。	“所有路由器组” (224.0.0.2)

组播路由器

路由器使用 IGMP 来获知哪个组播组在其本地网络上具有成员。每个网络选择一个称为查询器[1] 的指定路由器。通常一个网络中具有一个查询器。查询器将 IGMP 消息发送给网络中的所有主机，以请求组成员关系信息。当主机响应它们的成员关系报告时，路由器会提取这些消息中的信息，并在每个接口上更新它们的组成员关系列表。IGMPv3 路由器负责维护含有组播组地址、过滤模式 (“包括”或 “排除”) 以及组播源的列表。

下表对查询器发送的消息进行了介绍。

IGMP 版本	IGMP 消息	目标
IGMPv1、 v2 和 v3	查询器定期发送一般查询以请求组成员关系信息。	“所有主机”组 (224.0.0.1)
IGMPv2 和 v3	当查询器收到 IGMPv2 Leave Group 消息或 IGMPv3 成员关系报告 (指出组成员关系中的更改) 时，它会发送组特定查询。如果查询器在指定时间间隔内未收到响应，则将假定在其本地网络上不再有该组的其它成员，并将停止转发该组的组播信息流。	主机要离开的组播组。
IGMPv3	查询器发送特定于组和源的查询，以检验该特定组和源是否具有任何接收方。	主机将离开的组播组。

1. 对于 IGMPv1，将由每个组播路由协议来确定网络的查询器。对于 IGMPv2 和 v3，具有网络中最小 IP 地址的路由器接口即为查询器。

NETSCREEN 设备上的 IGMP

在某些路由器上，当启用了组播路由协议后，会自动启用 IGMP。而在 NetScreen 设备上，必须明确启用 IGMP 和组播路由协议。

接口上的 IGMP

在缺省情况下，所有接口都将禁用 IGMP。必须在与主机相连的所有接口上于路由器模式下启用 IGMP。处于路由器模式时，在缺省情况下， NetScreen 设备将运行 IGMPv2。可以更改缺省值，并运行 IGMPv1、IGMPv2 和 v3，或只运行 IGMPv3。

范例：在接口上启用 IGMP

本例中，将在与主机相连的接口 ethernet1 上于路由器模式下启用 IGMP。

WebUI

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

CLI

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp enable
save
```

范例：在接口上禁用 IGMP

本例中，将在接口 ethernet1 上禁用 IGMP。 NetScreen 设备将保留 IGMP 配置，但将禁用该配置。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > IGMP: 清除 **Protocol IGMP Enable**，然后单击 **Apply**。

CLI

```
unset interface ethernet1 protocol igmp enable
save
```

要删除 IGMP 配置，请输入 **unset interface** *interface* **protocol igmp router** 命令。

安全注意事项

在运行 IGMP 时，有一些安全问题必须引起您的注意。恶意用户可能会伪造 IGMP 查询、成员关系报告以及离开消息。在 NetScreen 设备上，可以将组播信息流仅限于已知主机和组播组。此外，还可以在您的网络中指定所允许的查询器。可通过首先创建访问列表，然后再将其应用到某个接口的方法来设置这些限制。

访问列表是指定 IP 地址和转发状态 (permit 或 deny) 的有先后顺序的语句列表。在 IGMP 中，访问列表中必须始终具有一个为 “允许” 的转发状态，并且必须指定以下内容之一：

- 主机可以加入的组播组
- 从 IGMP 路由器接口接收 IGMP 消息的主机
- 从 IGMP 路由器接口接收 IGMP 消息的查询器

创建访问列表后，即可将其应用到某个接口。一旦将访问列表应用到了某个接口，该接口就会只接受访问列表中允许通过的信息流。因此，要拒绝来自特定组播组、主机或查询器的信息流，只需将其排除在访问列表之外即可。(有关访问列表的其它信息，请参阅第 56 页上的 “访问列表”。)

范例：为接受组配置访问列表

本例中，将在 trust-vr 上创建一个访问列表。该访问列表将指定以下内容：

- 访问列表 ID 为 1
- 允许组播组 224.4.4.1/32 的信息流
- 该语句的序列号为 1

创建该访问列表后，允许 ethernet1 上的主机加入该访问列表中所指定的组播组。

WebUI

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

Access List ID: 1

Sequence No: 1

IP/Netmask: 224.4.4.1/32

Action: Permit (选择)

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

Accept Group's Access List ID: 1

CLI

```
set vrouter trust-vr access-list 1 permit ip 224.4.4.1/32 1
set interface ethernet1 protocol igmp accept groups 1
save
```

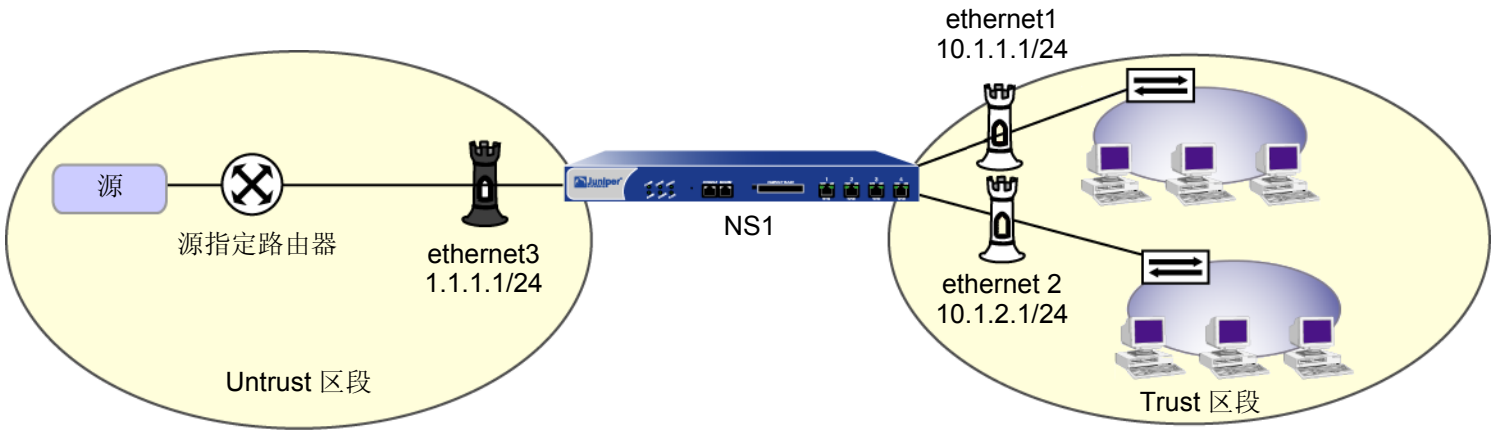
基本 IGMP 配置

要在 NetScreen 设备上运行 IGMP，只需在与主机直接相连的接口上于路由器模式下启用它即可。为了确保网络安全，请使用访问列表将组播信息流限制到已知组播组、主机和路由器。

范例：基本 IGMP 配置

在本例中，受 NetScreen 设备 NS1 保护的 Trust 区段中的主机是从 Untrust 区段中的源发出的组播流的潜在接收方。接口 ethernet1 和 ethernet2 与主机相连。组播源正在将数据传送到组播组 224.4.4.1 上。要在与主机相连的接口上配置 IGMP，请按以下步骤进行操作：

1. 将 IP 地址分配给接口，并将接口绑定到区段。
2. 创建指定了组播组 224.4.4.1/32 的访问列表。
3. 在 ethernet1 和 ethernet2 上于路由器模式下启用 IGMP。
4. 限制接口 (ethernet1 和 ethernet2) 只接收组播组 224.4.4.1/32 的 IGMP 消息。



WebUI

1. 区段和接口

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

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

Zone Name: Trust

IP Address/Netmask: 10.1.2.1/24

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

Zone Name: Untrust

IP Address/Netmask: 1.1.1.1/24

2. 访问列表

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 1

Sequence No: 1

IP/Netmask: 224.4.4.1/32

Action: Permit

3. IGMP

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Accept Group's Access List ID: 1

Network > Interfaces > Edit (对于 ethernet2) > IGMP: 输入以下内容，然后单击 **Apply**:

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Accept Group's Access List ID: 1

CLI

1. 区段和接口

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

set interface ethernet2 zone trust
set interface ethernet2 ip 10.2.1.1/24
```

2. 访问列表

```
set vrouter trust access-list 1 permit ip 224.4.4.1/32 1
```

3. IGMP

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp accept groups 1
set interface ethernet1 protocol igmp enable

set interface ethernet2 protocol igmp router
set interface ethernet2 protocol igmp accept groups 1
set interface ethernet2 protocol igmp enable
save
```

在 ethernet1 和 ethernet2 上配置 IGMP 后，必须配置组播路由协议 (例如 PIM) 以转发组播信息流。(有关 PIM 的信息，请参阅第 247 页上的 “PIM”。)

检验您的 IGMP 配置

要检验连通性并确保 IGMP 运行正常，可以使用多种 **exec** 和 **get** 命令。

- 要在特定接口上发送一般查询或组特定查询，请使用 **exec igmp interface** *interface* **query** 命令。例如，要从 ethernet2 发送一般查询，请输入：

  exec igmp interface ethernet2 query

  要将组特定查询从 ethernet2 发送到组播组 224.4.4.1，请输入：

  exec igmp interface ethernet2 query 224.4.4.1

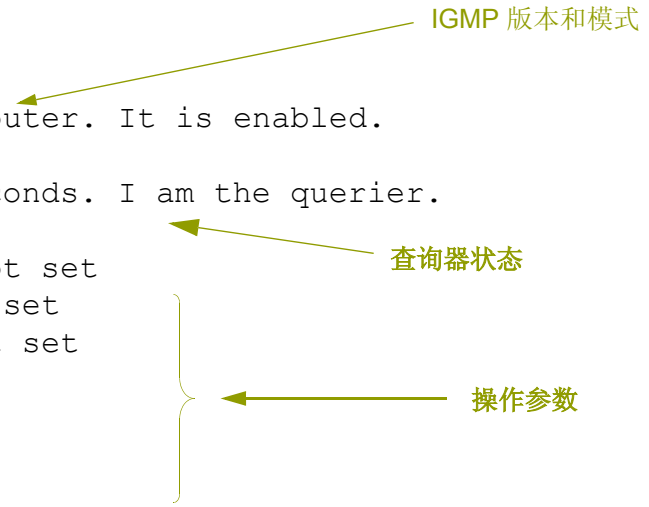
- 要在特定接口上发送成员关系报告，请使用 **exec igmp interface** *interface* **report** 命令。例如，要从 ethernet2 发送成员关系报告，请输入：

  exec igmp interface ethernet2 report 224.4.4.1

可通过输入以下命令来查看接口的 IGMP 参数：

```
ns-> get igmp interface

Interface trust support IGMP version 2 router. It is enabled.
IGMP proxy is disabled.
Querier IP is 10.1.1.90, it has up 23 seconds. I am the querier.
There are 0 multicast groups active.
    Inbound Router access list number: not set
    Inbound Host access list number: not set
    Inbound Group access list number: not set
    query-interval: 125 seconds
    query-max-response-time 10 seconds
    leave-interval 1 seconds
    last-member-query-interval 1 seconds
```



要显示有关组播组的信息，请输入以下 CLI 命令：

```
ns-> get igmp group
total groups matched: 1
multicast group  interface    last reporter   expire ver
*224.4.4.1       trust        0.0.0.0         ------ v2
```

IGMP 操作参数

在接口上于路由器模式下启用 IGMP 时，接口将作为查询器启动。作为查询器，接口将使用一些您可以对其进行更改的缺省值。当您在此级别上设置参数时，只会影响您指定的接口。下表对 IGMP 查询器接口参数及其缺省值进行了介绍。

IGMP 接口参数	说明	缺省值
General query interval	查询器接口将一般查询发送到 “所有主机” 组 (224.0.0.1) 的时间间隔。	125 seconds
Maximum response time	一般查询和主机发出响应之间的最大时间。	10 seconds
Last Member Query Interval	接口发送 “组特定” 查询的时间间隔。如果在第二个 “组特定” 查询后接口未收到响应，则它会假定在其本地网络上不再有该组的其它成员。	1 second

在缺省情况下，启用了 IGMPv2/v3 的路由器只接受具有 router-alert IP 选项的 IGMP 数据包，并且会丢弃不具有该选项的数据包。由于 IGMPv1 数据包不具有该选项，因此，在缺省情况下运行 IGMPv2/v3 的 NetScreen 设备会丢弃 IGMPv1 数据包。可以对 NetScreen 设备进行配置，使其停止检查 IGMP 数据包是否具有 router-alert IP 选项，并接受所有 IGMP 数据包，同时允许 IGMPv1 路由器向后兼容。例如，要允许 ethernet1 接口接受所有 IGMP 数据包 :

WebUI

Network > Interfaces > Edit (对于 ethernet1) > IGMP: 选择以下内容，然后单击 **OK**:

Packet Without Router Alert Option: Permit (选择)

CLI

```
set interface ethernet1 protocol igmp no-check-router-alert
save
```

IGMP 代理

路由器监听 IGMP 消息，并只将这些消息发送到路由器所连接的主机；路由器不会将 IGMP 消息转发到其本地网络之外的网络。通过启用 IGMP 代理，可以允许 NetScreen 设备上的接口转发 IGMP 消息超出其本地网络一个跳。IGMP 代理使得接口可将 IGMP 消息向上游转发到源，而不需组播路由协议的 CPU 系统开销。

当在 NetScreen 设备上运行 IGMP 代理时，与主机相连的接口起到了路由器的作用，而与上游路由器相连的接口起到了主机的作用。主机和路由器接口通常位于不同的区段中。要允许在区段间传送 IGMP 消息，必须配置组播策略。之后，要允许在区段间传送组播数据信息流，还必须配置防火墙策略。

在支持多个虚拟系统的设备上，必须在根虚拟系统 (vsys) 中配置一个接口，而在单独的 vsys 中配置另一个接口。然后，创建允许组播控制信息流在两个虚拟系统之间通过的组播策略。(有关虚拟系统的信息，请参阅第 5 卷，“VPN”。)

因为接口转发 IGMP 成员关系信息，所以它们在其所绑定的虚拟路由器的组播路由表中创建条目，同时构建从接收方至源的组播分布树。以下各节将介绍 IGMP 主机和路由器接口如何将 IGMP 成员关系信息向上游转发给源，以及它们如何将组播数据从源向下游转发至接收方。

将成员关系报告向上游发送给源

与 NetScreen 设备上的路由器接口相连的主机加入组播组时，它会将成员关系报告发送到组播组。当路由器接口收到来自相连主机的成员关系报告时，它会检查其是否具有组播组的条目。然后， NetScreen 设备会采取下列操作之一：

- 如果路由器接口具有组播组的条目，则它会忽略成员关系报告。
- 如果路由器接口不具有组播组的条目，则它会检查是否具有该组的组播策略，该策略指定路由器接口应将报告发送到哪个区段。
  - 如果没有该组的组播策略，则路由器接口不会转发报告。
  - 如果有该组的组播策略，则路由器接口将创建组播组的条目，并将成员关系报告转发到组播策略中指定的区段中的代理主机接口。

当代理主机接口收到成员关系报告时，它会检查其是否具有该组播组的 (*, G) 条目。

- 如果具有该组的 (*, G) 条目，则主机接口会将路由器接口添加到该条目的出口接口列表中。
- 如果不具有该组的 (*, G) 条目，则将创建这样一个条目；入口接口是代理主机接口，出口接口是路由器接口。然后，代理主机接口会将报告转发到其上游路由器。

将组播数据向下游发送到接收方

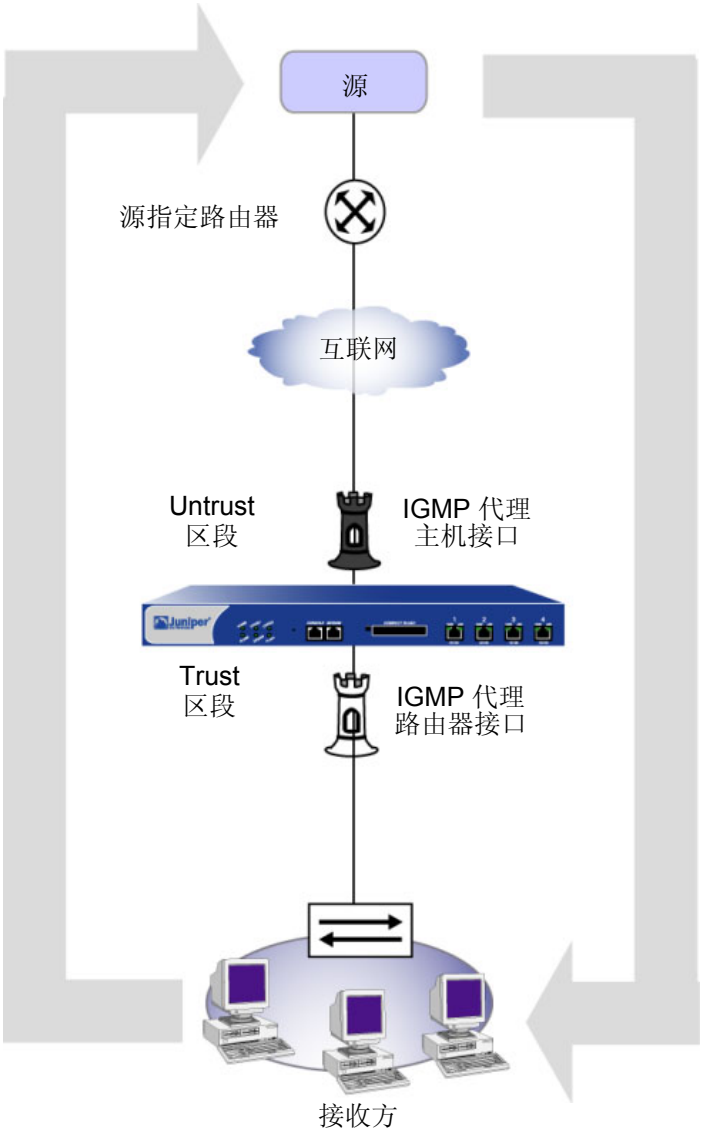
当 NetScreen 设备上的主机接口收到组播组的组播数据时，它会检查是否有该组的现有会话。

- 如果有该组的会话，则接口将根据会话信息转发组播数据。
- 如果没有该组的会话，则接口将检查该组是否在组播路由表中具有 (S, G) 条目。
  - 如果有 (S, G) 条目，则接口将相应地转发组播数据。
  - 如果没有 (S, G) 条目，则接口将检查是否有该组的 (*, G) 条目。
    - 如果没有该组的 (*, G) 条目，则接口将丢弃数据包。
    - 如果有该组的 (*, G) 条目，则接口将创建 (S, G) 条目。当接口收到该组的后续组播数据包时，它会将信息流转发到路由器接口 (出口接口)，而路由器接口会将该信息流依次转发到其所连接的主机。

3. IGMP 代理主机接口检查其是否具有组播组的 (*,G) 条目：
   - 如果有，则会将路由器接口添加到组播路由表条目的出接口中。
   - 如果没有，则会创建条目，并将成员关系报告转发到上游路由器。

2. IGMP 代理路由器接口检查组播组的条目：
   - 如果有，则将忽略成员关系报告。
   - 如果没有，并且没有该组的组播策略，则将丢弃成员关系报告。
     - 如果没有，但有该组的组播策略，则将在组播路由表中创建 (*,G) 条目，其中将主机作为 iif，将路由器作为 oif。它会将报告向上游转发到组播策略中指定的区段上的主机接口。

1. 主机向上游发送成员关系报告。



4. 源将组播数据向下游发送到接收方。

5. IGMP 代理主机接口检查该组的现有会话：
   - 如果有，则会转发组播数据。
   - 如果没有，则会检查该组的 (S,G) 条目：
     - 如果有，则会转发组播数据。
     - 如果没有，则会检查 (*, G) 条目：
       - 如果没有，将丢弃数据。
       - 如果有，将使用 (*, G) 条目的现有入和出接口，创建 (S, G) 条目，并转发数据。

6. IGMP 代理路由器接口将数据转发到接收方。

配置 IGMP 代理

本节介绍在 NetScreen 设备上配置 IGMP 代理所需的基本步骤：

1. 主机模式下，在上游接口上启动 IGMP。在缺省情况下，主机接口将启动 IGMP 代理。
2. 路由器模式下，在下游接口上启动 IGMP。
3. 启用路由器接口上的 IGMP 代理。
4. 配置允许组播控制信息流在区段间通过的组播策略。
5. 配置数据信息流在区段间通过的策略。

接口上的 IGMP 代理

在 NetScreen 设备上运行 IGMP 代理时，将下游接口配置为处于路由器模式，将上游接口配置为处于主机模式。(注意，接口既可以处于主机模式也可以处于路由器模式，但不能同时处于两种模式下。) 另外，对于转发组播信息流的路由器接口，它必须是本地网络中的查询器。要允许非查询器接口转发组播信息流，在启用接口上的 IGMP 时，必须指定关键字 **always**。

在缺省情况下，IGMP 接口只接受来自其自身子网的 IGMP 消息。而会忽略来自外部源的 IGMP 消息。运行 IGMP 代理时，必须使 NetScreen 设备能够接受从其它子网中的源发出的 IGMP 消息。

范例：接口上的 IGMP 代理

本例中，接口 ethernet1 的 IP 地址为 10.1.2.1/24，并且与上游路由器相连。将对 ethernet1 进行如下配置：

- 在主机模式下启用 IGMP
- 允许该接口接受来自所有源的 IGMP 消息，而不管子网如何

接口 ethernet3 的 IP 地址为 10.1.1.1/24，并与主机相连。将对 ethernet3 进行如下配置：

- 在路由器模式下启用 IGMP
- 即使该接口不是查询器，也允许它转发组播信息流
- 允许该接口接受从其它子网上的源发出的 IGMP 消息

WebUI

1. 区段和接口

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

Zone Name: Trust

IP Address/Netmask: 10.1.2.1/24

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

Zone Name: Trust

IP Address/Netmask: 10.1.1.1/24

2. IGMP

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

IGMP Mode: Host (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

Proxy: (选择)

Always (选择)

CLI

1. 区段和接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.2.1/24
set interface ethernet3 zone trust
set interface ethernet1 ip 10.1.1.1/24
```

2. IGMP

```
set interface ethernet1 protocol igmp host
set interface ethernet1 protocol igmp enable
set interface ethernet1 protocol igmp no-check-subnet
set interface ethernet3 protocol igmp router
set interface ethernet3 protocol igmp proxy
set interface ethernet3 protocol igmp proxy always
set interface ethernet3 protocol igmp enable
set interface ethernet3 protocol igmp no-check-subnet
save
```

创建组播策略

通常， NetScreen 设备只与其所连接的主机交换 IGMP 消息。对于 IGMP 代理， NetScreen 设备可能需要将 IGMP 消息发送到另一区段中的主机或路由器。要允许跨区段发送 IGMP 消息，必须配置明确允许进行此操作的组播策略。创建组播策略时，必须指定下列内容：

- 源 – 发起信息流的区段
- 目标 – 信息流要发送到的区段
- 组播组 – 可以是组播组、指定组播组的访问列表，或 “any”

此外，可以将策略指定为双向的，以便将策略应用到信息流的两个方向。

范例：IGMP 的组播组策略

本例中，路由器接口位于 Trust 区段，而主机接口位于 Untrust 区段。定义组播策略，该策略允许组播组 224.2.202.99/32 的 IGMP 消息在 Trust 和 Untrust 区段间通过。使用关键字 bi-directional，以允许双向信息流。

WebUI

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

MGroup Address: IP / Netmask (选择) 224.2.202.99/32

Bidirectional: (选择)

IGMP Message: (选择)

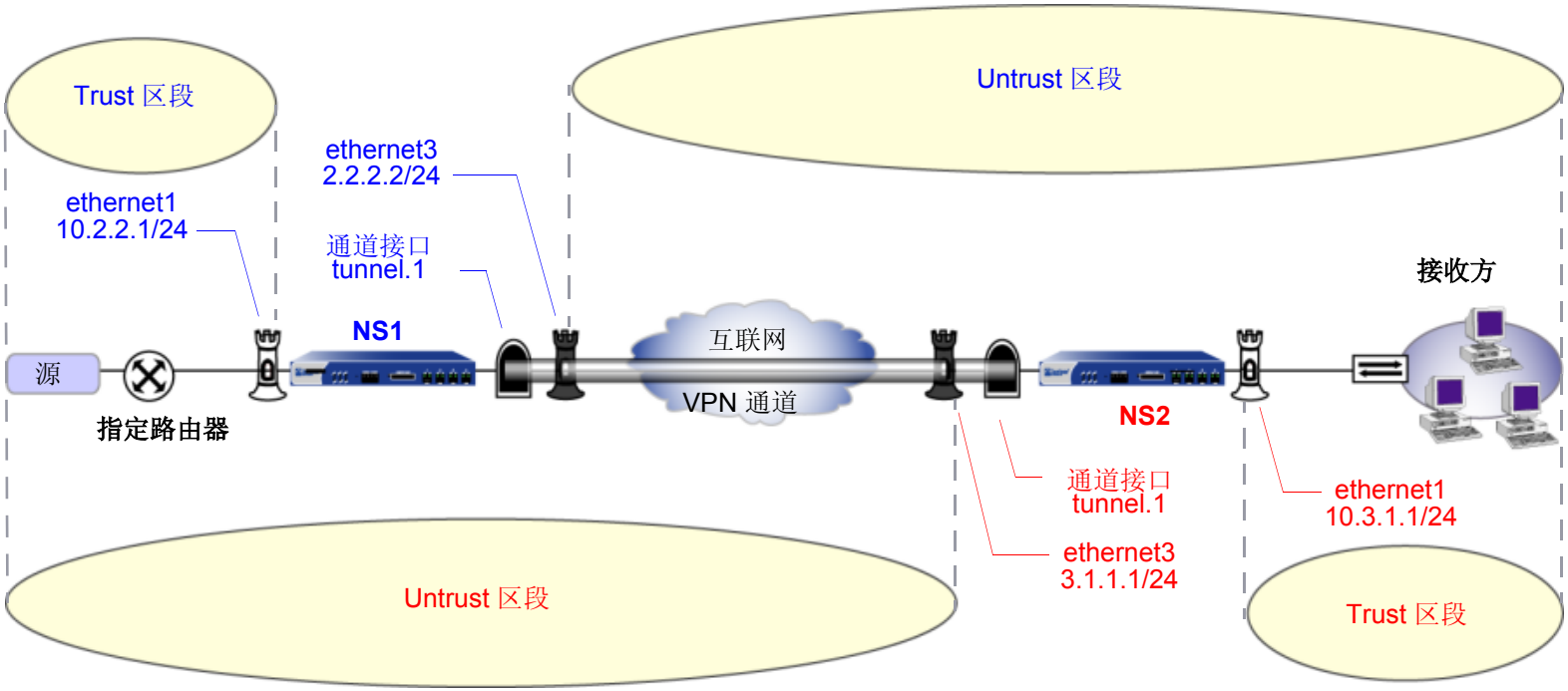
CLI

```
set multicast-group-policy from trust mgroup 224.2.202.99/32 to untrust
    igmp-message bi-directional
save
```

范例 : 基本 IGMP 代理配置

本例中，将在 NetScreen 设备 NS1 和 NS2 上配置 IGMP 代理。 NS1 与 NS2 通过 VPN 通道相连。在两个位置的 NetScreen 设备上执行下列步骤 :

1. 将 IP 地址分配给绑定到安全区段的物理接口。
2. 创建地址对象。
3. 启用主机和路由器接口上的 IGMP，并启用路由器接口上的 IGMP 代理。 (在缺省情况下，主机接口上的将启用 IGMP 代理。)
   - 在 NS1 的 ethernet1 上指定关键字 **always**，这样，即使该接口不是查询器，也会允许它转发组播信息流。
   - 在缺省情况下， IGMP 接口只接受来自其自身子网的 IGMP 数据包。本例中，接口位于不同的子网中。启用 IGMP 时，允许接口接受来自所有子网的 IGMP 数据包 (查询、成员关系报告和离开消息)。
4. 设置路由。
5. 配置 VPN 通道。
6. 配置数据信息流在区段间通过的防火墙策略。
7. 配置 IGMP 消息在区段间通过的组播策略。本例中，将组播信息流限制到一个组播组 (224.4.4.1/32)。



WebUI (NS1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: branch

IP Address/Domain Name:

IP/Netmask: (选择), 10.3.1.0/24

Zone: Untrust

3. IGMP

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

IGMP Mode: Host (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

Proxy (选择): Always (选择)

4. 路由

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

Network Address / Netmask: 10.3.1.0 / 24

Gateway (选择):

Interface: tunnel.1 (选择)

5. VPN

VPN > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: To_Branch

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 3.1.1.1

Preshared Key: fg2g4h5j

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: Compatible

Phase 1 Proposal (for Compatible Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

6. 策略

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

Source Address:

Address Book Entry: (选择), branch

Destination Address:

Address Book Entry: (选择), any (选择)

Service: any

Action: Permit

7. 组播策略

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

Mgroup Address: IP / Netmask (选择): 224.4.4.1/32

Bidirectional: (选择)

IGMP Message: (选择)

WebUI (NS2)

1. 接口

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

Zone Name: Trust

IP Address/Netmask: 10.3.1.1/24

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

Zone Name: Untrust

IP Address/Netmask: 3.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: mgroup1

IP Address/Domain Name:

IP/Netmask: (选择), 224.4.4.1/32

Zone: Trust

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

Address Name: source-dr

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.1/24

Zone: Untrust

3. IGMP

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Proxy (选择): Always (选择)

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

IGMP Mode: Host (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

4. 路由

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

Network Address / Netmask: 10.2.2.0 / 24

Gateway (选择):

Interface: tunnel.1 (选择)

5. VPN

VPN > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: To_Corp

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

Preshared Key: fg2g4hvj

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: Compatible

Phase 1 Proposal (for Compatible Security Level):
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

6. 策略

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

Source Address:

Address Book Entry: (选择), source-dr

Destination Address:

Address Book Entry: (选择), mgroup1

Service: ANY

Action: Permit

7. 组播策略

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

Mgroup Address: IP/Netmask (选择): 224.4.4.1/32

Bidirectional: (选择)

IGMP Message: (选择)

CLI (NS1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address untrust branch1 10.3.1.0/24
```

3. IGMP

```
set interface ethernet1 protocol igmp host
set interface ethernet1 protocol igmp enable
set interface ethernet1 protocol igmp no-check-subnet
set interface tunnel.1 protocol igmp router
set interface tunnel.1 protocol igmp proxy
set interface tunnel.1 protocol igmp proxy always
set interface tunnel.1 protocol igmp enable
set interface tunnel.1 protocol igmp no-check-subnet
```

4. 路由

```
set route 10.3.1.0/24 interface tunnel.1
```

5. VPN 通道

```
set ike gateway To_Branch address 3.1.1.1 main outgoing-interface ethernet3
    preshare fg2g4h5j proposal pre-g2-3des-sha
set vpn Corp_Branch gateway To_Branch sec-level compatible
set vpn Corp_Branch bind interface tunnel.1
set vpn Corp_Branch proxy-id local-ip 10.2.2.0/24 remote-ip 10.3.1.0/24 any
```

6. 策略

```
set policy name To_Branch from untrust to trust branch1 any any permit
```

7. 组播策略

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
    igmp-message bi-directional
save
```

CLI (NS2)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.3.1.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 3.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust mgroup1 224.4.4.1/32
set address untrust source-dr 10.2.2.1/24
```

3. IGMP

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp proxy
set interface ethernet1 protocol igmp proxy always
set interface ethernet1 protocol igmp enable
set interface tunnel.1 protocol igmp host
set interface tunnel.1 protocol igmp enable
set interface tunnel.1 protocol igmp no-check-subnet
```

4. 路由

```
set route 10.2.2.0/24 interface tunnel.1
```

5. VPN 通道

```
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface ethernet3
    preshare fg2g4hvj proposal pre-g2-3des-sha
set vpn Branch_Corp gateway To_Corp sec-level compatible
set vpn Branch_Corp bind interface tunnel.1
set vpn Branch_Corp proxy-id local-ip 10.3.1.0/24 remote-ip 10.2.2.0/24 any
```

6. 策略

```
set policy from untrust to trust source-dr mgroup1 any permit
```

7. 组播策略

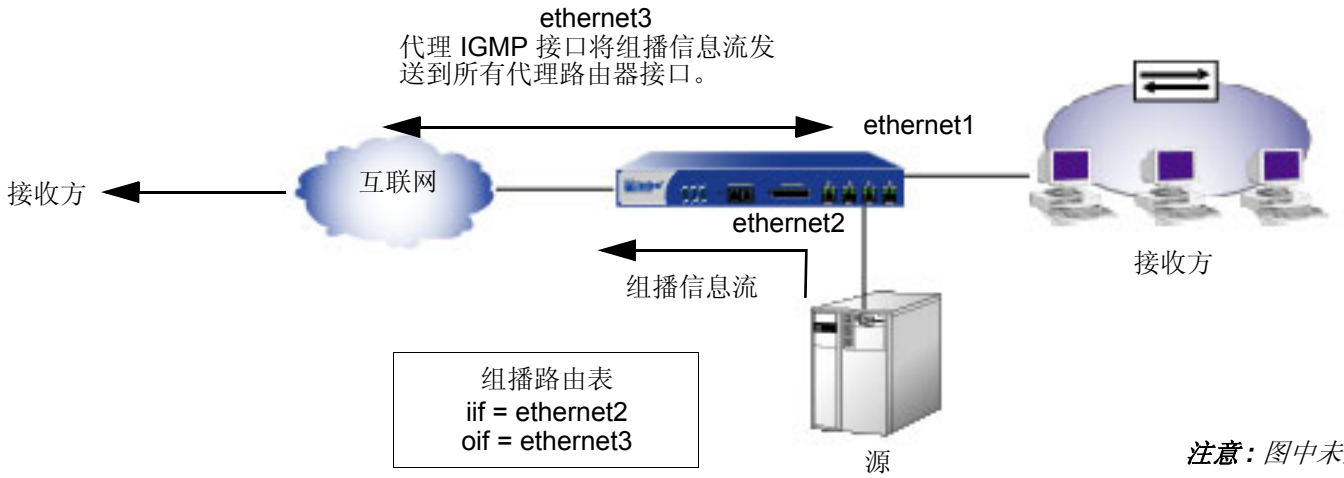
```
set multicast-group-policy from untrust mgroup 224.4.4.1/32 to trust
    igmp-message bi-directional
save
```

IGMP 发送方代理

在 IGMP 代理中，组播信息流通常从主机接口向下游流向路由器接口。在某些情况下，源可能与路由器接口位于同一网络中。当与某个接口相连接的源 (该源与 IGMP 路由器代理接口位于同一网络中) 发送组播信息流时，NetScreen 设备将检查下列内容 :

- 允许信息流从源区段流向 IGMP 代理主机接口所在区段的组播组策略
- 可接受源的访问列表

如果不存在源区段与代理 IGMP 接口所在区段间的组播策略，或者源未在可接受源的列表中，则 NetScreen 设备将丢弃信息流。如果存在源区段与代理 IGMP 接口所在区段间的组播策略，并且源在可接受源的列表中，则设备将在组播路由表中为该接口创建一个 (S,G) 条目 ; 入接口是源所连接的接口，而出接口是 IGMP 代理主机接口。然后，NetScreen 设备将数据向上游发送到 IGMP 代理主机接口，该接口将数据发送到其所连接的所有代理路由器接口 (与源相连的接口除外)。



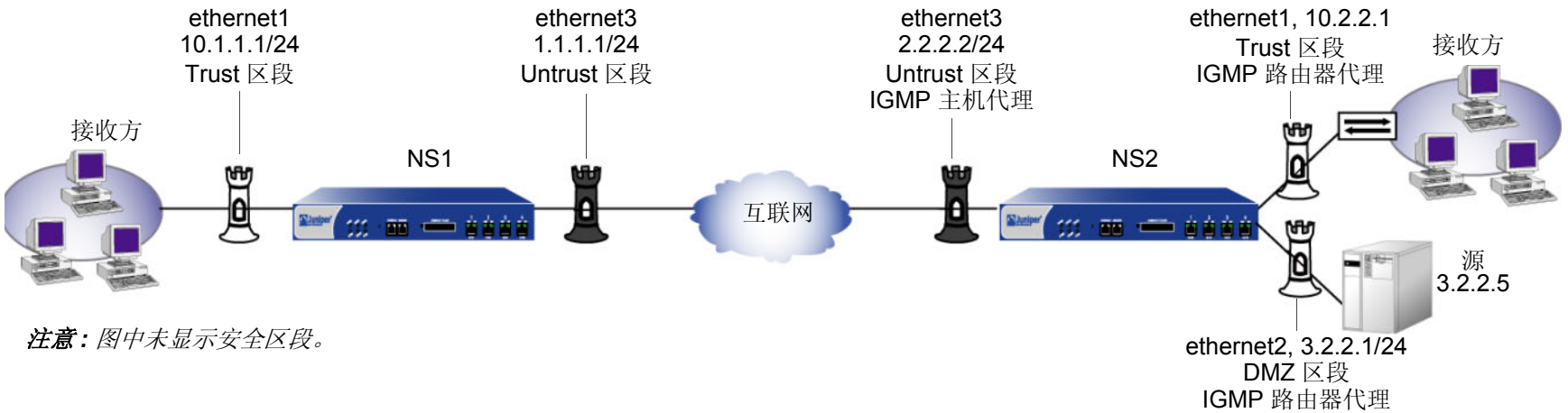
注意 : *图中未显示安全区段。*

范例 : IGMP 发送方代理

本例中，源与 ethernet2 接口相连，该接口被绑定到了 NS2 上的 DMZ 区段。源将组播信息流发送到组播组 224.4.4.1/32。有连接到 ethernet1 接口的接收方，该接口被绑定到了 NS2 上的 Trust 区段。ethernet 1 和 ethernet2 均为 IGMP 代理路由器接口。而绑定到 NS2 的 Untrust 区段的 ethernet3 接口是 IGMP 代理主机接口。也有连接到 ethernet1 接口的接收方，该接口被绑定到了 NS1 的 Trust 区段。在 NS2 上执行下列步骤 :

1. 将 IP 地址分配给绑定到安全区段的接口。
2. 创建地址对象。
3. 在 ethernet1 和 ethernet2 上 :
   - 在路由器模式下启用 IGMP 并启用 IGMP 代理。
   - 指定关键字 **always**，这样，即使接口不是查询器，它们也可转发组播信息流。
4. 在 ethernet3 上于主机模式下启用 IGMP。
5. 设置缺省路由。
6. 配置区段间的防火墙策略。
7. 配置区段间的组播策略。

> ***注意 :*** *本例仅就 NS2 的配置进行介绍，而对 NS1 的配置不做介绍。*



注意 : *图中未显示安全区段。*

WebUI (NS2)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.2.2.1/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

2. 地址

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

Address Name: mgroup1

IP Address/Domain Name:

IP/Netmask: (选择), 224.4.4.1/32

Zone: Trust

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

Address Name: source-dr

IP Address/Domain Name:

IP/Netmask: (选择), 3.2.2.5/32

Zone: DMZ

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

Address Name: proxy-host

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.2/32

Zone: Untrust

3. IGMP

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Proxy (选择): Always (选择)

Network > Interfaces > Edit (对于 ethernet2) > IGMP: 输入以下内容，然后单击 **Apply**:

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

Proxy (选择): Always (选择)

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

IGMP Mode: Host (选择)

Protocol IGMP: Enable (选择)

Packet From Different Subnet: Permit (选择)

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

5. 策略

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

Source Address:

Address Book Entry: source-dr

Destination Address:

Address Book Entry: (选择), mgroup1

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), source-dr

Destination Address:

Address Book Entry: (选择), mgroup1

Service: ANY

Action: Permit

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

Source Address:

Address Book Entry: (选择), proxy-host

Destination Address:

Address Book Entry: (选择), mgroup1

Service: ANY

Action: Permit

6. 组播策略

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

Mgroup Address: IP/Netmask (选择): 224.4.4.1/32

Bidirectional: (选择)

IGMP Message: (选择)

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

Mgroup Address: IP/Netmask (选择): 224.4.4.1/32

Bidirectional: (选择)

IGMP Message: (选择)

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

Mgroup Address: IP/Netmask (选择): 224.4.4.1/32

Bidirectional: (选择)

IGMP Message: (选择)

CLI (NS2)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet2 zone dmz
set interface ethernet2 ip 3.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. 地址

```
set address trust mgroup1 224.4.4.1/32
set address dmz source-dr 3.2.2.5/32
set address untrust proxy-host 2.2.2.2/32
```

3. IGMP

```
set interface ethernet1 protocol igmp router
set interface ethernet1 protocol igmp proxy always
set interface ethernet1 protocol igmp enable

set interface ethernet2 protocol igmp router
set interface ethernet2 protocol igmp proxy always
set interface ethernet2 protocol igmp enable

set interface ethernet3 protocol igmp host
set interface ethernet3 protocol igmp no-check-subnet
set interface ethernet3 protocol igmp enable
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

5. 策略

```
set policy from dmz to trust source-dr mgroup1 any permit
set policy from dmz to untrust source-dr mgroup1 any permit
set policy from untrust to trust proxy-host mgroup1 any permit
```

6. 组播策略

```
set multicast-group-policy from dmz mgroup 224.4.4.1/32 to untrust igmp-message
    bi-directional
set multicast-group-policy from dmz mgroup 224.4.4.1/32 to trust igmp-message
    bi-directional
set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
    igmp-message bi-directional
save
```

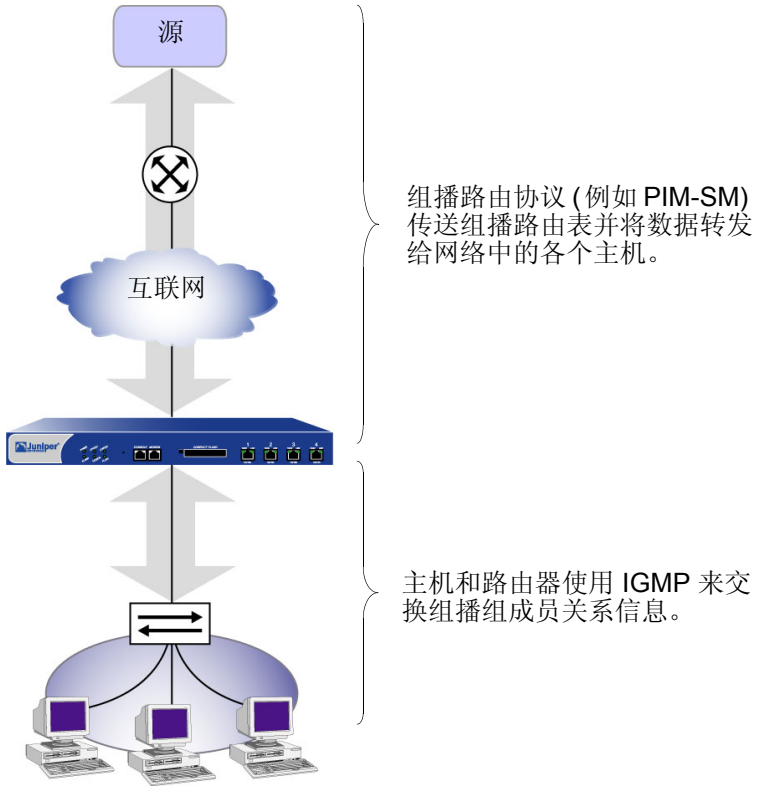
8

PIM

本章介绍 NetScreen 设备上的 “协议无关组播” 协议。本章包括以下几个部分：

PIM 概述

“协议无关组播” (PIM) 是在路由器间运行的组播路由协议。“互联网组管理协议” (IGMP) 在主机和路由器间运行，以交换组播组成员关系信息；而 PIM 在路由器间运行，以将组播信息流转发到整个网络中的组播组成员。 (有关 IGMP 的信息，请参阅第 205 页上的 “IGMP”。)



当您运行 PIM 时，必须同时配置静态路由或动态路由协议。因为 PIM 使用底层单播路由协议的路由表来执行其 RPF (反向路径转发) 检查，但却不依赖于单播路由协议的功能，所以 PIM 称为 “协议无关”。 (有关 RPF 的信息，请参阅第 195 页上的 “反向路径转发”。)

PIM 可在下列模式下运行：

- “PIM 密集模式” (PIM-DM) 在整个网络中洪泛组播信息，然后对没有接收主机的路由进行裁剪。
- “PIM 稀疏模式” (PIM-SM) 将组播信息流仅转发到请求该信息流的接收方。运行 PIM-SM 的路由器可使用共享路径树或最短路径树 (SPT) 来转发组播信息。(有关组播分布树的信息，请参阅第 251 页上的 “组播分布树”。)
  - “PIM 源特定组播模式”(PIM-SSM) 源自 PIM-SM。与 PIM-SM 类似，该模式也将组播信息流仅转发到特定接收方。与 PIM-SM 不同的是，该模式会立即形成到源的 SPT。

  NetScreen 设备支持 *draft-ietf-pim-sm-v2-new-06* 中所定义的 PIM-SM 以及 *RFC 3569, An Overview of Source-Specific Multicast (SSM)* 中所定义的 PIM-SSM。有关 PIM-SM 的信息，请参阅第 250 页上的 “PIM-SM”。有关 PIM-SSM 的信息，请参阅第 302 页上的 “PIM-SSM”。

PIM-SM

PIM-SM 是将组播信息流仅转发到特定接收方的组播路由协议。该协议可使用共享分布树或最短路径树 (SPT) 在整个网络中转发组播信息流。(有关组播分布树的信息，请参阅第 251 页上的 “组播分布树”。) 在缺省情况下，PIM-SM 使用在其根部具有一个汇聚点 (RP) 的共享分布树。组中的所有源先将其数据包发送到 RP，然后再由 RP 将这些数据沿共享分布树向下发送给网络中的所有接收方。当达到临界值时 （该数值可以被设置），接收方会形成到源的 SPT，这就缩短了接收方接收组播数据的时间。

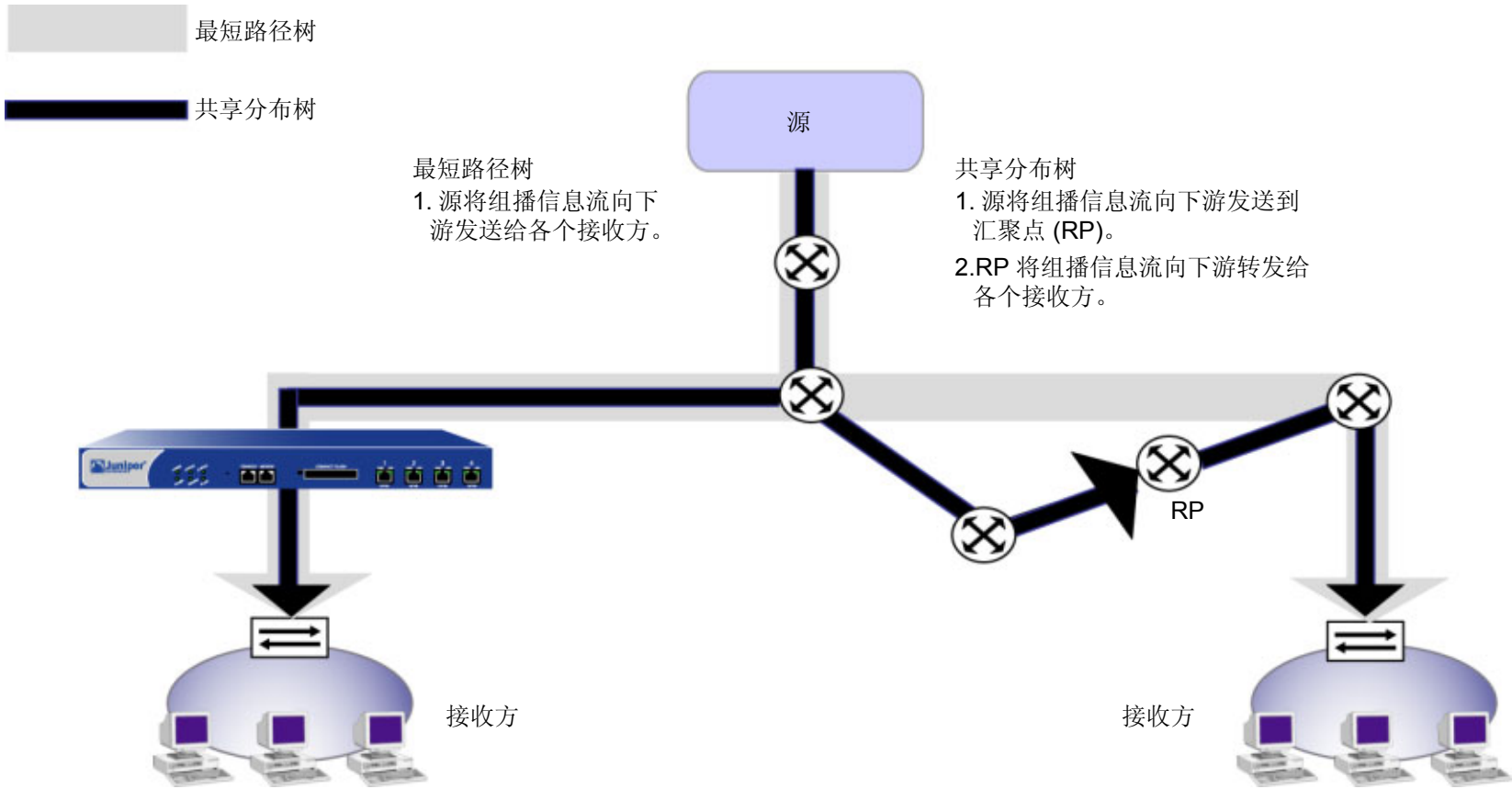
***注意：**在缺省情况下， NetScreen 设备会在收到第一个字节时切换为 SPT。*

不管使用那种类型的树来发送信息流，只有明确加入某个组播组的接收方才能接收该组的信息流。当收到组播控制消息并使用组播路由表向接收方发送组播数据信息流时， PIM-SM 将使用单播路由表来执行其反向路径转发 (RPF) 查找。

组播分布树

组播路由器通过组播分布树将组播信息流从源向下游转发到接收方。有两种类型的组播分布树：

- 最短路径树 (SPT) - 源位于树的根部，并由源将组播数据向下游转发给每个接收方。该类型的分布树也称作源特定树。
- 共享分布树 - 源将组播信息流传送到汇聚点 (RP)，该汇聚点通常为处于网络核心位置的路由器。然后再由 RP 将信息流向下游转发给分布树上的各个接收方。



指定路由器

当多路访问局域网 (LAN) 中存在多个组播路由器时，这些路由器将选举产生一个指定路由器 (DR)。源所在 LAN 上的 DR 负责将组播数据包从源发送到 RP 以及发送到位于源特定分布树上的各个接收方。接收方所在 LAN 上的 DR 负责将 join-prune 消息从接收方转发到 RP，并且负责将组播数据信息流发送给该 LAN 中的各个接收方。当接收方要加入或退出组播组时，它们会发送 join-prune 消息。

通过选择过程来选定 DR。LAN 中的每个 PIM-SM 路由器都各有一个用户可配置的 DR 优先级。PIM-SM 路由器在其定期发送给邻接路由器的 hello 消息中通告它们的 DR 优先级。当路由器收到 hello 消息时，会选择具有最高 DR 优先级的路由器作为 LAN 的 DR。如果存在多个具有最高 DR 优先级的路由器，则具有最高 IP 地址的路由器将成为 LAN 的 DR。

将汇聚点映射到组

汇聚点 (RP) 发送特定组播组的组播数据包。 PIM-SM 域是一组具有相同 RP-group 映射的 PIM-SM 路由器。可使用两种方式将组播组映射到 RP: 静态映射和动态映射。

静态 RP 映射

要在 RP 和组播组之间创建静态映射，必须为网络中每个路由器上的组播组配置 RP。每次更改 RP 的地址时，都必须重新配置 RP 地址。

动态 RP 映射

PIM-SM 还提供将 RP 动态映射到组播组的机制。首先，为每个组播组配置候选汇聚点 (C-RP)。然后， C-RP 再将 Candidate-RP 通告发送给 LAN 中一个被称为自举路由器 (BSR) 的路由器。通告中含有组播组 (路由器将成为该组的 RP) 和 C-RP 的优先级。

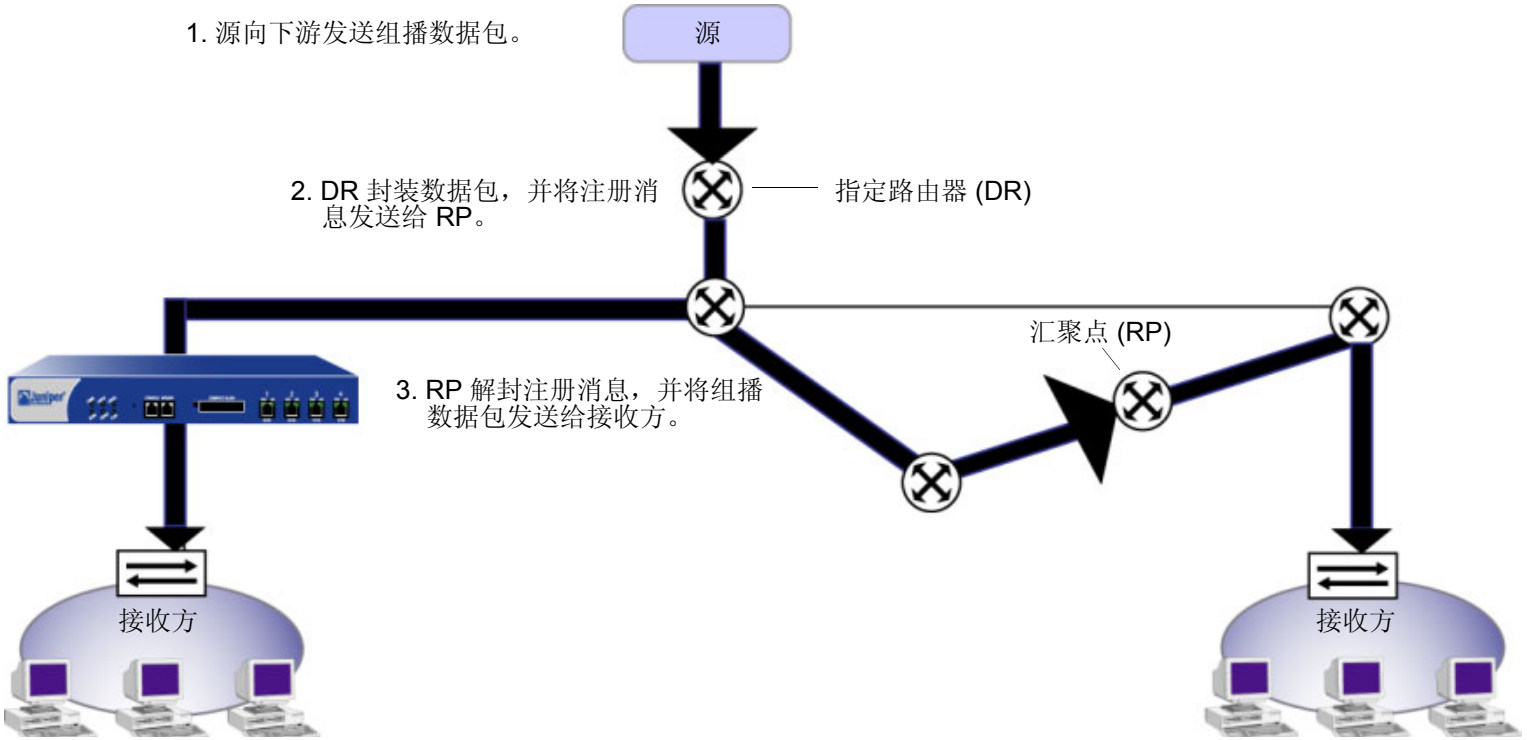
BSR 收集这些 C-RP 通告，然后再将它们以 BSR 消息的形式发送给域中的所有路由器。路由器收集这些 BSR 消息，并使用众所周知的散列算法为每个组播组选择一个活动 RP。如果所选的 RP 发生故障，则路由器会从候选 RP 中选择一个新的 RP-group 映射。有关 BSR 选择过程的信息，请参阅 *draft-ietf-pim-sm-bsr-03.txt*。

在分布树上转发信息流

本节将介绍 PIM-SM 路由器如何将加入消息发往组播组的汇聚点 (RP)，以及 RP 如何将组播数据传送到网络中的接收方。在组播网络环境中， NetScreen 设备可以充当 RP、源网络或接收方网络中的指定路由器或者中间路由器。

源将数据发送到组

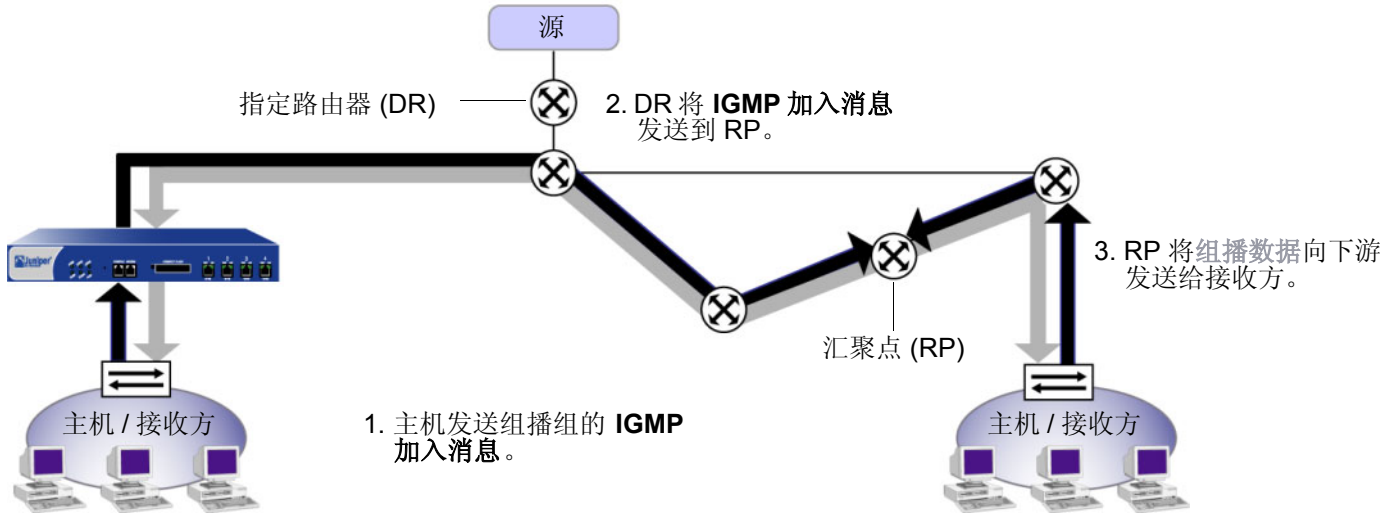
当源开始发送组播数据包时，它将向网络发送数据包。当该局域网 (LAN) 中的指定路由器 (DR) 收到组播数据包时，它会在单播路由表中查找出接口和通往 RP 的下一跳 IP 地址。然后， DR 会将组播数据包封装到被称为注册消息的单播数据包中，并将它们转发到下一跳 IP 地址。当 RP 收到注册消息后，将对数据包进行解封，并沿着通向接收方的分布树向下发送组播数据包。



如果源 DR 的数据传输速率达到了所配置的临界值，则 RP 会向源 DR 发送一条 PIM-SM 加入消息，因此 RP 可以接收本地组播数据，而不是注册消息。当源 DR 收到加入消息时，会向 RP 发送组播数据包和注册消息。当 RP 收到来自 DR 的组播数据包时，会向 DR 发送一条 register-stop 消息。当 DR 收到该 register-stop 消息时，会停止发送注册消息，并发送本地组播数据，然后再由 RP 将此数据向下游发送给接收方。

主机加入组

当主机加入组播组时，会将一条 IGMP 加入消息发送给该组播组。当主机所在 LAN 上的 DR 收到 IGMP 加入消息时，它会在该组中查找 RP。它会在组播路由表中创建一个 (*,G) 条目，并将 PIM-SM 加入消息向上游发送给通往 RP 的 RPF 邻接路由器。当上游路由器收到 PIM-SM 加入消息时，会执行相同的 RP 查找过程，同时还将检查该加入消息是否来自 RPF 邻接路由器。如果该消息确实来自 RPF 邻接路由器，则会将 PIM-SM 加入消息转发给 RP。在 PIM-SM 加入消息到达 RP 之前，会继续此过程。当 RP 收到加入消息时，会将组播数据向下游发送给接收方。



每个下游路由器收到组播数据时，都会执行 RPF 检查。每个路由器都会检查所收到的组播数据包是否来自同一个接口 (向 RP 发送信息流时所使用的接口)。如果 RPF 检查取得成功，则路由器会在组播路由表中查找相匹配的 (*, G) 转发条目。如果找到了 (*, G) 条目，则会将源放到该条目中 [该条目将成为 (S, G) 条目]，并向下游转发组播数据包。将沿分布树向下继续进行此过程，直到主机收到组播数据为止。

当信息流传输速率达到所配置的临界值时，主机所在 LAN 上的 DR 可以形成直接通往组播源的最短路径树。当 DR 开始接收直接来自源的信息流时，它会将源特定裁剪消息向上游发送到 RP。每个中间路由器会 “裁剪” 至主机的链接，使其脱离分布树，直到裁剪消息到达 RP 为止，之后 RP 会停止沿着分布树的该特定分支向下发送组播信息流。

NETSCREEN 设备上的 PIM-SM

NetScreen 设备有两个预定义的虚拟路由器 (VR): trust-vr 和 untrust-vr。每个虚拟路由器均为具有其自身路由表的单独路由选择组件。“协议无关组播 - 稀疏模式” (PIM-SM) 使用虚拟路由器的路由表，通过该虚拟路由器上的路由表来查询反向路径转发 (RPF) 接口和下一跳 IP 地址。因此，要在 NetScreen 设备上运行 PIM-SM，必须首先在虚拟路由器上配置静态路由或动态路由协议，然后在同一虚拟路由器上配置 PIM-SM。 (有关虚拟路由器的信息，请参阅第 19 页上的 “虚拟路由器”。) NetScreen 设备支持以下动态路由协议 :

- 开放式最短路径优先 (OSPF) - 有关 OSPF 的信息，请参阅第 65 页上的 “开放式最短路径优先 (OSPF)”。
- 边界网关协议 (BGP) - 有关 BGP 的信息，请参阅第 155 页上的 “边界网关协议 (BGP)”。
- 路由信息协议 (RIP) - 有关 RIP 的信息，请参阅第 111 页上的 “路由选择信息协议 (RIP)”。

以下各节将就在 NetScreen 设备上配置 PIM-SM 所需的下列几个基本步骤进行介绍 :

- 在 VR 中创建并启用 PIM-SM 实例。
- 在接口上启用 PIM-SM。
- 配置允许 PIM-SM 消息通过 NetScreen 设备的组播策略。

创建 PIM-SM 实例

可以为每个 VR 各配置一个 PIM-SM 实例。 PIM-SM 使用 VR 的单播路由表来执行其 RPF 检查。在 VR 上创建并启用 PIM-SM 路由选择实例后，即可在 VR 中的接口上启用 PIM-SM。

范例：在虚拟路由器中启用 PIM-SM 实例

本例中，将为 trust-vr 虚拟路由器创建并启用 PIM-SM 实例。

WebUI

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create PIM Instance: 选择 **Protocol PIM: Enable**，然后单击 **Apply**。

CLI

```
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol pim
ns(trust.vr/pim)-> set enable
ns(trust.vr/pim)-> exit
ns(trust-vr)-> exit
save
```

范例：移除 PIM-SM 实例

本例中，将从 trust-vr 虚拟路由器中删除 PIM-SM 实例。当您从虚拟路由器中删除 PIM-SM 实例后， NetScreen 设备将在接口上禁用 PIM-SM，并会删除所有 PIM-SM 接口参数。

WebUI

Network > Routing > Virtual Router (trust-vr) > Edit > Delete PIM Instance，然后在出现确认提示时单击 **OK**。

CLI

```
unset vrouter trust-vr protocol pim
deleting PIM instance, are you sure? y/[n] y
save
```

接口上的 PIM-SM

在缺省情况下，所有接口都将禁用 PIM-SM。在虚拟路由器中创建并启用 PIM-SM 后，必须在传送组播信息流的虚拟路由器中的接口上启用 PIM-SM。如果接口与接收方相连，还必须在该接口上于路由器模式下配置 IGMP。 (有关 IGMP 的信息，请参阅第 205 页上的 “IGMP”。)

当在绑定到区段的接口上启用 PIM-SM 时，在该接口所属的区段中将自动启用 PIM-SM。然后可为该区段配置 PIM-SM 参数。同样，当在该区段的接口上禁用 PIM-SM 参数时，会自动删除与该区段相关的所有 PIM-SM 参数。

范例 : 接口上的 PIM-SM

本例中，将在接口 ethernet1 上启用 PIM-SM。

WebUI

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

CLI

```
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
save
```

范例：在接口上禁用 PIM-SM

本例中，将在接口 ethernet1 上禁用 PIM-SM。注意，已启用 PIM-SM 的所有其它接口仍在传送及处理 PIM-SM 数据包。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > PIM: 清除 **Protocol PIM Enable**，然后单击 **Apply**。

CLI

```
unset interface ethernet1 protocol pim enable
save
```

组播组策略

在缺省情况下，NetScreen 设备不允许组播控制信息流 (例如 PIM-SM 消息) 在区段间通过。必须配置允许 PIM-SM 消息在区段间通过的组播组策略。组播组策略可对两种类型的 PIM-SM 消息进行控制 : static-RP-BSR 消息和 join-prune 消息。

Static-RP-BSR 消息

Static-RP-BSR 消息中含有与静态汇聚点 (RP) 和动态 RP-group 映射相关的信息。通过配置允许静态 RP 映射和自举 (BSR) 消息在区段间通过的组播策略，可使 NetScreen 设备能够在虚拟路由器中的区段间或两个虚拟路由器之间共享 RP-group 映射。路由器可以从其它区段获知 RP-group 映射，因此不必在所有区段中都配置 RP。

当 NetScreen 设备收到 BSR 消息时，会检验该消息是否来自其反向路径转发 (RPF) 邻居。之后会检查该 BSR 消息中是否存在组播组的组播策略。该设备会滤出该组播策略中不允许的组，并将允许组的 BSR 消息发送到策略所允许的所有目的地址区段。

Join-Prune 消息

组播组策略还可控制 join-prune 消息。当 NetScreen 设备在其下游接口收到源和组 (或源和 RP) 的 join-prune 消息时，将在单播路由表中查找 RPF 邻居和接口。

- 如果 RPF 接口与下游接口位于同一区段，则不需要进行组播策略验证。
- 如果 RPF 接口位于另一区段中，则 NetScreen 设备会检查是否存在这样一个组播策略 : 允许组的 join-prune 消息在下游接口所在的区段与 RPF 接口所在的区段间通过。
  - 如果存在允许 join-prune 消息在这两个区段间通过的组播策略，则 NetScreen 设备会将该消息转发给 RPF 接口。
  - 如果不存在允许 join-prune 消息在这两个区段间通过的组播策略，则设备将丢弃 join-prune 消息。

范例 : PIM-SM 的组播组策略

本例中，将定义一个双向组播组策略，该策略允许所有 PIM-SM 消息在组 224.4.4.1 的 Trust 和 Untrust 区段间通过。

WebUI

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

MGroup Address: IP/Netmask (选择) 224.4.4.1/32

Bidirectional: (选择)

PIM Message: (选择)

BSR-Static RP: (选择)

Join/Prune: (选择)

CLI

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 to untrust
    pim-message bsr-static-rp join-prune bi-directional
save
```

基本 PIM-SM 配置

NetScreen 设备可以充当汇聚点 (RP)、源指定路由器 (DR)、接收方 DR 以及中间路由器。但不能充当自举路由器。

可以在单个虚拟路由器 (VR) 上或跨两个 VR 配置 PIM-SM。要在单个虚拟路由器上配置 PIM-SM，请执行以下步骤：

1. 配置区段和接口。
2. 在 NetScreen 设备中的特定虚拟路由器上配置静态路由或动态路由协议，例如，“路由信息协议” (RIP)、“边界网关协议” (BGP) 或 “开放式最短路径优先” (OSPF)。
3. 创建允许单播和组播数据信息流在区段间通过的防火墙策略。
4. 在其中已配置了静态路由或动态路由协议的虚拟路由器上创建并启用 PIM-SM 路由选择实例。
5. 在可将信息流向上游转发到源或 RP、向下游转发到接收方的接口上启用 PIM-SM。
6. 在与主机相连的接口上启用 IGMP。
7. 配置允许 PIM-SM 消息在区段间通过的组播策略。

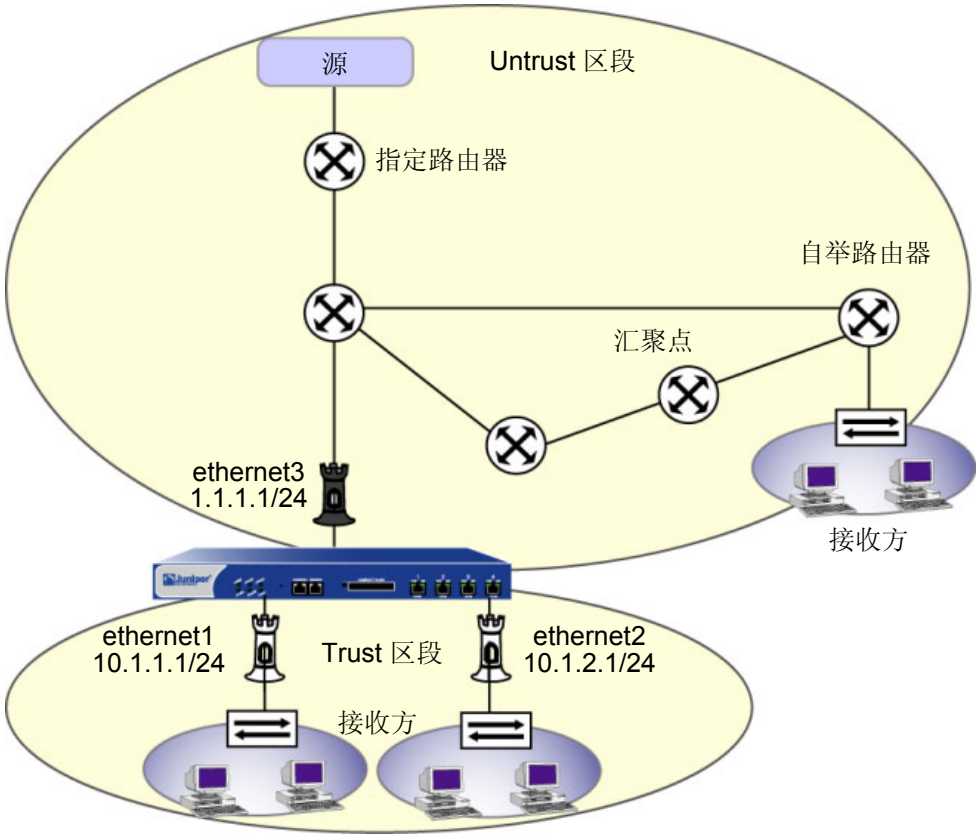
当跨两个 VR 配置 PIM-SM 时，必须在 VR 所在的区段 (RP 位于其中) 中配置 RP。然后，配置允许 join-prune 和 BSR-static-RP 消息在每个 VR 所在区段间通过的组播组策略。还必须在两个 VR 间导出单播路由，以确保反向路径转发 (RPF) 信息的精确性。有关导出路由的信息，请参阅第 60 页上的 “在虚拟路由器之间导出和导入路由”。

***注意：**如果 NetScreen 设备配置有多个 VR，则所有 VR 必须具有相同的 PIM-SM 选项。*

某些 NetScreen 设备支持多个虚拟系统。(有关虚拟系统的信息，请参阅第 9 卷，“虚拟系统”。) 在虚拟系统中配置 PIM-SM 的步骤与在根系统中配置 PIM-SM 的步骤相同。在分别位于不同虚拟系统上的两个虚拟路由器上配置 PIM-SM 时，必须配置代理 RP。 (有关配置代理 RP 的信息，请参阅第 284 页上的 “代理 RP”。)

范例：基本 PIM-SM 配置

本例中，将在 trust-vr 中配置 PIM-SM。您希望 Trust 区段中的主机接收组播组 224.4.4.1/32 的组播信息流。将 RIP 配置为 trust-vr 中的单点路由协议，并将创建允许数据信息流在 Trust 和 Untrust 区段间通过的防火墙策略。将在 trust-vr 中创建 PIM-SM 实例，并在 Trust 区段中的 ethernet1 和 ethernet2 上以及 Untrust 区段中的 ethernet3 上启用 PIM-SM。所有接口都处于路由模式。然后，在与接收方相连的 ethernet 1 和 ethernet2 上配置 IGMP。最后，创建允许 static-RP-BSR 和 join-prune 消息在区段间通过的组播策略。



WebUI

1. 区段和接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.2.1/24

选择以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone Name: Untrust

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: mgroup1

IP Address/Domain Name:

IP/Netmask: (选择), 224.4.4.1/32

Zone: Trust

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

Address Name: source-dr

IP Address/Domain Name:

IP/Netmask: (选择), 6.6.6.1/24

Zone: Untrust

3. IGMP

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

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

IGMP Mode: Router (选择)

Protocol IGMP: Enable (选择)

4. RIP

Network > Routing > Virtual Router (trust-vr) > Edit > Create RIP Instance: 选择 **Enable RIP**，然后单击 **OK**。

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

RIP Instance: (选择)

Protocol RIP: Enable (选择)

5. PIM-SM

Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: 选择以下内容，然后单击 **OK**。

Protocol PIM: Enable (选择)

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

Network > Interfaces > Edit (对于 ethernet2) > PIM: 输入以下内容，然后单击 **Apply**:

PIM Instance: (选择)

Protocol PIM: Enable (选择)

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

6. 策略

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

Source Address:

Address Book Entry: (选择), source-dr

Destination Address:

Address Book Entry: (选择), mgroup1

Service: any

Action: Permit

7. 组播策略

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

MGroup Address: IP/Netmask (选择) 224.4.4.1/32
Bidirectional: (选择)
PIM Message: (选择)
BSR Static RP: (选择)
Join/Prune: (选择)

CLI

1. 区段和接口

```
set interface ethernet 1 zone trust
set interface ethernet 1 ip 10.1.1.1/24
set interface ethernet1 nat

set interface ethernet 2 zone trust
set interface ethernet 2 ip 10.1.2.1/24
set interface ethernet2 nat

set interface ethernet 3 zone untrust
set interface ethernet 3 ip 1.1.1.1/24
```

2. 地址

```
set address trust mgroup1 224.4.4.1/32
set address untrust source-dr 6.6.6.1/24
```

3. IGMP

```
set interface ethernet 1 protocol igmp router
set interface ethernet 1 protocol igmp enable

set interface ethernet 2 protocol igmp router
set interface ethernet 2 protocol igmp enable
```

4. RIP

```
set vrouter trust-vr protocol rip
set vrouter trust-vr protocol rip enable
set interface ethernet3 protocol rip enable
```

5. PIM-SM

```
set vrouter trust-vr protocol pim
set vrouter trust-vr protocol pim enable

set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable

set interface ethernet2 protocol pim
set interface ethernet2 protocol pim enable

set interface ethernet3 protocol pim
set interface ethernet3 protocol pim enable
```

6. 策略

```
set policy from untrust to trust source-dr mgroup1 any permit
```

7. 组播策略

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
    pim-message bsr-static-rp join bi-directional
save
```

检验配置

要检验 PIM-SM 配置，请执行下面的命令：

```
ns-> get vrouter trust protocol pim
PIM-SM enabled
Number of interfaces : 1
SPT threshold        : 1 Bps
PIM-SM Pending Register Entries Count : 0
Multicast group accept policy list: 1

Virtual Router trust-vr - PIM RP policy
-----------------------------------------------
Group Address      RP access-list

Virtual Router trust-vr - PIM source policy
-----------------------------------------------
Group Address      Source access-list
```

要查看组播路由条目，请执行下面的命令：

```
ns->get vrouter trust protocol pim mroute
trust-vr - PIM-SM routing table
------------------------------------------------------------------------------
Register - R, Connected members - C, Pruned - P, Pending SPT Alert - G
Forward - F, Null - N , Negative Cache - E, Local Receivers - L
SPT - T, Proxy-Register - X, Imported - I, SGRpt state - Y, SSM Range Group - S
Turnaround Router - K
------------------------------------------------------------------------------
Total PIM-SM mroutes: 2

(*, 236.1.1.1)  RP 20.20.20.10          01:54:20/-          Flags: LF
  Zone             : Untrust
  Upstream         : ethernet1/2          State           : Joined
  RPF Neighbor     : local                Expires         : -
  Downstream       :
  ethernet1/2  01:54:20/-          Join          0.0.0.0           FC

(10.10.10.1/24, 238.1.1.1)              01:56:35/00:00:42  Flags: TLF  Register
      Prune
  Zone             : Trust
  Upstream         : ethernet1/1          State           : Joined
  RPF Neighbor     : local                Expires         : -
  Downstream       :
  ethernet1/2  01:54:20/-          Join          236.1.1.1           20.20.20.200 FC
```

可以在每个路由条目中检查下列内容：

- (S, G) 状态或 (*, G) 转发状态
- 如果转发状态是 (*, G)，则会显示 RP IP 地址；如果转发状态是 (S, G)，则会显示源 IP 地址
- 路由所属的区段
- “加入”状态以及入和出接口
- 计时器的值

要查看每个区段中的汇聚点，请执行下面的命令：

```
ns-> get vrouter trust protocol pim rp
Flags : I - Imported, A - Always(override BSR mapping)
        C - Static Config, P - Static Proxy
------------------------------------------------------------------------------
Trust
  238.1.1.1/32       RP: 10.10.10.10     192    Static  -     C
    Registering : 0
    Active Groups : 1
                238.1.1.1
Untrust
  236.1.1.1/32       RP: 20.20.20.10     192    Static  -     P
    Registering : 0
    Active Groups : 1
                236.1.1.1
```

要检验是否存在“反向路径转发”邻居，请执行下面的命令：

```
ns-> get vrouter trust protocol pim rpf
Flags : RP address - R, Source address - S
Address          RPF Interface      RPF Neighbor    Flags
-----------------------------------------------------
10.10.11.51      ethernet3          10.10.11.51     R
10.150.43.133    ethernet3          10.10.11.51     S
```

要查看 NetScreen 设备发送给虚拟路由器中各个邻居的 join-prune 消息的状态，请执行下面的命令：

```
ns-> get vrouter untrust protocol pim join
Neighbor         Interface       J/P          Group           Source
-------------------------------------------------------------------------
1.1.1.1          ethernet4:1    (S,G)     J  224.11.1.1      60.60.0.1
                                (S,G)     J  224.11.1.1      60.60.0.1
```

配置 RP

当希望将某个特定 RP 绑定到一个或多个组播组时，可以配置静态汇聚点 (RP)。可以配置多个静态 RP，每个 RP 映射到不同的组播组。

当网络中不存在自举路由器时，必须配置静态 RP。虽然 NetScreen 设备可以接收并处理自举消息，但却不能充当自举路由器。

当希望将 RP 动态映射到组播组时，可以将虚拟路由器配置为候选 RP (C-RP)。可以为每个区段创建一个 C-RP。

静态 RP

配置静态 RP 时，您需指定以下内容：

- 静态 RP 的区段
- 静态 RP 的 IP 地址
- 定义静态 RP 的组播组的访问列表 (有关访问列表的信息，请参阅第 199 页上的 “访问列表”。)

为了确保访问列表中的组播组始终使用同一 RP，请将关键字 **always** 包括在内。当未将该关键字包括在内，且 NetScreen 设备发现了动态映射到同一组播组的另一 RP 时，设备会使用该动态 RP。

范例：创建静态 RP

本例中，将首先创建组播组 224.4.4.1 的访问列表，然后再为该组创建一个静态 RP。静态 RP 的 IP 地址是 1.1.1.5/24。指定关键字 **always**，以确保 NetScreen 设备始终使用与该组的 RP 相同的 RP。

WebUI

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 2

Sequence No: 1

IP/Netmask: 224.4.4.1/32

Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Address > New: 选择以下内容，然后单击 **OK**:

Zone: Trust (选择)

Address: 1.1.1.5

Access List: 2

Always: (选择)

CLI

```
set vrouter trust-vr access-list 2 permit ip 224.4.4.1/32 1
set vrouter trust-vr protocol pim zone trust rp address 1.1.1.5 mgroup-list 2
    always
save
```

候选 RP

当将虚拟路由器配置为 C-RP 时，需指定下列内容：

- 在其中配置 C-RP 的区段
- 通告为 C-RP 的接口的 IP 地址
- 定义 C-RP 的组播组的访问列表
- 通告的 C-RP 优先级

范例：创建候选 RP

本例中，将在被绑定到 Trust 区段的 ethernet1 接口上启用 PIM-SM。创建对 C-RP 的组播组进行定义的访问列表。然后在 trust-vr 所在的 Trust 区段中创建 C-RP。将 C-RP 的优先级设置为 200。

WebUI

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 1

Sequence No: 1

IP / Netmask: 224.2.2.1/32

Action: Permit

Select Add Seq No: 输入以下内容，并单击 **OK**:

Sequence No: 2

IP/Netmask: 224.3.3.1/32

Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Candidate > Edit (Trust Zone): 选择以下内容，并单击 **OK**。

Interface: ethernet1 (选择)

Access List: 1 (选择)

Priority: 200

CLI

```
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
set vrouter trust-vr access-list 1 permit ip 224.2.2.1/32 1
set vrouter trust-vr access-list 1 permit ip 224.3.3.1/32 2
set vrouter trust-vr protocol pim zone trust rp candidate interface ethernet1
    mgroup-list 1 priority 200
save
```

安全注意事项

运行 PIM-SM 时，可以在虚拟路由器 (VR) 级上设置某些选项，以便对进出 VR 的信息流进行控制。在 VR 级上所定义的设置会影响 VR 中所有启用了 PIM-SM 的接口。

当接口收到来自其它区段的组播控制信息流 (IGMP 或 PIM-SM 消息) 时， NetScreen 设备将首先检查是否存在允许信息流的组播策略。如果 NetScreen 设备找到了允许信息流的组播策略，则会针对可应用到信息流的所有 PIM-SM 选项对虚拟路由器进行检查。例如，如果将虚拟路由器配置为可接受来自访问列表中指定的组播组的 join-prune 消息，则 NetScreen 设备会检查信息流是否适用于列表中的某个组播组。如果适用，设备将允许信息流。如果不适用，设备将丢弃信息流。

限制组播组

可以限制 VR 只转发某一组特定组播组的 PIM-SM join-prune 消息。可在访问列表中指定所允许的组播组。当您使用此功能时， VR 会丢弃未位于访问列表中的组的 join-prune 消息。

范例 : 限制组播组

本例中，将创建 ID 号为 1 的访问列表，此列表允许下列组播组 : 224.2.2.1/32 和 224.3.3.1/32。然后对 trust-vr 进行配置，使其接受来自访问列表中的组播组的 join-prune 消息。

WebUI

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 1

Sequence No: 1

IP/Netmask: 224.2.2.1/32

Action: Permit

Select Add Seq No: 输入以下内容，并单击 **OK**:

Sequence No: 2

IP/Netmask: 224.3.3.1/32

Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance: 选择以下内容，然后单击 **Apply**:

Access Group: 1 (选择)

CLI

```
set vrouter trust-vr access-list 1 permit ip 224.2.2.1/32 1
set vrouter trust-vr access-list 1 permit ip 224.3.3.1/32 2
set vrouter trust-vr protocol pim accept-group 1
save
```

限制组播源

可以控制组播组所能接收的组播源。在访问列表中标识所允许的源，然后将访问列表链接到组播组。这样即可防止未经授权的源将数据发送到您的网络中。当您使用此功能时，NetScreen 设备会丢弃来自未位于该列表中的源的组播数据。如果虚拟路由器是区段中的汇聚点，则在接受来自源的注册消息之前，会对访问列表进行检查。NetScreen 设备将丢弃并非来自所允许源的注册消息。

范例：限制组播源

本例中，将首先创建一个 ID 号为 5 的访问列表，该列表指定允许源 1.1.1.1/32。然后再配置 trust-vr，使其可接受来自访问列表中指定源的组播组 224.4.4.1/32 的组播数据。

WebUI

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 5

Sequence No: 1

IP / Netmask: 1.1.1.1/32

Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > MGroup: 选择以下内容，然后单击 **Add**:

MGroup: 224.4.4.1/32

Accept Source: 5 (选择)

CLI

```
set vrouter trust-vr access-list 5 permit ip 1.1.1.1/32 1
set vrouter trust-vr protocol pim mgroup 224.4.4.1/32 accept-source 5
save
```

限制 RP

可以控制将哪些汇聚点 (RP) 映射到组播组。在访问列表中标识允许的 RP，然后将访问列表链接到组播组。当虚拟路由器 (VR) 收到特定组的自举消息时，会检查与该组相对应的所允许 RP 的列表。如果未找到一个匹配项，则它不会为组播组选择 RP。

范例：限制 RP

在本例中，将创建一个 ID 号为 6 的访问列表，该列表指定允许 RP 2.1.1.1/32。然后配置 trust-vr，使其可接受组播组 224.4.4.1/32 的访问列表中的 RP。

WebUI

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 6

Sequence No: 1

IP / Netmask: 2.1.1.1/32

Action: Permit

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > MGroup: 选择以下内容，然后单击 **Add**:

MGroup: 224.4.4.1/32

Accept RP: 6 (选择)

CLI

```
set vrouter trust-vr access-list 6 permit ip 2.1.1.1/32 1
set vrouter trust-vr protocol pim mgroup 224.4.4.1/32 accept-rp 6
save
```

PIM-SM 接口参数

可以更改已启用 PIM-SM 的每个接口的某些缺省值。当您在此级别上设置参数时，只会影响您指定的接口。

下表对 PIM-SM 接口参数及其缺省值进行了介绍：

PIM-SM 接口参数	说明	缺省值
Neighbor policy	控制邻居的邻接关系。有关其它信息，请参阅第 281 页上的 “邻居策略”。	禁用
Hello interval	指定接口将 hello 消息发送给其邻接路由器的时间间隔。	30 seconds
Designates router priority	为所选的指定路由器指定接口的优先级。	1
Join-Prune interval	指定接口发送 join-prune 消息的时间间隔 (以秒为单位)。	60 seconds
Bootstrap border	指定接口是自举边界。有关其它信息，请参阅第 283 页上的 “自举边界”。	禁用

邻居策略

可以对可与接口形成邻接关系的邻居进行控制。 PIM-SM 路由器定期发送 hello 消息，以通告其自身为 PIM-SM 路由器。如果使用了此功能，则接口将检查其所允许的或所禁止的邻居的列表，并与所允许的邻居形成邻接关系。

范例：定义邻居策略

本例中，将创建一个指定下列内容的访问列表：

- ID 号为 1
- 第一条语句允许 2.1.1.1/24
- 第二条语句允许 2.1.1.3/24

然后指定 ethernet1 可以与访问列表中的邻居形成邻接关系。

WebUI

Network > Routing > Virtual Routers > Access List: > New (对于 trust-vr): 输入以下内容，并单击 **OK**:

Access List ID: 1

Sequence No: 1

IP/Netmask: 2.1.1.1/24

Action: Permit

Select Add Seq No: 输入以下内容，并单击 **OK**:

Sequence No: 2

IP/Netmask: 2.1.1.3/24

Action: Permit

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

Accepted Neighbors: 1

CLI

```
set vrouter trust-vr access-list 1 permit ip 2.1.1.1/24 1
set vrouter trust-vr access-list 1 permit ip 2.1.1.3/24 2
set interface ethernet1 protocol pim neighbor-policy 1
save
```

自举边界

作为自举 (BSR) 边界的接口可接收并处理 BSR 消息。不过，即使存在允许 BSR 消息在区段间通过的组播组策略，该接口也不能将这些消息转发到其它接口。这样可确保 RP-to-group 映射始终处于区段内。

范例：定义自举边界

本例中，将把 ethernet1 配置为自举边界。

WebUI

Network > Interfaces > Edit (对于 ethernet1) > PIM: 选择 **Bootstrap Border**，然后单击 **Apply**:

CLI

```
set interface ethernet1 protocol pim boot-strap-border
save
```

代理 RP

PIM-SM 域是一组具有相同 “汇聚点 (RP)-group” 映射的 PIM-SM 路由器。在具有动态 RP-group 映射的 PIM-SM 域中，域中的 PIM-SM 路由器接听来自同一自举路由器 (BSR) 的消息，以选择它们的 RP-group 映射。在具有静态 RP-group 映射的 PIM-SM 域中，必须在域中的每个路由器上配置静态 RP。(有关 RP-group 映射的信息，请参阅第 273 页上的 “配置 RP”。)

在 NetScreen 设备上，第 3 层区段上所绑定的接口既可以在 NAT 模式下运行，也可以在路由模式下运行。当设备的不同接口允许在不同的模式下时，在该设备上运行 PIM-SM，每个区段必须处于不同的 PIM-SM 域中。例如，如果 Trust 区段中的接口处于 NAT 模式，而 Untrust 区段中的接口处于路由模式，则每个区段必须处于不同的 PIM-SM 域中。此外，当跨越处于两个不同虚拟系统的两个虚拟路由器配置 PIM-SM 时，每个虚拟路由器必须各自处于单独的 PIM-SM 域中。

通过配置代理 RP 可将组播组从一个 PIM-SM 域通告给另一个 PIM-SM 域。代理 RP 通过静态 RP 或通过组播组策略所允许的自举消息来充当从其它 PIM-SM 域获知的组播组的 RP。代理 RP 可充当其域中的接收方的共享树的根，并且它可以形成到源的最短路径树。

可以为虚拟路由器中的每个区段配置一个代理 RP。要在区段中配置代理 RP，必须在该区段中配置候选 RP (C-RP)。然后， NetScreen 设备将 C-RP 的 IP 地址通告为代理 RP 的 IP 地址。当您配置 C-RP 时，请不要在组播组列表中指定任何组播组。这样可使 C-RP 充当自其它区段中导入的任何组的代理 RP。如果指定了组播组，则 C-RP 将充当列表中所指定组的真正 RP。

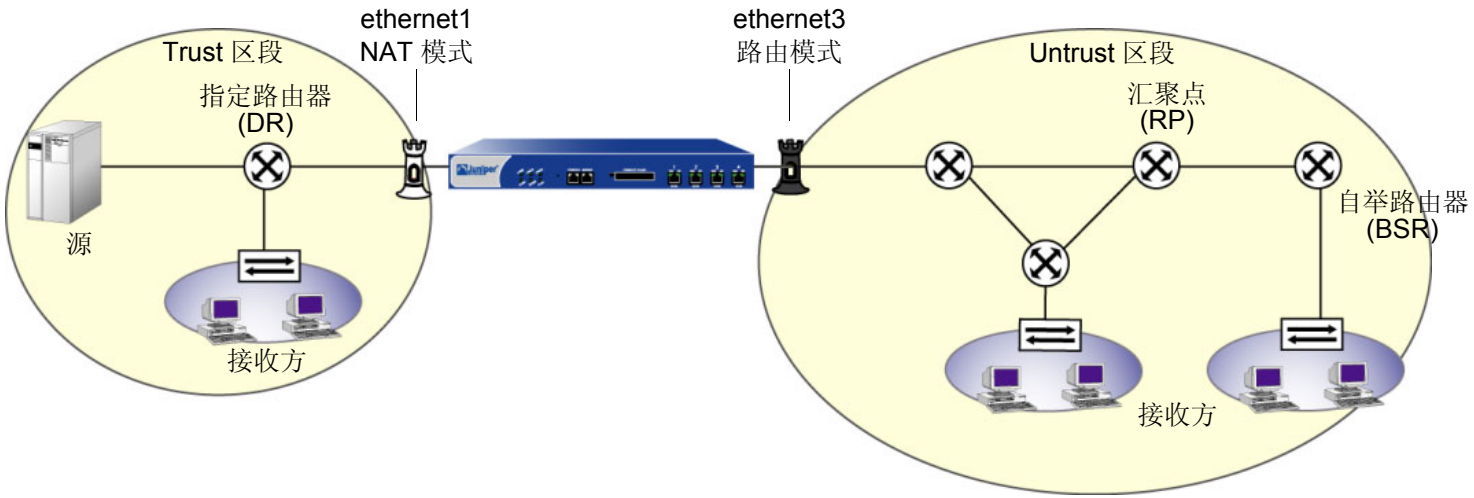
如果区段中存在 BSR，则代理 RP 会将其自身通告为自其它区段中导入的组播组的 RP。如果代理 RP 所在的区段中不存在 BSR，则代理 RP 会充当自其它区段中导入的组播组的静态 RP。然后，必须在区段中的所有其它路由器上将 C-RP 的 IP 地址配置为静态 RP。

代理 RP 支持使用源地址转换的映射 IP (MIP)。 MIP 是从一个 IP 地址到另一个 IP 地址的直接一对一映射。当您希望 NetScreen 设备在其接口处于 NAT 模式下的区段中将私有地址转换为其它地址时，可以配置 MIP。当代理 RP 所在区段中的 MIP 主机发送注册消息时， NetScreen 设备会将源 IP 地址转换为 MIP 地址，并将一条新注册消息发送给真正的 RP。当 NetScreen 设备收到 MIP 地址的 join-prune 消息时，该设备会将 MIP 映射到初始源地址并将其发送到源。

代理 RP 还支持区段间的组播组地址转换。可以配置组播策略，该策略指定初始组播组地址和转换后的组播组地址。当 NetScreen 设备在代理 RP 所在区段中的接口上收到 join-prune 消息时，会对组播组进行转换，如需要，还可将加入消息发送到真正的 RP。

考虑以下示例：

- Trust 区段中的 ethernet1 处于 NAT 模式， Untrust 区段中的 ethernet3 处于 “路由”模式。
- Trust 区段中存在源的 MIP。
- Trust 区段中的源将组播信息流发送到组播组 224.4.4.1/32。
- Trust 区段和 Untrust 区段中都存在接收方。
- 存在允许 PIM-SM 消息在 Trust 和 Untrust 区段间通过的组播策略。
- Trust 区段被配置为代理 RP。
- RP 和 BSR 位于 Untrust 区段中。



数据流如下：

1. 源将数据发送到组播组 224.4.4.1/32。
2. 指定路由器 (DR) 封装数据并将 “注册”消息发往 RP。
3. Trust 区段中的 RP 代理会收到 “注册”消息，并将初始源 IP 地址更改为 MIP 的 IP 地址。然后再将该消息转发至组播组的 RP。

4. 代理 RP 将 (*, G) 加入发送到真正的 RP。
5. Trust 区段中的接收方将加入消息发送到代理 RP。
6. 代理 RP 将组播数据包发送到 Trust 区段中的接收方。

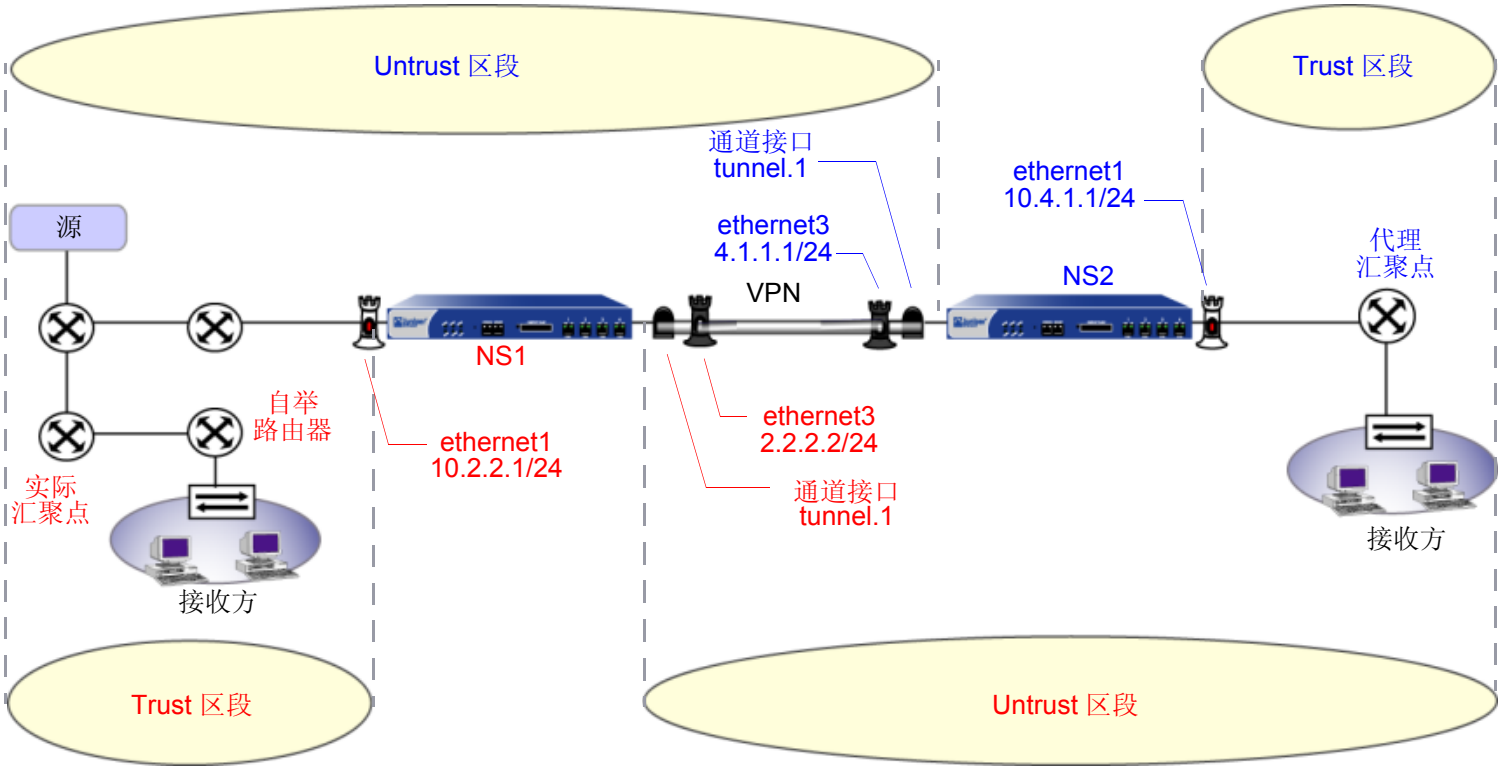
配置代理 RP

要配置代理 RP，必须执行下列操作：

1. 在特定的虚拟路由器上创建 PIM-SM 实例。
2. 在相应接口上启用 PIM-SM。
3. 在代理 RP 所在区段中配置候选 RP。
4. 配置代理 RP。

范例：代理 RP 配置

本例中， NetScreen 设备 NS1 和 NS2 通过 VPN 通道相连。两个设备都在运行动态路由协议 BGP。将在 NS1 和 NS2 上的 ethernet1 和 tunnel.1 上配置 PIM-SM。然后，在 NS2 上，将 ethernet1 配置为静态 RP，并在 trust-vr 所在 Trust 区段中创建一个代理 RP。



WebUI (NS1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: mgroup1

IP Address/Domain Name:

IP/Netmask: (选择), 224.4.4.1/32

Zone: Trust

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

Address Name: branch

IP Address/Domain Name:

IP/Netmask: (选择), 10.4.1.0/24

Zone: Untrust

3. PIM-SM

Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: 选择 **Protocol PIM: Enable**，然后单击 **OK**。

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

4. VPN

VPN > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**。

Gateway Name: To_Branch

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 4.1.1.1

Preshared Key: fg2g4h5j

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: Compatible

Phase 1 Proposal (for Compatible Security Level):
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

5. BGP

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

Virtual Router ID: Custom (选择)

在文本框中输入 0.0.0.10

Network > Routing > Virtual Router (trust-vr) > Edit: 选择 **Create BGP Instance**。

AS Number (必需): 65000

BGP Enabled: (选择)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 65000

Remote IP: 4.1.1.1

Outgoing Interface: ethernet3

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors > Configure (对于刚刚添加的对等方): 选择 **Peer Enabled**，然后单击 **OK**。

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Networks: 在 IP / Netmask 字段中输入 **2.2.2.0/24**，然后单击 **Add**。之后在 IP / Netmask 字段中输入 10.2.2.0/24，并再次单击 **Add**。

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

Protocol BGP: Enable (选择)

6. 策略

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

Source Address:

Address Book Entry: (选择), branch

Destination Address:

Address Book Entry: (选择), mgroup1

Service: any

Action: Permit

7. 组播策略

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

MGroup Address: IP / Netmask (选择) 224.4.4.1/32

Bidirectional: (选择)

PIM Message: (选择)

BSR Static IP: (选择)

Join/Prune: (选择)

WebUI (NS2)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.4.1.1/24

选择 **NAT**，然后单击 **Apply**。

> IGMP: 输入以下内容，然后单击 **Apply**:

IGMP Mode: Router

Protocol IGMP: Enable (选择)

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 4.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: mgroup1

IP Address/Domain Name:

IP/Netmask: (选择), 224.4.4.1/32

Zone: Trust

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

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.0/24

Zone: Untrust

3. PIM-SM

Network > Routing > Virtual Router (trust-vr) > Edit > Create PIM Instance: 选择 **Protocol PIM: Enable**，然后单击 **OK**。

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

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

PIM Instance: (选择)

Protocol PIM: Enable (选择)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit PIM Instance > RP Address > New: 选择以下内容，然后单击 **OK**:

Zone: Trust (选择)

Address: 10.4.1.1/24

4. VPN

VPN > AutoKey Advanced > Gateway > New: 输入以下内容，然后单击 **OK**:

Gateway Name: To_Corp

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 2.2.2.2

Preshared Key: fg2g4h5j

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: Compatible

Phase 1 Proposal (for Compatible Security Level):
pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

5. BGP

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

Virtual Router ID: Custom (选择)

在文本框中输入 0.0.0.10

Network > Routing > Virtual Router (trust-vr) > Edit: 选择 **Create BGP Instance**。

AS Number (必需): 65000

BGP Enabled: (选择)

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 65000
Remote IP: 2.2.2.2
Outgoing Interface: ethernet3

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Neighbors > Configure (对于刚刚添加的对等方): 选择 **Peer Enabled**，然后单击 **OK**。

Network > Routing > Virtual Router (trust-vr) > Edit > Edit BGP Instance > Networks: 在 IP/Netmask 字段中，输入 **4.1.1.0/24**，然后单击 **Add**。

在 IP/Netmask 字段中，输入 **10.4.1.0/24**，然后单击 **Add**。

Network > Interfaces > Edit (对于 ethernet3) > BGP: 选择 **Protocol BGP: Enable**，然后单击 **Apply**。

6. 策略

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

Source Address:
  Address Book Entry: (选择), corp
Destination Address:
  Address Book Entry: (选择), mgroup1
Service: any
Action: Permit

7. 组播策略

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

MGroup Address: IP/Netmask (选择) 224.4.4.1/32
Bidirectional: (选择)
PIM Message: (选择)
BSR Static IP: (选择)
Join/Prune: (选择)

CLI (NS1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust mgroup1 224.4.4.1/32
set address untrust branch 10.4.1.0/24
```

3. PIM-SM

```
set vrouter trust-vr
set vrouter trust-vr protocol pim enable

set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
set interface tunnel.1 protocol pim
set interface tunnel.1 protocol pim enable
```

4. VPN 通道

```
set ike gateway To_Branch address 4.1.1.1 main outgoing-interface ethernet3
    preshare fg2g4h5j proposal pre-g2-3des-sha
set vpn Corp_Branch gateway To-Branch3 sec-level compatible
set vpn Corp_Branch bind interface tunnel.1
set vpn Corp_Branch proxy-id local-ip 10.2.2.0/24 remote-ip 10.4.1.0/24
```

5. BGP

```
set vrouter trust-vr router-id 10
set vrouter trust-vr protocol bgp 6500
set vrouter trust-vr protocol bgp enable
set vrouter trust-vr protocol bgp neighbor 4.1.1.1
set vrouter trust-vr protocol bgp network 2.2.2.0/24
set vrouter trust-vr protocol bgp network 10.2.2.0/24
set interface ethernet3 protocol bgp enable
set interface ethernet3 protocol bgp neighbor 4.1.1.1
```

6. 策略

```
set policy name To-Branch from untrust to trust branch any any permit
```

7. 组播策略

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
    pim-message bsr-static-rp join bi-directional
save
```

CLI (NS2)

1. 接口

```
set interface ethernet 1 zone trust
set interface ethernet 1 ip 10.4.1.1/24
set interface ethernet 1 protocol igmp router
set interface ethernet 1 protocol igmp enable

set interface ethernet 3 zone untrust
set interface ethernet 3 ip 4.1.1.1/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust mgroup1 224.4.4.1/32
set address untrust corp 2.2.2.0/24
```

3. PIM-SM

```
set vrouter trust protocol pim
set interface ethernet1 protocol pim
set interface ethernet1 protocol pim enable
set interface tunnel.1 protocol pim
set interface tunnel.1 protocol pim enable
set vrouter trust protocol pim zone trust rp proxy
set vrouter trust protocol pim zone trust rp candidate interface ethernet1
set vrouter trust protocol pim enable
```

4. VPN 通道

```
set ike gateway To_Corp address 2.2.2.2 main outgoing-interface ethernet3
    preshare fg2g4h5j proposal pre-g2-3des-sha
set vpn Branch_Corp gateway To_Corp sec-level compatible
set vpn Branch_Corp bind interface tunnel.1
set vpn Branch_Corp proxy-id local-ip 10.4.1.0/24 remote-ip 10.2.2.0/24
```

5. BGP

```
set vrouter trust-vr router-id 10
set vrouter trust-vr protocol bgp 6500
set vrouter trust-vr protocol bgp enable
set vrouter trust-vr protocol bgp neighbor 2.2.2.2
set vrouter trust-vr protocol bgp network 4.1.1.0/24
set vrouter trust-vr protocol bgp network 10.4.1.0/24
set interface ethernet3 protocol bgp neighbor 2.2.2.2
```

6. 策略

```
set policy name To-Corp from untrust to trust corp any any permit
```

7. 组播策略

```
set multicast-group-policy from trust mgroup 224.4.4.1/32 any to untrust
    pim-message bsr-static-rp join bi-directional
save
```

PIM-SM 和 IGMPv3

运行有“互联网组管理协议”(IGMP) 版本 1、2 或 3 的接口可以运行 PIM-SM。当在运行有 IGMPv1 或 v2 的接口上运行 PIM-SM 时，加入某个组播组的主机可以接收从任何源发过来给这个组播组的数据。 IGMPv1 和 v2 成员关系报告中仅指出了主机要加入哪些组播组。该报告中不含有与组播信息流的源有关的信息。当 PIM-SM 收到 IGMPv1 和 v2 成员关系报告后，会在组播路由表中创建 (*,G) 条目，同时允许所有源发送到组播组。这称为 “所有源组播模式” (ASM)。在该模式下，接收方在不了解将数据发送到组播组的源的情况下，就加入了该组播组。由网络来维护与源有关的信息。

运行 IGMPv3 的主机会指出它们要加入哪些组播组，以及它们要从中接收组播信息流的源。IGMPv3 成员关系报告中含有组播组地址、过滤模式 (“包括”或 “排除”) 以及源列表。

如果过滤模式为 “包括”，则接收方只接受从源列表中的地址所发出的组播信息流。当 PIM-SM 收到含有源列表和过滤模式 “包括”的 IGMPv3 成员关系报告时，会在组播路由表中为源列表中的所有源创建 (S,G) 条目。

如果过滤模式为 “排除”，则接收方不会接受从该列表中的源发出的组播信息流，而会接受来自所有其它源的组播信息流。当 PIM-SM 收到含有源列表和过滤模式 “排除”的 IGMPv3 成员关系报告时，会为该组创建一个 (*,G) 条目并为源列表中的源发送一条裁剪消息。此时，如果接收方不知道源的地址，则可能需要配置汇聚点。

PIM-SSM

除了支持 PIM-SM 之外， NetScreen 设备还支持 “PIM 源特定组播” (PIM-SSM)。 PIM-SSM 遵循源特定模式 (SSM)，在该模式下，组播信息流还可传送到通道，而不仅仅是组播组。通道由源和组播组组成。接收方会向具有已知源和组播组的通道进行注册。接收方通过 IGMPv3 提供有关源的信息。 LAN 上的指定路由器将消息发送到源，而不发送到汇聚点 (RP)。

IANA 已将组播地址范围 232/8 预留给了 IPv4 中的 SSM 服务。如果设备上同时运行 IGMPv3 和 PIM-SM，则可确保 PIM-SSM 在该地址范围内运行。 NetScreen 设备将按如下方式处理地址范围 232/8 内的组播组的 IGMPv3 成员关系报告：

- 如果报告中所含的过滤模式为 “包括”，则设备会将报告直接发送到源列表中的源。
- 如果报告中所含的过滤模式为 “排除”，则设备会丢弃报告。设备不会处理地址范围 232/8 内的组播组的 (*,G) 报告。

NetScreen 设备上的 PIM-SSM

在 NetScreen 设备上配置 PIM-SSM 步骤与配置 PIM-SM 的步骤大体相同，其不同之处如下：

- 必须在与接收方相连的接口上配置 IGMPv3。 (在缺省情况下， NetScreen 设备将启用 IGMPv2。)
- 当您配置组播组策略时，应允许 join-prune 消息。 (不使用自举消息。)
- 不配置 RP。

索引

M

N

O

P

R

S

V

W

Y

Z