NetScreen 概念与范例

ScreenOS 参考指南

第 6 卷：动态路由

ScreenOS 5.0.0

编号 093-0929-000-SC

修订本 E

Copyright Notice

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

Information in this document is subject to change without notice.

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

路由是 NetScreen 设备和系统等安全设备的基本部分。通过动态路由，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信息，并自动建立及更新路由表。由于设备能自动调整路由表，因此使用动态路由协议可以大大缩短更改网络拓扑结构与调整路由表之间的时间延迟。

第 6 卷，“动态路由”介绍如何在 NetScreen 设备上配置虚拟路由器、如何在协议或虚拟路由器之间重新分配路由表条目以及如何在 NetScreen 设备上配置以下动态路由协议。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)。

约定

本文档包含几种类型的约定，以下部分将加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

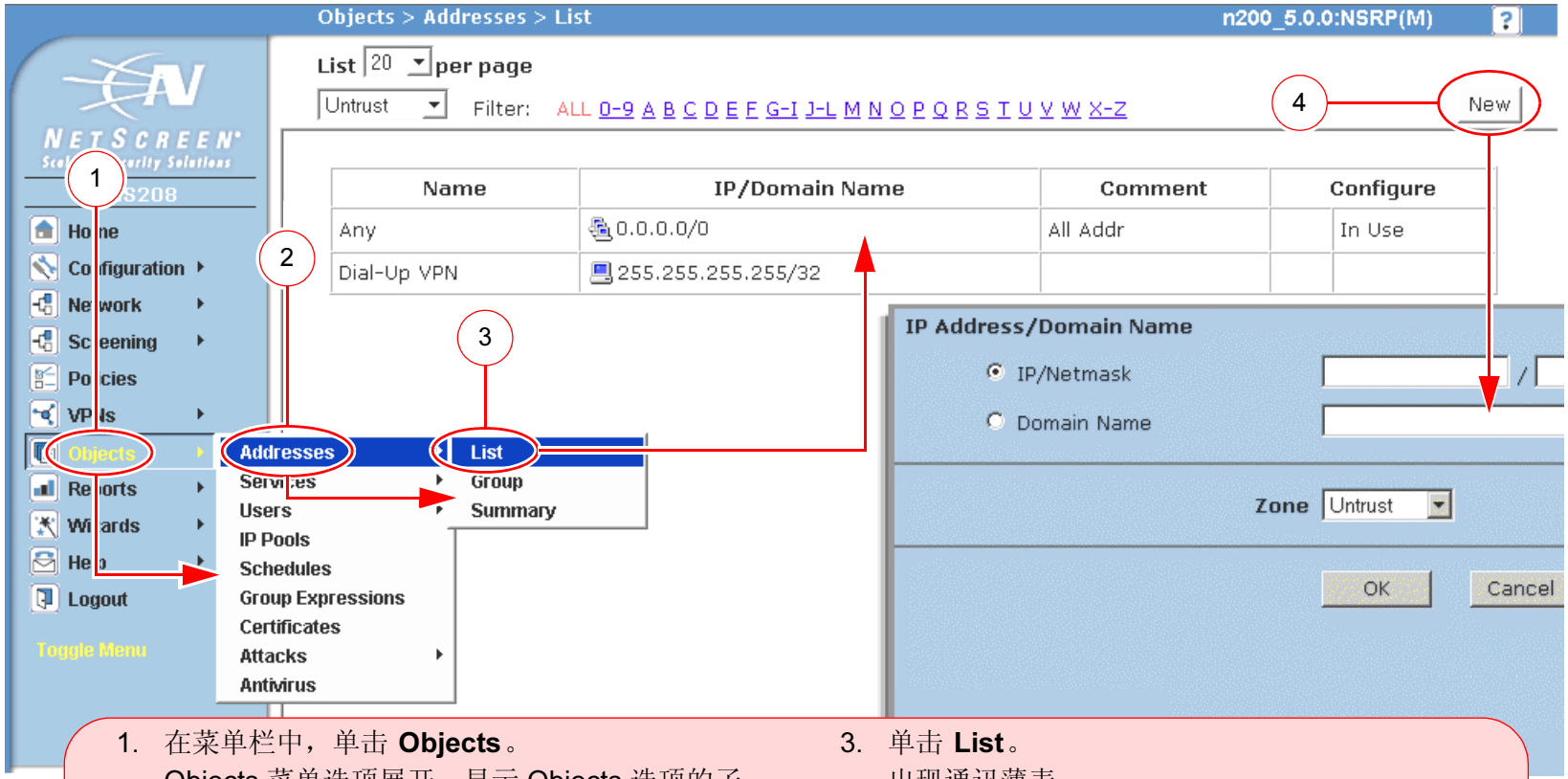
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

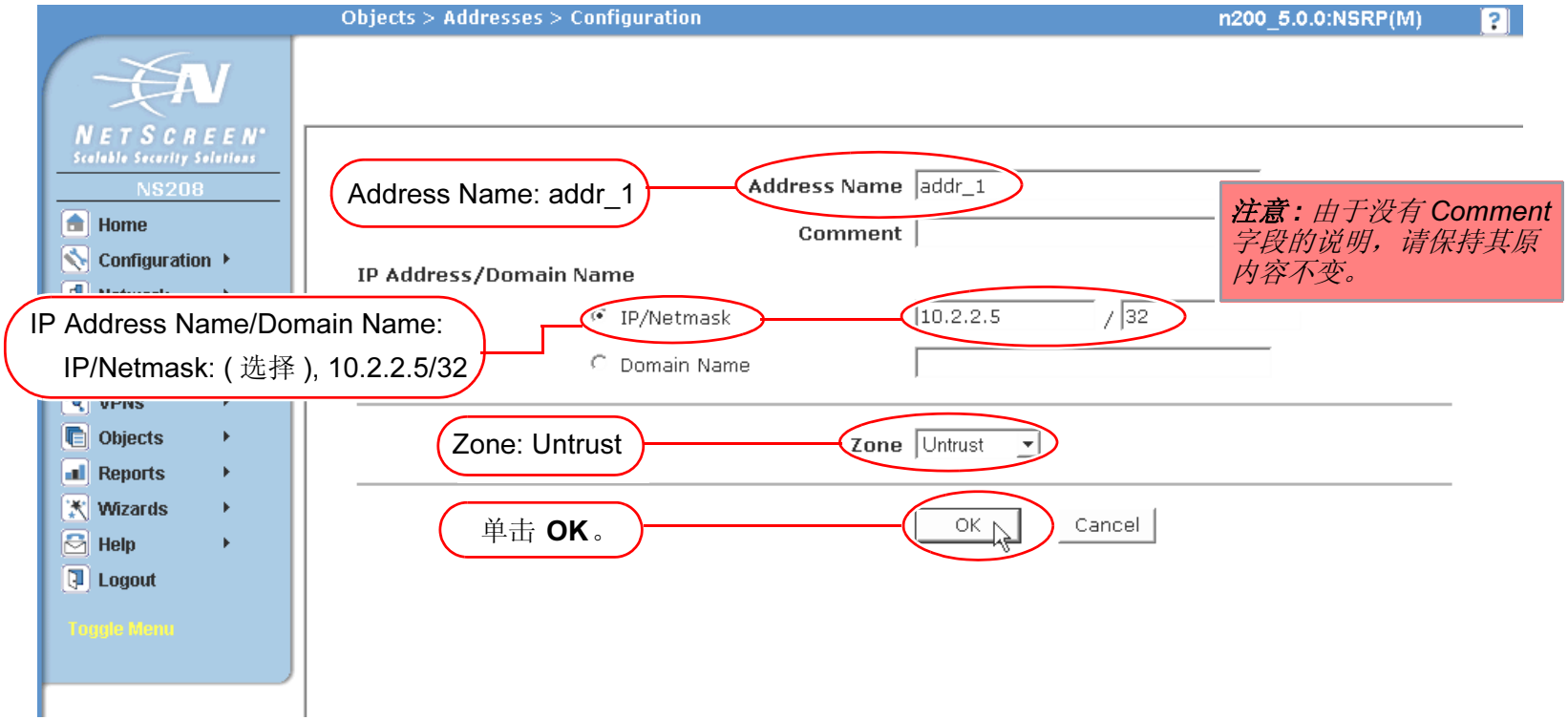
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

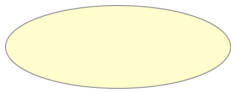


插图约定

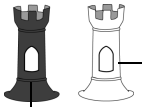
下列图形构成了贯穿本书的插图所用的基本图像集：

通用 NetScreen 设备

虚拟路由域



安全区段



安全区段接口

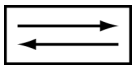
白色 = 受保护区段接口
（例如：Trust 区段）

黑色 = 区段外接口
（例如：Untrust 区段）

通道接口

VPN 通道

路由器图标



交换机图标

包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）

互联网

动态 IP (DIP) 池

台式计算机

便携式计算机

通用网络设备
（例如：NAT 服务器，
接入集中器）

服务器

命名约定和字符类型

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

- 如果名称字符串包含一个或多个空格，则整个名称字符串的两边必须用双引号 (“) ；例如，**set address trust “local LAN” 10.1.1.0/24**。
- NetScreen 会删除一组双引号内文本的前导或结尾空格，例如，**“ local LAN ”** 将变为 **“local LAN”**。
- NetScreen 将多个连续的空格处理为单个空格。
- 尽管许多 CLI 关键字不区分大小写，但名称字符串是区分大小写的。例如，**“local LAN”** 不同于 **“local lan”**。

ScreenOS 支持以下字符类型：

- 单字节字符集 (SBCS) 和多字节字符集 (MBCS)。SBCS 的例子是 ASCII、欧洲语和希伯莱语。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。*

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

NETSCREEN 文档

要获取任何 NetScreen 产品的技术文档，请访问 www.netscreen.com/resources/manuals/。

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

1

虚拟路由器

路由是 NetScreen 设备和系统等安全设备的基本部分。如果没有路由，安全设备就不能将安全信息流有效地转发到目标位置。可以配置 NetScreen 设备只使用静态路由，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 2 卷中的 “路由表和静态路由” 一章。) 通过动态路由， NetScreen 设备可使用通用协议更改路由器及其它网络设备的路由信息，并自动建立及更新路由表。由于设备能自动调整路由表，因此使用动态路由协议可以大大缩短更改网络拓扑结构与调整路由表之间的时间延迟。

本章介绍如何在 NetScreen 设备上配置虚拟路由器以及如何在协议或虚拟路由器之间重新分配路由表条目。本卷的其余各章介绍如何在 NetScreen 设备上配置特定的动态路由协议。

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) 同时支持静态和动态路由协议，因此可以在一个虚拟路由器上同时启用二者。 NetScreen 设备上有两个预定义的虚拟路由器 :

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

不能删除 trust-vr 或 untrust-vr 虚拟路由器。在某些 NetScreen 设备上，可以创建及配置其它虚拟路由器 (有关创建自定义虚拟路由器的详细信息，请参阅第 7 页上的 “自定义虚拟路由器”)。可以为预定义和自定义虚拟路由器创建某些参数 (请参阅第 13 页上的 “修改虚拟路由器”)。

使用两个 VR

通过将路由信息划分给两个虚拟路由器，可以控制给定路由域中对其它路由域可见的信息。例如，可以将企业网内部所有安全区的路由信息保留在预定义虚拟路由器 trust-vr 中，而将企业网外部所有区段的路由信息保留在另一个预定义虚拟路由器 untrust-vr 中。由于一个虚拟路由器的路由表信息对另一个虚拟路由器不可见，因此可以将内部网的路由信息与公司外部的不可信源分离开来。

在 VR 之间转发信息流

NetScreen 设备上存在两个虚拟路由器时，不能在位于不同 VR 的区段之间自动转发信息流，即使存在允许信息流的策略。为了让信息流从一个虚拟路由器流向另一个虚拟路由器，首先要确保路由表中存在相应的条目。要进行此操作，可以：

- 在一个虚拟路由器上定义一个静态路由，并将另一个 VR 定义成该路由的下一跳跃。此路由甚至可以是该虚拟路由器的缺省路由。例如，可以为 trust-vr 配置一个缺省路由，并将 untrust-vr 作为下一跳跃。如果出站封包中的目的地址不与 trust-vr 路由表中的其它任何条目匹配，则将该封包转发到 untrust-vr。有关配置静态路由的详细信息，请参阅第 2 卷中的 “路由表和静态路由”一章。
- 将路由从一个虚拟路由器的路由表导出到另一个 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 中收到的封包转发到 trust-vr 中的目的地址。有关详细信息，请参阅第 30 页上的 “在 VR 之间导出和导入路由”。

配置两个虚拟路由器

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

可以将安全区只绑定到一个虚拟路由器上。当多个安全区之间不存在地址重叠时，可以将它们绑定到一个虚拟路由器。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虚拟路由器后，该区段中的所有接口都属于该虚拟路由器。也可以更改安全区的绑定对象，将绑定到一个虚拟路由器的安全区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以及解除接口绑定的详细信息，请参阅第 **2**-67 页上的 “接口”。)

下面是将安全区绑定到 untrust-vr 虚拟路由器的基本步骤 :

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，则不能修改区段到虚拟路由器的绑定。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 虚拟路由器。
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 安全区被绑定到 trust-vr 虚拟路由器，ethernet3 接口被绑定到 Untrust 安全区。(Untrust 安全区没有绑定其它接口。) 必须先将 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 安全区绑定到 untrust-vr 虚拟路由器。

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、区段和虚拟路由器之间的绑定。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、区段和虚拟路由器之间的绑定；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
------------------------------------------------------------
```

自定义虚拟路由器

某些 NetScreen 设备[1] 允许您除了使用两个预定义的虚拟路由器外，还可以创建自定义虚拟路由器。可以修改用户定义虚拟路由器的所有方面，包括虚拟路由器 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 : 创建自定义虚拟路由器

在本例中，将创建一个名为 trust2-vr 的自定义虚拟路由器，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 设备支持自定义虚拟路由器。要创建自定义虚拟路由器，需要有软件许可密钥。

范例：删除自定义虚拟路由器

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

WebUI

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])，请键入 **Y**。

```
save
```

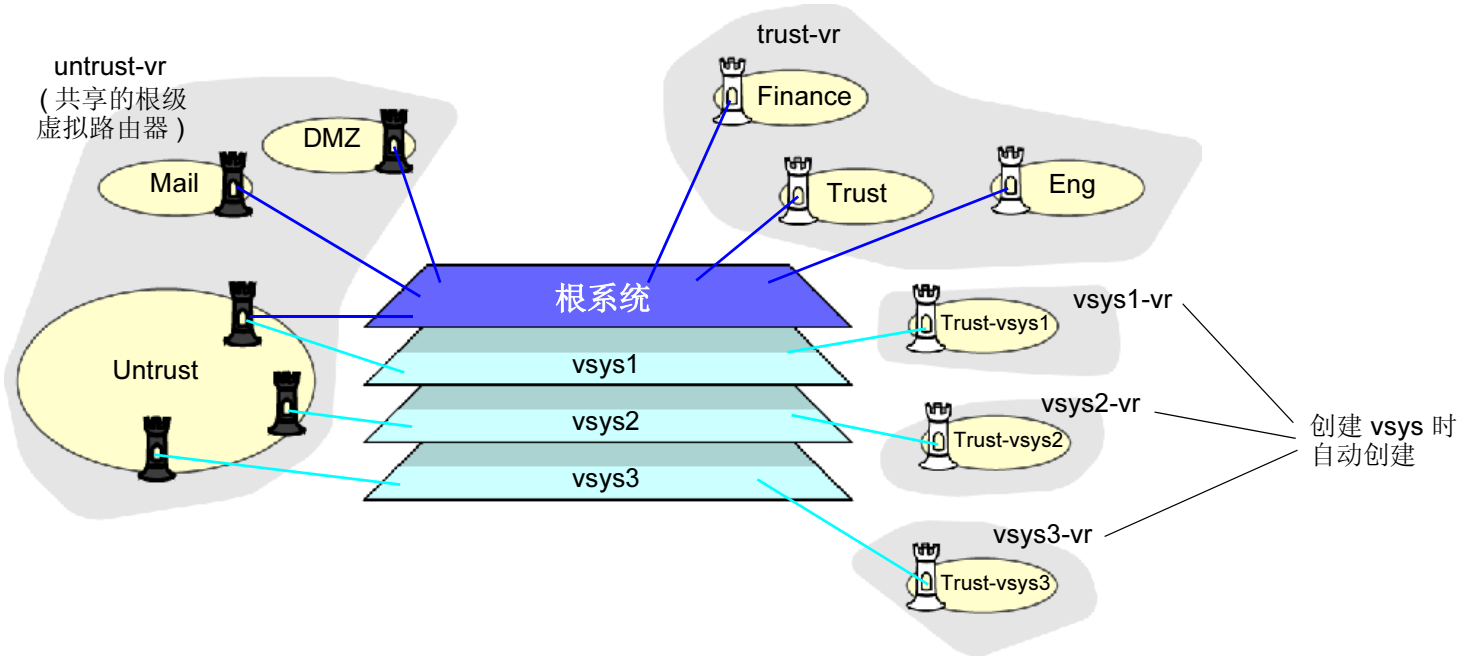
注意：*不能删除预定义的 untrust-vr 和 trust-vr 虚拟路由器，但可以删除任何用户定义的虚拟路由器。要修改用户定义虚拟路由器的名称或更改虚拟路由器 ID，必须先删除该虚拟路由器，然后用新的名称或虚拟路由器 ID 重新创建它。*

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 :

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

可以为 vsys 定义一个或多个自定义虚拟路由器。有关虚拟系统的详细信息，请参阅第 **7**-1 页上的 “虚拟系统”。在下图中，三个 vsys 各有两个与之相关的虚拟路由器 : 名为 *vsysname*-vr 的 vsys 级虚拟路由器以及 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 VR

在本例中，将为 vsys my-vsys1 定义一个自定义虚拟路由器 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
```

在以下提示后键入 **Y**:

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

在创建 vsys 时创建的 vsys 级虚拟路由器是 vsys 的缺省虚拟路由器。可以将 vsys 的缺省虚拟路由器更改为自定义虚拟路由器。例如，将本例中先前创建的自定义虚拟路由器 vr-1a 设置成 vsys my-vsys1 的缺省虚拟路由器：

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 Trust-*vsysname* 被绑定到创建 vsys 时创建的 vsys 级虚拟路由器。当然，可以将预定义安全区 Trust-*vsysname* 及任何用户定义的 vsys 级安全区绑定到可供 vsys 使用的任意虚拟路由器上。

在缺省情况下， untrust-vr 可被所有 vsys 共享。虽然不能共享 vsys 级的虚拟路由器，但可以定义任何根级虚拟路由器供 vsys 共享。这样，即可在 vsys 级的虚拟路由器中定义路由，将共享的根级虚拟路由器用作下一跳跃。还可以在 vsys 级虚拟路由器和共享的根级虚拟路由器之间配置路由的重新分配。

范例 : 使用共享的 VR 定义路由

在本例中，根级虚拟路由器 my-router 包含指向网络 4.0.0.0/8 的路由表条目。如果配置根级虚拟路由器 my-router 可被 vsys 共享，则可以在 vsys 级虚拟路由器中定义指向目的地址 4.0.0.0/8 的路由，并将 my-router 作为下一跳跃。在本例中， vsys 是 my-vsys1， vsys 级虚拟路由器是 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
```

在以下提示后键入 **Y**:

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

修改虚拟路由器

可通过 WebUI 或 CLI 修改预定义或自定义虚拟路由器。例如，修改虚拟路由器 trust-vr:

WebUI

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

CLI

```
set vrouter trust-vr
```

可以修改虚拟路由器的下列参数 :

- 虚拟路由器 ID (有关详细信息，请参阅第 14 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 16 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 17 页上的 “路由优选级”)
- 指示虚拟路由器根据数据包的源 IP 地址转发信息流 (在缺省情况下，虚拟路由器根据数据包的目的 IP 地址转发信息流。有关详细信息，请参阅第 19 页上的 “基于源的路由”。)
- (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跃
- (仅限于缺省的根级虚拟路由器) 让动态路由 MIB 的 SNMP 陷阱变成私有
- 允许将非活动接口上的路由看作通告 (在缺省情况下，只能将活动接口上定义的活动路由重新分配给其它协议或导出到其它虚拟路由器。)
- 指示虚拟路由器忽略接口子网地址的重叠 (在缺省情况下，不能为同一虚拟路由器中的接口配置重叠的子网 IP 地址。)
- 允许虚拟路由器与其 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 会将 VR 中活动接口的最高 IP 地址自动选择为路由器标识符。

注意：*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 虚拟路由器使用同一个路由器 ID，因此上述做法可能会产生路由问题。因此，NetScreen 建议您始终明确分配虚拟路由器 ID，该路由器 ID 在网络中应是唯一的。可以将虚拟路由器 ID 设置成 loopback 接口的地址，前提是该 loopback 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 8 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 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

每个虚拟路由器都从一个系统级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] 及设备上配置的虚拟路由器个数。可以限制为特定虚拟路由器分配的最大路由表条目数。这样有利于防止某虚拟路由器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 (对于 trust-vr): 输入以下内容，然后单击 **OK**:

Maximum Route Entry:

Set limit at: (选择), 20

CLI

```
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。如果表中包含多个路由指向同一目的地址，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]。

路由优选级

路由优选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，虚拟路由器会根据获知该路由的协议为该路由添加一个优选级值。低优选级值 (接近 0 的数) 优先于高优选级值 (远离 0 的数)。

在虚拟路由器中，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选级值，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) 的优选级发生了变化，新的优选级将显示在路由表中。但要等到重新获知 (通过先禁用、后启用动态路由协议来实现) 该路由后，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 : 设置路由优选级

在本例中，您将为任何将被添加到 untrust-vr 的路由表中的 “直连[5]” 路由指定优选级值为 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. 当路由器有一个 IP 地址在目标网络上的接口时，就会有一条直连路由。

路由度量

路由度量用于确定封包到达给定目标采取的最佳路径。路由器使用路由度量来权衡到达同一目标的两个路由，并确定选择使用哪个路由。如果存在多个路由指向同一目的网络，则度量值最小的路由优先。

路由度量可以根据封包到达目标必须经过的路由器数量、路径的相对速度和带宽、组成该路径的链接成本得出，也可以将这些因素 (和其它因素) 综合在一起来确定。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。直连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其它度量值。

基于源的路由

可以指示 ScreenOS 虚拟路由器根据数据包的源 IP 地址 (不只局限于目的 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。

在缺省情况下，ScreenOS 只使用目的 IP 地址在虚拟路由器的路由表中查找最佳路由。在虚拟路由器上启用基于源的路由后， ScreenOS 会先根据源 IP 地址执行路由表查找。如果 ScreenOS 根据源 IP 地址找不到路由，则会使用目的 IP 地址查找路由。

在特定虚拟路由器上可以将基于源的路由定义为静态路由。基于源的路由只能在配置它们的虚拟路由器生效。例如，不能将其它虚拟路由器指定为基于源的路由的下一跳跃。也不能将基于源的路由重新分配给其它虚拟路由器或路由协议。

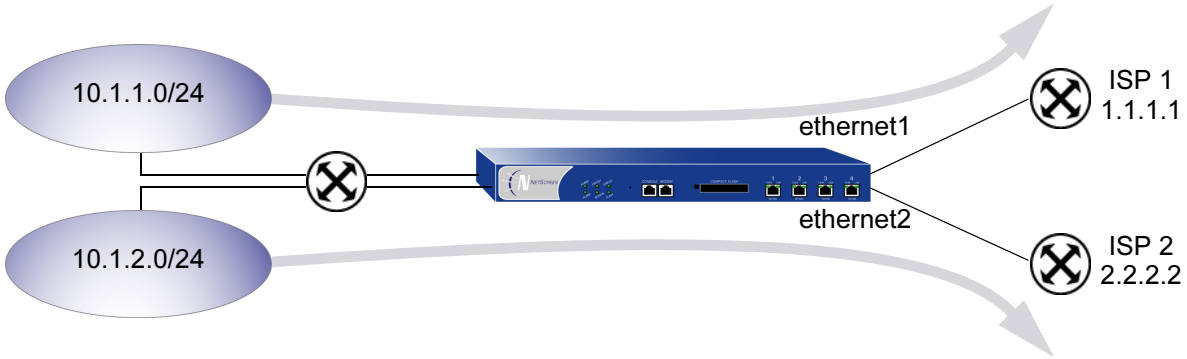
使用此功能 :

1. 要为特定虚拟路由器创建一个或多个基于源的路由，请指定以下信息 :
   - 应用基于源的路由的虚拟路由器的名称
   - ScreenOS 执行路由表查找依据的源 IP 地址 (此地址作为路由表条目出现。)
   - 转发封包的外向接口的名称
   - 基于源的路由的下一跳跃 (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跃。不能指定另一个虚拟路由器作为基于源的路由的下一跳跃。)
   - 基于源的路由的度量值 (如果有多个基于源的路由具有同一前缀，设备只使用度量值最低的路由执行路由查找，并将具有同一前缀的其它路由标上 “inactive” 字样。)
2. 在虚拟路由器上启用基于源的路由。在指定虚拟路由器中查找任意路由表时，ScreenOS 先使用封包的源 IP 地址作为查找依据。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

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：

- 子网 10.1.1.0/24，转发接口为 ethernet1，下一跳跃为 ISP 1 的路由器 (1.1.1.1)
- 子网 10.1.2.0/24，转发接口为 ethernet2，下一跳跃为 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: ethernet1 (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: ethernet2 (选择)

Gateway IP Address: 2.2.2.2

***注意：**在 WebUI 中，缺省度量值为 1。*

Network > Routing > Source Routing: 选择 **Source Routing** (对于 trust-vr)。

CLI

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

路由重新分配

虚拟路由器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 (例如 OSPF、 RIP 或 BGP) 只将满足以下条件的路由通告给其邻接方或对等方 :

- 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 协议的路由域，则 OSPF 域必须从 BGP 域中导入所有路由，以通知其所有 OSPF 邻接方如何到达 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。将路由添加到虚拟路由器的路由表时，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。从虚拟路由器的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 *Route Map*，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 接口的直连路由。
7. 在任意两个协议之间，可以只定义一条重新分配规则。

配置 Route Map

Route Map 由一组语句构成，设备按先后顺序在路由上应用这些语句。Route Map 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 Route Map 中指定的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 Route Map 语句中的条件匹配，该路由不是允许就是被拒绝。Route Map 语句还能修改匹配路由的特定属性。每次比较到 Route Map 结尾，都意味着明确的拒绝；换言之，如果某路由不与任何 Route Map 条目匹配，则该路由被拒绝。

下面是可在 Route Map 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 26 页上的 “路由过滤”。
BGP Community	用于匹配指定的公共组列表。请参阅第 26 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 26 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 26 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，则可设置该路由的可选属性值。可以在 Route Map 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。
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。
RIP offset metric	在 1-16 之间设置匹配路由的偏移值。偏移值会增加度量值，从而降低该路径被选中的几率。
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跃设置成指定 IP 地址。
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、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：从路由对等方发出的内向路由；从 NetScreen 虚拟路由器发出、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，属于路由信息的一部分。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 108 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 116 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。

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: permit
- IP Address/Netmask Filtering: 1.1.1.1/24
- Sequence Number: 10 (访问列表中该语句到其它语句的相对位置)

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 : 将路由重新分配给 OSPF

在本例中，将重新分配通过自治系统 65000 进入 OSPF 的指定 BGP 路由。首先配置 AS 路径列表，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 108 页上的 “AS 路径访问列表”。）接着，将配置 Route Map “rtmap1”，以便匹配 AS 路径访问列表中的路由。最后，在 OSPF 中使用 Route Map “rtmap1” 指定重新分配规则，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. Route Map

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. Route Map

```
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 VR 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，则可以允许一个 VR 获知另一个 VR 上的特定路由。要进行此操作，必须在源 VR 上定义*导出规则*，随后源 VR 会将路由导出到目的 VR 中。导出路由时，虚拟路由器允许其它 VR 获知其网络。在目的 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。如果目的 VR 上没有导入规则，它会接受导出的全部路由。

在虚拟路由器之间导出和导入路由：

1. 在源 VR 上，定义导出规则。
2. （可选）在目的 VR 上，定义导入规则。此步骤可选，通过导入规则，可以进一步控制目的虚拟路由器从源虚拟路由器接受的路由。

在 NetScreen 设备上，可通过指定以下信息配置导出或导入规则：

- 目的虚拟路由器（对于导出规则）或源虚拟路由器（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 / 导入路由的新属性或修改属性

配置导出、导入规则与配置重新分配规则类似。可以配置 *Route Map*，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虚拟路由器，以便自动向其它虚拟路由器导出路由。不能导出网络中与 NAT 模式的接口直连的路由。

范例：配置导出规则

在本例中，trust-vr 虚拟路由器中指向网络 1.1.1.1/24 的 OSPF 路由将被导出到 untrust-vr 路由域中。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 Route Map “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 虚拟路由器中。

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. Route Map

   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. Route Map

```
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
```

2

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。其中覆盖以下主题：

OSPF 概述

“开放式最短路径优先” (OSPF) 路由协议是用于在单个 “自治系统” (AS) 内部运行的 “内部网关协议” (IGP)。运行 OSPF 的路由器通过在整个 AS 内部定期发布*链接状态通告* (LSA)，来发布其状态信息 (例如可用接口以及邻接方可达性等)。

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。 LSA 遍及路由域内部的持续发布将使 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，确定到达 AS 内部任意网络的最佳路径。这通过生成*最短路径树*完成，它是到达 AS 内部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，所有路由器都被分组到名为 area 0 (通常表示为 area 0.0.0.0) 的单个 “骨干” 区域中。。但是地理分布较广的网络通常会被分割到多个区域中。这是因为随着网络的扩展，链接状态数据库也会不断扩张，将其分成较小的组，会令其更易扩展。

区域可以减少网络内流通的路由信息量，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。切记，所有区域都必须与 area 0 直接相连，只有一个区域例外 (稍后介绍)。

AS 外部通告描述的路由指向其它自治系统的目的地址，这些外部通告遍及整个 AS。可以将特定 OSPF 区域配置为 *Stub 区域*； AS 外部通告不会遍及这些区域。 OSPF 中使用两类常见的 Stub 区域 :

- **Stub 区域** - 一个区域，对于通过非 OSPF 源 (例如 BGP) 获取的路由，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 Stub 区域中不允许汇总路由，可将其看成*完全剩余区域*。
- **Not So Stubby 区域 (NSSA)** - 类似正常的 Stub 区域，但 NSSA 不能从当前区域外的非 OSPF 源接收路由。但是，仍可获取区域内被检测到的外部路由，并将其传递到其它区域。

路由器分类

参与 OSPF 路由的路由器根据其在网络中的功能或位置进行分类 :

- **内部路由器** - 所有接口都属于同一区域的路由器。
- **骨干路由器** - 有一个接口在骨干区域的路由器。
- **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 汇总来自非骨干区域的路由，以便发布到骨干区域。在运行 OSPF 的 NetScreen 设备上，在缺省情况下创建骨干区域。如果在 ScreenOS 上创建了第二个区域，该设备将作为 ABR 运行。
- **AS 边界路由器** - 某个 OSPF 区域与另一 AS 相接时，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 路由信息。

Hello 协议

如果两个路由器在同一子网络上都具有接口，则被认为是相互*邻接*。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*。如果两个路由器之间未建立邻接，则它们不能交换路由信息。

如果某个网络上具有多个路由器，则必须将其中一个路由器建立为*指定路由器* (DR)，将另一个建立为*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信息的路由器。如果 DR 失效， BDR 将成为指定路由器。

网络类型

ScreenOS 支持以下网络类型 :

- 广播网络
- 点对点网络

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播送到所有相连的路由器。广播网络上的路由器对，被认定为可相互通信。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 封包发送到组播地址 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*是连接多个路由器的网络，但它不能将消息播送到相连路由器。在非广播网络上，需要将以往多点广播的 OSPF 协议封包发送到每一个邻接路由器。 ScreenOS 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。点对点网络的一个实例是两台通过 IPSec VPN 通道连接的 NetScreen 设备。在点对点网络上， OSPF 路由器将 Hello 封包发送到多点传送地址 224.0.0.5，动态检测其邻接路由器。

链接状态通告

每个 OSPF 路由器都会发出定义路由器本地状态信息的 LSA。另外，根据路由器的 OSPF 功能，路由器还可发出其它类型的 LSA。下表为这些 LSA 类型的汇总：

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	描述到达区域外但仍在 AS 内的目的地的路由。有两种类型： 类型 3 LSA 摘要描述到达网络的路由。 类型 4 LSA 摘要描述到达 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

类似 RIP 和 BGP，可以为 NetScreen 设备上的每个虚拟路由器创建 OSPF。如果一个系统中存在多个虚拟路由器 (VR)，则可启用多个 OSPF 实例，为每个 VR 创建一个 OSPF 实例。。

注意：在 NetScreen 设备上配置动态路由协议之前，应分配一个虚拟路由器 ID，如第 1 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 路由实例。此步骤还会自动创建一个 OSPF 骨干区域，区域 ID 为 0.0.0.0，不能删除该区域 ID。
2. (可选) 除非所有 OSPF 接口都连接到骨干区域，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，则需创建新的 OSPF 区域 (除骨干区域外)。可将新区域配置为正常、Stub 或 NSSA 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，含骨干区域。
4. 在每个接口上启用 OSPF。
5. 验证 OSPF 配置正确且运行正常。

本节介绍如何使用 CLI 或 WebUI，执行下例所示的每一项任务。在本例中，将配置 NetScreen 设备充当 ABR，通过接口 ethernet3 接口连接到 area 0，并通过 ethernet1 接口连接到 area 10。

还可以配置其它可选 OSPF 参数，如下所示：

- 全局参数，例如虚拟链接，根据 OSPF 协议在 VR 级上设置 (请参阅第 53 页上的 “全局 OSPF 参数”)
- 接口参数，例如认证，根据 OSPF 协议在每个接口上设置 (请参阅第 59 页上的 “OSPF 接口参数”)
- 与安全相关的 OSPF 参数，即可以在 VR 级上设置，也可以在每个接口上设置 (请参阅第 62 页上的 “安全配置”)

创建 OSPF 路由实例

在 NetScreen 设备的特定虚拟路由器上创建并启用 OSPF 路由实例。创建 OSPF 路由实例时还会自动创建 OSPF 骨干区域。在 VR 上创建并启用 OSPF 路由实例后， OSPF 将在 VR 中所有启用 OSPF 的接口上传输及接收封包。

范例：创建 OSPF 实例

在下例中，首先为 trust-vr 虚拟路由器分配路由器 ID 0.0.0.10。接着在 trust-vr 上创建 OSPF 路由实例。 (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 1 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 路由实例

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

> ***注意：*** *在 CLI 中，必须先创建 OSPF 路由实例，然后才能启用它。因此，必须发出两个独立的 CLI 命令，以启用 OSPF 路由实例。*

范例：删除 OSPF 实例

在本例中，将禁用 trust-vr 中的 OSPF 路由实例。 OSPF 会禁止 trust-vr 中所有启用 OSPF 的接口传输及处理封包。

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 路由实例。*

定义 OSPF 区域

区域可以减少网络内需要流通的路由信息量，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。

所有区域都必须连接到 area 0。在缺省情况下，在 NetScreen 虚拟路由器上创建 OSPF 路由实例时，该虚拟路由器会定义 area 0。如需创建其它 OSPF 区域，可根据需要将其定义为 stub 区域或 NSSA 区域。有关上述区域类型的详细信息，请参阅第 36 页上的 “区域”。

可以配置下列可选区域参数 :

区域参数	说明	缺省值
缺省路由的度量	(仅限于 NSSA 和 stub 区域) 指定缺省路由通告的度量值。	1
缺省路由的 度量类型	(仅限于 NSSA 区域) 指定缺省路由的外部度量类型 (1 或 2)。	1
无汇总	(仅限于 NSSA 和 stub 区域) 指定*不*将汇总 LSA 通告给区域。	将汇总 LSA 通告给区域
范围	区域范围 (所有区域) 指定要在汇总 LSA 中通告的 IP 地址汇总以及是否通告它们。	

范例 : 创建 OSPF 区域

在下例中，将创建区域 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 不汇总从一个区域指向另一个区域的路由。通过配置区域范围，可将某区域内的一组子网统一成单个网络地址，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 :

- 10.1.1.0/24 将被通告
- 10.1.2.0/24 不被通告

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，VR 的接口上一律未启用 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输或接收封包，但接口配置参数仍将保留。

注意： 如果禁用了 VR 中的 OSPF 路由实例 (请参阅第 42 页上的“范例 : 删除 OSPF 实例”)，OSPF 会禁止在 VR 中所有启用 OSPF 的接口上传输及处理封包。

范例 : 在接口上启用 OSPF

在本例中，将在 ethernet1 (先前分配给 area 10) 和 ethernet3 接口 (先前分配给 area 0) 上启用 OSPF 路由实例。

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 : 禁用接口上的 OSPF

在本例中，只禁用 ethernet1 接口上的 OSPF 路由实例。注意，仍然可以在 trust-vr 虚拟路由器中启用了 OSPF 的其它任何接口上传输及处理 OSPF 封包。

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
```

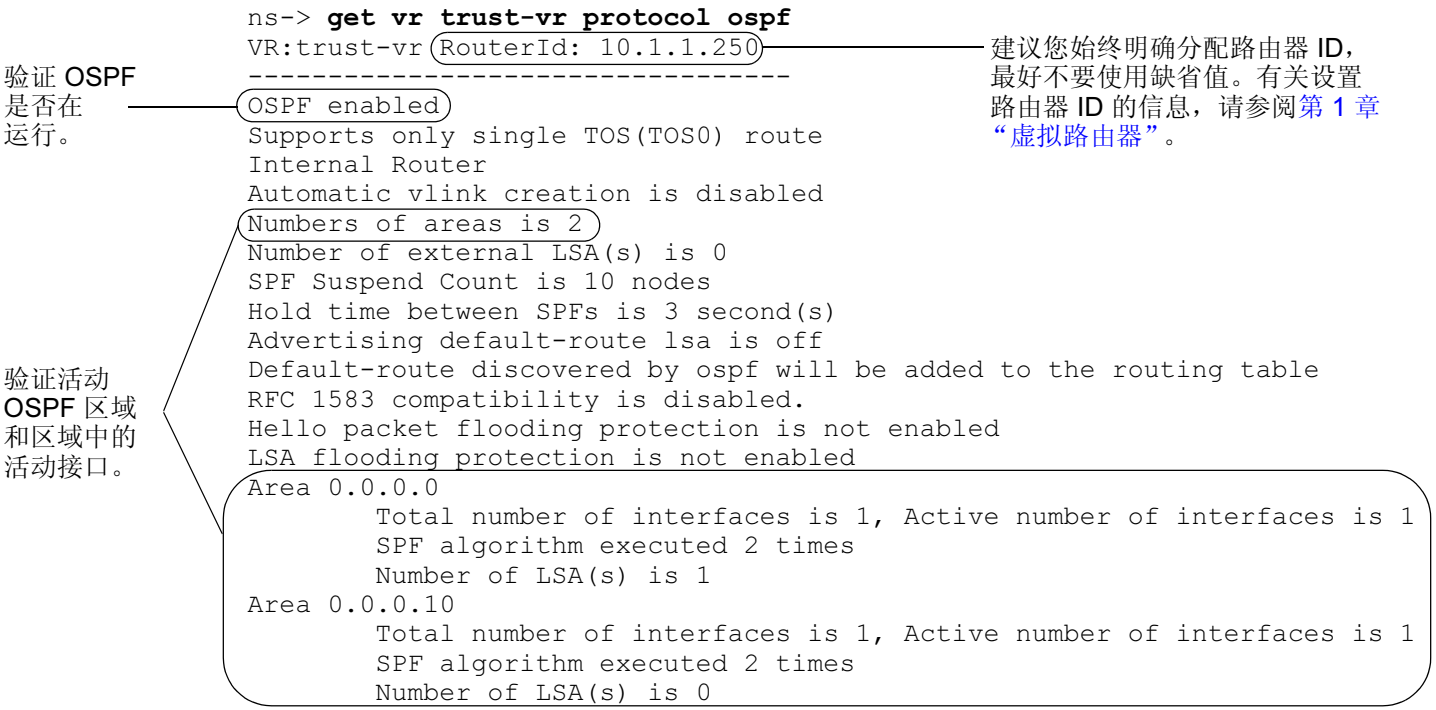
注意 : 如果禁用了 VR 中的 OSPF 路由实例 (请参阅第 42 页上的“范例 : 删除 OSPF 实例”)，OSPF 会禁止在 VR 中所有启用 OSPF 的接口上传输及处理封包。

验证配置

通过执行以下 CLI 命令，可以查看通过 WebUI 或 CLI 输入的配置信息：

```
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
```

通过执行以下 CLI 命令，可以验证 VR 上运行的 OSPF:



通过执行以下 CLI 命令，可以验证接口上是否启用 OSPF 并查看接口的状态：

```
ns-> get vr 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
```

可以为虚拟路由器配置优先级，作为被选为 DR 或 BDR 的依据。请参阅第 59 页上的 “OSPF 接口参数”。

通过执行以下 CLI 命令，可以验证 NetScreen 设备上的 OSPF 路由实例是否已和 OSPF 邻接方之间建立邻接关系：

```
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
```

表明已和这些接口上的邻接方建立了全面的邻接关系。

重新分配路由

路由重新分配是指在路由选择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 VR 中的 OSPF 路由实例：

- 通过 BGP 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 Route Map，以过滤重新分配的路由。有关为重新分配路由创建 Route Map 的详细信息，请参阅第 1 章 “虚拟路由器”。

范例：将路由重新分配给 OSPF

在下例中，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名为 add-bgp 的 Route Map。

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 路由实例后，可将多个路由捆绑成一个统一或*汇总*网络路由。通过汇总多个地址，可将一系列路由看作一个路由，从而简化了处理。

在复杂的大型网络中使用路由汇总的一个优点是，可以将拓扑变化与其它路由器隔离开。即，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修改其路由表。

除减少了骨干路由器上路由表中的条目外，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。可汇总区域内路由或外部路由。

范例 : 汇总重新分配的路由

在下例中，要将 Route Map add-bgp 定义的 BGP 路由重新分配给当前的 OSPF 路由实例。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
```

全局 OSPF 参数

本节介绍可以在 VR 级上配置的可选 OSPF 全局参数。在 VR 级上配置 OSPF 参数后，该参数设置会影响所有启用 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 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。还可以指定度量值 / 是否保留路由的初始度量以及度量类型 (ASE 类型 1 或类型 2)。还可以指定始终通告缺省路由。	不通告缺省路由。
Reject default route	指定不将 OSPF 中获知的任何缺省路由添加到路由表中。	将 OSPF 中获知的缺省路由添加到路由表中。
Automatic virtual link	指定虚拟路由器无法达到 OSPF 骨干时自动创建虚拟链接。	禁用
Maximum hello packets	指定虚拟路由器在一个 hello 接口上接收的最大 OSPF hello 封包数。	10
Maximum LSA packets	指定虚拟路由器在指定的几秒内接收的最大 OSPF LSA 封包数。	无缺省值
RFC 1583 compatibility	指定 ScreenOS OSPF 路由实例与早期 OSPF 版本 RFC 1583 兼容。	ScreenOS 支持 OSPF 版本 2，如 RFC 2328 中定义。
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、传输延迟或邻接方不工作间隔。	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的网络匹配，即使有更特定的前缀覆盖该缺省路由。

在下例中，将通告当前 OSPF 路由实例的缺省路由。

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 网络中的所有区域都必须直接连接到骨干区域。有时，需要创建一个不能实际连接到骨干区域的新区域。为解决此问题，可创建一个虚拟链接。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骨干区域相连。

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：

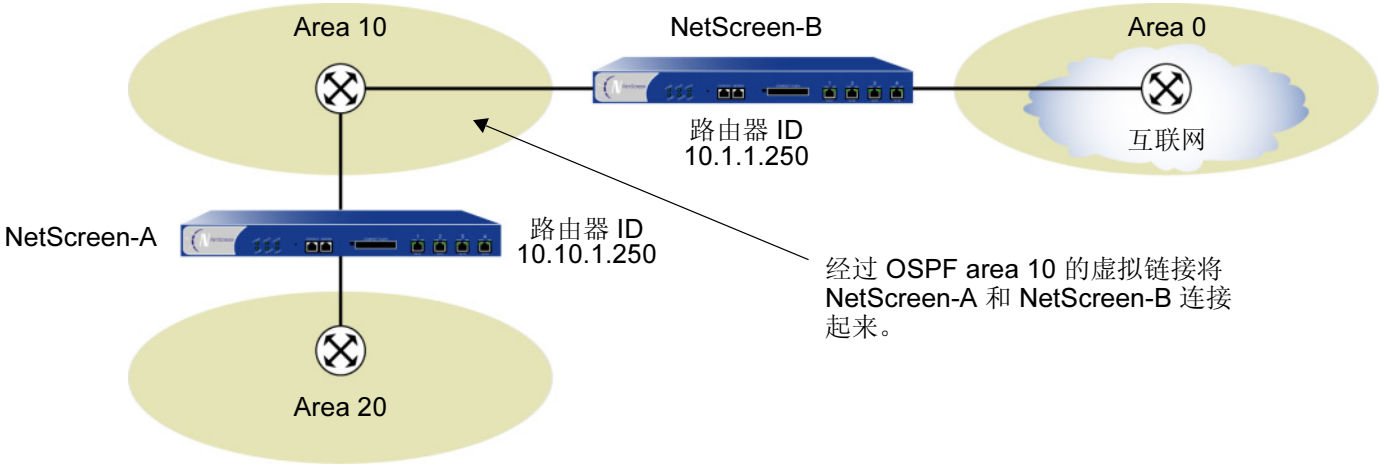
- 虚拟链接经过的 OSPF 区域的 ID。不能创建经过骨干或 Stub 区域的虚拟链接。
- 虚拟链接另一端路由器的 ID。

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 邻接方的响应起，经过多少秒后邻接方决定停止运行。	40 秒
Hello interval	指定 OSPF 连续发送 hello 封包间隔的秒数。	10 秒
Retransmit interval	指定经过多少秒后，接口向不响应初始 LSA 的邻接方重新发送 LSA。	5 秒
Transmit delay	指定传输接口上发送的链接状态更新封包间隔的秒数。	1 秒

范例：创建虚拟链接

在下例中，将创建一个通过 OSPF area 10 的虚拟链接，一端连接到 NetScreen-A (路由器 ID 为 10.10.1.250)，另一端连接到 NetScreen-B (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 1 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 设备上识别虚拟链接另一端设备的路由器 ID。



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 VR 无法到达网络骨干时，可引导 VR 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。在下例中，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

本节介绍在接口级上配置的 OSPF 参数。在接口级上配置 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 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。接口的相关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 (越满足需求)。	1 代表大于等于 100 MB 的链接 10 代表 10 MB 链接 100 代表 1 MB 链接
Dead interval	指定自收不到 OSPF 邻接方的响应起，经过多少秒后 OSPF 决定停止运行邻接方。	40 秒
Hello interval	指定 OSPF 向网络发送 hello 封包的时间间隔，以秒为单位。	10 秒
Link type	将接口指定为点对点链接。	将以太网接口看作广播接口
Neighbor list	以一个或多个访问列表的形式，指定有资格构成邻接关系的 OSPF 邻接方所在的子网。	无 (与接口上的所有邻接方均能构成邻接关系)

OSPF 接口参数	说明	缺省值
Passive Interface	指定作为 OSPF 路由 (而非外部路由) 通告给 OSPF 域的接口 IP 地址，但该接口不传输或接收 OSPF 封包。当接口上同时启用了 BGP 时此选项非常有用。	启用 OSPF 的接口传输并接收 OSPF 封包
Priority	指定虚拟路由器的优先级，作为选择 “指定路由器” 或 “备份指定路由器” 时的依据。路由器的优先级值越大，越有可能 (但不一定) 选中。	1
Retransmit interval	指定经过多少秒后，接口向不响应初始 LSA 的邻接方重新发送 LSA。	5 秒
Transit delay	指定传输接口上发送的链接状态更新封包间隔的秒数。	1 秒

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、 dead 间隔和重新传输间隔值。*

范例 : 设置 OSPF 接口参数

在本例中，将为 ethernet1 接口配置以下 OSPF 参数 :

- 将 OSPF hello 消息间隔的时间增加到 15 秒。
- 将 OSPF 重新传输间隔的时间增加到 7 秒。
- 将 LSA 传输间隔的时间增加到 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，应在同一安全级别上配置 OSPF 域中的所有路由器。否则，只要一个 OSPF 路由器遭受破坏，整个 OSPF 路由域都有可能瘫痪。*

认证邻接方

由于 LSA 没有加密且多数协议分析器都提供 OSPF 封包的解封机制，因此 OSPF 路由器很容易被欺骗。认证 OSPF 邻接方是防止这类攻击的最佳方法。

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

对于发送方和接收方 OSPF 路由器，MD5 认证使用同一个密钥。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封包的情况下，定期更改成对路由器上的 MD5 密钥。

范例：配置明文密码

在本例中，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。注意，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) > OSPF: 输入以下内容，然后单击 **Apply**:

Authentication:

MD5 Keys: (选择)

1234567890123456

9876543210987654

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 active-md5-key-id 1
save
```

过滤 OSPF 邻接方

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。

在缺省情况下， NetScreen 虚拟路由器上的 OSPF 路由实例与启用 OSPF 的接口上正在通信的所有 OSPF 邻接方建立邻接关系。通过定义包含符合条件的 OSPF 邻接方的子网列表，可以限制接口上的设备与 OSPF 路由实例构成邻接关系。只有指定子网内的主机或路由器可以与 OSPF 路由实例构成邻接关系。要指定包含符合条件的 OSPF 邻接方的子网，需要在虚拟路由器级上定义子网的访问列表。

范例 : 配置邻接方列表

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

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) 加入路由域中，以便将封包返回给自己。随后，该路由器既可以丢弃封包，引发服务中断，也可以在转发封包之前获得封包中的机密信息。在 NetScreen 设备上，在缺省情况下 OSPF 接受在 OSPF 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 : 删除缺省路由

在下例中，将指定不从 OSPF 获取缺省路由。

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能使用 OSPF hello 封包或 LSA 欺骗其邻接方。通过 LSA，OSPF 路由器可以为链接状态数据库提供设备、网络和路由信息。每个路由器都从网络上其它路由器发送的 LSA 检索信息，为路由表提取路径信息。使用 LSA 泛滥保护，可管理进入虚拟路由器的 LSA 数量。如果虚拟路由器接收的 LSA 过多，路由器将由于 LSA 泛滥而失败。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 虚拟路由器上，可以配置每个 hello 间隔内接收的最大 hello 封包数以及某时间间隔内在 OSPF 接口上接收的最大 LSA 数。超过配置的临界值的封包将被丢弃。在缺省情况下，OSPF hello 封包的临界值为每个 hello 间隔 10 个封包 (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 个封包。 Hello 间隔保持缺省值 10 秒不变，可以在每个 OSPF 接口上配置该间隔。

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

在本例中，将创建每 10 秒钟 10 个封包的 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: 10

Maximum LSAs: 10

CLI

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

3

路由信息协议 (RIP)

本章介绍 NetScreen 设备上的 “路由信息协议” (RIP) 版本 2 路由协议。其中覆盖以下主题：

RIP 概述

“路由信息协议”(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，如同 RFC 2082 的定义。

如上文所述， RIP 适用于中等规模的网络，还可以使用 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 个跳跃。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 个跳跃，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 不支持 “点对多点”接口。

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。

RIP 路由数据库包含的每个条目代表可通过 RIP 路由实例到达的每个目的地址。 RIP 路由数据库包括以下信息 :

- 目标的 IPv4 地址。注意 RIP 不区分网络与主机。
- 第一个路由器的 IP 地址以及指向目的地址的路由 (下一跳跃)。
- 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 作为每个经过网段的度量值。
- 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

类似 OSPF 和 BGP，可以在 NetScreen 设备上为每个虚拟路由器创建 RIP。如果系统中存在多个虚拟路由器 (VR)，则可启用多个 RIP 实例，每个 VR 实施一个实例。

***注意：**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，如第 1 章 “虚拟路由器”中所述。*

本节介绍在 NetScreen 设备上配置 RIP 的基本步骤：

1. 在虚拟路由器中创建 RIP 路由实例。
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。

本节将逐一介绍如何使用 CLI 或 WebUI 执行上述任务。

还可以配置其它的可选 RIP 参数，如下所示：

- 全局参数，例如计时器和可信任 RIP 邻接方，根据 RIP 协议在 VR 级上设置 (请参阅第 78 页上的 “全局 RIP 参数”)
- 接口参数，例如邻接方认证，根据 RIP 协议为每个接口设置 (请参阅第 80 页上的 “RIP 接口参数”)
- 与安全相关的 RIP 参数，既可以在 VR 级上设置，也可以为每个接口设置 (请参阅第 82 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 路由实例。在 VR 上创建并启用 RIP 路由实例后，通过 RIP 可在 VR 中所有启用 RIP 的接口上传输及接收封包。

在 VR 中删除 RIP 路由实例后，VR 中所有接口的相应 RIP 配置也会被删除。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 1 章 “虚拟路由器”。

范例 : 创建 RIP 实例

在下例中，将为虚拟路由器 trust-vr 分配路由器 ID 0.0.0.10。随后，将在 trust-vr 上创建一个 RIP 路由实例。

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. RIP 路由实例

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 路由实例

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

> ***注意：*** *在 CLI 中，必须先创建 RIP 路由实例，然后才能启用它。因此，必须发出两个独立的 CLI 命令，以启用 RIP 路由实例。*

范例：删除 RIP 实例

在本例中，将禁用 trust-vr 中的 RIP 路由实例。随后 RIP 会停止 trust-vr 中所有启用 RIP 的接口传输及处理封包。

WebUI

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

Network > Routing > Virtual Router (trust-vr) > Edit > Delete RIP Instance，并在确认提示后输入 **OK**。

CLI

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

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

在接口上启用 RIP

在缺省情况下， VR 中的所有接口都未启用 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封包。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 路由实例 (请参阅第 73 页上的 “范例 : 删除 RIP 实例”)， RIP 会禁止 VR 中所有启用 RIP 的接口传输及处理封包。

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 : 禁用接口上的 RIP

在本例中，将禁用 Trust 接口上的 RIP。

WebUI

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

CLI

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

重新分配路由

路由重新分配是指在路由选择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 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 Route Map 过滤重新分配的路由。有关为重新分配的路由创建 Route Map 的详细信息，请参阅第 1 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 1。可以更改缺省度量值 (请参阅第 78 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 虚拟路由器中的 RIP 邻接方。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 Route Map，该 Route Map 允许与配置的访问列表相匹配的地址。使用 Route Map，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 acc-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
```

全局 RIP 参数

本节介绍可以在 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 (例如 OSPF 或 BGP) 导入 RIP 的路由的缺省度量值。	10
Update timer	指定何时将 RIP 路由的更新发给邻接方，以秒为单位。	30 秒
Maximum packets per update	指定每次更新时接收的最大封包数。	无最大值
Invalid timer	指定自邻接方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 秒
Flush timer	指定自路由失效起，经过多久后被删除，以秒为单位。	120 秒
Maximum neighbors	允许的最大 RIP 邻接方数。	16
Trusted neighbors	指定定义 RIP 邻接方的访问列表。如果不指定邻接方， RIP 会通过组播或广播来检测接口上的邻接方	所有邻接方都是可信任的
Allow neighbors on different subnet	允许在不同子网中指定 RIP 邻接方。	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。	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

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 邻接方。以下命令将缺省路由通告给 trust-vr 虚拟路由器中的 RIP 邻接方，度量值为 5 (必须自行输入)。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 poison-reverse，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)。	禁用
RIP metric	指定接口的 RIP 度量。	1
Authentication	指定明文密码或 MD5 认证。	不使用认证。
Passive mode	指定接口只能接收 RIP 封包，但不能传输该封包。	No
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

可以在 VR 级或接口级上定义内向和外向 Route Map 的过滤器。在接口级上定义的 Route Map 过滤器优先于在 VR 级上定义的 Route Map 过滤器。例如，如果在 VR 级上定义了一个内向 Route Map，并在接口级上定义了另一个内向 Route Map，则接口级上定义的内向 Route Map 优先。

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 poison reverse。

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，应在同一安全级别上配置 RIP 域中的所有路由器。否则，只要一个 RIP 路由器遭受破坏，整个 RIP 路由域都有可能瘫痪。*

邻接方认证

由于 RIP 封包没有加密且多数协议分析器都提供 RIP 封包的解封机制，因此 RIP 路由器很容易被欺骗。 RIP 邻接方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，验证从邻接方接收的 RIP 封包。接口上收到的所有未经验证的 RIP 封包都会被丢弃。在缺省情况下， RIP 接口一律不启用认证。

对于发送方和接收方 RIP 路由器，MD5 认证均使用同一个密钥。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封包的情况下，定期更改一对路由器上的 MD5 密钥。

范例 : 配置 MD5 密钥

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。注意，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 邻接方

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 邻接方的设备。在缺省情况下，RIP 邻接方只能是 NetScreen 虚拟路由器所在子网中的设备。

范例 : 配置可信任邻接方

在本例中，将为 trust-vr 虚拟路由器中运行的 RIP 路由实例配置以下全局参数 :

- 最大邻接方数为 1。
- 可信任邻接方的 IP 地址 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，以便将封包返回给自己。随后，该路由器既可以丢弃封包，引发服务中断，也可以在转发封包之前获得封包中的机密信息。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 虚拟路由器中运行的 RIP 路由实例，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使用 RIP 路由更新封包欺骗其邻接方。在 NetScreen 虚拟路由器上，可以配置某时间间隔内接收的最大更新封包数，以免受更新封包的泛滥。所有超过配置的更新临界值的封包都将被丢弃。如果不设置更新临界值，将接收所有封包。

如果邻接方的路由表较大，进行快闪更新时给定期间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。超过临界值的更新封包将被丢弃，无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更新封包数设置为 4。

WebUI

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

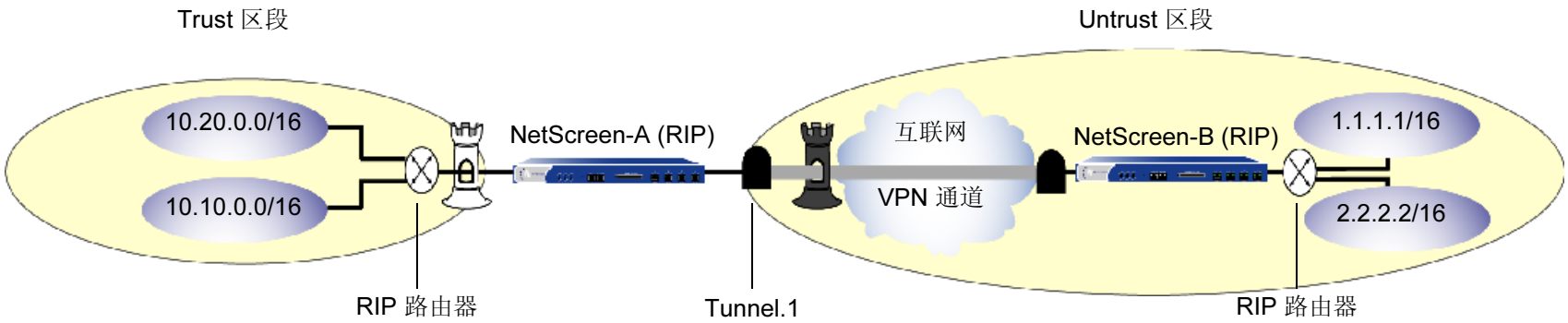
Maximum Number Packets per Update Time: (选择), 4

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 虚拟路由器中创建并启用 RIP 路由实例。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 邻接方。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，接着配置 Route Map *abcd*，以允许与访问列表匹配的路由。随后将调用该 Route Map，过滤通告给 RIP 邻接方的路由。



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
```

4

边界网关协议 (BGP)

本章介绍 NetScreen 设备上的 “边界网关协议” (BGP)。其中覆盖以下主题：

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。ScreenOS 支持 BGP 版本 4 (BGP-4)，如 RFC 1771 中定义。

两个 *BGP 对等方*可以建立一个 *BGP 会话*，以交换路由信息。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。路由表发生变化时， BGP 路由器还会与对等方交换更新消息。BGP 路由器负责维护与其构成会话的所有对等方当前的路由表版本，并定期向对等方发送激活消息，以验证连接是否存在。

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接方时，还会加入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** 消息用于互相标识要启动 BGP 会话的 BGP 对等方。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 : *如果交换公开消息时，对等方指出其支持的协议功能不被 NetScreen 设备支持，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 秒向对等方发送一次激活消息。可以配置该时间间隔。

路径属性

BGP 路径属性是描述路由特征的一组参数。 BGP 先结合各对等方描述的路由属性，然后比较指向同一目的地址的所有路径，选择到达该目的地址使用的最佳路由。路径属性包括 :

- **Origin** 描述获知路由的来源，可以是 IGP、 EGP 或不完整。这是一个众所周知的必需 BGP 路径属性[2]。
- **AS-Path** 包含传送路由通告时经过的自治系统的列表。这是一个众所周知的必需 BGP 路径属性。
- **Next-Hop** 是路由器的 IP 地址，用于发送该路由上的信息流。这是一个众所周知的必需 BGP 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)。

2. 所有 BGP 实现方案都必须能识别众所周知的必需 BGP 路径属性，这些属性必须出现在路由描述中。

- **Local-Pref** 是一个度量，用于通知 BGP 对等方该路由本地路由器的优先级。
- **Atomic-Aggregate** 通知 BGP 对等方，本地路由器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

为 BGP 路由实例配置的大多数路径属性值中，不是必需就是可选设置。例如，对于由 NetScreen 设备上的 BGP 通告的路由，创建 BGP 路由实例时，会将指定的 AS 号附加到 AS 路径属性中。BGP 路由器将路由通告给对等方之前，可以选择添加或修改路径属性。

外部和内部 BGP

将不同 ISP 网相互连接或将企业网连接到 ISP 网后，可以在自治系统之间使用外部 BGP (EBGP)。内部 BGP (IBGP) 在 AS (例如企业网) 内使用。IBGP 的主要用途是将 EBGP 获知的路由分配给 AS 中的路由器。因此，IBGP 路由器可将其 EBGP 对等方获知的路由重新通告给 IBGP 对等方，但不能将 IBGP 对等方获知的路由通告给其它 IBGP 对等方。上述限制使网络中不存在路由通告回路，但也说明 IBGP 网必须是全网状结构 (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建立会话)。

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

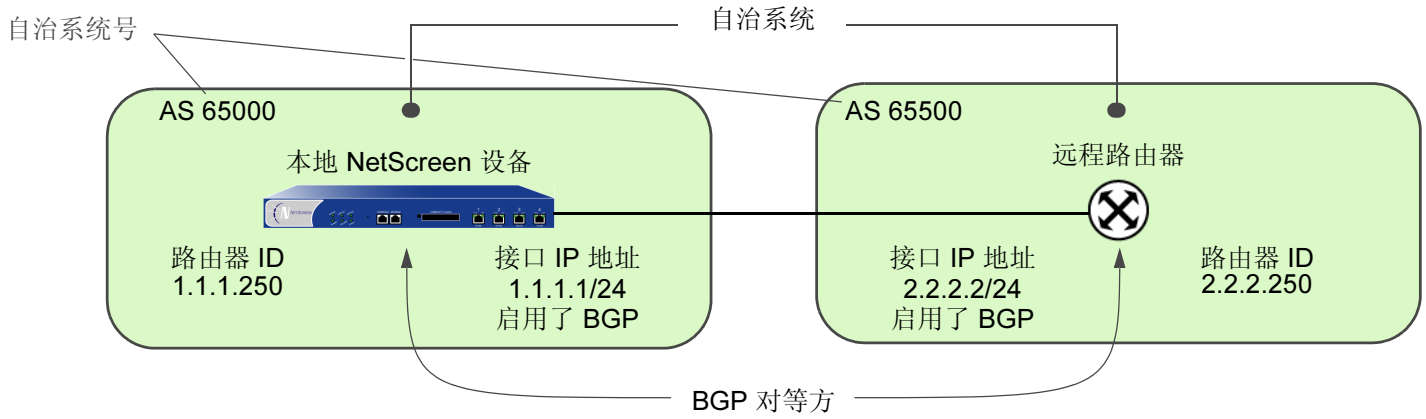
类似 RIP 和 OSPF，可以为 NetScreen 设备上的每个虚拟路由器创建 BGP 实例。如果设备上存在多个虚拟路由器，则可启用多个 BGP 实例，每个 VR 实施一个实例。

> ***注意：***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，如第 1 章 “虚拟路由器”中所述。

本节介绍在 NetScreen 设备的虚拟路由器中配置 BGP 的基本步骤：

1. 要在虚拟路由器中创建并启用 BGP 路由实例，首先要为 BGP 实例分配一个自治系统号，然后才能启用该实例。
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. 验证 BGP 配置正确且运行正常。

本节介绍如何使用 CLI 或 WebUI，执行下例所示的每一项任务。在本例中，将 NetScreen 设备配置成 AS 65000 中的 BGP 对等方。 NetScreen 设备将与 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上创建并启用 BGP 路由实例。要创建 BGP 路由实例，需要先指定虚拟路由器所在自治系统的 AS 号[3]。如果虚拟路由器是 IBGP 路由器，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 路由实例后，即可联系该 BGP 路由实例并在该实例与配置的 BGP 对等方之间建立会话。

范例 : 创建 BGP 路由实例

在下例中，首先将为 trust-vr 虚拟路由器分配路由器 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 1 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)

3. 自治系统号是全球唯一的编号，用于交换 EBGP 路由信息及标识 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 属于私用范畴，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**，然后在确认提示时单击 **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 设备上的接口不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 : 禁用接口上的 BGP

在本例中，将禁用接口 ethernet4 上的 BGP。注意，启用 BGP 的其它任何接口仍然可以传输及处理 BGP 封包。

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，这样才能启动 BGP 会话。需要指定 BGP 对等方的 IP 地址，还可以配置一些可选参数来建立并维护会话。对等方既可以是内部 (IBGP) 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，则会将该消息记入日志。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*，从而将对等方组作为一个整体来配置参数。注意，不能将 IBGP 和 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，“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 与邻接方之间的节点数。	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。*	无
Hold time	X	X	自收不到对等方消息起，经过多长时间后认为与该对等方之间的连接中断。	180 秒
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 属性的值。	0
Next-hop self	X	X	对于发送到对等方的路由，下一跳跃路径属性被设置成本地 VR 接口的 IP 地址。	不更改下一跳跃属性

BGP 参数	对等方	对等方组	说明	缺省值
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，经过多长时间后再次尝试建立 BGP 会话。	120 秒
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 Route Map 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 106 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，即可配置对所有对等方组成员应用的参数 (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

通过执行以下 CLI 命令，可以查看通过 WebUI 或 CLI 输入的配置 :

```
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
```

通过执行以下 CLI 命令，可以验证 VR 上运行的 BGP:

验证 BGP 正在运行。

```
ns-> get vr 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
```

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 1 章“虚拟路由器”。

通过执行以下 CLI 命令，可以验证是否启用 BGP 对等方或对等方组并查看 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
```

表明对等方已启用，会话处于活动状态。

会话状态可能是以下某种情况：

- **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[4]
- **OpenSent** - BGP 正在等待对等方的 “OPEN” 消息
- **OpenConfirm** - BGP 正在等待对等方的 “KEEPALIVE” 或 “NOTIFICATION” 消息
- **Established** - BGP 正在与对等方交换 “UPDATE” 封包

4. 如果会话状态在 “活动” 和 “连接” 之间不停变化，则表明对等方之间的连接出现问题。

安全配置

本节介绍 BGP 路由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，应在同一安全级别上配置 BGP 域中的所有路由器。否则，只要一个 BGP 路由器遭受破坏，整个 BGP 路由域都有可能瘫痪。*

认证邻接方

由于 BGP 封包没有加密且多数协议分析器都提供 BGP 封包的解封机制，因此 BGP 路由器很容易被欺骗。认证 BGP 对等方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 封包。对于发送方和接收方 BGP 路由器， MD5 认证使用同一个密钥。从指定对等方接收的所有未经验证的 BGP 封包都会被丢弃。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。接着将使用密钥 1234567890123456 根据 MD5 认证配置对等方。

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) 加入路由域中，以便将封包返回给自己。随后，该路由器既可以丢弃封包，引发服务中断，也可以在转发封包之前获得封包中的机密信息。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 虚拟路由器中运行的 BGP 路由实例，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。本节还将说明某些比较复杂的参数配置。

下表介绍 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	创建聚合的地址。	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 116 页上的 “BGP 公共组”。	
AS confederation	创建联合。请参阅第 113 页上的 “联合”。	
Flap damping	阻止路由的通告，直到它变稳定。	禁用
Hold time	自收不到对等方消息起，经过多长时间后认为与该对等方之间的连接中断。	180 秒
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 属性的值。	0
Network	添加虚拟路由器可到达的网络或子网条目。添加到 BGP 中的条目将被通告给所有 BGP 对等方。请参阅第 109 页上的 “带条件的路由通告”。	
Route redistribution	将其它路由协议的路由导入 BGP。请参阅第 107 页上的 “重新分配路由”。	
Reflector	将本地 BGP 实例配置成客户端的路由反射器。请参阅第 109 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，经过多少时间后重新尝试建立会话。	120 秒
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选择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 VR 中的 BGP 路由实例 :

- 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 Route Map，以过滤重新分配的路由。有关为重新分配路由创建 Route Map 的详细信息，请参阅第 1 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 路由域的路由重新分配到当前的 BGP 路由域中。 CLI 和 WebUI 范例都假设先前已创建名为 add-ospf 的 Route Map。

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。使用 *AS 路径访问列表*，可根据 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 虚拟路由器的 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
```

带条件的路由通告

可以指定虚拟路由器能到达的网络和子网。随后，这些网络将被通告给所有 BGP 对等方。如果指定的网络不可达，则不会将其添加到 BGP 中，因此也不会通告给 BGP 对等方。根据需要，可以指定只通告一个网络，前提是另一个指定的网络地址可以到达。例如， CLI 命令 **set network 4.4.4.0/24 check 5.5.5.0/24** 指示 BGP 只通告 4.4.4.0/24 网络，前提是虚拟路由器可以到达 5.5.5.0/24 网络。如果 5.5.5.0/24 网络不可达，BGP 不会通告 4.4.4.0/24 网络。根据需要，还可以指定在不考虑可达性的情况下通告某网络。例如，CLI 命令 **set network 4.4.4.0/24 no-check** 指示 BGP 始终通告 4.4.4.0/24 网络。

路由反射

由于 IBGP 路由器不能将一个 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 92 页上的 “外部和内部 BGP”)，因此需要配置*全网状*的 IBGP 会话，此时 BGP AS 中的每个路由器是都该 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两两之间直接相连，而是要求每个路由器与其它所有路由器之间建立并维护 IBGP 会话。例如，在拥有 8 个路由器的 AS 中， 8 个路由器中的每一个都需要与其它 7 个路由器构成对等关系。

全网状配置的 IBGP 会话不适于扩展。通过以下公式，可计算出一个 AS 需要的全网状 IBGP 会话数 :

(x * (x-1))/2

对于包含 8 个路由器的 AS，全网状 IBGP 会话数应为 28。如果 AS 中有 20 个路由器，该网络中需要的全网状 IBGP 会话数应为 190。

路由反射是解决 IBGP 扩展问题的一种方法，在 RFC 1966 中介绍。*路由反射*是一个路由器，它将 IBGP 获知的路由传送给指定的 IBGP 邻接方 (*客户端*)，因此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。客户端使用路由反射器交换路由，路由反射器则在客户端之间反射路由。

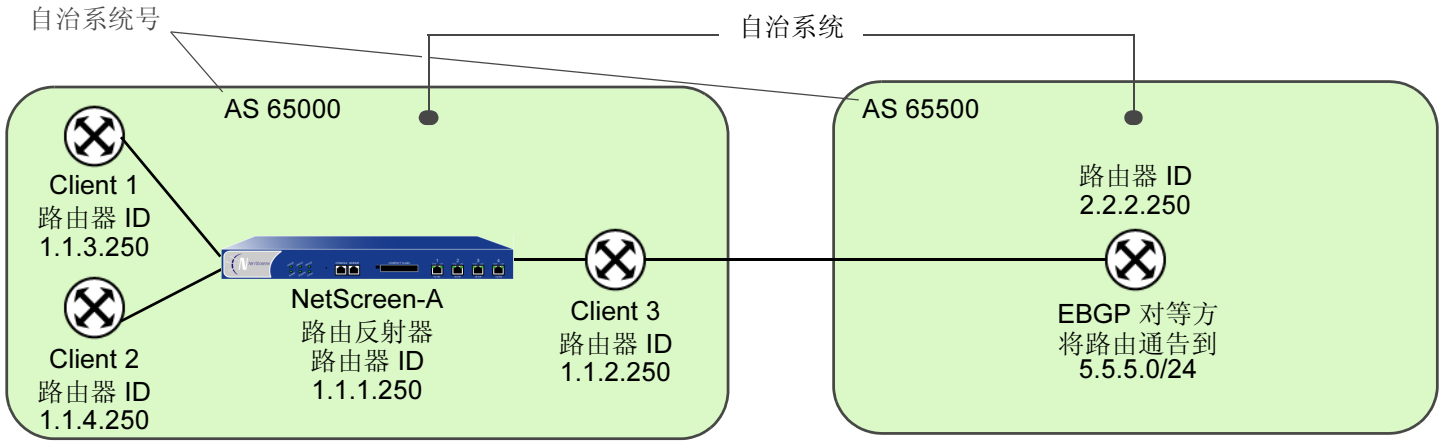
在 NetScreen 设备上，可以指定本地虚拟路由器充当路由反射器。根据需要，可以指定路由反射器的群集 ID。一旦指定了群集 ID， BGP 路由实例会将群集 ID 附加到路由的群集列表属性中。群集 ID 有利于防止路由回路的产生，因为本地 BGP 路由实例的群集 ID 出现在路由的群集列表中时，它会放弃该路由。

注意：*配置群集 ID 之前，必须先禁用 BGP 路由实例。*

在本地虚拟路由器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，随后 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**。

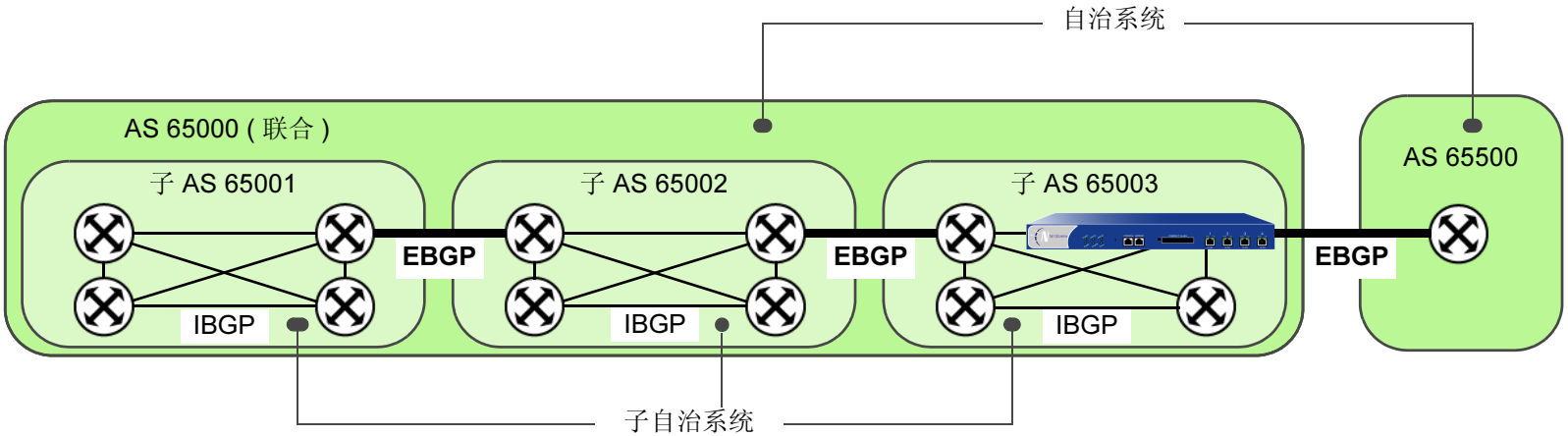
> Configure (对于 Remote IP 1.1.4.250): 选择 **Reflector Client**，然后单击 **OK**。

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 109 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，在 RFC 1965 中介绍。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自治系统 (只有一个标识符)，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。



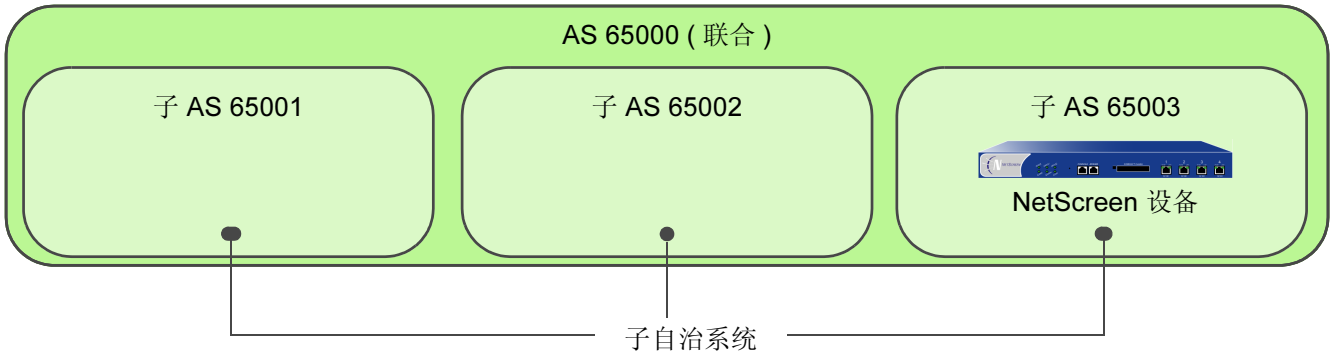
对于联合中的每一个路由器，需要指定以下信息：

- 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
- 联合支持 RFC 1965 (缺省值) 还是 RFC 3065[5]

5. AS 路径属性 (请参阅第 91 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将目的地址分组 (称作公共组) 的方法，分组后，BGP 路由器即可使用公共组控制接受、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 (假设该路由没有公共组路径属性)，也可以修改路由中的公共组 (假设路由包含公共组路径属性)。公共组路径属性提供了分配路由信息的另一种方法，无论基于 IP 地址前缀还是 AS 路径属性。公共组路径属性有多种用途，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*，包含 AS 标识符和公共组标识符。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 Route Map，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，还可以添加或删除路由的公共组。

例如，如果 ISP 向客户提供互联网连接功能，则可以为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。来自其它 ISP 的路由被分配了不同的公共组号，因此不会通告给对等 ISP。

索引

W

Y

Z