NetScreen 概念与范例

ScreenOS 参考指南

第 5 卷：动态路由

ScreenOS 4.0.0

编号 093-0523-000-SC

版本 F

Copyright Notice

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

路由是安全设备的基本部分。如果缺少路由，安全设备无法有效地将安全信息流发送到期望的目标位置。动态路由可缩短网络拓扑的更改与网络上信息流传送之间的时间间隔。

第 5 卷，“动态路由”介绍了配置“开放式最短路径优先”(OSPF) 和“边界网关协议”(BGP) 的方法。本卷介绍以下内容：

- OSPF 概述、 OSPF 命令、基本配置以及高级配置
- BGP 概述、 BGP 命令、基本配置以及高级配置

约定

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

WebUI 导航约定

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

范例：Objects > Addresses > List > New

要访问新地址配置对话框，请执行以下操作：

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

CLI 约定

本手册中的每一条 CLI 命令说明都展现了命令语法的某些方面。此语法可包括选项、开关、参数及其它功能。为阐明语法规则，一些命令说明使用了*相关性定义符*。这种定义符指示哪些命令功能是强制性的，以及适用于哪些环境中。

相关性定义符

每一语法说明都使用特殊字符来展示命令功能之间的相关性。

- { 和 } 符号表示强制功能。由这些符号括起来的功能对于命令的执行是必需的。
- [和] 符号表示可选功能。包含在这些符号中的功能，尽管省略它们可能使命令执行后得到相反的结果，但它们对命令的执行并非是必需的。
- | 符号表示两个功能之间的一个“或”关系。当这个符号出现在同一行上的两个功能之间时，可使用两个功能中的任一个（但不能两个都使用）。当这个符号出现在行尾时，可使用该行上的功能，或下一行上的功能。

嵌套的相关性

多数 CLI 命令有*嵌套的*相关性，这使得功能在某些环境中是可选的，而在另一些环境中，则是强制性的。下面给出了三种假设功能，用以对这种原则进行示范。

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

定义符 [和] 包围了整个子句。因此，可省略 **feature_1**、**feature_2** 和 **feature_3**，并且仍能成功执行该命令。可是，由于 { 和 } 定义符包围着 **feature_2** 和 **feature_3**，所以如果包括 **feature_1**，则必须包括 **feature_2** 或 **feature_3** 中的任一个。否则，将不能成功执行该命令。

以下例子说明了 **set interface** 命令的某些功能相关性。

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

括号 { 和 } 表示必须指定 **flood** 或 **arp** 中的任一个。但是，括号 [和] 表示对于 **arp** 而言， **trace-route** 选项并非必需。因而，这条命令可以采取以下任一种形式：

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

CLI 命令及功能的可用性

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

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

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

NETSCREEN 文档

要获得任何 NetScreen 产品的技术文档，请访问 www.netscreen.com/support/manuals.html。欲访问最新的 NetScreen 文档，请参阅 **Current Manuals** 部分。欲访问以前版本中的已存档文档，请参阅 **Archived Manuals** 部分。

欲获得有关某一 NetScreen 产品版本的最新技术信息，请参阅该版本的发行说明文档。欲获得发行说明，请访问 www.netscreen.com/support 并选择 **Software Download**。选择产品及其版本，然后单击 **Go**。（欲完成此下载任务，您必须是注册用户。）

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

1

OSPF 任务参考

本章介绍 “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) 是在单个“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 内部定期发布*链接状态通告* (LSA)，来发布其状态信息 （即，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 在遍及 AS 内部的持续发布将使 AS 内的所有路由器都创建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 （根部）。

有关 LSA、链接状态数据库以及区域的详细信息，将在本章的后续部分阐述。

区域

通过使用*区域*，OSPF 允许对网络按逻辑进行分组或按地理位置分组。区域还可减少网络内流通的路由信息量，因为路由器只维护其驻留区域的链接状态数据库。不维护本地区域以外的网络 / 路由器的链接状态信息。

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“中枢”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。切记，所有区域都必须与 area 0 直接相连，只有一个区域例外，这将在以后部分介绍。

位于两个区域之间的路由器被称为*区域边界路由器*，因为所有区域都必须与 area 0 直接相连，故中枢区域以外的所有区域都被称为*剩余区域*。 OSPF 中使用两种通用类型的剩余区域，每种都具有其自身的特点：

- **剩余区域：**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。如果剩余区域中不允许汇总路由，则它可被认为是一个*完全剩余区域*。
- **不完全剩余区域 (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，仍可获取区域内被检测到的外部路由，并将其传递到其它区域。

首先在虚拟路由器级对区域进行配置，然后可配置接口，使其驻留于在虚拟路由器级定义的区域中。

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。
- **中枢路由器：**有一个接口在中枢区域的路由器。
- **区域边界路由器：**OSPF 区域与另一区域相接时，两个区域间的路由器被称为区域边界路由器。区域边界路由器 (ABR) 是在多个区域中（其中一个为中枢区域）都具有接口的路由器。ABR 将来自非中枢区域的路由进行汇总，以发送回 area 0。如果第二个区域在 ScreenOS 内创建，则设备与 ABR 功能相同。
- **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 内发布外部 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。

网络上有多个路由器时，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)。指定路由器单独负责将 LSA 大量发向网络，这些 LSA 中包含所有连接到网络的、已启用 OSPF 的路由器的列表。DR 被认为是 OSPF 网络内最重要的路由器，因为它是唯一能与网络上其它路由器建立邻接关系的路由器。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。正是这种类型的层级结构使得 OSPF 可进行扩展，同时最小化无效的网络通信量。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
- 非广播网络
- 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 封包发送到多点传送地址 224.0.0.5，动态检测其邻接路由器。对于广播网络，Hello 协议将为网络选定 “指定路由器” 和 “备份指定路由器”。

非广播网络

*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，必须将通常为多点传送的 OSPF 协议封包发送到每一邻接路由器。

在非广播网络上， OSPF 以以下两种模式之一运行：

- 非广播多路访问 (NBMA) 模拟广播网络上的 OSPF 操作。
- 点对多点将网络视为多个点对点网络的集合。

在非广播网络上，需为 OSPF 路由器输入配置信息，以确定其邻接方。对于 NBMA 网络， Hello 协议将为网络选定“指定路由器”和 “备份指定路由器”。

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。通过 56KB 串行线相连的两个路由器即为点对点网络的一个范例。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 发送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	到另一 AS 中某个网络的路由。通常为缺省路由 (0.0.0.0/0)。

NetScreen 设备上的 OSPF

在 NetScreen 设备上，OSPF 基于虚拟路由器而启用，并在虚拟路由器级和接口级具有配置参数。因为系统中可存在多个虚拟路由器，故也可在单个设备上运行多个 OSPF 实例。

根据 RFC 2328 的定义，ScreenOS 支持 OSPF 版本 2。也可将 OSPF 配置成与 OSPF 的较早版本 RFC 1538 兼容。

VPN 通道上的 OSPF 支持

IPsec VPN 通道支持 OSPF，并需使用基于路由的 VPN。在绑定到单个通道接口（已编号或未编号）的 VPN 上，可启用 OSPF。将 VPN 绑定到通道接口后，可使用与物理接口相同的方式启用并配置 OSPF。为通道接口启用 OSPF 后，网络类型即成为点对点型。

OSPF 认证

ScreenOS 提供了简单的密码和 MD5 认证，以验证从邻接方接收到的 OSPF 封包。可在虚拟路由器级配置认证；此时，所有与该虚拟路由器相关的 OSPF 接口都使用同一认证方法。也可在接口级配置认证。

OSPF 接口特征

在接口级可配置多个 OSPF 参数。以下为 OSPF 接口特征：

- **Authentication type（认证类型）**：认证启用接口以验证接口上的 OSPF 通信。NetScreen 支持两种类型的 OSPF 认证方案：Message Digest 版本 5 (MD-5) 和明文密码。这两种方法都允许一个 OSPF 对等方认证其收到的来自另一合法 OSPF 对等方的封包。
- **Cost（开销）**：在 OSPF 中，路由的开销决定了它的适用性。与网络接口相关的开销取决于与该接口连接到的链接的带宽。带宽越高，开销值就越低或越适合需求。缺省开销为 10。
- **Dead interval（不工作间隔）**：不工作间隔是 OSPF 确定其某个邻接方未运行之前，所间隔的最长时间。缺省值为 40 秒。
- **Hello interval（Hello 间隔）**：OSPF 路由实例定期发出 Hello 封包。缺省值为 10 秒。
- **Retransmit interval（重新传输间隔）**：重新传输间隔是指为属于指定接口的邻接方重新传输 LSA 的间隔时间。缺省值为 5 秒。
- **Transit Delay（传输延迟）**：传输延迟是指当前接口发送的链接状态更新封包传输之间的时间。缺省值为 1 秒。
- **Priority（优先级）**：优先级用于选定“指定路由器”和“备份指定路由器”。数字越大，OSPF 路由实例就越有可能被选定为 DR 或 BDR。缺省值为 10。

OSPF 命令

可使用 **ospf** 上下文相关命令和 **interface** 命令，在 NetScreen 设备中配置 OSPF。

OSPF 环境启动

要发出 **ospf** 上下文相关命令，请执行以下操作：

1. 执行 **set vrouter** 命令，进入 **vrouter** 环境。

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

   其中 *vrouter* 为虚拟路由器名称。

2. 执行 **set protocol ospf** 命令，进入 ospf 环境。

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

有关 **ospf** 上下文相关命令的详细信息，请参阅第 **2**-58 页上的褒 LI 中的环境相关命令 ”。

基本 OSPF 配置任务

以下配置任务是大多数 OSPF 实施必须执行的。

在虚拟路由器级启用 OSPF 实例

可在虚拟路由器级或接口级启用或禁用 OSPF 实例。在虚拟路由器级启用或禁用 OSPF 实例时，虚拟路由器内的所有 OSPF 接口都将被影响。在接口级启用或禁用 OSPF 时，只影响特定的 OSPF 接口。

可使用 WebUI 或 CLI **set protocol ospf** 命令在虚拟路由器内创建 OSPF 实例。

范例：启动 OSPF 实例

在下例中，将以缺省选项启用 trust-vr 中的 OSPF。

WebUI

Network > Routing > Virtual Routers > trust-vr：选择 **Create OSPF Instance**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr)-> save

> ***注意：****使用* ***unset protocol ospf*** *命令禁用 OSPF 实例。*

移除 OSPF 虚拟路由实例

可使用 WebUI 或 CLI **unset enable** 命令，将 OSPF 路由实例从创建它的虚拟路由器移除。

范例：禁用 OSPF

在下例中，将禁用当前 OSPF 路由实例。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Delete OSPF Instance。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> unset enable
4. ns(trust-vr/ospf)-> save

创建 OSPF 区域

要在 NetScreen 设备上配置或显示 OSPF 区域的详细信息，请使用 WebUI 或 CLI **set area** 命令。

范例：创建 OSPF 区域

在下例中，将创建区域 ID 为 10 的 OSPF 剩余区域。

WebUI

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

Area ID: 10

Type: stub

Action: Add

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set area 10 stub
4. ns(trust-vr/ospf)-> save

指定到区域的接口

在虚拟路由器级创建区域后，即可使用 WebUI 或 CLI **set interface** 命令为该区域指定接口。

范例：为 OSPF 区域指定接口

在下例中，将接口 ethernet1 指定到 OSPF 区域 10。

WebUI

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

CLI

1. ns-> set interface ethernet1 protocol ospf area 10
2. ns-> save

重新分配路由

路由重新分配是将路由从网络的使用另一路由选择协议的其它部分，导入当前路由选择域的过程。此过程允许传递其它路由选择协议的路由信息，特别是已知路由。

重新分配路由时，将影响给定域中生成的外部 LSA 数。对于要通告的外部 LSA，路由器将执行重新分配。要配置路由重新分配，请确定源路由选择协议，以及将通告这些新获得的外部路由的目的地（或目标）路由选择协议。因为不同协议使用不同参数引入，故重新分配提供了一个本地参考值，作为比较协议间路径适用性的一种途径。

配置路由重新分配时，必须首先指定一个路由图，以定义分配路由。有关配置路由图的详细信息，请参阅第 2 卷，“基本原理”中第 3 章的路由重新分配。

可使用 WebUI 或 CLI **set redistribute route-map** 命令，来重新分配路由。

范例：将 BGP 路由重新分配到 OSPF 中

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 map1 的路由图。

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: map1

Protocol: BGP

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set redistribute route-map map1 protocol bgp
4. ns(trust-vr/ospf)-> save

OSPF 接口配置

本节介绍 OSPF 接口配置任务。

显示 OSPF 接口详细信息

使用 CLI **get interface** 命令，可显示已配置 OSPF 路由选择实例的接口的详细信息。

范例：显示 OSPF 接口信息

在下例中，将显示已配置 OSPF 路由选择实例的接口的详细信息。

WebUI

注意：*只能通过 CLI 查看接口的 OSPF 配置详细信息。*

CLI

ns-> get interface ethernet1 protocol ospf

```
VR: trust-vr RouterId: 212.1.1.1
---------------------------------
Interface: ethernet2/1
IpAddr: 20.20.20.20/16, OSPF: enabled, Router: enabled
Type: Ethernet  Area: 0.0.0.10  Priority: 100  Cost: 1
Transit delay: 60s  Retransmit interval: 5s  Hello interval: 10s
Router Dead interval: 40s  Authentication-Type: MD-5
Authentication-Key: ****************
MD-5 KeyId: 1
State: Designated Router  DR: 20.20.20.20(self)  BDR: 0.0.0.0
Neighbors:
Valid neighbor access list numbers in Vrouter (trust-vr)
-------------------------------------------------------------------------
```

在接口上设置明文密码

要在接口上配置明文密码作为 OSPF 通信的认证方法，请使用 WebUI 或 CLI **set interface** 命令。

范例：配置明文密码认证方法

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

1. ns-> set interface ethernet1 protocol ospf authentication password 12345678
2. ns-> save

在接口上设置 MD5 密码

要配置消息整理 (MD5) 密码作为接口上所有 OSPF 通信的认证方法，请使用 WebUI 或 CLI **set interface** 命令。

范例：配置 MD5 密码认证方法

在下例中，将在接口 ethernet1 上为 OSPF 设置消息整理密码 1234567890123456 和密钥 ID 1。

WebUI

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

MD5 Key: （选择）, 1234567890123456
Key ID: 1

CLI

1. ns-> set interface ethernet1 protocol ospf authentication md5 1234567890123456 key 1
2. ns-> save

为 OSPF 接口设置开销值

可使用 WebUI 或 CLI **set interface** 命令为 OSPF 接口设置开销值。

范例：为 OSPF 接口配置开销

在本例中，将在接口 ethernet1 上为 OSPF 设置开销值。

WebUI

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

Cost: 20

CLI

1. ns-> set interface ethernet1 protocol ospf cost 20
2. ns-> save

为 OSPF 接口设置不工作间隔

不工作间隔是邻接方被确定为未运行前所间隔的最大时间量。要在 NetScreen 设备的物理接口上设置不工作间隔，请使用 WebUI 或 CLI **set interface** 命令。

范例：配置不工作间隔

在本例中，将在接口 ethernet1 上为 OSPF 设置 100 秒的不工作间隔 。

WebUI

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

Neighbor Dead Interval: 100

CLI

1. ns-> set interface ethernet1 protocol ospf dead-interval 100
2. ns-> save

为 OSPF 接口设置 Hello 间隔

Hello 间隔是当前路由选择实例发送到网络的 Hello 封包实例之间的时间间隔量。要设置 hello 间隔，请使用 WebUI 或 CLI **set interface** 命令。

范例：配置 Hello 间隔

在本例中，将在接口 ethernet1 上为 OSPF 设置 100 秒的 hello 间隔。

WebUI

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

Hello Interval: 100

CLI

1. ns-> set interface ethernet1 protocol ospf hello-interval 100
2. ns-> save

为 OSPF 接口设置 Neighbor List （邻接方列表）

可使用 WebUI 或 CLI **set interface** 命令，配置当前 OSPF 虚拟路由选择实例的对等方或 Neighbor List （邻接方列表）。

范例：配置 Neighbor List （邻接方列表）

在本例中，将在接口 ethernet1 上为 OSPF 创建 Neighbor List （邻接方列表）。

WebUI

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

Neighbor List: 4 | 5 | 6

CLI

1. ns-> set interface ethernet1 protocol ospf neighbor-list 4 5 6
2. ns-> save

为 OSPF 接口设置重新传输间隔

重新传输间隔值指定接口向 （未响应原始 LSA 的）邻接方重新发送 LSA 前，间隔的时间量 （秒） 。可使用 WebUI 或 CLI **set interface** 命令为 OSPF 接口指定重新传输间隔。

范例：配置重新传输间隔

在下例中，将在接口 ethernet1 上为 OSPF 设置 100 秒的重新传输间隔。

WebUI

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

Retransmit Interval: 100

CLI

1. ns-> set interface ethernet1 protocol ospf retransmit-interval 100
2. ns-> save

在 OSPF 接口上设置优先级值

网络上的路由器通过选择进程成为指定路由器。这种指定通过比较路由器的优先级值进行。该值越大，路由器就越有可能被选为 DR。可使用 WebUI 或 CLI **set interface** 命令在 OSPF 接口上配置优先级值。

范例：配置优先级值

在本例中，将为 OSPF 接口 ethernet1 设置优先级值 100。

WebUI

Network > Interfaces > Edit（对于 ethernet1）> OSPF：在 Priority 字段中键入 **100**，然后单击 **Apply**。

CLI

1. ns-> set interface ethernet1 protocol ospf priority 100
2. ns-> save

在 OSPF 接口上设置传输延迟值

要在接口上设置链接状态更新封包传输间的时间间隔量，需要设置传输延迟值。要在 OSPF 接口上配置传输延迟值，请使用 WebUI 或 CLI **set interface** 命令。

范例：配置传输延迟

在下例中，将在 OSPF 接口 ethernet1 上设置 10 秒的传输延迟。

WebUI

Network > Interfaces > Edit（对于 ethernet1）> OSPF：在 Transit Delay 字段中键入 **10**，然后单击 **Apply**。

CLI

1. ns-> set interface ethernet1/1 protocol ospf transit_delay 10
2. ns-> save

OSPF 虚拟链接配置

本节介绍 OSPF 虚拟链接配置任务。

创建虚拟链接

OSPF 网络中的所有区域都必须直接连接到中枢区域。有时，需要创建一个实际上并不连接到中枢区域的新区域。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中枢区域相连。

要创建或显示当前路由实例的虚拟链接的详细信息，请使用 WebUI 或 CLI **set vlink** 命令。

范例：创建到中枢区域的虚拟链接

在下例中，将使用路由 ID 为 10.10.10.20 的 0.0.0.10 区域创建一个虚拟链接。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

CLI

1. ns(trust-vr/ospf)-> set vlink area 0.0.0.10 router-id 10.10.10.20
2. ns(trust-vr/ospf)-> save

自动创建虚拟链接

当虚拟路由器无法到达网络中枢时，可引导它自动为实例创建虚拟链接。让虚拟路由器自动创建虚拟链接，可替代手动创建每个虚拟链接，后者所需时间更多。可使用 WebUI 或 CLI **set autovlink** 命令，配置虚拟路由器自动创建虚拟链接。

范例：创建自动虚拟链接

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

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set auto-vlink
4. ns(trust-vr/ospf)-> save

为虚拟链接创建消息整理

要为 OSPF 虚拟路由实例上的虚拟链接启用 MD5 认证，请使用 WebUI 或 CLI **set vlink authentication md5** 命令。

范例：创建使用 MD5 认证的虚拟链接

在下例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20， MD5 密码为 1234567890123456。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：输入以下内容，然后单击 **OK**：

Authentication

MD5:（选择）

MD5 Key (16 characters): 1234567890123456

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area-id 0.0.0.10 router-id 10.10.10.20 authentication-type md5 1234567890123456
4. ns(trust-vr/ospf)-> save

为虚拟链接创建明文密码

要配置明文密码作为 OSPF 虚拟路由实例上虚拟链接的认证方法，请使用 WebUI 或 CLI **set vlink authentication** 命令。

范例：创建具有明文密码的虚拟链接

在下例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20，明文密码为 12345678。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：输入以下内容，然后单击 **OK**：

Authentication

Password: （选择）

Password (8 characters): 12345678

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area-id 0.0.0.10 router-id 10.10.10.20 authentication-type password 12345678
4. ns(trust-vr/ospf)-> save

为虚拟链接邻接方创建不工作间隔

要为通过虚拟链接可到达的邻接方创建不工作间隔，请使用 WebUI 或 CLI **set vrouter protocol ospf vlink dead-interval** 命令。

范例：配置虚拟链接邻接方不工作间隔

在下例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20，不工作间隔为 50 秒。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：在 Router 不工作间隔字段中键入 **50**，然后单击 **OK**：

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area 0.0.0.10 router 10.10.10.20 dead-interval 50
4. ns(trust-vr/ospf)-> save

为虚拟链接创建 Hello 间隔

要为 OSPF 虚拟路由实例上的虚拟链接创建 hello 间隔，请使用 WebUI 或 CLI **set vrouter protocol ospf hello-interval** 命令。

范例：配置虚拟链接 Hello 间隔

在下例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20， hello 间隔为 30 秒。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：在 Hello Interval 字段中，键入 **30**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area 0.0.0.10 router 10.10.10.20 hello-interval 30
4. ns(trust-vr/ospf)-> save

为虚拟链接创建重新传输间隔

要为跨越虚拟链接接口的各邻接方指定链接状态通告 (LSA) 重新传输的时间间隔，请使用 WebUI 或 CLI **set vlink area router retransmit-interval** 命令。

范例：配置虚拟链接重新传输间隔

在本例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20，重新传输间隔为 20 秒。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：在 Retransmit Interval 字段中，键入 **20**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area 0.0.0.10 router 10.10.10.20 retransmit-interval 20
4. ns(trust-vr/ospf)-> save

为虚拟链接配置传输延迟值

要配置当前虚拟链接发送的链接状态更新封包的各次传输间隔的时间，请使用 WebUI 或 CLI **set vlink transit-delay** 命令。

范例：配置虚拟链接传输延迟

在本例中，将创建一个虚拟链接，其区域 ID 为 10，路由 ID 为 10.10.10.20，传输延迟为 100 秒。

WebUI

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: 0.0.0.10

Router ID: 10.10.10.20

> Configure：在 Transit Delay 字段中，键入 **100**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set vlink area 0.0.0.10 router-id 10.10.10.20 transit-delay 100
4. ns(trust-vr/ospf)-> save

OSPF 信息

本节介绍显示 OSPF 信息的任务

显示 OSPF 路由实例的统计信息

使用 CLI **get statistics** 命令，显示以下与 OSPF 路由实例相关对象的信息：

- Hello Packets （Hello 封包）
- Link State Requests （链接状态请求）
- Link State Acknowledgments （链接状态应答）
- Link State Updates （链接状态更新）
- Database Descriptions （数据库说明）
- Areas Created （创建的区域）
- Shorted Path First Runs （缩短路径优先运行）
- Packets Dropped （丢弃的封包）
- Errors Received （收到的错误）
- Bad Link State Requests （错误的链接状态请求）

范例：显示 OSPF 统计信息

在下例中，将显示为 trust-vr 虚拟路由器中 OSPF 记录的各种统计信息。

WebUI

> ***注意：****只能通过 CLI 显示上述统计信息。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get statistics

```
VR: untrust-vr RouterId: 0.0.0.0
---------------------------------
Packet Type     Transmit Receive
-------------------------------------------------------------------------
Hello                   0        0
LS Request              0        0
LS Acknowledge          0        0
LS Update               0        0
Database Desc           0        0

AreaId          SPF Runs
-----------------------------------------
0.0.0.0         1
0.0.0.10                 0

Packets Dropped:
None

Receive Errors:
None

Bad LS Requests: 0
```

注意：*使用* ***clear*** *命令将所有封包类型重新设置为 0。*

显示重新分配条件的详细信息

使用 WebUI 或 CLI **get rules-redistribute** 命令，显示为路由（从另一路由域中非 OSPF 路由器导入）设置的条件的详细信息。

范例：显示重新分配条件

在下例中，将显示当前已配置的重新分配规则。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit OSPF Instance > Redistributable Rules

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get rules-redistribute

```
VR: trust-vr RouterId: 1.1.1.2
---------------------------------
trust-vr
==========
 Redistribution Rules
-------------------------------------------------
IP-Prefix           Source-Protocol Cost ASE-Type Tag
-------------------------------------------------------------------------------
100.123.1.4/16      any               10        1 0.0.0.10
```

显示已重新分配路由的详细信息

使用 **routes-redistribute** 命令，显示已被当前 OSPF 虚拟路由实例从另一路由域中的非 OSPF 路由器导入的路由的详细信息。

范例：显示已重新分配路由的详细信息

在下例中，将显示已被当前 OSPF 虚拟路由实例从另一路由域中的非 OSPF 路由器导入的路由的有关信息。

WebUI

> ***注意：****只能通过 CLI 显示上述信息。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get routes-redistribute

```
VR: trust-vr RouterId: 1.1.1.2
---------------------------------
IP-Prefix          Cost ASE-Type Forwarding-IP   Tag
-----------------------------------------------------------------
1.1.1.0            20  1       0.0.0.0         0.0.0.0
```

显示 OSPF 数据库中的对象

使用 CLI **get database** 命令，显示当前 OSPF 路由器的数据库中的对象。

范例：显示 OSPF 数据库对象

在下例中，将显示当前 OSPF 路由实例 OSPF 数据库中 area 0 的路由 LSA 详细信息。

WebUI

> ***注意：****只能使用 CLI 显示这些统计信息。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get database area 0 router

```
Link-State-Id   Adv-Router-IDAge    Sequence    Checksum
-------------------------------------------------------
20              1.1.1.0     20      2           1
```

显示剩余区域详细信息

使用 WebUI 或 CLI **get stub** 命令，显示已在当前 OSPF 虚拟路由实例上创建的剩余区域的详细信息。

范例：显示剩余区域详细信息

在下例中，将显示在当前 OSPF 路由实例上创建的剩余区域的类型。

WebUI

Network > Routing > Virtual Routers > Edit （对于 trust-vr） > Edit OSPF Instance > Area > Configure

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get stub

```
VR: untrust-vr RouterId: 0.0.0.0
---------------------------------
Area-ID: 0.0.0.10 (Stub)
        Total number of interfaces is 0, Active number of interfaces is 0
        Route Imports: None, SPF Runs: 0
        Number of ABR(s): 0, Number of ASBR(s): 0
        Number of LSA(s): 0, Checksum: 0x0
        Default route metric type is ext-type-1, metric is 1
        Type-3 LSA Filter: disabled
```

显示 OSPF 配置

使用 CLI **get config** 命令显示 OSPF 配置。

范例：列出 OSPF 配置命令

在下例中，将显示所有 OSPF 配置命令的列表。

WebUI

> ***注意：****要查看 OSPF 命令，必须使用 CLI。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> get config

```
VR: untrust-vr RouterId: 0.0.0.0
----------------------------------
set protocol ospf
set disable
set auto-vlink
set advertise-def-route always metric 10 metric-type 1
set area 0.0.0.10 nssa
exit
```

其它 OSPF 配置

本节介绍显示 OSPF 信息的任务

将 OSPF 绑定到通道接口

要将通道接口绑定到 NetScreen 设备上的 OSPF 路由实例，请使用 WebUI 或 CLI **set interface tunnel** 命令。

范例：将通道绑定到 OSPF 路由实例

在下例中，将 OSPF 绑定到通道接口 tunnel.1。

WebUI

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

Available Interfaces: tunnel.1

使用 **Add** 按钮，将 tunnel.1 接口从 Available Interfaces 栏移动到 Selected Interfaces 栏中。

CLI

1. ns-> set interface tunnel.1 protocol ospf
2. ns-> save

通告所有区域中的缺省路由

每个路由器在其路由表中都有一个缺省路由。缺省路由与路由表中每个目的地网络匹配，虽然有更特定的前缀覆盖缺省路由。通常，缺省路由为 0.0.0.0/0。

使用 WebUI 或 CLI **set advertise-default-route** 命令，可通告或显示整个 AS 内的当前缺省路由。

范例：通告缺省路由

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：*缺省度量为 1，缺省度量类型为 ASE 类型 1。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set advertise-default-route always metric 1 metric-type 1
4. ns(trust-vr/ospf)-> save

配置汇总路由

在大型网络中，可能存在成百上千的网络地址。在这些环境中，某些路由器中可能会拥挤着大量路由信息。*路由聚合*，也称为路由汇总，减少了路由器必须维护的路由数量，因为它以一个汇总地址代表一系列的网络地址。在大型、复杂网络中使用路由汇总的另一个优点是，它能阻隔其它路由器的拓扑变更。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。

除减少了中枢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。可以汇总区域内路由或外部路由。

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，可使一系列路由被识别为一个路由，以简化处理。注意，执行重新分配时需要路由图。

使用 WebUI 或 CLI **set summary-import** 命令，可汇总路由重新分配。

范例：汇总重新分配的路由

在下例中，将汇总网络地址 2.1.1.0/16 下的一组已重新分配路由。

WebUI

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: 2.1.1.0/16

Tag: 20

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set redistribute route-map abcd protocol static
4. ns(trust-vr/ospf)-> set redistribute route-map abcd protocol bgp
5. ns(trust-vr/ospf)-> set summary-import 2.1.1.0/16 tag 20
6. ns(trust-vr/ospf)-> save

移除缺省路由

使用 WebUI 或 CLI **set reject-default-route** 命令，可移除从 OSPF 获取的缺省路由。

范例：从路由表移除缺省路由

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

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set reject-default-route
4. ns(trust-vr/ospf)-> save

设置区域范围

配置区域范围后，区域边界路由器便可对区域内通告的网络进行汇总。区域范围能将一组子网统一到单个网络地址中，以在汇总链接通告中进行通告。配置区域范围时，还可指定是要通告还是要保留定义的区域范围。

要配置区域范围，请使用 WebUI 或 CLI **set area** 命令。

范例：配置区域范围

在下例中，将为区域 0.0.0.10 创建区域范围 20.20.0.0/16。

WebUI

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

IP: 20.20.0.0

NetMask: 255.255.0.0

Type:（选择）Advertise

Action: Add

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set area 0.0.0.10 range 20.20.0.0/16 advertise
4. ns(trust-vr/ospf)-> save

设置 Hello 泛滥攻击临界值

使用 WebUI 或 CLI **set hello-threshold** 命令，可配置指定时间内允许的最大 hello 封包数。

范例：配置 Hello 临界值

在下例中，将配置 20 个封包的临界值。

WebUI

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

Prevent Hello Packet Flooding Attack: On

Max hello packet: 20

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set hello-threshold 20
4. ns(trust-vr/ospf)-> save

设置 LSA 临界值

“链接状态通告”(LSA) 使 OSPF 路由器能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。

要设置虚拟路由器在特定时间内接收的 LSA 数量，请使用 WebUI 或 CLI **set lsa-threshold** 命令，配置每个邻接方在每个 LSA 间隔内可接收的最大 LSA 数，以防止 LSA 泛滥。

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

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set lsa-threshold 10 10
4. ns(trust-vr/ospf)-> save

配置 RFC-1583 环境

使用 **set rfc-1583** 命令，可设置或显示 OSPF，如 Request for Comments 1583 文档所规定。

范例：改变到 RFC-1583 环境

在下例中，将环境改变到与 RFC 1583 指定环境兼容的环境。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit OSPF Instance：选中 **rfc-1583 compatible** 复选框，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol ospf
3. ns(trust-vr/ospf)-> set rfc-1583
4. ns(trust-vr/ospf)-> save

2

BGP 任务参考

BGP （边界网关协议）是互联网上自治系统 (AS) 之间进行通信的路由协议。每个自治系统中的对等路由器都使用 BGP 来交换路由信息。每个 BGP 对等路由器都需要明确的配置，带有其通告给（和接收自）对等设备的网络层可到达性信息。

本章介绍了在 BGP 环境下，配置本地虚拟路由器的重要的以及通用的程序。

BGP 命令

本节简要介绍了 BGP 环境，以及配置使用 BGP 协议的本地虚拟路由器的 CLI 命令。

注意：*关于 BGP 命令的详细信息，请参阅* NetScreen CLI Reference Guide *的第一卷。*

启动环境

必须先启动 **bgp** 环境，然后才能执行 BGP 命令。启动 **bgp** 环境需要两个步骤：

1. 执行 **set vrouter** 命令，进入 **vrouter** 环境：

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

   其中 *vrouter* 为虚拟路由器名称。（在本例中，*vrouter* 是 trust-vr 虚拟路由器。）

2. 执行 **set protocol bgp** 命令，进入 **bgp** 环境。

   ```
   ns(trust-vr)-> set protocol bgp
   ```

有关环境的详细信息，请参阅第 **2**-58 页上的 “CLI 中的环境相关命令”。

基本 BGP 命令介绍

以下命令在 **bgp** 环境中可执行。

aggregate

使用 **aggregate** 命令可创建、显示或删除聚合。

聚合是一种技术，该技术将一定范围内的路由地址汇总为单个路由条目，表示为 IP 地址和子网掩码。聚合能减少路由器的路由表大小，同时保持其连接性水平。另外，聚合还能减少通告地址的数量，从而减少开销。

命令选项：**get**、 **set**、 **unset**

always-compare-med

使用 **always-compare-med** 命令可启用、禁用或显示当前的 **always-compare-med** 设置。启用此设置时， NetScreen 设备使用多出口点识别器 (MED) 比较来自每个自治系统 (AS) 的路径。 MED 确定到每个邻接 AS 的最合适的进入或退出点。

命令选项：**get**、 **set**、 **unset**

as-path-access-list

使用 **as-path-access-list** 命令可创建、移除或显示 AS 路径访问列表中的规则表达式。

AS 路径访问列表起到信息包过滤机制的作用。 NetScreen 设备能参考这一列表，并根据包括在该列表中的规则表达式来允许或禁止 BGP 信息包。

命令选项：**get**、 **set**、 **unset**

community-list

使用 **community-list** 命令可在公共组列表中输入路由器、从该列表中移除路由器，或者显示该列表。

公共组由包含相同公共组属性的路由组成。此属性是根据某些有用的标准将路由分类的标识符。所有带有相同公共组属性的路由被称作同一公共组的成员。当路由器需要以相同方法处理两个或更多已通告的路由时，可使用公共组属性。

命令选项：**get**、 **set**、 **unset**

confederation	使用 **confederation** 命令可创建联合、移除联合，或显示联合信息。 联合是将一个 AS 划分为若干个较小的子 AS，并将它们分组的技术。使用联合能减少 AS 中的连接数量，从而简化路由处理。 命令选项：**get**、 **set**、 **unset**
enable	使用 **enable** 命令可启用或禁用 BGP。 命令选项：**get**、 **set**、 **unset**
flap-damping	使用 **flap-damping** 命令可启用或禁用 **flap-damping** 设置。 启用此设置会阻塞路由的通告，直至路由稳定。 Flap 衰减允许 NetScreen 设备在 AS 边界路由器 （与出现不稳定情况的区域相邻）包含不稳定路由。 命令选项：**get**、 **set**、 **unset**
hold-time	使用 **hold-time** 命令可指定或显示从 BGP 邻接方收到消息之间的最大空闲时间 （以秒为单位）。 命令选项：**get**、 **set**、 **unset**
ignore-default-route	使用 **ignore-default-route** 命令可启用、禁用或显示 **ignore-default-route** 设置。启用此项设置能使 NetScreen 设备忽略从 BGP 对等路由器发出的缺省路由通告。 命令选项：**get**、 **set**、 **unset**
keepalive	使用 **keepalive** 命令可指定在激活信息包传输之间的最大空闲时间（以秒为单位）。这些传输确保了本地 BGP 路由器和邻接路由器之间的 TCP 连接。 命令选项：**get**、 **set**、 **unset**
local-pref	使用此命令可配置 BGP 路由器上的 LOCAL_PREF 度量。这一度量表示优先选择一组路径（与另一组相比）。 命令选项：**get**、 **set**、 **unset**

med	使用 **med** 命令可指定或显示本地多出口点识别器 (MED) ID 编号。当同一邻接自治系统 (AS) 具有多个退出 / 进入点时， MED 确定最适合的进入或退出点。 命令选项：**get**、 **set**、 **unset**
neighbor	使用 **neighbor** 命令可设置或显示本地 BGP 虚拟路由器的常规配置参数。建立到另一自治系统 (AS) 的 BGP 连接时，设备将使用这些参数。 命令选项：**clear**、 **exec**、 **get**、 **set**、 **unset**
network	使用 **network** 命令可创建、显示或删除网络和子网条目。 BGP 虚拟路由器将这些条目通告给对等设备，事先不请求重新分配到 BGP 中 （如静态路由表条目）。 命令选项：**get**、 **set**、 **unset**
redistribute	使用 **redistribute** 命令，可导入由使用非 BGP 协议的外部路由器通告的路由，或者显示当前的 **redistribute** 设置。 命令选项：**get**、 **set**、 **unset**
reflector	使用 **reflector** 命令可允许本地 BGP 虚拟路由器充当路由反射器。 *路由反射器*是将 “内部 BGP (IBGP)” 获知的路由传送到指定 IBGP 邻接方 （*客户机*）的路由器，从而排除了网格状网络中每个路由器与其它每个路由器通信的需求。客户机使用路由反射器将路由通告到整个自治系统 (AS)。 命令选项：**get**、 **set**、 **unset**
synchronization	使用 **synchronization** 命令可启用与 “内部网关协议 (IGP)” 的同步。 命令选项：**set**、 **unset**

基本 BGP 配置任务

以下配置任务是大多数 BGP 实施必须进行的。

创建虚拟路由器的 BGP 实例

要启用或禁用特定 BGP 虚拟路由实例，可使用 WebUI 或 CLI 的 **set enable** 命令。

范例：启动虚拟路由实例

注意：*虚拟路由器（如 trust-vr）一次只能拥有一个 BGP 虚拟路由实例。因此，如果已经存在一个实例，就不能创建新的 BGP 虚拟路由实例。*

在下例中，将启动一个虚拟路由实例（AS ID 为 20）并启用 BGP：

WebUI

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 (required): 20

BGP Enabled: （选择）

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp 20
3. ns(trust-vr/bgp)-> set enable
4. ns(trust-vr/bgp)-> save

指定从 AS 可到达的网络

在 BGP 网络的初始设置期间，需要构建一个从虚拟路由器可到达的网络的列表。BGP 虚拟路由器将这些网路条目通告给对等设备，事先不请求重新分配到 BGP 中（如静态路由表条目）。要创建网络列表中的条目，可使用 WebUI 或 CLI 的 **set network** 命令。

范例：创建从本地虚拟路由器可到达的网络

在下例中，将创建一个从本地虚拟路由器可到达的网络 (192.169.1.0/24)：

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Networks：
在 IP/Netmask 字段中输入 192.168.1.0/24，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set network 192.169.1.0/24
4. ns(trust-vr/bgp)-> save

启用聚合路由

聚合将一定范围内的路由地址汇总为单个路由条目，并表示为 IP 地址和子网掩码。可使用 WebUI 或 CLI 的 **set aggregate** 命令来创建、显示或删除 BGP 聚合。

范例：创建聚合路由条目

下例假设内部网络包含 192.168.10.0/24 的以下子网：

- 192.168.10.0/28
- 192.168.10.16/28
- 192.168.10.32/28
- 192.168.10.128/30

将各个路由聚合到一个通告 (192.168.10.0/24) 中，而不是发送给每个子网。

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 **OK**：

IP/Netmask: 192.168.10.0/24

Aggregate State （选择 Enable）

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> unset enable
4. ns(trust-vr/bgp)-> set aggregate ip 192.168.10.0/24
5. ns(trust-vr/bgp)-> set enable
6. ns(trust-vr/bgp)-> save

启用重新分配

当虚拟路由器通过其它动态协议（或通过静态配置）获知路由时，并不将这些路由自动通告给 BGP 对等方。必须先将这些路由导入到 BGP 协议中。要导入此类路由或显示目前的路由重新分配设置，请使用 WebUI 或 CLI **set redistribute** 命令。

关于导入路由重新分配规则和导入路由的详细信息，请参阅第 **2**-74 页上的 “路由重新分配”。

范例：创建重新分配规则

在下例中，为所有从 OSPF 获知的路由创建重新分配规则，并根据现有的路由图 (Corp_Office) 过滤路由：

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 **OK**：

Route Map: Corp_Office

Protocol: OSPF

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set redistribute route-map Corp_Office protocol ospf
4. ns(trust-vr/bgp)-> save

配置 BGP 邻接方

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。要确认虚拟路由器的邻接方，可使用 WebUI 或 **set neighbor** 命令。

注意：*如果邻接方与本地 BGP 发送方在相同 AS 中，则这两个设备使用 IBGP 来建立连接。*

范例：配置邻接方的虚拟路由器

在下例中，配置与邻接方连接的虚拟路由器。此邻接方具有以下属性：

- IP 地址为 192.4.55.4
- 驻留在 ID 号为 20 的 AS 中

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: 20

Remote IP: 192.4.55.4

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set neighbor 192.4.55.4 remote-as 20
4. ns(trust-vr/bgp)-> save

启用带有 IP 地址的 BGP 对等方

设置了虚拟路由器和对等方之间的连接后，必须启用此连接。要执行此操作，可使用 WebUI 或 CLI 的 **set neighbor** 命令。

范例：启用 BGP 对等方连接

在下例中，启用本地虚拟路由器和 BGP 邻接方 (192.4.55.4) 之间的连接：

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Neighbors > Configure（对于 192.4.55.4）：选择 **Peer Enabled**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set neighbor 192.4.55.4 enable
4. ns(trust-vr/bgp)-> save

配置等待时间计时器

网络稳定后，可能需要修改从 BGP 发送方到其邻接方的消息传输之间的最大时间间隔。要指定或显示此间隔，可使用 WebUI 或 CLI 的 **hold-time** 命令。

范例：设置等待时间值

在下例中，将 **hold-time** 值设置为 60 秒：

WebUI

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

Hold Time: Enable （选择）

Hold Time: 60

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set hold-time 60
4. ns(trust-vr/bgp)-> save

配置 Keepalive 计时器

Keepalive 传输确保了本地 BGP 路由器和邻接路由器之间的 TCP 连接始终不断。要设置或显示 Keepalive 信息包传输之间的空闲时间间隔 （以秒为单位），可使用 WebUI 或 CLI 的 **keepalive** 命令。

范例：设置 Keepalive 计时器

在下例中，创建 Keepalive 值 20：

WebUI

> ***注意：****不能通过 WebUI 特别设置 Keepalive 时间间隔值。但是，由于 Keepalive 值始终为 Hold Time 值的 1/3，因而将 Hold Time 值设置为 60 秒就间接将 Keepalive 值设置为 20 秒。*

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance：选择 **Hold Time Enable**，在 Hold Time 字段中键入 **60**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set keepalive 20
4. ns(trust-vr/bgp)-> save

启用路由 Flap 衰减

Flap 衰减包含在 AS 边界路由器（与出现不稳定情况的区域相邻）不稳定路由。 **flap-damping** 设置阻塞路由通告，直至路由稳定。要启用或禁用此设置，可使用 WebUI 或 CLI 的 **set flap-damping** 命令。

范例：启用 Flap 衰减

在下面的范例中，您在 Trust-VR 上配置的 BGP 实例上启用分配程序衰减。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance：选择 **Route flap damping state**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set flap-damping
4. ns(trust-vr/bgp)-> save

废除来自对等路由器的缺省路由通告

您可以指示在虚拟路由器上配置的 BGP 实例忽略来自 BGP 对等的缺省路由通告。要启用、禁用或显示此 设置，可使用 WebUI 或 CLI 的 **ignore-default-route** 命令。

范例：忽略缺省路由通告

在下面的范例中，您启用在 Trust-VR 上定义的 BGP 实例忽略从 BGP 对等接收的缺省路由通告。

WebUI

Network > Routing > Virtual Routers > Edit （对于 trust-vr）> Edit BGP Instance：选择 **Ignore default route from peer**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set ignore-default-route
4. ns(trust-vr/bgp)-> save

高级 BGP 配置任务

下列配置任务为可选任务，仅在高级网络环境中为必要任务。

将路由图应用到来自指定邻接方的路由

路由图充当进出 BGP 邻接方的路由的过滤器。要将路由图条目应用到指定邻接方的内向和外向路由中，可使用 WebUI 或 CLI 的 **set neighbor** 命令。

范例：应用路由图

在下例中，将两个现有路由图 （ID 编号为 10 和 15）应用到现有邻接方配置 (192.168.1.182) 中。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Neighbors > Configure（对于 192.168.1.182）：输入以下内容，然后单击 **OK**：

Incoming Map-Tag: 10

Outgoing Map-Tag: 15

Peer Enabled: （选择）

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set neighbor 192.168.1.182 route-map 10 in
4. ns(trust-vr/bgp)-> set neighbor 192.168.1.182 route-map 15 out
5. ns(trust-vr/bgp)-> save

为路径指定 Weight（权）

weight（权）值表示本地 BGP 虚拟路由实例和邻接方之间路由的优先级。此值越高，路由的优先级就越大。要设置此优先级，可使用 WebUI 或 CLI 的 **set neighbor** 命令。

范例：指定权值

在下面的范例中，您在 IP 地址 192.4.55.4 为 BGP 邻接方指定权值 30。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Neighbors > Configure（对于 192.168.1.182）：在 Weight 字段中键入 **30**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set neighbor 192.4.55.4 weight 30
4. ns(trust-vr/bgp)-> save

设置 AS 路径访问列表

AS 路径访问列表起到信息包过滤机制的作用。NetScreen 设备根据列表中包含的规则表达式来允许或拒绝 BGP 信息包。要创建、移除或显示 AS 路径访问列表中的规则表达式，可使用 WebUI 或 CLI 的 **as-path-access-list** 命令。

在 “AS Path String” 字段中指定标准：

表达式	说明
‘^’	指定路径的开始。
‘$’	指定路径的结束。

范例：创建 AS 路径访问列表中的条目

在下例中，创建了一个 AS 路径访问列表条目 （ID 编号为 10），与 100 开始的路径匹配。

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: 10

Permit: Permit

AS Path String: ^100

Action: Add

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set as-path-access-list 10 permit ^100
4. ns(trust-vr/bgp)-> save

配置公共组列表

公共组由包含相同公共组属性的路由组成。该属性是根据某些有用的标准将路由分类的标识符。所有具有相同公共组属性的路由即为相同公共组成员。当路由器需要以相同方法处理两个或更多已通告的路由时，可使用公共组属性。

要为公共组指定路由、从公共组中移除一个路由，或者显示公共组属性，可使用 WebUI 或 CLI 的 **community-list** 命令。

注意： *有关何时以及如何使用公共组的准则，不在本手册的介绍范围内。*

范例：创建公共组列表

在下例中，配置了两个设备 （对等方 A 和对等方 B）上的公共组。

在对等方 A 上，使用属性 100:500 配置一个 ID 为 1 的公共组列表。然后为内部网络配置一个静态路由，对等方 A 将此路由以及公共组属性一同通告给对等方 B。公共组属性使得对等方 B 能够选择性地将此静态路由插入到其路由表中。然后创建两个访问列表 (ACL)，并将它们应用到为路由重新分配配置的路由图中。这样就允许将已连接的和静态的路由插入到本地路由表中。最后，配置邻接方设置，允许设备附加具有公共组属性（在路由图中指定）的路由更新。

在对等方 B 上，使用属性 100:500 配置 ID 编号为 1 的公共组列表。然后配置访问列表，并将其应用到为路由重新分配配置的路由图中。然后将该路由图应用到访问列表中，这样，对等方 B 能将接收自对等方 A （具有附加的公共组 100:500）的静态路由插入本地路由表。最后，配置邻接方设置，将路由图与对等方 A 关联。

CLI (对等方 A)

公共组列表

1. ns-> set vrouter trust-vr
2. ns(trust-vr)->set protocol bgp
3. ns(trust-vr/bgp)-> set community-list 1 permit 6554100
4. ns(trust-vr/bgp)-> exit

静态路由

5. ns(trust-vr)-> set route 10.1.1.0/24 interface ethernet3 gateway 192.128.1.254

访问列表 (对于所有网络)

6. ns(trust-vr)-> set access-list 1
7. ns(trust-vr)-> set access-list 1 permit ip 0.0.0.0/0 1

访问列表 (对于 10.1.1.0/24 网络)

8. ns(trust-vr)-> set access-list 2
9. ns(trust-vr)-> set access-list 2 permit ip 10.1.1.0/24 1

路由图 (ACL 1)

10. ns(trust-vr)-> set route-map name “Import_ACL1” permit 90
11. ns(trust-vr)-> set match ip 1
12. ns(trust-vr)->exit

路由图 (ACL 2)

13. ns(trust-vr)-> set route-map name “Import_ACL2” permit 100
14. ns(trust-vr)-> set match ip 2
15. ns(trust-vr)-> set community 1

路由重新分配

16. ns(trust-vr)-> set protocol bgp redistribute route-map “Import_ACL1” protocol connected
17. ns(trust-vr)-> set protocol bgp redistribute route-map “Import_ACL2” protocol static

邻接方

18. ns(trust-vr)-> set neighbor 172.16.1.254 send-community
19. ns(trust-vr)-> set neighbor 172.16.1.254 route-map “Import_ACL2” out
20. ns(trust-vr/bgp)-> save

CLI (对等方 B)

公共组列表

1. ns-> set vrouter trust-vr
2. ns(trust-vr)->set protocol bgp
3. ns(trust-vr/bgp)-> set community-list 1 permit 6554100

访问列表 (对所有网络)

4. ns(trust-vr/bgp)-> set access-list 1
5. ns(trust-vr/bgp)-> set access-list 1 permit ip 0.0.0.0/0 1

路由图 (ACL 1)

6. ns(trust-vr/bgp)-> set route-map name “Import_Comm1” permit 90
7. ns(trust-vr/bgp)-> set match ip 1
8. ns(trust-vr/bgp)-> set match community 1

路由重新分配

9. ns(trust-vr/bgp)-> set protocol bgp redistribute route-map “Import_Comm1” protocol imported

邻接方

10. ns(trust-vr/bgp)-> set neighbor 172.16.1.254 route-map “Import_Comm1” in
11. ns(trust-vr/bgp)-> save

设置本地优先

与另一路由相比，虚拟路由器优先选择某外部路由的程度取决于 LOCAL_PREF 属性。 LOCAL_PREF 的值越高，优先级越大。路由器始终将此属性通告给内部对等方 （即，在同一 AS 中的对等方），并通告给邻接的联合，而不通告给外部对等方。

路由器收到包含 LOCAL_PREF 值的路由时，不会修改路由。BGP 路由器通告的非 BGP 路由具有缺省的 LOCAL_PREF 值 100。

要设置或显示 LOCAL_PREF 属性，可使用 WebUI 或 CLI 的 **local-pref** 命令。

范例：设置本地优先

在下例中，为通告给 IBGP 对等方的所有非 BGP 路由配置本地优先值 20：

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Parameters：在 **Local Preference** 字段中键入 **20**，然后单击 **OK**。

CLI

1. ns(trust-vr/bgp)-> set local-pref 20
2. ns(trust-vr/bgp)-> save

设置多出口点识别器 (MED)

多出口点识别器 (MED) 是一个可选的属性，在有多个到同一 AS 的连接时，用于选择外部 BGP 连接。当所有其它因素都相等时，虚拟路由器使用 MED 值最低的连接。

如果 EGBP 更新包含 MED 值，则路由器将 MED 发送给 AS 内的所有 IGBP 对等方。

如果将 MED 分配给虚拟路由器，则此值将覆盖任何从外部对等方的更新消息中收到的 MED。

要设置或显示 MED 值，可使用 WebUI 或 CLI 的 **med** 命令。

范例：设置 MED

在下例中，用值 20 来覆盖缺省值 (100)。当虚拟路由器将外部路由重新通告给 IBGP 对等方时，这些路由的 MED 值为 20：

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance：在 Default MED 字段中键入 **20**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set med 20
4. ns(trust-vr/bgp)-> save

设置多出口点识别器 (MED) 比较

您可以启用在 Trust-VR 上配置的 BGP 实例使用多出口点识别器 (MED) 比较来自每个自治系统 (AS) 的路径。MED 确定到每个邻接 AS 的最合适的进入或退出点。要启用、禁用或显示此设置，可使用 WebUI 或 CLI 的 **always-compare-med** 命令。

范例：设置 MED 比较

在下面的范例中，您启用 Trust-VR 上的 BGP 实例比较从每个 AS 接收的路径。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance：选择 **Always compare med state**，然后单击 **OK**。

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set always-compare-med
4. ns(trust-vr/bgp)-> save

配置路由反射器

*路由反射器*是将内部 BGP (IBGP) 获知的路由传送给指定的 IBGP 邻接方 （*客户机*）的路由器。这样，网格中的每个路由器就不必与其它每个路由器进行通信。客户机使用路由反射器将路由通告到整个自治系统 (AS)。要配置路由反射器，可使用 WebUI 或 CLI 的 **set reflector** 命令。

范例：指定路由反射器

在下例中，指定集群 （ID 编号为 10）中的路由反射器：

WebUI

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

Route Reflector: Enable

Cluster ID: 10

CLI

1. ns-> set vrouter trust-vr
2. s(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set reflector cluster-id 10
4. ns(trust-vr/bgp)-> save

将邻接方设置为路由反射器客户机

设置了传递路由信息的路由反射器后，必须配置接收此信息的客户机设备。要将 IBGP 邻接方配置为客户机，可使用 CLI 的 **neighbor** 命令。

范例：配置 IBGP 邻接方

在下例中，将 IBGP 邻接方 (292.55.4.3) 配置为客户机。

WebUI

注意：*要将邻接方设置为路由反射器客户机，必须使用 CLI。*

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set neighbor 192.55.4.3 reflector-client
4. ns(trust-vr/bgp)-> save

配置联合

联合将一个 AS 分为若干个较小的子 AS，并将它们分组，从而减小了 AS 内的连接数，并简化了网格创建的路由矩阵。要创建联合、移除联合或显示联合信息，可使用 WebUI 或 CLI 的 **confederation** 命令。

范例：创建联合

在下例中，创建一个联合 (200) 并添加一个成员 (30)。

WebUI

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

Enable: （选择）

ID: 200

Supported RFC: RFC 1965

Peer Member Area ID: 30

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set confederation id 200
4. ns(trust-vr/bgp)-> set confederation peer 30
5. ns(trust-vr/bgp)-> save

注意：*不必指定 RFC 1965。 NetScreen BGP 联合缺省支持此 RFC。*

添加 AS 成员到联合中

要将 AS 添加到联合中，可使用 WebUI 或 CLI 的 **set confederation** { ... } **peer** 命令。

范例：添加新联合

下例中，将 AS (45040) 添加到联合中。

WebUI

Network > Routing > Virtual Routers > Edit（对于 trust-vr）> Edit BGP Instance > Confederation：在 **Peer member area ID** 中键入 **45040**，然后单击 **Add**：

CLI

1. ns-> set vrouter trust-vr
2. ns(trust-vr)-> set protocol bgp
3. ns(trust-vr/bgp)-> set confederation peer 45040
4. ns(trust-vr/bgp)-> save

索引