NetScreen 概念与范例

ScreenOS 参考指南

第 1 卷：概述

ScreenOS 4.0.0

编号 093-0519-000-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

第 1 卷：概述

第 2 卷：基本原理

第 3 卷：管理

第 4 卷 : VPN

第 5 卷：动态路由

第 6 卷：虚拟系统

第 7 卷：NSRP

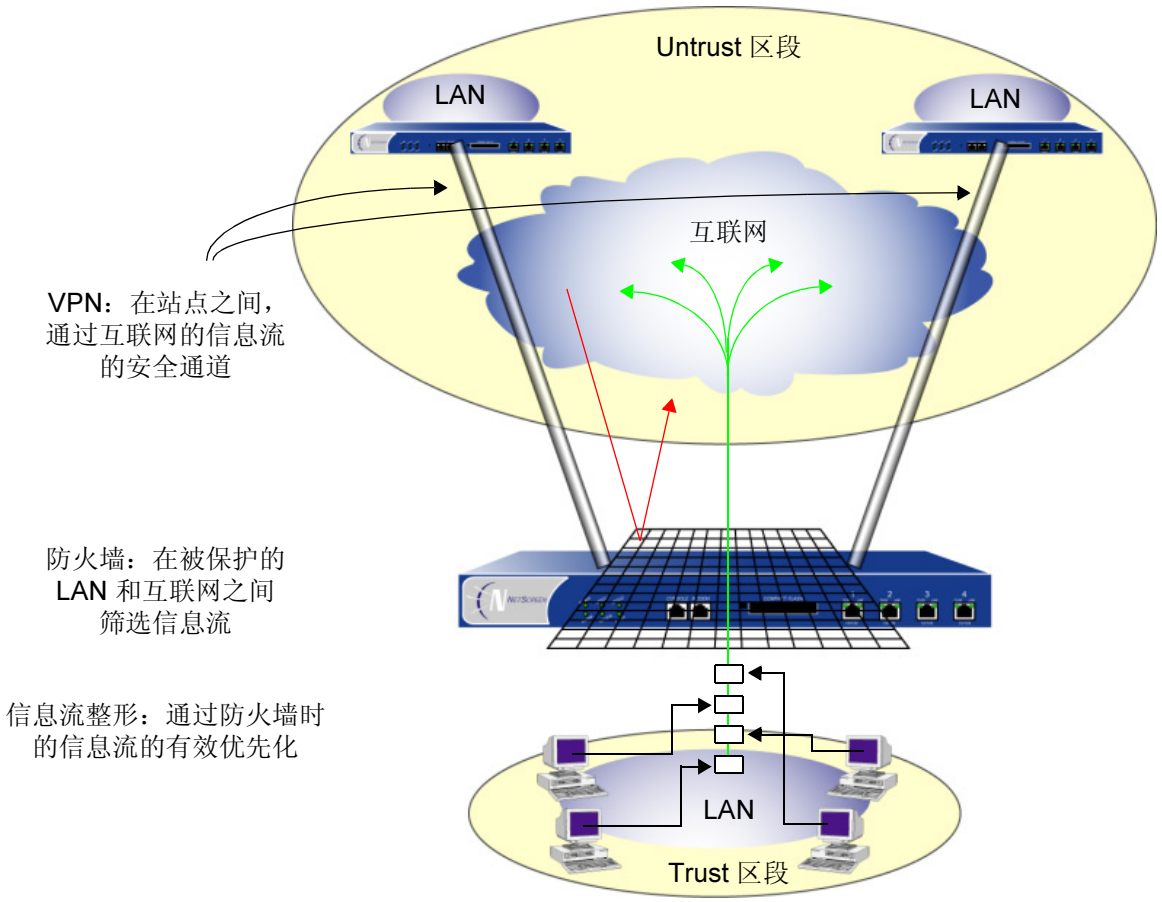
前言

NetScreen 设备是基于 ASIC 的、经 ICSA 认证[1]的互联网安全装置和安全系统，它结合防火墙、虚拟专用网 (VPN) 和信息流整形功能，当连接到互联网时，对安全区段，如内部局域网 (LAN) 或隔离区段 (DMZ) 提供灵活的保护。

- **防火墙：**防火墙筛选通过专用 LAN 和公用网 （如互联网）之间边界的信息流。
- **VPN：**VPN 提供一个在两个或多个远程网络装置之间的安全通道。
- **信息流整形：**信息流整形功能允许对通过 NetScreen® 防火墙的信息流进行管理监控和控制，来维护网络的服务质量 (QoS) 级别。

注意：*有关 NetScreen 符合 “联邦信息处理标准” (FIPS)，以及有关在 FIPS 模式下安装一个符合 FIPS 的 NetScreen 设备的说明，请参阅 NetScreen 文档 CD-ROM 上适用于各个平台的* NetScreen Cryptographic Module Security Policy *文档。*

1. “互联网计算机安全联盟” (ICSA) 是一个组织，它致力于连接到互联网上公司的所有类型的网络安全。作为 ICSA 的功能之一，它向以下几种安全产品提供产品证书，如病毒防护、防火墙、 PKI、入侵检测、 IPSec 和加密技术。 ICSA 已经认证了 NetScreen 有关防火墙和 IPSec 的所有产品。



NetScreen ScreenOS 是这样一个操作系统，它提供需要设置和管理任何 NetScreen 安全设备或系统的所有功能。*“NetScreen 概念与范例 ScreenOS 参考指南”* 提供关于通过 ScreenOS 配置和管理 NetScreen 设备的实用参考指南。

NETSCREEN 文档

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

欲获得 NetScreen 产品版本上的最新技术信息，请参阅该版本的记录资料。欲获得版本注释，请浏览 www.netscreen.com/support 并选定 **Software Download**。选定产品及其版本，然后单击 **Go**。（欲执行此下载任务，您必须是注册用户。）

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

概念与范例组织

*“NetScreen 概念与范例 ScreenOS 参考指南”*是一套多卷资料。以下信息概括和总结了每卷的资料：

第 1 卷，“概述”

- 在 *“NetScreen 概念与范例 ScreenOS 参考指南”中*，“目录”包含了所有卷的主目录。
- 附录 A，“词汇表”提供所有关键术语的定义，这些术语贯穿于 *“NetScreen 概念与范例 ScreenOS 参考指南”的所有卷中。*
- “索引”是一个主索引，它包括 *“NetScreen 概念与范例 ScreenOS 参考指南”的所有卷。*

第 2 卷，“基本原理”

- 第 1 章，“ScreenOS 体系结构”介绍 “USGA （Universal Security Gateway Architecture，通用安全网关体系结构）”的基本元素，NetScreen ScreenOS 中的体系结构，同时用一个包含四部分的范例来举例说明一种基于企业的配置，该配置中结合了这些元素中的大部分。在本章及以后所有各章中，每个概念都附有说明性的范例。
- 第 2 章，“区段”解释安全区段、通道区段和功能区段。
- 第 3 章，“路由和虚拟路由器”介绍虚拟路由器的概念，并解释如何在 NetScreen 设备上配置虚拟路由器。它还包含有关路由表条目的信息。
- 第 4 章，“接口”说明 NetScreen 设备上的各种物理的、逻辑的和虚拟的接口，而且包含各种防火墙攻击的信息，以及 NetScreen 提供的阻拦攻击选项。
- 第 5 章，“接口模式”解释 “透明”、“网络地址转换” (NAT) 和 “路由器”接口操作模式的概念。
- 第 6 章，“为策略构建块”讨论有关创建策略和虚拟专用网 (VPN) 的各个元素：地址（包括 VIP 地址）、用户和服务。它还介绍了几个支持 H.323 协议的配置的范例。
- 第 7 章，“策略”探究策略的组成及功能，而且给他们的创建和应用提供指导。

- 第 8 章，“用户认证”详述 NetScreen 支持的各种认证方法和用途。
- 第 9 章，“信息流整形”说明如何管理接口带宽、策略级别和优先化服务。
- 第 10 章，“系统参数”介绍“域名系统 (DNS)”寻址的概念；使用“动态主机配置协议 (DHCP)”去分配或传递 TCP/IP 设置； URL 过滤；下载及上载系统配置和软件；设置系统时钟。

第 3 卷，“管理”

- 第 1 章，“管理”说明本地和远程管理 NetScreen 设备的各种不同的可用方法。本章还解释了属于可被定义的四个网络管理员级别中的每一个级别的权限。最后，它说明了如何确保本地和远程管理信息流的安全。
- 第 2 章，“监控 NetScreen 设备”说明各种监控方法，并对解释监控输出提供指导。
- 附录 A，“SNMP MIB 文件”列出和简要描述了 MIB 编辑器可用的 “管理信息库 (MIB)”文件。

第 4 卷，“VPN”

- 第 1 章，“IPSec”提供有关 IPSec 的背景信息，介绍一个以主动模式和主模式 IKE （因特网密钥交换）协商的 “阶段 1”流序列，最后介绍了有关 “NAT 穿透”的信息。
- 第 2 章，“公开密钥密码术”提供有关如何获得和加载数字证书和证书撤消列表 (CRL) 的信息。
- 第 3 章，“基于路由的 VPN”提供基于路由的 VPN 配置的多方面的范例，包括集中星型和背对背通道设计。
- 第 4 章，“基于策略的 VPN”提供有关基于策略的 VPN 配置的多方面的范例，这些配置是关于 LAN 到 LAN 和客户端到 LAN 的通信的，而这些通信使用 “手动密钥”和 “自动密钥”IKE 机制。它还详细说明了，如何使用通道接口，去提供基于策略的 NAT，这个 NAT 是有关通过站点之间的 VPN 通道的信息流的，在这些站点之间有使用一个重叠的地址空间的可信任网络。
- 第 5 章，“L2TP （Layer 2 Tunneling Protocol，第 2 层通道协议）”解释 “第 2 层通道协议 (L2TP)”，它单独使用以及与 IPSec （IPSec 上的 L2TP）配合使用。

第 5 卷，“动态路由”

- 第 1 章，“OSPF 任务参考”介绍路由的基本原理、概念及路由如何适配安全设备（重点强调 NetScreen 设备）。
- 第 2 章，“BGP 任务参考”提供了基本路由概念和术语。

第 6 卷，“虚拟系统”

- 第 1 章，“虚拟系统”提供虚拟系统的概念、专用的和共享的接口，以及基于 VLAN 和基于 IP 的信息流分类。它还介绍如何建立虚拟系统，以及创建虚拟系统管理员。

第 7 卷，“NSRP”

- 第 1 章，“NSRP”说明如何对冗余组中的 NetScreen 设备布线、配置和管理，以便提供使用“NetScreen 冗余协议 (NSRP)”的高可用性。

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)。以下介绍这两种界面使用的约定。

WebUI 导航约定

本书中用一个尖角符号 (>) 来指示在 WebUI 中的导航，其方法是单击菜单选项和链接。

范例：Objects > Addresses > List > New

为访问新的地址配置对话框，请执行以下操作：

1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示出一个对象选项子菜单。
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，显示出一个 Addresses 选项子菜单。
3. 单击 **List**。
   出现通讯簿列表。
4. 在右上角单击 **New** 链接。
   出现新的地址配置对话框。

CLI 约定

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

相关性定义符

每个语法说明使用特殊字符来显示命令功能之间的相关性。

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

嵌套的相关性

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

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

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

以下范例说明一些 **set interface** 命令功能的相关性。

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

这个 { 和 } 括号说明指定的任一个 **flood** 或 **arp** 是强制性的。但是，[和] 括号说明，对于 **arp** 而言，**trace-route** 选项是非强制性的。因而，这条命令可以采取以下任一种格式：

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

CLI 命令及功能的可用性

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

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

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

A

词汇表

10BaseT：最常用的以太网形式称为 10BaseT，它表示使用铜双绞线电缆时的最高传输速度为 10 Mbps。以太网是将计算机连接到局域网 (LAN) 的一种标准。电缆距离最长为 325 英尺（100 米），每段的设备数最多为 1，每个网络的设备数最多为 1024。另请参阅 *100BaseT* 和 *非屏蔽双绞线 (UTP)*。

100BaseT：快速以太网的另一种说法，是将计算机连接到局域网 (LAN) 的一种已改进的标准。100BaseT 以太网除了可以用最高速度 100 Mbps 传输数据外，其工作方式几乎与常规以太网一样。与较慢的同类标准 10BaseT 相比，它更昂贵、更不常用。另请参阅 *10BaseT*。

AS：请参阅 *自治系统*。

AS 号：映射到 BGP 路由实例的本地自治系统的标识号。ID 号可以是任何有效整数。

AS 路径访问列表：一种访问列表，BGP 路由实例用来允许或拒绝相邻路由实例发送到当前虚拟路由实例的封包。

AS 路径属性类：BGP 提供了四类路径属性：Well-Known Discretionary、Optional Transitive 和 Optional Non-Transitive。

AS 路径字符串：作为 AS 路径标识符的字符串。与 AS 路径访问列表 ID 一起配置。

原子聚合：BGP 路由器用来将本地系统选择了一个广义路由的信息通知到其它 BGP 路由器的对象。

安全参数索引：(SPI) 是一个十六进制值，可对每个通道进行唯一标识。它还会告知 NetScreen 设备使用哪个密钥解密封包。

安全联盟：SA 是 VPN 参与者之间用于确保信道安全的有关方法和参数的单向协议。对于双向通信，必须至少有两个 SA，每个方向使用一个。在“自动密钥 IKE”协商期间，VPN 参与者会协商并同意“阶段 1”和“阶段 2”的 SA。另请参阅 *安全参数索引*。

安全区段：一个安全区段是一个或多个网络段的集合，这些网络段需要遵守按策略入站和出站信息流的规定。

BGP：一种自治系统间的路由协议。BGP 路由器和自治系统交换互联网的路由信息。

不工作间隔：某一路由实例确定另一路由实例未运行之前所花费的时间。

策略：策略为防火墙提供初始保护机制，允许用户根据 IP 会话详细信息来确定通过它的信息流内容。可使用策略在安全区域对资源进行保护，使其免受来自其它区段（区段间策略）或来自区段内部（区段内策略）的攻击。还可使用策略来监控试图通过防火墙的信息流。

成员 AS：包含在 BGP 联合体中的自治系统的名称。

重新分配：从使用其它路由协议的网络的另一部分将路由导入当前路由域的过程。发生此过程时，当前域必须转换来自其它协议的所有信息（尤其是已知路由）。例如，如果当前位于 OSPF 网络，并且该网络连接到 BGP 网络，OSPF 域必须导入 BGP 网络的所有路由，以通知其所有设备有关如何到达 BGP 网络中的所有设备的信息。所有路由信息的接收过程称为路由重新分配。

重新分配列表：从使用其它协议的另一个路由域导入的当前路由域的路由列表。

传输控制协议/网际协议 (TCP/IP)：TCP/IP 是一组通信协议，它支持局域网和广域网的对等连接功能。（通信协议是一组规则，它允许使用不同操作系统的计算机彼此之间互相通信。） TCP/IP 可控制“互联网”上计算机之间的数据传输方式。

等待时间：在 OSPF 中，开始进行“最短路径优先”(SPF) 计算的实例之间的最大时间长度。在 BGP 中，BGP 发送方与其邻接方之间消息传输的时间长度。

电路级代理：代理或代理服务器是一项技术，用于在 Web 服务器上高速缓存信息并作为某一 Web 客户端与该 Web 服务器之间的中介。它主要为用户存储最常用和最近已用过的万维网内容，目的是使访问更快速并且增强了服务器的安全性。这对于 ISP 而言比较常见，尤其是当它们链接到互联网的速度较慢时。在 Web 上，代理将首先尝试查找本地数据，如果未找到数据，则从数据长期驻留的远程服务器上获取数据。代理服务器还是允许通过防火墙直接访问互联网的机构。它们打开服务器上的套接字，允许通过该套接字与互联网进行通信。例如，如果计算机在受保护的网络内且要使用 Netscape 浏览 Web，则可在防火墙上设置代理服务器。可在计算机中将代理服务器配置为允许 HTTP 请求访问端口 80，然后将所有请求重新定向到适当位置。

动态路由：一种路由方法，适用于通过分析进入路由更新消息以调整到已更改的网络环境。如果该消息指示出网络已更改，路由软件会重新计算路由并发送新的路由更新消息。这些消息留置在网络中，以引导路由器重新运行其算法，并相应地更改其路由表。动态路由有两种常用形式，包括“距离向量路由”和“链接状态路由”。

对等方：请参阅 *邻接设备*。

多出口区分符：BGP 属性，用于确定“自治系统”进入点的相对优先级。

ESP/AH：IP 级安全协议（AH 和 ESP），最初是由 Network Working Group 提出的，旨在建立 IP 安全机制和 IPSec。在此处概括地使用术语 IPSec 来指封包、密钥和与这些协议相关的路由。“IP 认证报头 (AH)”协议提供认证。“封装安全性协议 (ESP)”既提供认证，又提供加密。

防火墙：是为信息流输入及提供保护并控制一个网络与另一个网络连接的设备。许多公司使用防火墙保护任何由网络连接的服务器，使其免受登录者的（有意或无意的）破坏。这种保护可以是一台配备安全装置的专用计算机，也可以是基于软件的保护。

访问列表：要限制路由器获悉或发出的路由信息，可根据发到或来自某一相邻路由器的路由更新信息进行过滤。过滤器由一个访问列表组成，该列表适用于发到或来自相邻路由器的更新信息。可按每个相邻路由器或每个对等组过滤路由信息。

非屏蔽双绞线 (UTP)：也称为 10BaseT。是用于电话线的标准电缆。也可用于连接以太网。另请参阅 *10BaseT*。

负载均衡：负载均衡是到两个或多个处理器的工作映射（或重新映射），目的是提高并发计算的效率。

GBIC：“千兆位接口连接器”(GBIC) 是一种用于将某些 NetScreen 设备连接到光纤网络的接口模块卡。

隔离区段 (DMZ)：源自军事术语，是两个敌对方之间的禁战区。DMZ 以太网将不同团体控制的网络和计算机连接在一起。它们可以是外部的，也可以是内部的。外部 DMZ 以太网通过路由器链接区域网络。

公共组：公共组是 BGP 对象的组合。通过更新公共组，将用新属性自动更新其成员目标。

广播网络：广播网络是一种支持许多路由器的网络，能够彼此直接通信。以太网就是广播网络中的一个范例。

动态过滤：一种可在 VPN 通道内使用的 IP 服务。过滤器是某些 NetScreen 设备控制从一个网络到另一个网络的信息流的一种方法。当 TCP/IP 将数据包发送到防火墙后，防火墙中的过滤功能会查看数据包中的报头信息，然后相应地进行发送。过滤器对诸如 IP 源地址或目标地址范围、TCP 端口、UDP、“互联网控制消息协议 (ICMP)”或 TCP 响应等标准起作用。另请参阅*通道*和*虚拟专用网 (VPN)*。

过滤列表：获准将封包发送到当前路由域的一个 IP 地址列表。

Hello 间隔：“Hello 封包”实例之间的时间长度。

Hello 封包：是通告信息（例如，它的存在与可用性）的封包，它将信息通告给生成封包的路由器周围的网络。

互联网：也称为“网络”。最初是由“美国国防部”设计，其目的在于使用通信信号抵御核战争并且服务于美国在全球的军事机构。“互联网”最初被称作 ARPAnet。该系统由链接在一起的计算机网络构成，便于在全球范围内提供数据通信服务，例如，远程登录、文件传输、电子邮件及新闻组。“互联网”是连接现有计算机网络的一种方式，它极大扩展了每套参与系统的触及范围。

互联网控制信息协议 (ICMP)：有时，网关或目的主机使用 ICMP 与源主机通信，例如，报告一个数据报处理中出现的错误。ICMP 使用 IP 的基本支持，似乎是更高级别的协议，但是，它实际上也是 IP 的组成部分，因此必须由每个 IP 模块执行。ICMP 消息在出现以下几种情况时发送：例如，数据报无法到达其目的地，网关没有转发数据报的缓冲容量，以及网关可引导主机在较短的路由上发送信息流。“网际协议”的设计并非完全可靠。这些控制消息的目的是在通信环境中提供关于问题的反馈，而并非使 IP 更可靠。

互联网密钥交换 (IKE)：一种在不安全的媒体（例如，互联网）上进行加密和认证的密钥交换方法。

IP 安全性 (IPSec)：由“互联网工程工作小组”(IETF) 制定的安全标准。它是一个协议套件，提供您对安全通信所需要的一切 — 认证、完整性及机密性 — 甚至可以在更大型的网络中进行实际密钥交换。另请参阅 *DES-CBC* 和 *ESP/AH*。

IP 地址：通常，TCP/IP 网络上的每个节点有一个 IP 地址。如下表中的 IP 地址类及格式所示，IP 地址由网络编号部分和主机编号部分组成：

表 0-1

类	节点数量	地址格式
A	> 32,768	nnn.hhh.hhh.hhh
B	256–32,768	nnn.nnn.hhh.hhh
C	< 256	nnn.nnn.nnn.hhh

此格式称为十进制点格式。“n”表示网络编号位，“h”表示主机编号位，例如，128.11.2.30。如果您将数据发送到网络以外，例如，发送到“互联网”，则需要从中央授权机构（目前是“网络信息中心”）获得网络编号。另请参阅*网络掩码*和*子网掩码*。

IP 网关：也称为路由器，网关是一个程序或一种专用设备，该设备将 IP 数据报从一个网络传输到另一个网络，直到抵达最终目标。

ISAKMP：“互联网安全协会和密钥管理协议”(ISAKMP) 为“互联网”密钥管理提供了一个框架，并且为安全属性的协商提供了具体的协议支持。此协议自身不建立会话密钥，但是，它可以配合多种会话协议建立协议使用，提供一个完整的“互联网”密钥管理解决方案。

Keep Alive：两激活封包之间的时间长度（以秒为单位），它可确保本地 BGP（边界网关协议）路由器和邻接路由器间 TCP 连接成功。此值等于等待时间的三分之一。缺省值为 60 秒。

集群：BGP AS 中的一组路由器，其中一个路由器被设置为路由反射器，其它则为该反射器的客户端。该反射器负责将它从另一 AS 中的设备处获悉的路由和地址信息通知到客户端。

注意：*术语“集群”的另一含义与高可用性有关。请参阅“NetScreen 冗余协议 (NSRP)”。*

集群列表：封包在通过 BGP 路由反射器集群时所记录的一个路径列表。

集线器：集线器是用于将计算机链接到一起的硬件设备（通常在以太网连接上使用）。它用做公用布线点，以便信息能通过一个中央位置流动到网络上其它任何一台计算机。集线器在物理以太网层重复信号。它保持标准总线类型网络的行为（例如，细电缆网），但是位于星状中心的集线器会生成星状拓扑。此配置可实现集中的管理。

加密：加密是将数据变成只有预定接收方可读取的形式的过程。要解密消息，加密数据的接收方必须具有适当的解密密钥。在传统加密方案中，发送方和接收方使用相同的密钥加密和解密数据。公开密钥加密方案使用两种密钥：任何人都可以使用的公开密钥和只有创建者拥有的相应私有密钥。通过这种方法，任何人都可以发送用所有者的公开密钥加密的消息，但只有所有者才拥有解密必需的私有密钥。DES（数据加密标准）和 3DES（三重 DES）是最流行的公开密钥加密方案中的两种方案。

静态路由：用户定义的路由，使得封包以指定路径在源节点和目标节点之间移动。静态路由算法是网络管理员在开始路由之前建立的表映射。这些映射不会更改，除非网络管理员要这样做。使用静态路由的算法设计简单，并在网络信息流相对可预知以及网络设计相对简单的环境中运行良好。

只要不改变路由，软件就会记住静态路由。但是，通过对管理距离值进行合理指定，也可用动态路由信息覆盖静态路由。要做到这一点，必须确保静态路由的管理距离超过动态协议的管理距离。

局部优先级：为了比“多出口区分符”(MED) 值为封包路径选择提供更好的信息，BGP 提供了一种称为 LOCAL_PREF 或局部优先级值的属性。可配置 LOCAL_PREF 属性使其有更高的值，以便使接收自可以提供期望路径的路由器比接收自提供较低期望值的路径的路由器所提供的前缀更高。此值越高，则路由的优先程度越高。LOCAL_PREF 属性为度量值，实际中最常用于表达一组路径相对其它路径的优先级。

局域网 (LAN)：任何将办公环境内的资源互联的网络技术，通常速度很快（如以太网）。局域网是一种短距离网络，用于将一座建筑物内的一组计算机链接到一起。10BaseT 以太网是最常用的 LAN 形式。一种称为集线器的硬件设备用做公用布线点，可通过网络将数据从一台机器发送到另一台。LAN 的距离通常限制在 1,640 英尺（500 米）以内，可在较小的地理区域内提供低成本、高带宽的联网功能。

距离向量：依靠某一算法的路由策略，该算法通过使路由器偶而向所有直接连接的相邻路由器广播其路由表的整个副本而起作用。此更新信息将识别每个路由器知道的网络和这些网络彼此间的距离。该距离以跳越计数的方式测定，或以封包在其源设备和试图到达的设备之间必须穿越的路由域数量测定。

聚合：将几个不同的路由组合在一起的过程，其中只有某一个路由通告自身身份。此项技术可使路由器的路由表最小化。

聚合器：根据网络掩码的值，将多个路由绑定到一个通用广义路由下的对象。

聚合状态：当某个路由器是绑定到一个地址的多个虚拟 BGP 路由实例之一时，则其即处于聚合状态。

连接状态：当发自某一路由器的封包到达另一路由器时，在源路由器和目的路由器之间会进行协商。协商将经过六种状态：空闲、连接、活动、开放发送、开放连接和确立。

联合体：BGP AS 中的一个对象，是 AS 中路由实例的一个子集。通过将 BGP AS 中的设备组合成联合体，可减少 AS 中路由连接矩阵（称为网格）的复杂性。

链接状态：链接状态路由协议使用通常称为“最短路径优先”(SPF) 的算法运作。与距离向量协议中依赖从直接连接的邻接路由器获得传播的信息不同，链接状态系统中的每台路由器都有网络的完整拓扑，并根据此拓扑计算 SPF 信息。

链接状态通告：启用 OSPF 路由器使设备、网络和路由信息可用于链接状态数据库的传送。每台路由器会检索来自网络中其它路由器发送的 LSA 中的信息，以构建整个互联网图，单个路由实例可从中提取路径信息以便在其路由表中使用。

邻接方：当两个路由器可以相互交换路由信息时，它们即被视为已构建了邻接方。点对点网络仅有两个路由器，因此这些路由器会自动形成邻接方。但点对多点网络是一系列的多个点对点网络。当这种更复杂的网络方案中的路由器组成对时，它们即被视为彼此相邻。

邻接设备：要开始配置 BGP 网络，首先需要在当前设备与对等设备之间建立连接，相邻设备称为*邻接设备*或*对等方*。虽然最初此对等设备可能看似不需要的信息，但实际上它对于 BGP 的工作方式非常重要。与 RIP 或 OSPF 不同的是，要使 BGP 工作，必须配置当前路由器及其邻接路由器这两台设备。虽然这需要更多工作，却能使联网的规模更大，因为 BGP 不使用对于内部建网标准所固有的受限通告技术。

有两种类型的 BGP 邻接设备：**内部邻接设备**位于同一个自治系统中，而**外部邻接设备**位于不同的自治系统中。两邻接设备之间需建立可靠连接，这可通过在两者之间建立 TCP 连接实现。在真正建立连接之前，在两预期邻接设备之间会发生握手过程，这包括多个阶段或*状态*。请参阅*连接状态*。

路由表：虚拟路由器内存中的一个列表，包含某路由器当前正在向其传送封包的所有已连接的网络和远程网络的实时视图。

路由重新分配：从一个虚拟路由器到另一个虚拟路由器的路由规则导出操作。

路由反射器：一个路由器，它的 BGP 配置允许在“内部 BGP”(IBGP) 邻接路由器或同一 BGP AS 内部的邻接路由器之间进行路由的重新通告。路由反射器客户机是使用路由反射器将其路由重新通告到整个 AS 的设备。它还依赖该路由反射器了解网络其余部分的路由信息。

路由器：一种硬件或虚拟（在 NetScreen 环境中）设备，可将数据分配到本地路由域内部或外部的其它所有路由器和接收点。路由器还用作过滤器，只允许经过授权的设备将数据传送到本地网络中，从而保证私有信息的安全。除了支持这些连接外，路由器还可处理错误、保存网络使用情况统计数据并且处理安全问题。

路由图：路由图和 BGP 配合使用，可控制并修改路由信息，还可定义在路由域间重新分配路由的条件。路由图包含一个路由图条目的列表，每个条目包含一个序列号、一个匹配项和一个设置值。路由图条目按递增序列号的顺序计算。某条目返回匹配条件后，不会再进一步计算路由图。找到匹配项后，路由图会执行对该条目的许可或拒绝操作。如果路由图条目不是一个匹配项，则会为匹配标准进行下一条目的计算。

路由文件布置和分配程序衰减：BGP 提供一项技术，可以阻拦靠近源路由的某处的通告，直到路由变得稳定为止。此方法称为*分配程序衰减*。路由文件布置和分配程序衰减允许在临近发生不稳定区域的 AS 边界路由器处存在路由不稳定。在路由拓扑增长时，对不必要的传播进行限制的效果是维持合理的路由更改收敛时间。

MD5：“信息整理”（版本）5 是可以通过任意长度的消息生成 128 位消息摘要（或散列）的算法。生成的散列（如同输入的“指印”）用于验证确认性。

MED 比较：“多出口区分符”(MED) 属性用于确定到达位于当前“自治系统”(AS) 内部或之后的特定前缀的理想链接。MED 包含一个度量值，该值表示进入该 AS 的优先程度。配置某链路的 MED 值，使其低于其它链路的 MED 值，即可建立该链路对其它链路的优先级。MED 值越低，该链接的优先级就越高。工作方式为：由一个 AS 设置 MED 值，其它 AS 使用该值确定要选择的路径。

媒体访问控制 (MAC) 地址：用于唯一标识网络接口卡的地址，如以太网适配器。对于以太网，MAC 地址是由 IEEE 分配的 6 个八位长字节地址。在 LAN 或其它网络中，MAC 地址是计算机的唯一硬件编号 （在以太网 LAN 中，它与以太网地址相同。）。从计算机连接到“互联网”（或“互联网”协议认为是互联网的主机）时，通信表会将您的 IP 地址与计算机在 LAN 上的物理 (MAC) 地址相关联。MAC 地址由远程通信协议的“数据链路控制 (DLC)”层中的“媒体访问控制”子层使用。用于每种类型的物理设备都有不同的 MAC 子层。

密钥管理：依靠签署和 / 或加密的私有密钥的形式使用秘密信息，是保护信息完整性和私密性的唯一合理途径。对这些秘密信息的管理和处理通常称为“密钥管理”。包括的活动有密钥的选择、交换、存储、认证、到期、撤消、更改和传输。管理信息安全系统的大部分操作在密钥管理中执行。

NetScreen 冗余协议 (NSRP)：一种专有协议，可提供配置和执行对象 (RTO) 冗余和高可用性 (HA) 集群中的 NetScreen 设备的设备故障切换机制。

内部网：该名称从“互联网”这个词衍生而来，它是一个类似于 Web 的访问受限制的网络，但它不在 Web 上。通常，内部网由一个公司所有并且进行管理，可以使公司与它的雇员分享资源，而不会让访问“互联网”的每个人获得机密信息。

前缀：代表路由的一个 IP 地址。

桥接器：一种根据数据链层信息在网络段间转发信息流的设备。这些网络段共享通用网络层的地址空间。

区段：一个区段可以是一个应用了安全措施的网络空间段（安全区段）、一个绑定了 VPN 通道接口的逻辑片段（通道区段），或者是一个执行特定功能的物理或逻辑实体（功能区段）。

区域：OSPF 是路由协议中最基本的排序方法。OSPF 区域将互联网络划分成更小、更易于管理的组件。此项技术可减少每个路由器必须存储和保持的有关所有其它路由器的信息量。当该区域中的某个路由器需要区域内部或外部另一个设备的信息时，它会与存储该信息的特定路由器联系。该路由器即被称为“区域边界路由器”(ABR)，它包含所有设备的基本信息。此外，ABR 区域边界路由器过滤所有进入区域的信息，以避免引起区域中其它路由器因收到它们不需要的信息而停顿。

区域边界路由器：一种在“区域 0”中至少有一个接口并在另一个区域中至少有一个接口的路由器。

区域范围：由下限和上限定义的 IP 地址序列，指示出某个区域内设备的一系列地址。

RJ-45：RJ-45 连接器与标准电话连接器类似，但宽度是其两倍（使用八芯线），并且使用多条线；将计算机连接到局域网 (LAN) 或电话机。

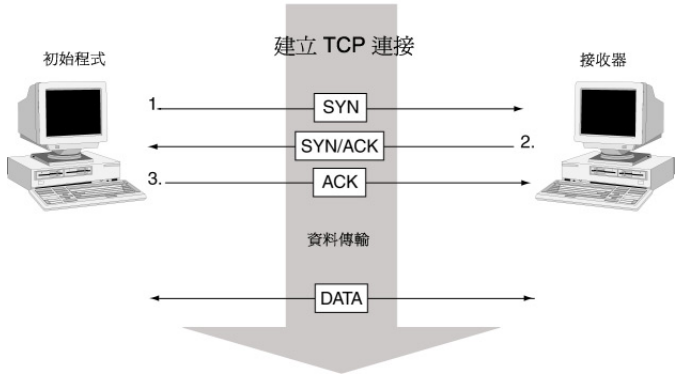
认证：认证可确保将数字数据传输到预定的接收方。认证还可向接收方确保信息及其来源（来自何处）的完整性。最简单的认证形式要求有获准访问特定帐户的用户名和密码。认证协议可以根据私有密钥加密，例如 DES 或 3DES，也可以根据使用数字签名的公开密钥系统进行加密。

认证报头 (AH)：请参阅 *ESP/AH*。

SHA-1：“安全散列算法 1”，一种用于从任意长度的消息生成 160 位散列的算法 （通常认为它比 MD5 更安全，因为它生成的散列更大。）。

三方握手：一个建立的具有三方封包交换的 TCP 连接，即通常所说的三方握手。程序如下所述：

1. 发起方发送 SYN（同步 / 开始）封包。
2. 接收方使用 SYN/ACK（同步 / 确认）封包回复。
3. 发起方使用 ACK（确认）封包响应。
4. 此时，已经建立该连接的两个端点，可以开始数据传输。



数据加密标准 (DES)：由美国标准技术研究所 (NIST) 开发的一种 40 位和 56 位加密算法。DES 最初是由 IBM 开发的一种数据块加密方法。后来，经过美国政府认证用于传输任何非绝密类的数据。DES 使用的是私有密钥加密算法。密钥由 64 位数据组成，这些数据经转换后与要发送消息的前 64 位组合。要采用加密，可通过使用由 16 个步骤组成的复杂过程将消息分解为 64 位的数据块，以便每个数据块可与密钥组合。虽然 DES 的保密性比较低，并仅有一次迭代，但是，如果使用稍稍不同的密钥对其进行重复，就可获得极佳的安全性能。

数据加密标准 - 密码块链 (DES-CBC)：直到最近，三重 DES (3DES) 最重要的用途才变为单一 DES 密钥加密，当所考虑的数据块密码实际上源自多重加密的结果时，确实没有必要考虑有人会如何执行各种数据块密码模式。但是，当 DES 接近其有效寿命期时，会更多地考虑使用日益广泛的三重 DES。特别是执行三重 DES 的 CBC 模式时，有两种显著的方法。在 CBC 模式中使用单一 DES 时，加密前，密文与明文进行“异或”操作。然而在使用三重 DES 时，我们可能在从密文到明文的所有三项 DES 操作中使用反馈，这称为外部 CBC。或者，我们可能在各单个加密组件中运行反馈，进而达到三重 (DES-CBC) 的效果。因为存在解密者根本看不到的内部反馈，所以这称为内部 CBC。在性能方面，使用内部 CBC 选项可能有几项优点，但经过调查，使用外部 CBC 实际上更安全。外部 CBC 是在 CBC 模式中使用三重 DES 的推荐方法。

通道：一种数据封装方法。使用 VPN 通道，专业移动设备用户会拨入当地的“互联网服务提供商”的“出现点” (POP) 而不会直接拨入其企业网络。这意味着无论专业移动设备用户位于何处，只需花费本地通话费用，就能拨入支持 VPN 通道技术的本地“互联网服务提供商”，并获得对其企业网络的访问权。当远程用户使用支持 VPN 通道的“互联网服务提供商”拨入其企业网络时，远程用户以及其组织都知道它是安全连接。所有的远程拨入用户均需经过“互联网服务提供商”站点的验证服务器进行验证，然后经过其企业网络的另一验证服务器再次验证。这意味着只有经过授权的远程用户才能访问其企业网络，并且只能访问授权其访问的主机。

通道接口：通道接口是出口或入口，发送到或接收自 VPN 通道的信息流均要经过它。可对通道接口进行编号（即指定一个 IP 地址），也可以不进行编号。编号后的通道接口可位于通道区段或安全区段。无编号的通道接口只能位于至少包含一个安全区段接口的安全区段。无编号的通道接口借用安全区段接口的 IP 地址。

通道区段：通道区段是安装有一个或多个通道接口的逻辑段。通道区段与作为其传输工具的安全区段相关联。

通告：路由器用来向网络中的其它设备通告自身身份，并传输基本信息（包括 IP 地址、网络掩码和其它数据）的一种方法。

通用安全网关体系结构 (USGA)：是一种 ScreenOS 体系结构，提供管理员能自定义并绑定到预定义和用户定义的安全区段的通用接口。

统一资源定位 (URL)：实现用电子方式指定可用资源位置的标准方法。也指位置或地址，URL 指定文件在服务器上的位置。常规 URL 语法为协议 :// 地址。例如，http://www.srl.rmit.edu.au/pd/index.html 表明协议为 http 协议，地址是 www.srl.rmit.edu.au/pd/index.html。

Trust：两个 NetScreen 区段中的一个，可以确保封包不被当前 NetScreen 域外部的设备看到。

Untrust：使当前 NetScreen 域之外的设备能看见封包的两个 NetScreen 区段之一。

Windows 互联网命名服务 (WINS)：WINS 是一项将 IP 地址映射到基于 Windows NT 服务器网络的 NetBIOS 计算机名上的服务。WINS 服务器将 Windows 网络环境下使用的 NetBIOS 名称映射到基于 IP 的网络中使用的 IP 地址上。

外部网：两个或几个内部网的连接。内部网是一种内部 Web 网络，允许某公司内部的用户进行通信和交换信息。外部网将虚拟空间和另一公司的内部网连接起来，从而允许这两个（或几个）公司在其自己的虚拟空间共享资源并通过互联网进行通信。此项技术极大地增强了公司间的相互沟通。

外部邻接路由器：两个不同的自治系统中的两个对等 BGP 路由器。

网关：驻留在当前路由域进入点的路由器，通常被称为缺省网关。

网际协议 (IP)：一种“互联网”标准协议，该协议定义了称为数据报的数据基本单位。数据报用在无连接、尽力而为的传输系统中。“网际协议”定义信息如何在“互联网”上的系统之间传送。

网络层可达到性信息：每个 AS 都有一个路由方案，该方案会指出通过它可到达的目的地。此路由方案称为“网络层可达到性信息”(NLRI) 对象。BGP 路由器定期生成并接收 NLRI 更新信息。各 NLRI 更新信息均包含可达到性信息包可通过的 AS 列表信息。NLRI 更新所说明的通用值包括：网络编号、该信息所通过的 AS 列表以及其它路径属性列表。

网络地址转换 (NAT)：用于将安全 IP 地址从地址池中转换为临时的外部注册 IP 地址的标准。这允许具有秘密指定的 IP 地址的“可信”网络获得对互联网的访问权。它还意味着您不必为网络中的每一台机器都获取注册的 IP 地址。

网络掩码：一个网络掩码可指出 IP 地址中指示网络标识的部分以及指示主机标识的部分。例如，IP 地址和网络掩码 10.20.30.1 255.255.255.0（或 10.20.30.1/24）是指 10.20.30.0 子网中的所有主机。IP 地址和网络掩码 10.20.30.1 255.255.255.255（或 10.20.30.1/32）是指一台单独主机。另请参阅 *IP 地址* 和 *子网掩码*。

无级路由：无论网络大小或类别如何，均支持域间路由。网络地址分为三类（但在 BGP 中，这些是透明的），使网络具有更大的灵活性。

虚拟 IP 地址：一个 VIP 地址将在一个 IP 地址上收到的信息流映射到基于封包包头中的目标端口号的另一地址。

虚拟安全接口 (VSI)：第 3 层中的逻辑实体，与 VSD 组中多个第 2 层物理接口相链接。VSI 绑定到一个设备的物理接口上，该设备充当 VSD 组的主设备。如果存在故障切换设备，并且它成为新的主设备，则 VSI 转移到 VSD 组中另一设备的物理接口上。

虚拟安全设备 (VSD)：是由一组物理 NetScreen 设备组成的单独逻辑设备。

虚拟局域网 (VLAN)：组成单独广播域的设备的逻辑（而非物理）分组。通过在传输数据的帧报头中使用标记（而不是通过在物理子网中的位置）来识别 VLAN 成员。在 IEEE 802.1Q 标准中介绍了 VLAN。

虚拟路由器：虚拟路由器是执行路由功能的 ScreenOS 组件。在缺省情况下，NetScreen 设备支持两个虚拟路由器：不信任虚拟路由器和可信虚拟路由器。

虚拟适配器：由 NetScreen 设备分配给远程 XAuth 用户，以便在 VPN 连接中使用的 TCP/IP 设置（IP 地址、DNS 服务器地址和 WINS 服务器地址）。

虚拟系统：虚拟系统 (vsys) 是主系统的一部分，作为一个单独实体显示给用户。虚拟系统彼此独立地驻留在同一 NetScreen 设备中。每个虚拟系统都可由其自身的管理员进行管理。

虚拟专用网 (VPN)：VPN 是一种简单、具有成本效益和安全的方法。采用这种方法，企业的远程办公人员和流动的专业人员可通过本地拨号访问企业网或另一“互联网服务提供商”。通过“互联网”的安全秘密连接比专线连接更具有成本效益。由于通道、筛选、加密及 IPSec（互联网协议安全性）等技术和标准的存在，令实现 VPN 成为可能。

以太网：一种局域网技术，由施乐公司的 Palo Alto Research Center 发明。以太网是一种使用 CSMA/CD 技术的尽力而为的传输系统。以太网可通过多种电缆方案互连，包括粗同轴电缆、细同轴电缆、双绞线和光纤电缆。以太网是将计算机连接到局域网 (LAN) 的一种标准。最常用的以太网形式称为 10BaseT，它表示使用铜双绞线电缆时的最高传输速度为 10 Mbps。

映射 IP 地址：MIP 是从一个 IP 地址到另一个 IP 地址发出的信息流的直接一对一映射。

用户数据报协议 (UDP)：TCP/IP 协议套件中的一个协议，“用户数据报协议”或 UDP 允许应用程序将数据报发送到远程机器上的其它应用程序中。UDP 协议主要在不保证传输和重复检测时提供不可靠和无连接数据报服务。它不使用应答，也不控制到达顺序。

执行对象 (RTO)：正常操作时在内存中动态创建的代码对象。RTO 的示例有会话表条目、ARP 高速缓存条目、证书、DHCP 租用和“IPSec 阶段 2”安全联盟 (SA) 等。

中继端口：中继端口允许交换机通过单个物理端口捆绑来自多个 VLAN 的信息流，并按封包的帧报头中的 VLAN 标识符 (VID) 对封包进行排序。

子接口：一个子接口是一个物理接口的逻辑分支，它从自己来源的物理接口借用所需的带宽。子接口是对物理上现有端口的某接口同一功能的抽象，并且通过 802.1Q VLAN 标记方法进行识别。

子网掩码：在较大规模的网络中，可使用子网掩码定义子网。例如，对于 B 类网络，如果子网掩码为 255.255.255.0，则指定小数点格式的前两部分为网络 ID，而第三部分为子网 ID。第四部分为主机 ID。如果不想在 B 类网络中使用子网，则应使用子网掩码 255.255.0.0。一个网络可划分为一个和多个物理网络，以构成主网络的一个子网。子网掩码是 IP 地址中用于代表网络内的子网的部分。使用子网掩码可允许使用通常不可用的网络地址空间，并可确保网络信息流不发送到整个网络中（除非希望这样做）。另请参阅 *IP 地址*和*网络掩码*。

自治系统 (AS)：AS 是一组与其余网络段分开并由单一技术管理的路由器。此路由器组使用一种内部网关协议 (IGP) 或几种 IGP 以及通用度量法在组内发送封包。该组还使用外部网关协议 (EGP) 向其它 AS 发送封包。每个 AS 均有一项路由计划，指示出通过它可到达的目标。此项计划即称为“网络层可达性信息 (NLRI)”对象。BGP 路由器定期生成并接收 NLRI 更新信息。

自治系统边界路由器：一种路由器，将某个运行一种路由协议的 AS 连接到运行不同协议的另一个 AS。

自治系统路径：当前传输过程中，路由器更新信息已到达的所有自治系统的一个列表。

索引

数字

A

B

C

F

G

H

I

J

M

N

S

T

U

V

W

X

Y

Z