NetScreen 概念与范例

ScreenOS 参考指南

第 3 卷：管理

ScreenOS 5.1.0

编号 093-1368-000-SC

修订本 B

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

Juniper Networks NetScreen 设备提供不同的方法来管理设备，既可本地管理，也可远程管理。第 3 卷 “管理”，介绍管理 NetScreen 设备的各种方法并解释 ScreenOS 的管理级别。本卷还介绍了如何保证 NetScreen 设备本地和远程管理的安全，以及如何监控设备的活动情况。附录中包含 “NetScreen 管理信息库” (MIB) 文件的概述，该文件支持 NetScreen 设备和 SNMP 管理应用程序之间的通信。

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

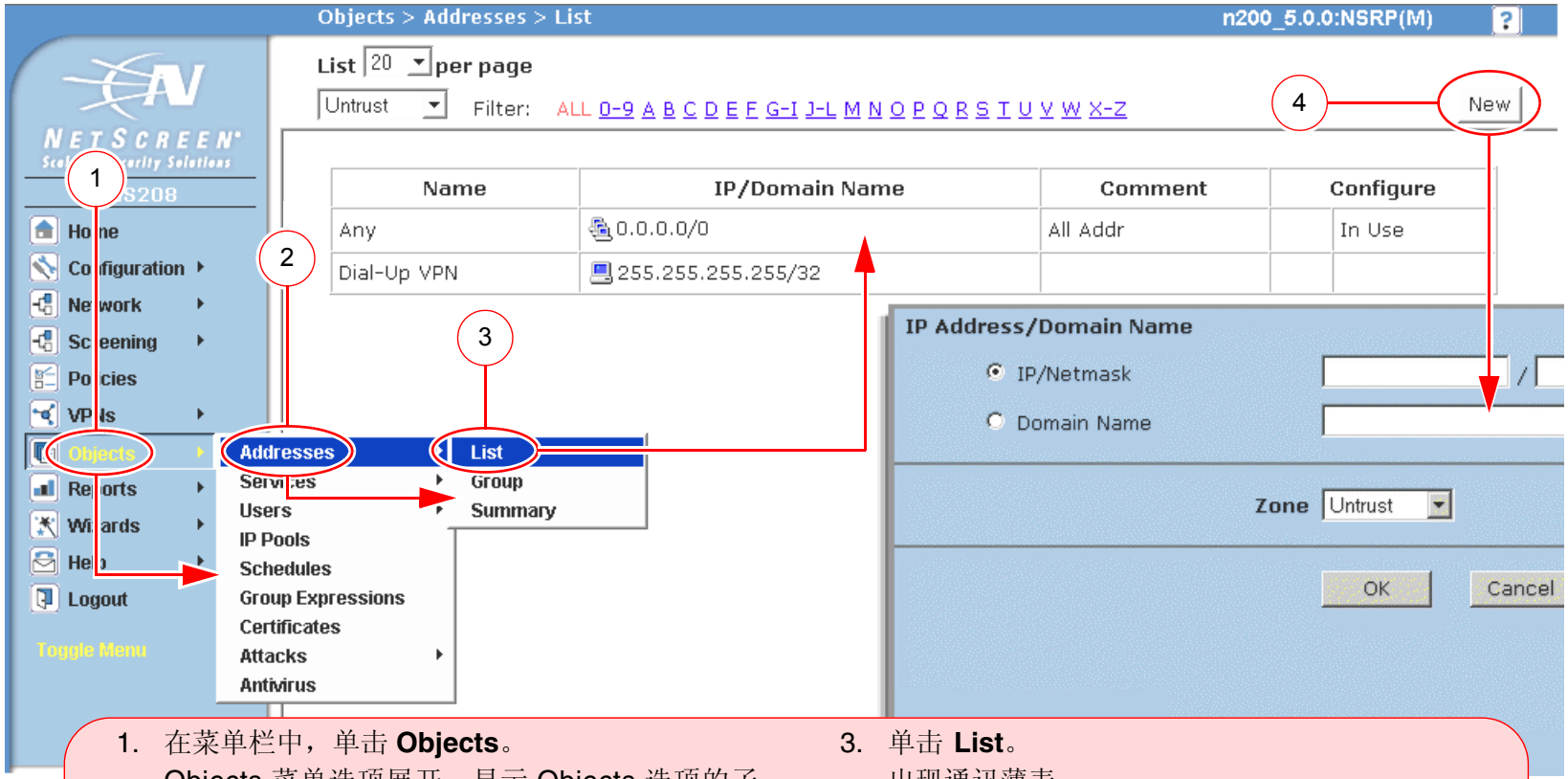
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

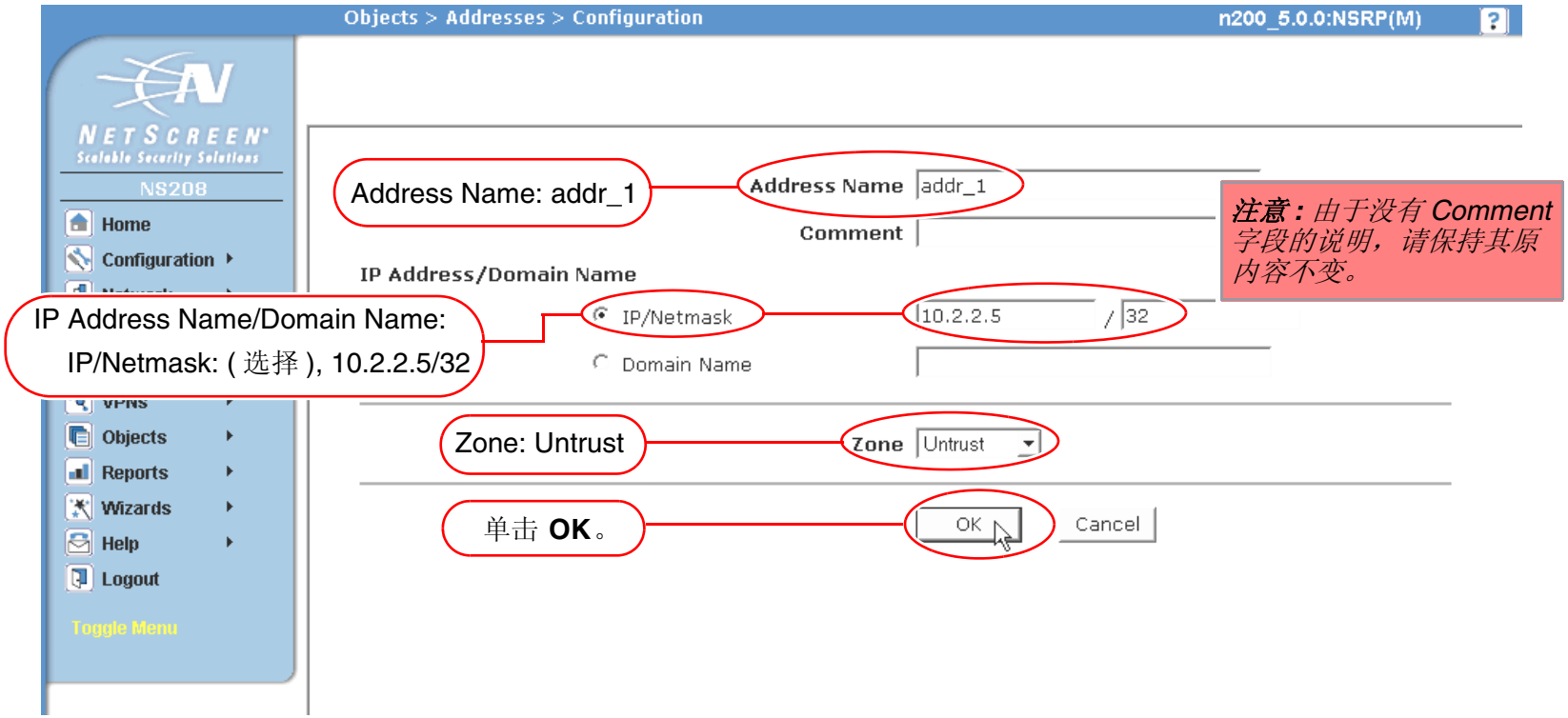
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

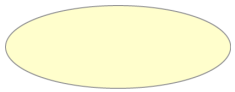


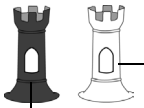
插图约定

下列图形构成了贯穿本书的插图所用的基本图像集：


通用 NetScreen 设备


虚拟路由选择域

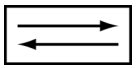

安全区段


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


通道接口

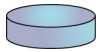

VPN 通道


路由器图标


交换机图标


包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）


互联网


动态 IP (DIP) 池


台式计算机


便携式计算机


通用网络设备
（例如：NAT 服务器，
接入集中器）


服务器

命名约定和字符类型

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

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

ScreenOS 支持以下字符类型 :

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

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

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

JUNIPER NETWORKS NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

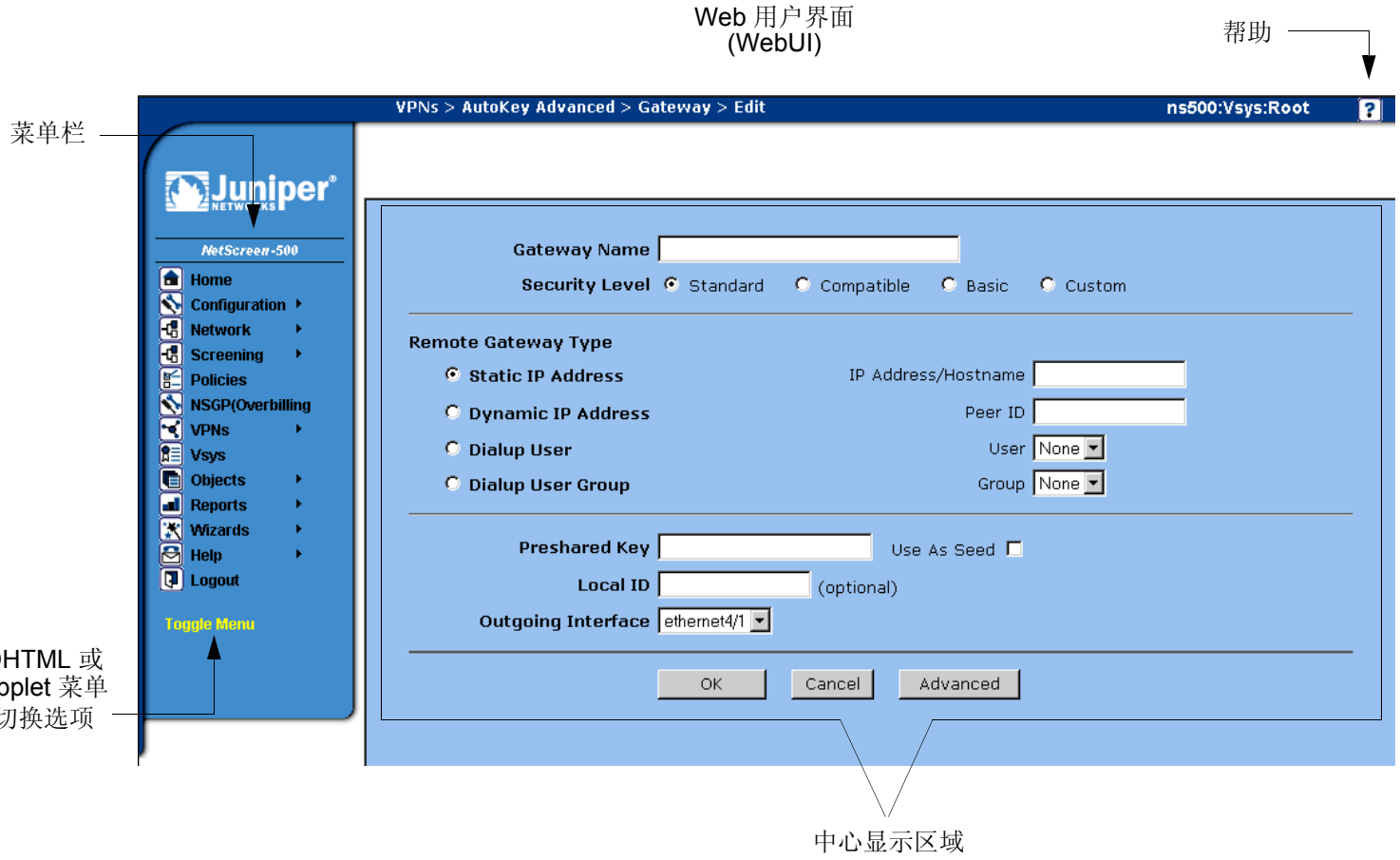
1

管理

本章介绍了多种管理方法及工具、保障管理信息流安全的方法，以及可以分配给 admin 用户的管理权限级别。本章包括以下部分：

通过 WEB 用户界面进行管理

为了便于管理，您可以使用 Web 用户界面 (WebUI)。 NetScreen 设备使用 Web 技术，该技术提供了配置和管理软件的 Web 服务器界面。



要使用 WebUI，必须具备以下条件：

- Netscape Communicator (版本 4.7 或更高版本) 或 Microsoft Internet Explorer (版本 5.5 或更高版本)
- 与 NetScreen 设备的 TCP/IP 网络连接

WebUI 帮助

可以在以下网址查看 WebUI 帮助文件 : http://help.juniper.net/help/english/*screenos_version* /ns*platform_number* (例如， http://help.juniper.net/help/english/5.1.0/ns500)。

还可以选择重新放置帮助文件。您可能想要将其存储在本地，并使 WebUI 指向管理员的工作站或本地网络上的某个安全服务器。倘若您无法访问互联网，必须将帮助文件存储在本地方可对其进行访问。

将帮助文件复制到本地驱动器

帮助文件可在文档 CD 中获得。可将 WebUI 修改为指向本地 CD 驱动器中 CD 上的帮助文件。也可以将文件从 CD 复制到本地网络上的服务器或工作站上的另一驱动器，并将 WebUI 配置成从以上位置调用帮助文件。

注意：*如果要从文档 CD 直接运行帮助文件，可以跳过此步骤。继续进行下面的 “将 WebUI 指向新的帮助位置”。*

1. 加载工作站 CD 驱动器中的文档 CD。
2. 导航到该 CD 驱动器，然后复制名为 “help” 的目录。
3. 导航到要存储 Help 目录的位置，将其粘贴到该处。

将 WebUI 指向新的帮助位置

现在必须重新定向 WebUI，使其指向 Help 目录的新位置。更改新文件路径的缺省 URL，其中 *path* 是从管理员工作站到 Help 目录的具体路径。

1. Configuration > Admin > Management: 在 Help Link Path 字段中，替换缺省的 URL **http://help.juniper.net/help/english/*screenos_version*/ns*platform_number***

   为

   (对于本地驱动器) **file://*path*…/help**

   或

   (对于本地服务器) **http://*server_name*…/*path*/help**

2. 单击 **Apply**。

   单击 WebUI 右上角的 **help** 链接，此时设备将使用您在 Help Link Path 字段中指定的新路径来查找相应的帮助文件。

HTTP

可使用标准 Web 浏览器通过 “超文本传输协议” (HTTP) 远程访问、监视和控制网络安全配置。

可通过在虚拟专用网 (VPN) 通道中封装 HTTP 管理信息流或通过 “安全套接字层” (SSL) 协议来保障它的安全。还可以通过将管理信息流与网络用户信息流完全分离来进一步保障它的安全。为此，可以通过 MGT 接口运行所有管理信息流 (在某些 NetScreen 设备上适用)，或者将某个接口绑定到 MGT 区段并使其专用于管理信息流。

***注意：**有关详细信息，请参阅第 7 页上的 “安全套接字层”、第 58 页上的 “用于管理信息流的 VPN 通道” 和第 37 页上的 “MGT 和 VLAN1 接口”。*

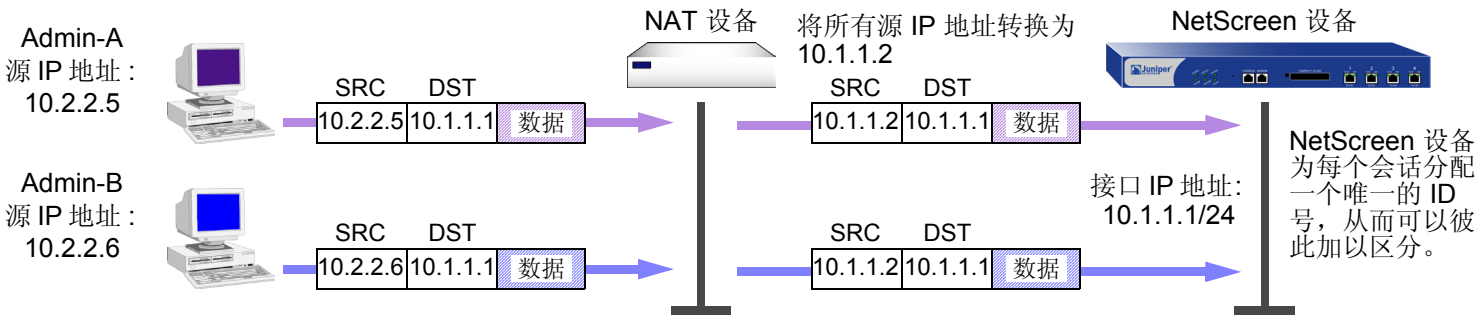
会话 ID

NetScreen 设备为每个 HTTP 管理会话分配一个唯一的会话 ID。对于支持虚拟系统 (vsys) 的 NetScreen 设备而言，该 ID 在所有系统 (根和 vsys) 上是全局唯一的。

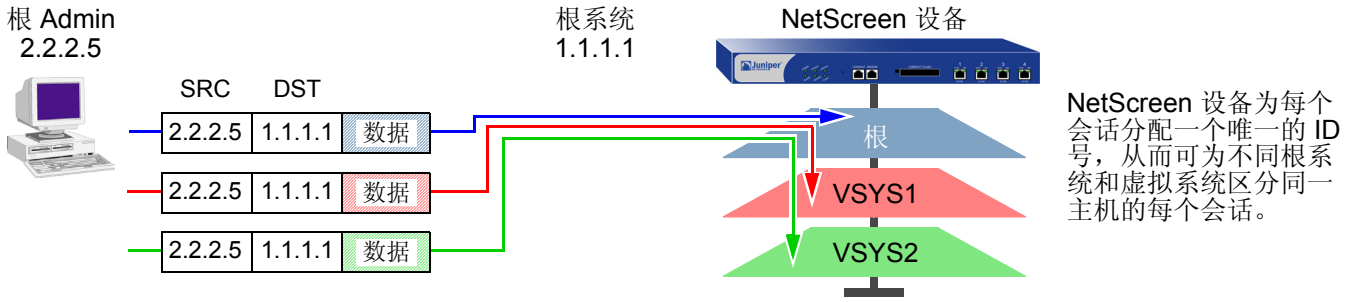
每个会话 ID 是一个 39 字节的数字，由五个伪随机生成的数字组合而成。 ID 生成过程的随机性 (相对于简单的数字增量方案而言) 使得预测 ID 几乎不可能。此外，这种随机性与 ID 的长度相结合，使得两个并发管理会话绝对不太可能有同一 ID 偶然重复的情况发生。

对于 NetScreen 管理员，使用会话 ID 具有以下两个优点：

- 对于为所有出站数据包分配相同源 IP 地址的 NAT 设备， NetScreen 设备可区分其后多个 admin 中的并发会话。



- NetScreen 设备可以区分从同一源 IP 地址经由根系统到不同虚拟系统的并发根级 admin 会话。

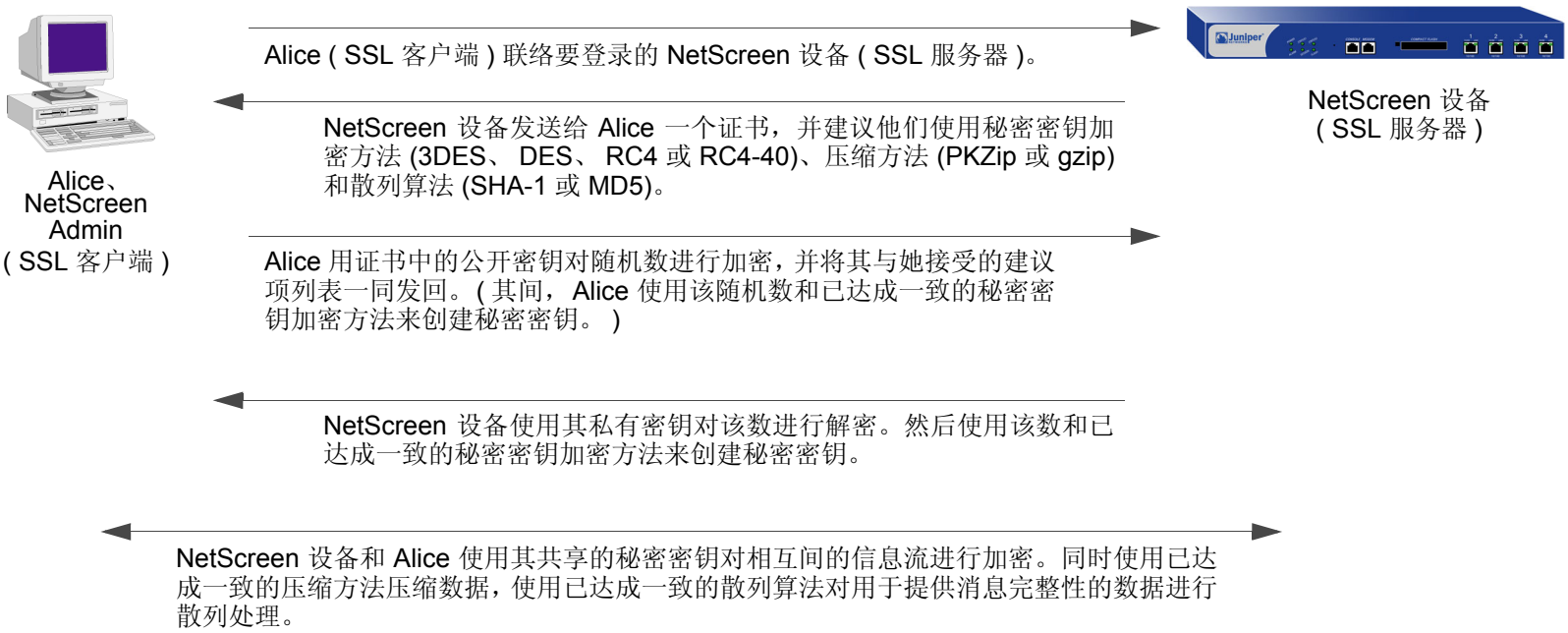


安全套接字层

“安全套接字层” (SSL) 是一套协议，该套协议可在通过 TCP/IP 网络通信的 Web 客户端与 Web 服务器之间提供安全连接。SSL 由 “SSL 握手协议” (SSLHP) 和 “SSL 记录协议” (SSLRP) 组成，通过前者客户端和服务器可进行相互认证以及协商加密方法，后者向更高级的协议 (如 HTTP) 提供基本安全服务。这两个协议运用于 “开放式系统互连” (OSI) 模型中的以下两层 :

- SSLHP 在应用层 (第 7 层)
- SSLRP 在表示层 (第 6 层)

SSL 不依赖应用协议，而是使用 TCP 来提供安全服务。SSL 首先使用证书认证服务器或客户端及服务器，然后对会话期间发送的信息流进行加密。NetScreen 仅支持服务器 (NetScreen 设备) 的认证，不支持客户端 (尝试通过 SSL 连接到 NetScreen 设备的 admin) 的认证。



NetScreen 设备可将使用 HTTP (缺省端口 80) 的管理信息流重定向到 SSL (缺省端口 443)。 SSL 的缺省证书是自动生成的自签名证书，不过如果需要，可在以后使用另一不同证书。由于 SSL 与 PKI 密钥 / 证书管理集成在一起，所以可从证书列表的任意项中选择 SSL 证书。还可将同一证书用于 IPSec VPN.

***注意：** 有关将管理 HTTP 信息流重定向到 SSL 的信息，请参阅第 11 页上的 “将 HTTP 重定向到 SSL”。有关自签名证书的信息，请参阅第 **5**-47 页上的 “自签证书”。有关获取证书的信息，请参阅第 **5**-29 页上的 “证书和 CRL”。*

SSL 的 ScreenOS 实现提供了以下功能、兼容性和集成 :

- SSL 服务器认证 (并非 SSL 服务器与客户端认证)，也即，NetScreen 设备向尝试通过 SSL 连接的管理员进行自我认证，但管理员不使用 SSL 向设备进行自我认证
- SSL 版本 3 兼容性 (并非版本 2)
- 与 Netscape Communicator 4.7x 及更高版本和 Internet Explorer 5.x 以后版本的兼容性[1]
- “公开密钥基础” (PKI) 密钥管理集成 (请参阅第 **5**-23 页上的 “公开密钥密码术”。)
- 以下 SSL 加密算法 :
  - 使用 40 位密钥的 RC4-40
  - 使用 128 位密钥的 RC4
  - DES: 使用 56 位密钥的数据加密标准
  - 3DES: 使用 168 位密钥的三重 DES
- 与 VPN 相同的 SSL 认证算法 :
  - “消息摘要” 版本 5 (MD5)—128 位密钥
  - “安全散列算法” 版本 1 (SHA-1)—160 位密钥

***注意：** RC4 算法总是与 MD5 配对使用，而 DES 和 3DES 总是与 SHA-1 配对使用。*

1. 检查您的 Web 浏览器，查看加密方法的强度以及浏览器支持的加密方法。(NetScreen 设备和您的 Web 浏览器必须支持 SSL 所用相同种类及规模的加密方法。) 在 Internet Explorer 5x 中，单击**帮助**、**关于 Internet Explorer**，然后阅读 “加密强度”。要获取高级安全包，请单击**更新信息**链接。在 Netscape Communicator 中，单击**帮助**、**关于 Communicator**，然后阅读有关 RSA® 的部分。要更改 SSL 配置设置，请单击**安全性信息**、**导航器**、**配置 SSL v3**。

SSL 配置

设置 SSL 的基本步骤如下：

1. 利用 NetScreen 设备在其初始启动期间自动生成的自签名证书，创建另一自签名证书，或者获取 CA 签名证书并将其加载到 NetScreen 设备[2]。

   注意：*有关自签名证书的详细信息，请参阅第* ***5-47*** *页上的 “自签证书”。有关申请和加载证书的详细信息，请参阅第* ***5-29*** *页上的 “证书和 CRL”。*

2. 启用 SSL 管理[3]：

   ### *WebUI*

   Configuration > Admin > Management: 输入以下内容，然后单击 **Apply**:

   SSL: (选择)

   Port: 使用缺省端口号 (443) 或将其更改为另一端口[4]。

   Certificate: 从下拉列表中选择所要使用的证书。

   Cipher: 从下拉列表中选择所要使用的加密方法。

   ### *CLI*

   ```
   set ssl port num
   set ssl cert id_num[5]
   set ssl encrypt { { 3des | des } sha-1 | { rc4 | rc4-40 } | md5 }
   set ssl enable
   save
   ```

2. 确保指定 Web 浏览器同样支持的位长度。
3. 在缺省情况下会启用 SSL。
4. 如果更改 SSL 端口号，则 admin 在其 Web 浏览器中输入 URL 时需要指定该非缺省端口号。
5. 要了解证书的 ID 号，请使用以下命令：**get pki x509 list cert**。

3. 配置用以管理 NetScreen 设备的接口，以允许进行 SSL 管理 :

WebUI

Network > Interfaces > Edit (对于要管理的接口): 启用 **SSL** 管理服务复选框，然后单击 **OK**。

CLI

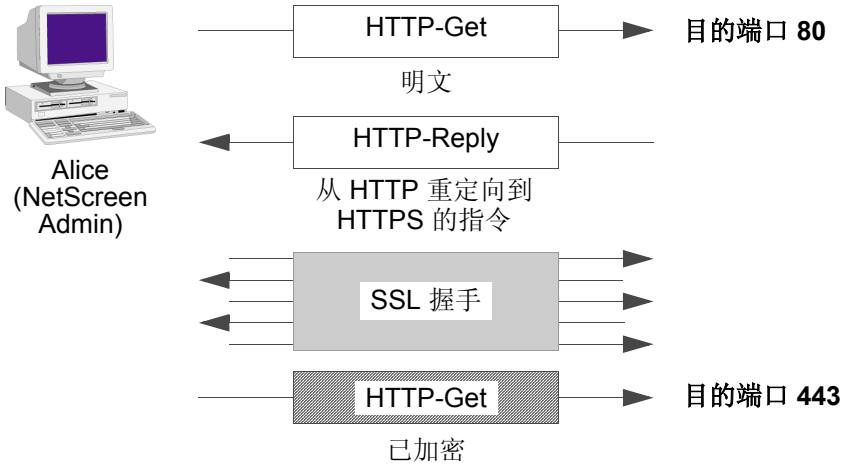
```
set interface interface manage ssl
save
```

4. 通过 SSL 端口连接到 NetScreen 设备。也即，当您在浏览器的 URL 字段中输入用于管理 NetScreen 设备的 IP 地址时，将 “http” 更改为 “https”，并在 IP 地址后加上冒号和 HTTPS (SSL) 端口号 (如果已更改了其缺省值) (例如， https://123.45.67.89:1443)。

将 HTTP 重定向到 SSL

NetScreen 设备可将使用 HTTP (缺省端口 80) 的管理信息流重定向到 SSL (缺省端口 443)。

HTTP 到 SSL 重定向



NetScreen 设备

在 SSL 握手期间，NetScreen 设备将其证书发送给 Alice。Alice 用证书中包含的公开密钥对随机数进行加密，并将其发回给 NetScreen 设备，该设备使用其私有密钥对该数进行解密。然后，参与双方使用共享随机数和协商的秘密密钥加密方法 (3DES、DES、RC4 或 RC4-40) 创建共享秘密密钥，用来对相互间的信息流进行加密。同时使用已达成一致的压缩方法 (PKZip 或 gzip) 压缩数据，使用已达成一致的散列算法 (SHA-1 或 MD-5) 对用于提供消息完整性的数据进行散列处理。

要启用重定向并对 SSL 使用缺省自动生成的自签名证书，请执行以下任一操作：

WebUI

Configuration > Admin > Management: 输入以下内容，然后单击 **Apply**:

Redirect HTTP to HTTPS: (选择)

Certificate: Default – System Self-Signed Cert

CLI

```
set admin http redirect[6]
save
```

虽然 HTTP 不具备 SSL 的安全性，但可以配置 NetScreen 设备，使其不重定向 HTTP 信息流。要禁用 HTTP 到 SSL 重定向机制，请清除 **Redirect HTTP to HTTPS** 选项 (WebUI)，或输入 **unset admin http redirect** 命令 (CLI)。

6. 不必通过输入 CLI 命令来应用与 SSL 一同使用的自动生成的自签名证书，因为缺省情况下 NetScreen 设备会将其应用于 SSL。如果先前已分配了与 SSL 一同使用的另一证书，而现在要改为使用缺省证书，则必须使用以下命令取消分配另外的那个证书：**unset ssl cert** *id_num*，其中 *id_num* 是先前分配证书的 ID 号。

通过命令行界面进行管理

高级管理员可通过命令行界面 (CLI) 进行更加精细的控制。要用 CLI 来配置 NetScreen 设备，可使用任何仿真 VT100 终端的软件。有了终端仿真器，便可使用 Windows、 UNIX™ 或 Macintosh® 操作系统中的控制台来配置 NetScreen 设备。要通过 CLI 进行远程管理，可使用 Telnet 或 “安全外壳” (SSH)。通过控制台端口进行直接连接后，便可使用 Hyperterminal®。

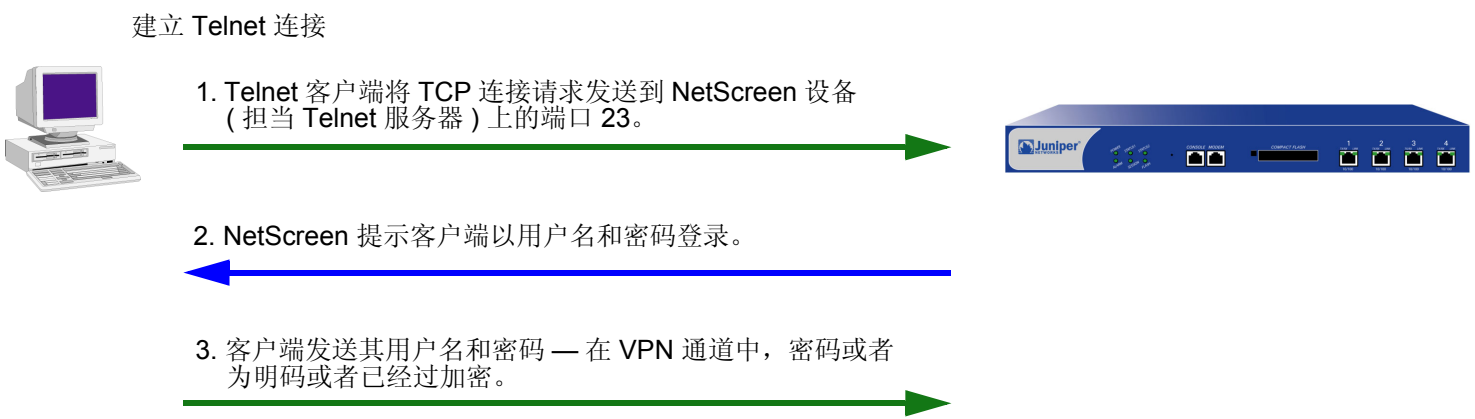
***注意：**有关 ScreenOS CLI 命令的完整列表，请参阅* NetScreen CLI 参考指南。

Telnet

Telnet 是一种登录及终端仿真协议，该协议使用客户端 / 服务器关系连接到网络设备并通过 TCP/IP 网络对这些设备进行远程配置。管理员在管理工作站上启动 Telnet 客户端程序并与 NetScreen 设备上的 Telnet 服务器程序建立连接。登录后，管理员可发出 CLI 命令，将其发送给 NetScreen 设备上的 Telnet 程序，对设备进行有效配置，如同通过直接连接进行操作一样。使用 Telnet 管理 NetScreen 设备需要以下条件：

- 管理工作站上有 Telnet 软件
- 与 NetScreen 设备具有以太网连接

建立 Telnet 连接的设置过程如下：



为了最大程序地减少未授权用户登录到设备的几率，可以限制 NetScreen 设备终止 Telnet 会话之前所允许的不成功登录尝试次数。此限制也可防止某些类型的攻击，如自动进行的词典式攻击。

缺省情况下，在关闭 Telnet 会话之前， NetScreen 设备最多允许三次不成功的登录尝试。要更改此数目，请输入以下命令：

```
set admin access attempts number
```

注意：必须使用 CLI 来设置此限制。

保障 Telnet 连接安全

可以通过将 Telnet 信息流与网络用户信息流完全分离来保障其安全。根据 NetScreen 设备型号，可通过 MGT 接口运行所有管理信息流，或者使某个接口 (如 DMZ) 完全专用于管理信息流。

此外，为了确保 admin 用户在通过 Telnet 管理 NetScreen 设备时使用安全连接，可以要求这类用户仅通过虚拟专用网 (VPN) 通道[7] 来执行 telnet。设置了此限制后，如果有人试图不通过 VPN 通道而执行 telnet，设备将拒绝访问。

要限制通过 VPN 进行 Telnet 访问，请输入以下命令：

```
set admin telnet access tunnel
```

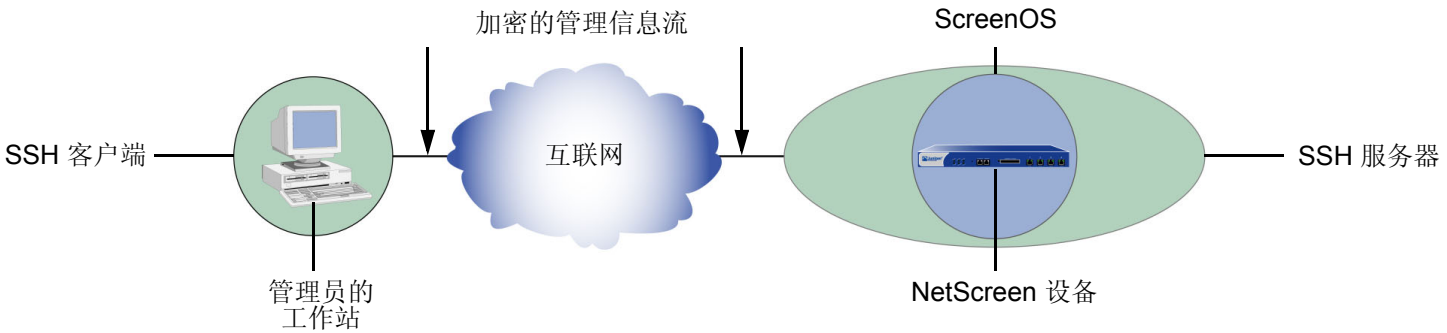
注意：必须使用 CLI 来设置此限制。

7. 有关 VPN 通道的信息，请参阅第 5 卷，“VPN”。

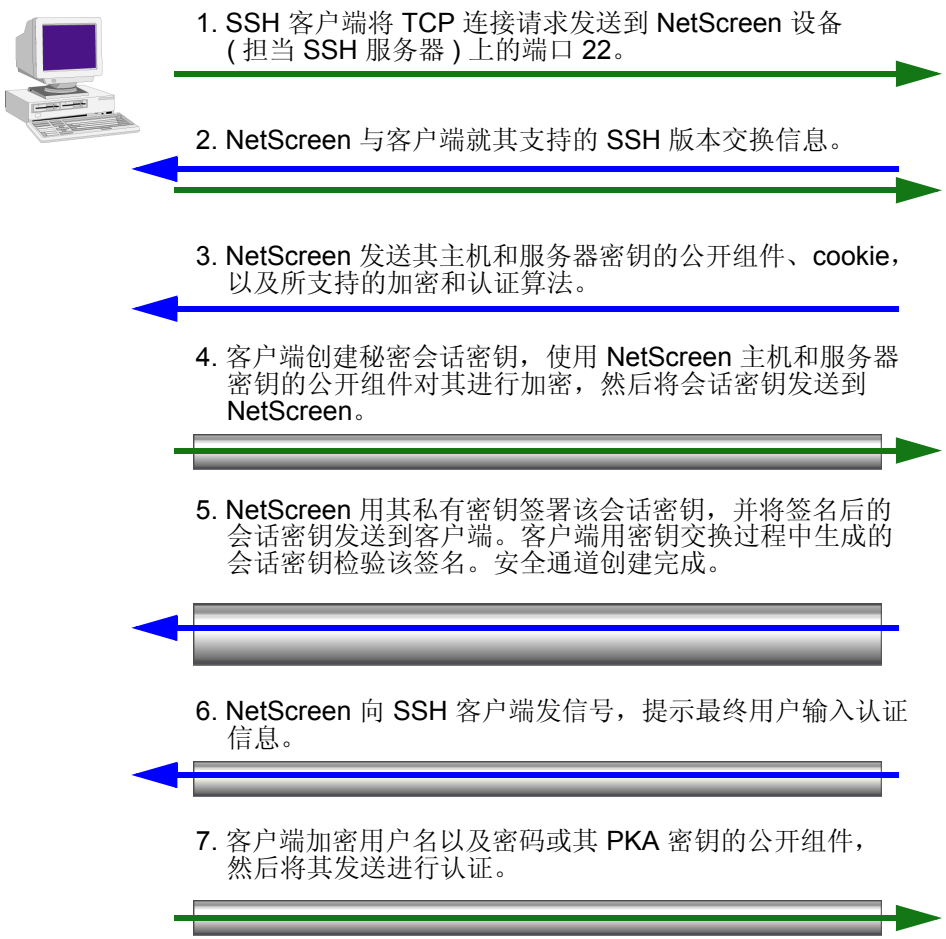
安全外壳

NetScreen 设备中内置的 “安全外壳” (SSH) 服务器提供了一种手段，借此，管理员可以使用能识别 “安全外壳” (SSH) 的应用程序以一种安全的方式来远程管理该设备。SSH 允许安全地打开远程命令外壳并执行命令。通过 SSH 可以防止 IP 或 DNS 欺骗攻击以及密码或数据拦截。

您可以选择在 NetScreen 设备上运行 SSH 版本 1 (SSHv1) 还是 SSH 版本 2 (SSHv2) 服务器。普遍认为 SSHv2 比 SSHv1 更安全，而且目前正在将其制定为 IETF 标准。但是，SSHv1 已得到广泛部署和普遍应用。注意，SSHv1 与 SSHv2 彼此并不兼容。也就是说，不能使用 SSHv1 客户端连接到 NetScreen 设备上的 SSHv2 服务器，反之亦然。客户端控制台或终端应用程序必须与服务器运行相同的 SSH 版本。



基本的 SSH 连接过程如下所示：



密钥

主机密钥：公开 / 私有密钥对中的公开密钥组件，用于向客户端进行 NetScreen 设备 /vsys 认证以及加密会话密钥。(每个 vsys 都有各自的主机密钥。) 主机密钥被永久绑定到设备 /vsys。

服务器密钥：临时 RSA 公开 / 私有密钥对，用于加密会话密钥。(在缺省情况下，NetScreen 每隔一小时为每个 vsys 生成一个新密钥。)

会话密钥：客户端与 NetScreen 在连接建立期间一同创建的临时秘密密钥 (DES 或 3DES)，用以对通信加密 (会话结束时，它将被废弃)。

PKA 密钥：持久的 RSA 公开 / 私有密钥，驻留于 SSH 客户端。开始 SSH 连接之前，必须在 NetScreen 设备上加载客户端的公开密钥，并且必须将 PKA 密钥与 admin 用户绑定。

注意：*公开 / 私有密钥对是这样的一组密钥，用其中一个加密的信息能够而且只能用另一个来解密。*

NetScreen 设备上一次最多只允许五个 SSH 会话。

客户端要求

如前所述，客户端应用程序必须与 NetScreen 设备上的服务器运行相同的 SSH 版本。必须将 SSHv2 客户端配置成请求 Diffie-Hellman 密钥交换算法和 “数字签名算法” (DSA) 进行公开密钥设备认证。必须将 SSHv1 客户端配置成请求 RSA 进行公开密钥设备认证。

NetScreen 设备上的基本 SSH 配置

以下是在 NetScreen 设备上配置 SSH 的基本步骤：

1. 确定将对 SSH 使用密码还是 “公开密钥认证” (PKA)。如果使用 PKA，则在进行 SSH 连接之前，必须将 PKA 密钥与 admin 绑定。有关使用密码或 PKA 的详细信息，请参阅第 19 页上的 “认证”。
2. 确定需要在 NetScreen 设备上启用哪个 SSH 版本。 (切记，客户端应用程序和 NetScreen 设备上的服务器必须运行相同的 SSH 版本。) 如果在先前 ScreenOS 版本的 NetScreen 设备上启用了 SSH，则 SSHv1 将在您现在启用 SSH 时运行。要查看 NetScreen 设备上哪个 SSH 版本是活动的但却未启用，请输入 CLI **get ssh** 命令：

```
ns-> get ssh
SSH V1 is active
SSH is not enabled
SSH is not ready for connections
Maximum sessions: 8
Active sessions: 0
```

在以上所示的输出中， SSHv1 是活动的，并且会在启用 SSH 时运行。如要使用另一不同的 SSH 版本，请确保删除随先前版本创建的所有密钥。例如，要清除 SSHv1 密钥并使用 SSHv2，请输入以下 CLI 命令：

```
ns-> delete ssh device all
```

出现以下消息：

```
SSH disabled for vsys: 1
PKA key deleted from device: 0
Host keys deleted from device: 1
Execute the 'set ssh version v2' command to activate SSH v2 for the device
```

要使用 SSHv2，请输入以下 CLI 命令：

```
ns-> set ssh version v2
```

注意：设置 SSH 版本并不会在 NetScreen 设备上启用 SSH。

3. 如果不想将端口 22 (缺省端口) 用于 SSH 客户端连接，可以指定一个介于 1024 和 32767 之间的端口号[8]。

```
ns-> set admin ssh port 1024
```

4. 为根系统或虚拟系统启用 SSH。有关以每个 vsys 为基础启用和使用 SSH 的其它信息，请参阅第 21 页上的“SSH 和 Vsys”。

   为根系统启用 SSH:

```
ns-> set ssh enable
```

   要为 vsys 启用 SSH，需要先进入该 vsys，然后启用 SSH:

```
ns-> set vsys v1
ns(v1)-> set ssh enable
```

5. 在 SSH 客户端将要进行连接的接口上启用 SSH。

```
ns-> set interface manage ssh
```

6. 将 NetScreen 设备上生成的主机密钥分发给 SSH 客户端。有关详细信息，请参阅第 22 页上的 “主机密钥”。

8. 也可以使用 WebUI 来更改端口号，并在 Configuration > Admin > Management 页面上启用 SSHv2 和 SCP。

认证

管理员可通过两种认证方法之一使用 SSH 连接到 NetScreen 设备。

- **密码认证：**此方法供需要配置或监视 NetScreen 设备的管理员使用。 SSH 客户端发起与 NetScreen 设备的 SSH 连接。如果在接收连接请求的接口上启用了 SSH 管理功能， NetScreen 设备会向 SSH 客户端发信号，提示用户输入用户名和密码。 SSH 客户端获得此信息后将其发送到 NetScreen 设备，后者将该信息与 admin 用户帐户中的用户名和密码进行比较。如果它们匹配， NetScreen 设备即会认证该用户。如果它们不匹配， NetScreen 设备将拒绝连接请求。
- **公开密钥认证 (PKA):** 此方法增强了密码认证方法的安全性并允许运行自动脚本。通常， SSH 客户端不发送用户名和密码，而是发送用户名和公开 / 私有密钥对的公开密钥组件[9]。 NetScreen 设备将其与可绑定到 admin 的最多四个公开密钥进行比较。如果其中一个密钥匹配， NetScreen 设备即会认证该用户。如果其中没有任何一个匹配， NetScreen 设备将拒绝连接请求。

这两种认证方法都要求在 SSH 客户端登录前建立安全连接。 SSH 客户端与 NetScreen 设备建立 SSH 连接后，必须使用用户名和密码或用户名和公开密钥进行自我认证。

密码认证和 PKA 都要求在 NetScreen 设备上为 admin 用户创建一个帐户，然后在想要用来通过 SSH 连接管理 NetScreen 设备的接口上启用 SSH 管理功能。 (有关创建 admin 用户帐户的信息，请参阅第 46 页上的 “定义 Admin 用户”。) 密码认证方法不需要在 SSH 客户端上做进一步设置。

9. 支持的认证算法有用于 SSHv1 的 RSA 和用于 SSHv2 的 DSA。

另一方面，要为 PKA 作准备，必须首先执行以下任务：

1. 在 SSH 客户端上，使用密钥生成程序来生成公开和私有密钥对。(该密钥对或者是用于 SSHv1 的 RSA 或者是用于 SSHv2 的 DSA。有关详细信息，请参阅 SSH 客户端应用程序文档。)

   ***注意：**如果要使用 PKA 进行自动登录，则必须在 SSH 客户端加载一个代理程序，用以加密 PKA 公开 / 私有密钥对的私有密钥组件，以及在存储器中存放私有密钥的加密版本。*

2. 将公开密钥从本地 SSH 目录移动到 TFTP 服务器上的某个目录[10]，然后启动 TFTP 程序。
3. 登录到 NetScreen 设备，以便能通过 CLI 对其进行配置。
4. 要将公开密钥从 TFTP 服务器加载到 NetScreen 设备，请输入以下 CLI 命令之一：

   对于 SSHv1:

   ```
   exec ssh tftp pka-rsa [ username name ] file-name name_str ip-addr
        tftp_ip_addr
   ```

   对于 SSHv2:

   ```
   exec ssh tftp pka-dsa [ user-name name ] file-name name_str ip-addr
        tftp_ip_addr
   ```

   username 或 **user-name** 选项仅可用于根 admin，因此只有根 admin 才能将 RSA 密钥绑定到另一 admin。当您作为根 admin 或读 / 写 admin 只输入命令而没有输入用户名时，NetScreen 设备会将密钥绑定到您自己的 admin 帐户；也即，它会将密钥绑定到输入命令的 admin。

   ***注意：**对于每个 admin 用户， NetScreen 设备最多支持四个 PKA 公开密钥。*

10. 也可以将公开密钥文件的内容直接粘贴到 CLI 命令 **set ssh pka-rsa [username** *name_str* **] key** *key_str* (对于 SSHv1) 或 **set ssh pka-dsa [user-name** *name_str* **] key** *key_str* (对于 SSHv2) 中 (将其粘贴到变量 *key_str* 所示位置)，或者粘贴到 WebUI 的 Key 字段中 (Configuration > Admin > Administrators > SSH PKA)。但是， CLI 与 WebUI 有大小限制：公开密钥大小不能超过 512 位。通过 TFTP 加载密钥时，不存在此限制。

当管理员尝试在已启用 SSH 管理功能的接口上通过 SSH 登录时， NetScreen 设备首先检查该管理员是否绑定了公开密钥。如果是这样， NetScreen 设备将使用 PKA 认证该管理员。如果该管理员未绑定公开密钥， NetScreen 设备会提示输入用户名和密码。(您可以使用以下命令强制 admin 只使用 PKA 方法 : **set admin ssh password disable username** *name_str*。) 无论您想要管理员使用哪种认证方法，在您初次定义其帐户时，仍必须包括密码。不过当您以后为此用户绑定了公开密钥时，该密码将变得无关紧要。

SSH 和 Vsys

对于支持 vsys 的 NetScreen 设备，可以每个 vsys 为基础启用和配置 SSH。每个 vsys 都有自己的主机密钥 (参阅第 22 页上的 “主机密钥”)，并且为系统的 admin 维护和管理一个 PKA 密钥。

注意，最大 SSH 会话数为设备级限制，介于 2 到 24 之间，依具体设备而定。如果登录到设备的 SSH 客户端数已达到最大，其它 SSH 客户端便无法再登录到该 SSH 服务器。根系统和 vsys 共享同一 SSH 端口号。这意味着 : 如果更改了 SSH 端口的缺省端口号 22，所有 vsys 的 SSH 端口也会随之更改。

主机密钥

主机密钥允许 NetScreen 设备向 SSH 客户端进行自我标识。在支持虚拟系统 (vsys) 的 NetScreen 设备上，每个 vsys 都有自己的主机密钥。在 vsys (对于支持 vsys 的设备) 或在 NetScreen 设备上首次启用 SSH 时，会生成对于该 vsys 或设备唯一的主机密钥。该主机密钥被永久绑定到该 vsys 或设备，并且如果在禁用了 SSH 后再次启用 SSH，仍将使用同一主机密钥。

必须以下面两种方式之一将 NetScreen 设备上的主机密钥分发给 SSH 客户端 :

- 手动 — 根 admin 或 vsys admin 通过电子邮件、电话等将主机密钥发送给客户端 admin 用户。接收的 admin 将主机密钥存储到 SSH 客户端系统的相应 SSH 文件中。 (SSH 客户端应用程序确定文件位置和格式。)
- 自动 — 当 SSH 客户端连接到 NetScreen 设备时，SSH 服务器将主机密钥的未加密公开组件发送给客户端。SSH 客户端搜索其本地主机密钥数据库，查看所收到的主机密钥是否已映射到 NetScreen 设备的地址。如果主机密钥未知 (在客户端的主机密钥数据库中没有到 NetScreen 设备地址的映射)，则 admin 用户可以决定是否接受该主机密钥。否则会终止连接。 (有关接受未知主机密钥的信息，请参阅相应的 SSH 客户端文档。)

为了检验 SSH 客户端是否已收到正确的主机密钥，客户端系统上的 admin 用户可以对所收到的主机密钥进行 SHA 散列处理。然后，客户端 admin 用户可以将此 SHA 散列信息与 NetScreen 设备上主机密钥的 SHA 散列信息进行比较。在 NetScreen 设备上，可以通过执行 CLI 命令 **get ssh host-key** 来显示主机密钥的 SHA 散列信息。

范例 : SSHv1 使用 PKA 进行自动登录

在此范例中，您 (作为根 admin) 将为运行自动脚本的远程主机设置 SSHv1 公开密钥认证 (PKA)。此远程主机访问 NetScreen 设备的唯一目的是每天晚上下载配置文件。由于自动进行认证，因此 SSH 客户端登录到 NetScreen 设备时无需人员干预。

定义一个名为 cfg 的 admin 用户帐户，其密码为 cfg 且具有读写权限。在绑定到 Untrust 区段的接口 ethernet1 上启用 SSH 管理功能。

如前所述，在 SSH 客户端上使用密钥生成程序生成一个 RSA 公开 / 私有密钥对，将文件名为 “idnt_cfg.pub” 的公开密钥文件移动到 TFTP 服务器上的某个目录，然后启动 TFTP 程序。 TFTP 服务器的 IP 地址是 10.1.1.5。

WebUI

Configuration > Admin > Administrators > New: 输入以下内容，然后单击 **OK**:

Name: cfg

New Password: cfg

Confirm Password: cfg

Privileges: Read-Write (选择)

SSH Password Authentication: (选择)

Network > Interfaces > Edit (对于 ethernet1): 在 Service Options 中选择 **SSH**，然后单击 **OK**。

> ***注意 :*** *仅可通过* ***exec ssh*** *命令从 TFTP 服务器加载 SSH 的公开密钥文件。*

CLI

```
set admin user cfg password cfg privilege all
set interface ethernet1 manage ssh
exec ssh tftp pka-rsa username cfg file-name idnt_cfg.pub ip-addr 10.1.1.5
save
```

安全复制 (SCP)

通过 “安全复制” (SCP) 可以使用 SSH 协议在远程客户端与 NetScreen 设备间传输文件。(SSH 协议向 SCP 连接提供认证、加密和数据完整性。) NetScreen 设备作为 SCP 服务器，接受来自远程主机上 SCP 客户端的连接。

SCP 要求在开始文件传输之前对远程客户端进行认证。 SCP 认证过程与用于认证 SSH 客户端的过程完全相同。可以用密码或 PKA 密钥来认证 SCP 客户端。一旦 SCP 客户端经过认证，便可在它与 NetScreen 设备间传输一个或多个文件。 SCP 客户端应用程序会确定用于指定源和目标文件名的确切方法；请参阅 SCP 客户端应用程序文档。

在 NetScreen 设备上，缺省情况下禁用 SCP。要启用 SCP，必须同时启用 SSH。

WebUI

Configuration > Admin > Management: 选择以下内容，然后单击 **Apply**:

Enable SSH: (选择)

Enable SCP: (选择)

CLI

```
set ssh enable
set scp enable
save
```

以下是一个 SCP 客户端命令的范例，该命令将配置文件从 NetScreen 设备 (管理员名称是 “netscreen”， IP 地址是 10.1.1.1) 的闪存中复制为客户端系统上的 “ns_sys_config_backup” 文件 :

```
scp netscreen@10.1.1.1:ns_sys_config ns_sys_config_backup
```

也可以向 NetScreen 设备或从中复制 ScreenOS 映像。要从 SCP 客户端将名为 “ns.5.1.0r1” 的映像保存到 NetScreen 设备，请输入以下 SCP 客户端命令 (其中，管理员的登录名为 “netscreen”， NetScreen 设备的 IP 地址为 10.1.1.1):

```
scp ns.5.1.0r1 netscreen@10.1.1.1:image
```

然后输入 **reset** 命令，重启要加载和运行新 ScreenOS 映像的 NetScreen 设备。

要将 ScreenOS 映像从 NetScreen 设备复制到 SCP 客户端并以名称 “current_image_backup” 保存该映像，请输入以下 SCP 客户端命令 :

```
scp netscreen@10.1.1.1:image current_image_backup
```

您需要查阅 SCP 客户端应用程序文档，以了解如何指定管理员名称、设备 IP 地址、源文件和目标文件。

串行控制台

可通过经由控制台端口从管理员工作站到 NetScreen 设备的直接串行连接来管理 NetScreen 设备。虽然直接连接并不总是可行，但只要 NetScreen 设备周围是安全的，这种连接就是最安全的设备管理方法。

注意：*为防止未授权用户以根 admin 身份远程登录，可以要求根 admin 只通过控制台登录到 NetScreen 设备。有关此限制的附加信息，请参阅第 57 页上的 “限制根 Admin 通过控制台访问”。*

根据 NetScreen 设备型号，创建串行连接需要以下电缆之一 :

- 阴性 DB-9 到阳性 DB-25 直通串行电缆
- 阴性 DB-9 到阳性 DB-9 直通串行电缆
- 阴性 DB-9 到阳性 MiniDIN-8 串行电缆
- 与附带 RJ-45 到 RJ-45 直通以太网电缆的 RJ-45 适配器相连的阴性 DB-9 电缆

还需要在管理工作站上安装“超级终端”软件 (或另一种 VT100 终端仿真器)，其中“超级终端”端口设置配置如下 :

- 串行通信 9600 bps
- 8 位
- 无奇偶校验
- 1 个停止位
- 无流量控制

注意 : *有关使用“超级终端”的详细信息，请参阅* NetScreen CLI Reference Guide *的“Getting Started”一章或任一安装指南的“Initial Configuration”一章。*

调制解调器端口

通过将管理员工作站连接到 NetScreen 设备的调制解调器端口，也可以管理该设备。调制解调器端口的功能与控制台端口类似，只是您不能为调制解调器端口定义参数或使用这种连接来上载图像。

为防止未授权用户通过直接连接控制台或调制解调器端口来管理设备，可以输入下列命令来禁用这两个端口 :

```
set console disable
set console aux disable
```

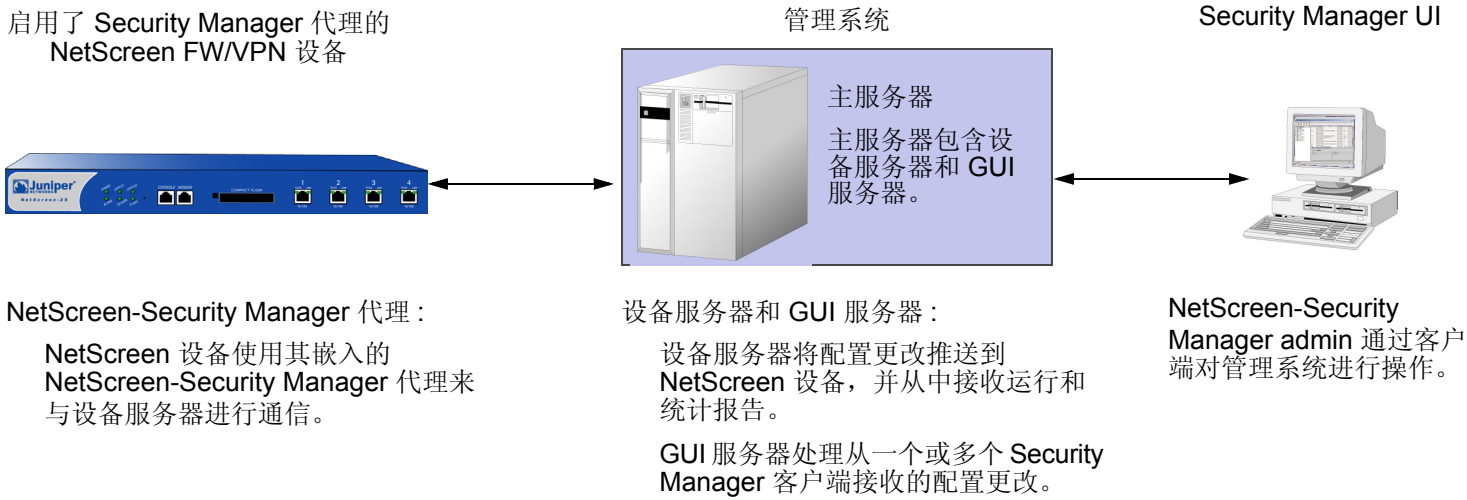
注意 : *在 NetScreen-5XT 上，只能使用调制解调器端口连接到外部调制解调器。*

通过 NETSCREEN-SECURITY MANAGER 进行管理

NetScreen-Security Manager 是一个企业级管理应用程序，用于在 LAN 或 WAN 环境中配置和监视多个设备。Security Manager UI 使管理员能从中心位置部署、配置和管理许多设备。

NetScreen-Security Manager 通过两个组件与 NetScreen 设备实现远程通信。

- *管理系统*，驻留在外部主机上的一组服务。这些服务处理、跟踪和存储设备与 Security Manager UI 之间交换的设备管理信息。
- *代理*，驻留在每个被管理 NetScreen 设备上的一种服务。“代理”从外部 “管理系统”接收配置参数，并将其推送至 NetScreen ScreenOS。“代理”还会监视设备并将报告回传给 “管理系统”。“代理”可以下载签名包、证书以及 NetScreen 设备与 NetScreen-Security Manager 之间的各项权利。



有关这些组件及其它 NetScreen-Security Manager 组件的详细信息，请参阅 *NetScreen-Security Manager 2004 Administrator's Guide*。

在代理与管理系统之间建立初始连接

必须先在 “代理” (驻留在设备上) 与 “管理系统” (驻留在外部主机上) 之间建立初始通信， NetScreen-Security Manager 方可访问和管理 NetScreen 设备。根据 NetScreen 设备的当前可用性，初始化最多可能需要两个用户分别位于两个不同站点。这些用户可能包括 *Security Manager 管理员*以及*现场用户*，前者使用客户端主机上的 Security Manager UI，后者通过控制台会话在 NetScreen 设备上执行 CLI 命令。可能的初始化情况如下。

- 情况 1: 设备已有已知 IP 地址，并且通过网络基础结构可以访问到该设备。

  在这种情况下，Security Manager 管理员使用客户端主机上的 Security Manager UI 添加该设备。(不需要现场用户。) NetScreen 设备自动连回到 “管理系统”，并准备向驻留在那里的 NetScreen-Security Manager 数据库发送配置信息。

- 情况 2: 访问不到 IP 地址。

  在这种情况下，两个用户都执行初始化任务。管理员通过 Security Manager UI 添加该设备。管理员还要确定现场用户需要哪些 CLI 命令，并将这些命令发送给该用户，然后该用户通过控制台执行这些命令。该设备自动与 “管理系统” 连接，并准备向 NetScreen-Security Manager 数据库发送配置信息。

- 情况 3: 该设备是新装置且包含出厂缺省设置。

  在这种情况下，两个用户都执行初始化任务。现场用户可以使用名为 *Configlet* 的加密配置脚本，该脚本由 Security Manager 管理员生成。过程如下 :

  a. Security Manager 管理员使用 Security Manager UI 中的 Add Device 向导选择设备平台和 NetScreen ScreenOS 版本。

  b. 管理员编辑该设备并输入所需的任何配置。

  c. 管理员激活该设备。

  d. 管理员生成并传送 Configlet 文件 (或者象情况 2 中那样，传送必要的 CLI 命令) 给现场用户。

  e. 现场用户执行 Configlet (或 CLI 命令)。

有关详细信息，请参阅 *NetScreen-Security Manager 2004 Administrator's Guide* 中的 “Adding Devices”。

启用、禁用和取消设置代理

必须先启用驻留在 NetScreen 设备上的 “代理”，该设备方可与 “管理系统”进行通信。

如果要取消设置 NetScreen-Security Manager，请使用 **unset nsmgmt all** 命令。此命令将代理设置成其初始缺省值，这样代理就像是从未连接到 NetScreen-Security Manager 一样。当您想要重新配置 NetScreen-Security Manager 设置时，可使用 unset nsmgmt all 命令。

要启用 NetScreen 设备上的 “代理”，请执行以下任一操作：

WebUI

Configuration > Admin > NSM: 选择 **Enable Communication with NetScreen Security Manager (NSM)**，然后单击 **Apply**。

CLI

```
set nsmgt enable
save
```

要禁用 NetScreen 设备上的 “代理”，请执行以下任一操作：

WebUI

Configuration > Admin > NSM: 清除 **Enable Communication with NetScreen Security Manager (NSM)**，然后单击 **Apply**。

CLI

```
unset nsmgt enable
save
```

更改管理系统服务器地址

“代理”用于标识外部 “管理系统”服务器的 IP 地址是一个可配置参数。

范例 : 设置主服务器 IP 地址

在下例中，将主服务器 IP 地址设置为 1.1.1.100。

WebUI

Configuration > Admin > NSM: 输入以下内容，然后单击 **Apply**:

Primary IP Address/Name: 1.1.1.100

CLI

```
set nsmgmt server primary 1.1.1.100
save
```

设置报告参数

“代理”监视 NetScreen 设备事件并将报告回传给 “管理系统”。这样就允许 Security Manager 管理员从 Security Manager UI 查看事件。

“代理”所跟踪的事件类别如下：

- *警报* 报告潜在危险攻击或流量异常，包括通过深入检查而检测到的攻击。
- *日志事件* 报告设备配置变化以及设备上出现的非严重变化。
- *协议散布* 事件报告由下列协议产生的消息：
  - AH (认证报头)
  - ESP (封装安全性负荷)
  - GRE (通用路由封装)
  - ICMP (互联网控制消息协议)
  - OSPF (开放最短路径优先)
  - TCP (传输控制协议)
  - UDP (用户数据报协议)
- *统计* 消息报告以下统计信息：
  - 攻击统计信息
  - 以太网统计信息
  - 通信流量统计信息
  - 策略统计信息

范例：启用警报和统计信息报告

在下例中，启用向 “管理系统”传送所有警报和统计消息。

WebUI

Configuration > Admin > NSM: 输入以下内容，然后单击 **Apply**:

Attack Statistics: (选择)

Policy Statistics: (选择)

Attack Alarms: (选择)

Traffic Alarms: (选择)

Flow Statistics: (选择)

Ethernet Statistics: (选择)

Deep Inspection Alarms: (选择)

Event Alarms: (选择)

CLI

```
set nsmgmt report statistics attack enable
set nsmgmt report statistics policy enable
set nsmgmt report alarm attack enable
set nsmgmt report alarm traffic enable
set nsmgmt report statistics flow enable
set nsmgmt report statistics ethernet enable
set nsmgmt report alarm idp enable
set nsmgmt report alarm other enable
save
```

配置同步

如果 NetScreen ScreenOS 配置自上次与 NetScreen-Security Manager 同步后发生了变化，则 NetScreen 设备会将该变化通知 NetScreen-Security Manager 管理员。例如，当设备管理员使用控制台、 telnet、 SSH 或 Web UI 更改 NetScreen 设备配置时， NetScreen 设备会发送消息。使用 NetScreen-Security Manager 以外的任何应用程序更改配置都会造成配置不同步。 NetScreen-Security Manager 配置文件必须与 NetScreen 设备配置文件同步，才能使 NetScreen-Security Manager 正常工作。将配置文件导入到 NetScreen-Security Manager 后，同步即告完成。有关导入设备的详细信息，请参阅 *Juniper Networks NetScreen-Security Administrator's Guide*。

下例显示用于查看配置状态的命令。

范例：查看配置状态

在下例中，将查看 NetScreen 设备的配置同步状态。

WebUI

***注意：**必须使用 CLI 来检索运行配置状态。*

CLI

```
get config nsmgmt-dirty
```

***注意：**如果非 NetScreen-Security Manager 应用程序未曾更改配置文件，则命令返回空白，否则返回 "yes"。*

范例：检索配置散列信息

NetScreen-Security Manager 使用配置散列信息来检验 NetScreen 设备的配置同步。在下例中，将检索特定虚拟系统的运行配置散列信息：

WebUI

> ***注意：****必须使用 CLI 来检索运行配置散列信息。*

CLI

```
ns-> enter vsys vsys1
ns(vsys1)-> get config hash
a26a16cd6b8ef40dc79d5b2ec9e1ab4f
ns(vsys1)->
ns(vsys1)-> exit
```

配置时戳

IA NetScreen 设备提供两种配置时戳：运行配置和保存配置。运行配置时戳是指上次对每个虚拟系统执行设置命令或取消设置命令的时间。保存配置时戳是指上次保存设备配置的时间。

范例：检索配置时戳

在下例中， NetScreen 设备将检索 vsys1 虚拟系统上次的运行和保存配置时戳：

WebUI

注意： *必须使用 CLI 来检索运行和保存配置时戳。*

CLI

```
get config timestamp vsys vsys1
get config saved timestamp
```

注意： *如果在命令中省略* ***vsys vsys_name****， NetScreen 设备会检索根系统的配置时戳。如果时戳不可用，则显示“未知”消息。*

控制管理信息流

ScreenOS 为配置和管理 NetScreen 设备提供了下列选项：

- **WebUI:** 选择此选项将允许接口通过 Web 用户界面 (WebUI) 接收 HTTP 管理信息流。
- **Telnet:** 作为互联网等 TCP/IP 网络的终端仿真程序，Telnet 是远程控制网络设备常用的方式。选择此选项可启用 Telnet 管理功能。
- **SSH:** 可使用“安全命令外壳”(SSH) 通过以太网连接或拨号调制解调器管理 NetScreen 设备。必须具有与 SSH 协议版本 1.5 兼容的 SSH 客户端。这些客户端适用于 Windows 95 及更高版本、Windows NT、Linux 和 UNIX。 NetScreen 设备通过其内置的 SSH 服务器与 SSH 客户端通信，该服务器提供设备配置与管理服务。选择此选项可启用 SSH 管理功能。
- **SNMP:** NetScreen 设备同时支持 SNMPv1 和 SNMPv2c 以及 RFC-1213 中定义的所有相关“管理信息库 II”(MIB II) 组。选择此选项可启用 SNMP 管理功能。
- **SSL:** 选择此选项将允许接口通过 WebUI 接收 NetScreen 设备的 HTTPS 安全管理信息流。
- **NS Security Manager:** 选择此选项将允许接口接收 NetScreen-Security Manager 信息流。
- **Ping:** 选择此选项将允许 NetScreen 设备响应 ICMP 回应请求 (或称 ping)，以确定是否可以通过网络访问特定的 IP 地址。
- **Ident-Reset:** 与 “邮件”或 FTP 发送标识请求相类似的服务。如果它们未收到确认，会再次发送请求。处理请求期间禁止用户访问。启用 Ident-reset 选项后， NetScreen 设备将发送 TCP 重置通知以响应发往端口 113 的 IDENT 请求，然后恢复因未确认标识请求而被阻止的访问。

要使用这些选项，可根据安全和管理需要在一个或多个接口中启用它们。

MGT 和 VLAN1 接口

某些 NetScreen 设备具有一个物理管理接口 (MGT)，专门用于管理信息流。当接口处于 NAT、“路由”或 “透明”模式时，可使用此接口管理信息流。

在 “透明”模式下，可将所有 NetScreen 设备配置成允许通过逻辑接口 VLAN1 进行管理。为使管理信息流能够到达 VLAN1 接口，必须同时在 VLAN1 和第 2 层区段 (V1-Trust、V1-Untrust、V1-DMZ、用户定义的第 2 层区段) 上启用所需的管理选项，管理信息流将经过这些区段到达 VLAN1。

为保持最高级别的安全性， Juniper Networks 建议您将管理信息流专门限制到 VLAN1 或 MGT 接口，而将用户信息流限制到安全区接口。将管理信息流与网络用户信息流分离可大大增加管理安全性并确保稳定的管理带宽。

范例 : 通过 MGT 接口进行管理

在本例中，将 MGT 接口的 IP 地址设置为 10.1.1.2/24，并使 MGT 接口能够接收 Web 和 SSH 管理信息流。

WebUI

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

IP Address/Netmask: 10.1.1.2/24

Management Services: WebUI, SSH: (选择)

CLI

```
set interface mgt ip 10.1.1.2/24
set interface mgt manage web
set interface mgt manage ssh
save
```

范例 : 通过 VLAN1 接口进行管理

在本例中，将 VLAN1 接口的 IP 地址设置为 10.1.1.2/24，并使 VLAN1 接口能够通过 V1-Trust 区段接收 Telnet 和 Web 管理信息流。

WebUI

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

IP Address/Netmask: 10.1.1.1/24

Management Services: WebUI, Telnet: (选择)

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

Management Services: WebUI, Telnet: (选择)

CLI

```
set interface vlan1 ip 10.1.1.1/24
set interface vlan1 manage web
set interface vlan1 manage telnet
set zone v1-trust manage web
set zone v1-trust manage telnet
save
```

管理接口

在具有多个网络信息流物理接口而没有 MGT 接口的 NetScreen 设备上，可以将一个物理接口专用于管理，从而将管理信息流与网络用户信息流完全分离。例如，可通过绑定到 Trust 区段的接口对设备进行本地管理访问，通过绑定到 Untrust 区段的接口进行远程管理。

范例：设置管理接口选项

在本例中，将 ethernet1 绑定到 Trust 区段，将 ethernet3 绑定到 Untrust 区段。为 ethernet1 分配 IP 地址 10.1.1.1/24 以及管理 IP 地址 10.1.1.2。(请注意，管理 IP 地址必须与安全区段接口 IP 地址位于同一子网中。) 还要允许 ethernet 1 接收 Web 和 Telnet 信息流。然后为 ethernet3 分配 IP 地址 1.1.1.1/24，并阻止所有管理信息流去往该接口。

WebUI

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Manage IP: 10.1.1.2

Management Services:

WebUI: (选择)

SNMP: (清除)

Telnet: (选择)

SSL: (清除)

SSH: (清除)

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Management Services:

WebUI: (清除)

SNMP: (清除)

Telnet: (清除)

SSL: (清除)

SSH: (清除)

CLI

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 manage-ip 10.1.1.2
set interface ethernet1 manage web
unset interface ethernet1 manage snmp
set interface ethernet1 manage telnet
unset interface ethernet1 manage ssl
unset interface ethernet1 manage ssh
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24[11]
save
```

11. 将接口绑定到 Trust 和 V1-Trust 区段以外的任何安全区段后，在缺省情况下会禁用所有管理选项。因此，在本例中，不必禁用 ethernet3 上的管理选项。

管理 IP

绑定到安全区段的任何物理、冗余或聚合接口或子接口都可拥有至少两个 IP 地址：

- 一个用于连接到网络的接口 IP 地址。
- 一个用于接收管理信息流的逻辑管理 IP 地址。

当 NetScreen 设备为“高可用性”(HA) 冗余组中的备份单元时，可通过该单元的管理 IP 地址 (一个或多个地址) 对其进行访问和配置。

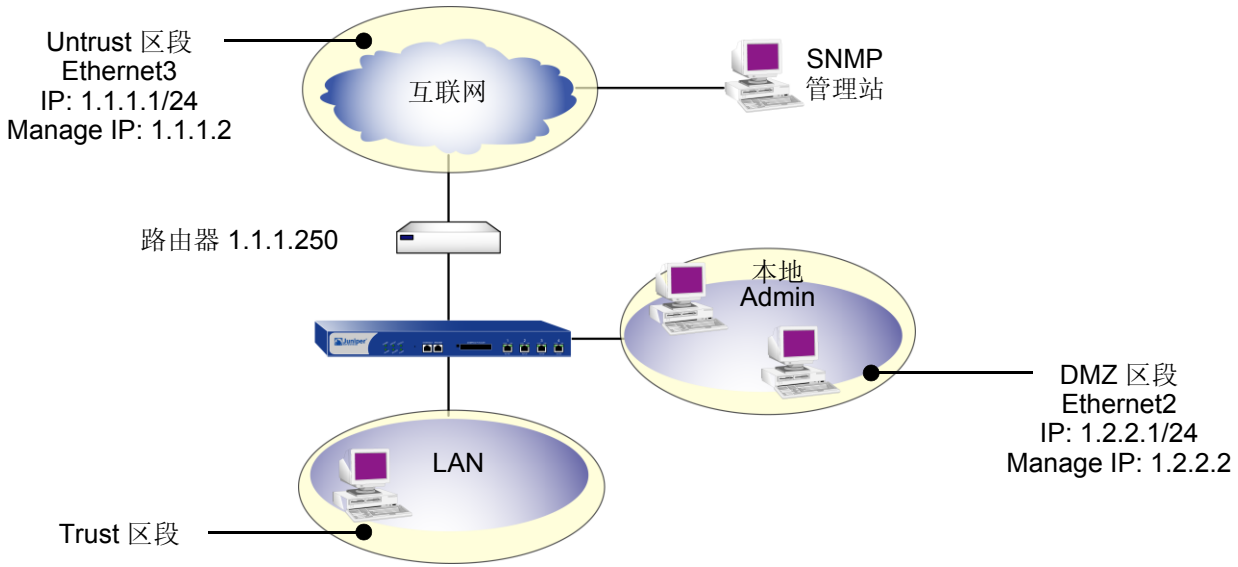
注意：*管理 IP 地址在以下两个方面不同于 VLAN1 地址：*

- *当 NetScreen 设备处于“透明”模式时，VLAN1 IP 地址可以是 VPN 通道的端点，但管理 IP 地址则不能。*
- *可以定义多个管理 IP 地址，每个网络接口一个，但只能定义一个 VLAN1 IP 地址，该地址用于整个系统。*

如果在 WebUI 的接口配置页上选择 Manageable 选项，则可通过接口 IP 地址或与该接口关联的管理 IP 地址来管理 NetScreen 设备。

范例：设置多个接口的管理 IP

在本例中，将 ethernet2 绑定到 DMZ 区段，将 ethernet3 绑定到 Untrust 区段。在每个接口上设置管理选项，以提供对特定种类管理信息流的访问。允许 DMZ 区段中的一组本地管理员在 ethernet2 上进行 HTTP 和 Telnet 访问，允许在 ethernet3 上进行 SNMP 访问以便从远程站点对中央设备进行监视。 Ethernet2 和 ethernet3 各有一个管理 IP 地址，管理信息流将被引向该地址。还要设置一条路由，将自行生成的 SNMP 信息流引到 ethernet3 外面 1.1.1.250 处的外部路由器。



WebUI

Network > Interfaces > Edit (ethernet2): 输入以下内容，然后单击 **OK**:

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

Manage IP: 1.2.2.2

Management Services:

WebUI: (选择)

Telnet: (选择)

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

Management Services:

SNMP: (选择)

CLI

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24
set interface ethernet2 manage-ip 1.2.2.2
set interface ethernet2 manage web
set interface ethernet2 manage telnet

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage-ip 1.1.1.2
set interface ethernet3 manage snmp
save
```

管理级别

NetScreen 设备支持多个管理用户。对于管理员所作的任何配置更改， NetScreen 设备都会记录以下信息：

- 进行更改的管理员的姓名
- 从中进行更改的 IP 地址
- 更改时间

存在若干管理用户级别。其中某些级别的可用性取决于 NetScreen 设备的型号。以下各部分列出了所有 admin 级别以及各级别的权限。 admin 只有在使用有效的用户名和密码成功登录之后才可行使这些权限。

根管理员

根管理员具有完全管理权限。每个 NetScreen 设备只有一个根管理员。根管理员具有以下权限：

- 管理 NetScreen 设备的根系统
- 添加、删除和管理其他所有管理员
- 建立和管理虚拟系统并为其分配物理或逻辑接口
- 创建、删除和管理虚拟路由器 (VR)
- 添加、删除和管理安全区段
- 为安全区段分配接口
- 执行资源恢复
- 将设备设置为 FIPS 模式
- 将设备重置为其缺省设置
- 更新固件
- 加载配置文件
- 清除指定 admin 或所有活动 admin 的全部活动会话

可读 / 写管理员

可读/写管理员与根管理员具有相同的权限，但不能创建、修改或删除其他 admin 用户。可读/写管理员具有以下权限：

- 创建虚拟系统并为每个系统分配一个虚拟系统管理员
- 监视任何虚拟系统
- 跟踪统计 (不能将该权限委派给虚拟系统管理员)

只读管理员

只读管理员只具有使用 WebUI 进行查看的权限，并且只能发出 **get** 和 **ping** CLI 命令。只读管理员具有以下权限：

- 根系统中的只读权限，可使用以下四种命令：**enter**、 **exit**、 **get** 和 **ping**
- 虚拟系统中的只读权限

虚拟系统管理员

某些 NetScreen 设备支持虚拟系统。每个虚拟系统 (vsys) 都是一个唯一的安全域，具有仅适用于该 vsys 的权限的虚拟系统管理员可以对其进行管理。虚拟系统管理员通过 CLI 或 WebUI 独立对虚拟系统进行管理。在每个 vsys 上，虚拟系统管理员具有以下权限：

- 创建和编辑 auth、 IKE、 L2TP、 Xauth 以及 “手动密钥” 用户
- 创建和编辑服务
- 创建和编辑策略
- 创建和编辑地址
- 创建和编辑 VPN
- 修改虚拟系统管理员登录密码
- 创建和管理安全区段
- 添加和删除虚拟系统只读管理员

虚拟系统只读管理员

虚拟系统只读管理员与只读管理员具有同一组权限，但仅限于特定虚拟系统范围内。虚拟系统只读管理员针对其具体的 vsys 具有通过 WebUI 进行查看的权限，并且只能在其 vsys 内发出 **enter**、 **exit**、 **get** 和 **ping** CLI 命令。

注意：*有关虚拟系统的详细信息，请参阅第* ***9-1*** *页上的 “虚拟系统”。*

定义 Admin 用户

根管理员是唯一可以创建、修改和删除 admin 用户的管理员。在下例中，执行该过程的管理员必须为根管理员。

范例 : 添加只读 Admin

在本例中，您将作为根 admin 添加一个名为 Roger 且密码为 2bd21wG7 的只读管理员。

WebUI

Configuration > Admin > Administrators > New: 输入以下内容，然后单击 **OK**:

Name: Roger

New Password: 2bd21wG7[12]

Confirm New Password: 2bd21wG7

Privileges: Read-Only (选择)

CLI

```
set admin user Roger password 2bd21wG7 privilege read-only
save
```

12. 密码最长可为 31 个字符且区分大小写。

范例：修改 Admin

在本例中，您作为根 admin 将 Roger 的权限由只读更改为可读 / 写。

WebUI

Configuration > Admin > Administrators > Edit (对于 Roger): 输入以下内容，然后单击 **OK**:

Name: Roger

New Password: 2bd21wG7

Confirm New Password: 2bd21wG7

Privileges: Read-Write (选择)

CLI

```
unset admin user Roger
set admin user Roger password 2bd21wG7 privilege all
save
```

范例：删除 Admin

在本例中，您将作为根 admin 删除 admin 用户 Roger。

WebUI

Configuration > Admin > Administrators: 在 Roger 对应的 Configure 栏中单击 **Remove**。

CLI

```
unset admin user Roger
save
```

范例：清除 Admin 的会话

在本例中，您将作为根 admin 终止 admin 用户 Roger 的所有活动会话。执行以下命令时， NetScreen 设备会关闭所有活动会话并自动从系统中注销 Roger。

WebUI

> ***注意：****必须使用 CLI 来清除 admin 的会话。*

CLI

```
clear admin name Roger
save
```

保障管理信息流安全

要在设置期间保障 NetScreen 设备安全，请执行以下步骤：

1. 在 Web 界面中更改管理端口。

   请参阅第 50 页上的 “更改端口号”。

2. 更改用于进行管理访问的用户名和密码。

   请参阅第 51 页上的 “更改 Admin 登录名和密码”。

3. 为 admin 用户定义管理客户端 IP 地址。

   请参阅第 56 页上的 “限制管理访问”。

4. 关闭任何不必要的接口管理服务选项。

   请参阅第 36 页上的 “控制管理信息流”。

5. 禁用接口上的 ping 和 Ident-Reset 服务选项，两者都会响应未知方发起的请求，并且可能会暴露网络信息：

   ### *WebUI*

   Network > Interfaces > Edit (对于要编辑的接口): 禁用以下服务选项，然后单击 **OK**:

   Ping: 选择此选项将允许 NetScreen 设备响应 ICMP 回应请求 (或称 “ping”)，以确定是否可从该设备访问特定 IP 地址。

   Ident-Reset: 当诸如 “邮件” 或 FTP 等服务发送了标识请求而未收到确认时，会再次发送该请求。请求进行期间禁止用户访问。若启用了 Ident-Reset 复选框， NetScreen 设备会自动恢复用户访问。

   ### *CLI*

   ```
   unset interface interface manage ping
   unset interface interface manage ident-reset
   ```

更改端口号

更改 NetScreen 设备监听的 HTTP 管理信息流端口号可以提高安全性。缺省设置为端口 80，这是 HTTP 信息流的标准端口号。更改端口号后，在下次尝试联络 NetScreen 设备时，必须在 Web 浏览器的 URL 字段中键入新的端口号。(在下例中，管理员需要输入 http://188.30.12.2:15522。)

范例 : 更改端口号

在本例中，绑定到 Trust 区段的接口的 IP 地址为 10.1.1.1/24。要通过此接口上的 WebUI 管理 NetScreen 设备，必须使用 HTTP。要增加 HTTP 连接的安全性，要将 HTTP 端口号由 80 (缺省值) 改为 15522。

WebUI

Configuration > Admin > Management: 在 HTTP Port 字段中，键入 **15522**，然后单击 **Apply**。

CLI

```
set admin port 15522
save
```

更改 Admin 登录名和密码

在缺省情况下， NetScreen 设备的初始登录名为 **netscreen**。初始密码也为 **netscreen**。由于这些信息已被广泛公布， Juniper Networks 建议您立即更改登录名和密码。登录名和密码均区分大小写。它们可以包含除 ? 和 " 之外可从键盘输入的任何字符。妥善记录新的 admin 登录名和密码。

***警告：**请务必记录新的密码。如果忘记了密码，则必须将 NetScreen 设备重置为其出厂设置，并且所有配置内容都将丢失。有关详细信息，请参阅第 55 页上的 "重置设备到出厂缺省设置"。*

可使用内部数据库或外部 auth 服务器认证 NetScreen 设备的 admin 用户[13]。当 admin 用户登录到 NetScreen 设备时，它会首先检查本地内部数据库以进行认证。如果不存在任何条目并且连接了外部 auth 服务器，它会在外部 auth 服务器数据库中检查是否有匹配条目。admin 用户成功登录到外部 auth 服务器后， NetScreen 设备会在本地维护该 admin 的登录状态。

***注意：**有关 admin 用户级别的详细信息，请参阅第 44 页上的 "管理级别"。有关使用外部 auth 服务器的详细信息，请参阅第 **8**-20 页上的 "外部 Auth 服务器"。*

当根 admin 更改 admin 用户配置文件的任何属性 (如用户名、密码或权限) 时，该 admin 当前打开的任何管理会话会自动终止。如果根 admin 为自己更改了上述任何属性，或者根级可读 / 写 admin 或 vsys 可读 / 写 admin 更改了自己的密码，则除了该用户进行更改所处的会话外，其当前打开的所有 admin 会话[14] 都会终止。

13. NetScreen 支持通过 RADIUS、SecurID 和 LDAP 服务器进行 admin 用户认证。(有关详细信息，请参阅第 **8**-3 页上的 "Admin 用户"。) 尽管根 admin 帐户必须存储在本地数据库中，但是可以在外部 auth 服务器中存储根级读 / 写和根级只读 admin 用户。要在外部 auth 服务器上存储根级和 vsys 级 admin 用户并查询其权限，服务器必须是 RADIUS，并且必须在其上加载 netscreen.dct 文件。(请参阅第 **8**-25 页上的 "NetScreen 词典文件"。)

14. HTTP 或 HTTPS 会话使用 WebUI 的方式是不同的。由于 HTTP 不支持持久连接，因此一旦您对自己的用户配置文件作了更改，会自动将您从该会话和其它所有打开的会话中注销。

范例：更改 Admin 用户的登录名和密码

在本例中，您作为根 admin 将可读 / 写管理员的登录名由 “John” 改为 “Smith”，将其密码由 xL7s62a1 改为 3MAb99j2[15]。

***注意：**有关不同级别管理员的信息，请参阅第 44 页上的 “管理级别”。*

WebUI

Configuration > Admin > Administrators > Edit (对于 John): 输入以下内容，然后单击 **OK**:

Name: Smith

New Password: 3MAb99j2

Confirm New Password: 3MAb99j2

CLI

```
unset admin user John
set admin user Smith password 3MAb99j2 privilege all
save
```

15. 应避免使用实际词语作为密码，因为这样的密码在遭到词典式攻击时可能会被猜出或发现，可以使用由字母和数字组成的表面上随机的字符串。要创建这样的易记字符串，可编写一句话，然后使用每个词的首字母。例如，“Charles will be 6 years old on November 21” 变成 “Cwb6yooN21”。

范例 : 更改自己的密码

拥有读 / 写权限的 admin 用户可以更改其自己的管理员密码，但不能更改其登录名。在本例中，拥有读 / 写权限且登录名为 “Smith” 的管理员将其密码由 3MAb99j2 改为 ru494Vq5。

WebUI

Configuration > Admin > Administrators > Edit (对于首次输入): 输入以下内容，然后单击 **OK**:

Name: Smith

New Password: ru494Vq5

Confirm New Password: ru494Vq5

CLI

```
set admin password ru494Vq5
save
```

设置根 Admin 密码的最小长度

在一些公司中，某人最初可能将设备配置为根 admin，但以后由另一个人担任根 admin 角色并管理该设备。为了防止后来的根 admin 使用可能较易破译的短密码，最初的根 admin 可以对根 admin 的密码设置一个 1 到 31 之间的最小长度要求。

注意，仅当您是根 admin 并且您自己的密码满足欲设置的最小长度要求时，才能设置该最小密码长度。否则，NetScreen 设备会显示一条错误消息。

要为根 admin 的密码指定最小长度，请输入以下命令：

```
set admin password restrict length number
```

注意： *必须使用 CLI 来设置此限制。*

重置设备到出厂缺省设置

如果丢失了 admin 密码，可以使用下列步骤将 NetScreen 设备重置为其缺省设置。此时将会丢失配置内容，但会恢复设备访问。要执行此操作，需要建立控制台连接，在 *NetScreen CLI 参考指南* 和相应的安装指南中对此进行了详细描述。

***注意：**在缺省情况下，会启用设备恢复功能。可输入 **unset admin device-reset** 命令来禁用该功能。另外，如果 NetScreen 设备处于 FIPS 模式，会自动禁用恢复功能。*

1. 出现登录提示时，键入设备的序列号。
2. 出现密码提示时，再次键入该序列号。

   将显示以下消息：

   !!!! Lost Password Reset !!!! You have initiated a command to reset the device to factory defaults, clearing all current configuration, keys and settings. Would you like to continue? y/n

3. 按 **Y** 键。

   将显示以下消息：

   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory default configuration, which is: System IP: 192.168.1.1; username: netscreen; password: netscreen. Would you like to continue? y/n

4. 按 **Y** 键重置设备。

   现在即可使用 *netscreen* 作为缺省用户名和密码进行登录。

限制管理访问

可以从一个或多个子网地址管理 NetScreen 设备。在缺省情况下，受信接口上的任何主机都可管理 NetScreen 设备。要限制对特定工作站的管理能力，必须配置管理客户端 IP 地址。

注意：*所分配的管理客户端 IP 地址会立即生效。如果通过网络连接对设备进行管理而在分配时未包括您所在工作站，则 NetScreen 设备会立即终止当前会话，并且您将无法再从该工作站管理设备。*

范例：限制对单个工作站的管理

在本例中， IP 地址为 172.16.40.42 的工作站上的管理员是唯一被指定对 NetScreen 设备进行管理的管理员。

WebUI

Configuration > Admin > Permitted IPs: 输入以下内容，然后单击 **Add**:

IP Address / Netmask: 172.16.40.42/32

CLI

```
set admin manager-ip 172.16.40.42/32
save
```

范例 : 限制对子网的管理

在本例中，指定 172.16.40.0/24 子网中的一组工作站管理员对 NetScreen 设备进行管理。

WebUI

Configuration > Admin > Permitted Ips: 输入以下内容，然后单击 **Add**:

IP Address / Netmask: 172.16.40.0/24

CLI

```
set admin manager-ip 172.16.40.0 255.255.255.0
save
```

限制根 Admin 通过控制台访问

您还可以要求根 admin 只能通过控制台登录到 NetScreen 设备。此限制要求根 admin 实地接触要登录的设备，从而防止未授权用户以根 admin 身份远程登录。设置了此限制后，如果有人试图以根 admin 身份通过其它方式 (如 WebUI、 Telnet 或 SSH) 登录，则即使在进入接口上启用了这些管理选项，设备也会拒绝访问。

要将根 admin 限制为只能通过控制台进行访问，请输入下列命令 :

```
set admin root access console
```

注意 : *必须使用 CLI 来设置此限制。*

用于管理信息流的 VPN 通道

可以使用虚拟专用网 (VPN) 通道，保障从动态分配或固定 IP 地址对 NetScreen 设备进行远程管理的安全性。使用 VPN 通道可以保护任何种类的信息流，如 NetScreen-Security Manager、HTTP、Telnet 或 SSH。(有关创建 VPN 通道以保障 Security Manager 报告、系统日志报告或 SNMP 陷阱等自发信息流安全方面的信息，请参阅第 107 页上的 “自行生成的信息流的 VPN 通道”。)

NetScreen 支持两种类型的 VPN 通道配置 :

- **基于路由的 VPN**: NetScreen 设备使用路由表条目将信息流引向绑定到 VPN 通道的通道接口。 (有关详细信息，请参阅第 5 卷，“VPN”。)
- **基于策略的 VPN**: NetScreen 设备使用策略中明确提到的 VPN 通道名，引导信息流通过 VPN 通道。 (有关详细信息，请参阅第 5 卷，“VPN”。)

对于每种 VPN 通道配置类型，有以下各种类型的 VPN 通道 :

- **手动密钥** : 可以在通道两端手动设置定义 “安全联盟” (SA) 的三要素 : 安全参数索引 (SPI)、加密密钥和认证密钥。要更改 SA 中的任何元素，必须在通道两端手动将其输入。
- **具有预共享密钥的自动密钥 IKE**: 一个或两个预共享秘密 (一个用于认证，一个用于加密) 起着种子值的作用。 IKE 协议使用它们在通道两端生成一组对称密钥；也即，使用同一密钥进行加密和解密。这些密钥按预先定义的时间间隔自动重新生成。
- **具有证书的自动密钥 IKE**: 凭借 “公开密钥基础” (PKI)，通道两端的参与者使用一个数字证书 (用于认证) 和一个 RSA 公开 / 私有密钥对 (用于加密)。加密是不对称的。也即，密钥对中的一个用于加密，另一个用于解密。

> ***注意 :*** *有关 VPN 通道的完整说明，请参阅第 5 卷，“VPN”。有关 NetScreen-Remote 的详细信息，请参阅 NetScreen-Remote 用户指南。*

如果使用基于策略的 VPN 配置，必须用任一区段中某个接口的 IP 地址创建一个通讯簿条目，但不能是出接口所绑定的区段。然后可以在涉及该 VPN 通道的策略中将其用作源地址。此地址还用作远程 IPSec 对等方的端实体地址。如果使用的是基于路由的 VPN 配置，则无需这样的通讯簿条目。

范例 : 通过基于路由的手动密钥 VPN 通道进行管理

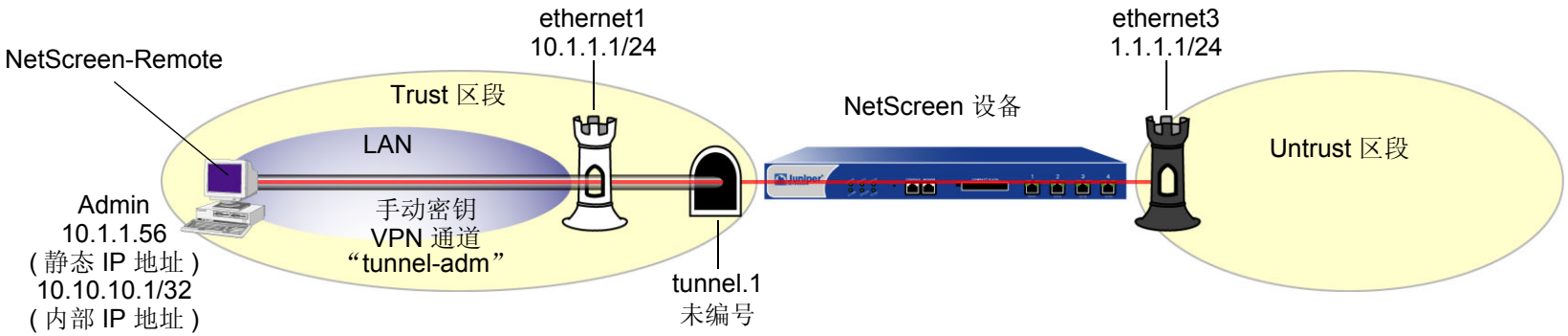
在本例中，将设立一个基于路由的手动密钥 VPN 通道以提供管理信息流的机密性。该通道从 admin 工作站 (地址为 10.1.1.56) 上运行的 NetScreen-Remote VPN 客户端延伸到 ethernet1 (10.1.1.1/24)。该 admin 的工作站和 ethernet1 都位于 Trust 区段中。将该通道命名为 “tunnel-adm”。创建一个未编号的通道接口，命名为 tunnel.1，并将其绑定到 Trust 区段和 VPN 通道 “tunnel-adm”。

NetScreen 设备使用 NetScreen-Remote 上配置的内部 IP 地址 (10.10.10.1) 作为对等方网关地址 10.1.1.56 之外目标的目的地址。定义一个通过 tunnel.1 去往 10.10.10.1/32 的路由。由于下面两个原因，策略并非必要 :

- 该 VPN 通道所保护的管理信息流终结于 NetScreen 设备本处，而不是经过该设备去往另一安全区段。
- 这是一个基于路由的 VPN，意味着路由查询 (而非策略查询) 会将目的地址链接到与相应 VPN 通道绑定的通道接口。

注意 : *可将本例与第 65 页上的 “范例 : 通过基于策略的手动密钥 VPN 通道进行管理” 进行比较。*

NetScreen-Remote 使用 ethernet3 的 IP 地址 (1.1.1.1) 作为 10.1.1.1 处远程网关之外目标的目的地址。NetScreen-Remote 配置将远程方 ID 类型指定为 “IP address”，将相应协议指定为 “All”。



WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: Tunnel.1

Zone (VR): Trust (trust-vr)

Unnumbered: (选择)

Interface: ethernet1(trust-vr)[16]

16. 该未编号通道接口借用指定安全区段接口的 IP 地址。

2. VPN

VPNs > Manual Key > New: 输入以下内容，然后单击 **OK**:

VPN Tunnel Name: tunnel-adm

Gateway IP: 10.1.1.56

Security Index (HEX Number): 5555 (Local) 5555 (Remote)

Outgoing Interface: ethernet1

ESP-CBC: (选择)

Encryption Algorithm: DES-CBC

Generate Key by Password[17] : netscreen1

Authentication Algorithm: MD5

Generate Key by Password: netscreen2

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Bind to Tunnel Interface: (选择)， Tunnel.1

3. 路由

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

Network Address/Netmask: 10.10.10.1/32

Gateway: (选择)

Interface: Tunnel.1

Gateway IP Address: 0.0.0.0

17. 由于 NetScreen-Remote 将密码处理成密钥，这一点与其它 NetScreen 产品不同，因此请在配置通道后执行如下操作 : (1) 返回 Manual Key Configuration 对话框 (在“tunnel-adm”相应的 Configure 栏中单击 **Edit**)； (2) 复制生成的十六进制密钥； (3) 在配置通道的 NetScreen-Remote 端时使用这些十六进制密钥。

CLI

1. 接口

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

set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone trust

set interface tunnel.1 ip unnumbered interface ethernet1[18]
```

2. VPN

```
set vpn tunnel-adm manual 5555 5555 gateway 10.1.1.56 outgoing ethernet1 esp
    des password netscreen1 auth md5 password netscreen2[19]
set vpn tunnel-adm bind interface tunnel.1
```

3. 路由

```
set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1
save
```

18. 该未编号通道接口借用指定安全区段接口的 IP 地址。

19. 由于 NetScreen-Remote 将密码处理成密钥，这一点与其它 NetScreen 产品不同，因此请在配置通道后执行如下操作：(1) 键入 **get vpn admin-tun**; (2) 复制由 “netscreen1” 和 “netscreen2” 生成的两个十六进制密钥；(3) 在配置通道的 NetScreen-Remote 端时使用这些十六进制密钥。

NetScreen-Remote 安全策略编辑器

1. 单击 **Options** > **Global Policy Settings**，选中 **Allow to Specify Internal Network Address** 复选框。
2. 单击 **Options > Secure > Specified Connections**。
3. 单击 **Add a new connection**，在出现的新连接图标旁键入 **Admin**。
4. 配置连接选项：

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 1.1.1.1

   Protocol: All

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 10.1.1.1

5. 单击 unix 图标左侧的加号，展开连接策略。
6. 单击 **My Identity**，在 Select Certificate 下拉列表中，选择 **None**，在 Internal Network IP Address 中，键入 **10.10.10.1**。
7. 单击 **Security Policy**，然后选择 **Use Manual Keys**。
8. 单击位于 Security Policy 图标左侧的加号，然后单击 Key Exchange (Phase 2) 左侧的加号，进一步展开策略。
9. 单击 **Proposal 1**，然后选择以下 IPSec 策略：

   Encapsulation Protocol (ESP): (选择)

   Encrypt Alg: DES

   Hash Alg: MD5

   Encapsulation: Tunnel

10. 单击 **Inbound Keys**，然后在 Security Parameters Index 字段中键入 **5555**。
11. 单击 **Enter Key**，输入以下内容[20]，然后单击 **OK**:

    Choose key format: Binary

    ESP Encryption Key: dccbee96c7e546bc

    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
12. 单击 **Outbound Keys**，然后在 Security Parameters Index 字段中键入 **5555**。
13. 单击 **Enter Key**，输入以下内容[20]，然后单击 **OK**:

    Choose key format: Binary

    ESP Encryption Key: dccbee96c7e546bc

    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
14. 单击 **Save**。

20. 它们是您在配置 NetScreen 设备后所复制的那两个生成密钥。

范例 : 通过基于策略的手动密钥 VPN 通道进行管理

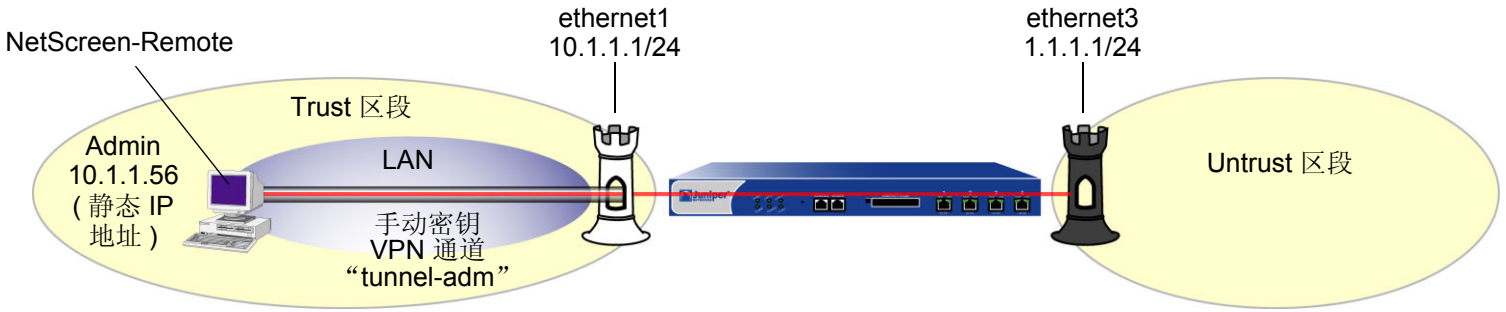
在本例中，将为管理信息流设立一个基于策略的手动密钥 VPN 通道。该通道从 admin 工作站 (地址为 10.1.1.56) 上运行的 NetScreen-Remote VPN 客户端延伸到 ethernet1 (10.1.1.1/24)。该 admin 的工作站和 ethernet1 都位于 Trust 区段中。将该通道命名为 “tunnel-adm” 并绑定到 Trust 区段。

NetScreen 设备使用 NetScreen-Remote 上配置的内部 IP 地址 (10.10.10.1) 作为对等方网关地址 10.1.1.56 之外目标的目的地址。定义指定 10.10.10.1/32 的 Trust 区段通讯簿条目，以及指定 ethernet3 IP 地址的 Untrust 区段通讯簿条目。尽管 ethernet3 接口的地址为 1.1.1.1/24，但您所创建的地址具有 32 位网络掩码 : 1.1.1.1/32. 在您所创建的涉及通道 “tunnel-adm” 的策略中使用此地址以及该 admin 的工作站内部地址。策略是必需的，因为这是一个基于策略的 VPN，意味着策略查询 (而非路由查询) 会将目的地址链接到相应的 VPN 通道。

还必须定义一个通过 ethernet1 去往 10.10.10.1/32 的路由。

> ***注意 :*** *可将本例与第 59 页上的 “范例 : 通过基于路由的手动密钥 VPN 通道进行管理” 进行比较。*

NetScreen-Remote 使用 IP 地址 1.1.1.1 作为 10.1.1.1 处远程网关之外目标的目的地址。NetScreen-Remote 通道配置将远程方 ID 类型指定为 IP 地址，将相应协议指定为 “All”。



WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: Untrust-IF

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.1/32

Zone: Untrust

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

Address Name: admin

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.10.1/32

Zone: Trust

3. VPN

VPNs > Manual Key > New: 输入以下内容，然后单击 **OK**:

VPN Tunnel Name: tunnel-adm

Gateway IP: 10.1.1.56

Security Index (HEX Number): 5555 (Local) 5555 (Remote)

Outgoing Interface: ethernet1

ESP-CBC: (选择)

Encryption Algorithm: DES-CBC

Generate Key by Password[21] : netscreen1

Authentication Algorithm: MD5

Generate Key by Password: netscreen2

4. 路由

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

Network Address/Netmask: 10.10.10.1/32

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

21. 由于 NetScreen-Remote 将密码处理成密钥，这一点与其它 NetScreen 产品不同，因此请在配置通道后执行如下操作：(1) 返回 Manual Key Configuration 对话框 (在“tunnel-adm”对应的 Configure 栏中单击 **Edit**)；(2) 复制生成的十六进制密钥；(3) 在配置通道的 NetScreen-Remote 端时使用这些十六进制密钥。

5. 策略

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

Source Address:

Address Book Entry: (选择), admin

Destination Address:

Address Book Entry: (选择), Untrust-IF

Service: Any

Action: Tunnel

Tunnel:

VPN: tunnel-adm

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

CLI

1. 接口

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

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

2. 地址

```
set address trust admin 10.10.10.1/32
set address untrust Untrust-IF 1.1.1.1/32
```

3. VPN

```
set vpn tunnel-adm manual 5555 5555 gateway 10.1.1.56 outgoing ethernet1 esp
    des password netscreen1 auth md5 password netscreen2[22]
```

4. 路由

```
set vrouter trust-vr route 10.10.10.1/32 interface ethernet1
```

5. 策略

```
set policy top from trust to untrust admin Untrust-IF any tunnel vpn tunnel-adm
set policy top from untrust to trust Untrust-IF admin any tunnel vpn tunnel-adm
save
```

22. 由于 NetScreen-Remote 将密码处理成密钥，这一点与其它 NetScreen 产品不同，因此请在配置通道后执行如下操作：(1) 键入 **get vpn admin-tun**; (2) 复制由 “netscreen1” 和 “netscreen2” 生成的两个十六进制密钥；(3) 在配置通道的 NetScreen-Remote 端时使用这些十六进制密钥。

NetScreen-Remote 安全策略编辑器

1. 单击 **Options > Secure > Specified Connections**。
2. 单击 **Add a new connection**，在出现的新连接图标旁键入 **Admin**。
3. 配置连接选项：

   Connection Security: Secure
   Remote Party Identity and Addressing:
   ID Type: IP Address, 1.1.1.1
   Protocol: All
   Connect using Secure Gateway Tunnel: (选择)
   ID Type: IP Address, 10.1.1.1

4. 单击 unix 图标左侧的加号，展开连接策略。
5. 单击 **My Identity**，然后在 Select Certificate 下拉列表中选择 **None**。
6. 单击 **Security Policy**，然后选择 **Use Manual Keys**。
7. 单击位于 Security Policy 图标左侧的加号，然后单击 Key Exchange (Phase 2) 左侧的加号，进一步展开策略。
8. 单击 **Proposal 1**，然后选择以下 IPSec 策略：

   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: DES
   Hash Alg: MD5
   Encapsulation: Tunnel

9. 单击 **Inbound Keys**，然后在 Security Parameters Index 字段中键入 **5555**。
10. 单击 **Enter Key**，输入以下内容[23]，然后单击 **OK**:

    Choose key format: Binary

    ESP Encryption Key: dccbee96c7e546bc

    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
11. 单击 **Outbound Keys**，然后在 Security Parameters Index 字段中键入 **5555**。
12. 单击 **Enter Key**，输入以下内容[20]，然后单击 **OK**:

    Choose key format: Binary

    ESP Encryption Key: dccbee96c7e546bc

    ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
13. 单击 **Save**。

23. 它们是您在配置 NetScreen 设备后所复制的那两个生成密钥。

2

监控 NetScreen 设备

本章将论述以下有关监控 NetScreen 设备的主题：

存储日志信息

所有 NetScreen 设备都允许在内部 (在闪存中) 和外部 (在多个位置处) 存储事件和流量日志数据。尽管在内部存储日志信息很方便，但存储器容量有限。当内部存储器空间完全填满时， NetScreen 设备就开始用最新的日志条目覆盖最早的日志条目。如果在保存所记录的信息之前存在先进先出 (FIFO) 机制，就会丢失数据。为了减少这种数据丢失，可以将事件和流量日志存储到外部系统日志或 WebTrends 服务器中，或存储到 NetScreen-Global PRO 数据库中。 NetScreen 设备将新事件和流量日志条目发送到外部存储位置 (每秒一次)。

下表列出了记录数据的可能目标位置 :

- **控制台 :** 当您通过控制台来排除 NetScreen 设备的故障时，这是显示所有日志条目的很有用的目标位置。此外，您可以选举在此只出现报警消息 (关键的、警示的、紧急的)，这样，如果在触发报警时您恰好在使用控制台，即可立即提醒您。
- **内部 :** NetScreen 设备上的内部数据库是存储日志条目的方便位置，但空间有限。
- **电子邮件 :** 将事件和流量日志发送给远程管理员的一个方便的方法。
- **SNMP:** 除了传送 SNMP 陷阱之外， NetScreen 设备也能将报警消息 (关键的、警示的、紧急的) 从其事件日志发送到 SNMP 公共组。
- **系统日志 :** NetScreen 设备可在内部存储所有事件和流量日志条目，这些条目也可以发送到系统日志服务器中。由于系统日志服务器的存储容量比 NetScreen 设备上的内部闪存大得多，因此，通过将数据发送到系统日志服务器，可以减少日志条目超过最大内部存储空间时发生的数据丢失。系统日志存储指定的安全设备中的警示事件和紧急事件，以及所指定设备中的所有其它事件 (包括信息流数据)。
- **WebTrends:** 允许以比系统日志更加图形化的格式来查看关键事件、警示事件和紧急事件的日志数据，而系统日志是一个基于文本的工具。
- **CompactFlash (PCMCIA):** 这种存储设备的优点就是便于携带。在 CompactFlash 卡上存储数据后，可以从 NetScreen 设备中取出该卡，并在其它设备上存储或装载它。

事件日志

NetScreen 提供可用于监控系统事件的事件日志，例如，由 admin 生成的配置更改，以及自行生成的同操作行为和攻击有关的消息和报警。 NetScreen 设备将系统事件按以下严重性级别进行分类 :

- **Emergency (紧急):** 关于 SYN 攻击、Tear Drop 攻击及 Ping of Death 攻击的消息。有关这些类型的攻击的详细信息，请参阅第 4 卷的 “攻击检测和防御机制”。
- **Alert (警示):** 关于需要立即引起注意的情况 (例如防火墙攻击和许可密钥到期) 的消息。
- **Critical (关键):** 关于可能影响设备功能的情况 [例如高可用性 (HA) 状态更改] 的消息。
- **Error (错误):** 关于可能影响设备功能的错误情况 (例如反病毒扫描失败或与 SSH 服务器通信失败) 的消息。
- **Warning (警告):** 关于可能影响设备功能的情况 (例如连接到电子邮件服务器失败或认证失败、超时和成功) 的消息。
- **Notification (通知):** 关于常规事件 (包括由 admin 发起的配置更改) 的消息。
- **Information (信息):** 可提供关于系统操作一般信息的消息。
- **Debugging (调试):** 可提供调试时所用详细信息的消息。

事件日志显示每个系统事件的日期、时间、级别及说明。通过 WebUI 或 CLI 可以查看 NetScreen 设备的闪存中存储的每一类系统事件。也可在指定位置打开或保存文件，然后用 ASCII 文本编辑器 (如 Notepad 或 WordPad) 来查看该文件。也可以将其发送到外部存储空间 (请参阅第 74 页上的 “存储日志信息”)。

注意：*关于事件日志中所出现消息的详细信息，请参阅* NetScreen Message Log *参考*指南。

查看事件日志

通过使用 CLI 或 WebUI 可以查看设备中存储的事件日志。在 WebUI 和 CLI 中，可按严重性级别显示日志条目以及按关键字搜索事件日志。

要按严重性级别显示事件日志，请执行以下操作之一：

WebUI

Reports > System Log > Event: 从 Log Level 下拉列表中选择一个严重性级别。

CLI

```
get event level { emergency | alert | critical | error | warning | notification
    | information | debugging }
```

要按关键字搜索事件日志，请执行以下操作之一：

WebUI

Reports > System Log > Event: 在 search 字段中键入最多 15 个字符长的单词或短语，然后单击 **Search**。

CLI

```
get event include word_string
```

范例：按照严重性级别和关键字查看事件日志

本例中，将查看具有 “warning” 严重性级别的事件日志条目，并搜索关键字 “AV”。

WebUI

Reports > System Log > Event:

Log Level: Warning (选择)

Search: 输入 AV，然后单击 **Search**。

CLI

```
get event level warning include av

Date       Time     Module Level Type Description
2003-05-16 15:56:20 system warn 00547 AV scanman is removed.
2003-05-16 09:45:52 system warn 00547 AV test1 is removed.
Total entries matched = 2
```

排序和过滤事件日志

此外，可以使用 CLI 按照下列条件来排序或过滤事件日志：

- **源或目标 IP 地址：**只有某些事件才会包含源或目标 IP 地址，如 Land 攻击或 ping 泛滥攻击。当按源或目标 IP 地址排序事件日志时，设备将排序并显示仅包含源或目标 IP 地址的事件日志。设备将忽略不包含源或目标 IP 地址的所有事件日志。

  当您通过指定源或目标 IP 地址或地址范围来过滤事件日志时，设备将显示指定的源或目标 IP 地址或地址范围的事件日志条目。

- **日期：**可以仅按照日期、或者按照日期和时间排序事件日志。当按照日期和时间排序日志条目时，设备将按照日期和时间的降序列出日志条目。

  也可以通过指定起始日期、终止日期或日期范围来过滤事件日志条目。当指定起始日期时，设备将显示其日期 / 时间戳位于该起始日期之后的日志条目。当指定终止日期时，设备将显示其日期 / 时间戳位于该终止日期之前的日志条目。

- **时间：**当按照时间排序日志时，设备将按照时间的降序显示日志条目，而不管日期如何。当指定起始时间时，设备将显示其时间戳位于该起始时间之后的的日志条目，而不管日期如何。当指定终止时间时，设备将显示其时间戳位于该终止时间之前的日志条目，而不管日期如何。如果同时指定了起始和终止时间，设备将显示其时间戳处于该指定的时间段内的日志条目。

- **消息类型 ID 号：**可以显示含特定消息类型 ID 号的事件日志条目，或者可显示含有指定范围内的消息类型 ID 号的日志条目。设备将按照日期和时间的降序显示含有所指定的消息类型 ID 号的日志条目。

范例：按照 IP 地址排序事件日志条目

本例中，将查看包含 10.100.0.0 到 10.200.0.0 范围内的源 IP 地址的事件日志条目。这些日志条目也按照源 IP 地址排序。

WebUI

> ***注意：****必须使用 CLI 按地址条目来排序事件日志。*

CLI

```
get event sort-by src-ip 10.100.0.0-10.200.0.0
```

下载事件日志

可在指定位置打开或保存事件日志，然后用 ASCII 文本编辑器 (如 Notepad 或 WordPad) 来查看该文件。也可以将日志条目发送到外部存储空间 (请参阅第 74 页上的 “存储日志信息”)。可以通过 WebUI 下载整个事件日志。可以通过 CLI 按照严重性级别下载事件日志。

范例 : 下载事件日志

本例中，将事件日志下载到本地目录中。使用 WebUI，将其下载到 “C:\netscreen\logs”。使用 CLI，将其下载到 IP 地址为 10.1.1.5 的 TFTP 服务器的根目录下。将文件命名为 “evnt07-02.txt”。

WebUI

1. Reports > System Log > Event: 单击 **Save**。

   File Download 对话框提示您打开该文件 (使用 ASCII 编辑器) 或将其保存到磁盘。

2. 选择 **Save** 选项，然后单击 **OK**。

   File Download 对话框提示您选择目录。

3. 指定 **C:\netscreen\logs**，将文件命名为 “evnt07-02.txt”，然后单击 **Save**。

CLI

```
get event > tftp 10.1.1.5 evnt07-02.txt
```

范例：下载关键事件的事件日志

本例中，将在事件日志中输入的关键事件下载到 IP 地址为 10.1.1.5 的 TFTP 服务器的根目录下 (CLI)。将文件命名为 “crt_evnt07-02.txt”。

WebUI

> ***注意：****必须使用 CLI 按严重性级别下载条目。*

CLI

```
get event level critical > tftp 10.1.1.5 crt_evnt07-02.txt
```

流量日志

NetScreen 设备可以监控和记录先前配置的策略所允许或拒绝的信息流。可以为所配置的每个策略启用记录选项。当为允许信息流的策略启用记录选项时，设备会记录该策略所允许的信息流。当为拒绝信息流的策略启用记录选项时，设备会记录试图通过该设备，但因该策略而被丢弃的信息流。

流量日志记录每个会话的下列元素：

- 连接开始的日期和时间
- 源地址和端口号
- 转换后的源地址和端口号
- 目标地址和端口号
- 会话的持续时间
- 会话中使用的服务

要记录 NetScreen 设备接收到的所有信息流，必须为所有策略启用记录选项。要记录特定信息流，只需对应用到该信息流的策略启用记录选项。要对策略启用记录选项，请执行下列操作之一：

WebUI

Policies > (From: *src_zone*, To: *dst_zone*) New：选择 **Logging**，然后单击 **OK**。

CLI

```
set policy from src_zone to dst_zone src_addr dst_addr service action log
```

除了记录策略的信息流外，设备还将维护该策略所应用到的所有网络信息流的字节数。当启用计数选项时，设备在显示流量日志条目时将包含下列信息：

- 从源传送到目标的信息流的字节数
- 从目标传送到源的信息流的字节数

要对策略启用计数选项，请执行下列操作之一：

WebUI

Policies > (From: *src_zone*, To: *dst_zone*) New > Advanced: 选择 **Counting**，单击 **Return**，然后单击 **OK**。

CLI

```
set policy from src_zone to dst_zone src_addr dst_addr service action log count
```

查看流量日志

通过 WebUI 或 CLI 可以查看 NetScreen 设备上的闪存中存储的流量日志条目：

WebUI

Policies >  (对于策略 ID *number*)

或

Reports > Policies >  (对于策略 ID *number*)

CLI

```
get log traffic policy number
```

范例：查看流量日志条目

本例中，将查看 ID 号为 3、而且此前已为其启用了记录的策略的流量日志详细信息：

WebUI

Policies: 单击 ID 号为 3 的策略的  图标。

将出现以下信息：

Date/Time	Source Address/Port	Destination Address/Port	Translated Source Address/Port	Translated Destination Address/Port	Service	Duration	Bytes Sent	Bytes Received
2003-01-09 21:33:43	1.1.1.1:1046	10.1.1.5:80	1.1.1.1:1046	10.1.1.5:80	HTTP	1800 sec.	326452	289207

CLI

```
get log traffic policy 3
```

排序和过滤流量日志

与事件日志类似，在使用 CLI 查看流量日志时，可以按照下列条件排序或过滤日志条目：

- **源或目标 IP 地址：**可以按照源或目标 IP 地址排序流量日志。也可以通过指定源或目标 IP 地址或地址范围来过滤流量日志。
- **日期：**可以仅按照日期或按照日期和时间排序流量日志。设备按照日期和时间的降序列出日志条目。

  也可以通过指定起始日期、终止日期或日期范围来过滤事件日志条目。当指定起始日期时，设备将显示其日期 / 时间戳位于该起始日期之后的日志条目。当指定终止日期时，设备将显示其日期 / 时间戳位于该终止日期之前的日志条目。
- **时间：**当按照时间排序流量日志时，设备将按照时间的降序显示日志条目，而不管日期如何。当指定起始时间时，设备将显示其时间戳位于该起始时间之后的的日志条目，而不管日期如何。当指定终止时间时，设备将显示其时间戳位于该终止时间之前的日志条目，而不管日期如何。如果同时指定了起始和终止时间，设备将显示其时间戳处于该指定的时间段内的日志条目。

范例：按照时间排序流量日志

本例中，将按照时间排序来查看时间戳位于 01:00 之后的流量日志。

WebUI

> ***注意：****只能通过 CLI 来按时间排序流量日志。*

CLI

```
get log traffic sort-by time start-time 01:00:00
```

下载流量日志

也可在指定位置打开或保存日志，然后用 ASCII 文本编辑器 (如 Notepad 或 WordPad) 来查看该文件。

也可以将流量日志条目发送到外部存储空间 (请参阅第 74 页上的“存储日志信息”)。当会话终止时，NetScreen 设备会在流量日志中生成一个条目。当使 NetScreen 设备将流量日志条目发送到外部存储位置时，设备每秒钟发送一次新条目。由于会话结束时 NetScreen 设备会生成一个流量日志条目，因此，对于在过去的一秒内结束的所有会话，NetScreen 设备都将发送流量日志条目。也可以包含这样一些流量日志条目 : 它们带有用电子邮件发送给 admin 的事件日志条目。

范例 : 下载流量日志

本例中，将下载 ID 号为 12 的策略的流量日志。使用 WebUI 时，将其下载到本地目录 “C:\netscreen\logs”。使用 CLI 时，将其下载到 IP 地址为 10.10.20.200 的 TFTP 服务器的根目录下。将文件命名为 “traf_log11-21-02.txt”。

WebUI

1. Reports > Policies >  (对于策略 ID 12): 单击 **Save**。

   File Download 对话框提示您打开该文件 (使用 ASCII 编辑器) 或将其保存到磁盘。
2. 选择 **Save** 选项，然后单击 **OK**。

   File Download 对话框提示您选择目录。
3. 指定 C:\netscreen\logs，将文件命名为 traf_log11-21-02.txt，然后单击 **Save**。

CLI

```
get log traffic policy 12 > tftp 10.10.20.200 traf_log11-21-02.txt
```

SELF 日志

NetScreen 提供了 self 日志，以监控和记录在 NetScreen 设备上终止的所有数据包。例如，如果在接口上禁用了一些管理选项 (如 WebUI、SNMP 和 ping)，且 HTTP、SNMP 或 ICMP 信息流被发送到该接口上，则对于每个被丢弃的数据包，将会有与之相对应的条目出现在 self 日志中。

要激活 self 日志，请执行下列操作之一 :

WebUI

Configuration > Report Settings > Log Settings: 选中 **Log Packets Terminated to Self** 复选框，然后单击 **Apply**。

CLI

```
set firewall log-self
```

当启用 self 日志时， NetScreen 设备将在两个位置记录条目 : self 日志和流量日志。与流量日志类似， self 日志中显示有每个在 NetScreen 设备上终止的被丢弃数据包的日期、时间、源地址 / 端口、目标地址 / 端口、持续时间和服务等信息。 Self 日志条目通常具有一个源区段 Null 和一个目标区段 “self”。

查看 Self 日志

通过 CLI 或 WebUI 可以查看 NetScreen 设备的闪存中存储的 self 日志。

WebUI

Reports > System Log > Self

CLI

```
get log self
```

排序和过滤 Self 日志

与事件和流量日志类似，在使用 CLI 查看 self 日志时，可以按照下列条件来排序或过滤日志条目：

- **源或目标 IP 地址：**可以按照源或目标 IP 地址排序 self 日志。也可以通过指定源或目标 IP 地址或地址范围来过滤 self 日志。
- **日期：**可以仅按照日期或按照日期和时间排序 self 日志。设备将按照日期和时间的降序列出日志条目。

  也可以通过指定起始日期、终止日期或日期范围来过滤 self 日志条目。当指定起始日期时，设备将显示其日期 / 时间戳位于该起始日期之后的日志条目。当指定终止日期时，设备将显示其日期 / 时间戳位于该终止日期之前的日志条目。
- **时间：**当按照时间排序 self 日志时， NetScreen 设备将按照时间的降序显示日志条目，而不管日期如何。当指定起始时间时，设备将显示其时间戳位于该起始时间之后的的日志条目，而不管日期如何。当指定终止时间时，设备将显示其时间戳位于该终止时间之前的日志条目，而不管日期如何。如果同时指定了起始和终止时间，设备将显示其时间戳位于该指定的时间段内的日志条目。

范例：按照时间过滤 Self 日志

本例中，将按照终止时间过滤 self 日志。 NetScreen 设备将显示其时间戳位于指定的终止时间之前的日志条目：

WebUI

> ***注意：****只能通过 CLI 来按时间过滤 self 日志。*

CLI

```
get log self end-time 16:32:57

================================================================================
Date        Time        Duration Source IP         Port Destination IP    Port Serv
================================================================================
2003-08-21 16:32:57    0:00:00 10.100.25.1          0 224.0.0.5            0 OSPF
2003-08-21 16:32:47    0:00:00 10.100.25.1          0 224.0.0.5            0 OSPF

           Total entries matched = 2
```

下载 Self 日志

也可将日志以文本文件的格式保存到指定的位置，然后使用 ASCII 文本编辑器 (如 Notepad 或 WordPad) 来查看该文件。

范例 : 下载 Self 日志

本例中，将 self 日志下载到本地目录 “C:\netscreen\logs” (WebUI) 或 IP 地址为 10.1.1.5 的 TFTP 服务器的根目录下 (CLI)。将文件命名为 “self_log07-03-02.txt”。

WebUI

1. Reports > System Log > Self: 单击 **Save**。

   File Download 对话框提示您打开该文件 (使用 ASCII 编辑器) 或将其保存到磁盘。
2. 选择 **Save** 选项，然后单击 **OK**。

   File Download 对话框提示您选择目录。
3. 指定 C:\netscreen\logs，将文件命名为 self_log07-03-02.txt，然后单击 **Save**。

CLI

```
get log self > tftp 10.1.1.5 self_log07-03-02.txt
```

资源恢复日志

NetScreen 提供资源恢复日志，显示设备每次使用资源恢复程序恢复其缺省设置的相关信息 (参阅第 55 页上的 “重置设备到出厂缺省设置”)。除了可通过 WebUI 或 CLI 查看资源恢复日志外，还可在指定位置打开或保存该文件。使用 ASCII 文本编辑器 (如 Notepad) 来查看该文件。

范例 : 下载资源恢复日志

本例中，将资源恢复日志下载到本地目录 “C:\netscreen\logs” (WebUI) 或 IP 地址为 10.1.1.5 的 TFTP 服务器的根目录下 (CLI)。将文件命名为 “sys_rst.txt”。

WebUI

1. Reports > System Log > Asset Recovery: 单击 **Save**。

   File Download 对话框提示您打开该文件 (使用 ASCII 编辑器) 或将其保存到磁盘。
2. 选择 **Save** 选项，然后单击 **OK**。

   File Download 对话框提示您选择目录。
3. 指定 C:\netscreen\logs，命名文件为 sys_rst.txt，然后单击 **Save**。

CLI

```
get log asset-recovery > tftp 10.1.1.5 sys_rst.txt
```

流量报警

NetScreen 设备支持当流量超出策略中所定义的临界值时进行流量报警。可配置 NetScreen 设备，使其每当 NetScreen 设备生成流量报警时，即可通过以下一种或多种方式来发出警示：

- 控制台
- 内部 (事件日志)
- 电子邮件
- SNMP
- 系统日志
- WebTrends
- NetScreen-Global PRO

可设置警告临界值以检测异常活动。要了解异常活动的构成，必须先建立正常活动的基准。要为网络信息流创建这样的基准，必须观察一段时间内的信息流模式。然后，在确定了流量大小 (认为其属于正常流量) 之后，可设置高于该值的警告临界值。超出该临界值的流量会触发一个警告，以提醒您流量已偏离了基准。然后就可对该情况进行评估，确定导致偏离的原因，以及是否需要采取行动以对此作出反应。

也可使用流量报警来提供受破坏系统的基于策略的入侵检测和通知。下面提供了为达到这些目的而使用流量报警的范例。

范例：基于策略的入侵检测

本例中，在 DMZ 区段内存在一个 IP 地址为 211.20.1.5 的 Web 服务器 (名为 “web1”)。想要对从 Untrust 区段通过 Telnet 访问此 Web 服务器的所有尝试进行检测。要实现此目的，可创建一策略，拒绝由 Untrust 区段内任何地址发往 DMZ 区段内名为 web1 的 Web 服务器的 Telnet 流量，并将流量报警临界值设置为 64 字节。由于最小的 IP 数据包为 64 字节，即使只有一个试图从 Untrust 区段发往 Web 服务器的 Telnet 数据包，也会触发警告。

WebUI

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

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (选择), 211.20.1.5/32

Zone: DMZ

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), web1

Service: Telnet

Action: Deny

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页：

Counting: (选择)

Alarm Threshold: 64 Bytes/Sec, 0 Kbytes/Min

CLI

```
set address dmz web1 211.20.1.5/32
set policy from untrust to dmz any web1 telnet deny count alarm 64 0
save
```

范例：受破坏系统通知

本例中，将使用流量报警来提供受破坏系统的通知。DMZ 区段内有一台 IP 地址为 211.20.1.10 (名称为 ftp1) 的 FTP 服务器。希望能允许 FTP-get 信息流到达此服务器。不希望有来自 FTP 服务器的任何种类的信息流。如出现这种信息流则说明系统已受到破坏，这可能是与 NIMDA 病毒相似的病毒所导致的。在 Global 区段内定义 FTP 服务器的地址，这样就能创建两个全域策略。

WebUI

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

Address Name: ftp1

IP Address/Domain Name:

IP/Netmask: (选择), 211.20.1.10/32

Zone: Global

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), ftp1

Service: FTP-Get

Action: Permit

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

Source Address:

Address Book Entry: (选择), ftp1

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Deny

> Advanced: 输入以下内容，然后单击 **Return**，设置高级选项并返回基本配置页 :

Counting: (选择)

Alarm Threshold: 64 Bytes/Sec, 0 Kbytes/Min

CLI

```
set address global ftp1 211.20.1.10/32
set policy global any ftp1 ftp-get permit
set policy global ftp1 any any deny count alarm 64 0
save
```

范例：发送电子邮件警示

本例中，如果有警告，则通过电子邮件警示来设置通知。邮件服务器地址为 172.16.10.254，通知的第一个电子邮件地址为 jharker@juniper.net，第二个电子邮件地址为 driggs@juniper.net。 NetScreen 设备包含具有通过电子邮件发送的事件日志的流量日志。

WebUI

Configuration > Report Settings > Email: 输入以下信息，然后单击 **Apply**:

Enable E-Mail Notification for Alarms: (选择)

Include Traffic Log: (选择)

SMTP Server Name: 172.16.10.254[1]

E-Mail Address 1: jharker@juniper.net

E-Mail Address 2: driggs@juniper.net

CLI

```
set admin mail alert
set admin mail mail-addr1 jharker@juniper.net
set admin mail mail-addr2 driggs@juniper.net
set admin mail server-name 172.16.10.254
set admin mail traffic-log
save
```

1. 如果启用了 DNS，则可为邮件服务器使用主机名，如 mail.netscreen.com。

系统日志

NetScreen 设备可以为达到预定义的严重性级别 (请参阅第 75 页上的 “事件日志”中的严重性级别列表) 的系统事件生成系统日志消息，并可有选择性地为策略允许通过防火墙的信息流生成系统日志消息。设备最多可将这些消息发送到四个指定的系统日志主机，这些主机运行在 UNIX/Linux 系统下。对于每个系统日志主机，可以指定下列各项 :

- NetScreen 设备包含流量日志条目、事件日志条目，还是既包含流量日志条目又包含事件日志条目
- 是否将信息流通过 VPN 通道发送到系统日志服务器，如果通过 VPN 通道传送信息流，将使用哪个接口作为源接口 (有关相应的范例，请参阅第 109 页上的 “范例 : 通过基于路由的通道的自行生成的信息流”和第 119 页上的 “范例 : 通过基于策略的通道的自行生成的信息流”)
- NetScreen 设备将系统日志消息发送到哪个端口
- 安全设备和常规设备；前者分类并发送紧急和警示级消息到系统日志主机；后者分类并发送所有与安全无关的事件的其它消息

在缺省情况下，NetScreen 设备通过 UDP (端口 514) 将消息发送到系统日志主机。为了提高消息发送的可靠性，可以将每个系统日志主机的传输协议改为 TCP。

可使用系统日志消息为系统管理员创建电子邮件警示，或使用 UNIX 系统日志约定在指定主机的控制台上显示消息。

注意 : *在 UNIX/Linux 平台上，修改文件 /etc/rc.d/init.d/syslog，这样系统日志就能从远程源地点 (syslog -r) 中检索信息。*

范例 : 启用多个系统日志服务器

本例中，将 NetScreen 设备配置为 : 通过 TCP 将事件日志和流量日志发送到拥有下列 IP 地址 / 端口号的三个系统日志服务器 : 1.1.1.1/1514、 2.2.2.1/2514 和 3.3.3.1/3514。将安全级别和设备级别都设置为 Local0。

WebUI

Configuration > Report Settings > Syslog: 输入以下内容，然后单击 **Apply**:

Enable syslog messages: 选择此选项以便将日志发送到指定的系统日志服务器。

No.: 选择 1、 2 和 3 以表示正在添加 3 个系统日志服务器。

IP/Hostname: 1.1.1.1, 2.2.2.1, 3.3.3.1

Port: 1514, 2514, 3514

Security Facility: Local0, Local0, Local0

Facility: Local0, Local0, Local0

Event Log: (选择)

Traffic Log: (选择)

TCP: (选择)

CLI

```
set syslog config 1.1.1.1 port 1514
set syslog config 1.1.1.1 log all
set syslog config 1.1.1.1 facilities local0 local0
set syslog config 1.1.1.1 transport tcp
set syslog config 2.2.2.1 port 2514
set syslog config 2.2.2.1 log all
set syslog config 2.2.2.1 facilities local0 local0
set syslog config 2.2.2.1 transport tcp
set syslog config 3.3.3.1 port 3514
set syslog config 3.3.3.1 log all
```

```
set syslog config 3.3.3.1 facilities local0 local0
set syslog config 2.2.2.1 transport tcp
set syslog enable
save
```

WebTrends

NetIQ 提供了一个名为 WebTrends Firewall Suite 的产品，该产品允许您依据 NetScreen 设备所创建的日志创建自定义报告。 WebTrends 分析日志文件并以图形格式显示所需的信息。可以创建有关所有事件和严重性级别的报告，或者主要报告某一方面 (如防火墙攻击) 的事件。 (有关 WebTrends 的其它信息，请参阅 WebTrends 产品文档。)

也可通过 VPN 通道发送 WebTrends 消息。在 WebUI 中，使用 **Use Trust Zone Interface as Source IP for VPN** 选项。在 CLI 中，使用 **set webtrends vpn** 命令。

范例 : 启用通知事件的 WebTrends

下例中，将向 WebTrends 主机 (172.10.16.25) 发送通知消息。

WebUI

1. WebTrends 设置

   Configuration > Report Settings > WebTrends: 输入以下内容，然后单击 **Apply**:

   Enable WebTrends Messages: (选择)
   WebTrends Host Name/Port: 172.10.16.25/514

2. 严重性级别

   Configuration > Report Settings > Log Settings: 输入以下内容，然后单击 **Apply**:

   WebTrends Notification: (选择)

> ***注意 :*** *在处于 “透明” 模式下的 NetScreen 设备上启用 WebTrends 时，必须设置静态路由。请参阅第* ***6-1*** *页上的 “路由表和静态路由”。*

CLI

1. WebTrends 设置

```
set webtrends host-name 172.10.16.25
set webtrends port 514
set webtrends enable
```

2. 严重性级别

```
set log module system level notification destination webtrends
save
```

SNMP

NetScreen 设备的 “简单网络管理协议” (SNMP) 代理使网络管理员可以查看有关网络以及网络上的设备的统计数据，并可接收所需的系统事件通知。

NetScreen 支持 RFC-1157, “A Simple Network Management Protocol” 中所述的 SNMPv1 协议，并支持以下各个 RFC 中所述的 SNMPv2c 协议：

- *RFC-1901, “Introduction to Community-based SNMPv2”*
- *RFC-1905, “Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)”*
- *RFC-1906, “Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)”*

NetScreen 也支持 RFC-1213, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II” 中定义的所有相关管理信息库 II (MIB II) 组。 NetScreen 还有企业专用的 MIB 文件，可将其加载到 SNMP MIB 浏览器。附录中包含 NetScreen MIB 列表。 (请参阅附录 A, “SNMP MIB 文件”。)

出现指定事件和情形时， NetScreen SNMP 代理会相应地生成以下陷阱或通知：

- **冷启动陷阱：**开启 NetScreen 设备使之处于可操作状态时，生成冷启动陷阱。
- **SNMP 认证故障陷阱：**如果有人试图使用不正确的 SNMP 公共组字符串来连接 NetScreen 设备，或者如果在 SNMP 公共组中未定义试图建立连接的主机的 IP 地址，则 NetScreen 设备中的 SNMP 代理将触发认证故障陷阱。 (在缺省情况下，将启用此选项。)
- **系统报警陷阱：**NetScreen 设备出错条件和防火墙条件将触发系统警告。为了涵盖与硬件、安全和软件相关的警告，定义了三个 NetScreen 企业陷阱。 (有关防火墙设置和警告的详细信息，请参阅第 **4**-206 页上的 “ICMP 碎片” 和第 92 页上的 “流量报警”。)
- **流量报警陷阱：**流量超过策略中设置的警告临界值时，触发流量报警。 (有关配置策略的详细信息，请参阅第 **2**-293 页上的 “策略”。)

下表列出了可能的报警类型及其相关的陷阱号：

陷阱企业 ID	说明
100	硬件问题
200	防火墙问题
300	软件问题
400	流量问题
500	VPN 问题
600	NSRP 问题
800	DRP 问题
900	接口故障切换问题
1000	防火墙攻击

注意：*网络管理员必须有 SNMP 管理器应用程序，如 HP OpenView® 或 SunNet Manager™，以便浏览 SNMP MIB II 数据并从可信或不可信的接口接收陷阱。互联网上也存在一些共享且免费的 SNMP 管理器应用程序。*

NetScreen 设备出厂时不带有 SNMP 管理器的缺省配置。要配置 NetScreen 设备的 SNMP，必须先创建公共组，定义其关联的主机并分配权限 (读 / 写或只读)。

创建 SNMP 公共组时，可以按照 SNMP 管理站的要求指定该公共组是支持 SNMPv1、 SNMPv2c，还是同时支持这两个 SNMP 版本。 (为了向后兼容仅支持 SNMPv1 的早期 ScreenOS 版本，在缺省情况下 NetScreen 设备支持 SNMPv1。) 如果 SNMP 公共组同时支持两个 SNMP 版本，则必须为每个公共组成员指定陷阱版本。

出于安全方面的考虑，具有读 / 写权限的 SNMP 公共组成员只能更改 NetScreen 设备的下列变量 :

- **sysContact** - NetScreen 设备的 admin 的联络信息，以备 SNMP admin 需要与其联系时使用。该信息可以是 NetScreen admin 的姓名、电子邮件地址、电话号码、在办公室中的位置，或者这类信息的组合。
- **sysLocation** - NetScreen 设备的物理位置。这可以是下列任何内容 : 国家、城市或建筑物的名称，直至设备在网络操作中心 (NOC) 的机架上的准确位置。
- **sysName** - SNMP 管理员用于 NetScreen 设备的名称。通常，该名称为一个完全合格的域名 (FQDN)，但也可以是对 SNMP admin 有意义的任何名称。
- **snmpEnableAuthenTraps** - 可通过该变量来启用或禁用 NetScreen 设备中的 SNMP 代理，使得当有人试图用不正确的 SNMP 公共组名称与 SNMP 代理进行联系时即会生成一个陷阱。
- **ipDefaultTTL** - 只要传输层协议没有提供活动时间 (TTL) 值，就会将该缺省值插入始发自 NetScreen 设备的数据报 IP 报头内的 TTL 字段中。
- **ipForwarding** - 该变量可指示 NetScreen 设备是否转发信息流 (发往 NetScreen 设备本身的信息流除外)。在缺省情况下， NetScreen 设备指示不转发信息流 (伪装其真实特性的骗术)。

执行概述

以下概括了 Juniper Networks 如何在其设备中执行 SNMP:

- SNMP 管理员被分组到 SNMP 公共组中。 NetScreen 设备最多可支持三个公共组，每个公共组最多可有八个成员。
- 公共组成员可以是单个主机，也可以是处于某个子网内的所有主机，这取决于定义成员时使用的网络掩码。在缺省情况下，NetScreen 设备为 SNMP 公共组成员分配一个 32 位的网络掩码 (255.255.255.255)，该网络掩码将 SNMP 公共组成员定义为单个主机。
- 如果将 SNMP 公共组成员定义为子网，则该子网上的任何设备都可以轮询 NetScreen 设备以获得 SNMP MIB 信息。但是， NetScreen 设备不能将 SNMP 陷阱发送给子网，只能将其发送给单个主机。
- 每个公共组具有对 MIB II 数据的只读或读写权限。
- 每个公共组可支持 SNMPv1 和 / 或 SNMPv2c。如果公共组同时支持两个版本的 SNMP，则必须为每个公共组成员指定陷阱版本。
- 可允许或拒绝每个公共组接收陷阱。
- 可通过任意物理接口访问 MIB II 数据和陷阱。
- 对设置为可接收陷阱的各公共组中的每台主机，每个系统报警 (分类为具有严重性级别关键、警示或紧急的系统事件) 都生成单个 NetScreen 企业 SNMP 陷阱。
- NetScreen 设备将 “冷启动 / 上行链路 / 下行链路” 陷阱发送到设置为可接收陷阱的公共组内的所有主机。
- 如果为公共组指定了 trap-on，则将会出现允许流量报警的选项。
- 可以通过基于路由或基于策略的 VPN 通道发送 SNMP 消息。有关详细信息，请参阅第 107 页上的 “自行生成的信息流的 VPN 通道”。

范例：定义读 / 写 SNMP 公共组

本例中，将创建一个名为 *MAge11* SNMP 的公共组。为其分配读 / 写权限并使其成员可接收 MIB II 数据和陷阱。该公共组拥有两个成员：1.1.1.5/32 和 1.1.1.6/32。其中每个成员都有 SNMP 管理器应用程序，每个应用程序运行不同版本的 SNMP: SNMPv1 和 SNMPv2c。

注意：*由于公共组名称将充当密码，因此请小心保护其秘密性。*

将提供 NetScreen 设备的本地 admin 的联络信息，以备 SNMP 公共组成员需要与其联系时使用 — name: al_baker@mage.com。还将提供 NetScreen 设备所在的位置 — location: 3-15-2。这些数字表明该设备位于三楼第十五排第二个位置处。

还将启用 SNMP 代理，使得一旦某人非法尝试建立与 NetScreen 设备的 SNMP 连接，即会生成一个陷阱。认证故障陷阱是一个全局性设置，其适用于所有 SNMP 公共组，缺省情况下将禁用该设置。

最后，在之前绑定到 Trust 区段中的接口 ethernet1 上启用 SNMP 可管理性。该接口是 SNMP 管理器应用程序与 NetScreen 设备中的 SNMP 代理通信所使用的接口。

WebUI

Configuration > Report Settings > SNMP: 输入以下设置，然后单击 **Apply**:

System Contact: al_baker@mage.com

Location: 3-15-2

Enable Authentication Fail Trap: (选择)

Configuration > Report Settings > SNMP > New Community: 输入以下设置，然后单击 **OK**:

Community Name: MAge11

Permissions:

Write: (选择)

Trap: (选择)

Including Traffic Alarms: (清除)

Version: ANY (选择)

Hosts IP Address/Netmask and Trap Version:
1.1.1.5/32 v1
1.1.1.6/32 v2c

Network > Interfaces > Edit (对于 ethernet1): 输入以下设置，然后单击 **OK**:

Service Options:

Management Services: SNMP

CLI

```
set snmp contact al_baker@mage.com
set snmp location 3-15-2
set snmp auth-trap enable
set snmp community MAge11 read-write trap-on version any
set snmp host Mage 1.1.1.5/32 trap v1
set snmp host Mage 1.1.1.6/32 trap v2
set interface ethernet1 manage snmp
save
```

自行生成的信息流的 VPN 通道

可以使用虚拟专用网 (VPN) 通道来确保从固定的 IP 地址对 NetScreen 设备进行远程监控的安全性。利用 VPN 通道，可以保护发往 NetScreen 设备和由此发出的信息流。从 NetScreen 设备发出的信息流类型可以包括 : NetScreen-Global PRO 报告、发送到系统日志和 WebTrends 服务器的事件日志条目以及 SNMP MIB 陷阱。

NetScreen 支持两种类型的 VPN 通道配置 :

- **基于路由的 VPN**: NetScreen 设备使用路由表条目将信息流引向绑定到 VPN 通道上的通道接口。

  如要要通过基于路由的 VPN 通道来发送 NetScreen 设备所生成的事件日志条目、NetScreen-Global PRO 报告或 SNMP 陷阱等信息流，必须手动输入通向适当目标的路由。该路由必须指向已绑定到 VPN 通道的通道接口，您希望 NetScreen 设备将信息流通过该 VPN 通道引向 NetScreen 设备。不需要任何策略。

- **基于策略的 VPN**: NetScreen 设备使用在策略中明确引用的 VPN 通道名称来通过 VPN 通道引导信息流。

  如要通过基于策略的 VPN 通道发送自行生成的信息流，必须在策略中包含源地址和目标地址。源地址可使用 NetScreen 设备上接口的 IP 地址。目标地址可使用存储服务器或 SNMP 公共组成员的工作站 (如果位于远程 NetScreen 设备的后面) 的 IP 地址。如果远程 SNMP 公共组成员使用 NetScreen-Remote VPN 客户端来建立与本地 NetScreen 设备的 VPN 连接，请使用在 NetScreen-Remote 上定义的内部 IP 地址作为目标地址。

  注意 : *在 ScreenOS 5.0.0 之前的版本中，源地址必须是绑定到 Trust 区段的缺省接口，而目标地址必须位于 Untrust 区段中。在当前版本中已没有此限制。*

如果远程网关或端实体拥有动态分配的 IP 地址，则 NetScreen 设备不能启动 VPN 通道的形成，原因在于无法预先确定这些地址，进而不能定义到这些地址的路由。出现此种情况时，必须由远程主机来启动 VPN 连接。一旦建立了基于策略或基于路由的 VPN 通道，通道的两端都可发起信息流 (若策略允许)。另外，对于基于路由的 VPN 而言，必然会存在一个经由 VPN 通道通向端实体的路由 – 该路由可能是您手动输入的路由，也可能是本地 NetScreen 设备在建立通道后通过交换动态路由消息而接收到的路由。(有关动态路由协议的信息，请参阅第 6 卷的 “路由”。) 也可以使用带有 rekey 选项或 IKE 心跳信号的 VPN 监控来确保建立通道后，该通道将始终保持连接状态 (而不管 VPN 的活动性如何)。(有关这些选项的详细信息，请参阅第 **5**-355 页上的 “VPN 监控” 和第 **5**-436 页上的 “监控机制”。)

对于每个 VPN 通道配置类型，可以使用下列类型 VPN 通道中的任何一种：

- **手动密钥**：可以在通道两端手动设置定义“安全联盟”(SA) 的三种元素：安全参数索引 (SPI)、加密密钥和认证密钥。要更改 SA 中的任一元素，必须在通道的两端对其进行手动输入。
- **具有预共享密钥的自动密钥 IKE**：一个或两个预共享密钥 (一个用于认证，一个用于加密) 充当种子值。IKE 协议使用它们在通道的两端生成一组对称密钥；即，使用相同的密钥进行加密和解密。这些密钥按预先定义的时间间隔自动重新生成。
- **具有证书的自动密钥 IKE**：凭借“公开密钥基础”(PKI)，通道两端的参与者使用一个数字证书 (用于认证) 和一个 RSA 公开 / 私有密钥对 (用于加密)。加密是不对称的；即密钥对中的一个密钥用于加密，而另一个用于解密。

> ***注意：****有关 VPN 通道的完整说明，请参阅第 5 卷的“VPN”。有关 NetScreen-Remote 的详细信息，请参阅* NetScreen-Remote 用户指南。

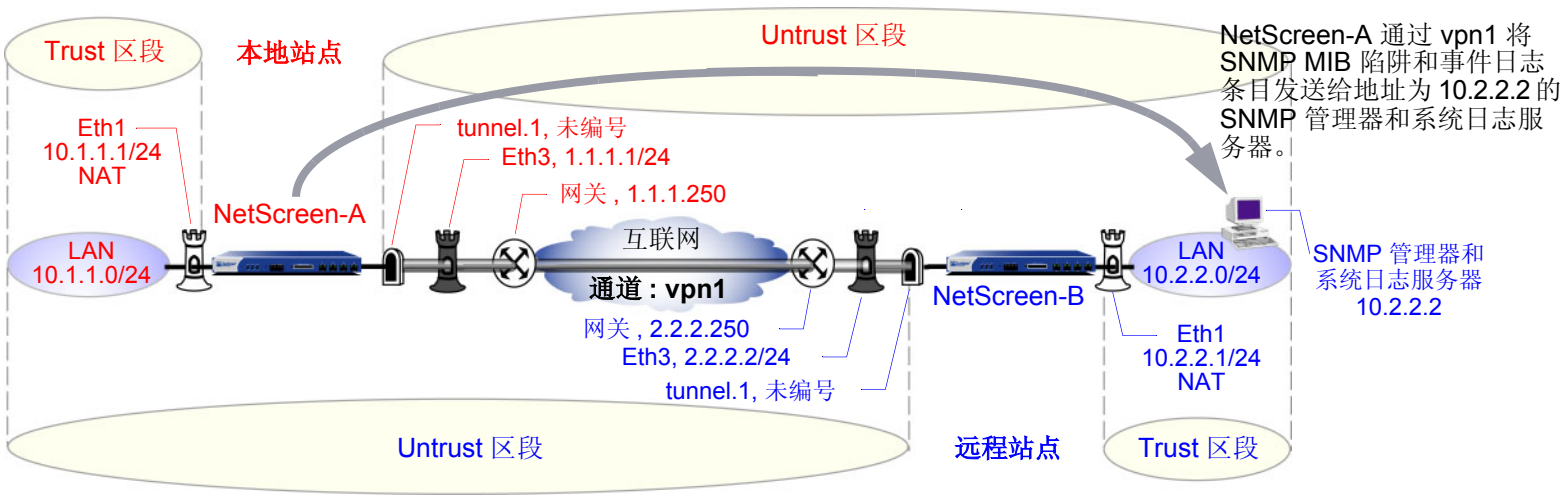
范例：通过基于路由的通道的自行生成的信息流

本例中，将对本地 NetScreen 设备 (NetScreen-A) 进行配置，使其通过基于路由的自动密钥 IKE VPN 通道将 SNMPv1 MIB 陷阱和系统日志报告发送给位于远程 NetScreen 设备 (NetScreen-B) 后面的 SNMP 公共组成员。通道将预共享密钥 (Ci5y0a1aAG) 用于数据源认证，并将预定义的安全级别 “Compatible” 用于 “阶段 1” 和 “阶段 2” 提议。您将以 NetScreen-A 本地 admin 的身份来创建 tunnel.1 接口，并将其绑定到 vpn1。您和 NetScreen-B 的 admin 将定义以下代理 ID:

	NetScreen-A		NetScreen-B
本地 IP	10.1.1.1/32	本地 IP	10.2.2.2/32
远程 IP	10.2.2.2/32	远程 IP	10.1.1.1/32
服务	Any	服务	Any

将 ethernet1 绑定到 Trust 区段，而将 ethernet3 绑定到 Untrust 区段。缺省网关 IP 地址为 1.1.1.250。所有区段都在 trust-vr 路由选择域中。

***注意：**可将本例与第 119 页上的 “范例：通过基于策略的通道的自行生成的信息流”进行比较。*



NetScreen-B 的远程 admin 使用类似的设置定义自动密钥 IKE VPN 通道的另外一端，因此预共享密钥、提议和代理 ID 相匹配。

还将配置一个名为 “remote_admin” 的具有读 / 写权限的 SNMP 公共组，并启用该公共组来接收陷阱。将地址为 10.2.2.2/32 的主机定义为公共组成员[2]。

WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24[3]

选择以下内容，然后单击 **OK**:

Interface Mode: NAT (选择)[4]

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Service Options:

Management Services: SNMP

2. 本例假定远程 admin 已安装了系统日志服务器和支持 SNMPv1 的 SNMP 管理器应用程序。远程 admin 在其 NetScreen 设备上设置 VPN 通道时，使用 1.1.1.1 作为远程网关，使用 10.1.1.1 作为目标地址。
3. 远程 admin 配置 SNMP 管理器时，必须在 “Remote SNMP Agent” 字段中输入 **10.1.1.1**。它是 SNMP 管理器发送查询的目标地址。
4. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet1(trust-vr)

2. 系统日志和 SNMP

Configuration > Report Settings > Syslog: 输入以下内容，然后单击 **Apply**:

Enable Syslog Messages: (选择)

No.: 选择 1 以表明您正在添加 1 个系统日志服务器。

IP / Hostname: 10.2.2.2

Port: 514

Security Facility: auth/sec

Facility: Local0

Configuration > Report Settings > SNMP > New Community: 输入以下内容，然后单击 **OK**:

Community Name: remote_admin

Permissions:

Write: (选择)

Trap: (选择)

Including Traffic Alarms: (清除)

Version: V1

Hosts IP Address/Netmask:

10.2.2.2/32 V1

Trap Version:

V1

3. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: to_admin

Type: Static IP, Address/Hostname: 2.2.2.2

Preshared Key: Ci5y0a1aAG

Security Level: Compatible

Outgoing interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 “自动密钥 IKE” 配置页 :

Bind To: Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 10.1.1.1/32

Remote IP/Netmask: 10.2.2.2/32

Service: ANY

4. 路由

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

Network Address/Netmask: 10.2.2.2/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: (选择) 1.1.1.250

CLI (NetScreen-A)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24[5]
set interface ethernet1 nat[6]
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage snmp
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. VPN

```
set ike gateway to_admin address 2.2.2.2 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.1.1.1/32 remote-ip 10.2.2.2/32 any
```

5. 远程 admin 配置 SNMP 管理器时，必须在 “Remote SNMP Agent” 字段中输入 **10.1.1.1**。它是 SNMP 管理器发送查询的目标地址。
6. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

3. 系统日志和 SNMP

```
set syslog config 10.2.2.2 auth/sec local0
set syslog enable
set snmp community remote_admin read-write trap-on version v1
set snmp host remote_admin 10.2.2.2/32
```

4. 路由

```
set vrouter trust-vr route 10.2.2.2/32 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

WebUI (NetScreen-B)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet1(trust-vr)

2. 地址

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

Address Name: addr1

IP Address/Domain Name:
IP/Netmask: 10.2.2.2/32

Zone: Trust

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

Address Name: ns-a

IP Address/Domain Name:
IP/Netmask: 10.1.1.1/32

Zone: Untrust

3. 服务组

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

Group Name: s-grp1

选择 **Syslog**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **SNMP**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: to_admin

Type: Static IP, Address/Hostname: 1.1.1.1

Preshared Key: Ci5y0a1aAG

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 “自动密钥 IKE” 配置页 :

Bind To: Tunnel Interface: (选择), tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 10.2.2.2/32

Remote IP/Netmask: 10.1.1.1/32

Service: Any

5. 路由

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

Network Address/Netmask: 10.1.1.1/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: (选择) 2.2.2.250

6. 策略

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

Source Address:

Address Book Entry: (选择), addr1

Destination Address:

Address Book Entry: (选择), ns-a

Service: s-grp1

Action: Permit

Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), ns-a

Destination Address:

Address Book Entry: (选择), addr1

Service: s-grp1

Action: Permit

Position at Top: (选择)

CLI (NetScreen-B)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. 地址

```
set address trust addr1 10.2.2.2/32
set address untrust ns-a 10.1.1.1/32
```

3. 服务组

```
set group service s-grp1
set group service s-grp1 add syslog
set group service s-grp1 add snmp
```

4. VPN

```
set ike gateway to_admin address 1.1.1.1 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.2.2.2/32 remote-ip 10.1.1.1/32 any
```

5. 路由

```
set vrouter trust-vr route 10.1.1.1/32 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

6. 策略

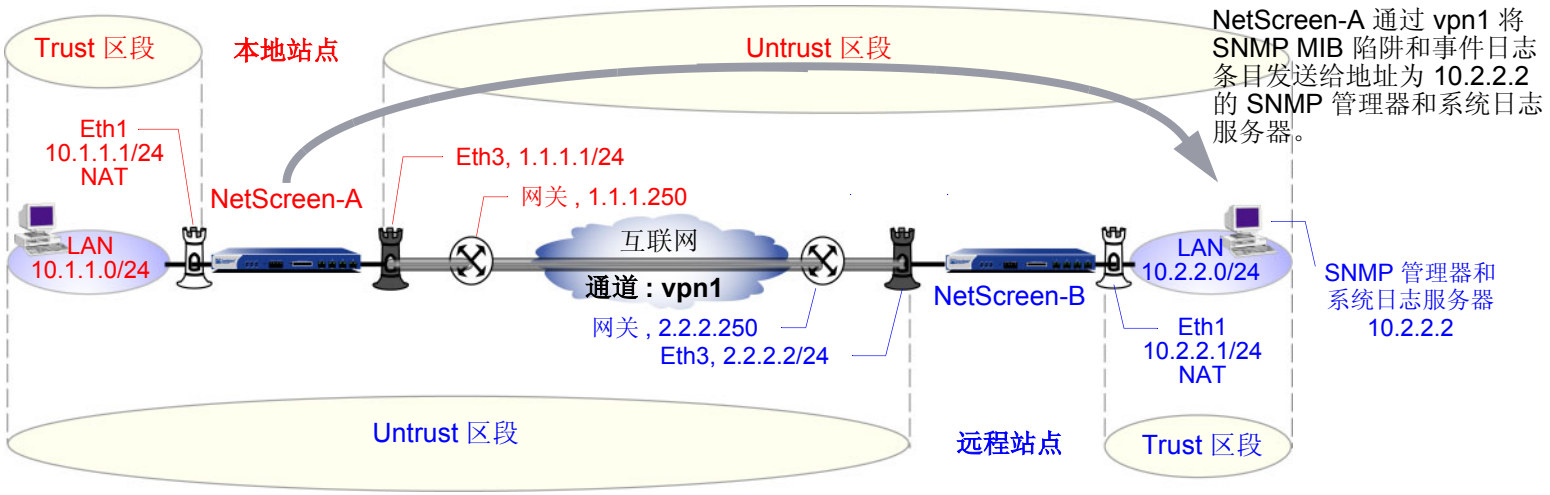
```
set policy top from trust to untrust addr1 ns-a s-grp1 permit
set policy top from untrust to trust ns-a addr1 s-grp1 permit
save
```

范例：通过基于策略的通道的自行生成的信息流

本例中，将对本地 NetScreen 设备 (NetScreen-A) 进行配置，使其通过基于策略的自动密钥 IKE VPN 通道 (vpn1) 将 SNMPv2c MIB 陷阱和系统日志报告[7] 发送给位于远程 NetScreen 设备 (NetScreen-B) 后面的 SNMP 公共组成员。通道将预共享密钥 (Ci5y0a1aAG) 用于数据源认证，并将预定义的安全级别 “Compatible” 用于 “阶段 1” 和 “阶段 2” 提议。

您和远程 admin 都将 ethernet1 绑定到 Trust 区段，并将 ethernet3 绑定到 NetScreen-A 和 NetScreen-B 上的 Untrust 区段。 NetScreen-A 的缺省网关 IP 地址为 1.1.1.250。 NetScreen-B 的缺省网关 IP 地址为 2.2.2.250。所有区段都在 trust-vr 路由选择域中。

注意：*可将本例与第 109 页上的 “范例：通过基于路由的通道的自行生成的信息流”进行比较。*



还将配置一个名为 “remote_admin” 的具有读 / 写权限的 SNMP 公共组，并启用该公共组来接收陷阱。将位于 10.2.2.2/32 的主机定义为公共组成员。

7. 本例假定远程 admin 已安装系统日志服务器和支持 SNMPv2c 的 SNMP 管理器应用程序。远程 admin 在其 NetScreen 设备上设置 VPN 通道时，使用 1.1.1.1 作为远程网关，使用 10.1.1.1 作为目标地址。

NetScreen-A 上的入站和出站策略与 NetScreen-B 上的出站和入站策略相匹配。这些策略中使用的地址和服务如下：

- 10.1.1.1/32， NetScreen-A 上的 Trust 区段接口的地址
- 10.2.2.2/32， SNMP 公共组成员的主机和系统日志服务器的地址
- 名为 “s-grp1”的服务组，其中包含 SNMP 和系统日志服务

从您与 NetScreen-B 的 admin 创建的策略中，两个 NetScreen 设备可获得 vpn1 的下列代理 ID:

	NetScreen-A		NetScreen-B
本地 IP	10.1.1.1/32	本地 IP	10.2.2.2/32
远程 IP	10.2.2.2/32	远程 IP	10.1.1.1/32
服务	Any	服务	Any

***注意：** NetScreen 在代理 ID 中将服务组当作 “any”。*

WebUI (NetScreen-A)

1. 接口 – 安全区段

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

Zone Name: Trust

Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24[8]

选择以下内容，然后单击 **OK**:
Interface Mode: NAT (选择)[9]

8. 远程 admin 配置 SNMP 管理器时，必须在 “Remote SNMP Agent” 字段中输入 **10.1.1.1**。它是 SNMP 管理器发送查询的目标地址。
9. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

Service Options:

Management Services: SNMP

2. 地址

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

Address Name: trust_int

IP Address/Domain Name:
IP/Netmask: 10.1.1.1/32

Zone: Trust

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

Address Name: remote_admin

IP Address/Domain Name:
IP/Netmask: 10.2.2.2/32

Zone: Untrust

3. 服务组

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

Group Name: s-grp1

选择 **Syslog**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **SNMP**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: to_admin

Type: Static IP, Address/Hostname: 2.2.2.2

Preshared Key: Ci5y0a1aAG

Security Level: Compatible

Outgoing Interface: ethernet3

5. 系统日志和 SNMP

Configuration > Report Settings > Syslog: 输入以下内容，然后单击 **Apply**:

Enable Syslog Messages: (选择)

Source Interface: ethernet1

No.: 选择 1 以表明您正在添加 1 个系统日志服务器。

IP/Hostname: 10.2.2.2

Port: 514

Security Facility: auth/sec

Facility: Local0

Configuration > Report Settings > SNMP > New Community: 输入以下内容，然后单击 **OK**:

Community Name: remote_admin

Permissions:

Write: (选择)

Trap: (选择)

Including Traffic Alarms: (清除)

Version: V2C

Hosts IP Address/Netmask:

10.2.2.2/32 V2C

Trap Version:

V2C

Source Interface:

ethernet1 (选择)

Configuration > Report Settings > SNMP: 输入以下内容，然后单击 **Apply**:

Enable Authentication Fail Trap: (选择)

6. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

7. 策略

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

Source Address:

Address Book Entry: (选择), trust_int

Destination Address:

Address Book Entry: (选择), remote_admin

Service: s-grp1

Action: Tunnel

Tunnel VPN: vpn1

Modify matching outgoing VPN policy: (选择)

Position at Top: (选择)

CLI (NetScreen-A)

1. 接口 – 安全区段

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat[10]
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage snmp
```

2. 地址

```
set address trust trust_int 10.1.1.1/32
set address untrust remote_admin 10.2.2.2/32
```

3. 服务组

```
set group service s-grp1
set group service s-grp1 add syslog
set group service s-grp1 add snmp
```

10. 在缺省情况下，绑定到 Trust 区段的所有接口都处于 NAT 模式。因此，对于绑定到 Trust 区段的接口，此选项已经启用。

4. VPN

```
set ike gateway to_admin address 2.2.2.2 outgoing-interface ethernet3 preshare
    Ci5y0a1aAG sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
```

5. 系统日志和 SNMP

```
set syslog config 10.2.2.2 auth/sec local0
set syslog src-interface ethernet1
set syslog enable
set snmp community remote_admin read-write trap-on version v2c
set snmp host remote_admin 10.2.2.2/32 src-interface ethernet1
```

6. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

7. 策略

```
set policy top from trust to untrust trust_int remote_admin s-grp1 tunnel vpn
    vpn1
set policy top from untrust to trust remote_admin trust_int s-grp1 tunnel vpn
    vpn1
save
```

WebUI (NetScreen-B)

1. 接口 – 安全区段

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

2. 地址

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

Address Name: addr1

IP Address/Domain Name:

IP/Netmask: 10.2.2.2/32

Zone: Trust

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

Address Name: ns-a

IP Address/Domain Name:

IP/Netmask: 10.1.1.1/32

Zone: Untrust

3. 服务组

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

Group Name: s-grp1

选择 **Syslog**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

选择 **SNMP**，并使用 **<<** 按钮将服务从 Available Members 栏移动到 Group Members 栏中。

4. VPN

VPNs > AutoKey IKE > New: 输入以下内容，然后单击 **OK**:

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: to_admin

Type: Static IP, IP Address: 1.1.1.1

Preshared Key: Ci5y0a1aAG

Security Level: Compatible

Outgoing interface: ethernet3

5. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: (选择) 2.2.2.250

6. 策略

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

Source Address:

Address Book Entry: (选择), addr1

Destination Address:

Address Book Entry: (选择), ns-a

Service: s-grp1

Action: Tunnel

Tunnel VPN: vpn1

Modify matching outgoing VPN policy: (选择)

Position at Top: (选择)

CLI (NetScreen-B)

1. 接口 – 安全区段

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
```

2. 地址

```
set address trust addr1 10.2.2.2/32
set address untrust ns-a 10.1.1.1/32
```

3. 服务组

```
set group service s-grp1
set group service s-grp1 add syslog
set group service s-grp1 add snmp
```

4. VPN

```
set ike gateway to_admin address 1.1.1.1 outgoing-interface ethernet3 preshare
    Ci5y0a1sec-level compatible
set vpn vpn1 gateway to_admin sec-level compatible
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

6. 策略

```
set policy top from trust to untrust addr1 ns-a s-grp1 tunnel vpn vpn1
set policy top from untrust to trust ns-a addr1 s-grp1 tunnel vpn vpn1
save
```

计数器

NetScreen 提供了屏幕、硬件和流量计数器来监控信息流。计数器为指定区段和接口提供处理信息，并帮助校验所需策略的配置。

NetScreen 提供了以下屏幕计数器，用来监控常规的防火墙活动及查看受指定策略影响的信息流总量：

- **Bad IP Option Detection** – 由于构造不良或 IP 选项不完整而被丢弃的帧数
- **Dst IP-based session limiting** – 达到会话临界值后被丢弃的会话数
- **FIN bit with no ACK bit** – 带有非法标记组合的已检测和已丢弃数据包数
- **Fragmented packet protection** – 被阻塞的 IP 数据包碎片的数目
- **HTTP Component Blocked** – 被阻塞的含 HTTP 组件的数据包数目
- **HTTP Component Blocking for ActiveX controls** – 被阻塞的 ActiveX 组件的数目
- **HTTP Component Blocking for .exe files** – 被阻塞的含 .exe 文件的 HTTP 数据包数目
- **HTTP Component Blocking for Java applets** – 被阻塞的 Java 组件数目
- **HTTP Component Blocking for .zip files** – 被阻塞的含 .zip 文件的 HTTP 数据包数目
- **ICMP Flood Protection** – 作为 ICMP (因特网控制信息协议) 泛滥一部分的已阻塞 ICMP 数据包数
- **ICMP Fragment** – 设置了 More Fragments 标记或在偏移字段中指出了偏移量的 ICMP 帧数
- **IP Spoofing Attack Protection** – 作为 IP 欺骗攻击的一部分而被阻塞的 IP 地址数
- **IP Sweep Protection** – 检测及阻塞的 IP 扫描攻击数据包数
- **Land Attack Protection** – 作为不可信 Land 攻击的一部分而被阻塞的数据包数
- **Large ICMP Packet** – IP 长度超过 1024 的已检测 ICMP 帧数
- **Limit session** – 由于达到会话极限而不能传送的数据包数
- **Loose Src Route IP Option** – 启用了 “松散源路由” 选项后检测到的 IP 数据包数
- **Malicious URL Protection** – 阻塞的不可信恶意 URL 数
- **Ping-of-Death Protection** – 太大或不规则的不可信和已拒绝的 ICMP 数据包数
- **Port Scan Protection** – 检测及阻塞的端口扫描数
- **Record Route IP Option** – 启用了 “记录路由” 选项后检测到的帧数

- **Security IP Option** – 设置了 “IP 安全性” 选项后丢弃的帧数
- **Src IP-based session limiting** – 达到会话临界值后被丢弃的会话数
- **Source Route IP Option Filter** – 过滤的 IP 源路由数
- **Stream IP Option** – 设置了 “IP 流” 标识符后被丢弃的数据包数
- **Strict Src Route IP Option** – 启用了 “严格源路由” 选项后检测到的数据包数
- **SYN-ACK-ACK-Proxy DoS** – 由于 SYN-ACK-ACK-proxy DoS SCREEN 选项而被阻塞的数据包数
- **SYN and FIN bits set** – 带有非法标记组合的已检测数据包数
- **SYN Flood Protection** – 作为不可信 SYN 泛滥的一部分而被检测的 SYN 数据包数
- **SYN Fragment Detection** – 作为不可信 SYN 碎片攻击的一部分而被丢弃的数据包碎片数
- **Timestamp IP Option** – 设置了 “互联网时间戳” 选项后被丢弃的 IP 数据包数
- **TCP Packet without Flag** – 带有缺失或残缺标记字段的已丢弃非法数据包数
- **Teardrop Attack Protection** – 作为 Teardrop 攻击的一部分而被阻塞的数据包数
- **UDP Flood Protection** – 作为不可信 UDP 泛滥的一部分而被丢弃的 UDP 数据包数
- **Unknown Protocol Protection** – 作为未知协议的一部分而被阻塞的数据包数
- **WinNuke Attack Protection** – 作为不可信 WinNuke 攻击的一部分而被检测的数据包数

NetScreen 提供了以下硬件计数器来监控硬件性能及出错的数据包 :

- **drop vlan** – 由于缺少 VLAN 标记、未定义的子接口或由于 NetScreen 设备在 “透明” 模式下未启用 VLAN 中继而被丢弃的数据包数
- **early frame** – 用于以太网驱动程序缓冲区描述符管理的计数器
- **in align err** – 比特流中存在定位错误的内向数据包数
- **in bytes** – 收到的字节数
- **in coll err** – 内向冲突数据包数
- **in crc err** – 循环冗余校验 (CRC) 出错的内向数据包数
- **in dma err** – 存在直接存储器存取错误的内向数据包数
- **in misc err** – 存在混杂错误的内向数据包数
- **in no buffer** – 由于缓冲区不可用而无法接收的数据包数

- **in overrun** – 已传送的超载数据包数
- **in packets** – 接收到的数据包数
- **in short frame** – 含有少于 64 字节 (包括帧校验和) 的 ethernet 帧的内向数据包数
- **in underrun** – 已传送的欠载数据包数
- **late frame** – 用于以太网驱动程序缓冲区描述符管理的计数器
- **out bs pak** – 当搜索未知的 MAC 地址时，存放在后备存储器中的数据包数。当 NetScreen 设备转发数据包时，它首先检查目标 MAC 地址是否存在于 ARP 表中。如果在 APR 中不能找到目标 MAC 地址，则 NetScreen 设备会向网络发送一个 ARP 请求。在 NetScreen 设备收到第一个 ARP 请求回复之前，如果它收到另一具有相同目标 MAC 地址的数据包，则它会将 out bs pak 计数器的值加一。
- **out bytes** – 发送的字节数
- **out coll err** – 外向冲突数据包数
- **out cs lost** – 由于“多路访问载波监听 / 冲突检测”(CSMA/CD) 协议丢失了信号而被丢弃的外向数据包数[11]
- **out defer** – 延迟的外向数据包数
- **out discard** – 丢弃的外向数据包数
- **out heartbeat** – 外向心跳信号数据包数
- **out misc err** – 存在混杂错误的外向数据包数
- **out no buffer** – 由于缓冲区不可用而未发送的数据包数
- **out packets** – 发送的数据包数
- **re xmt limit** – 接口以半双工运行时超出重新传输限制而被丢弃的数据包数

NetScreen 还提供了以下流量计数器[12]，用来监控在信息流级别被检查的数据包数 :

- **address spoof** – 收到的不可信地址欺骗攻击数据包数
- **auth deny** – 用户认证被拒绝的次数
- **auth fail** – 用户认证失败的次数
- **big bkstr** – 等待 MAC 到 IP 的地址解析时由于过大而无法暂存到 ARP 后备存储器的数据包数

11. 有关“多路访问载波监听 / 冲突检测” (CSMA/CD) 协议的详细信息，请参阅 http://standards.ieee.org 上提供的 IEEE 802.3 标准。

12. 前面带有星号的计数器在本指南发布时尚不可用，始终显示 0。

- **connections** – 自上次引导后建立的会话数
- **encrypt fail** – 失败的点对点通道协议 (PPTP) 数据包数
- ***icmp broadcast** – 收到的 ICMP 广播数
- **icmp flood** – 逼近 ICMP 泛滥临界值时统计的 ICMP 数据包数
- **illegal pak** – 因为不符合协议标准而被丢弃的数据包数
- **in arp req** – 内向 arp 请求数据包数
- **in arp resp** – 外向 arp 请求数据包数
- **in bytes** – 收到的字节数
- **in icmp** – 收到的 “因特网控制信息协议” (ICMP) 数据包数
- **in other** – 其它以太网类型的内向数据包数
- **in packets** – 收到的数据包数
- **in self** – 发往 NetScreen 管理 IP 地址的数据包数
- ***in un auth** – 未经授权的 TCP、 UDP 和 ICMP 内向数据包数
- ***in unk prot** – 使用未知以太网协议的内向数据包数
- **in vlan** – 内向 vlan 数据包数
- **in vpn** – 收到的 IPSec (互联网协议安全性) 数据包数
- **invalid zone** – 发往无效安全区段的数据包数
- **ip sweep** – 超过指定的 IP 扫描临界值的已接收和已丢弃数据包数
- **land attack** – 收到的不可信 Land 攻击数据包数
- **loopback drop** – 因为不能通过 NetScreen 设备进行回传而被丢弃的数据包数。回传会话的范例 : 位于 Trust 区段内的主机将信息流发送给 MIP 或 VIP 地址，而该地址被映射到了同样位于该 Trust 区段内的服务器。 NetScreen 设备创建一个回传会话，该会话将这类信息流从该主机引导到 MIP 或 VIP 服务器。
- **mac relearn** – 因为 MAC 地址的位置发生变化，导致 MAC 地址获取表必须再获取与该 MAC 地址关联的接口的次数
- **mac tbl full** – MAC 地址获取表被完全填满的次数
- **mal url** – 发往被认为是恶意 URL 的已阻塞数据包数
- ***misc prot** – 使用 TCP、 UDP 或 ICMP 之外其它协议的数据包数

- **mp fail** – 在主处理器模块和处理器模块之间发送 PCI 消息时出现错误的次数
- **no conn** – 由于 “网络地址转换” (NAT) 连接不可用而被丢弃的数据包数
- **no dip** – 由于 “动态 IP” (DIP) 地址不可用而被丢弃的数据包数
- **no frag netpak** – netpak 缓冲区中的可用空间降至 70% 以下的次数
- ***no frag sess** – 不完整会话数超过最大 NAT 会话数一半的次数
- **no g-parent** – 因为无法找到父级连接而被丢弃的数据包数
- **no gate** – 由于没有可用入口而被丢弃的数据包数
- **no gate sess** – 由于未提供防火墙入口而被中断的会话数
- **no map** – 由于没有到可信方的映射而被丢弃的数据包数
- **no nat vector** – 由于入口不能使用 “网络地址转换” (NAT) 连接而被丢弃的数据包数
- ***no nsp tunnel** – 发送到未绑定任何 VPN 通道的通道接口上的已丢弃数据包数
- **no route** – 收到的不可路由的数据包数
- **no sa** – 由于未定义 “安全联盟” (SA) 而被丢弃的数据包数
- **no sa policy** – 由于没有与 SA 相关的策略而被丢弃的数据包数
- ***no xmit vpnf** – 由于碎片原因而被丢弃的 VPN 数据包数
- **null zone** – 由于错误地发送到绑定到 Null 区段的接口而被丢弃的数据包数
- **nvec err** – 由于 NAT 向量错误而被丢弃的数据包数
- **out bytes** – 发送的字节数
- **out packets** – 发送的数据包数
- **out vlan** – 外向 vlan 数据包数
- **ping of death** – 已接收到的不可信 Ping of Death 攻击数
- **policy deny** – 被定义的策略拒绝的数据包数
- **port scan** – 作为端口扫描尝试而统计的数据包数
- **proc sess** – 处理器模块上的总会话数超过最大临界值的次数
- **sa inactive** – 由于非活动 SA 而被丢弃的数据包数
- **sa policy deny** – 被 SA 策略拒绝的数据包数

- **sessn thresh** – 最大会话数量的临界值
- ***slow mac** – MAC 地址解析缓慢的帧数
- **src route** – 由于过滤源路由选项而被丢弃的数据包数
- **syn frag** – 由于碎片原因而被丢弃的 SYN 数据包数
- **tcp out of seq** – 接收到的序列号超出可接受范围的 TCP 片段数
- **tcp proxy** – 由于使用 TCP 代理 (如 SYN 泛滥保护选项或用户认证) 而被丢弃的数据包数
- **tear drop** – 作为不可信 Tear Drop 攻击的一部分而被阻塞的数据包数
- **tiny frag** – 收到的破碎小数据包数
- **trmn drop** – 被信息流管理丢弃的数据包数
- **trmng queue** – 在队列中等待的数据包数
- **udp flood** – 逼近 UDP 泛滥临界值时统计的 UDP 数据包数
- **url block** – 被阻塞的 HTTP 请求个数
- **winnuke** – 收到的 WinNuke 攻击数据包数
- **wrong intf** – 从处理器模块发送到主处理器模块的会话创建消息数
- **wrong slot** – 不正确地发送到错误的处理器模块的数据包数

范例 : 查看屏幕计数器

本例中，将查看 Trust 区段的 NetScreen 屏幕计数器。

WebUI

Reports > Counters > Zone Screen: 从 Zone 下拉列表中选择 **Trust**。

CLI

```
get counter screen zone trust
```

A

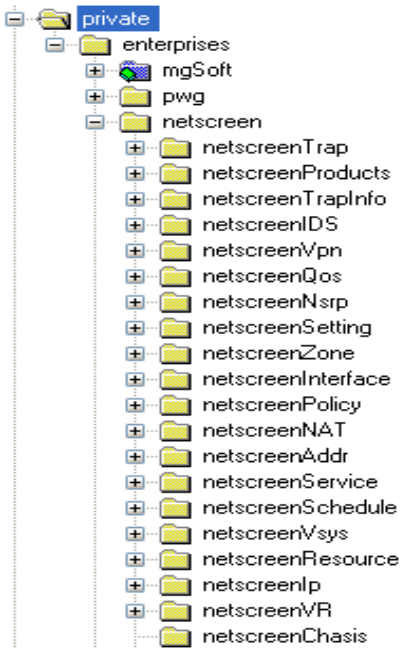
SNMP MIB 文件

Juniper Networks 提供 MIB 文件，用于支持组织的应用程序和 NetScreen 设备中 SNMP 代理之间的 SNMP 通信。要获得最新的 MIB 文件，请打开 Web 浏览器并访问 www.juniper.net/support。选择一个 NetScreen 产品，然后选择适用于 NetScreen 设备上加载的 ScreenOS 版本的 MIB 文件。

适用于 ScreenOS 当前版本的 MIB 文件与 ScreenOS 较早版本中的 SNMP 代理完全兼容。NetScreen MIB 文件具有多层的层次结构，说明如下：

一级 MIB 文件文件夹

MIB 文件是以分层式文件夹结构排列的。一级 MIB 文件夹如下所示：



每个文件夹包含一类 MIB 文件。

netscreenProducts	对不同的 NetScreen 产品系列指定 “对象标识符” (OID)。
netscreenTrapInfo	定义 NetScreen 设备发送的企业陷阱。
netscreenIDS	定义 NetScreen 设备侵入检测服务 (IDS) 配置。
netscreenVpn	定义 NetScreen 设备的 VPN 配置和运行时间信息。
netscreenQos	定义 NetScreen 设备的 “服务质量” 配置。

netscreenNsrp	定义 NetScreen 设备的 NSRP 配置。
netscreenSetting	定义 NetScreen 设备的其它配置设置，例如 DHCP、电子邮件、认证和管理员。
netscreenZone	定义 NetScreen 设备中的区段信息。
netscreenInterface	定义 NetScreen 设备的接口配置，包括虚拟接口。
netscreenPolicy	定义 NetScreen 设备的外向和内向策略配置。
netscreenNAT	定义 NAT 配置，包括 Map IP、Dynamic IP 和 Virtual IP。
netscreenAddr	表示 NetScreen 接口上的地址表。
netscreenService	说明 NetScreen 设备识别的服务 (包括用户定义的服务)。
netscreenSchedule	定义用户所配置 NetScreen 设备的任务调度信息。
netscreenVsys	定义 NetScreen 设备的虚拟系统 (VSYS) 配置。
netscreenResource	访问 NetScreen 设备的资源使用率信息。
netscreenIp	访问 NetScreen 设备的私有 IP 相关信息。
netScreen Chassis	清空将来的 MIB 支持文件夹的占位符文件夹。
netscreenVR	定义 NetScreen 设备的虚拟路由器 (VR) 配置。

二级 MIB 文件夹

本节介绍 NetScreen 设备的二级 MIB 文件。每个二级文件夹均包含有下一级文件夹或 MIB 文件。

netscreenProducts

netscreenGeneric	NetScreen 产品的通用对象标识符 (OID)
netscreenNs5	NetScreen-5XP OID
netscreenNs10	NetScreen-10XP OID
netscreenNs100	NetScreen-100 OID
netscreenNs1000	NetScreen-1000 OID
netscreenNs500	NetScreen-500 OID
netscreenNs50	NetScreen-50 OID
netscreenNs25	NetScreen-25 OID
netscreenNs204	NetScreen-204 OID
netscreenNs208	NetScreen-208 OID

netScreenIds

nsIdsProtect		NetScreen 设备上的 IDS 服务
	nsIdsProtectSetTable	在 NetScreen 设备上启用的 IDS 服务
	nsIdsProtectThreshTable	IDS 服务临界值配置
nsIdsAttkMonTable		侵入尝试的统计信息

netscreenVpn

netscreenVpnMon	显示 vpn 通道的 SA 信息
nsVpnManualKey	手动密钥配置
nsVpnIke	IKE 配置
nsVpnGateway	VPN 通道网关配置
nsVpnPhaseOneCfg	IPSec 阶段 1 配置
nsVpnPhaseTwoCfg	IPSec 阶段 2 配置
nsVpnCert	证书配置
nsVpnL2TP	L2TP 配置
nsVpnPool	IP 池配置
nsVpnUser	VPN 用户配置

netscreenQos

nsQosPly	策略的 QoS 配置

netscreenSetting

nsSetGeneral	NS 设备的通用配置
nsSetAuth	认证方法配置
nsSetDNS	DNS 服务器设置
nsSetURLFilter	URL 过滤设置
nsSetDHCP	DHCP 服务器设置
nsSetSysTime	系统时间设置
nsSetEmail	电子邮件设置
nsSetLog	系统日志设置
nsSetSNMP	SNMP 代理配置
nsSetGlbMng	全局管理配置
nsSetAdminUser	管理用户配置
nsSetWebUI	Web 用户界面配置

netscreenZone

nsZoneCfg	设备的区段配置

netscreenPolicy

NsPlyTable	策略配置
NsPlyMonTable	各项策略的统计信息

netscreenNAT

nsNatMipTable	映射 IP 配置
nsNatDipTable	动态 IP 配置
nsNatVip	虚拟 IP 配置

netscreenAddr

nsAddrTable	NetScreen 接口上的地址表

netscreenService

nsServiceTable	服务信息
nsServiceGroupTable	服务组信息
nsServiceGrpMemberTable	服务组成员信息

netscreenSchedule

nschOnceTable	单次调度信息
nschRecurTable	重复调度信息

netscreenVsys

nsVsysCfg	NetScreen 设备的虚拟系统 (VSYS) 配置

netscreenResource

nsresCPU	CPU 利用率
nsresMem	内存使用率
nsresSession	会话使用率

***注意：** ScreenOS 不再支持 failedSession 计数器。*

netscreenIp

nsIpArp	ARP 表

netscreenVR[1]

nsOSPF	开放式最短路径优先 (OSPF) 协议信息
nsBGP	边界网关协议 (BGP) 协议信息
nsRIP	路由选择信息协议 (RIP) 协议信息

1. NetscreenVR MIB 以“管理信息结构”第 2 版 (SMIv2) 为基础。所有其它 MIB 都是以 SMIv1 为基础。无论运行 SNMPv1 还是 SNMPv2c，都可以访问所有 MIB II 数据。

索引

M

N

P

R

S