NetScreen 概念与范例

ScreenOS 参考指南

第 3 卷 : 管理

ScreenOS 4.0.0

编号 093-0521-000-SC

版本 F

Copyright Notice

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

NetScreen 设备提供不同的方法管理该设备，既可本地管理，也可远程管理。第 3 卷，“管理”描述管理 NetScreen 设备的各种方法，解释 ScreenOS 的管理级别。本卷还描述了如何保证 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

本书介绍了配置 NetScreen 设备的两种管理方法。Web 用户界面 (WebUI) 和命令行界面 (CLI)。以下部分介绍本书使用的关于两种管理方法的约定。

WebUI 导航约定

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

范例：Objects > Addresses > List > New

要访问新的地址配置页，请执行以下操作：

1. 在菜单栏中，单击 **Objects**。
   对象菜单选项展开，显示出一个对象选项子菜单。
2. （Applet 菜单[1]）将鼠标光标悬停在 **Addresses** 上。
   （DHTML 菜单）单击 **Addresses**。
   地址选项展开，显示出一个地址选项子菜单。
3. 单击 **List**。
   出现通讯薄列表。
4. 在右上角单击 **New** 链接。
   出现新的地址配置页。

1. 可以选定 applet 或 DHTML 菜单类型中的任一个，方法是：在菜单栏底部，单击 **Toggle Menu** 选项。

CLI 约定

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

相关性定义符

每个语法说明中将介绍使用特殊字符来显示命令功能之间的相关性。

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

嵌套的相关性

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

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

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

以下例子说明一些 **set interface** 命令功能的相关性。

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

这个 { 和 } 括号说明指定的任一个 **flood** 或 **arp** 是必须遵循的。但是，[和] 括号说明，关于 **arp** 的 **trace-route** 选项不是必须遵循的。因而，这条命令可以采取以下任一种格式：

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

CLI 命令及功能的可用性

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

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

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

NETSCREEN 文档

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

欲在 NetScreen 产品版本上获得最新的技术信息，请参阅该版本的发行说明文档。欲获得发行说明，请浏览 www.netscreen.com/support 并选择 **Software Download**。选择产品及其版本，然后单击 **Go**。（欲执行此下载任务，您必须是注册用户。）

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

1

管理

本章介绍了多种管理方法及工具、保障管理流量安全的方法，以及可以指派给 admin 用户的管理权限级别。本章包括以下部分：

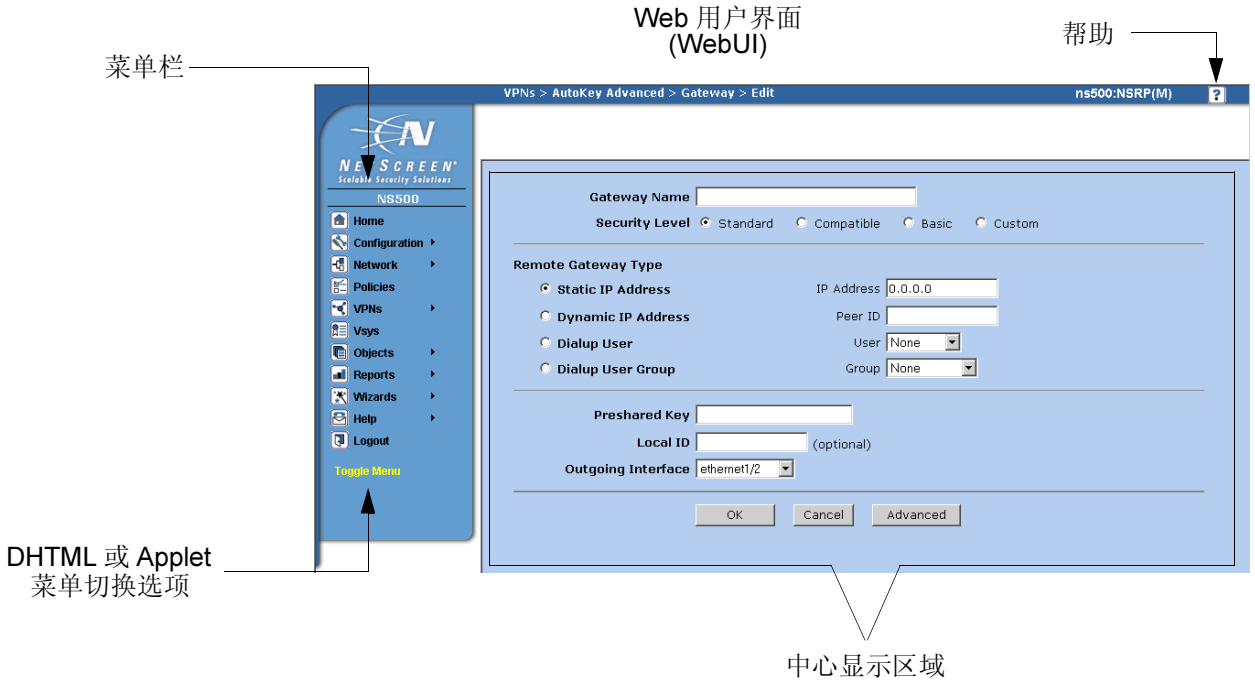
管理方法及工具

以下部分介绍管理方法以及用来应用每种方法的工具：

- 第 3 页上的 “Web 用户界面”
  - 第 8 页上的 “HTTP”
  - 第 9 页上的 “安全套接字层”
- 第 11 页上的 “命令行界面”
  - 第 11 页上的 “Telnet”
  - 第 13 页上的 “安全命令外壳”
  - 第 17 页上的 “串行控制台”
- 第 18 页上的 “NetScreen-Global PRO”

Web 用户界面

为了便于管理，您可使用 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。



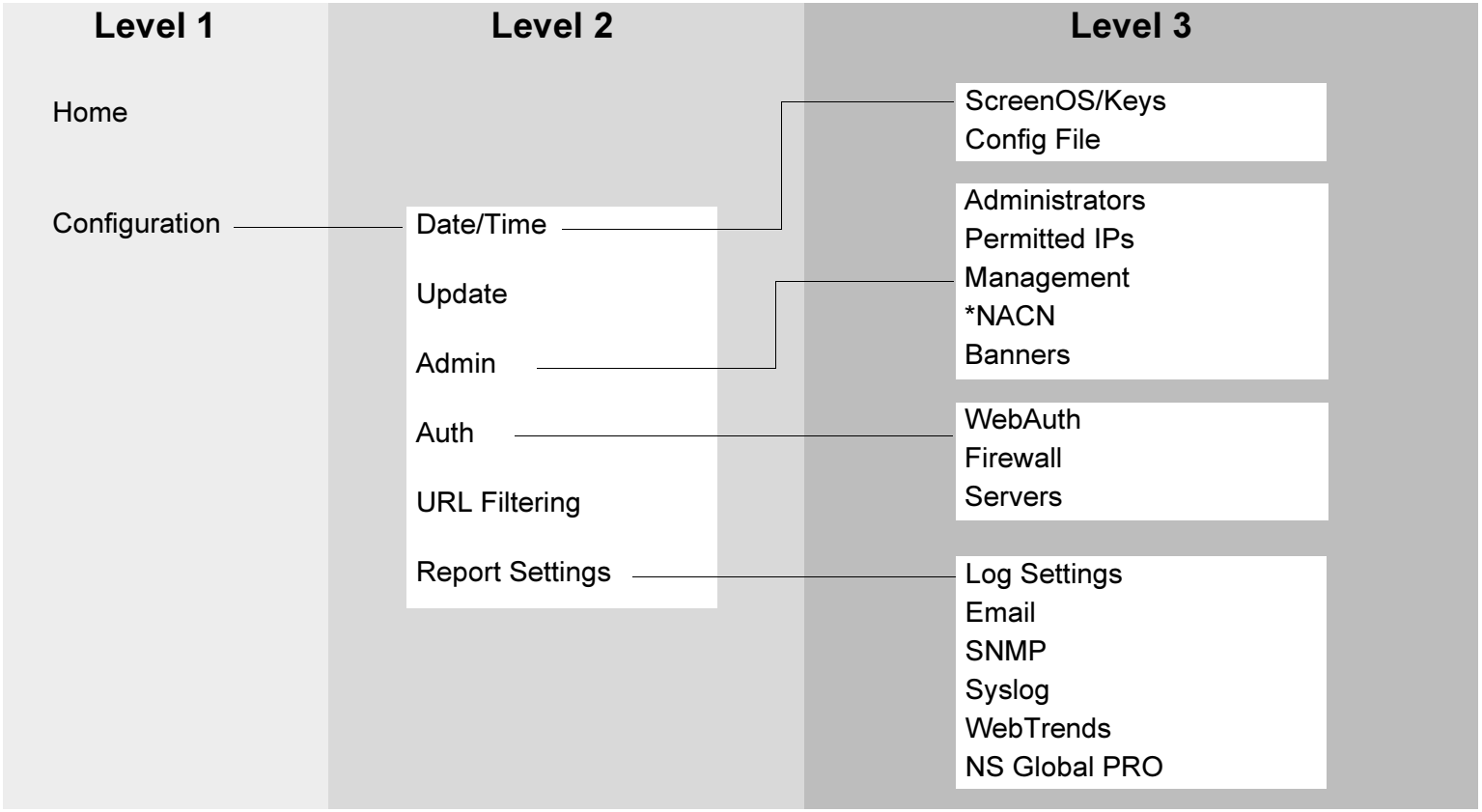
要使用 WebUI，必须具备以下条件：

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

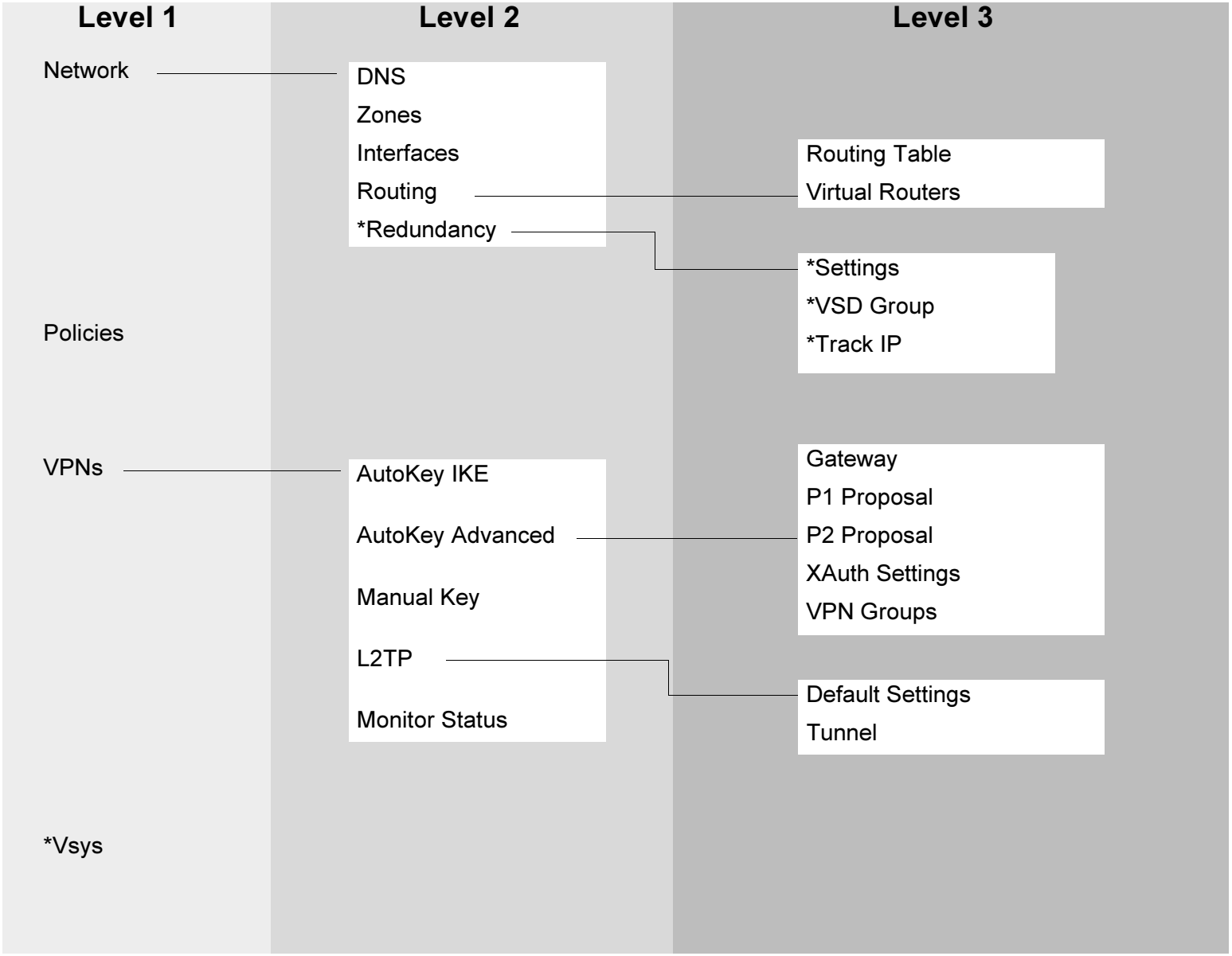
WebUI 导航级别图

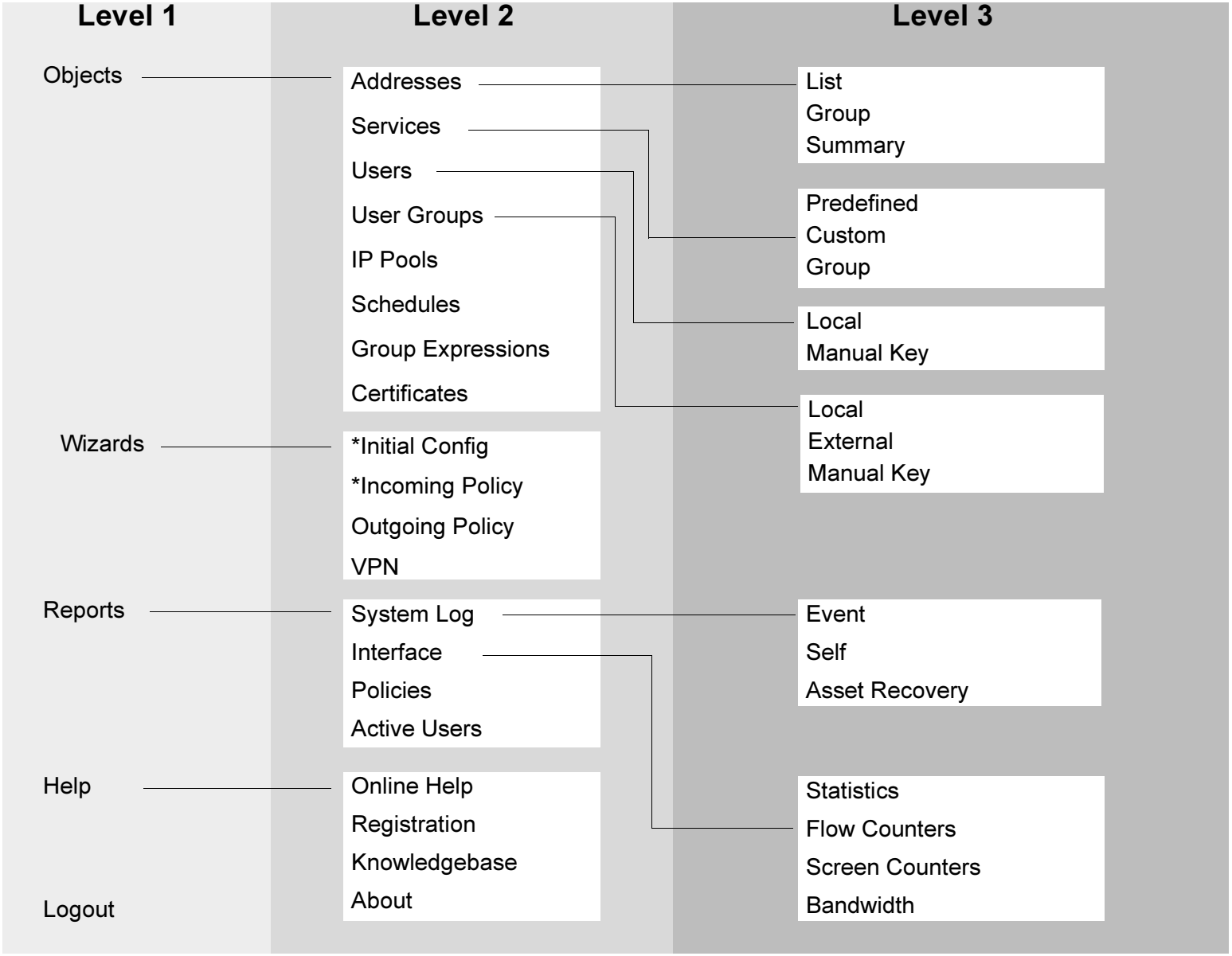
下图列出了 WebUI 中最高的三个导航级别[1]。根据 ScreenOS 功能的不同需要，可设定其它级别。

- Level 1 包含菜单栏中可见的选项。
- Level 2 包含 Level 1 中菜单项目的更具体的选项。
- Level 3 包含 Level 2 中某些选项的更具体的选项。



1. 如果在选项前有一个星号，则该选项仅可用于选定的 NetScreen 设备。


Level 1
Level 2
Level 3
Network
DNS
Zones
Interfaces
Routing
*Redundancy
Routing Table
Virtual Routers
*Settings
*VSD Group
*Track IP
Policies
VPNs
AutoKey IKE
AutoKey Advanced
Manual Key
L2TP
Monitor Status
Gateway
P1 Proposal
P2 Proposal
XAuth Settings
VPN Groups
Default Settings
Tunnel
*Vsys


Level 1
Level 2
Level 3
Objects
Addresses
List
Group
Summary
Services
Predefined
Custom
Group
Users
Local
Manual Key
User Groups
Local
External
Manual Key
IP Pools
Schedules
Group Expressions
Certificates
Wizards
*Initial Config
*Incoming Policy
Outgoing Policy
VPN
Reports
System Log
Event
Interface
Self
Policies
Asset Recovery
Active Users
Help
Online Help
Statistics
Registration
Flow Counters
Knowledgebase
Screen Counters
Logout
About
Bandwidth

WebUI 帮助

您可在 http://help.netscreen.com/help/english/<screenos_version>/ns<platform_number> 查看 WebUI 的“帮助”文件（例如， http://help.netscreen.com/help/english/4.0.0/ns500）。

还可以选择重新存放 “帮助”文件。您可能需要在本地存储它们，并将 WebUI 指向管理员的工作站或本地网络上一个安全的服务器。倘若您无法访问互联网，可以在本地存储 “帮助”文件以备使用。

将帮助文件复制到本地驱动器

“帮助”文件在文档 CD 上。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另一个驱动器，并配置 WebUI 从以上位置调用“帮助”文件。

注意： *如果您要从文档 CD 直接运行 “帮助”文件，则可以忽略此过程。继续第 8 页上的 “将 WebUI 指向新的帮助位置”。*

1. 在工作站的 CD 驱动器中加载文档 CD。
2. 找到此驱动器，然后复制命名为 help 的目录。

   Help 目录包含下列子目录：
   english/<ScreenOS_number>/ns<platform_number>。
3. 找到要存储的 Help 目录并粘贴到该位置。

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。将缺省的 URL 更改为新的文件路径，其中，

- **<path>** 是从管理员的工作站到 Help 目录的具体路径
- **<screenos_version>** 是在管理的 NetScreen 设备上加载的 ScreenOS 的版本
- **<platform_number>** 是 NetScreen 设备的平台号

1. Configuration > Admin > Management：在 Help Link Path 字段中，将缺省的 URL **http://help.netscreen.com/help/english/<screenos_version>/ns<platform_number>** 的下划线部分替换为

   （用于本地驱动器） **file://<path>/ ...**

   或

   （用于本地服务器） **http://<server_name>/<path>/ ...**

2. 单击 **Apply**。

   当单击 WebUI 右上角的 **help** 链接时，此设备使用您在 Help Link Path 字段中指定的新路径来找到合适的“帮助”文件。

HTTP

如果您使用标准的 Web 浏览器，则可通过使用 “超文本传输协议” (HTTP) 远程访问、监控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 流量或通过 “安全套接字层” (SSL) 协议保障它的安全。还可以通过将管理流量与网络用户流量完全分离来保障它的安全。如果使用一些型号的 NetScreen 设备，则可通过 MGT 接口或将一个接口 （例如， DMZ）完全专用于管理流量来运行所有的管理流量。

注意：*有关详细信息，请参阅第 43 页上的 “虚拟专用网”、“安全套接字层”（下文）和第 42 页上的 “管理区段接口”。*

安全套接字层

“安全套接字层” (SSL) 是一套协议，该套协议为在 TCP/IP 网络上通信的 Web 客户端和 Web 服务器之间提供安全的连接。 NetScreen ScreenOS 提供：

- Web SSL 支持
- SSL 版本 3 兼容性 （不是版本 2）
- Netscape Communicator 4.7x 与 Internet Explorer 5.x 兼容性[2]
- “公开密钥基础” (PKI) 密钥管理集成 （请参阅第 **4**-23 页上的 “公开密钥密码术”。）

SSL 不是单个的协议，而是由 “SSL 握手协议” (SSLHP) 组成，它允许服务器及客户端相互认证并协商一个加密方法，即“SSL 记录协议” (SSLRP)，该协议为更高级别的协议（例如， HTTP）提供了基本的安全服务。这两个协议在 “开放式系统互连” (OSI) 模式下的以下两个层中运行：

- 应用程序层第 7 层中的 SSLHP
- 演示层第 6 层中的 SSLRP

SSL 不依赖应用程序协议，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，然后在会话期间对发送的流量进行加密。使用 SSL 前，必须首先创建公开 / 私有密钥对，然后加载证书。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证书中选择 SSL 证书。还可将相同的证书用于 IPSec VPN。

注意：*有关获得证书的信息，请参阅第* ***4****-29 页上的 “证书和 CRL”。*

2. 检查您的 Web 浏览器，以查看密码的加密强度及浏览器支持的密码。（NetScreen 设备和您的 Web 浏览器必须支持用于 SSL 的相同种类及大小的密码。）在 Internet Explorer 5x 中，单击**帮助**和**关于 Internet Explorer**，然后阅读“密码的可靠性”。要获得高级的安全数据包，请单击**更新信息**链接。在 Netscape Communicator 中，单击**帮助**和**关于 Communicator**，然后阅读关于 RSA® 的部分。要更改 SSL 配置设置，请单击**安全信息** 、 **Navigator**、**配置 SSL v3**。

NetScreen 支持以下 SSL 的加密算法：

- 使用 40 位和 128 位密钥的 RC4
- DES：数据加密标准
- 3DES：三重 DES

NetScreen 支持与 VPN — “信息整理”版本 5 (MD5) 和 “加密散列算法”版本 1 (SHA-1) 相同的 SSL 认证算法。RC4 算法总是与 MD5 成对的，而 DES 和 3DES 总是与 SHA-1 成对。

设置 SSL 的基本步骤如下：

1. 获得证书并在 NetScreen 设备上加载[3]。

   有关请求并加载证书的详细信息，请参阅第 **4**-29 页上的“证书和 CRL”。

2. 启用 SSL 管理：

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

   Certificate：选择您要从下拉列表中使用的证书。

   Ciphe：选择您要从下拉列表中使用的密码。

3. 配置接口，通过该接口您可管理 NetScreen 设备，以允许进行 SSL 管理：

   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**。

4. 通过 SSL 端口连接到 NetScreen 设备。更确切的说，当您在浏览器的 URL 字段中输入管理 NetScreen 设备的 IP 地址时，将“http”更改为“https”，然后在 IP 地址后加上冒号和 HTTPS (SSL) 端口号（例如，https://123.45.67.89:1443）。

3. 确保指定 Web 浏览器也支持的长度。

命令行界面

高级管理员可通过使用命令行界面 (CLI) 进行更好的控制。要为 NetScreen 设备配置 CLI，可使用任何仿真 VT100 终端的软件。如果使用终端机仿真器，可使用 Windows、UNIX™ 或 Macintosh® 操作系统中的控制台配置 NetScreen 设备。要通过 CLI 进行远程管理，可使用 Telnet 或“安全命令外壳”(SCS)。要通过控制台端口进行直接连接，可使用“Hyperterminal®”。

注意：*有关 ScreenOS CLI 命令的完整列表，请参阅* NetScreen CLI Reference Guide。

Telnet

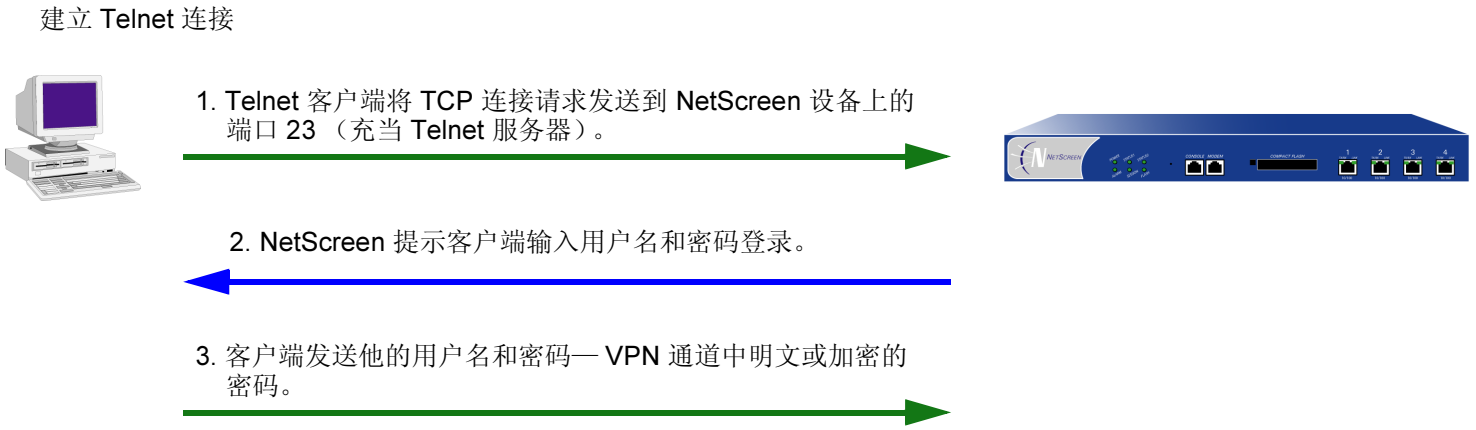
Telnet 是一个登录及终端仿真协议，该协议使用客户端 / 服务器关系连接到 TCP/IP 网络上的网络设备并进行远程配置。管理员在管理工作站上运行 Telnet 客户端程序并与 NetScreen 设备上 Telnet 服务器程序创建连接。登录后，管理员可发出 CLI 命令，将其发送到 NetScreen 设备上的 Telnet 程序，对设备进行有效的配置，好像通过直接连接运行一样。使用 Telnet 管理 NetScreen 设备需要以下条件：

- 管理工作站上有 Telnet 软件
- “以太网”连接到 NetScreen 设备

可通过在虚拟专用网 (VPN) 通道中[4] 封装 Telnet 流量或通过将其与网络用户流量完全分离来保障它的安全。可通过 MGT 接口或将一个接口 （例如， DMZ）完全专用于管理流量来运行所有的管理流量，具体取决于 NetScreen 设备型号。

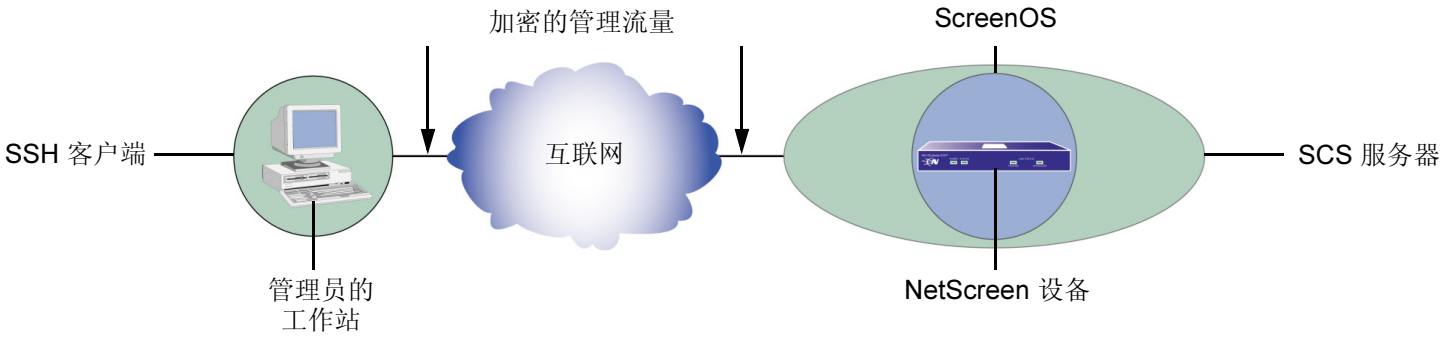
4. 有关 VPN 通道的信息，请参阅第 4 卷和 “VPN”。

建立 Telnet 连接的设置过程如下：



安全命令外壳

NetScreen 设备中内置的 “安全命令外壳” (SCS) 服务器提供一种方法，凭借这种方法，管理员可通过使用 “安全外壳” (SSH) 以一种安全的方式远程管理该设备。SSH 允许安全地打开远程的命令外壳并执行这些命令。NetScreen 设备上运行的 SCS 任务是执行 SSH 1.x 服务器组件，它允许 SSH 1.x 兼容的客户端控制台 / 终端应用程序连接到 NetScreen 设备。



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：**需要进行配置或监控 NetScreen 设备的管理员通常使用此方法。 SSH 客户端启用 SSH 连接到 NetScreen 设备。如果在接收连接请求的接口上启用 SCS 可管理性，则 NetScreen 设备用信号通知 SSH 客户端，以提示用户输入用户名和密码。SSH 客户端收到此信息后，会将之发送到 NetScreen 设备，它将其与 admin 用户帐户的用户名和密码进行比较。如果它们匹配，NetScreen 设备就认证此用户。如果它们不匹配，NetScreen 设备就拒绝连接请求。
- **公开密钥认证 (PKA)：**此方法增强了密码认证的安全性并允许自动运行脚本。通常， SSH 客户端不发送用户名和密码，而是发送用户名和 RSA 公开 / 私有密钥对的公开密钥组件。NetScreen 设备将其与四个公开密钥（可绑定到 admin）进行比较。如果其中一个密钥匹配，NetScreen 设备就认证此用户。如果其中没有一个匹配， NetScreen 设备就拒绝连接请求。

这两种认证方法都需要在 SSH 客户端登录前建立一个安全的连接。基本连接设置过程如下所示：

为 SSH 建立一个安全连接

1. SSH 客户端将 TCP 连接请求发送到 NetScreen 设备上的端口 22 （充当 SCS 服务器）。

2. NetScreen 与客户端交换关于它们支持的 SSH 版本的信息。

3. NetScreen 发送其主机和服务器密钥的公开组件、cookie、及其支持的加密和认证算法。

4. 客户端创建一个会话密钥，并使用 NetScreen 主机和服务器密钥的公开组件对其进行加密，然后将会话密钥发送到 NetScreen。

5. NetScreen 发送一条确认信息，即它已对会话密钥进行加密。安全通道即创建完成。

6. NetScreen 发信号通知 SSH 客户端以提示最终用户认证信息。

7. 客户端加密用户名和密码或 PKA 密钥的公开组件，然后将其发送进行认证。

密钥

主机密钥：持久的 RSA 公开 / 私有密钥对用于认证 NetScreen 设备并加密会话密钥（NetScreen 将其存储在快速存储器中）。

服务器密钥：临时的 RSA 公开 / 私有密钥对用于加密会话密钥（在缺省情况下，NetScreen 每小时生成一个新的密钥）。

会话密钥：在连接设置期间，客户端与 NetScreen 共同创建临时的密钥（DES 或 3DES），以对通信加密（会话结束时，它将被废除）。

PKA 密钥：持久的 RSA 公开 / 私有密钥对驻留于 SSH 客户端。启动 SSH 连接前，必须在 NetScreen 设备上加载客户端的公开密钥。

注意：*公开 / 私有密钥对 = 一对加密密钥，一个密钥加密的内容，可以且只能用另一个密钥解密。*

SSH 客户端与 NetScreen 设备建立 SSH 连接后，他必须输入用户名和密码或用户名和公开密钥认证他自己。

密码认证和 PKA 需要在 NetScreen 设备上为 admin 用户创建一个帐户，然后在接口上通过要管理的 NetScreen 设备（通过 SSH 连接进行管理）启用 SCS 可管理性。（有关创建 admin 用户帐户的信息，请参阅第 29 页上的 “定义 Admin 用户”）。密码认证方法不需要在 SSH 客户端上进行任何其它设置。

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，生成 RSA 公开和私有密钥对。

   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，以加密 PKA 公开 / 私有密钥对的私有密钥组件，并在存储器中保存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[5]上的目录，然后运行 TFTP 程序。
3. 登录到 NetScreen 设备，以便可通过 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，可输入以下 CLI 命令：

   exec scs tftp pka-rsa [username *name* **] file-name** *name_str* **ip-addr** *tftp_ip_addr*

   username *name* 选项仅用于根 admin，因此只有根 admin 可以将 RSA 密钥绑定到另一个 admn。当您 — 作为根 admin 或可读 / 写管理 — 只输入命令没有输入用户名时，NetScreen 设备将密钥绑定到您自己的 admin 帐户；即它绑定密钥到输入命令的 admin。

   注意：*对于每个 admin 用户， NetScreen 设备可支持四个 PKA 公开密钥。*

5. 还可以将公开密钥文件内容直接粘贴到 CLI 命令 **set scs pka-rsa [username** *name_str* **] key** *key_str*，（粘贴到显示变量 *key_str* 的地方）或粘贴到 WebUI 中 Key 字段 (Configuration > Admin > Management > SCS)。但是， CLI 与 WebUI 有大小限制：公开密钥大小不可超过 512 位。通过 TFTP 加载密钥时，不存在此限制。

管理员尝试通过已启用 SCS 可管理性的界面上的 SCS 登录，NetScreen 设备首先检查是否公开密钥被绑定到那个管理员。如果是这样的话， NetScreen 设备就使用 PKA 认证此管理员。如果某个公开密钥没有被绑定到管理员，那么 NetScreen 设备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 scs password disable username** *name_str*。）无论您要管理员使用哪种认证方法，当您初次定义他或她的帐户时，仍然要定义密码，即使后来将公开密钥绑定到此用户 （该密码才无效）。

范例：SCS 使用 PKA 进行自动登录

在此范例中，请您 （作为根 admin）为自动运行脚本的远程主机设置 SCS 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 设备时无须人员操作。

您定义了一个 admin 用户帐户，名为 cfg，密码为 cfg，还有读写权限。可在接口 ethernet1（被绑定到 Untrust 区段）上启用 SCS 可管理性。

您以前已经在 SSH 客户端上使用过密钥生成程序以生成 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 服务器上的目录中，然后运行 TFTP 程序。 TFTP 服务器的 IP 地址是 10.1.1.5。

WebUI

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

   Name: cfg

   New Password: cfg

   Confirm Password: cfg

   Privileges: ALL （选择）

2. Interfaces > Edit（对于 ethernet1）：选择 **SCS**，然后单击 **OK**。

> ***注意：****您只可通过* ***exec scs*** *命令从 TFTP 服务器加载 SCS 的公开密钥文件 。*

CLI

1. set admin user cfg password cfg privilege read-write
2. set interface ethernet1 manage scs
3. exec scs tftp pka-rsa username cfg file-name idnt_cfg.pub ip-addr 10.1.1.5
4. save

串行控制台

可通过直接的串行连接（通过控制台端口从管理员工作站连接到 NetScreen 设备）管理 NetScreen 设备。不可能始终实现直接连接，但是如果 NetScreen 设备周围是安全的，那么这种连接就是管理设备最安全的方法。

根据 NetScreen 设备模式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 终端机仿真器），“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 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”一章或安装程序指南的“Initial Configuration”一章。*

NetScreen-Global PRO

安全管理解决方案的 NetScreen-Global PRO 系列由两个产品组成，它们提供从中央位置大规模配置 NetScreen 设备的配置和监控能力。

- NetScreen-Global PRO
- NetScreen-Global PRO Express

使用 NetScreen-Global PRO，可从单一的位置管理多达 10,000 个 NetScreen 设备。 Policy Manager 组件允许您将策略配置到 NetScreen 设备。 Report Manager 组件提供系统事件和攻击警报的实时与历史报告。

使用 NetScreen-Global PRO Express，可从单一的位置管理多达 100 个 NetScreen 设备。 NetScreen-Global PRO Express 将 Policy Manager 与实时监控器和 Report Manager 的实时报告组件组合在一起。

NetScreen-Global PRO 采用基于任务的管理方案，使得具有多种权限级别和访问权限的多个管理员可进行安全的、并发的访问。这些管理员可访问 NetScreen-Global PRO 系统的相关区域以更改配置并查看报告和统计。

注意： *有关详细信息，请参阅 NetScreen-Global PRO 文档。*

NetScreen 地址更改通知 (NACN)

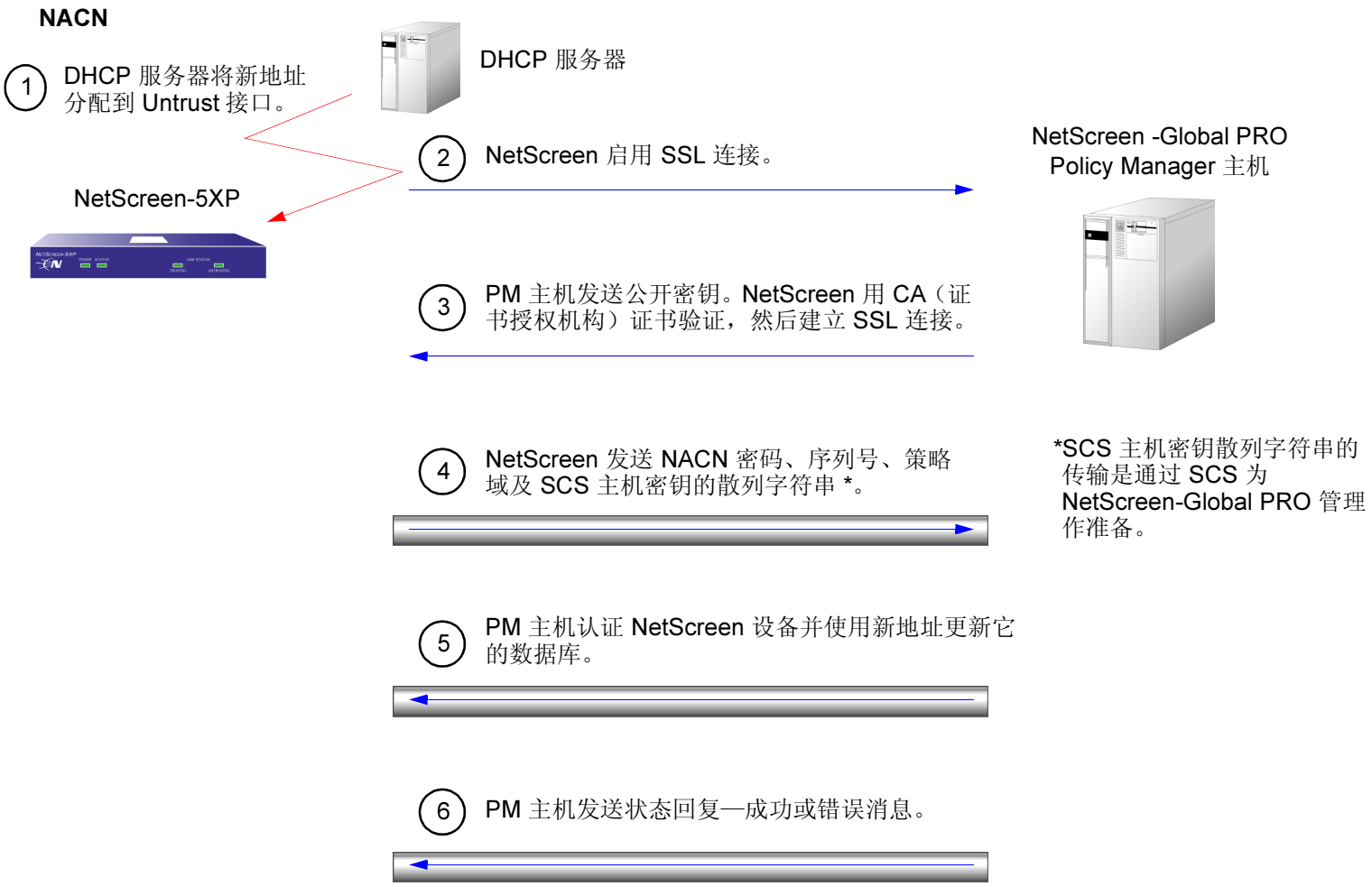
NetScreen-Global PRO Policy Manager 主机（或“PM 主机”）联系 NetScreen 设备前，必须具有 NetScreen 设备接口当前的 IP 地址。如果 NetScreen 设备在其监视器接口上有一个静态的 IP 地址，则这样相对容易些。

但是， NetScreen 设备的监视器界面可能有一个动态分配的 IP 地址，该 IP 地址使用“以太网点对点协议”(PPPoE) 或“动态主机配置协议”(DHCP)。在这些情况下，NetScreen 设备使用“NetScreen 地址更改通知”(NACN) 以监控特定的接口（请参阅下文的“监控器接口”），然后当监控器接口的 IP 地址更改时，向 NetScreen-Global PRO 注册。

如果在 NetScreen 设备 （NetScreen-Global PRO PM 主机[6]）上启用 NACN，该设备将以任何 PPPoE 或 DHCP 分配的新地址自动向 NetScreen-Global PRO 注册。这将预防 NetScreen-Global PRO 与 NetScreen 设备之间的通信中断。

6. 您必须在 NetScreen-Global PRO PM 主机上输入 NetScreen 设备的序列号和 NACN 密码。有关详细信息，请参阅 NetScreen-Global PRO 文档。

NetScreen 设备使用“安全套接外壳”(SSL) 以加密与 NetScreen-Global PRO 的通信。此交换过程如以下图解所示：



注意：*有关 SSL 的详细信息，请参阅第 9 页上的“安全套接字层”。*

除了配置和启用 NACN 之外，还必须完成以下任务：

- 输入 NetScreen-Global PRO 一级 （和二级） Policy Manager (PM) 主机的 IP 地址和 NACN 密码。
- 在该接口上确定监控器接口并启用 SCS 或 Telnet[7] （或两者）的可管理性。
- 在 NetScreen 设备上设置系统时钟。
- 在 NetScreen 设备上激活预先安装的 CA 证书。
- （可选的）在 Global PRO 服务器上输入 X.509 证书的主题名称以防拦截式攻击。

范例：设置 NACN

在以下范例中，可启用 NetScreen 设备上的 NACN 并配置下列 NACN 设置：

- 一级 PM 主机 IP 地址及密码：210.3.3.1; swordfish
- 二级 PM 主机 IP 地址：210.3.3.2; trout
- 一级和二级 PM 主机上的策略域：dept1
- 监控器接口：Untrust
- 端口：11122
- PM 主机发送的本地证书的主题名称：

  CN=Marketing,OU=Marketing,O=Ajax,L=Chicago,ST=IL,C=US,Email=jdoe@ajax.com

使用 CLI，在 NetScreen 设备上激活预先安装的 NetScreen CA 证书 “phonehome1ca1”。当 NetScreen 设备对 NetScreen-Global PRO PM 主机启用 SSL 连接时，此 CA 证书可验证 PM 主机发送的缺省的本地证书。

当 NetScreen 设备上的监控器接口的 IP 地址更改时， NetScreen 设备在一级 PM 主机 （IP 地址为 210.3.3.1）上使用 NACN 协议启用到端口 11122 的 SSL 连接。

还可以在 NetScreen 设备上启用 SCS 服务器，然后在不信任接口启用 SCS 可管理性。

7. NetScreen-Global PRO 可使用 “安全命令外壳” (SCS) 或 Telnet 将配置的更改内容发送到 NetScreen 设备。为了安全起见，NetScreen 建议您使用 SCS。

WebUI

一级和二级 PM 主机

> ***注意：****可通过 CLI 命令* ***exec pki x509 install-factory-certs phonehome1ca1*** *仅激活预先安装的 CA 证书“phonehome1ca1”。*

1. Configuration > Admin > NACN：输入以下内容，然后单击 **Apply**：

   Enable NACN: （选择）

   Primary PM Host

   Hostname/IP Address: 210.3.3.1

   Password: swordfish

   Policy Domain: dept1[8]

   Monitored Interface: Untrust

   Port: 11122

   Selected CA: OU=(c) 2001 NetScreen Technologies

   Cert Subject Name: CN=Marketing,OU=Marketing,O=Ajax,L=Chicago,ST=IL,C=US,Email=jdoe@ajax.com,[9]

8. 定义策略域并不是必需的，但是这样做可在 Global PRO 数据库潜在的大量策略域中迅速地搜索到 NetScreen 设备。
9. 确保在 Cert Subject Name 字符串的结尾加上逗号。此证书名称与 Policy Manager 控制台登录到 Policy Manager 主机所使用的证书名称一致。有关详细信息，请参阅 NetScreen-Global PRO 文档。

Secondary PM Host

Hostname/IP Address: 210.3.3.2

Password: trout

Policy Domain: dept1

Monitored Interface: Untrust

Port: 11122

Selected CA: OU=(c) 2001 NetScreen Technologies

Cert Subject Name:
CN=Marketing,OU=Marketing,O=Ajax,L=Chicago,ST=IL,C=US,Email=jdoe@ajax.com,

SCS

2. Configuration > Admin > Management：选择 **Enable SCS** 复选框，然后单击 **Apply**。
3. Network > Interfaces > Edit（对于 untrust）：输入以下内容，然后单击 **OK**：

   Management Services:

   SCS: （选择）

CLI

1. exec pki x509 install-factory-certs phonehome1CA1

   注意：*以下命令，* ***get ssl ca-list****，显示当前激活的 CA 证书，以及它们的 ID 号。在此范例中，假设列出的 CA 证书中有一个证书的 ID 号为 2。*

2. get ssl ca-list

一级 PM 主机

3. set global-pro policy-manager primary ca-idx 2
4. set global-pro policy-manager primary cert-subject “CN=Marketing,OU=Marketing,O=Ajax,L=Chicago,ST=IL,C=US,Email=jdoe@ajax.com,”[10]
5. set global-pro policy-manager primary outgoing untrust
6. set global-pro policy-manager primary host 210.3.3.1
7. set global-pro policy-manager primary password swordfish
8. set global-pro policy-manager primary policy-domain dept1

二级 PM 主机

9. set global-pro policy-manager secondary ca-idx 2
10. set global-pro policy-manager secondary cert-subject “CN=Marketing,OU=Marketing,O=Ajax,L=Chicago,ST=IL,C=US,Email=jdoe@ajax.com,”
11. set global-pro policy-manager secondary outgoing untrust
12. set global-pro policy-manager secondary host 210.3.3.2
13. set global-pro policy-manager secondary password trout
14. set global-pro policy-manager secondary policy-domain dept1

SCS

15. set scs enable
16. set interface untrust manage scs
17. set global-pro policy-manager nacn
18. save

10. 确保在“Cert Subject Name”字符串的结尾加上逗号。此证书名称与 Policy Manager 控制台登录到 Policy Manager 主机所使用的证书名称一致。有关详细信息，请参阅 NetScreen-Global PRO 资料。

管理接口选项

可将 NetScreen 设备配置为允许通过一个或多个接口对设备进行管理。例如，可通过将接口绑定到 Trust 区段对设备进行本地管理访问，还可通过将接口绑定到 Untrust 区段对设备进行远程管理。在 NetScreen 设备上有多个网络流量的物理接口 （但是没有专用的管理接口），您可以将一个物理接口专用于管理，以将管理流量与网络用户流量完全分离。

注意：*（透明模式）要启用管理信息流到达 VLAN1，您必须同时在 VLAN1 接口和伪接口或管理信息流通过以到达 VLAN1 的接口 （V1-Trust、 V1-Untrust、 V1-DMZ、用户定义第二层接口）上启用您想要的管理选项。*

要启用一个接口以允许使用多种管理方法通过 WebUI 和 CLI 穿越该接口，请执行以下操作：

WebUI

Network > Interfaces > Edit（对于要编辑的接口）：选择下面要启用的管理服务选项，然后单击 **OK**[11]：

WebUI：选择此选项以允许接口通过 Web 用户界面 (WebUI) 接收管理的 HTTP 流量。

Telnet：是 TCP/IP 网络的终端仿真程序，例如，互联网。 Telnet 是远程控制网络设备常见的方式。选择此选项可启用 Telnet 可管理性。

SCS：可使用与 SSH 兼容的“安全命令外壳”(SCS) 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 及其更高的版本、Windows NT、 Linux 和 UNIX。 NetScreen 设备通过内置的 SCS 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 SCS 可管理性。

11. 通过 CLI，可使 NetScreen 设备在便于保持不中断网络操作的时间定期重置：**set timer** *date_str time_str* **action reset**。

SNMP：NetScreen 设备支持 RFC-1157 中所述的“简单网络管理协议”版本 1.5 (SNMPv1) 和 RFC-1213 中所述的所有相关的“管理信息库 II”(MIB II) 组。选择此选项可启用 SNMP 可管理性。

SSL：选择此选项以允许接口通过 WebUI 接收 NetScreen 设备安全管理的 HTTPS 流量。

NS-Global PRO：选择此选项可允许接口接收 NetScreen-Global PRO 流量。

Ping：选择此选项允许 NetScreen 设备响应 ICMP 回应请求或“ping”，它确定是否可以在网络上访问特定的 IP 地址。

Ident-Reset：类似发送标识请求的“邮件”或 FTP 服务。如果他们没有接收到确认，他们会再次发送请求。处理请求时，没有用户可以进行访问。通过启用“Ident-reset”选项， NetScreen 设备发送 TCP 重设通知以回复发送到端口 113 的 IDENT （标识）请求，然后恢复因未确认标识请求而被锁定的访问。

CLI

要启用所有管理服务及 ping（但是不启用 ident-reset）：

```
set interface interface manage
```

要启用特定的管理及网络服务：

```
set interface interface manage { global-pro | ident-reset | ping | scs | snmp | ssl | telnet | web }
```

管理的级别

NetScreen 设备支持多个管理用户。对于管理员进行的任何配置的更改， NetScreen 设备记录以下信息：

- 进行更改的管理员的姓名
- 进行更改的 IP 地址
- 更改的时间

有几个管理用户的级别。这些级别的可用性取决于 NetScreen 设备的模式。以下部分列出了所有的 admin 级别，以及每一级别的特权。仅当 admin 用有效的用户名和密码成功登录后，才能访问这些特权。

根管理员

根管理员具有完全的管理权限。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、删除和管理所有其他的管理员
- 建立和管理虚拟系统，然后为它们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
- 分配接口到安全区段

可读 / 写管理员

可读 / 写管理员具有与根管理员相同的权限，但是他不能创建、修改或删除其他的 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
- 监控任何虚拟系统
- 跟踪统计 （一个虚拟系统管理员所不具有的权限）

只读管理员

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

- 在根系统中具有只读权限，可使用以下四种命令：**enter**、 **exit**、 **get** 和 **ping**
- 在虚拟系统中具有只读权限

虚拟系统网络管理员

某些 NetScreen 设备支持虚拟系统。每个虚拟系统 (vsys) 是一个唯一安全的域，具有仅应用于 vsys 权限的虚拟系统网络管理员可管理虚拟系统。虚拟系统网络管理员通过 CLI 或 WebUI 独立地对虚拟系统进行管理。在每个 vsys 上，虚拟系统网络管理员具有以下权限：

- 创建并编辑 auth、 IKE、 L2TP、 XAuth 和 “手动密钥”用户
- 创建并编辑服务
- 创建并编辑策略
- 创建并编辑地址
- 创建并编辑 VPN
- 修改虚拟系统网络管理员的登录密码
- 添加并管理安全区段

虚拟系统只读管理员

虚拟系统只读管理员具有与只读管理员相同的权限，但是仅限于特定的虚拟系统中。虚拟系统只读管理员具有使用 WebUI 查看特定的 vsys 的权限，他只能在他的 vsys 中发出 **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* ***6-1*** *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。在以下范例中，执行此过程的管理员一定是根管理员。

范例：添加只读 Admin

在此范例中，您—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 Password: 2bd21wG7

Privileges: READ ONLY

CLI

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

12. 密码最长可为 31 字符并且区分大小写。

范例：修改 Admin

在此范例中，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 Password: 2bd21wG7

Privileges: ALL

CLI

1. set admin user Roger password 2bd21wG7 privilege all
2. save

范例：删除 Admin

在此范例中，您—作为根 admin —删除 admin 用户 Roger。

WebUI

Configuration > Admin > Administrators：在“Configure”栏中为 Roger 单击 **Remove**。

CLI

1. unset admin user Roger
2. save

保证管理流量的安全

要在设置期间保证 NetScreen 设备的安全，请执行以下步骤：

1. 在 Web 界面，更改管理端口。

   请参阅第 32 页上的“更改端口号”。

2. 更改用户名和密码，以便管理访问。

   请参阅第 33 页上的“更改 Admin 登录名和密码”。

3. 为 admin 用户定义管理客户端的 IP 地址。

   请参阅第 37 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 25 页上的“管理接口选项”。

5. 禁用接口上的 ping 和 ident-reset 服务选项，两者都响应未知方发起的请求，并能显示有关网络的信息：

   ### *WebUI*

   Network > Interfaces > Edit（对于要编辑的接口）：禁用下列设备选项，然后单击 **OK**：

   Ping：选择此选项允许 NetScreen 设备响应 ICMP 回应请求或“ping”，它确定是否可从设备到达特定的 IP 地址。

   Ident-Reset：当服务（如“邮件”或 FTP）发送标识请求并且没有收到肯定应答时，它再次发送请求。尽管请求进行中，但禁止用户访问权限。“Ident-Reset”复选框启用时，NetScreen 设备自动恢复用户访问权限。

CLI

unset interface *interface* manage ping

unset interface *interface* manage ident-reset

更改端口号

更改 NetScreen 设备监听的端口号，以提高 HTTP 管理流量的安全性。缺省设置为端口 80，它是 HTTP 流量的标准端口号。更改端口号后，在下次尝试联系 NetScreen 设备时，必须在 Web 浏览器的 URL 字段中键入新的端口号。（下例中，管理员必须输入 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，则必须使用 HTTP。要增加 HTTP 连接的安全性，应将 HTTP 端口号从 80 （缺省值）更改为 15522。

WebUI

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

CLI

1. set admin port 15522
2. save

更改 Admin 登录名和密码

缺省情况下，NetScreen 设备初始的登录名为 netscreen。初始密码也为 netscreen。由于它们已众所周知，因此应立即更改登录名和密码。登录名和密码都区分大小写。每个都必须为一个单词、字母数字，但是不能有符号。用安全的方式记录新的 admin 登录名和密码。

警告： *务必记录新的密码。如果将它忘记，则必须将 NetScreen 设备重置到出厂设置，并且将丢失所有的配置。有关详细信息，请参阅第 36 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认证服务器认证 NetScreen 设备的 Admin 用户[13]。admin 用户登录到 NetScreen 设备时，它首先检查本地内部数据库，以便进行认证。如果不存在条目，并且连接了外部认证服务器，则它在外部认证服务器数据库中检查匹配条目。admin 用户成功登录到外部认证服务器后，NetScreen 设备本地高速缓存来自外部认证服务器的该 admin 的登录状态。当 admin 用户通过 WebUI 管理或监控 NetScreen 设备时，每当 admin 用户单击一个链接时，高速缓存的数据迅速加快进行 HTTP 要求的连续认证检查。通过参考本地高速缓存，NetScreen 设备不必中继用户和外部认证服务器间的认证检查，因此可以提供对用户操作的更快响应。

注意： *有关 admin 用户级别的详细信息，请参阅第 27 页上的 “管理的级别”。有关使用外部认证服务器的详细信息，请参阅第 **2** -254 页上的 “外部 Auth 服务器”。*

当根 admin 更改 admin 用户简介的任何属性—用户名、密码或权限时—admin 当前打开的任何 admin 会话自动终止。如果根 admin 为自己更改这些属性的任何一个部分，或者如果根级读 / 写 admin 或 vsys 读 / 写 admin 更改自己的密码，则用户当前打开的所有 admin 会话[14] 终止，除进行更改的会话外。

13. NetScreen 支持 admin 用户认证的 RADIUS、SecurID 和 LDAP 服务器。（有关详细信息，请参阅第 **2** -340 页上的 “Admin 用户”。）尽管根 admin 帐户必须存储在本地数据库中，但是可以在外部认证服务器中存储根级读 / 写和根级只读 admin 用户。要在外部认证服务器上存储根级和 vsys 级 admin 用户并查询他们的权限，服务器必须是 RADIUS，并且必须在服务器上加载 netscreen.dct 文件。（请参阅第 **2** -259 页上的 “NetScreen 词典文件”。）

14. HTTP 或 HTTPS 会话使用 WebUI 的方式是不同的。因为 HTTP 不支持持久连接，因此对自己的用户简介所作的任何更改，将自动注销该会话和所有打开的其它会话。

范例：更改 Admin 用户的登录名和密码

根管理员决定将超级管理员的登录名由 John 更改为 Smith，密码由 xL7s62a1 更改为 3MAb99j2[15]。

注意：*有关管理员不同级别的信息，请参阅第 27 页上的 “管理的级别”。*

WebUI

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

Name: Smith

Old Password: xL7s62a1

New Password: 3MAb99j2

Confirm Password: 3MAb99j2

CLI

1. unset admin user John
2. set admin user Smith password 3MAb99j2 privilege all
3. save

15. 避免使用实际词作为密码，因为这样可通过词典式攻击猜到或发现该密码，可以使用字母和数字组成的随机字符串。要创建这种易于记忆的字符串，可编写一句话并使用每个词的第一个字母。例如，“Charles will be 6 years old on November 21”变成 “Cwb6yooN21”。

范例：更改自己的密码

非根用户可以更改他们自己的管理员密码，但是不能更改他们的登录名。在本例中，登录名为“starling”的超级管理员将她的密码从 3MAb99j2 更改为 ru494Vq5。

WebUI

Configuration > Admin > Administrators > Edit（对于第一个条目）：输入以下内容，然后单击 **OK**：

Name: starling

Old Password: 3MAb99j2

New Password: ru494Vq5

Confirm Password: ru494Vq5

CLI

1. set admin password ru494Vq5
2. save

重置设备到出厂缺省设置

如果丢失 admin 密码，则可以使用下列步骤将 NetScreen 设备重置到其缺省设置。配置将丢失，但是对设备的访问将恢复。要执行此操作，需要建立控制台连接，在 *NetScreen CLI Reference Guide* 和安装指南中对其进行了详细描述。

注意：*缺省情况下，设备恢复特征被启用。可通过输入* ***unset admin device-reset*** *命令禁用它。同样，如果 NetScreen 设备处于 FIPS 模式，恢复特征被自动禁用。*

1. 在登录提示下，键入设备的序列号。
2. 在密码提示下，再次键入序列号。

   出现以下消息：

   !!!! 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
   （!!!! 丢失密码重置 !!!! 您已发出将设备重置为出厂缺省值的命令，这将清除所有当前配置、密钥和设置。是否要继续 ? y/n）
3. 按 **y** 键。

   出现以下消息：

   !! 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
   （!! 重新确认丢失密码重置 !! 如果继续，设备的全部配置都将被拭除。另外，永久性计数器将递增，以指示此设备已被重置。这是您取消此命令的最后机会。如果继续，设备将返回出厂缺省值，即：系统 IP：192.168.1.1; 用户名：netscreen; 密码：netscreen。是否要继续 ? y/n）
4. 按 **y** 键，重置设备。

   现在可以用 *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。缺省情况下，可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： *管理客户端 IP 地址的指派立即生效。如果通过网络连接对设备进行管理，而工作站不包括在指派中，则 NetScreen 设备立即终止当前会话，并且不再能从该工作站管理设备。*

范例：限制对单一工作站的管理

在本例中， IP 地址为 172.16.40.42 的工作站管理员是指定管理 NetScreen 设备的唯一管理员。

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

1. set admin manager-ip 172.16.40.42/32
2. save

范例：限制对子网的管理

在本例中， 172.16.40.0/24 子网中的一组工作站管理员被指定管理 NetScreen 设备。

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

1. set admin manager-ip 172.16.40.0 255.255.255.0
2. save

管理 IP

任何绑定到安全区段的接口都至少可以具有两个 IP 地址：

- 一个连接到网络的接口 IP 地址。
- 一个用于接收管理流量的逻辑管理 IP 地址。

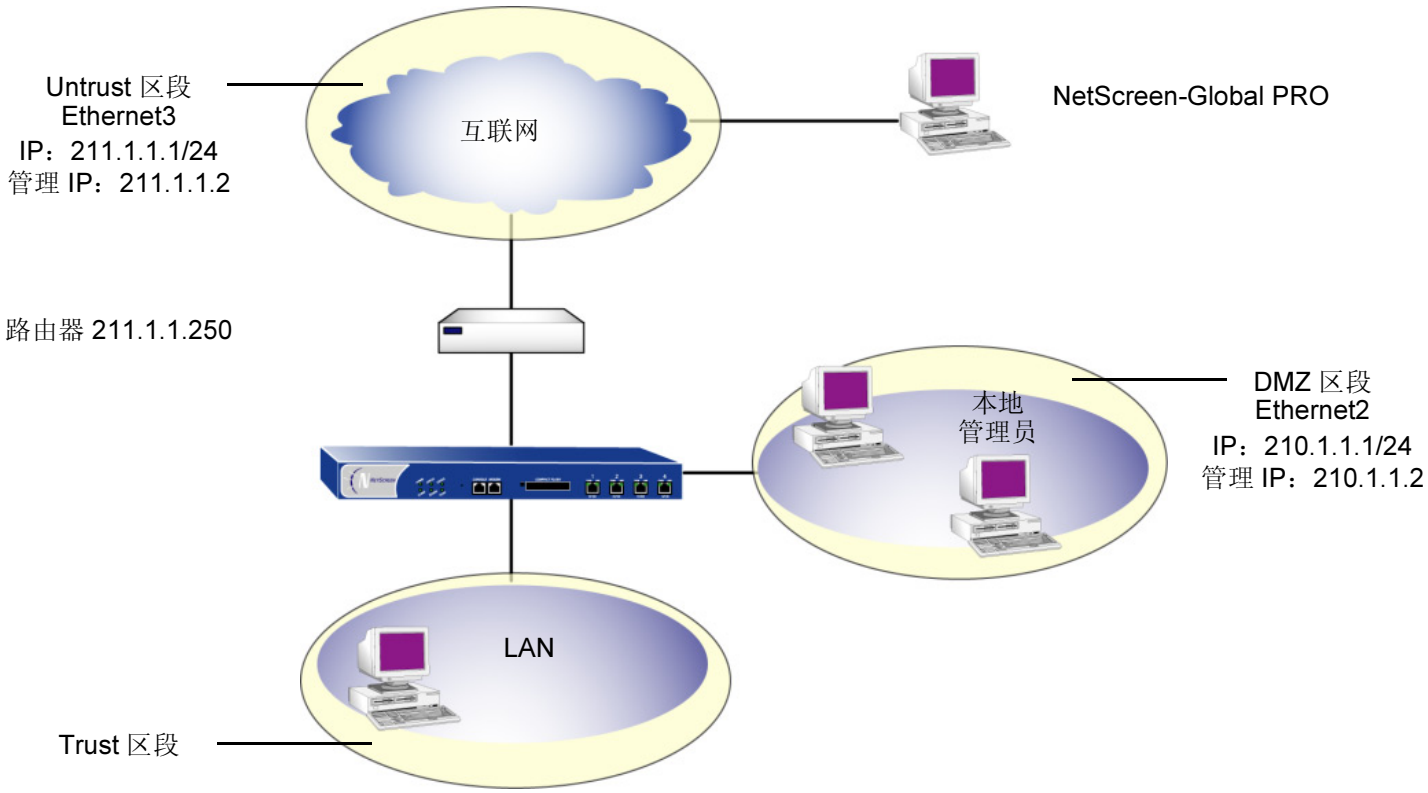
NetScreen 设备为“高可用性 (HA)”冗余组中的备份设备时，可通过设备的管理 IP 地址（一个或多个地址）进行访问和配置。

注意：*管理 IP 地址在以下两个方面与 VLAN1 地址不同：*

- *NetScreen 设备处于“透明”模式时， VLAN1 IP 地址可以是 VPN 通道的端点，但是管理 IP 地址不能是 VPN 通道的端点。*
- *可以定义多个管理 IP 地址，每个网络接口一个；但是对于整个系统只能定义一个 VLAN1 IP 地址。*

范例：设置多个接口的管理 IP

在本例中， ethernet2 被绑定到 DMZ 区段，而 ethernet3 被绑定到 Untrust 区段。在每个接口设置管理选项，以提供使用每个接口对特定种类管理流量的访问。允许 HTTP、 SNMP 和 Telnet 在 ethernet2 上访问 DMZ 区段中的一组本地管理员， NetScreen-Global PRO 在 ethernet3 上从远程站点访问中央管理。Ethernet2 和 ethernet3 都有一个管理 IP 地址，指向不同种类的管理流量。



***注意：**也需要设置将自行生成的 NetScreen-Global PRO 流量直接路由到使用 ethernet3，以到达 IP 地址为 211.1.1.250 的外部路由器。将自行生成的 SNMP 流量路由到 DMZ 区段中的 SNMP 公共组是不必要的，因为公共组在本地附加的子网中。*

WebUI

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

   Zone Name: DMZ

   IP Address/Netmask: 210.1.1.1/24

   Manage IP: 210.1.1.2

   Management Services: WebUI, Telnet, SNMP: （选择）

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

   Zone Name: Untrust

   IP Address/Netmask: 211.1.1.1/24

   Manage IP: 211.1.1.2

   Management Services: NS-Global PRO: （选择）

CLI

1. set interface ethernet2 ip 210.1.1.1/24
2. set interface ethernet2 manage-ip 210.1.1.2
3. set interface ethernet2 manage web
4. set interface ethernet2 manage telnet
5. set interface ethernet2 manage snmp
6. set interface ethernet3 ip 211.1.1.1/24
7. set interface ethernet3 manage-ip 211.1.1.2
8. set interface ethernet3 manage global-pro
9. save

管理区段接口

在缺省情况下，有两种接口绑定到 “管理 (MGT)” 区段：

- **VLAN1**：以 “透明” 模式运行 NetScreen 设备时，使用此接口终止管理流量和 VPN 通道。以 “透明” 模式操作时，可将所有 NetScreen 设备配置为允许通过 VLAN1 接口进行管理。
- **MGT**：某些 NetScreen 设备也具有一个物理接口—管理 (MGT) —专用于管理流量。以 NAT 或 “路由” 模式运行 NetScreen 设备时，使用此接口管理流量。

要保持最高级的安全性，NetScreen 建议限制管理流量专用 VLAN1 或 MGT 接口，而用户流量专用安全区段接口。从网络用户流量分离管理流量大大增加了管理安全性，并确保了稳定的管理带宽。

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，并启用 MGT 接口接收 SCS 和 Web 管理流量。

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, SCS: （选择）

CLI

1. set interface mgt ip 10.1.1.2/24
2. set interface mgt manage web
3. set interface mgt manage scs
4. save

虚拟专用网

可以使用虚拟专用网 (VPN) 通道，保证从动态分配的或固定的 IP 地址对 NetScreen 设备进行远程管理和监控的安全性。使用 VPN 通道可以保护任何种类的流量，如 NetScreen-Global PRO、 HTTP、 Telnet 或 SNMP。

NetScreen 支持三种方法创建 VPN 通道：

- *手动密钥：*可以在两个通道端手动设置定义 “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。要在 SA 中更改任何元素，必须在通道的两端将其手动输入。
- *具有预共享密钥的自动密钥 IKE：*一个或两个预共享机密—一个用于认证，另一个用于加密—起种子值作用。IKE 协议使用它们在通道的两端产生一组对称密钥；即，使用相同的密钥进行加密和解密。在预定义间隔，这些密钥自动重新生成。
- *具有证书的自动密钥 IKE：*使用 “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 VPN 章。有关 NetScreen-Remote 的详细信息，请参阅* NetScreen-Remote User’s Guide。

要将 NetScreen 设备生成的流量（如系统日志报告、NetScreen-Global PRO 报告或 SNMP 陷阱）通过 VPN 通道发送到 Untrust 区段中的管理员，必须将绑定到 Trust 区段的缺省接口指定为策略中的源地址。（尽管流量实际上源于 NetScreen 设备自身，但是必须将缺省的 Trust 区段接口指定为源地址。）

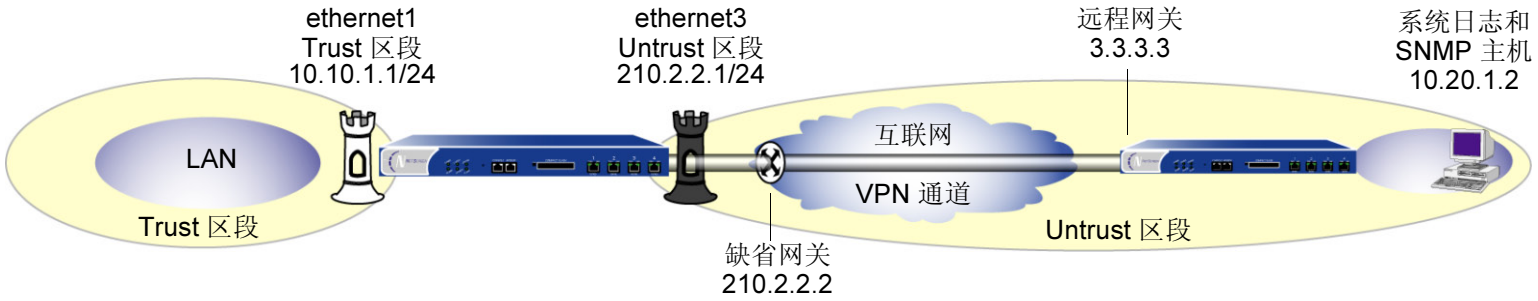
缺省接口是绑定到区段的第一个接口。最初，缺省接口是预先绑定到 Trust 区段的接口。如果将多个接口绑定到 Trust 区段，则预先绑定的接口保留作为缺省接口。如果在以后解除绑定 Trust 区段接口，则 NetScreen 设备使用绑定到 Trust 区段的其它接口中的第一个接口。要知道哪个接口是区段的缺省接口，请查看 WebUI 上 Zones > Zone 页中的 “Default IF” 栏，或在 CLI 中键入 **get zone** 命令。

> ***注意：****要生成由 NetScreen 设备产生的管理流量的通道，源地址必须为绑定到 Trust 区段的缺省接口，并且目的地址必须在 Untrust 区段中。*

范例：通过 IPSec 通道发送 SNMP 和系统日志报告

在本例中， NetScreen 设备后面的远程管理员通过 “自动密钥 IKE IPSec” 通道，从另一台 NetScreen 设备接收 SNMP 陷阱和系统日志报告[16]。通道使用预共享密钥 (Ci5y0a1aAG) 作为数据源认证，并且建议将阶段 1 和阶段 2 的安全级别预定义为 “Compatible”。

注意： *下例中， ethernet1 被绑定到 Trust 区段，而 ethernet3 被绑定到 Untrust 区段。缺省网关的 IP 地址为 210.2.2.2。所有区段都在 trust-vr 路由域中。*



WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.1.1[17] /24

16. 本例假定远程 admin 已安装系统日志服务器和 SNMP 管理器。远程 admin 在 NetScreen 设备上设置 VPN 通道时，使用 210.2.2.1 作为远程网关，使用 10.10.1.1 作为目的地址。

17. 远程 admin 配置 SNMP 管理器时，必须在 “Remote SNMP Agent” 字段中输入 **10.10.1.1**。它是 SNMP 管理器发送查询的地址。

2. Network > Interfaces > Edit（对于 ethernet1/2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.2.2.1/24

地址

3. 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: 10.10.1.1/32
   Zone: Trust
4. 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: 10.20.1.2/32
   Zone: Untrust

VPN

5. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：
   VPN Name: admin
   Security Level: Compatible
   Remote Gateway: Create a Simple Gateway: （选择）
   Gateway Name: to_admin
   Type: Static IP, IP Address: 3.3.3.3
   Preshared Key: Ci5y0a1aAG
   Security Level: Compatible
   Outgoing interface ethernet3

系统日志和 SNMP

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

   Enable Syslog Messages: （选择）

   Use Trust Zone Interface as Source IP for VPN: （选择）

   Syslog Host Name/Port: 10.20.1.2

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

   Community Name: remote_admin

   Permissions: Write, Trap: （选择）

   Hosts: 10.20.1.2

8. Configuration > Report Settings > SNMP：选择 **Use Trust Zone Interface as Source IP for VPN**，然后单击 **Apply**。

路由

9. 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） 210.2.2.2

策略

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

    Source Address:

    Address Book: （选择） , trust_int

    Destination Address:

    Address Book: （选择） , remote_admin

    Service: SNMP

    Action: Tunnel

    Tunnel VPN: admin

    Modify matching outgoing VPN policy: （清除）

    Position at Top: （选择）

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

    Source Address:

    Address Book: （选择） , trust_int

    Destination Address:

    Address Book: （选择） , remote_admin

    Service: SYSLOG

    Action: Tunnel

    Tunnel VPN: admin

    Modify matching outgoing VPN policy: （清除）

    Position at Top: （选择）

CLI

接口 – 安全区域

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 210.2.2.1/2

地址

5. set address trust trust_int 10.10.1.1/24
6. set address untrust remote_admin 10.20.1.2/24

VPN

7. set ike gateway to_admin ip 3.3.3.3 outgoing-interface ethernet3 preshare Ci5y0a1sec-level compatible
8. set vpn admin gateway to_admin sec-level compatible

系统日志和 SNMP

9. set syslog config 10.20.1.2 auth/sec local0
10. set syslog vpn
11. set syslog enable
12. set snmp community remote_admin read-write trap-on
13. set snmp host remote_admin 10.20.1.2
14. set snmp vpn

路由

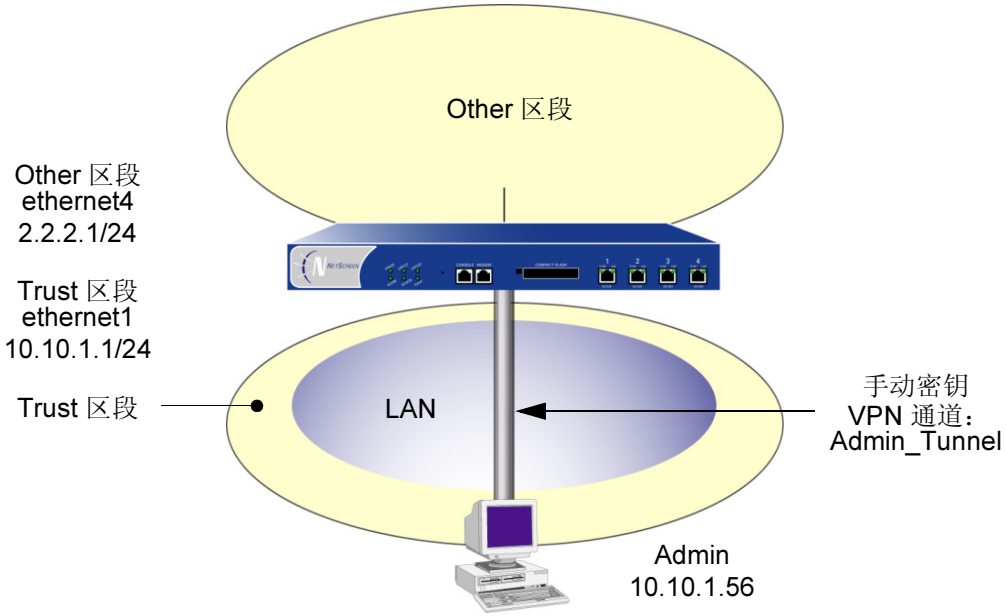
15. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 210.2.2.2

策略

16. set policy top from trust to untrust trust_int remote_admin snmp tunnel vpn admin
17. set policy top from trust to untrust trust_int remote_admin syslog tunnel vpn admin
18. save

范例：从 Trust 区段通过 VPN 通道进行管理

在本例中，设置 VPN 通道以提供管理流量的网络安全机密性。手动密钥 VPN 通道从工作站 (10.10.1.56) 扩展到绑定至 Trust 区段 (10.10.1.1/24) 的接口。工作站使用 NetScreen-Remote。也创建称为 “Other” 的区段，其唯一目的是为指定 VPN 通道的策略提供目的区段和目的地址。



WebUI

接口和区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.1.1/24

2. Network > Zones > New：输入以下内容，然后单击 **OK**：

   Zone Name: Other

   Virtual Router Name: trust-vr

   注意：*Trust 区段被预先配置。不必创建它。*

3. Network > Interfaces > Edit (ethernet4)：输入以下内容，然后单击 **OK**：

   Zone Name: Other

   IP Address/Netmask: 2.2.2.1/24

地址

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

   Address Name: Admin

   IP Address/Domain Name:

   IP/Netmask: 10.10.1.56/24

   Zone: Trust

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

   Address Name: Other_Interface

   IP Address/Domain Name:

   IP/Netmask: 2.2.2.1/24

   Zone: Other

VPN

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

   VPN Tunnel Name: Admin_Tunnel

   Gateway IP: 10.10.1.56

   Security Index: 4567 (Local) 5555 (Remote)

   Outgoing Interface: ethernet1

   ESP-CBC: （选择）

   Encryption Algorithm: DES-CBC

   Generate Key by Password[18] : 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 Zone: （选择） Untrust_Tun

18. 由于 NetScreen-Remote 将密码处理到密钥中，而不同于其它 NetScreen 产品，因此在配置通道后，应进行如下操作：(1) 返回 “手动密钥配置” 对话框（对于 “Admin 通道”，单击 “Configure” 栏中的 **Edit**）； (2) 复制生成的十六进制密钥； (3) 在配置通道端的 NetScreen-Remote 时使用十六进制密钥。

策略

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

   Source Address: Address Book: Admin

   Destination Address: Address Book: Other_Interface

   Service: ANY

   Action: Tunnel

   Tunnel VPN: Admin_Tunnel

   Modify matching outgoing VPN policy: （选择）

   Position at Top: （选择）

CLI

接口和区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.1.1/24
3. set zone name Other
4. set interface ethernet4 zone Other
5. set interface ethernet4 ip 2.2.2.1/24

地址

6. set address trust Admin 10.10.1.56/24
7. set address Other Other_Interface 2.2.2.1/24

VPN

8. set vpn Admin_Tunnel manual 4567 5555 gateway 10.10.1.56 outgoing ethernet1 esp des password netscreen1 auth md5 password netscreen2

策略

9. set policy top from trust to Other Admin Other_Interface any tunnel vpn Admin_Tunnel
10. set policy top from Other to trust Other_Interface Admin any tunnel vpn Admin_Tunnel
11. save

2

监控 NetScreen 设备

本章论述了下列关于监控 NetScreen 设备的主题：

存储日志信息

所有 NetScreen 设备都允许在内部 （闪存区域）和外部 （在许多位置）存储事件和信息流日志数据。尽管在内部存储日志信息很方便，但内存的数量是有限的。当内部存储空间被完全占用时， NetScreen 设备会用最新的日志条目覆盖最旧的日志条目。如果在保存日志信息之前先进先出 (FIFO) 机制发挥作用，就会丢失数据。要减少这种数据损失，可将事件和信息流日志存储在外部的系统日志或 WebTrends 服务器中，或 NetScreen-Global PRO 数据库中。

以下列出了日志数据的可能存储目的：

- **Console （控制台）：**通过控制台对 NetScreen 设备进行故障排除时，它是可以显示所有日志条目的有用的存储目的。或者，您可选择只在此处显示警报消息 （危急、警告、紧急），如果警报被触发时您恰好在使用该控制台，您即可看见警报。
- **Internal （内部）：**NetScreen 设备上的内部数据库是存储日志条目的方便目的地，但空间有限。
- **Email （电子邮件）：**向远程管理员发送事件和信息流日志的一种方便方法。
- **SNMP：**除了传输 SNMP 陷阱之外， NetScreen 设备也可将警报消息（危急、警告、紧急）从其事件日志发送到 SNMP 公共组。
- **Syslog （系统日志）：**NetScreen 设备可内部存储的所有事件和信息流日志也可发送到系统日志服务器中。由于系统日志服务器比 NetScreen 设备上的内部闪存存储器具有更大的存储能力，因此，将数据发送到系统日志服务器可减少日志条目超出最大内部存储空间时所发生的数据损失。
- **WebTrends：**允许查看与系统日志 （一种基于文本的工具）相比更加图形化的危急、警告和紧急级别的事件。
- **NetScreen-Global PRO：**除了多设备配置工具外， NetScreen-Global PRO 还提供了与查看和存储报告有关的卓越的监控能力。
- **CompactFlash (PCMCIA)：**此目的的优点是便于携带。在 CompactFlash 卡上存储数据后，可从 NetScreen 设备上移除该卡，并将其存储或安装到另一设备上。

事件日志

NetScreen 提供了用于监控系统事件和网络流量的事件日志。 NetScreen 设备将系统事件按以下严重性级别分类：

- **Emergency （紧急）**：生成关于 SYN （同步空闲字符）攻击、 Tear Drop 攻击及 Ping of Death 攻击的消息。关于这些攻击类型的详细信息，请参阅第 **2**-33 页上的 “防火墙选项”。
- **Alert （警示）**： 生成多用户认证故障的消息及其它未包含在紧急类别中的防火墙攻击的消息。
- **Critical （关键）**： 生成 URL 阻塞、流量警告、高可用性 (HA) 状态改变及全域通信的消息。
- **Error （错误）**： 生成 admin 登录故障的消息。
- **Warning （警告）**： 生成 admin 登录和注销、登录和注销故障及用户认证故障、成功和超时的消息。
- **Notification （通知）**： 生成链接状态改变、流量日志及配置改变的消息。
- **Information （信息）**： 生成任一种未在其它类别中指定的消息。
- **Debugging （调试）**： 生成所有消息。

事件日志显示每个系统事件的日期、时间、级别及说明。可通过 WebUI 或 CLI 查看存储在 NetScreen 设备的快闪存储器中的每一类别的系统事件。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。也可选择将它们发送到外部存储空间 （请参阅第 56 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 Reference Guide。

查看事件日志

可按严重性级别显示日志条目以及按关键字在 WebUI 和 CLI 中查询事件日志。可用 CLI 将严重性级别和关键字结合，以精确查询。若包括开始和结束时间、消息类型 ID 号和排除关键字，则查询会更精确。例如，可用以下参数执行查询：

get event level notif type 00037 start-time 07/18 end-time 07/19 include “zone trust” exclude block

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 下拉列表中选择严重性级别。

CLI

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

要按关键字查询事件日志，请执行以下操作之一：

WebUI

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

CLI

get event include *word_string*

范例：下载关键事件的事件日志

在本例中，可将事件日志中输入的关键事件下载到本地目录“C:\netscreen\logs”(WebUI) 或 IP 地址为 10.10.20.200 的 TFTP 服务器的根目录下 (CLI)。命名文件为 “crt_evnt.txt07-02.txt”。

WebUI

1. Reports > System Log > Event：在 Search 旁，为 Log Level 设置输入 **Critical**，然后单击 **Search**。

   出现带有“关键事件”查询结果的表。单击 **Save**。

   File Download 向导提示您打开文件（使用 ASCII 编辑器）或将其保存到磁盘。
2. 选择 **Save this file to disk** 选项，然后单击 **OK**。

   File Download 向导提示您选择目录。
3. 指定 **C:\netscreen\logs**，命名文件为“crt_evnt.txt07-02.txt”，然后单击 **Save**。

CLI

```
get event level critical > tftp 10.10.20.200 crt_evnt.txt07-02.txt
```

信息流日志

NetScreen 提供了信息流日志来监控并记录策略允许通过防火墙的信息流。信息流日志记录了每个会话的以下元素：

- 连接开始的日期和时间
- 源地址和端口号
- 转译的源地址和端口号
- 目的地址和端口号
- 会话持续时间
- 会话中使用的服务

要将 NetScreen 设备收到的所有信息流都记入日志，必须为所有策略启用记录选项。要将特定信息流记入日志，可以只对适用于该信息流的策略启用记录。要对某个策略启用记录选项，请执行以下操作之一：

WebUI

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

CLI

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

可通过 CLI 或 WebUI 查看存储在 NetScreen 设备的闪存存储器中的信息流日志。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。此外，还可将其发送到外部存储空间 （请参阅第 56 页上的 “存储日志信息”）。也可将信息流日志和事件日志一起用电子邮件发送给 admin。

范例：下载信息流日志

在本例中，下载 ID 编号为 12 的策略的信息流日志。对于 WebUI，将其下载到本地目录 “C:\netscreen\logs” 中。对于 CLI，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 ID 为 12 的策略）： 单击 **Save**。

   File Download 向导提示打开该文件（使用 ASCII 编辑器）或将其保存到磁盘。
2. 选择 **Save this file to disk** 选项，然后单击 **OK**。

   File Download 向导提示您选择目录。
3. 指定 C:\netscreen\logs，命名文件为 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，来监控并记录所有丢弃的封包（如被某个策略拒绝的封包）以及在 NetScreen 设备上自行终止的信息流（如管理信息流）。 与信息流日志相似，该 self 日志显示每个丢弃封包或终止于 NetScreen 设备的会话的日期、时间、源地址 / 端口、目的地址 / 端口、持续时间和服务。

可通过 CLI 或 WebUI 查看存储在 NetScreen 设备上的闪存存储器中的 self 日志。

也可在指定位置将日志保存为文本文件，然后用 ASCII 文本编辑器（如 Notepad 或 WordPad）来查看该文件。

范例：下载 Self 日志

在本例中，可将 self 日志下载到本地目录“C:\netscreen\logs”(WebUI) 或 IP 地址为 10.10.20.200 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 向导提示打开该文件（使用 ASCII 编辑器）或将其保存到磁盘。

2. 选择 **Save this file to disk** 选项，然后单击 **OK**。

   File Download 向导提示您选择目录。

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 10.10.20.200 self_log07-03-02.txt
```

系统日志

系统日志允许将系统事件记录在一单独文件中，以便以后查看。NetScreen 设备以预先定义的严重性级别为系统事件生成系统日志消息（参阅第 57 页上的“事件日志”中的严重性级别列表），并通过 UDP（514 端口）将这些消息发送到运行在 UNIX/Linux 系统上的系统日志主机上。可使用系统日志消息为系统管理员创建电子邮件警示，或在使用 UNIX 系统日志惯例的指定主机控制台上显示消息。

***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资源 (syslog -r) 中检索信息。*

也可通过 VPN （虚拟专用网）通道发送系统日志消息。在 WebUI 中，选择 **Use Trust Interface as Source IP for VPN**。在 CLI 中，使用 **set syslog vpn** 命令。

系统日志按层次组织消息，从而设置级别时需设置该级别及其上面的所有级别。例如，警示设置将生成警示和紧急消息，而调试设置会生成所有级别的消息。

***注意：**也可发送带有系统日志消息的流量日志。*

WebTrends

WebTrends 提供了称为 WebTrends Firewall Suite 的产品，允许您自定义关键、警示和紧急事件的系统日志报告，以图形形式显示需要的信息。可创建着重于防火墙攻击（紧急级别事件）等方面或安全级别为关键、警示和紧急的所有事件的报告。

***注意：**WebTrends Syslog Server 和 WebTrends Firewall Suite 必须运行在同一 Windows NT 系统上。必须具有管理员权限才能进行配置。*

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

范例：启用通知事件的系统日志和 WebTrends

在以下范例中，建立系统日志设备，将通知消息发送到位于 172.10.16.25 处 WebTrends 系统日志服务器上的 514 端口。安全和设备级别设置为 Local0。在系统事件消息中包含有流量日志。

WebUI

系统日志设置

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

   Enable syslog messages: （选择）

   Include Traffic Log: （选择）

   Syslog Host Name/Port: 172.10.16.25/514[1]

   Security Facility: Local0

   Facility: Local0

WebTrends 设置

2. 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

1. 系统日志主机端口号必须与 WebTrends 端口号匹配。

安全级别

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

   WebTrends Notification: （选择）

   Syslog Notification: （选择）

> ***注意：****启用以“透明”模式在 NetScreen 设备上运行的系统日志和 WebTrends 时，必须配置静态路由。**请参阅第 **2**-65 页上的“路由表配置”。*

CLI

系统日志设置

1. set syslog config 172.10.16.25 local0 local0
2. set syslog port 514
3. set syslog traffic
4. set syslog enable

WebTrends 设置

5. set webtrends host-name 172.10.16.25
6. set webtrends port 514
7. set webtrends enable

安全级别

8. set log module system level notification destination syslog
9. set log module system level notification destination webtrends
10. 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关于网络及其上设备的统计数据，以及接收所关注的系统事件通知。

NetScreen 支持 RFC-1157 中所述的 SNMPv1 协议，“简单网络管理协议”。NetScreen 也支持 RFC-1213 中定义的所有相关 管理信息库 II (MIB II) 组，“基于 TCP/IP 的互联网网络管理的管理信息库：MIB-II”。 NetScreen 还有企业专有的 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：**如果发送错误的公共组字符串，则 SNMP 管理器触发认证故障陷阱。
- **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。定义了三个 NetScreen 企业陷阱包括了与硬件、安全和软件相关的警告。（关于防火墙设置和警告的详细信息，请参阅第 **2**-33 页上的“防火墙选项”和第 82 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。（关于配置策略的详细信息，请参阅第 **2**-215 页上的 “策略”。）

下表列出了可能的警告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

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 数据并从可信或不信任的接口接收陷阱。也可从互联网上获取几种共享及免费的 SNMP 管理器应用程序。*

NetScreen 设备发运时不带有缺省的 SNMP 管理配置。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[2]）。

2. 由于安全原因，具有读写权限的公共组成员只能更改 NetScreen 设备上的 sysContact 和 sysLocation 变量。

执行概述

下列条目概括了如何在 NetScreen 设备中执行 SNMP：

- 网络管理员最多可创建三个公共组，每个公共组最多包含八台主机。主机必须单独列出；不能按范围指定主机。
- 每个公共组具有对 MIB II 数据的只读或读写权限。
- 可允许或禁止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。
- 对设置为接收陷阱的每个公共组中的每台主机，每个系统警告生成单独的 NetScreen 企业 SNMP 陷阱。
- 冷启动 / 上行链路 / 下行链路陷阱被发送到设置为接收陷阱的公共组内的所有主机上。
- 如果为公共组指定 trap-on，也可选择允许流量报警。

也可通过 VPN （虚拟专用网）通道发送 SNMP 消息。在 WebUI 中，选择 **Use Trust Interface as Source IP for VPN**。在 CLI 中，使用 **set snmp vpn** 命令。

范例：设置 SNMP 公共组

在本例中，为两个名称分别为“JCarney”和“TCooper”的公共组配置 SNMP。在第一个公共组中，其成员可读取 MIB II 数据并接收陷阱。在第二个公共组中，其成员可读写 MIB II 数据、接收陷阱及流量报警。联系人是“Miami”的“John Fisher”。JCarney 公共组主机 IP 地址为 172.16.20.181、172.16.40.245 和 172.16.40.55。TCooper 公共组主机 IP 地址为 172.16.20.250。

注意：*MIB II 系统组变量 sysContact、 sysName （与 NetScreen 设备的主机名相同）为读写对象。所有其它变量均为只读。*

WebUI

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

   System Contact: John Fisher

   Location: Miami

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

   Community Name: JCarney

   Permissions: Trap: （选择）

   Hosts: 172.16.20.181
   172.16.40.245
   172.16.40.55

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

   Community Name: TCooper

   Permissions: Write, Trap: （选择）

   Including Traffic Alarms: （选择）

   Hosts: 172.16.20.250

CLI

1. set snmp contact John Fisher
2. set snmp location Miami
3. set snmp community JCarney read-only trap-on
4. set snmp host JCarney 172.16.20.181
5. set snmp host JCarney 172.16.40.245
6. set snmp host JCarney 172.16.40.55
7. set snmp community TCooper read-write trap-on traffic
8. set snmp host TCooper 172.16.20.250
9. save

VPN 监控

NetScreen ScreenOS 可以使用 SNMP VPN 监控对象和陷阱来确定有效 VPN 的状态和条件。

注意：*为使 SNMP 管理器应用程序能识别 VPN 监控 MIB （管理信息库），必须将 NetScreen 专用的 MIB 扩展文件导入到应用程序中。可在随 NetScreen 设备附带的 NetScreen 文档 CD 中找到 MIB 扩展文件。*

若在“手动密钥”或“自动密钥 IKE VPN”通道中启用 VPN 监控功能， NetScreen 设备就能激活其 SNMP VPN 监控对象，这些对象包含以下数据：

- 活动 VPN 会话总数
- 每个会话的开始时间
- 每个会话的 “安全联盟 (SA)”元素：
  - ESP （封装安全性负荷）加密 （DES 或 3DES）和认证算法 （MD5 或 SHA-1）类型
  - AH 算法类型 （MD5 或 SHA-1）
  - 密钥交换协议 （自动密钥 IKE 或手动密钥）
  - 阶段 1 认证方法 （预共享密钥或证书）
  - VPN 类型 （拨号或对等连接）
  - 对等方及本地网关 IP 地址
  - 对等方及本地网关 ID
  - 安全参数索引 (SPI) 号
- 会话状态参数
  - VPN 监控状态 （连接或中断）
  - 通道状态 （连接或中断）
  - 阶段 1 和 2 状态 （非活动或活动）
  - 阶段 1 和 2 生存期 （重定密钥前的秒数；阶段 2 生存期也用重定密钥前剩余的字节数进行报告）

启用 VPN 监控后，NetScreen 设备在指定的时间间隔（可按秒配置）内通过通道来 ping 远程网关，以监控两个 VPN 网关之间的网络连接性能。[3] 取决于通道远端设备的类型及本地 NetScreen 设备是运行在 Layer 3（第 3 层）（NAT 或路由模式）还是Layer 2（第 2 层）（透明模式），本地 NetScreen 设备用来发送和接收 ping 请求的源接口会有所不同：

如果本地设备运行在	并且远程设备为 VPN 客户机（如 NetScreen-Remote），则	并且远程设备为另一台 NetScreen 设备，则
Layer 3 （第 3 层）	源接口可以是具有 IP 地址、处于 MGT 区段之外任意区段中的任意接口*。	无论指定何种源接口， NetScreen 设备都使用外向接口作为源接口。
Layer 2 （第 2 层）	不能使用 VPN 监控功能。	无论指定何种源接口， NetScreen 设备都使用外向接口作为源接口。

* 如果源接口在不同于外向接口的区段内 （或者如果在相同区段并启用了内部区段阻塞），则必须创建策略，允许通过 VPN 通道执行 ping。

注意：*绑定到通道接口的 VPN 通道不能支持 VPN 监控。*

VPN 监控 MIB 时，将记录 ping 操作是否引发响应、连续的平均成功响应、响应等待时间以及最后 30 次尝试的平均响应等待时间。

如果 ping 动作指出 VPN 状态已改变（由于[4]连续的成功和未成功 ping 请求数超出用户可定义的临界值），则 NetScreen 设备触发以下 SNMP 陷阱之一：

- **Up to Down**：VPN 通道处于连接状态，但在指定数目的连续请求后， ping 请求并未引起响应。
- **Down to up**：VPN 通道处于中断状态，但 ping 请求引起了响应。

3. 要改变 ping 时间间隔，可使用以下 CLI 命令：**set vpnmonitor interval** *number*。缺省值为 10 秒。
4. 要改变 ping 的临界值，可使用以下 CLI 命令：**set vpnmonitor threshold** *number*。缺省值为 10 个连续 ping 请求。

要启用 VPN 监控，请执行以下操作：

WebUI

VPNs > Manual Key > New ：配置 VPN，单击 **Advanced**，选择 **VPN Monitor** 复选框并从 Source Interface 下拉列表中选择一接口，单击 **Return** 返回基本 VPN 配置页，然后单击 **OK**。

或者

VPNs > AutoKey IKE > New ：配置 VPN，单击 **Advanced**，选择 **VPN Monitor** 复选框并从 Source Interface 下拉列表中选择一接口，单击 **Return** 返回基本 VPN 配置页，然后单击 **OK**。

CLI

1. set vpn *name_str* monitor [source-interface *interface*][5]
2. set vpnmonitor frequency *number* [6]
3. set vpnmonitor threshold *number* [7]
4. save

5. 如果不选择源接口， NetScreen 设备使用外向接口作为缺省接口。
6. VPN 监控频率以秒为单位。
7. VPN 监控临界值数是连续的成功和未成功 ping 请求数，它确定了通过 VPN 通道是否可达到远程网关。

计数器

NetScreen 提供了屏幕、硬件和流量计数器来监控流量。计数器为指定接口提供处理信息，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流量总数。

- **Block Java/Active X Component** – 阻塞的 Java 或 ActiveX 组件数
- **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 封包数
- **UDP Flood Protection** – 作为不可信 UDP 泛滥的一部分而丢弃的 UDP 封包数
- **WinNuke Attack Protection** – 作为不可信 WinNuke 攻击的一部分而检测的封包数
- **Port Scan Protection** – 检测及阻塞的端口扫描数
- **IP Sweep Protection** – 检测及阻塞的 IP 扫描攻击封包数
- **Tear-drop Attack Protection** – 作为 Tear Drop 攻击的一部分而阻塞的封包数
- **SYN Flood Protection** – 作为不可信 SYN 泛滥的一部分而检测的 SYN 封包数
- **IP Spoofing Attack Protection** – 作为 IP 欺骗攻击的一部分而阻塞的 IP 地址数
- **Ping-of-Death Protection** – 太大或不规则的不可信和已拒绝 ICMP 封包数
- **Source Route IP Option Filter** – 过滤的 IP 源路由数
- **Land Attack Protection** – 作为不可信陆地攻击的一部分而阻塞的封包数
- **SYN Fragment Detection** – 作为不可信 SYN 碎片攻击的一部分而丢弃的封包碎片数
- **TCP Packet without Flag** – 带有缺失或残缺标记字段的已丢弃非法封包数
- **Unknown Protocol Protection** – 作为未知协议的一部分而阻塞的封包数
- **Bad IP Option Detection** – 由于残缺或不完整的 IP 选项而丢弃的帧数
- **IP Record Route Option** – 启用了 “记录路由” 选项的已检测帧数
- **IP Timestamp Option** – 设置了 “互联网时戳” 选项集的已丢弃 IP 封包数
- **IP Security Option** – 设置了 “IP 安全” 选项集的已丢弃帧数

- **IP Loose Src Route Option** – 启用了 “松散源路由” 选项的已检测 IP 封包数
- **IP Strict Src Route Option** – 启用了 “严格源路由” 选项的已检测封包数
- **IP Stream Option** – 设置了 “IP 流” 标识符集的已丢弃封包数
- **ICMP Fragment** – 设置了 More Fragments 标记集或在偏移字段中指出了偏移量的 ICMP 帧数
- **Large ICMP Packet** – IP 长度超过 1024 的已检测 ICMP 帧数
- **SYN and FIN bits set** – 带有非法标记组合的已检测封包数
- **FIN bit with no ACK bit** – 带有非法标记组合的已检测和已丢弃封包数
- **Malicious URL Protection** – 阻塞的不可信恶意 URL 数
- **limit session** – 由于达到会话限制而不能递送的封包数
- **SYN-ACK-ACK-Proxy DoS** – 由于 SYN-ACK-ACK-proxy DoS SCREEN 选项而阻塞的封包数

NetScreen 提供了以下硬件计数器来监控硬件性能及出错的封包：

- **in bytes** – 收到的字节数
- **out bytes** – 发送的字节数
- **in packets** – 收到的封包数
- **out packets** – 发送的封包数
- **in no buffer** – 由于缓冲区不可用而无法接收的封包数
- **out no buffer** – 由于缓冲区不可用而未发送的封包数
- **in overrun** – 已传输的超载封包数
- **in underrun** – 已传输的欠载封包数
- **in coll err** – 内向冲突封包数
- **out coll err** – 外向冲突封包数
- **in crc err** – 循环冗余校验 (CRC) 出错的内向封包数
- **in align err** – 比特流中定位错误的内向封包数

- **in short frame** – 存在 **in short frame error** 的内向封包数
- **out bs pak** – 查询未知 MAC 地址时存在于后备存储器中的封包数
- **early frame** – 用于以太网驱动程序缓冲区描述符管理的计数器
- **late frame** – 用于以太网驱动程序缓冲区描述符管理的计数器
- **in err** – 至少有一个错误的内向封包数
- **in unk** – 收到的未知封包数
- **in misc err** – 存在混杂错误的内向封包数
- **out misc err** – 存在混杂错误的外向封包数
- **in dma err** – 存在直接存储器存取错误的内向封包数
- **out discard** – 丢弃的外向封包数
- **out defer** – 延迟的外向封包数
- **out heartbeat** – 外向心跳信号封包数
- **re xmt limit** – 接口以半双工运行时超出重新传输限制而丢弃的封包数
- **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” 模式时未启用 VLAN 中继而丢弃的封包数
- **out cs lost** – 由于 “多路访问载波监听 / 冲突检测” (CSMA/CD) 协议丢失了信号而丢弃的外向封包数[8]

8. 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。

NetScreen 还提供了以下流量计数器[9]，用来监控在数据流层检查的封包数：

- **in bytes** – 收到的字节数
- **out bytes** – 发送的字节数
- **in packets** – 收到的封包数
- **out packets** – 发送的封包数
- **in vlan** – 内向的 vlan 封包数
- **out vlan** – 外向的 vlan 封包数
- **in arp req** – 内向的 arp 请求封包数
- **in arp resp** – 外向的 arp 请求封包数
- ***in un auth** – 未经授权的 TCP、 UDP 和 ICMP 内向封包数
- ***in unk prot** – 使用未知以太网协议的内向封包数
- **in other** – 其它以太网类型的进入封包数
- **no mac address** – （仅限 NetScreen-5000 系列）源或目标 IP 地址不存在 MAC 地址的会话数
- **mac relearn** – 由于 MAC 地址发生了改变而使得 MAC 地址学习表必须再学习 MAC 地址相关接口的次数
- ***slow mac** – MAC 地址解析缓慢的帧数
- **syn frag** – 由于碎片原因而丢弃的 SYN 封包数
- ***misc prot** – 使用 TCP、 UDP 或 ICMP 之外其它协议的封包数
- **mal url** – 发往确定为恶意 URL 的已阻塞封包数
- **null zone** – 错误地发往绑定到 Null 区段接口的已丢弃封包数
- ***no xmit vpnf** – 由于碎片原因而丢弃的 VPN 封包数
- ***no frag sess** – 不完整会话数超过最大 NAT 会话数一半的次数

9. 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。

- **no frag netpak** – netpak 缓冲区中的可用空间降至 70% 以下的次数
- **sessn thresh** – 最大会话数量的临界值
- ***no nsp tunnel** – 发送到未绑定任何 VPN 通道的通道接口上的已丢弃封包数
- **ip sweep** – 超出指定 ip 扫描临界值的已接收和已丢弃封包数
- **tcp out of seq** – 序列号超出可接受范围的已接收 TCP 封包数
- **wrong intf** – （仅限 NetScreen-1000）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** – （仅限 NetScreen-1000）错误地发送到不正确处理器模块的封包数
- ***icmp broadcast** – 收到的 ICMP 广播数
- **mp fail** – （仅限 NetScreen-1000）在主处理器模块和处理器模块间发送 PCI 消息时出现问题次数
- **proc sess** – （仅限 NetScreen-1000）处理器模块上的会话总数超出最大临界值的次数
- **invalid zone** – 发往无效安全区段的封包数
- **in icmp** – 收到的 “因特网控制信息协议” (ICMP) 封包数
- **in self** – 发往 NetScreen 管理 IP 地址的封包数
- **in vpn** – 收到的 IPSec （互联网协议安全性）封包数
- **trmn drop** – 被流量管理丢弃的封包数
- **trmng queue** – 在队列中等待的封包数
- **tiny frag** – 收到破碎的小封包数
- **connections** – 自上次引导后建立的会话数
- **loopback drop** – 由于封包不能回送而丢弃的封包数
- **tcp proxy** – 由于使用 TCP 代理 （如 SYN 泛滥保护选项或用户认证）而丢弃的封包数
- **no g parent** – 由于无法找到父级连接而丢弃的封包数

- **no gate sess** – 由于未提供防火墙入口而中断的会话数
- **no nat vector** – 由于入口不能使用 “网络地址转换” (NAT) 连接而丢弃的封包数
- **no map** – 由于没有到可信方的映射而丢弃的封包数
- **no conn** – 由于 “网络地址转换” (NAT) 连接不可用而丢弃的封包数
- **no dip** – 由于 “动态 IP” (DIP) 地址不可用而丢弃的封包数
- **no gate** – 由于没有可用入口而丢弃的封包数
- **no route** – 收到的不可路由的封包数
- **no sa** – 由于未定义 “安全联盟” (SA) 而丢弃的封包数
- **no sa policy** – 由于没有与 SA 相关的策略而丢弃的封包数
- **sa inactive** – 由于非活动 SA 而丢弃的封包数
- **sa policy deny** – 被 SA 策略拒绝的封包数
- **policy deny** – 被定义的策略拒绝的封包数
- **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 后备存储器的封包数
- **land attack** – 收到的不可信陆地攻击封包数
- **no route** – 收到的不可路由的封包数
- **tear drop** – 作为不可信 Tear Drop 攻击一部分而阻塞的封包数
- **src route** – 由于过滤源路由选项而丢弃的封包数
- **pingdeath** – 收到的不可信 Ping of Death 攻击封包数
- **address spoof** – 收到的不可信地址欺骗攻击封包数
- **url block** – 阻塞的 HTTP 请求数
- **nvec err** – 由于 NAT 向量错误而丢弃的封包数
- **enc fai** – 失败的点对点通道协议 (PPTP) 封包数
- **illegal pak** – 由于是非法封包而丢弃的封包数

范例：查看屏幕和流量计数器

在本例中，将查看 ethernet1 接口的 NetScreen 屏幕和流量计数器。

WebUI

1. Reports > Interface > Screen Counters：从 Interface 下拉列表中选择 **ethernet1**。
2. Reports > Interface > Statistics：从 Interface 下拉列表中选择 **ethernet1**。

CLI

1. get counter screen interface ethernet1
2. get counter flow interface ethernet1

资源恢复日志

NetScreen 提供了资源恢复日志，显示每一次设备使用资源恢复程序来返回其缺省设置的相关信息（请参阅第 36 页上的 “重置设备到出厂缺省设置”）。除了通过 WebUI 或 CLI 查看资源恢复日志外，也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 “系统恢复日志”

在本例中，可将资源恢复日志下载到本地目录 “C:\netscreen\logs” (WebUI) 或 IP 地址为 10.10.20.200 的 TFTP 服务器的根目录下 (CLI)。命名文件为 “sys_rst.txt”。

WebUI

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

   File Download 向导提示打开该文件（使用 ASCII 编辑器）或将其保存到磁盘。
2. 选择 **Save this file to disk** 选项，然后单击 **OK**。

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

CLI

```
get log self > tftp 10.10.20.200 sys_rst.txt
```

流量报警

流量超出在策略中定义的临界值时， NetScreen 设备支持流量报警。可配置 NetScreen 设备，只要 NetScreen 设备生成流量报警，就能通过以下一种或多种方法来发出警示：

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

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。要为网络流量创建这样的基准，必须观察一段时间内的流量模式。然后，在确定了认为是正常的流量数之后，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，以引起对背离基准的注意。然后就可估计其情形，确定引起背离的原因，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，提供折衷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

在本例中，有一个在 DMZ 区段内 IP 地址为 211.20.1.5 （名称为 “web1”）的 Web 服务器。想要检测从 Untrust 区段通过 Telnet 访问该 Web 服务器的所有尝试。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，并可设置 64 字节的流量报警临界值。由于最小的 IP 封包为 64 字节，即使只有一个试图从 Untrust 区段发往 Web 服务器的 Telnet 封包，都会触发警告。

WebUI

1. 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

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

   Source Address:

   Address Book: （选择） , Any

   Destination Address:

   Address Book: （选择） , web1

   Service: Telnet

   Action: Deny

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

   Counting: （选择）

   Alarm Threshold: 64 Bytes/Sec

CLI

1. set address dmz web1 211.20.1.5/32
2. set policy from untrust to dmz any web1 telnet deny count alarm 64
3. save

范例：折衷系统通知

在本例中，使用流量报警来提供折衷系统的通知。有一台在 DMZ 区段内 IP 地址为 211.20.1.10 （名称为 ftp1）的 FTP 服务器。希望能允许由 FTP 获取的流量能到达此服务器。不希望有来自此 FTP 服务器的任何种类的流量。如出现这种流量则说明系统已被折衷，可能是与 NIMDA 病毒相似的病毒所导致。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

1. 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

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

   Source Address:

   Address Book: （选择）, Any

   Destination Address:

   Address Book: （选择）, ftp1

   Service: FTP-Get

   Action: Permit

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

   Source Address:

   Address Book: （选择）, ftp1

   Destination Address:

   Address Book: （选择）, Any

   Service: ANY

   Action: Deny

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

   Counting: （选择）

   Alarm Threshold: 64 Bytes/Sec

CLI

1. set address global ftp1 211.20.1.10/32
2. set policy global any ftp1 ftp-get permit
3. set policy global ftp1 any any deny count alarm 64
4. save

范例：发送电子邮件警示

在本例中，如果有警告，则通过电子邮件警示来设置通知。邮件服务器位于 172.16.10.254，通知的第一个电子邮件地址为 jharker@netscreen.com，第二个地址为 driggs@netscreen.com。NetScreen 设备包括流量日志及通过电子邮件发送的事件日志。

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[10]

E-Mail Address 1: jharker@netscreen.com

E-Mail Address 2: driggs@netscreen.com

CLI

1. set admin mail alert
2. set admin mail mail-addr1 jharker@netscreen.com
3. set admin mail mail-addr2 driggs@netscreen.com
4. set admin mail server-name 172.16.10.254
5. set admin mail traffic-log
6. save

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

A

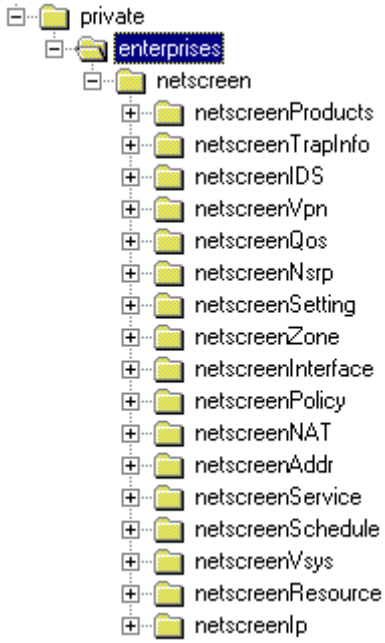
SNMP MIB 文件

NetScreen 提供 MIB 文件，支持企业的应用程序和 NetScreen 设备中 “SNMP Agent” 之间的 SNMP 通信。要获得最新的 MIB 文件，请从 www.netscreen.com/support 下载。

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 文件是以多层层次结构组织的，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：



每个文件夹包含一类 MIB 文件。

netscreenProducts	对不同的 NetScreen 产品系列指派 “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 “映射 IP”、“动态 IP” 和 “虚拟 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 IP 相关信息。
netScreenChassis	清空将来的 MIB 支持文件夹的占位符文件夹

二级 MIB 文件夹

本节介绍 NetScreen 设备的二级 MIB 文件夹。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：NetScreen 不再支持 failedSession 计数器。

netscreenIp

nsIpArp	ARP 表

索引

N

P

Q

R

S

T

V

W

X

Y

Z