NetScreen 概念与范例

ScreenOS 参考指南

第 6 卷：虚拟系统

ScreenOS 4.0.0

编码 093-0524-000-SC

版本 F

Copyright Notice

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

可将单个 NetScreen 安全系统逻辑划分成多个虚拟系统，以提供多客户式托管服务。每个虚拟系统 (vsys) 都是一个唯一的安全域，可由其自己的管理员（称作“虚拟系统管理员”或“vsys admin”）进行管理，管理员可以通过设置自己的地址薄、用户列表、自定义服务、 VPN 和策略以使自己的安全域个性化。

第 6 卷，“虚拟系统”将介绍虚拟系统、专用和共享接口，以及基于 VLAN 和基于 IP 的通信流分类。本卷还将介绍如何创建 vsys （必须具有根级管理员权限）以及定义 vsys admin。

约定

本书介绍了配置 NetScreen 设备的两种管理方法：Web 用户界面（WebUI）和命令行界面（CLI）。以下介绍这两种界面使用的约定。

WebUI 导航约定

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

范例：Objects > Addresses > List > New

要访问新地址配置对话框，请执行以下操作：

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

CLI 约定

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

虚拟系统

可将单个 NetScreen 安全系统[1] 逻辑划分成多个虚拟系统，以提供多客户式托管服务。每个虚拟系统 (vsys) 都是一个唯一的安全域，并且可以拥有自己的管理员 （称作 “虚拟系统管理员”或 “vsys admins”），管理员可以通过设置自己的地址薄、用户列表、自定义服务、 VPN 和策略以使自己的安全域个性化 （不过，只有根级管理员才可以设置防火墙安全选项、创建虚拟系统管理员以及定义接口和子接口）。

注意： *有关 NetScreen 支持的各种管理级别的详细信息，请参阅第* ***3*** *-27 页上的 “管理的级别”。*

NetScreen 虚拟系统支持两种通信流分类：基于 VLAN 和基于 IP，这两种类别可独立使用或同时使用。本章讨论虚拟系统的下列概念和具体实现：

1. NetScreen 设备一般分为以下两类：安全系统和装置。只有 NetScreen 安全系统才可支持虚拟系统。要查看哪种平台支持此功能，请参阅 NetScreen 市场文献。

创建 Vsys 对象

要创建 vsys 对象，根管理员或根级读 / 写 admin 必须完成以下任务：

- 定义虚拟系统
- （可选）定义一个或多个 vsys admin[2]

创建 vsys 对象后，根级 admin 需要进行其它配置才能使其发挥作用。他必须为 vsys 配置子接口或接口，以及可能共享的虚拟路由器和共享安全区。接下来的配置取决于是否想让此 vsys 支持基于 VLAN 或基于 IP 的通信流分类或两者的组合。完成这些配置后，根级管理员可以退出虚拟系统，允许 vsys admin（如果已定义）登录并开始配置地址、用户、服务、 VPN 和策略。

范例：创建 Vsys 对象和 Vsys Admin

在此例中，作为根级 admin，您可以创建三个 vsys 对象：vsys1、 vsys2、 vsys3。为 vsys1 创建名为 Alice、密码为 wIEaS1v1 的 vsys admin[3]。为 vsys2 创建名为 Bob、密码为 pjF56Ms2 的 vsys admin。 vsys3 没有 vsys admin。

注意：*Vsys 名称、 admin 名称以及密码是区分大小写的。 Vsys “abc” 不同于 vsys “ABC”。*

通过 WebUI 创建 vsys 之后，您仍然处于在根级。进入新创建的 vsys 需要单独的步骤：

Vsys：单击 **Enter**（对于想要进入的虚拟系统）。

出现已进入的 vsys 的 WebUI 页， vsys 的名称位于中央显示区 — Vsys:*Name* 上方。

2. 根级管理员可以为每个 vsys 定义一个具有读写权限的 vsys admin 和一个具有只读权限的 vsys admin。
3. 只有根级管理员才可创建 vsys admin 配置文件 （用户名和密码）。由于 NetScreen 设备使用用户名来确定用户所属的 vsys，所以 vsys admin 不能更改其用户名。但是， vsys admin 可以 （也应当）更改其密码。

通过 CLI 创建 vsys 时，您会立即进入刚刚创建的系统。（要从根级进入某一现有 vsys，请使用 **enter vsys** *name_str* 命令）。进入 vsys 后，请注意， CLI 命令提示符会发生变化，其中将包括当前正在其中发布命令的系统的名称。

WebUI

1. Vsys > New：输入以下内容，然后单击 **OK**：
   VSYS Name：vsys1
   VSYS Admin Name：Alice
   VSYS Admin Password：wIEaS1v1
   Confirm Password：wIEaS1v1
2. Vsys > New：输入以下内容，然后单击 **OK**：
   VSYS Name：vsys2
   VSYS Admin Name：Bob
   VSYS Admin Password：pjF56Ms2
   Confirm Password：pjF56Ms2
3. Vsys > New：输入以下内容，然后单击 **OK**：
   VSYS Name：vsys3

CLI

1. ns-> set vsys vsys1
2. ns(vsys1)-> set admin name Alice
3. ns(vsys1)-> set admin password wIEaS1v1
4. ns(vsys1)-> save[4]
5. ns(vsys1)-> exit
6. ns-> set vsys vsys2
7. ns(vsys2)-> set admin name Bob
8. ns(vsys2)-> set admin password pjF56Ms2
9. ns(vsys2)-> save
10. ns(vsys2)-> exit
11. ns-> set vsys vsys3
12. ns(vsys3)-> save

4. 发完命令后，必须在发出 **exit** 命令前先发 **save** 命令，否则 NetScreen 设备会丢失所做的更改。

虚拟路由器

当根级 admin 创建 vsys 对象时， vsys 自动使以下虚拟路由器为其所用：

- 所有共享的根级虚拟路由器，如 untrust-vr

  vsys 和根系统共享 Untrust 区段，同样，它们还共享 untrust-vr 以及在根级定义为可共享的其它虚拟路由器。

- 它自己的虚拟路由器

  缺省情况下， vsys 级的虚拟路由器命名为 *vsysname-vr*。您也可以自定义其名称以使该名称更有意义。这是 vsys 专用的虚拟路由器，缺省由该路由器来维护 Trust-*vsysname* 区段的路由表。所有 vsys 级的虚拟路由器皆不可共享。

您可以选择任一共享虚拟路由器或 vsys 级的虚拟路由器作为 vsys 的缺省虚拟路由器。要更改缺省虚拟路由器，进入 vsys，然后使用以下 CLI 命令：**set vrouter** *name* **default-vrouter**。

作为根级管理员，如果您想要所有 vsys 区段都在 untrust-vr 路由选择域中（例如，如果所有绑定到 Trust -*vsysname* 区段的接口都在 “路由” 模式下），则可以通过将 vsys 级安全区段从 *vsysname*-vr 改为 untrust-vr 的方式来免除 vsysname-vr。有关虚拟路由器的详细信息，请参阅第 **2** -51 页上的 “路由和虚拟路由器”。

***注意：** 此 ScreenOS 的发行版本不支持虚拟系统内用户定义的虚拟路由器。*

区段

当根级 admin 创建 vsys 对象时，将自动继承或创建以下区段：

- 所有共享区段 （从根系统继承而来）
- 共享的 Null 区段 （从根系统继承而来）
- Trust-*vsys_name* 区段
- Untrust-Tun-*vsys_name* 区段
- Self-*vsys_name* 区段
- Global-*vsys_name* 区段

vsys 与根系统共享 Untrust 区段和 Null 区段。 vsys 中的所有其它区段都属于此 vsys。

注意：*有关各区段类型的信息，请参阅第* ***2****-29 页上的 “区段”。*

接口

vsys 的 Untrust 和 Trust 区段可以支持以下三种接口：

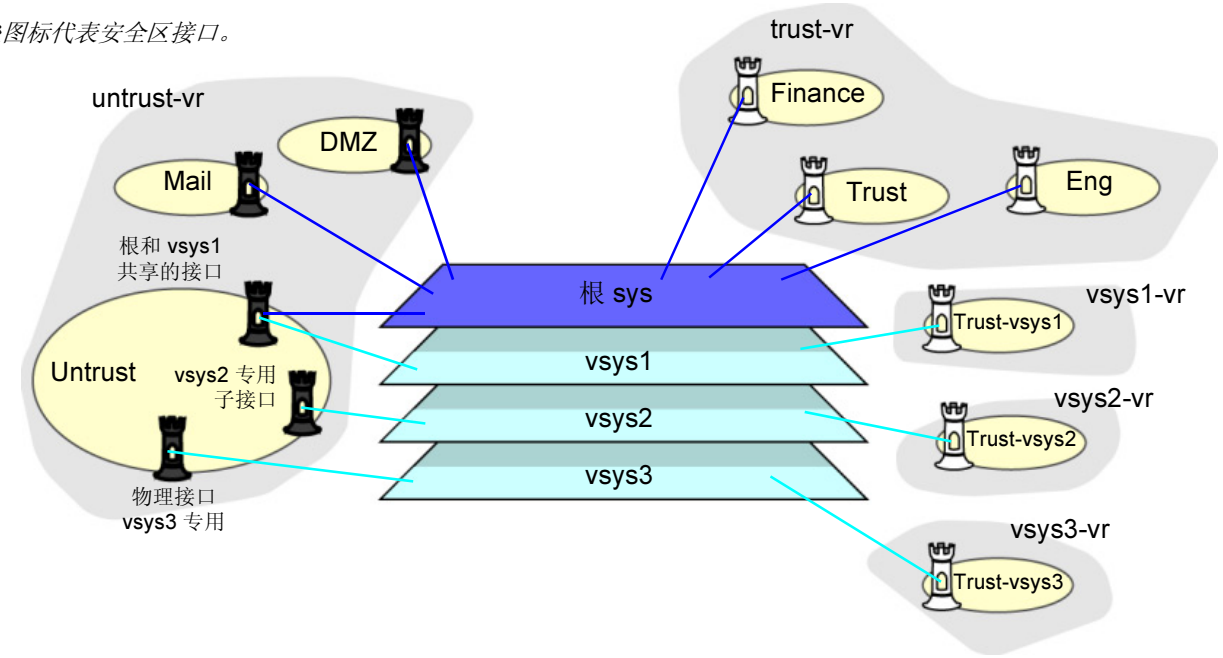
Untrust 区段接口类型	**Trust 区段接口类型**
• 物理接口	• 专用物理接口
• 子接口 （带有 VLAN 标记，作为一种中继* 入站和出站通信流的方法）	• 子接口 （带有 VLAN 标记）
• 与根系统共享的接口 （物理接口、子接口、冗余接口、聚合接口）	• 与根系统共享的物理接口 （以及基于 IP 的通信流分类†）

* 要了解 VLAN 标记和中继概念，请参阅第 18 页上的 “VLAN”。

† 有关基于 IP 的通信流分类的详细信息，请参阅第 28 页上的 “基于 IP 的通信流分类”。

可以同时将以上接口类型中的一种、两种或全部三种绑定到安全区段。也可将每一类型的多个接口绑定到某一区段。

注意： *堡垒图标代表安全区接口。*



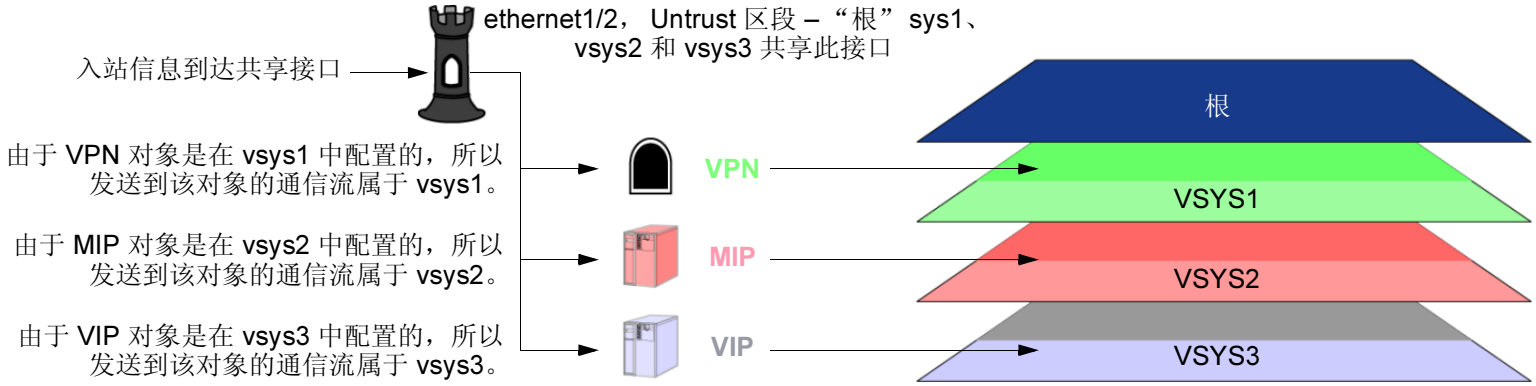
通信流分类

NetScreen 设备必须将其接收的每一个封包进行分类，以便将其传输到适当系统。NetScreen 设备接收两种用户通信流，并将其以两种不同方式进行分类：

- 发往设备本身上的 IP 地址的通信流，如加密 VPN 通信流以及发往 MIP 或 VIP 的通信流
- 发往设备之外的 IP 地址的通信流

发往 NetScreen 设备的通信流

对于发往 NetScreen 设备上的某一对象 （VPN、 MIP 或 VIP）的通信流，此设备通过该对象与在其中配置该对象的系统间的关联来确定通信流所属的系统。



入站通信流也可以通过 VPN 通道抵达 vsys ；但是，如果外向接口是共享接口，则不能为 vsys 以及到同一远程站点的根系统创建 “自动密钥 IKE VPN”通道。

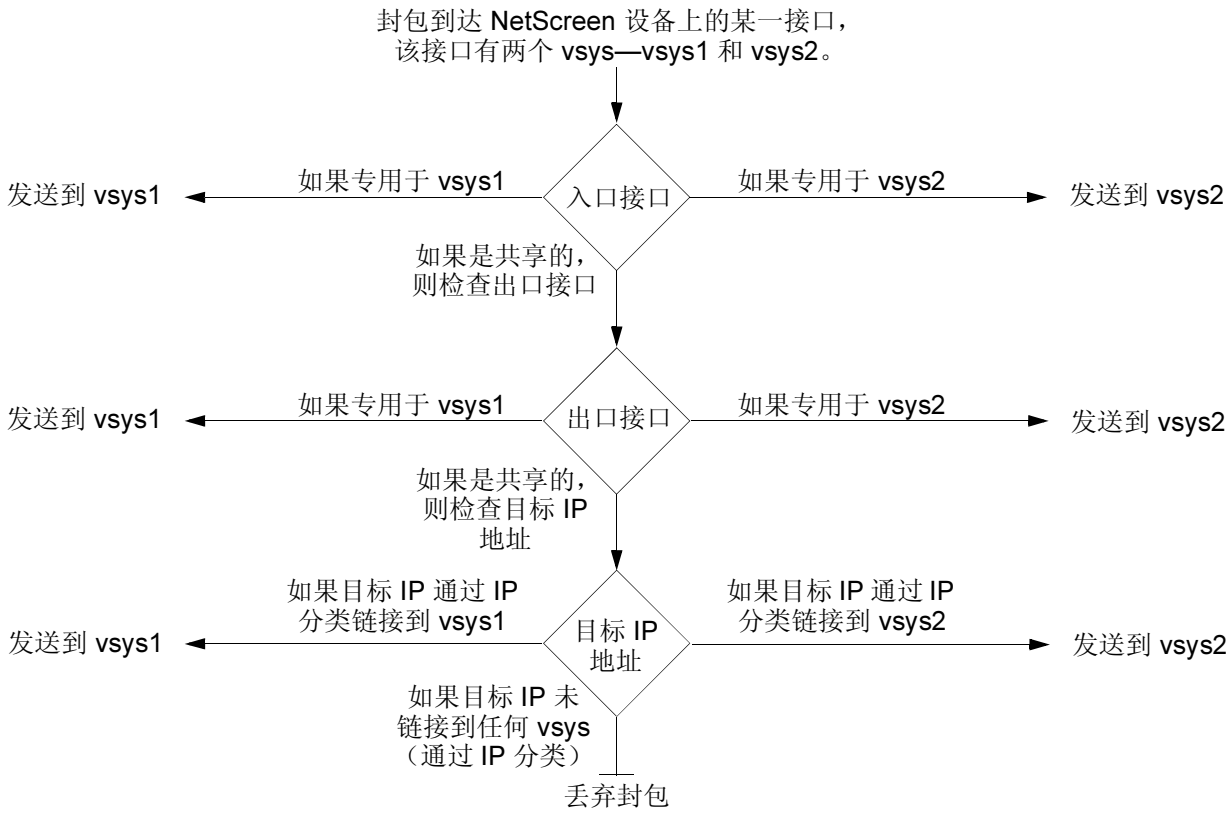
直通信息

对于发往不在 NetScreen 设备上的 IP 地址的通信流 （即通常所说的 “直通信息”），设备采用通过基于 VLAN 和基于 IP 的通信流分类而实现的技术。基于 VLAN 的通信流分类使用帧头中的 VLAN 标记[5] 来标识入站通信流所属的系统。基于 IP 的通信流分类使用 IP 封包头中的目标 IP 地址来标识入站通信流所属的系统。

NetScreen 设备用于确定封包所属的系统的过程按以下顺序进行：

1. 如果入口接口是专用[6] 接口，NetScreen 设备会将通信流与该接口专属的系统联系起来。
2. 如果入口接口是共享接口，NetScreen 设备将检查出口接口是共享的还是专用的。
3. 如果出口接口是专用的，NetScreen 设备会将通信流与该接口专属的系统联系起来。
4. 如果入口和出口接口都是共享的，则 NetScreen 会将通信流与目标 IP 地址绑定的系统联系起来。

5. VLAN 标记要求使用子接口。子接口必须是系统专用的，这一点与共享接口相反，共享接口由所有系统共享。
6. 有关共享和专用接口的详细信息，请参阅第 12 页上的 “专用和共享接口”。


封包到达 NetScreen 设备上的某一接口，
该接口有两个 vsys—vsys1 和 vsys2。
入口接口
如果专用于 vsys1
发送到 vsys1
如果专用于 vsys2
发送到 vsys2
如果是共享的，
则检查出口接口
出口接口
如果专用于 vsys1
发送到 vsys1
如果专用于 vsys2
发送到 vsys2
如果是共享的，
则检查目标 IP
地址
目标 IP
地址
如果目标 IP 通过 IP
分类链接到 vsys1
发送到 vsys1
如果目标 IP 通过 IP
分类链接到 vsys2
发送到 vsys2
如果目标 IP 未
链接到任何 vsys
（通过 IP 分类）
丢弃封包

专用和共享接口

有两种接口，它们会影响 NetScreen 设备将入站通信流恰当地分类到正确系统的方式，这两种接口分别是：专用接口和共享接口。

专用接口

系统（虚拟和根系统）可以拥有多个专门由系统自己使用的接口或子接口。此类接口不可为其它系统所共享。您可以将某接口专用于某系统，如下所示：

- 当在根系统中配置物理接口、子接口、冗余接口或聚合接口并将其绑定到不可共享区段时，该接口仍将专用于根系统。
- 当导入一个物理或聚合接口到 vsys 中并将其绑定到共享的 Untrust 区段或 Trust-*vsys_name* 区段时，此接口将变成该 vsys 的专用接口。
- 当在 vsys 中配置子接口时，该接口将属于此 vsys。

注意：*当系统中有专用子接口时，NetScreen 设备必须采用基于 VLAN 的通信流分类方法来正确地分类入站通信流。*

共享接口

系统（虚拟和根系统）可以与其它系统共享某一接口。对于可共享的接口，必须在根级对其进行配置并将其绑定到共享虚拟路由器中的共享区段。缺省情况下，预先定义的 untrust-vr 为共享虚拟路由器，预先定义的 Untrust 区段为共享区段。因此， vsys 可以共享任何绑定到 Untrust 区段的根级物理接口、子接口、冗余接口或聚合接口。

要在 Untrust 区段以外的某一区段创建共享接口，必须将该区段定义为根级共享区段。要做到这一点，该区段必须属于某一共享虚拟路由器，如 untrust-vr 或定义为可共享的任何其它根级虚拟路由器。然后，当将根级接口绑定到此共享区段时，该接口将自动变成共享接口。

注意：*要创建虚拟路由器，必须获得 vsys 许可密钥，它将为您提供定义在 vsys 或根系统中使用的虚拟系统、虚拟路由器和安全区段的能力。*

共享虚拟路由器可支持共享和不可共享的根级安全区段。您可以将绑定到共享虚拟路由器的根级区段定义为可共享或不可共享。任何绑定到共享虚拟路由器并且定义为可共享的根级区段都将变成共享区段，也可供虚拟系统使用。任何绑定到共享虚拟路由器并且定义为不可共享的根级区段仍将为专用区段，仅供根系统使用。如果将 vsys 级区段绑定到专用于该 vsys 的虚拟路由器或在根系统中创建的共享虚拟路由器，该区段仍为专用区段，仅供为其创建该区段的 vsys 使用。

共享区段可以支持共享和专用接口。任何绑定到共享区段的根级接口将成为共享接口，也可用于虚拟系统。任何绑定到共享区段的 vsys 级接口仍为专用接口，仅可用于为其创建该接口的 vsys。

不可共享区段仅可由在其中创建该区段的系统使用，并且仅支持该系统的专用接口。所有 vsys 级区段都是不可共享的。

要创建共享接口，必须先创建一个共享虚拟路由器 （或使用预先定义的 untrust-vr），创建一个共享安全区段 （或使用预先定义的 Untrust 区段），然后将此接口绑定到共享区段。必须在根系统中执行所有三个步骤。

WebUI 和 CLI 中的选项如下所示：

1. 要创建共享虚拟路由器：

   ### WebUI

   Network > Routing > Virtual Routers > New：选择 **Shared and accessible by other vsys** 选项，然后单击 **Apply**。

   ### CLI

   set vrouter name *name_str*

   set vrouter *name_str* **shared**

   （不可将已有共享虚拟路由器改为不共享，除非先删除所有的虚拟系统。但是，可以随时将非共享虚拟路由器改成共享虚拟路由器。）

2. 要创建共享区段，在根级下执行以下操作：

WebUI

注意：在本版发行时，能通过 CLI 定义共享区段。

CLI

set zone name *name_str*

set zone *zone* **vrouter** *sharable_vr_name_str*

set zone *zone* **shared**

3. 要创建共享接口，在根级下执行以下操作：

WebUI

Network > Interfaces > New（或 Edit，用于现有接口）：配置该接口并将其绑定到共享区段，然后单击 **OK**。

CLI

set interface *interface* **zone** *shared_zone_name_str*

当两个或更多个系统共享一个接口时，NetScreen 设备必须采用基于 IP 的通信流分类方法来正确地分类入站通信流。（有关基于 IP 的通信流分类的详细信息，包括演示如何为多个 vsys 对其进行配置的示例，请参阅第 28 页上的 “基于 IP 的通信流分类”。）

导入和导出物理接口

您可以使一个或多个物理接口专用于某一 vsys。事实上，是将物理接口从根系统导入到虚拟系统中。将物理接口导入 vsys 后，该接口即由 vsys 专用。

注意： *在将接口导入到虚拟系统前，该接口必须处于根级的 Null 区段中。*

范例：将物理接口导入到虚拟系统

在此例中，将把物理接口 ethernet4/1 导入到 vsys1 中。将其绑定到 Untrust 区段并为其分配 IP 地址 210.1.1.1/24。

WebUI

1. Vsys：单击 **Enter**（对于 vsys1）。
2. Network > Interfaces：单击 **Import**（对于 ethernet4/1）。
3. Network > Interfaces > Edit（对于 ethernet4/1）：输入以下内容，然后单击 **OK**：

   Zone Name：Untrust-vsys1

   IP Address/Netmask：210.1.1.1/24
4. 单击 **Exit Vsys** 按钮（在菜单栏的底部）返回到根级。

CLI

1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet4/1 import
3. ns(vsys1)-> set interface ethernet4/1 zone untrust-vsys1
4. ns(vsys11)-> set interface ethernet4/1 ip 210.1.1.1/24
5. ns(vsys1)-> save
6. ns(vsys1)-> exit

范例：从虚拟系统导出物理接口

在此例中，将物理接口 ethernet4/1 绑定到 vsys1 中的 Null 区段，并为其分配 IP 地址 0.0.0.0/0。然后将接口 ethernet4/1 导出到根系统。

WebUI

1. Vsys：单击 **Enter**（对于 vsys1）。
2. Network > Interfaces > Edit（对于 ethernet4/1）：输入以下内容，然后单击 **OK**：

   Zone Name：Null

   IP Address/Netmask：0.0.0.0/0
3. Network > Interfaces：单击 **Export**（对于 ethernet4/1）。

   现在，接口 ethernet4/1 可以在根系统中使用了。
4. 单击 **Exit Vsys** 按钮（在菜单栏的底部）返回到根级。

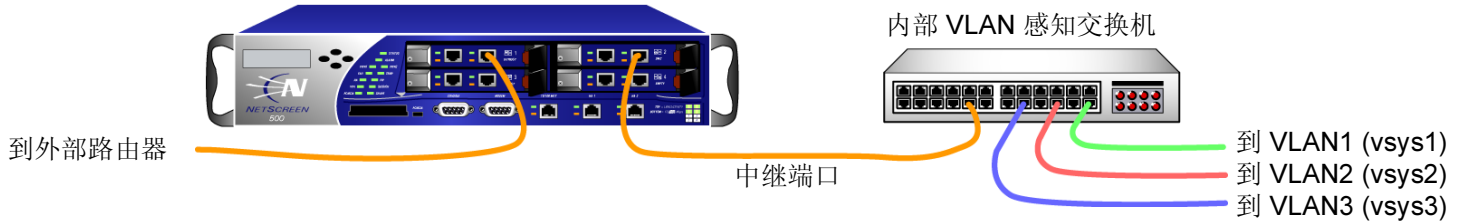
CLI

1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet4/1 ip 0.0.0.0/0
3. ns(vsys1)-> set interface ethernet4/1 zone null
4. ns(vsys1)-> set interface ethernet4/1 export
5. ns(vsys1)-> save

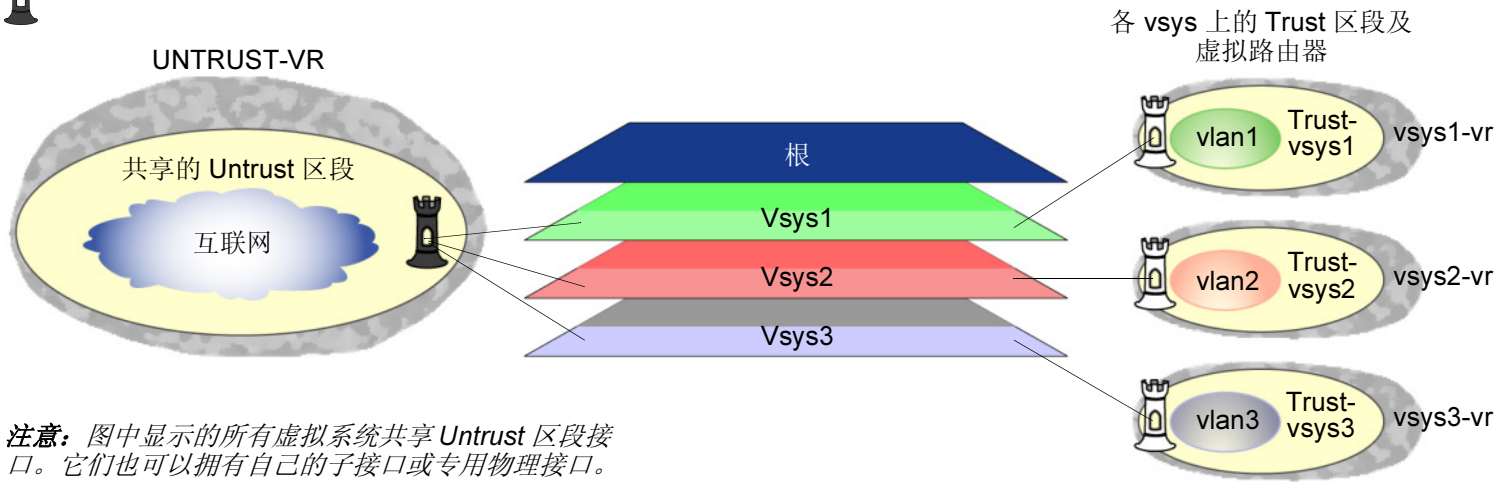
   现在，接口 ethernet4/1 可以在根系统中使用了。
6. ns(vsys1)-> exit

基于 VLAN 的通信流分类

当采用基于 VLAN 的通信流分类时，NetScreen 设备使用 VLAN 标记[7]将通信流导向绑定到不同系统的各个子接口[8]。缺省情况下，vsys 具有两个安全区段 — 共享的 Untrust 区段以及自身的 Trust 区段。每个 vsys 都可以与根系统以及其它虚拟系统共享 Untrust 区段接口。vsys 还可以拥有自己的子接口或绑定到 Untrust 区段的专用物理接口（从根系统导入）。



注意：*堡垒图标代表安全区接口。*



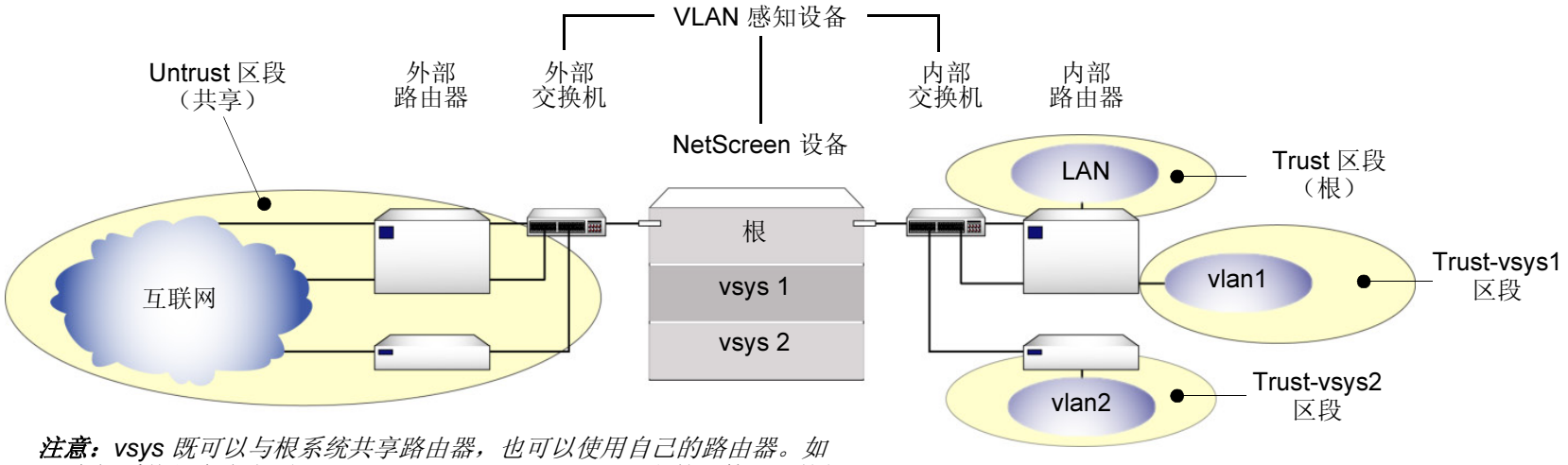
注意：*图中显示的所有虚拟系统共享 Untrust 区段接口。它们也可以拥有自己的子接口或专用物理接口。*

7. NetScreen 支持符合 IEEE 802.1Q VLAN 标准的 VLAN。
8. 可以通过将物理接口从根系统导入到虚拟系统的方式来使其专用于该虚拟系统。（请参阅第 15 页上的 “导入和导出物理接口”。）当使用物理接口时，该接口上的通信流无需 VLAN 标记。

VLAN

每个 VLAN 都通过子接口绑定到某一系统。如果 vsys 与根系统共享 Untrust 区段接口并且拥有绑定到其 Trust-*vsys_name* 区段的子接口，则必须将此 vsys 与 Trust-*vsys_name* 区段中的 VLAN 联系起来。如果此 vsys 还拥有自己的绑定到 Untrust 区段的子接口，还必须将此 vsys 与 Untrust 区段中的另一 VLAN 联系起来。

子接口源于物理接口，随后将充当中继端口。中继端口允许 “Layer 2 （第 2 层）” 网络设备通过单个物理端口捆绑来自多个 VLAN 的通信流，并按帧头中的 VLAN 标识符 (VID) 对各个封包进行分类。VLAN 中继允许一个物理接口支持多个逻辑子接口，每个子接口必须以唯一的 VLAN 标记进行标识。内向以太网帧中的 VLAN 标识符 （标记）指示其要发往的预定子接口（以及由此而及的系统）。当将 VLAN 与某一接口或子接口联系起来时，NetScreen 设备自动将该物理端口定义为中继端口。当在 “透明” 模式下使用根级 VLAN 时，必须使用以下 CLI 命令以手动方式将所有物理端口定义为中继端口：**set interface vlan1 vlan trunk**。



注意：*vsys 既可以与根系统共享路由器，也可以使用自己的路由器。如果虚拟系统具有绑定到 Untrust 和 Trust-*vsys_name *区段的子接口，外部和内部交换机必须是 VLAN 感知式的。*

当 vsys 使用绑定到 Trust-*vsys_name* 区段的子接口（非专用物理接口）时， Trust-*vsys_name* 区段中的内部交换机和内部路由器必须具有支持 VLAN 的能力。如果在某一物理接口上创建了多个子接口，则必须将连接交换机的端口定义为中继端口并使其成为使用该端口的所有 VLAN 中的成员。

当 vsys 使用绑定到共享 Untrust 区段的子接口（非共享接口或专用物理接口）时，接收其入站和出站通信流的外部交换机和外部路由器必须具有支持 VLAN 的能力。路由器会对内向帧进行标记，以便当内向帧到达 NetScreen 设备时，路由器可以将其导向正确的子接口。

虽然 vsys 不能处于“透明”模式下（因为它要求接口或子接口 IP 地址必须唯一），但根系统可以处于“透明”模式下[9]。要使根系统在“透明”模式下运行时支持 VLAN，请使用以下 CLI 命令以使绑定到“Layer 2（第 2 层）”安全区段的物理接口能够充当中继端口：**set interface vlan1 vlan trunk**。

定义子接口和 VLAN 标记

Trust-*vsys_name* 区段子接口将 vsys 链接到其内部的 VLAN。Untrust 区段子接口将 vsys 链接到公共的 WAN，通常是因特网。子接口具有以下属性：

- 唯一的 VLAN ID（从 1 到 4095）
- 公用或私有 IP 地址[10]（缺省情况下， IP 地址是私有的）
- A、 B 或 C 类子网的网络掩码
- 相关联的 VLAN

vsys 可以有一个 Untrust 区段子接口和多个 Trust-*vsys_name* 区段子接口。如果虚拟系统自己没有 Untrust 区段子接口，它将共享根级 Untrust 区段接口。 NetScreen 设备还支持根级子接口和 VLAN。

9. 当根系统处于“透明”模式下时，它不支持虚拟系统。但是，它可以在“透明”模式下支持根级 VLAN。
10. 有关公用和私有 IP 地址的信息，请参阅第 **2**-90 页上的“公开 IP 地址”和第 **2**-91 页上的“私有 IP 地址”。

vsys1 与根系统共享 Untrust 区段接口。
vsys2 和 **vsys100** 具有自己的绑定到 Untrust 区段的专用子接口。

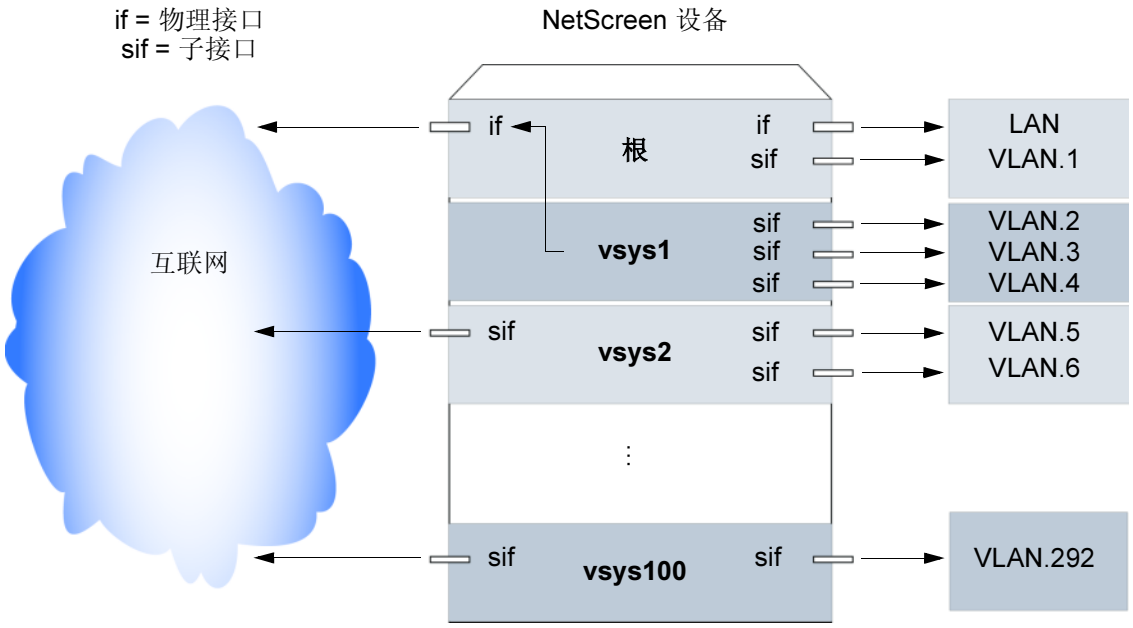
根系统具有绑定到其 Trust 区段的物理接口和子接口。

vsys1 具有三个绑定到其 Trust-vsys1 区段的子接口，每个接口都通往不同的 VLAN。

vsys2 具有两个绑定到其 Trust-vsys2 区段的子接口，每个接口都通往不同的 VLAN。

vsys100 具有一个绑定到其 Trust-vsys100 区段的子接口。

***注意：**各物理接口上的所有 VLAN ID 都必须唯一。*



NetScreen 设备支持符合 IEEE 802.1Q 的 VLAN 标记。标记是以太网帧头内的添加位，指示特定 VLAN 中的从属关系。通过将 VLAN 绑定到 vsys，此标记还可用于确定帧所属的 vsys，从而确定出应用到该帧的策略。如果 VLAN 未绑定到 vsys，那么在 NetScreen 设备的根系统中设置的策略将被应用到该帧。

根级管理员可以创建 VLAN、为其指定成员以及将其绑定到 vsys。（为 VLAN 指定成员可以通过多种方法 （协议类型、 MAC 地址、端口号）完成，此内容超出了本文档的范围。）vsys admin（如果有的话）接着可以通过创建地址、用户、服务、 VPN 和策略来管理 vsys。如果没有 vsys admin，那么根级管理员将执行这些任务。

***注意：**如果根级 admin 未将 VLAN 关联到 vsys， VLAN 将在 NetScreen 设备根系统中运行。*

要为 vsys 创建 VLAN，根级管理员必须执行以下三个任务：进入虚拟系统、定义子接口并将其与 VLAN 联系起来。

注意：vsys 中的所有子网都必须是互不相关的，也就是说，在同一 vsys 的子网中，一定没有重叠的 IP 地址。例如：Subinterface1 – 10.2.2.1 255.255.255.0 和 Subinterface2 – 10.2.3.1 255.255.255.0 是不相关的，因此，将链接到可接受的子网。

但是，具有以下子接口的子网相互重叠，因而在同一 vsys 中是不可接受的：Subinterface1 – 10.2.2.1 255.255.0.0 和 Subinterface2 – 10.2.3.1 255.255.0.0。

不同虚拟系统中子网的地址范围可以重叠。

范例：定义三个子接口和 VLAN 标记

在此例中，将为在第 3 页上的 “范例：创建 Vsys 对象和 Vsys Admin”中创建的三个虚拟系统 — vsys1、 vsys2 和 vsys3 定义子接口和 VLAN 标记。前两个子接口用于两个在 NAT 模式下运行的私有虚拟系统，第三个子接口用于在“路由”模式下运行的公用虚拟系统。子接口为 10.1.1.1/24、 10.2.2.1/24 和 210.3.3.1/24。在 ethernet3/2 上创建所有三个子接口。

WebUI

1. Vsys：单击 **Enter**（对于 vsys1）。
2. Network > Interfaces > New Sub-IF（对于 ethernet3/2）：输入以下内容，然后单击 **OK**：

   Interface Name：ethernet3/2.1

   Zone Name：Trust-vsys1

   IP Address/Netmask：10.1.1.1/24

   VLAN Tag：1[11]

11. 可以定义在 “路由”模式或 NAT 模式下运行的虚拟系统。缺省为 NAT 模式，因此，在此例中无需指定何时创建前两个子接口。

3. Vsys：单击 **Enter**（对于 vsys2）。
4. Network > Interfaces > New Sub-IF（对于 ethernet3/2）：输入以下内容，然后单击 **OK**：

   Interface Name：ethernet3/2.2

   Zone Name：Trust-vsys2

   IP Address/Netmask：10.2.2.1/24

   VLAN Tag：2
5. Vsys：单击 **Enter**（对于 vsys3）。
6. Network > Interfaces > New Sub-IF（对于 ethernet3/2）：输入以下内容，然后单击 **Apply**：

   Interface Name：ethernet3/2.3

   Zone Name：Trust-vsys3

   IP Address/Netmask：210.3.3.1/24

   选择 **Interface Mode**：**Route**，然后单击 **OK**。
7. 单击 **Exit Vsys** 返回到根级。

CLI

1. ns-> enter vsys vsys1
2. ns(vsys1)-> set interface ethernet3/2.1 zone trust-vsys1
3. ns(vsys1)-> set interface ethernet3/2.1 ip 10.1.1.1/24 tag 1[12]
4. ns(vsys1)-> save
5. ns(vsys1)-> exit
6. ns-> enter vsys vsys2
7. ns(vsys2)-> set interface ethernet3/2.2 zone trust-vsys2
8. ns(vsys2)-> set interface ethernet3/2.2 ip 10.2.2.1/24 tag 2
9. ns(vsys2)-> save
10. ns(vsys2)-> exit
11. ns-> enter vsys vsys3
12. ns(vsys3)-> set interface ethernet3/2.3 zone trust-vsys3
13. ns(vsys3)-> set interface ethernet3/2.3 ip 210.3.3.1/24 tag 3
14. ns(vsys3)-> set interface ethernet3/2.3 route
15. ns(vsys3)-> save
16. ns(vsys3)-> exit

12. 可以定义在 “路由”模式或 NAT 模式下运行的虚拟系统。缺省为 NAT 模式，因此，在此例中无需指定何时创建前两个子接口。

VLAN 之间的通信

不限制 vsys 中的 VLAN 成员彼此间的通信访问。不同 vsys 的 VLAN 成员彼此间不能通信，除非协同的 vsys 管理员配置了明确的策略，允许各自系统的成员间可以互相通信。

根级 VLAN 间的通信流在由根级策略设置的参数范围内运行。虚拟系统 VLAN 间的通信流在由协同虚拟系统策略设置的参数范围内运行[13]。只有允许离开始发虚拟系统的通信流和允许进入目标虚拟系统的通信流可以通过。换句话说，两个虚拟系统的虚拟系统管理员都必须设置策略，允许通信流以正确的方向 （外向和内向）流动。

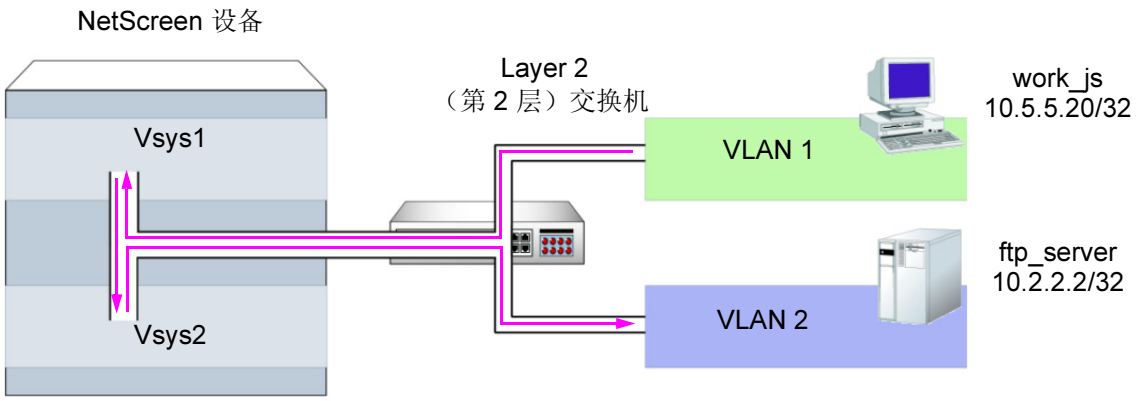
范例：VLAN 间的通信

在此例中，将设置两组策略以启动 VLAN 1 中的工作站 （work_js， IP 地址为 10.5.5.20/32）和 VLAN 2 中的服务器（ftp_server， IP 地址为 10.2.2.2/32）之间的通信流。如果满足以下两个条件，两者之间就可以进行连接：

- vsys1 的 vsys admin 设置的策略允许通信流从 VLAN 1 中的工作站流到 VLAN 2 中的服务器。
- vsys2 的 vsys admin 设置的策略允许通信流从 VLAN 1 中的工作站流到 VLAN 2 中的服务器。

请注意， NetScreen 设备上的内部接口前的网络设备是 “Layer 2 （第 2 层）” 交换机。这将迫使来自 VLAN 1 的通信流流到 VLAN 2 以通过交换机到达用于“Layer 3（第 3 层）”路由选择的 NetScreen 设备。如果网络设备是“Layer 3（第 3 层）”路由器，则 VLAN1 和 VLAN2 间的通信流就可以通过此路由器，同时绕过 NetScreen 设备上设置的所有策略。

13. 在根系统中设置的策略不影响在虚拟系统中设置的策略，反之亦然。



WebUI

Vsys1

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

   Address Name: work_js

   IP Address/Domain Name:

   IP/Netmask: 10.5.5.20/32

   Zone: Trust-vsys1

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

   Address Name: ftp_server

   IP Address/Domain Name:

   IP/Netmask: 10.2.2.2/32

   Zone: Untrust

3. Policies >（From：Trust-vsys1，To：Untrust）New：输入以下内容，然后单击 **OK**：

   Source Address：

   Address Book：（选择）， work_js

   Destination Address：

   Address Book：（选择）， ftp_server

   Service：FTP-Get

   Action：Permit

Vsys2

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

   Address Name：ftp_server

   IP Address/Domain Name：10.2.2.2

   Netmask：255.255.255.255

   Zone：Trust-vsys2

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

   Address Name：work_js

   IP Address/Domain Name：

   IP/Netmask：10.5.5.20/32

   Zone：Untrust

3. Policies >（From：Untrust，To：Trust-vsys2）New：输入以下内容，然后单击 **OK**：

   Source Address：

   Address Book：（选择）， work_js

   Destination Address：

   Address Book：（选择）， ftp_server

   Service：FTP-Get

   Action：Permit

CLI

Vsys1

1. set address trust-vsys1 work_js 10.5.5.20/32
2. set address untrust ftp_server 10.2.2.2/32
3. set policy from trust-vsys1 to untrust work_js ftp_server ftp-get permit
4. save

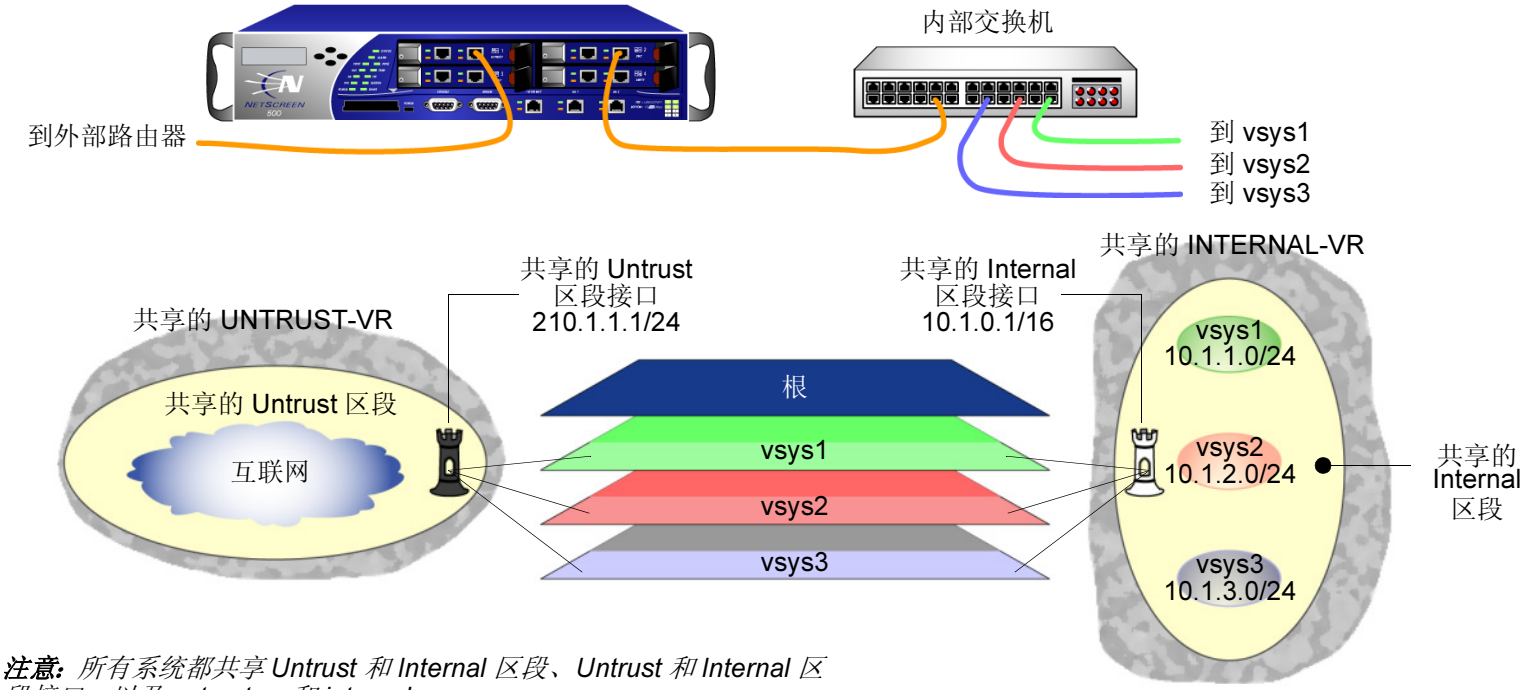
Vsys2

1. set address trust-vsys2 ftp_server 10.2.2.2/32
2. set address untrust work_js 10.5.5.20/32
3. set policy from untrust to trust-vsys2 work_js ftp_server ftp-get permit
4. save

基于 IP 的通信流分类

基于 IP 的通信流分类允许您不用 VLAN 而使用虚拟系统。 NetScreen 设备使用 IP 地址 （而不是 VLAN 标记）分类通信流，将子网或 IP 地址范围与特定系统 （根或 vsys）联系起来。单独采用基于 IP 的通信流分类方法来分类通信流，所有系统共享以下各项：

- untrust-vr 和用户定义的 internal-vr
- Untrust 区段和用户定义的内部区段
- Untrust 区段接口和用户定义的内部区段接口[14]



注意：*所有系统都共享 Untrust 和 Internal 区段、Untrust 和 Internal 区段接口，以及 untrust-vr 和 internal-vr。*

14. 即使将基于 VLAN 的通信流分类方法用于内部通信流，但对于外部通信流，所有系统都将使用共享的 Untrust 区段以及共享的 Untrust 区段接口 （除非系统有专用接口）。可以采取混合方法，在一边使用共享接口，在另一边使用专用接口（具有 VLAN 标记）。基于 VLAN 和基于 IP 的通信流分类可以同时在同一系统内或不同系统间共存。

要为根系统或先前创建的虚拟系统指定子网或 IP 地址范围，必须在根级发出以下某一 CLI 命令：

set zone *zone* **ip-classification net** *ip_addr/mask* **{ root | vsys** *name_str* **}**

set zone *zone* **ip-classification range** *ip_addr1-ip_addr2* **{ root | vsys** *name_str* **}**

由于基于 IP 的通信流分类方法要求使用共享安全区段，所以虚拟系统不能使用重叠的内部 IP 地址，但对于基于 VLAN 的通信流分类方法却可以。此外，由于所有系统共享相同的内部接口，所以该接口的运行模式必须是 NAT 或“路由”模式；不可以将 NAT 模式和 “路由”模式混合用于不同的系统。从这层意义而言，基于 IP 的方法的编址方案就不如更常用的基于 VLAN 的方法所允许的方案灵活。

进一步讲，共享虚拟路由器、安全区段和接口自然就不如每一 vsys 专用一个内部虚拟路由器、内部安全区段以及内部和外部接口安全。当所有虚拟系统共享同样的接口时，某一 vsys 中的 vsys admin 可以使用 **snoop** 命令收集有关另一 vsys 的通信活动的信息。此外，由于在内部方也可以进行 IP 欺骗，NetScreen 建议您禁用共享内部接口上的 IP 欺骗 SCREEN 选项。在决定使用哪种通信流分类方案时，必须在基于 IP 方法提供的管理便利性与基于 VLAN 方法提供的增强安全性和更大的编址灵活性之间进行权衡。

范例：配置基于 IP 的通信流分类

在此例中，将为在第 3 页上的“范例：创建 Vsys 对象和 Vsys Admin”中创建的三个虚拟系统设置基于 IP 的通信流分类。您定义 trust-vr 为可共享的。建立新区段，命名为 *Internal*，然后将其绑定到 trust-vr。然后将 Internal 区段当作可共享区段。将 ethernet3/2 绑定到共享的 Internal 区段，为其分配 IP 地址 10.1.0.1/16，并选择 NAT 模式。

将 ethernet1/2 绑定到共享的 Untrust 区段并为其分配 IP 地址 210.1.1.1/24。 Untrust 区段中缺省网关的 IP 地址为 210.1.1.250。 Internal 和 Untrust 区段都在共享的 trust-vr 路由选择域中。

子网及其各自的 vsys 联系如下所示：

- 10.1.1.0/24 – vsys1
- 10.1.2.0/24 – vsys2
- 10.1.3.0/24 – vsys3

WebUI

虚拟路由器、安全区段和接口

1. Network > Routing > Virtual Routers > Edit（对于 trust-vr）：选中 **Shared and accessible by other vsys** 复选框，然后单击 **OK**。
2. Network > Zones > New：输入以下内容，然后单击 **OK**：

   Zone Name: Internal

   Virtual Router Name: trust-vr

   Zone Type: Layer 3
3. Network > Zones > Edit(对于 Internal)：选中 **Share Zone** 复选框，然后单击 **OK**。
4. Network > Interfaces > Edit（对于 ethernet3/2）：输入以下内容，然后单击 OK：

   Zone Name: Internal

   IP Address/Netmask：10.1.0.1/16

5. Network > Interfaces > Edit（对于 ethernet3/2）：输入以下内容，然后单击 OK：
   Zone Name: Untrust
   IP Address/Netmask：210.1.1.1/24

路由

6. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 OK：
   Network Address/Netmask: 0.0.0.0/0l
   Gateway: (select)
   Interface: ethernet1/2
   Gateway IP Address: 210.1.1.250

Trust 区段的 IP 分类

> ***注意：****在写入时，仅可通过 CLI 配置基于 IP 的通信流分类。*

CLI

虚拟路由器、安全区段和接口

1. set vrouter trust-vr shared
2. set zone name Internal
3. set zone Internal shared
4. set interface ethernet3/2 zone Internal
5. set interface ethernet3/2 ip 10.1.0.1/16
6. set interface ethernet3/2 nat
7. set interface ethernet1/2 zone untrust
8. set interface ethernet1/2 ip 210.1.1.1/24

路由

9. set vrouter trust-vr route 0.0.0.0/0 interface ethernet1/2 gateway 210.1.1.250

Trust 区段的 IP 分类

10. set zone Internal ip-classification net 10.1.1.0/24 vsys1
11. set zone Internal ip-classification net 10.1.2.0/24 vsys2
12. set zone Internal ip-classification net 10.1.3.0/24 vsys3
13. set zone Internal ip-classification
14. save

以 VSYS ADMIN 身份登录

与根级管理员从根级进入 vsys 不同， vsys admin 可直接进入自己的 vsys。当根级管理员退出 vsys 时，该管理员将退出到根系统。当 vsys admin 退出 vsys 时，将立即切断连接。

以下范例演示了如何以 vsys admin 身份登录到 vsys，如何更改密码以及注销。

范例：登录并更改密码

在此例中，您 （作为 vsys admin）将通过输入分配的登录名 jsmith 和密码 Pd50iH10 登录到 vsys1。将密码更改为 I6Dls13guh，然后注销。

注意：*vsys admin 不可以更改其登录名 （用户名），因为 NetScreen 设备将使用该名称来选择此次登录连接的路由以将转到相应的 vsys，该名称在所有 vsys admin 中必须唯一。*

WebUI

登录

1. 在 Web 浏览器的 URL 字段中，输入 vsys1 的 Untrust 区段接口 IP 地址。
2. 当出现 Network Password 对话框时，输入以下内容，然后单击 **OK**：

   User Name：jsmith

   Password：Pd50iH10

更改密码

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

   Vsys Admin Old Password：Pd50iH10

   Vsys Admin New Password：I6Dls13guh

   Confirm New Password：I6Dls13guh

注销

4. 单击 **Logout**，位于菜单栏的底部。

CLI

登录

1. 在“安全命令外壳”(SCS)、Telnet 或“超级终端”会话的命令行提示中，输入 vsys1 的Untrust区段接口 IP 地址。
2. 使用以下用户名和密码登录：
   - User Name：jsmith
   - Password：Pd50iH10

更改密码

3. set admin password I6Dls13guh
4. save

注销

5. exit

索引