NetScreen 概念与范例

ScreenOS 参考指南

第 10 卷 : 高可用性

ScreenOS 5.1.0

编号 093-1375-000-SC

修订本 B

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言 iii
约定 iv
CLI 约定 iv
WebUI 约定 v
插图约定 vii
命名约定和字符类型 viii
Juniper Networks NetScreen 文档 ix
第 1 章 NSRP 1
NSRP 概述 3
NSRP 和 NetScreen 的操作模式 8
基本主动 / 被动 NSRP 配置 8
缺省设置 9
范例 : 主动 / 被动配置的 NSRP 10
NSRP 集群 16
集群名称 18
范例 : 创建 NSRP 集群 19
执行对象 22
RTO 镜像状态 23
VSD 组 24
抢先选项 24
VSD 组成员状态 25
心跳信号消息 26
范例 : 创建两个 VSD 组 27
VSI 和静态路由 29
范例 : Trust 和 Untrust 区段 VSI 30
同步 34
同步配置 34
同步文件 35
同步 RTO 35
范例 : 手动重新同步 RTO 36
范例 : 将设备添加到活动的 NSRP 集群 37
同步系统时钟 38
双 HA 接口 39
控制消息 40
数据消息 (数据包转发) 41
动态路由选择警告信息 42
双 HA 链接探查 43
范例 : 手动发送链接探查 44
范例 : 自动发送链接探查 45
设置过程 46
全网状配置的电缆连接 46
双主动 NSRP 配置 50
范例 : 双主动配置的 NSRP 50
第 2 章 接口冗余 59
冗余接口 60
范例 : 为 VSI 创建冗余接口 62
聚合接口 67
范例 : 配置聚合接口 68
Dual Untrust 接口 69
接口故障切换 70
范例 : 将信息流强制转发到备份接口 70

范例：将信息流从备份接口切换回主接口 70
范例：自动改发信息流 71
确定接口故障切换 72
使用 IP 跟踪的接口故障切换 73
范例：接口故障切换 73
范例：由活动通道到备份通道的故障切换 78
使用 VPN 通道监控的接口故障切换 85
范例：双活动通道 86
范例：对通道故障切换应用权重 93
串行接口 103
调制解调器的设置 104
范例：配置调制解调器的设置 105
ISP 配置 106
范例：配置 ISP 信息 107
串行接口故障切换 108
范例：配置 Trust-Untrust 模式下的拨号备份 109
范例：删除串行接口的缺省路由 112
范例：为串行接口添加缺省路由 112
范例：指定策略在串行接口故障切换后处于非活动状态 113
第 3 章 故障切换 115
设备故障切换 (NSRP) 116
VSD 组故障切换 (NSRP) 117
为设备或 VSD 组故障切换配置对象监控 118
配置被监控对象 120
物理接口对象 120
范例：监控接口 120
区段对象 121
范例：监控接口 121
被跟踪 IP 对象 122
范例：跟踪 IP 地址确定设备故障切换 125
虚拟系统故障切换 130
范例：虚拟系统间负载共享的 VSI 130
第 4 章 NSRP-Lite 137
NSRP-Lite 简介 139
集群和 VSD 组 140
缺省设置 141
集群 142
集群名称 143
认证和加密 144
VSD 组 145
VSD 组成员状态 145
心跳信号消息 146
抢先选项 147
用电缆连接和配置 NSRP-Lite 148
范例：配置 NSRP-Lite 149
配置和文件同步 156
同步配置 156
同步文件 157
范例：将设备添加到活动的 NSRP 集群 157
自动配置同步 158
路径监控 159
设置临界值 160
对被跟踪的 IP 地址加权 160
VPN 通道故障切换的 IP 跟踪 161
范例：通过 VPN 通道的 IP 跟踪 162
索引 ..... IX-I

前言

第 10 卷，“高可用性”提供了 “NetScreen 冗余协议” (NSRP) 操作的概述，并说明了如何连接电缆、配置和管理一个冗余组中的 NetScreen 设备，从而使用 NSRP 提供高可用性。本卷还介绍 NetScreen 设备上提供接口冗余的各种方法，以及当存在冗余组件时如何为故障切换配置设备。此外还将介绍 NSRP-Lite，它是不支持执行对象 (RTO) 同步的 NSRP 的简化版。

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

- “CLI 约定”
- 第 v 页上的 “WebUI 约定”
- 第 vii 页上的 “插图约定”
- 第 viii 页上的 “命名约定和字符类型”

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

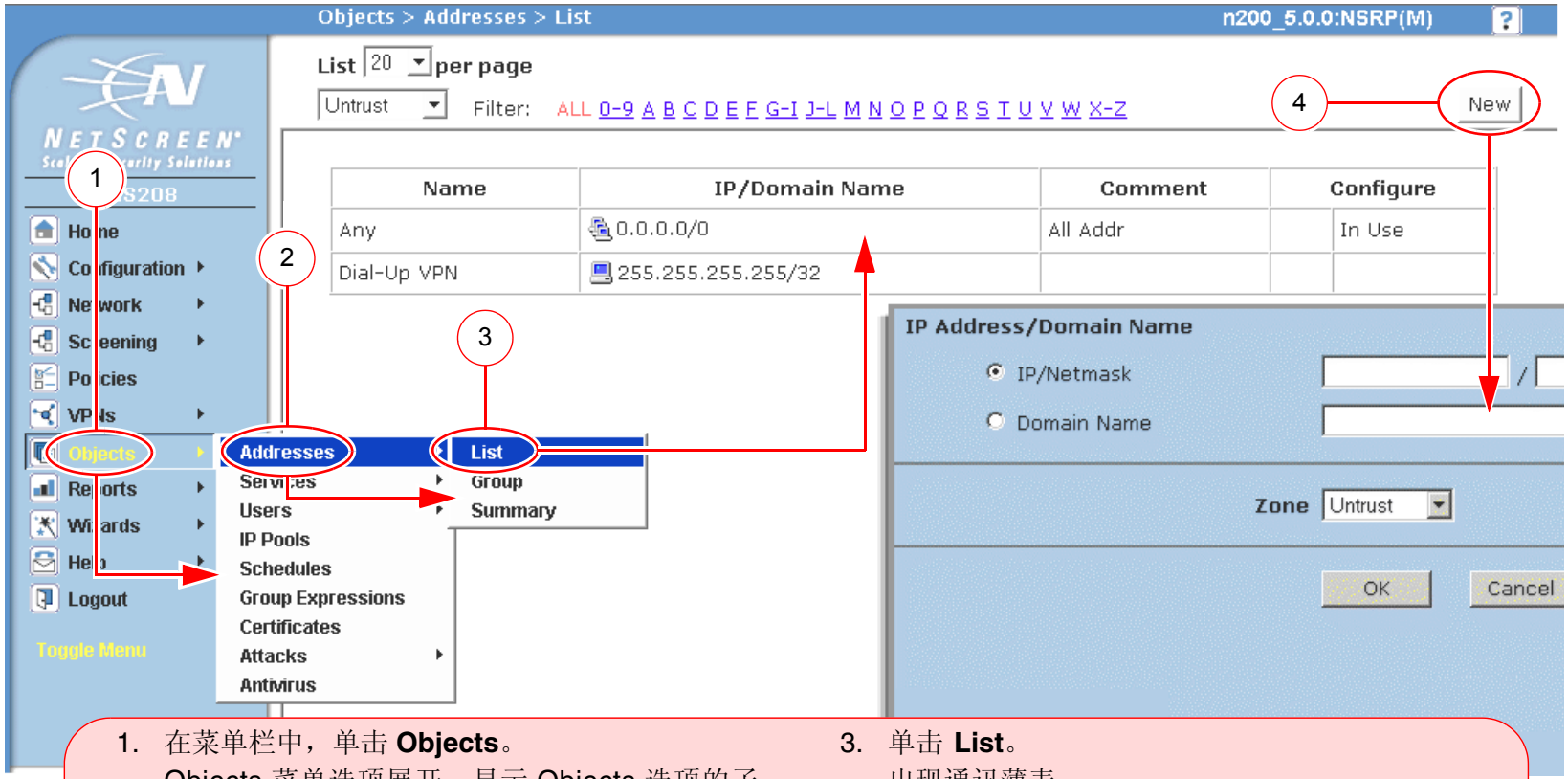
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

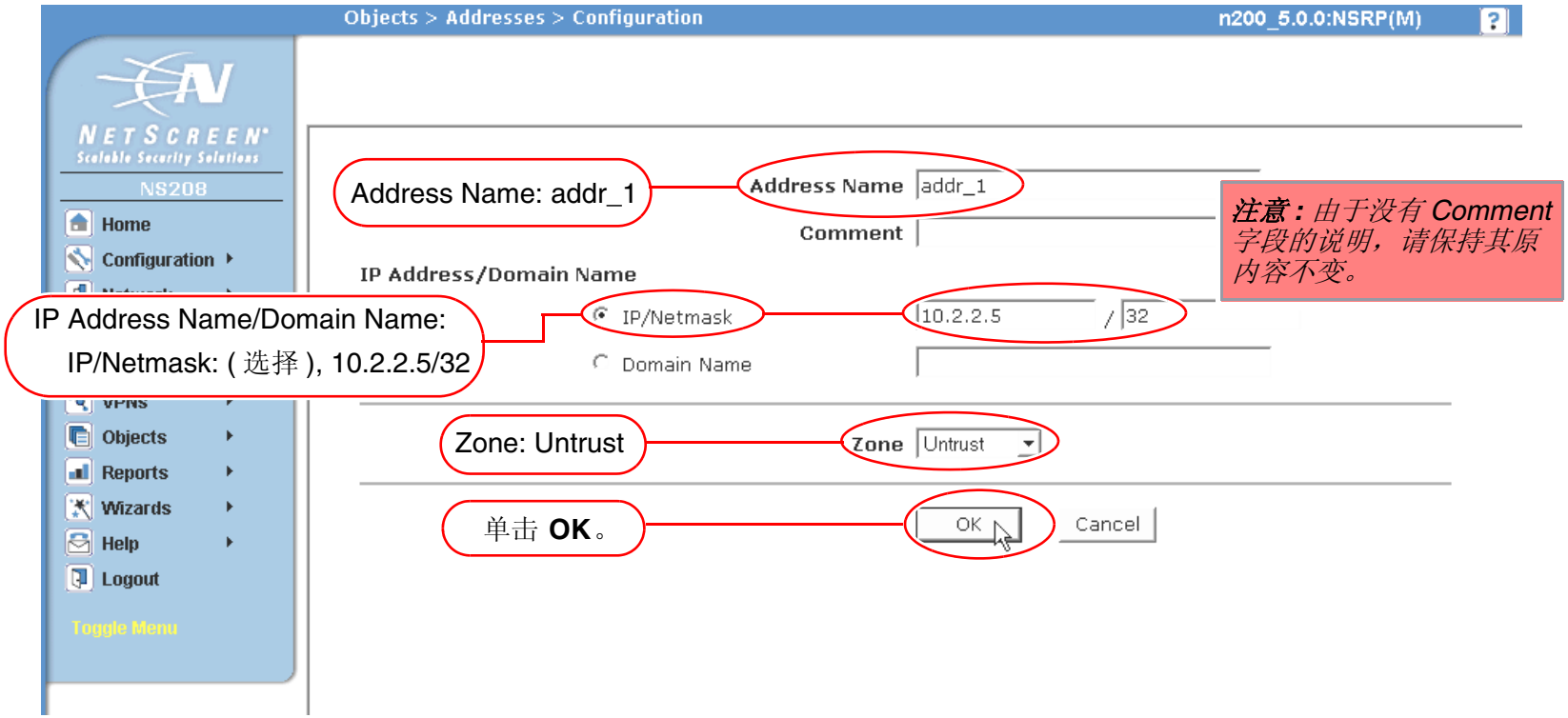
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

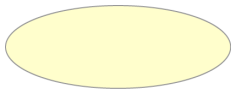


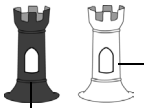
插图约定

下列图形构成了贯穿本书的插图所用的基本图像集：


通用 NetScreen 设备


虚拟路由选择域

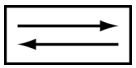

安全区段


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


通道接口

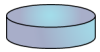

VPN 通道


路由器图标


交换机图标


包含单个子网的局域网 (LAN)
（例如：10.1.1.0/24）


互联网


动态 IP (DIP) 池


台式计算机


便携式计算机


通用网络设备
（例如：NAT 服务器，
接入集中器）


服务器

命名约定和字符类型

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

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

ScreenOS 支持以下字符类型 :

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

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

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

JUNIPER NETWORKS NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

NSRP

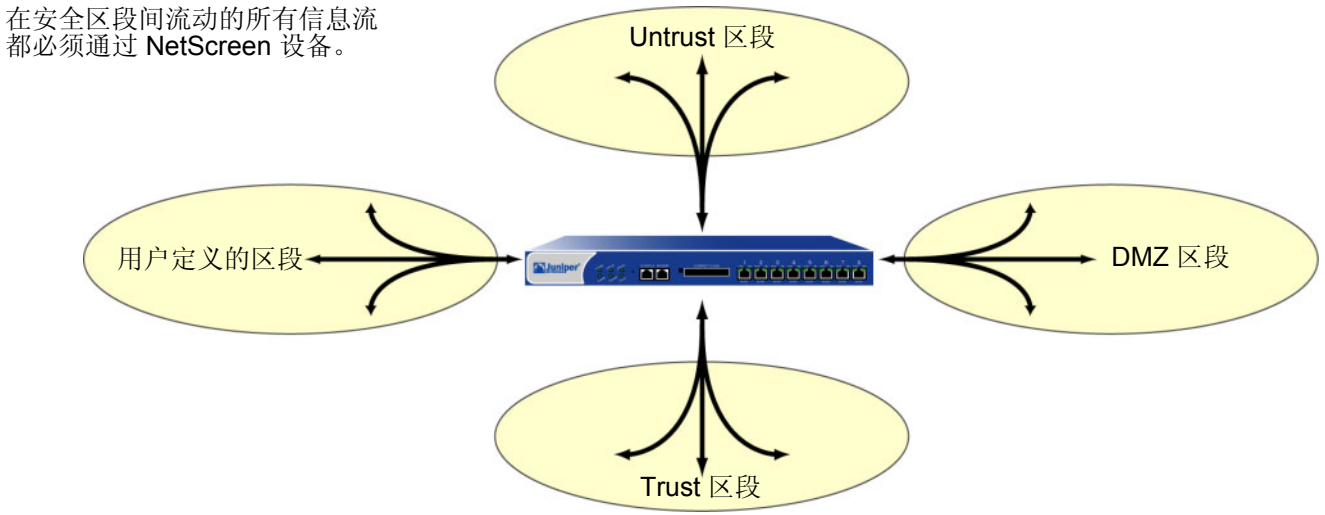
“NetScreen 冗余协议 (NSRP)”是一种在选定的 NetScreen 设备上支持的、可提供高可用性 (HA) 服务的专有协议。本章解释 NSRP 的组成并描述如何为 HA 使用 NSRP 配置 NetScreen 设备。本章所涵盖的具体主题如下：

- 第 3 页上的 “NSRP 概述”
- 第 8 页上的 “NSRP 和 NetScreen 的操作模式”
  - 第 8 页上的 “基本主动 / 被动 NSRP 配置”
- 第 16 页上的 “NSRP 集群”
  - 第 18 页上的 “集群名称”
  - 第 22 页上的 “执行对象”
- 第 24 页上的 “VSD 组”
  - 第 24 页上的 “抢先选项”
  - 第 25 页上的 “VSD 组成员状态”
  - 第 26 页上的 “心跳信号消息”
  - 第 29 页上的 “VSI 和静态路由”
- 第 34 页上的 “同步”
  - 第 34 页上的 “同步配置”
  - 第 35 页上的 “同步文件”
  - 第 35 页上的 “同步 RTO”
  - 第 38 页上的 “同步系统时钟”

- 第 39 页上的 “双 HA 接口”
  - 第 40 页上的 “控制消息”
  - 第 41 页上的 “数据消息 (数据包转发)”
  - 第 43 页上的 “双 HA 链接探查”
- 第 46 页上的 “设置过程”
  - 第 46 页上的 “全网状配置的电缆连接”
  - 第 50 页上的 “双主动 NSRP 配置”

NSRP 概述

要正确发挥网络防火墙的作用，必须将 NetScreen 设备放置在所有区段间信息流都必须通过的单一点上。

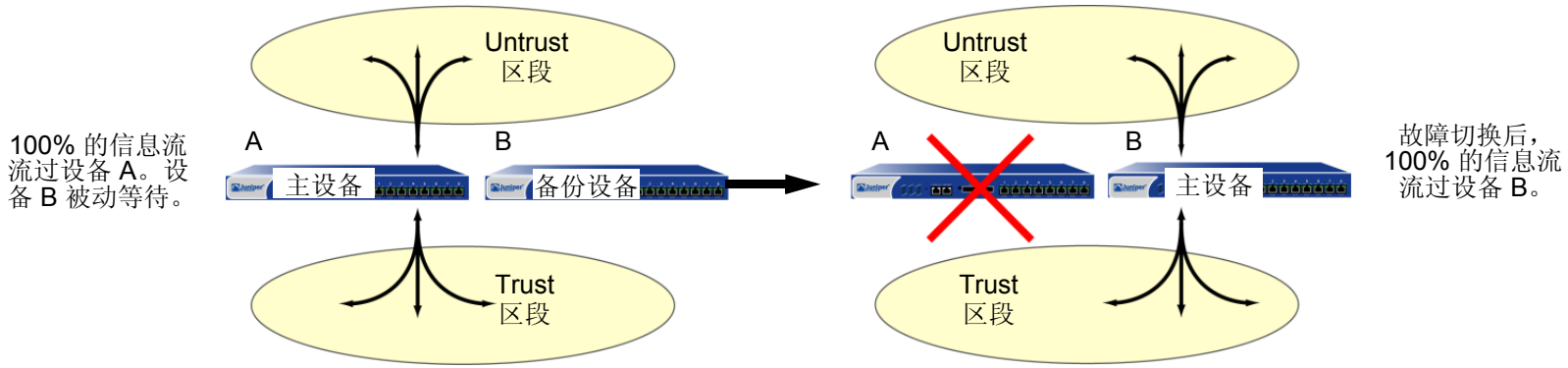


由于 NetScreen 设备是所有区段间信息流都必须通过的单一点，因此，保持信息流不中断流动至关重要，即使在设备或网络发生故障时也应如此。

要确保信息流的连续流动，可以通过冗余集群方式用电缆连接并配置两台 NetScreen 设备，其中一台作为主设备，另一台作为它的备份设备。主设备将其所有的网络和配置设置以及当前会话的信息传播到备份设备。当主设备出现故障时，备份设备会晋升为主设备并接管信息流处理。

注意：为简化故障切换概念，仅显示 Trust 和 Untrust 区段。

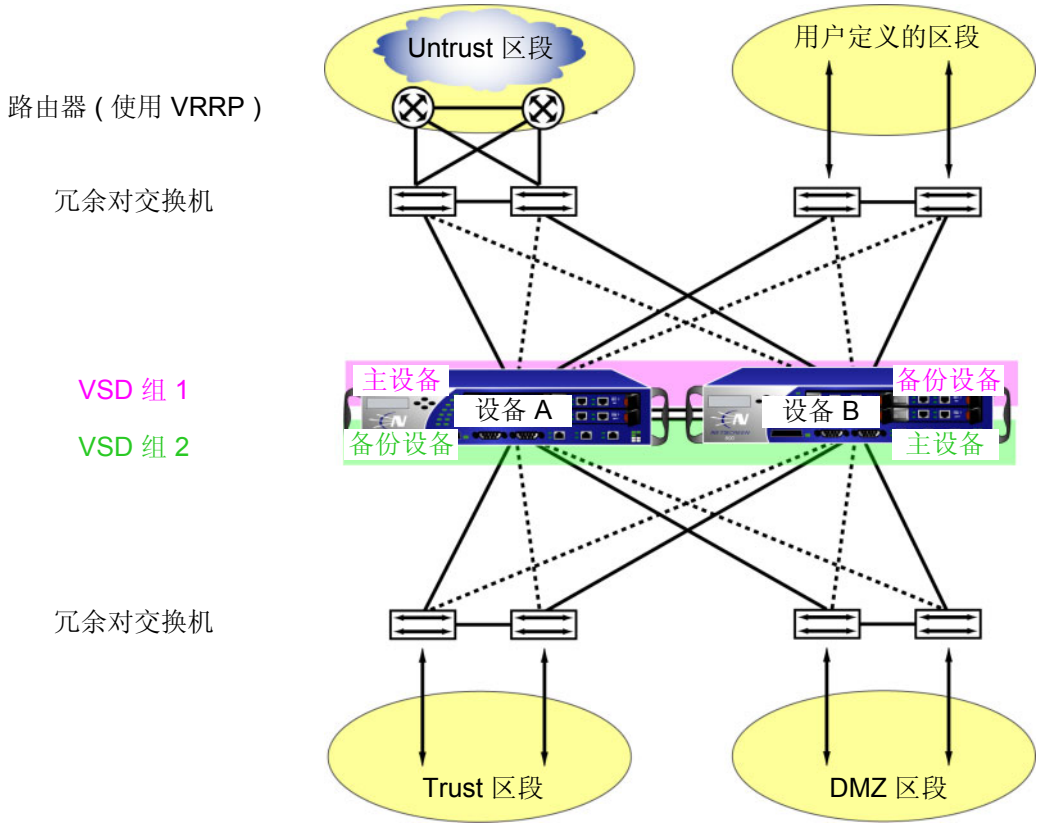
主动 / 被动故障切换



在这种情况下，两个设备处于主动 / 被动配置；即主设备为主动状态，处理所有防火墙和 VPN 活动；备份设备为被动[1] 状态，等待主设备让位时接管。

1. 尽管就未处理信息流而言，备份设备处于被动状态，但是在通过从主设备连续接收的配置设置和会话信息保持同步方面，却相当活跃。

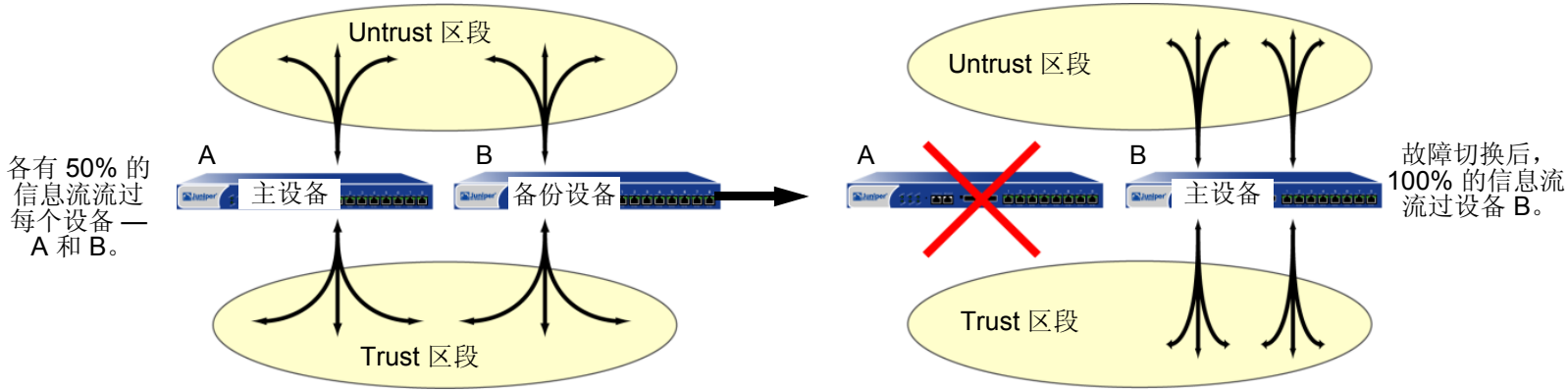
NetScreen 设备处于 “路由” 或 NAT 模式时，可以将冗余集群中的两台设备都配置为主动，通过具有负载均衡能力的路由器，运行诸如 “虚拟路由器冗余协议 (VRRP)” 等协议，共享它们之间分配的信息流。通过使用 “NetScreen 冗余协议 (NSRP)” 创建两个虚拟安全设备 (VSD) 组，每个组都具有自己的虚拟安全接口 (VSI)，即可实现此目的。设备 A 充当 VSD 组 1 的主设备，并充当 VSD 组 2 的备份设备。设备 B 充当 VSD 组 2 的主设备，并充当 VSD 组 1 的备份设备。此配置称为双主动 (请参阅下图)。由于有设备冗余，因此不存在单一故障点。



设备 A 和设备 B 各接收 50% 的网络和 VPN 信息流。设备 A 出现故障时，设备 B 变为 VSD 组 1 的主设备，同时继续作为 VSD 组 2 的主设备，并处理 100% 的信息流。在双主动配置中，故障切换导致的信息流重定向如下图所示。

注意：为简化故障切换概念，仅显示 Trust 和 Untrust 区段。

双主动故障切换



尽管处于双主动配置的两台设备分开的会话总数不能超过单个 NetScreen 设备的容量 (否则，在故障切换时，超额的会话将丢失[2])，但添加第二台设备却使可用的潜在带宽加倍。添加第二台主动设备还可保证两台设备都具有网络连接功能。

2. 在双主动配置中，每台设备都可在短期内容许信息流激增超过单个设备容量的 50% 的情况。但是，在此阶段出现故障切换时，超额的信息流将丢失。

除 NSRP 集群 (主要负责在组成员间传播配置并通告每个成员的当前 VSD 组状态) 外，还可以将设备 A 和设备 B 配置为 RTO 镜像组中的成员，该镜像组负责维持一对设备之间执行对象 (RTO)[3] 的同步性。在主设备让位时，通过维持所有当前会话，备份设备可立即在最短的服务停顿时间内承担主设备职责。

由于 NSRP 通信的机密特性，可以通过加密和认证保障所有 NSRP 信息流的安全。对于加密和认证， NSRP 分别支持 DES 和 MD5 算法。(有关这些算法的详细信息，请参阅第 **5**-7 页上的 “协议”。)

注意：*如果用 HA 电缆直接将一台 NetScreen 设备连接到另一台设备 (即不通过一个交换机转发其它种类的网络信息流)，则不必使用加密和认证。*

如果要用 “简单网络管理协议” (SNMP) 监控 NetScreen 设备，可从 www.juniper.net/support 下载专用的 NSRP MIB。(有关 SNMP 的详细信息，请参阅第 **3**-101 页上的 “SNMP”。)

NSRP 由两个基本元素组成，在以下部分中有相关的详细说明 :

- 第 16 页上的 “NSRP 集群”
- 第 24 页上的 “VSD 组”

有关基本主动 / 被动 NSRP 配置的范例，请参阅第 10 页上的 “范例 : 主动 / 被动配置的 NSRP”。有关双主动 NSRP 配置的范例，请参阅第 50 页上的 “范例 : 双主动配置的 NSRP”。

3. RTO 是设备正常操作时在 NetScreen 设备内存中动态创建的对象。RTO 允许设备了解它周围的网络并实施其策略。RTO 的范例有 TCP/UDP 会话、IPSec 阶段 2 安全联盟 (SA)、 DHCP 分配、 RSA 和 DSS 密钥对、 ARP 表和 DNS 高速缓存。

NSRP 和 NETSCREEN 的操作模式

NetScreen 设备接口可按以下三种模式之一运行，分别是 : NAT 模式、“路由”模式和 “透明”模式。接口处于 NAT 或 “路由”模式时， NetScreen 设备在 OSI 模型中的第 3 层运行。安全区段接口有 IP 地址，并且 NetScreen 设备象第 3 层路由器那样转发信息流。接口处于 “透明”模式时， NetScreen 设备在第 2 层运行。安全区段接口没有 IP 地址，并且 NetScreen 设备象第 2 层交换机那样转发信息流。

当 NetScreen 设备在第 3 层 (NAT 或 “路由”模式) 中运行时，它可以是双主动或主动 / 被动 NSRP 配置。要管理备份设备，必须使用设置每个安全区段接口的管理 IP 地址[4]。

当 NetScreen 设备在第 2 层 (“透明”模式) 运行时，只能为主动 / 被动 NSRP 配置。要管理备份设备，请使用在 VLAN1 接口上设置的管理 IP 地址。

基本主动 / 被动 NSRP 配置

执行最基本的主动 / 被动 NSRP 配置十分简单。可以通过单个 CLI 命令 — **set nsrp cluster id** *number* — 或在 WebUI 中为 NSRP 集群 ID 键入单个编号，将设备放在 NSRP 集群和 VSD 组中。

可以用 CLI 命令 **set nsrp rto sync all**，或在 WebUI 中，选择 Network > NSRP > Synchronization 页中的 **NSRP RTO Synchronization** 选项，然后单击 **Apply**，启用自动 RTO 同步。

接下来，必须选择设备要监控的端口，以便在检测到监控的任何一个端口上失去网络连接时，设备进行故障切换。

注意：*在 NSRP 能够发挥作用前，必须首先按第 46 页上的 “全网状配置的电缆连接”中的说明将两台 NetScreen 设备用电缆连接起来。另外，如果要为管理信息流维持 NSRP 集群中 NetScreen 设备的一个或多个物理接口的网络连通性，在启用 NSRP 前，应首先按第 **3**-41 页上的 “管理 IP”中的说明为这些接口设置管理 IP 地址。*

4. 除 VSD 组 0 以外，不能在 VSI 上为任何 VSD 组设置管理 IP 地址。

缺省设置

NSRP 的基本配置使用以下缺省设置 :

- VSD 组信息
  - VSD group ID: 0
  - Device priority in the VSD group: 100
  - Preempt option: disabled
  - Preempt hold-down time: 0 seconds
  - Initial state hold-down time: 5 seconds
  - Heartbeat interval: 1000 milliseconds
  - Lost heartbeat threshold: 3
- RTO 镜像信息
  - RTO synchronization: disabled
  - Heartbeat interval: 4 seconds
  - Lost heartbeat threshold: 16
- NSRP 链接信息
  - Number of gratuitous ARPs: 4
  - NSRP encryption: disabled
  - NSRP authentication: disabled
  - Interfaces monitored: none
  - Secondary path: none

在 NSRP 集群中设置一个 NetScreen 设备时， NetScreen 设备自动创建 VSD 组 0 并将物理接口转换为 VSD 组 0[5] 的 “虚拟安全接口 (VSI)”。

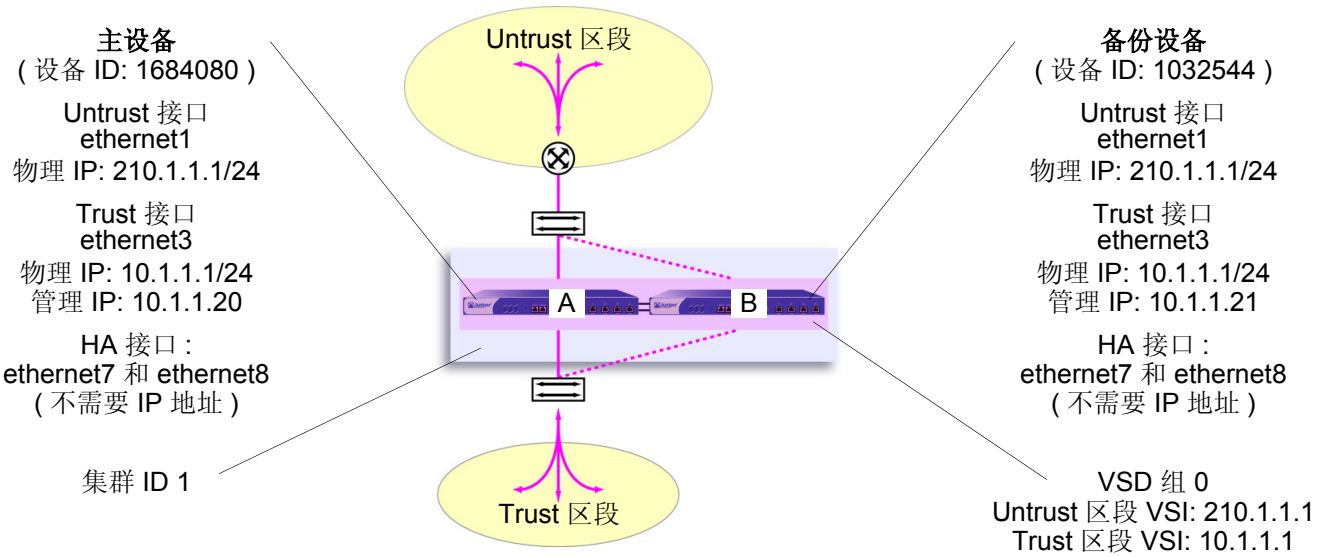
5. 用于指示 VSI 的约定为 **<interface_name>:<VSD_group_ID>**。例如，以下指示的冗余接口 *red1* 为 VSD 组 1 的 VSI: **red1:1**。但是，如果 VSD 组 ID 为 0，则不指定 VSD 组 ID。例如，如果冗余接口 *red2* 为 VSD 组 0 的 VSI，则它仅显示为 **red2**。

范例：主动 / 被动配置的 NSRP

在下例中，用电缆将 NetScreen-A 上的 ethernet7 连接到 NetScreen-B 上的 ethernet7。同样地，用电缆连接 ethernet8 接口。然后将 ethernet7 和 ethernet8 绑定到 HA 区段[6]。为两台设备上的 Trust 区段设置管理 IP 地址 (NetScreen-A 为 10.1.1.20，NetScreen-B 为 10.1.1.21)。然后将每台设备指派给 NSRP 集群 ID 1。设备成为 NSRP 集群的成员时，它们的物理接口的 IP 地址自动变成 VSD 组 ID 0 的 “虚拟安全接口 (VSI)” 的 IP 地址。每个 VSD 成员的缺省优先级为 100，具有更高设备 ID 的设备成为 VSD 组的主设备。

配置设备以监控端口 ethernet1 和 ethernet3，以便在任何一个端口失去网络连接时触发设备故障切换。还要启用 RTO 的自动同步。

> ***注意：****这是一个极为简化的范例，旨在说明 NSRP 配置的基本元素。有关更完整配置的详细信息，请参阅第 50 页上的 “范例：双主动配置的 NSRP”。*



6. 在缺省情况下， ethernet8 被帮定到 HA 区段。仅当已将其绑定到不同区段时，才有必要将其绑定到 HA 区段。

WebUI (NetScreen-A)

1. 接口

Network > Interfaces > Edit (对于 ethernet7): 输入以下内容，然后单击 **OK**:

Zone Name: HA

Network > Interfaces > Edit (对于 ethernet8): 输入以下内容，然后单击 **OK**:

Zone Name: HA

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 210.1.1.1/24

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Manage IP: 10.1.1.20

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

2. NSRP

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 输入以下内容，然后单击 **Apply**:

ethernet1: (选择); Weight: 255[7]

ethernet3: (选择); Weight: 255

Network > NSRP > Synchronization: 选择 **NSRP RTO Synchronization**，然后单击 **Apply**[8]。

Network > NSRP > Cluster: 在 Cluster ID 字段中，键入 **1**，然后单击 **Apply**。

WebUI (NetScreen-B)

3. 接口

Network > Interfaces > Edit (对于 ethernet7): 输入以下内容，然后单击 **OK**:

Zone Name: HA

Network > Interfaces > Edit (对于 ethernet8): 输入以下内容，然后单击 **OK**:

Zone Name: HA

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 210.1.1.1/24

7. NSRP 故障切换临界值的缺省设置为 255。因此，如果权重为 255 时 ethernet1 或 ethernet3 失败，则其故障将触发设备故障切换。
8. 如果没有启用自动 RTO 同步选项，则可以用 CLI 命令 **exec nsrp sync rto all** 手动同步 RTO。

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

Manage IP: 10.1.1.21

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

4. NSRP

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 输入以下内容，然后单击 **Apply**:

ethernet1: (选择); Weight: 255

ethernet3: (选择); Weight: 255

Network > NSRP > Synchronization: 选择 **NSRP RTO Synchronization**，然后单击 **Apply**。

Network > NSRP > Cluster: 在 Cluster ID 字段中，输入 **1**，然后单击 **Apply**。

CLI (NetScreen-A)

1. 接口

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha

set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24

set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.20
set interface ethernet3 nat
```

2. NSRP

```
set nsrp rto-mirror sync[9]
set nsrp monitor interface ethernet1[10]
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

9. 如果没有启用自动 RTO 同步选项，则可以用 CLI 命令 **exec nsrp sync rto all** 手动同步 RTO。

10. 被监控接口的缺省权重为 255，且缺省 NSRP 故障切换临界值为 255。因此，如果权重为 255 时 ethernet1 或 ethernet3 失败，则其故障将触发设备故障切换。在 CLI 中，如果未指定被监控接口的权重，则 NetScreen 设备将使用缺省值 (255)。

CLI (NetScreen-B)

3. 接口

```
set interface ethernet7 zone ha
set interface ethernet8 zone ha

set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24

set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.21
set interface ethernet3 nat
```

4. NSRP

```
set nsrp rto-mirror sync
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
set nsrp cluster id 1
save
```

***注意：**执行此配置后，键入 **get nsrp** 命令，检查设备自动创建的缺省 NSRP 设置 (如第 8 页所述)。*

NSRP 集群

NSRP 集群由一组实施相同的整体安全策略并且共享相同的配置设置的 NetScreen 设备组成。将 NetScreen 设备分配给 NSRP 集群时，对一个集群成员的配置所作的任何更改都将传播给其它成员。同一 NSRP 集群成员以下各项的设置将保持相同：

- 策略和策略对象 (如地址、服务、 VPN、用户和调度)
- 系统参数 (如认证服务器设置、 DNS、 SNMP、系统日志、 URL 阻塞、防火墙检测选项等等)

集群的成员不传播下列配置设置：

不传播的命令	
NSRP	
	• set/unset nsrp cluster id *number* • set/unset nsrp auth password *pswd_str* • set/unset nsrp encrypt password *pswd_str* • set/unset nsrp monitor interface *interface* • set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* } • set/unset nsrp rto-mirror …
Interface	
	• set/unset interface *interface* manage-ip *ip_addr* • set/unset interface *interface* phy … • set/unset interface *interface* bandwidth *number* • set/unset interface redundant *number* phy primary *interface* • 适用于本地接口的所有命令
IP Tracking	
	• 所有 IP 跟踪命令 (set/unset nsrp track-ip …)
Console Settings	
	• 所有控制台命令 (set/unset console …)
Hostname	
	• set/unset hostname *name_str*
SNMP	
	• set/unset snmp name *name_str*

不传播的命令	
Virtual Router	• set/unset vrouter *name_str* router-id *ip_addr*
Clear*	• 所有清除命令 (clear admin, clear dhcp, …)
Debug†	• 所有调试命令 (debug alarm, debug arp, …)

* 在缺省情况下，NSRP 集群成员不传播 **clear** 命令。要将一个 clear 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入命令中。例如， **clear cluster admin …**, **clear cluster dhcp …**

† 在缺省情况下，NSRP 集群成员不传播 **debug** 命令。要将一个 debug 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入 **debug** 命令中。例如， **debug cluster alarm …**, **debug cluster arp …**

在两台 NetScreen 设备能提供冗余网络连接前，必须通过指定介于 1 到 7 之间的集群 ID[11]，将这两台设备分组到同一 NSRP 集群中。当 NetScreen 设备成为集群的成员时，它自动成为 VSD 组 0 的一员，并且所有接口都成为 VSD 组 0 的 VSI。如果要保留某些接口作为本地接口并从选择的接口创建 VSI，则必须执行以下操作：

1. 移除 VSD 组 0。

   所有集群成员上的全部接口都变为本地接口。

2. 创建另一个 VSD 组，如 VSD 组 1。
3. 为该 VSD 组创建 VSI。

有关 VSD 组的详细信息，请参阅第 24 页上的 “VSD 组”。

集群成员也可同步执行对象 (RTO)，它可使新选定的 VSD 组主设备在故障切换后保持网络和 VPN 服务不中断。(有关 RTO 的详细信息，请参阅第 22 页上的 “执行对象”。)

11. 如指定 ID 为 0，则会从集群中移除设备。

集群名称

由于 NSRP 集群成员可以具有不同的主机名称，因此故障切换可破坏 SNMP 通信和数字证书的有效性，因为 SNMP 通信和证书的正常工作依赖于设备的主机名称。

要为所有集群成员定义单一的名称，请键入以下 CLI 命令：

```
set nsrp cluster name name_str
```

为 NetScreen 设备配置 SNMP 主机名 (**set snmp name** *name_str*)，以及在 PKCS10 证书请求文件中定义通用名称时使用集群名称。

所有集群成员使用一个名称，可实现 SNMP 通信和数字证书在设备故障切换后继续使用而不中断。

范例：创建 NSRP 集群

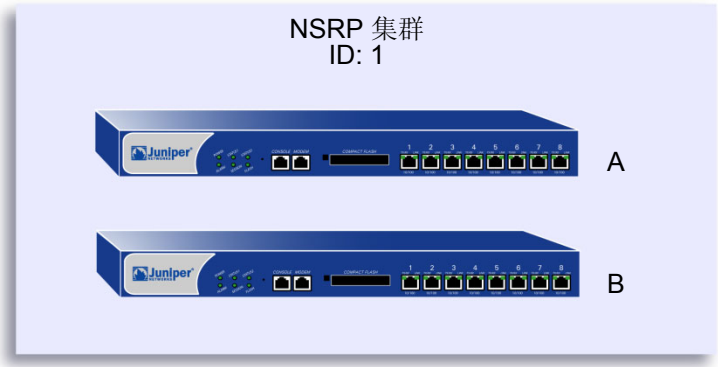
在本例中，将设备 A 和设备 B 分组到 NSRP 集群 ID 1 中，集群名称为“cluster1”。在每台设备上还要指定以下设置：

NSRP 通信安全：指定密码为 725dCaIgDL 和 WiJoaw4177，用于创建认证和加密密钥以保证 NSRP 通信安全。

将两台设备都分组到相同集群中并给定相同的认证和加密密码后，可以在设备 A 或设备 B 上输入下列设置 (在集群中一台设备上输入的大部分设置将传播给另一台设备。对于不传播命令的列表，请参阅第 16 页上的 “不传播的命令”)。

- **接口监控：**选择 ethernet1 (绑定到 Untrust 区段) 和 ethernet2 (绑定到 Trust 区段) 以监控第 2 层网络连接。
- **二级链接：**在 HA1 和 HA2 链接都停止作业时，指定 ethernet2 接口传送 VSD 心跳信号。此功能的目的是，防止在两个 HA 链接都失败时出现多个 VSD 组主设备。
- **无偿 ARP 广播：**将 ARP 广播的数量指定为 5 (缺省值为 4)。出现故障切换后，ARP 广播通知周围网络设备新的主设备的 MAC 地址。

(这些设备上的所有接口都变成 VSD 组 0 的 VSI。在 “VSD 组”部分，为这些设备创建次级 VSD 组。请参阅第 27 页上的 “范例：创建两个 VSD 组”。)



WebUI (NetScreen-A)

1. NSRP 集群和通信安全

   Network > NSRP > Cluster: 输入以下内容[12]，然后单击 **Apply**:

   Cluster ID: 1

   NSRP Authentication Password: (选择) 725dCaIgDL

   NSRP Encryption Password: (选择) WiJoaw4177

WebUI (NetScreen-B)

2. NSRP 集群和通信安全

   Network > NSRP > Cluster: 输入以下内容，然后单击 **Apply**:

   Cluster ID: 1

   Number of Gratuitous ARPs to Resend: 5

   NSRP Authentication Password: (选择) 725dCaIgDL

   NSRP Encryption Password: (选择) WiJoaw4177

3. NSRP 设置

   Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 选择 **ethernet1** 和 **ethernet2**，然后单击 **Apply**。

   Network > NSRP > Link: 从 Secondary Link 下拉列表中选择 **ethernet2**，然后单击 **Apply**。

12. 仅可以通过 CLI 设置集群名称。

CLI (NetScreen-A)

1. NSRP 集群和通信安全

```
set nsrp cluster id 1
set nsrp auth password 725dCaIgDL
set nsrp encrypt password WiJoaw4177
save
```

CLI (NetScreen-B)

2. NSRP 集群和通信安全

```
set nsrp cluster id 1
set nsrp auth password 725dCaIgDL
set nsrp encrypt password WiJoaw4177
save
```

3. NSRP 设置

```
set nsrp cluster name cluster1
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet2
set nsrp secondary-path ethernet2
set nsrp arp 5
save
```

执行对象

执行对象 (RTO) 是正常操作过程中在内存中动态创建的代码对象。RTO 的范例有会话表条目、ARP 高速缓存条目、DHCP 租用和 IPSec 安全联盟 (SA) 等。出现故障切换时，要由新的主设备维持当前的 RTO 以避免服务中断[13]，这一点至关重要。为实现此目的， NSRP 集群的成员对 RTO 进行备份。协同工作时，每个成员从其它成员备份 RTO，以便在双主动 HA 方案中的任一 VSD 组的主设备让位时， RTO 都能继续得到维持。

在当前的 ScreenOS 版本中，不必配置一个或多个 RTO 镜像组来在 NSRP 集群的成员中保持 RTO 同步。将 NetScreen 设备定义为集群的一员并指定 RTO 同步，可自动使本地设备发送和接收 RTO。

在缺省情况下，NSRP 集群成员不会同步 RTO。启用 RTO 同步前，必须首先同步集群成员之间的配置。除非集群中两个成员的配置相同，否则 RTO 同步将失败。(有关同步过程的范例，请参阅第 37 页上的 “范例 : 将设备添加到活动的 NSRP 集群”和第 50 页上的 “范例 : 双主动配置的 NSRP”。)

要启用 RTO 同步，请执行以下操作之一 :

WebUI

Network > NSRP > Synchronization: 选择 **NSRP RTO Synchronization** 复选框，然后单击 **Apply**。

CLI

```
set nsrp rto-mirror sync
save
```

13. 使用策略可指定要备份的会话和不备份的会话。对于不想备份的会话的信息流，应用禁用 HA 会话备份选项的策略。在 WebUI 中，清除 **HA Session Backup** 复选框。在 CLI 中，在 **set policy** 命令中使用 **no-session-backup** 参数。在缺省情况下，会话备份会启用。

RTO 镜像状态

两个 NSRP 集群成员发起它们的 RTO 镜像关系的过程由两种操作状态 — 设置和活动来开发。设备通过这两种状态的过程如下：

1. 将第一台设备添加到组中后，其状态为设置。在设置状态中，设备等待其对等方加入组。作为 RTO 的接收方，它定期传送接收方就绪消息 (receiver-ready)，宣布自身的可用性。作为 RTO 的发送方，它处于等待状态，直到从具有相同集群 ID 的设备获得接收方就绪消息为止。
2. 添加对等方，并且为 HA 用电缆正确连接两台设备后 (请参阅第 46 页上的 “全网状配置的电缆连接”)，会发生以下操作：
   a. 接收方发送一条接收方就绪消息。
   b. 发送方获得接收方就绪消息，并立即发送组活动消息，以便通知其对等方自己现在的状态为活动。
   c. 接收方然后也将自己的状态更改为活动。

除了将 RTO 从发送方传递到接收方外，两个活动镜像都按用户定义的间隔发送 RTO 心跳信号，以传达它们的操作状态。要定义间隔，请使用下列 CLI 命令：**set nsrp rto-mirror hb-interval** *number*。

如果设备没有从它的对等方收到指定数目的连续心跳信号，则它会将其状态从活动更改为设置。要定义引发状态转变所需的失去心跳信号临界值，请使用以下 CLI 命令：**set nsrp rto-mirror hb-threshold** *number*。

注意：**为维护同样的 RTO 心跳信号设置，将传播* ***set nsrp rto-mirror hb-interval *number 和* ***set nsrp rto-mirror hb-threshold*** *number。*

可以在 NSRP 集群中充当发送方的设备上使用以下命令禁用 RTO 会话同步：**set nsrp rto-mirror session off**。在设备上发布此命令只禁用该设备与集群中其它设备的会话同步。

VSD 组

“虚拟安全设备 (VSD)”组是一对物理 NetScreen 设备，它们共同组成一个的 VSD。一个物理设备充当 VSD 组的主设备。 VSD 的 “虚拟安全接口 (VSI)”被绑定到主设备的物理接口上。另一个物理设备充当备份设备[14]。如果主设备出现故障，则 VSD 故障切换到备份设备，并且 VSI 绑定转移到备份设备的物理接口，该备份设备立即晋升为主设备。

通过将两台 NetScreen 设备分组到两个 VSD 组中，每台物理设备在一个组中作为主设备，在另一个组中作为备份设备，两台设备都可作为主设备来积极处理信息流，同时互相备份以应对故障切换。

根据初始 NSRP 配置，优先级编号最接近 0 的 VSD 组成员成为主设备。(缺省值为 100。) 如果两台设备具有相同的优先级值，则具有最小 MAC 地址的设备成为主设备。

抢先选项

通过将要成为主设备的设备设置为抢先模式，可以确定优先级更高的编号 (更接近零) 是否能发起故障切换。如果在该设备上启用抢先选项，则在当前主设备具有优先级更低的编号 (离零更远) 时，该设备将成为 VSD 组的主设备。如果禁用此选项，优先级比备份设备低的主设备可保持其位置 (除非某些其它因素，如内部问题或网络连接故障，导致故障切换)。

使用抑制时间延迟故障切换，可防止在邻接的交换机端口忽隐忽现时快速故障切换造成的混乱，也可确保在新的主设备可用前，周围的网络设备有足够的时间协商新的链接。要启用或禁用抢先选项，请使用以下 CLI 命令 :

```
set/unset nsrp vsd-group id number preempt
```

可以使用以下 CLI 命令将抑制时间 (用于延迟抢先故障切换) 设置为介于 0 到 600 秒之间的任何时间长度 :

```
set nsrp vsd-group id number preempt hold-down number
```

14. 在当前版本中，一个 VSD 组可以有两个成员。在以后的版本中，可以有两个以上的成员。在这种情况下，一台设备充当主设备，另一台设备充当主备份设备，其余的 VSD 组成员充当备份设备。

VSD 组成员状态

VSD 组的成员可以处于以下六种状态之一：

- 主设备 – 处理发送到 VSI 的信息流的 VSD 组成员的状态。
- 主备份设备 – 当前主设备让位后将变成主设备的 VSD 组成员的状态。选择过程使用设备优先级确定要晋升的成员。请注意，在选择新的主设备时， RTO 对等方优先于任何其它 VSD 组成员，即使该成员具有更高优先等级。
- 备份设备 – 监控主备份的状态并在当前备份设备让位时，将一个备份设备选择为主备份设备的 VSD 组成员的状态。
- 初始 – 启动设备或通过 **set nsrp vsd-group id** *id_num* 命令添加设备时， VSD 组成员加入 VSD 时的瞬间状态。

  使用 **set nsrp vsd-group init-hold** *number* 命令，可指定 VSD 组成员在初始状态中停留的时间。缺省 (最小) 设置为 5。要确定初始状态抑制时间，将暂停初始化值乘以 VSD 心跳信号间隔 (暂停初始化 x 心跳信号间隔 = 初始状态抑制时间)。例如，如果暂停初始化值为 5，心跳信号间隔为 1000 毫秒，则初始状态抑制时间为 5000 毫秒，或为 5 秒 (5 x 1000 = 5000)。

  ***注意：** 如果减少 VSD 心跳信号间隔，则应增加暂停初始化值。有关配置心跳信号间隔的信息，请参阅第 26 页上的 “心跳信号消息”。*

- 无资格 – 管理员有意指派一个 VSD 组成员，使其不能参与选择过程的状态。要实现此目的，请使用 **set nsrp vsd-group id** *id_num* **mode ineligible** 命令。
- 不可操作 – 系统检查并确定设备有内部问题 (如没有处理板) 或网络连接问题 (如接口链接失败) 后 VSD 组成员的状态。

  ***注意：** 设备从无资格状态 (使用 **exec nsrp vsd-group id** id_num **mode { backup | init | master | pb }** 命令) 或不可操作状态 (系统或网络问题已修正) 返回时，必须首先通过初始状态。*

通过观察 HA LED 可确定设备状态。各种颜色 (黑色、绿色、黄色、红色) 的含义如下 :

- 黑色 : 设备未对 NSRP 启用。
- 绿色 : 设备对于 NSRP 启用；它是一个或多个 VSD 组中的主设备；并且没有处于不可操作模式。
- 黄色 : 设备对于 NSRP 启用；它不是任何 VSD 组中的主设备；并且没有处于不可操作模式。
- 红色 : 设备对于 NSRP 启用，但是它当前处于不可操作模式。

心跳信号消息

每个 VSD 组成员 (即使它处于初始、无资格或不可操作状态) 都可通过每秒发送心跳信号消息与它的组成员进行通信[15]。这些消息使每个成员知道所有其它成员当前的状态。心跳信号消息包括下列信息 :

- 设备的设备 ID
- VSD 组 ID
- VSD 组成员状态 (主设备、主备份设备或备份设备)
- 设备优先级
- RTO 对等方信息

发送 VSD 心跳信号的间隔可以配置 (200、600、800 或 1000 毫秒；缺省值为 1000 毫秒)。可普遍应用到所有 VSD 组的 CLI 命令为 **set nsrp vsd-group hb-interval** *number*。也可配置失去心跳信号临界值，用于确定认为 VSD 组成员丢失的时间。可普遍应用到所有 VSD 组的 CLI 命令为 **set nsrp vsd hb-threshold** *number*。失去心跳信号临界值的最小值为 3。

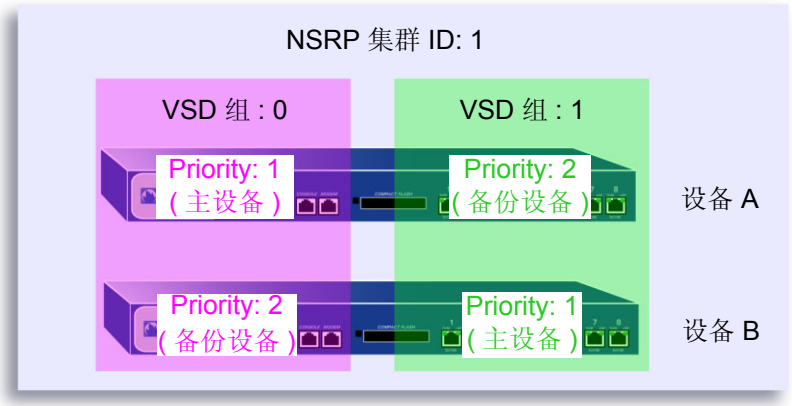
心跳信号消息通过 HA1 链接发送。有关 HA1 和 HA2 接口以及通过每个接口进行通信的消息类型的详细信息，请参阅第 39 页上的 “双 HA 接口”。

15. 如果设备处于不可操作状态，并且所有 HA 链接都中断，则它既不能发送也不能接收 VSD 心跳信号消息，除非为这些消息配置了二级路径。有关配置二级路径的详细信息，请参阅第 19 页上的 “范例 : 创建 NSRP 集群”。

范例 : 创建两个 VSD 组

本例继续进行设备 A 和设备 B 的配置，它们已经是同一 NSRP 集群和 VSD 组 0 的成员 (请参阅第 19 页上的 “范例 : 创建 NSRP 集群”)。

在本例中，创建第二个 VSD 组 — “组 1”。指派设备 A 在 “组 0” 中的优先级为 1，在 “组 1” 中的缺省优先级为 (100)。指派设备 B 在 “组 1” 中的优先级为 1，在 “组 0” 中的缺省优先级为 (100)。在两个 VSD 组中，在主设备上启用抢先选项并将抢先抑制时间设置为 10 秒。如果两台设备都是活动的，则设备 A 始终是 “组 0” 的主设备，设备 B 是 “组 1” 的主设备。



WebUI

1. 设备 A

Network > NSRP > VSD Group > Edit (对于 VSD group 0): 输入以下内容，然后单击 **OK**:

Priority: 1

Enable Preempt: (选择)

Preempt Hold-Down Time (sec): 10

Network > NSRP > VSD Group > New: 在 Group ID 字段中，键入 **1**，然后单击 **OK**。

2. 设备 B

Network > NSRP > VSD Group > Edit (对于 VSD group 1): 输入以下内容，然后单击 **OK**:

Priority: 1

Enable Preempt: (选择)

Preempt Hold-Down Time (sec): 10

CLI

3. 设备 A

```
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 0 preempt hold-down 10
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 1
save
```

4. 设备 B

```
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
save
```

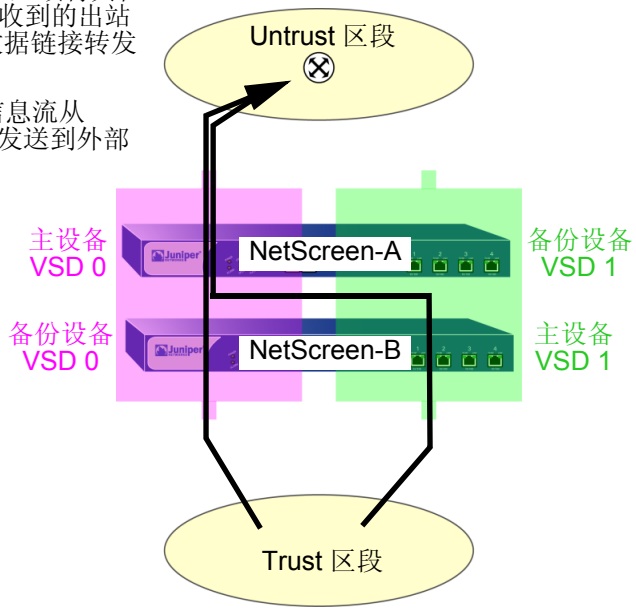
VSI 和静态路由

创建 VSD 组后，必须将 “虚拟安全接口 (VSI)” 绑定到 VSD。将 NetScreen 设备放置在 NSRP 集群中时，所有安全区段接口都变成 VSD 组 0 的 VSI。对于在 NetScreen 设备上配置的每个安全区段，必须手动将 VSI 指派给具有其它 ID 的 VSD。

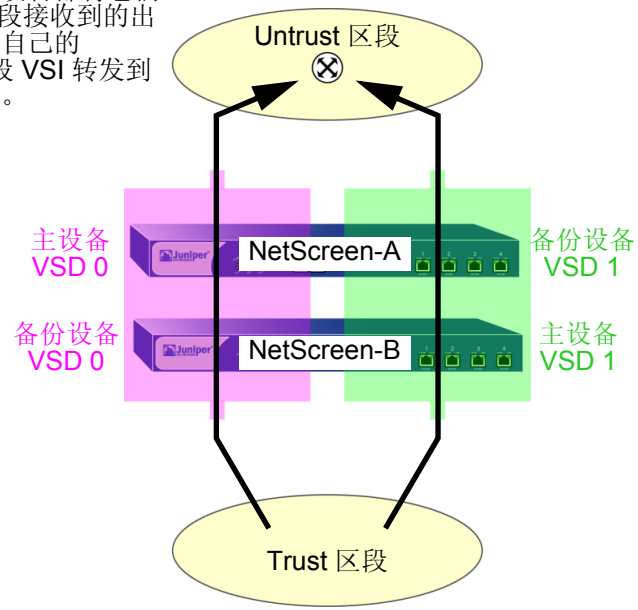
在缺省情况下， NetScreen 设备将一个条目添加到它的路由表中，用于 VSI 的直接子网。对于直接子网以外地址的静态路由，必须为每个 VSI 手动建立路由表条目，通过这些条目， NetScreen 设备将信息流转发到这些地址。例如，如果有两个 VSD 并且要配置到 Untrust 区段中的路由器的缺省路由，则必须为两个 VSD 的 Untrust 区段 VSI 建立路由表条目。如果仅在一个 VSD (如 VSD 0) 上设置缺省路由，则充当另一 VSD (如 VSD 1) 的主设备的 NetScreen 设备必须将所有发送给它的出站信息流通过 HA 数据链接发送到充当 VSD 0 主设备的设备。

如果缺省路由仅设置在 VSD 0 上，则作为 VSD 1 主设备的 NetScreen-B 必须将其在 Trust 区段 VSI 接收到的出站信息流通过 HA 数据链接转发到 NetScreen-A。

NetScreen-A 将信息流从 Untrust 区段 VSI 发送到外部路由器。



如果缺省路由设置在 VSD 0 和 1 上，则两台 NetScreen 设备都将它们在 Trust 区段接收到的出站信息流从自己的 Untrust 区段 VSI 转发到外部路由器。



范例 : Trust 和 Untrust 区段 VSI

本范例建立在以前的范例第 27 页上的 “范例 : 创建两个 VSD 组”基础之上，并假定已经在设备 A 和设备 B 上完成了以下操作 :

- 两台设备都放置在 NSRP 集群 1 中
- 创建了 VSD 组 1 (将设备放置在 NSRP 集群 1 中时， NetScreen 设备自动创建 VSD 组 0)

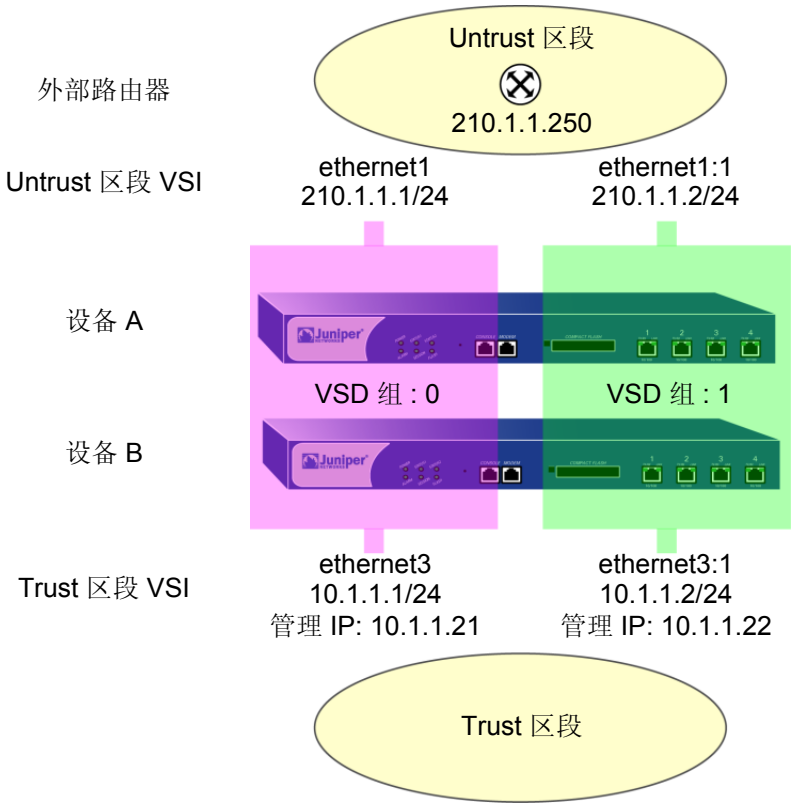
将 ethernet1 绑定到 Untrust 区段并为其指定 IP 地址 210.1.1.1/24。将 ethernet3 绑定到 Trust 区段，将其置于 NAT 模式并为其指定 IP 地址 10.1.1.1/24。将 10.1.1.21 定义为设备 A 的 ethernet3 上的管理 IP，将 10.1.1.22 定义为设备 B 的 ethernet3 上的管理 IP。然后为 VSD 组 1 创建以下 VSI:

- Untrust 区段 VSI ethernet1:1 (210.1.1.2/24)
- Trust 区段 VSI ethernet3:1 (10.1.1.2/24)

NetScreen 设备使用将设备放置在 NSRP 集群中时已经指派给本地接口的 IP 地址，自动为 VSD 组 0 创建 VSI。在本范例中， VSD 组 0 Untrust 区段 VSI 为 ethernet1[16]， IP 地址为 210.1.1.1/24。 VSD 组 0 Trust 区段 VSI 为 ethernet3， IP 地址为 10.1.1.1/24。

最后，设置两个到 Untrust 区段中的、地址为 210.1.1.250 的外部路由器的缺省路由 — 一个用于 VSD 0 上的 Untrust 区段 VSI，另一个用于 VSD 1 上的 Untrust 区段 VSI。所有安全区段都在 trust-vr 路由选择域中。

16. VSD 组 ID “0” 不会出现在 VSD 0 的 VSI 名称中。 VSI 仅由 *ethernet1* 标识，而不是由 *ethernet1:0* 标识。



WebUI (设备 A)

1. 接口 (VSD 组 0 的 VSI)

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

Zone Name: Trust

IP Address/Netmask: 10.1.1.1/24

Manage IP: 10.1.1.21

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 210.1.1.1/24

WebUI (设备 B)

2. 管理 IP 地址

Network > Interfaces > Edit (对于 ethernet3): 在 Manage IP 字段中输入 **10.1.1.22**，然后单击 **Apply**。

3. VSD 组 1 的 VSI

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

Interface Name: VSI Base: ethernet1

VSD Group: 1

IP Address / Netmask: 210.1.1.2/24

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

Interface Name: VSI Base: ethernet3

VSD Group: 1

IP Address / Netmask: 10.1.1.2/24

4. 路由

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

Network Address: 0.0.0.0

Netmask: 0.0.0.0

Gateway: (选择)

Interface: ethernet1:1

Gateway IP Address: 210.1.1.250

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

Network Address: 0.0.0.0

Netmask: 0.0.0.0

Gateway: (选择)

Interface: ethernet1:2

Gateway IP Address: 210.1.1.250

CLI (设备 A)

1. 接口

```
set interface ethernet3 zone trust
set interface ethernet3 ip 10.1.1.1/24
set interface ethernet3 manage-ip 10.1.1.21
set interface ethernet3 nat

set interface ethernet1 zone untrust
set interface ethernet1 ip 210.1.1.1/24
```

CLI (设备 B)

2. 管理 IP 地址

```
set interface ethernet3 manage-ip 10.1.1.22
```

3. 虚拟安全接口

```
set interface ethernet1:1 ip 210.1.1.2/24
set interface ethernet3:1 ip 10.1.1.1.2/24
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet1 gateway 210.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface ethernet1:1 gateway 210.1.1.250
save
```

同步

将新设备添加到活动 NSRP 集群中时，必须使 VSD 组主设备的配置和文件 (如 PKI 公开 / 私有密钥文件) 与新设备同步。同步配置和文件后，必须同步执行对象 (RTO)。集群成员由于任何原因而变为不同步后，也必须同步配置、文件和 RTO。

同步配置

如果在一台设备上进行配置更改时，集群中的另一设备重新启动 (或者所有 HA 链接都出现故障)，配置设置就可能变得不同步。要了解一台设备的配置与另一台设备的配置是否同步，请使用 **exec nsrp sync global-config check-sum** 命令。输出结果说明两台设备的配置是否同步，并提供本地和远程设备的校验和。

如果配置不同步，请使用以下命令将它们同步 : **exec nsrp sync global-config save** (然后重新启动设备) 或 **exec nsrp sync global-config run** (无需重新启动设备)。在同步配置前，如果没有在本地设备上使用 **unset all** 命令，则本地设备将远程设备的配置附加到现有设置上。但是，在同步配置后，每个复制的设置都将生成一条错误消息。要避免在同步配置时生成错误消息，可执行以下操作 :

1. 将本地和远程配置下载到工作站。
2. 使用应用程序 (如 WinDiff) 识别文件间的差异。
3. 在本地设备上手动输入已在远程设备上添加、修改或删除的设置。

注意 : *由于 NetScreen 设备使用 “NetScreen 可靠传输协议 (NSTP)”，它与 TCP 非常类似 (只是更轻量)，因此集群中活动设备上的配置很少变成不同步。*

同步文件

如果需要同步一个特定文件，请在要同步文件的设备上输入以下命令 : **exec nsrp sync file name** *name_str* **from peer**。如果要同步所有文件，请输入 **exec nsrp sync file from peer**。

可使用 RTO 同步或配置同步操作同步 PKI 对象 (如本地和 CA 证书、密钥对和 CRL):

- 如果启用了 RTO 同步，请输入 **exec nsrp sync global-config run** (无需重新启动设备)，然后输入 **exec nsrp sync rto pki from peer**
- 如果禁用了 RTO 同步，请输入 **exec nsrp sync global-config save**，然后重新启动设备。

同步 RTO

如果在集群中的一台设备上启用了 RTO 镜像同步 (请参阅第 22 页上的“执行对象”)，则设备重新启动时，RTO 会自动重新同步。但是，如果禁用 RTO 镜像同步 (可能在设备上执行调试或维护操作)，则再次启用 RTO 同步时，必须手动重新同步所有 RTO。要实现此目的，请使用 **exec nsrp sync rto all** 命令。如果仅重新同步选定的 RTO (如 ARP、 DNS、会话或 VPN)，可以使用以下 CLI 命令 : **exec nsrp sync rto** { **arp** | **auth-table** | **dhcp** | **dns** | **l2tp** | **phase1-sa** | **pki** | **rm** | **session** | **vpn** }。

要使 NSRP 集群中的成员在检测到集群中的其它成员时自动开始 RTO 同步，请使用 **set nsrp rto-mirror sync** 命令。当需要手动同步 RTO 时，使用 **exec nsrp sync rto** { **all** | **arp** | **auth-table** | **dhcp** | **dns** | **l2tp** | **phase1-sa** | **pki** | **rm** | **session** | **vpn** } 命令。

范例：手动重新同步 RTO

在本范例中，设备 A 和设备 B 在 NSRP 集群 1 以及 VSD 组 1 和 2 中。设备 A 是 VSD 组 1 的主设备，是 VSD 组 2 的备份设备。设备 B 是 VSD 组 2 的主设备，是 VSD 组 1 的备份设备。

您要在设备 B 上进行一些故障排除操作，同时又不希望将它从网络断开。可强制设备 B 变成 VSD 组 2 中的备份设备，然后禁用 RTO 同步。设备 A 变成两个 VSD 组的主设备。完成对设备 B 的故障排除后，请再次启用 RTO 镜像同步，然后手动重新同步从设备 A 到设备 B 的 RTO。最后重新将设备 B 指派为 VSD 组 2 的主设备。

WebUI

> ***注意：****RTO 的手动同步只能通过 CLI 进行。*

CLI

设备 B

```
exec nsrp vsd-group id 2 mode backup
unset nsrp rto-mirror sync
```

设备 B 不再处理信息流，也不使 RTO 与设备 A 同步。此时，可以对设备 B 进行故障排除，而不会影响设备 A 的信息流处理性能。

```
set nsrp rto-mirror sync
exec nsrp sync rto all from peer
exec nsrp vsd-group id 2 mode master
```

范例 : 将设备添加到活动的 NSRP 集群

在本范例中，将以前作为单个安全设备的设备 A，添加到 NSRP 集群中的 VSD 组 0 和 1 中，该集群的 ID 为 1，名称为 “cluster1”。必须撤消设备 A 上以前的配置，重新启动它，然后同步两个 VSD 组的主设备的配置、文件和 RTO。然后将设备 A 指派为 VSD 组 0 的主设备。

WebUI

> ***注意 :*** *冷启动同步功能只能通过 CLI 实现。*

CLI

设备 A

```
unset all[17]
```

出现以下提示 : “Erase all system config, are you sure y / [n]?”

按 **Y** 键。

系统配置返回到出厂缺省设置。

```
reset
```

出现以下提示 : “Configuration modified, save? [y] / n”

按 **N** 键。

出现以下提示 : “System reset, are you sure? y / [n]”

按 **Y** 键。

系统重新启动。

```
set nsrp cluster id 1
set nsrp cluster name cluster1
```

17. 如果不首先使用 **unset all** 命令，则 **exec nsrp sync global-config** 命令将新的配置设置附加到现有的设置上。(注意 : NetScreen 设备会为每个实现同步的复制设置生成一条错误消息。)

```
exec nsrp sync file
exec nsrp sync global-config
set nsrp rto-mirror sync
exec nsrp vsd-group id 0 mode master
save all[18]
```

同步系统时钟

NSRP 中包含一种机制，用于同步 NSRP 集群成员的系统时钟。当手动设置系统时钟时， NSRP 时间同步机制使各成员的时钟正确地保持同步。但是，如果使用 “网络时间协议” (NTP) 设置所有集群成员上的系统时钟，然后使用 NSRP 使时钟的时间同步，则时间可能变成不同步。尽管 NSRP 同步操作以秒为单位，但 NTP 服务器却采用次秒级的定时机制。由于处理延迟，可能导致每个集群成员的时间相差几秒，所以 Juniper Networks 建议您当所有集群成员均启用 NTP 时禁用 NSRP 时间同步，而且每个成员可通过 NTP 服务器更新各自的系统时钟。要禁用 NSRP 时间同步功能，请输入以下命令：

```
set ntp no-ha-sync
```

18. 使用 **save all** 命令保存所有虚拟系统和根级中的配置。而使用 **save** 命令仅保存根级中的配置。

双 HA 接口

NSRP 的基本原则是没有单一故障点。除冗余设备外， NetScreen 设备还具有专用的物理冗余 HA 接口 (HA1 和 HA2)，还可以将两个通用接口绑定到 HA 区段，以提供 HA 接口冗余。

另外，您可以创建冗余安全区段接口。

所有在集群成员之间传递的 NSRP 信息都通过两个 HA 接口传递。为更好地分配带外带宽， HA1 处理 NSRP 控制消息，而 HA2 处理网络数据消息。但是，如果任一个端口在有千兆位 HA1 和 HA2 接口的 NetScreen 设备上发生故障，则另一个活动端口会承担这两种信息流。对于必须将百兆位接口用于数据链接的 NetScreen 设备，数据链接的故障会导致仅有一个活动 HA 链接来控制消息。如果控制链接在此类设备上发生故障，则数据链接就变成为控制链接，仅能发送和接收控制消息。

如果 HA1 或 HA2 之一出现故障，则会通过另一个 HA 链接来发送控制和数据消息。

如果 ethernet7 或 ethernet8 之一发生故障，则通过另一个 HA 链接仅能发送控制消息。

***注意：**如果在 HA 端口之间使用交换机，则应使用基于端口的 VLAN，它不会与转发的数据包上的 VLAN 标记发生冲突。*

在没有专用 HA 接口的 NetScreen 设备上，必须将一个或两个物理以太网接口绑定到 HA 区段上。如果将一个千兆位接口绑定到 HA 区段上，则该 HA 链接同时支持控制和数据消息。如果将一个百兆位接口绑定到 HA 区段上，则该 HA 链接将仅支持控制消息。

如果将两个接口 (千兆位或百兆位) 绑定到 HA 区段上，则编号较小的接口变为控制链接，而编号较大的接口变为数据链接。例如，如果仅将 ethernet8 绑定到 HA 区段上，则 ethernet8 变为控制链接。如果再将 ethernet7 绑定到 HA 区段上，则 ethernet7 变为控制链接 (因为 ethernet7 的编号比 ethernet8 小)，ethernet8 变为数据链接。(有关将接口绑定到区段的信息，请参阅第 **2**-63 页上的 “将接口绑定到安全区段”。)

用电缆连接 HA 接口的顺序也会影响哪个接口变为控制链接、哪个接口变为数据链接。如果 ethernet7 和 ethernet8 都绑定到 HA 区段，但仅用电缆连接 ethernet8 接口，则 ethernet8 变为控制链接。如果再用电缆连接 ethernet7 接口，则 ethernet7 变为控制链接 (因为 ethernet7 处于活动状态，其编号比 ethernet8 小)，ethernet8 变为数据链接。这一原则也适用于 HA1 和 HA2 接口。

在没有专用 HA 接口的 NetScreen 设备上，也可以指定一个接口来绑定到安全区段以处理 HA 控制消息。使用 CLI 命令 **set nsrp interface** *interface*。

控制消息

有两种控制消息 : 心跳信号和 HA 消息。

心跳信号 : 定时发送心跳信号可在 NSRP 集群成员、 VSD 组成员和 RTO 镜像之间建立和维持通信。心跳信号不断通告发送方成员的状态、其系统的使用状况以及网络的连通性。三种心跳信号消息如下 :

- HA 物理链接心跳信号
- VSD 心跳信号
- RTO 心跳信号

HA 物理链接心跳信号是从 NSRP 每个成员的 HA1 和 HA2 接口向其它成员广播的消息。这些消息的目的是监视 HA 接口的使用状况。例如，如果一个成员没有从 HA1 收到三个连续的心跳信号，则这些设备会将控制消息的传输转移给 HA2。

VSD 心跳信号从 VSD 组中每个成员的 HA1 接口进行广播。 VSD 组使用这些消息来监视其所有成员的从属状态。例如，如果主设备通告它变为不可操作，则主要备份设备立刻变为 VSD 组的主设备。

镜像组的每个成员从 HA1 接口广播 RTO 心跳信号。这些消息的目的是找到一个活动的对等方，然后发送组活动消息来维持镜像关系。例如，如果一个设备没有从它的对等方收到 16 个连续的 RTO 心跳信号，则它会将其状态从活动转变为设置。

***注意：**如果从镜像组中删除了一个设备，它将进入未定义状态，并且会将一条 “组拆分” 消息传送到其对等方。该对等方立即从活动状态改变为设置状态，而不会等待丢失的心跳信号超越临界值。*

HA 消息：两种 HA 消息如下：

- 配置消息 – 主设备向其它 VSD 组成员发送的网络和配置设置
- RTO 消息 – 主设备向其它 RTO 镜像发送的 RTO

HA 消息中包括在不引起服务中断的情况下而使备份设备变为主设备的信息。

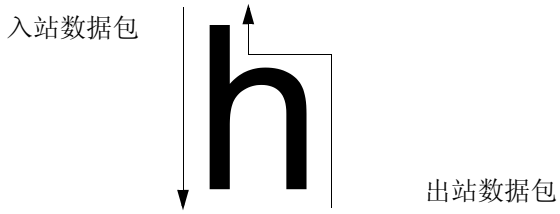
数据消息 (数据包转发)

数据消息为穿越防火墙的 IP 数据包， VSD 组中的备份必须将它们转发给作为主设备的设备。当数据包到达双主动配置中 NetScreen 设备的接口时，该设备首先识别哪个 VSD 组必须处理数据包。如果收到数据包的设备是识别 VSD 组的主设备，它自己将处理该数据包。如果该设备不是主设备，它会通过 HA 数据链接将数据包转发给主设备。

例如，一个负载均衡路由器可能会在会话中向设备 A (VSD 组 1 的主设备) 发送第一个数据包，该设备会在其会话表中创建一个条目。如果路由器通过轮询方式 (即，路由器依次向每个 NetScreen 设备发送数据包) 发送数据包来执行负载均衡，则该路由器可能将下一数据包发送到设备 B (VSD 组 1 的备份设备)。因为在设备 A 中存在一个会话条目，所以设备 B 通过数据链接[19] 将数据包转发给设备 A，由它来进行处理。

19. 如果没有数据链接，则收到数据包的 NetScreen 设备立即将它丢弃。

仅在 NetScreen 设备处于 “路由”模式中的双主动配置时，入站数据包才会通过数据链接转发。当处于 NAT 模式时，虽然接收返回出站数据包的 NetScreen 设备可能会通过数据链接将其转发给具有该数据包所属会话条目的设备，但是路由器总是将进入数据包发送到 MIP、VIP 或 VPN 通道网关。此种数据包转发方式产生了一个 “h”形的路径。像字母 *h* 的笔划一样，入站数据包通过一个设备直接发送，但是出站数据包通过其它设备发送到中途，然后通过数据链接转发给第一个设备。



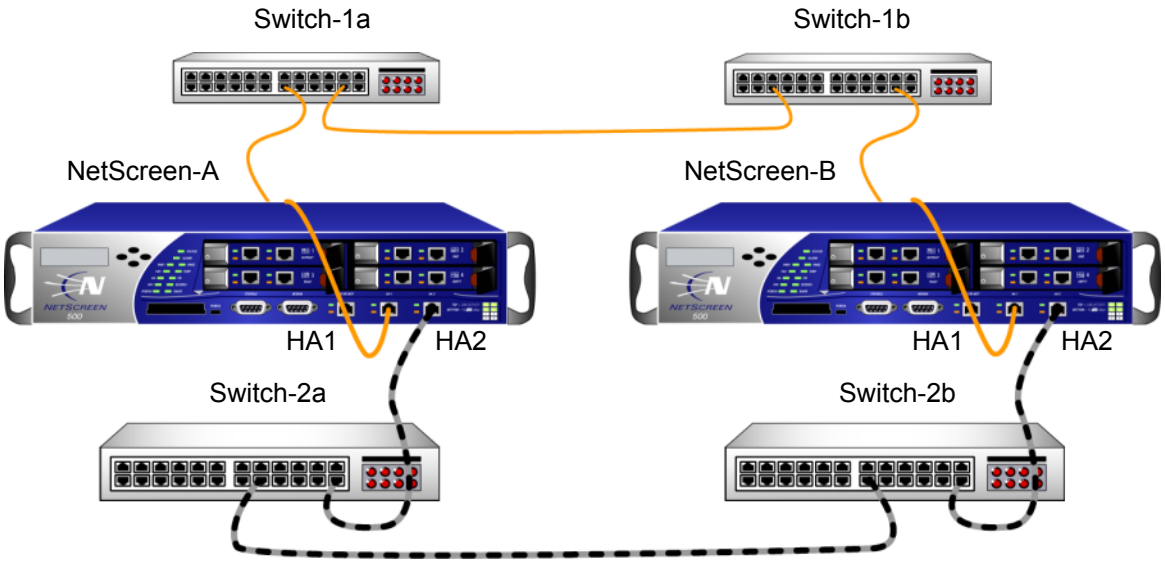
动态路由选择警告信息

如果 NSRP 集群处于动态路由选择环境中，并且您禁用数据包转发 (**unset nsrp data-forwarding**)，则可能会丢失到达非活动接口的信息流[20]。由于 NetScreen 设备无法通过数据链接将信息流转发给接口处于活动状态的 NetScreen 设备，因此它会丢弃信息流。当禁用数据包转发时，为了避免上述问题， NetScreen 设备指示属于设备次要 VSD 的接口的状态是 “断开”，而不只是 “非活动”。此状态会通知路由器不将信息流发送给这些接口。

20. 非活动接口是属于设备上次要 VSD 的接口。

双 HA 链接探查

可以连接冗余 HA 接口，方法是直接用电缆将一台设备上的 HA 端口连接到另一台设备上的 HA 端口。或者，可以通过一个或多个交换网络连接两个设备上的 HA 端口。在以下配置中，通过两台交换机 (Switch-1a 和 Switch-1b)，将设备 NetScreen-A 上的 HA1 端口连接到 NetScreen-B 上的 HA1 端口。为了提供冗余 HA 接口，通过 Switch-2a 和 Switch-2b 将设备 NetScreen-A 上的 HA2 端口连接到 NetScreen-B 上的 HA2 端口。在以下配置中，当 HA2 链接处理网络数据消息时，NetScreen-A 和 NetScreen-B 上的 HA1 端口间的链接处理 NSRP 控制消息。如果 NetScreen-A 上的 HA1 端口与 Switch-1a 之间的链接断开，则 NetScreen-A 将控制消息传输给 HA2 端口。但是，NetScreen-B 会因为 HA1 端口仍处于活动状态而不识别 HA1 链接的故障，并且拒绝由 HA2 链接上 NetScreen-A 发出的 NSRP 控制消息。



控制链接 = 实线形式橙色电缆

数据链接 = 虚线形式黑色 / 灰色电缆

为了防止出现这种情形，可以对 NetScreen 设备进行配置来监控 HA 链接的状态，方法是在 HA 链接上向对等方发送 NSRP 探查请求。如果收到 HA 链接上对等方的回复，则认为请求成功并且 HA 链接处于连接状态。如果在指定的限制时间内未收到对等方的回复，则认为 HA 链接处于断开状态。这使 NetScreen 设备在必要时能将控制消息传送给切换给可用 HA 链接，即使在任一台设备的 HA 端口上都没有物理故障。

在 HA 链接上发送探查请求的方法有两种：

- **管理员手动发送**：在特定 HA 链接上发送探查，每秒一次，发送次数可指定。如果在发送指定次数的探查后未收到对等方的回复，则认为 HA 链接处于断开状态。执行该命令后会立即发送探查。
- **ScreenOS 自动发送**：在所有 HA 链接上发送探查，每秒一次 (也可以指定发送探查的 HA 区段接口和时间间隔)。在缺省情况下，如果连续发送五个探查而没有收到对等方的回复，则认为链接处于断开状态；可以指定不同的临界值以便确定链接处于断开状态的时间。请注意即使主 HA 链接处于断开状态， NetScreen 设备也会继续在该链接上发送探查。如果主 HA 链接连接恢复且在链接上再次收到对等方的响应，则 NetScreen 设备会将控制消息的传输切换回主 HA 链接。

范例：手动发送链接探查

在本例中， NetScreen 设备上的 ethernet7 和 ethernet8 接口被绑定到 HA 区段。配置 5 个链接探查，将它们从 ethernet8 接口发送到对等方 MAC 地址 00e02000080。(请注意如果未指定 MAC 地址，则使用缺省 NSRP MAC 地址。)

WebUI

> ***注意：****必须使用 CLI 在 HA 链接上手动发送探查。*

CLI

```
exec nsrp probe ethernet8 00e02000080 count 5
```

范例：自动发送链接探查

在本例中， NetScreen 设备上的 ethernet7 和 ethernet8 接口被绑定到 HA 区段。配置链接探查，以三秒钟间隔自动将其发送给两个接口。还要设置临界值，以便当连续发送四个请求后仍未收到对等方回复时，认定 HA 链接处于断开状态。

WebUI

Network > NSRP > Link: 输入以下内容，然后单击 **Apply**:

Enable HA Link Probe: (选择)

Interval: 3

Threshold: 5

CLI

```
set nsrp ha-link probe interval 3 threshold 4
```

设置过程

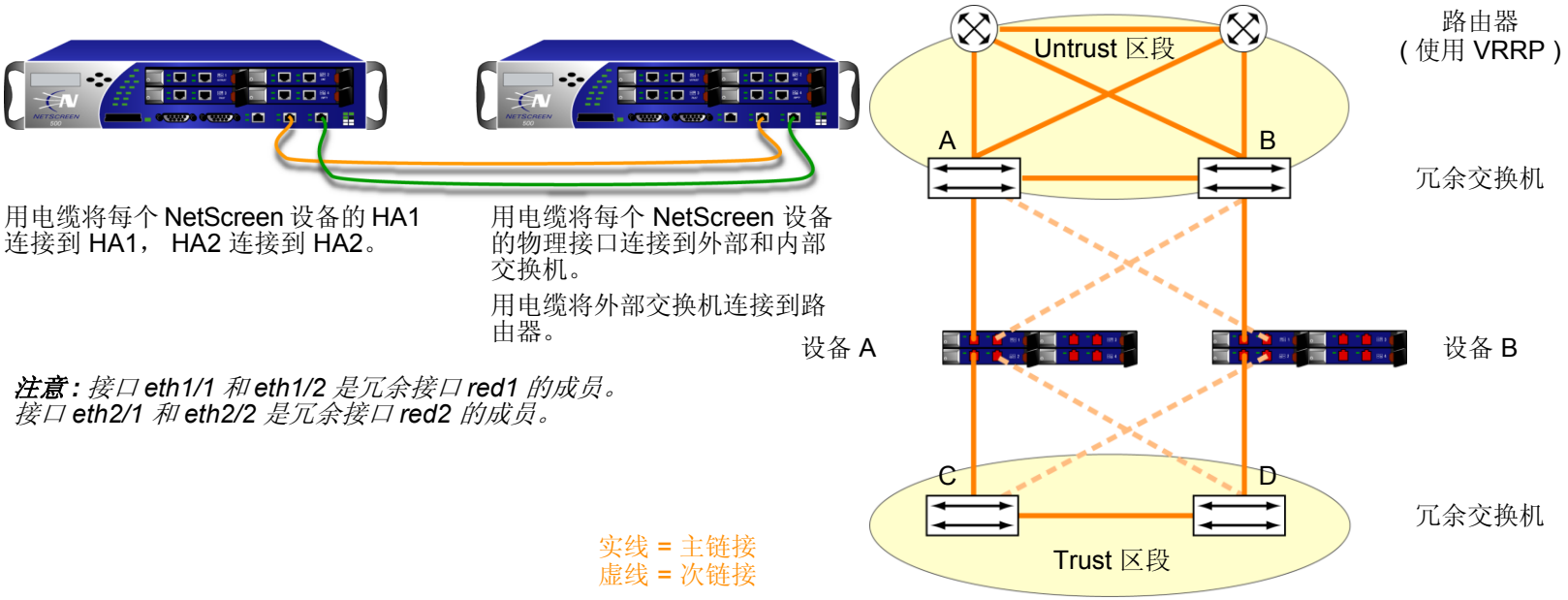
要配置两个 NetScreen 设备使其具有高可用性，必须用电缆将它们连接到网络并将它们互相连接，然后用 NSRP 对其进行 HA 配置。

全网状配置的电缆连接

下面的图表说明了两个设备 NetScreen 之间的电缆连接，以及它们同内部交换机冗余对和外部交换机冗余对之间的电缆连接。外部交换机然后将与一对运行 VRRP 的冗余路由器连接，完成全网状配置。第一个图表显示两台带有专用 HA 接口的 NetScreen 设备。第二个图表显示两个用网络接口来处理 HA 信息流的 NetScreen 设备。

***注意：**根据配置 NetScreen 设备的拓扑结构以及您使用的交换机和路由器种类的不同，在下图中提供的电缆连接可能会与您网络的要求有所不同。*

带有专用 HA 接口的 NetScreen 设备



***注意：**接口 eth1/1 和 eth1/2 是冗余接口 red1 的成员。*
接口 eth2/1 和 eth2/2 是冗余接口 red2 的成员。

如下所示，为 NSRP 用电缆连接全网状配置中的两个 NetScreen 设备 (设备 A 和设备 B):

NetScreen A 和 NetScreen B: HA 链接

1. 用电缆将每个 NetScreen 设备的 HA1 接口连接在一起。
2. 用电缆将每个 NetScreen 设备的 HA2 接口连接在一起。

NetScreen A: Redundant1 (eth1/1 和 eth1/2)， Untrust 区段

3. 用电缆将 ethernet1/1 和外部交换机 A 连接。 (ethernet1/1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。)
4. 用电缆将 ethernet1/2 和外部交换机 B 连接。 (ethernet1/2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。)

NetScreen A: Redundant2 (eth2/1 和 eth2/2)， Trust 区段

5. 用电缆将 ethernet2/1 和内部交换机 C 连接。 (ethernet2/1 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。)
6. 用电缆将 ethernet2/2 和内部交换机 D 连接。 (ethernet2/2 是绑定到 Trust 区段中 red2 上的另一个物理接口。)

NetScreen B: Redundant1 (eth1/1 和 eth1/2)， Untrust 区段

7. 用电缆将 ethernet1/1 和外部交换机 B 连接。 (ethernet1/1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。)
8. 用电缆将 ethernet1/2 和外部交换机 A 连接。 (ethernet1/2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。)

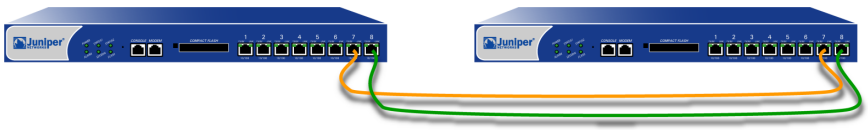
NetScreen B: Redundant2 (eth2/1 和 eth2/2)， Trust 区段

9. 用电缆将 ethernet2/1 和内部交换机 D 连接。 (ethernet2/1 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。)
10. 用电缆将 ethernet2/2 和内部交换机 C 连接。 (ethernet2/2 是绑定到 Trust 区段中 red2 上的另一个物理接口。)

交换机和路由器

11. 用电缆将冗余外部交换机连接在一起。
12. 用电缆将外部交换机与冗余路由器连接，其配置与 NetScreen 设备连接到交换机所使用的配置相同。
13. 用电缆将内部冗余交换机连接在一起。

将网络接口用于 HA 链接的 NetScreen 设备



将 ethernet7 和 ethernet8 绑定到每个 NetScreen 设备的 HA 区段。

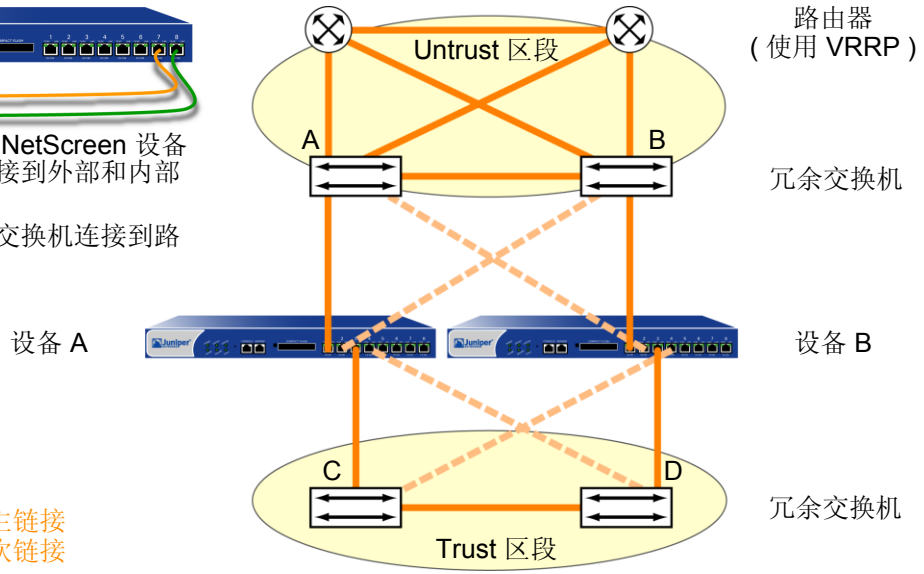
然后将绑定到 HA 区段的接口用电缆连接在一起：

- 设备 A 上的 eth7 连接到 设备 B 上的 eth7
- 设备 A 上的 eth8 连接到 设备 B 上的 eth8

用电缆将每个 NetScreen 设备的物理接口连接到外部和内部交换机。

用电缆将外部交换机连接到路由器。

***注意：** 接口 eth1 和 eth2 是冗余接口 red1 的成员。*
接口 eth3 和 eth4 是冗余接口 red2 的成员。



将 ethernet7 和 ethernet8 绑定到两个 NetScreen 设备 (设备 A 和设备 B) 上的 HA 区段后，如下所示，为 NSRP 用电缆按全网状配置连接 NetScreen 设备：

NetScreen A 和 NetScreen B: HA 链接

1. 用电缆将每个 NetScreen 设备的 ethernet7 接口连接在一起。
2. 用电缆将每个 NetScreen 设备的 ethernet8 接口连接在一起。

NetScreen A: Redundant1 (ethernet1 和 ethernet2)， Untrust 区段

3. 用电缆将 ethernet1 和外部交换机 A 连接。(ethernet1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。)
4. 用电缆将 ethernet2 和外部交换机 B 连接。(ethernet2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。)

NetScreen A: Redundant2 (ethernet3 和 ethernet4)， Trust 区段

5. 用电缆将 ethernet3 和内部交换机 C 连接。(ethernet3 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。)
6. 用电缆将 ethernet4 和内部交换机 D 连接。 (ethernet4 是绑定到 Trust 区段中 red2 上的另一个物理接口。)

NetScreen B: Redundant1 (ethernet1 和 ethernet2)， Untrust 区段

7. 用电缆将 ethernet1 和外部交换机 B 连接。(ethernet1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。)
8. 用电缆将 ethernet2 和外部交换机 A 连接。(ethernet2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。)

NetScreen B: Redundant2 (ethernet3 和 ethernet4)， Trust 区段

9. 用电缆将 ethernet3 和内部交换机 D 连接。(ethernet3 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。)
10. 用电缆将 ethernet4 和内部交换机 C 连接。 (ethernet4 是绑定到 Trust 区段中 red2 上的另一个物理接口。)

交换机和路由器

11. 用电缆将冗余外部交换机连接在一起。
12. 用电缆将外部交换机与冗余路由器连接，其配置与 NetScreen 设备连接到交换机所使用的配置相同。
13. 用电缆将内部冗余交换机连接在一起。

双主动 NSRP 配置

用电缆将 NetScreen 设备连接在一起并连接到周围的网络设备后，即可进行 HA 配置。完整的双主动配置包括以下步骤：

1. 创建 NSRP 集群，这将自动创建 VSD 组 0
2. 在集群中创建第二个 VSD 组
3. 启用设备故障跟踪方法，如接口监控和路径监控

范例：双主动配置的 NSRP

本例以第 62 页上的 “范例：为 VSI 创建冗余接口”中配置的接口为基础。在本例中，用 ID 1 创建 NSRP 集群并将两个 NetScreen 设备 (设备 A 和设备 B) 命名为 “cluster1”，它们没有配置任何用户定义的其它设置。

***注意：**为启用命令传播，必须先定义每个设备上的集群 ID 号。下列设置不能传播，并且必须在集群中的每个设备上进行配置：VSD 组、VSD 优先级、认证和加密密码、管理 IP 地址以及 IP 跟踪设置。所有其它命令都在集群的设备间传播。*

当创建了 NSRP 集群后， NetScreen 设备自动创建 VSD 组 0[21]。您可以定义 VSD 组 1。指定设备 A 在 VSD 组 0 中的优先级为 1，在 VSD 组 1 中的优先级为 100 (缺省值)。指定设备 B 在 VSD 组 1 中的优先级为 1，在 VSD 组 0 中保留其优先级为缺省值 (100)。

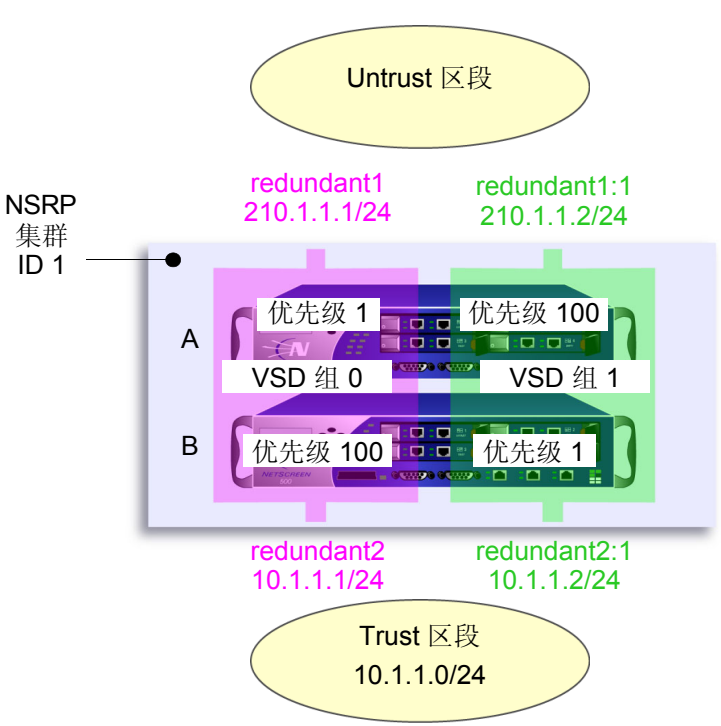
设置接口监控选项来监控两个冗余接口 (redundant1 和 redundant2)，以保证第 2 层网络的连通性。如果任何受监控接口的主接口出现故障，设备会立即故障切换到次接口。如果属于受监控冗余接口的两个物理接口都出现故障，则设备会故障切换到其它设备。

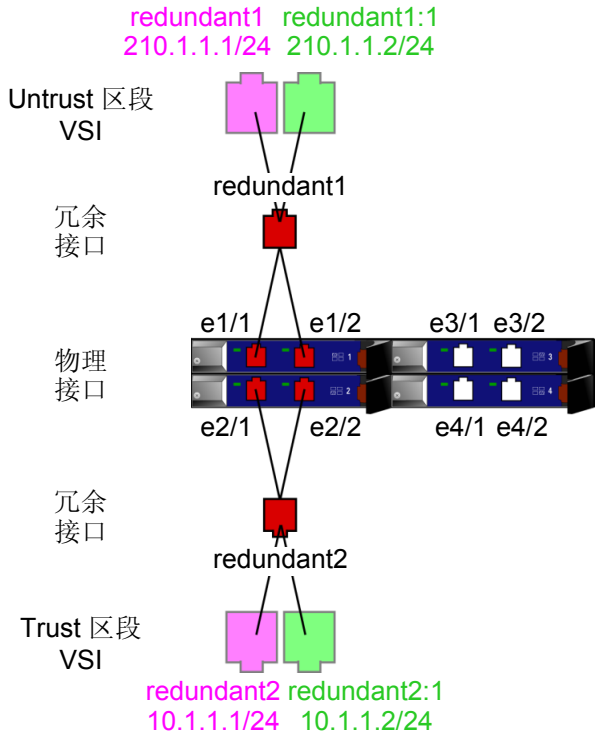
可以将 ethernet2/1 接口定义为 VSD 心跳信号消息的次链接，以及定义某设备发生 5 次故障切换后无偿的 ARP 数。因为 HA 电缆直接连接两个 NetScreen 设备，所以 NSRP 集群成员之间的通信不需要认证和加密。

还要为每个 Untrust 区段 VSI 设置一个到缺省网关 (210.1.1.250) 的路由，以及为每个 Trust 区段 VSI 设置一个到内部网络的路由。所有安全区段都在 trust-vr 路由选择域中。

21. VSD 组 ID “0”不会出现在 VSD 0 中的 VSI 名称中。 VSI 仅标识为 *redundant1*，而不是 *redundant1:0*。

最后，在使两台设备的配置同步之后，启用 RTO 同步。





Untrust 区段中缺省网关的 IP 地址为 210.1.1.250。

在此显示的地址和配置在两个 NetScreen 设备上都一样。

唯一不同的就是管理 IP 地址。

在设备 A 上，管理 IP 为 10.1.1.21 而且是在 redundant2 接口上。

在设备 B 上，管理 IP 为 10.1.1.22 而且是在 redundant2 接口上。

WebUI (设备 A)

1. 集群和 VSD 组

Network > NSRP > Cluster: 在 Cluster ID 字段键入 **1**，然后单击 **Apply**。

Network > NSRP > VSD Group > Edit (对于 Group ID 0): 输入以下内容，然后单击 **OK**:

Priority: 1

Enable Preempt: (选择)

Preempt Hold-Down Time (sec): 10[22]

Network > NSRP > VSD Group > New: 输入以下内容，然后单击 **OK**:

Group ID: 1

Priority: 100

Enable Preempt: (清除)

Preempt Hold-Down Time (s): 0

22. 抑制时间可以为 0 到 255 秒中的任何长度，可有效地延迟故障切换以防止快速故障切换带来的混乱。

WebUI (设备 B)

2. 集群和 VSD 组

Network > NSRP > Cluster: 输入以下内容，然后单击 **Apply**[23] :

Cluster ID: 1

Number of Gratuitous ARPs to Resend: 5[24]

Network > NSRP > Link: 从 Secondary Link 下拉列表中选择 **ethernet2/1**，然后单击 **Apply**[25]。

Network > NSRP > Synchronization: 选择 **NSRP RTO Synchronization**，然后单击 **Apply**。

Network > NSRP > VSD Group > New: 输入以下内容，然后单击 **OK**:

Group ID: 1

Priority: 1

Enable Preempt: (选择)

Preempt Hold-Down Time (sec): 10

3. 冗余接口和管理 IP

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

Interface Name: redundant1

Zone Name: Untrust

IP Address / Netmask: 210.1.1.1/24

Network > Interfaces > Edit (对于 ethernet1/1): 在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。

23. 只能通过 CLI 设置集群名称。

24. 此设置将指定当一个设备故障切换后，新 VSD 组的主设备会发送 5 个无偿的 ARP 数据包来宣布 VSI 和虚拟 MAC 地址关联到新主设备。

25. 如果 HA1 和 HA2 链接都出错，则 VSD 心跳信号消息通过 Trust 区段中的 ethernet2/1 传递。

Network > Interfaces > Edit (对于 ethernet1/2): 在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。

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

Interface Name: redundant2

Zone Name: Trust

IP Address / Netmask: 10.1.1.1/24

> 在 Manage IP 字段中输入 **10.1.1.22**，然后单击 **OK**。

Network > Interfaces > Edit (对于 ethernet2/1): 在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

Network > Interfaces > Edit (对于 ethernet2/2): 在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 选择 **redundant1** 和 **redundant2**，然后单击 **Apply**。

4. 虚拟安全接口

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

Interface Name: VSI Base: redundant1

VSD Group: 1

IP Address / Netmask: 210.1.1.2/24

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

Interface Name: VSI Base: redundant2

VSD Group: 1

IP Address / Netmask: 10.1.1.2/24

5. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: redundant1

Gateway IP Address: 210.1.1.250

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

Network Address: 0.0.0.0/0

Gateway: (选择)

Interface: redundant1:1

Gateway IP Address: 210.1.1.250

WebUI (设备 A)

6. 管理 IP 地址

Network > Interfaces > Edit (对于 redundant2): 在 Manage IP 字段中输入 **10.1.1.21**，然后单击 **OK**。

7. RTO 同步

Network > NSRP > Synchronization: 选择 **NSRP RTO Mirror Synchronization**，然后单击 **Apply**。

CLI (设备 A)

1. 集群和 VSD 组

```
set nsrp cluster id 1
set nsrp vsd-group id 0 preempt hold-down 10[26]
set nsrp vsd-group id 0 preempt
set nsrp vsd-group id 0 priority 1
set nsrp vsd-group id 1
set nsrp rto-mirror sync
save
```

26. 抑制时间可以为 0 到 255 秒中的任何长度，可有效地延迟故障切换以防止快速故障切换带来的混乱。

CLI (设备 B)

2. 集群和 VSD 组

```
set nsrp cluster id 1[27]
set nsrp cluster name cluster1
set nsrp rto-mirror sync
set nsrp vsd-group id 1 priority 1[28]
set nsrp vsd-group id 1 preempt hold-down 10[29]
set nsrp vsd-group id 1 preempt
set nsrp secondary-path ethernet2/1[30]
set nsrp arp 5[31]
set arp always-on-dest[32]
```

3. 冗余接口和管理 IP

```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24
set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1
set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.22
set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2
set nsrp monitor interface redundant1
set nsrp monitor interface redundant2
```

27. 因为设备 A 和 B 都是同一 NSRP 集群的成员，所以在设备 B 上后续输入的所有命令 (另外注明的除外) 都将传播给设备 A。
28. 此命令不传播。
29. 此命令不传播。
30. 如果 HA1 和 HA2 链接都出错，则 VSD 心跳信号消息通过 Trust 区段中的 ethernet2/1 传递。
31. 此设置将指定当一个设备故障切换后，新 VSD 组的主设备会发送 5 个无偿的 ARP 数据包来宣布 VSI 和虚拟 MAC 地址关联到新主设备。
32. 输入此命令后，NetScreen 设备总是执行 ARP 查找来获得目标 MAC 地址，而不是从原始以太网帧的源 MAC 中获得。本例中的外部路由器组成了一个运行 VRRP 的虚拟路由器。从此路由器发送来的帧使用虚拟 IP 地址作为源 IP，而不是用物理 MAC 地址作为源 MAC。如果该路由器故障切换且 NetScreen 设备从进入帧的源 MAC 中获得 MAC，则它将会把返回信息流引导到错误位置。通过执行 ARP 查找获得目标 MAC，NetScreen 设备可以将信息流正确发送到新的物理 MAC 地址所在的位置。

4. 虚拟安全接口

```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 210.1.1.250
set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 210.1.1.250
save
```

CLI (设备 A)

6. 管理 IP 地址

```
set interface redundant2 manage-ip 10.1.1.21
```

7. RTO 同步

```
set nsrp rto-mirror sync
save
```

2

接口冗余

本章介绍 NetScreen 设备提供接口冗余用到的几种方法。本章内容分为以下几个部分：

- 第 60 页上的 “冗余接口”
- 第 67 页上的 “聚合接口”
- 第 69 页上的 “Dual Untrust 接口”
  - 第 70 页上的 “接口故障切换”
  - 第 72 页上的 “确定接口故障切换”
- 第 103 页上的 “串行接口”
  - 第 104 页上的 “调制解调器的设置”
  - 第 106 页上的 “ISP 配置”
  - 第 108 页上的 “串行接口故障切换”

冗余接口

对于 HA 接口冗余，不是由 NetScreen 设备提供专用的物理冗余 HA 接口，就是由用户将两个通用接口绑定到 HA 区段。有关详细信息，请参阅第 39 页上的 “双 HA 接口”。还可以创建冗余的安全区段接口，如本节所述。

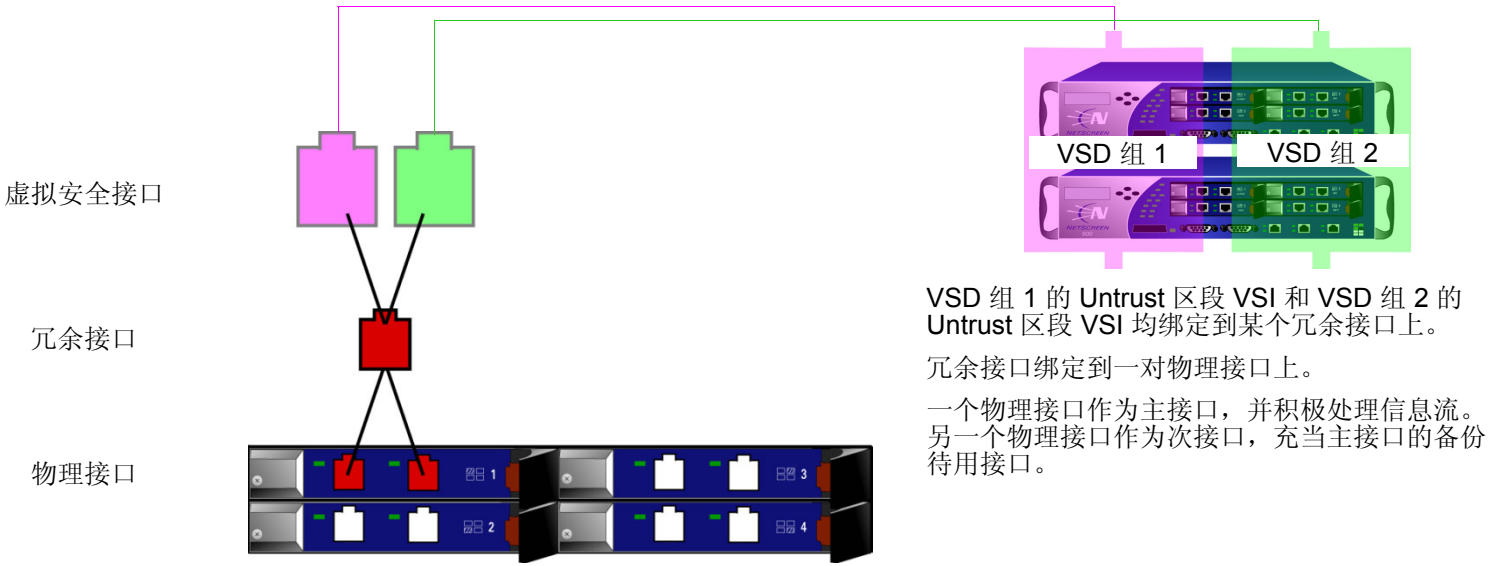
可以允许 VSI 将其绑定从一台设备的物理接口转移到另一台设备的物理接口，类似于应用该操作的虚拟化过程，VSI 可以将其绑定从同一设备的一个物理接口转移到另一个物理接口。例如，假设主接口到交换机的链接断开，该链接中断将导致从主接口到次接口的故障切换，从而避免了从 VSD 主设备到备份设备的故障切换。

还可以设置物理接口的等待时间，即发生接口故障切换后，经过多久该物理接口成为主接口。要设置冗余接口成员的等待时间，请使用以下命令，命令中的接口名称即物理接口名称 : **set interface** *interface* **phy holddown** *number*。注意，必须先输入此命令，然后才能让该接口成为冗余组的成员。

可将 VSI 绑定到下列接口类型之一：

- 子接口
- 物理接口
- 冗余接口，依次绑定到两个物理接口[1]

> ***注意：****不能将子接口分组到冗余接口中。但是，可以在冗余接口上定义一个 VLAN，同样也可以在子接口上定义一个 VLAN。有关子接口和 VLAN 的信息，请参阅第* ***9****-23 页上的“定义子接口和 VLAN 标记”。*



1. 可以在回传接口上配置 VSI，但不能将两个回传接口绑定到一个冗余接口上。

范例：为 VSI 创建冗余接口

在本例中，设备 A 和 B 是处于主动 / 主动配置的两个 VSD 组 (VSD 组 0 和 VSD 组 1) 的成员。设备 A 既是 VSD 组 0 的主设备，又是 VSD 组 1 的备份设备。设备 B 既是 VSD 组 1 的主设备，又是 VSD 组 0 的备份设备。NetScreen 设备链接到两对冗余交换机，即 Untrust 区段中的交换机 A 和 B，以及 Trust 区段中的交换机 C 和 D。

注意：*本例仅介绍在设备 A 上创建冗余接口。因为设备 A 和 B 是同一 NSRP 集群的成员，因此设备 A 会将除管理 IP 地址之外的所有的接口配置传播给设备 B，应在以下两个设备的 redundant2 接口上输入该管理 IP 地址：设备 A 10.1.1.21 和设备 B 10.1.1.22。*

将 ethernet1/1 和 ethernet1/2 放置在 redundant1 中，将 ethernet2/1 和 ethernet2/2 放置在 redundant2 中。在 redundant2 接口上，将设备 A 的管理 IP 定义为 10.1.1.21，并在此接口中将设备 B 的管理 IP 定义为 10.1.1.22。

绑定到同一冗余接口的物理接口连接到不同的交换机：

- Untrust 区段中绑定到冗余接口的物理接口：连接到交换机 A 的 ethernet1/1，连接到交换机 B 的 ethernet1/2
- Trust 区段中绑定到冗余接口的物理接口：连接到交换机 C 的 ethernet2/1，连接到交换机 D 的 ethernet2/2

注意：*物理接口并不一定要与其所绑定到的冗余接口位于同一安全区段中。*

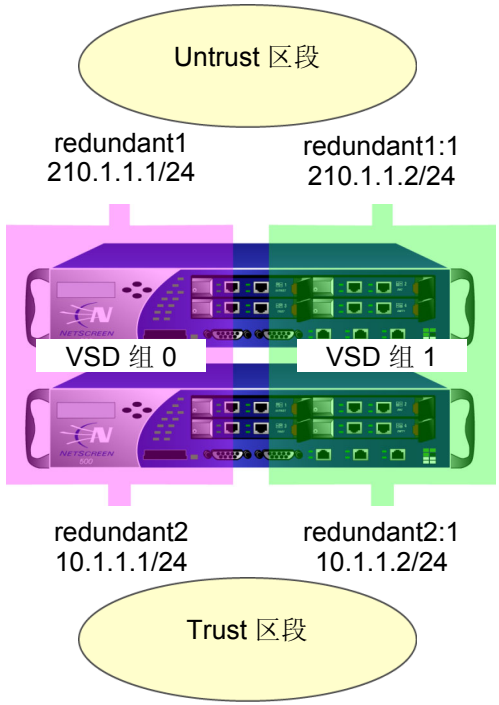
通过首先将 ethernet1/1 和 ethernet2/1 放置在其各自的冗余接口中，即可将它们指定为主接口。(可通过 CLI 命令 **set interface** *redundant1* **primary** *interface1/1* 更改主状态的分配。) 如果到主接口的链接断开，则 NetScreen 设备会通过次接口将信息流重新路由到另一交换机，而不要求 VSD 主设备进行故障切换。

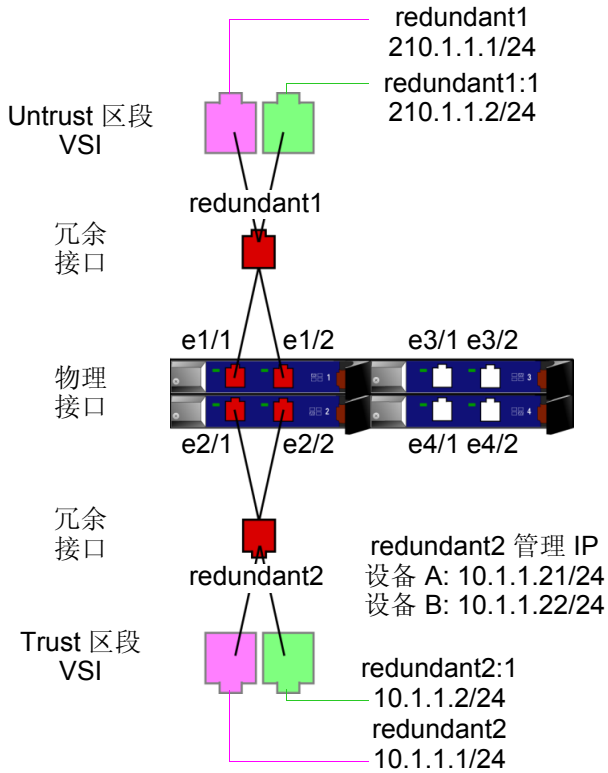
在本例中，ethernet1/1 上的电缆断开，引起了端口故障切换到 ethernet1/2。因此，所有由设备 A 和 B 接收和发送的信息流都将通过交换机 B。将设备 A 上 ethernet1/1 的电缆重新连接到交换机 A 可自动使该接口重新获得其先前的优先级。

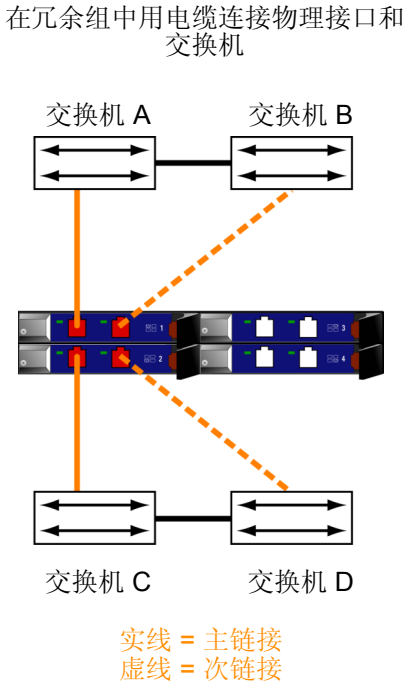
VSI 的 IP 地址：

VSD 组 0 的 VSI		VSD 组 1 的 VSI	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

注意：*如果多个 VSI 在同一个冗余接口、物理接口或子接口上，则这些 VSI 的 IP 地址既可以在同一子网中也可以在不同的子网中。如果 VSI 在不同的接口上，则它们的 IP 地址必须在不同的子网中。*







WebUI (设备 A)

冗余接口

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

Interface Name: redundant1

Zone Name: Untrust

IP Address / Netmask: 210.1.1.1/24

Network > Interfaces > Edit (对于 ethernet1/1): 在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。

Network > Interfaces > Edit (对于 ethernet1/2): 在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。

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

Interface Name: redundant2

Zone Name: Trust

IP Address / Netmask: 10.1.1.1/24

> 在 Manage IP 字段中输入 **10.1.1.21**，然后单击 **OK**。

Network > Interfaces > Edit (对于 ethernet2/1): 在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

Network > Interfaces > Edit (对于 ethernet2/2): 在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

虚拟安全接口

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

Interface Name: VSI Base: redundant1

VSD Group: 1

IP Address / Netmask: 210.1.1.2/24

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

Interface Name: VSI Base: redundant2

VSD Group: 1

IP Address / Netmask: 10.1.1.2/24

WebUI (设备 B)

Network > Interfaces > Edit (对于 redundant2): 在 Manage IP 字段中键入 **10.1.1.22**，然后单击 **OK**。

注意：*必须为每个 VSD 中的每个 VSI 输入到 VSI 的直接子网以外的地址的静态路由。有关为两个 Untrust 区段 VSI 添加缺省路由的范例，请参阅**第 50 页上的 “范例 : 双主动配置的 NSRP”**。*

CLI (设备 A)

冗余接口

```
set interface redundant1 zone untrust
set interface redundant1 ip 210.1.1.1/24

set interface ethernet1/1 group redundant1
set interface ethernet1/2 group redundant1

set interface redundant2 zone trust
set interface redundant2 ip 10.1.1.1/24
set interface redundant2 manage-ip 10.1.1.21
set interface redundant2 nat

set interface ethernet2/1 group redundant2
set interface ethernet2/2 group redundant2

set interface redundant1 primary ethernet1/1

set interface redundant2 primary ethernet2/1
```

虚拟安全接口

```
set interface redundant1:1 ip 210.1.1.2/24
set interface redundant2:1 ip 10.1.1.2/24
save
```

CLI (设备 B)

```
set interface redundant2 manage-ip 10.1.1.22
save
```

注意： *必须为每个 VSD 中的每个 VSI 输入到 VSI 的直接子网以外的地址的静态路由。有关为两个 Untrust 区段 VSI 添加缺省路由的范例，请参阅**第 50 页上的 “范例：双主动配置的 NSRP”**。*

聚合接口

NetScreen-5000 系统允许将两个或多个物理端口结合成一个虚拟端口。此虚拟端口称作*聚合接口*。只有 “安全端口模块” (SPM) 支持此功能。

- 在 5000-8G SPM 上，最多可以创建四个聚合接口。
- 在 5000-24FE SPM 上，最多可以创建五个聚合接口。

5000-8G SPM 只支持构成聚合接口的部分端口结合。例如，插槽 2 中的 5000-8G SPM 只支持以下端口结合 :

- ethernet2/1 和 ethernet2/2
- ethernet2/3 和 ethernet2/4
- ethernet2/5 和 ethernet2/6
- ethernet2/7 和 ethernet2/8

必须为聚合接口分配以下名称之一 : **aggregate1**、 **aggregate2**、 **aggregate3** 或 **aggregate4**。

注意 : *与使用多数其它端口和接口一样，必须为聚合接口分配一个 IP 地址，以便网络中的其它主机可以到达该接口。*

范例：配置聚合接口

在下例中，将两个 Gigabit Ethernet mini-GBIC 端口 (以 1 Gbps 的数据传输率运行) 结合成一个聚合接口 aggregate1 (以 2 Gbps 的数据传输率运行)。该聚合接口由 5000-8G SPM (位于插槽 2 中) 上的以太网端口 1 和 2 组成，且被绑定到 Trust 区段。

注意：**要查看系统上的可用物理端口，请转到 WebUI 中的 Network > Interfaces 屏幕或输入 CLI 命令* ***get interface*。*

WebUI

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

Interface Name: aggregate1

Zone Name: Trust (选择)

IP Address / Netmask: 10.1.1.0/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

As member of: aggregate1 (选择)

Network > Interfaces > Edit (对于 ethernet2/2): 输入以下内容，然后单击 **OK**:

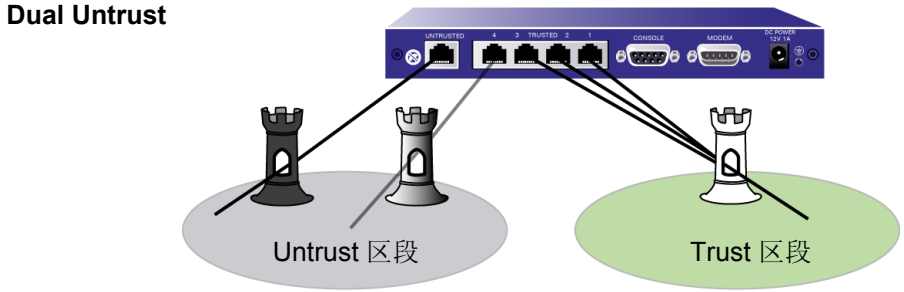
As member of: aggregate1 (选择)

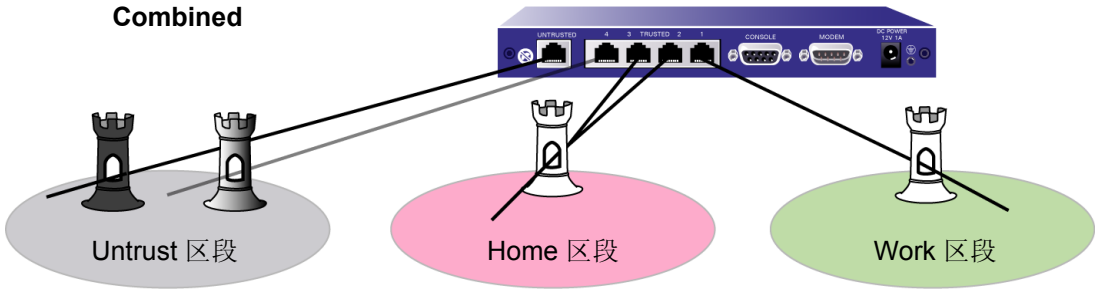
CLI

```
set interface aggregate1 zone trust
set interface aggregate1 ip 10.1.1.0/24
set interface aggregate1 nat

set interface ethernet2/1 aggregate aggregate1
set interface ethernet2/2 aggregate aggregate1
save
```

DUAL UNTRUST 接口

可以为某些 NetScreen 设备选择*端口模式*。端口模式自动为设备设置不同的端口、接口和区段绑定。某些端口模式可将另外一个备份接口绑定到 Untrust 区段 (请参阅第 **2** -39 页上的 “端口模式”)。对于各种端口模式，只有出现下述两种情况时才会用到备份接口 : 经过主接口的连接存在故障时；手动将流向主接口的信息流强制改发到备份接口。例如，在 NetScreen-5XT 上， Dual Untrust 和 Combined 端口模式提供了 Untrust 区段的备份接口。





接口故障切换

主接口和备份接口同时绑定到 Untrust 区段时 (请参阅第 **2** -45 页上的 “设置端口模式”)，可以以手动方式通过 WebUI 或 CLI 将流向主接口的信息流改发到备份接口。还可对 NetScreen 设备进行如下配置 : 一旦 ScreenOS 检测到主接口连接中断，就将信息流自动转发到备份接口。

范例 : 将信息流强制转发到备份接口

在本例中，将以手动方式将流向主接口的信息流强制改发到备份接口。

WebUI

Network > Untrust Failover: 选择 **Failover**，然后单击 **Apply**。接下来，单击 **Force to Failover**。

CLI

```
set failover enable
save
exec failover force
```

主接口再次可用后，需要使用 WebUI 或 CLI 将流向备份接口的信息流改发到主接口。

范例 : 将信息流从备份接口切换回主接口

在前例中，强制执行了从主接口到备份接口的故障切换。在本例中，将以手动方式将信息流从备份接口切换回主接口。

WebUI

Network > Untrust Failover: 单击 **Force to Revert**。

CLI

```
exec failover revert
```

范例：自动改发信息流

在本例中，将对 NetScreen-5GT 进行如下配置：当检测到主接口 IP 跟踪失败时，该设备将信息流自动改发到备份接口[2]。当主接口上的 IP 跟踪重新获得成功时， NetScreen-5GT 会将信息流从备份接口自动切换回主接口。

在缺省情况下，达到 IP 跟踪故障临界值与进行接口故障切换之间有一个 30 秒的间隔 (等待时间)。设置等待时间的目的是为了避免不必要的故障切换，这些不必要的切换可能会导致网络中的间歇等待时间或冲突。在本例中，将等待时间缩短为 20 秒。

WebUI

Network > Untrust Failover: 选择以下内容，然后单击 **Apply**:

Track IP: (选择)

Automatic Failover: (选择)

Failover: (选择)

Failover Holddown Time: 20

CLI

```
set failover type track-ip
set failover auto
set failover enable
set failover holddown 20
save
```

2. 有关设置 IP 跟踪以触发接口故障切换的信息，请参阅第 73 页上的 “使用 IP 跟踪的接口故障切换”。

确定接口故障切换

ScreenOS 在主接口的连接上检测到物理链接故障 (例如没有插入电缆) 时，会发生接口故障切换。还可以定义以下类型的接口故障切换 :

- 不能使用 IP 跟踪经过给定接口到达某些 IP 地址时
- 当主 Untrust 接口上使用 VPN 通道监控的某些 VPN 通道变为不可到达时

接口故障切换顺序如下 :

1. NetScreen 设备确定主接口上的接口监控已失败。该接口可能处于物理连接中断状态，或者 IP 跟踪或 VPN 监控可能出现了故障。
2. NetScreen 设备将等待，直到故障切换等待时间已过。
3. 故障切换等待时间过后，主接口的状态由连接变为中断，备份接口的状态由中断变为连接， NetScreen 设备将使用主接口的信息流改发到备份接口。
4. NetScreen 设备在当前处于激活状态的备份接口上使用 DHCP 或 PPPoE 连接到其 ISP。

> ***注意 :*** *接收到新的出站信息流或刚刚进行故障切换 (**set pppoe name** name **auto-connect**) 后，NetScreen 设备可启动新的 PPPoE 连接。*

恢复顺序与故障切换顺序基本相反 :

1. NetScreen 设备确定主接口上的接口监控已取得成功。该接口可能在物理上已重新建立了连接，或者可能已重新成功进行了 IP 跟踪或 VPN 监控。
2. NetScreen 设备将等待，直到故障切换等待时间已过。
3. 故障切换等待时间过后，备份接口的状态由连接变为中断，主接口的状态由中断变为连接， NetScreen 设备将使用备份接口的信息流改发到主接口。
4. NetScreen 设备在当前处于重新激活状态的主接口上使用 DHCP 或 PPPoE 连接到其 ISP。

> ***注意 :*** *NetScreen 设备在主接口上连接到的 ISP 可以与其在备份接口上连接到的 ISP 相同，也可以与之不同。*

使用 IP 跟踪的接口故障切换

即使物理链接仍处于活动状态，也可以指定当不能通过主 Untrust 区段接口到达某些 IP 地址时， NetScreen 设备将于何时故障切换到备份 Untrust 区段接口。类似于 NSRP 中使用的功能， ScreenOS 使用第 3 层路径监控或 *IP 跟踪* 来监控经过主接口的 IP 地址。如果不能通过主 Untrust 区段接口到达 IP 地址，则 NetScreen 设备会认为该接口处于中断状态，且与该接口相关联的所有路由均处于中断状态。主 Untrust 区段接口变为中断状态后，将故障切换到备份 Untrust 区段接口。注意，可以只配置 IP 跟踪，而不配置自动接口故障切换。

***注意：** 有关在接口上配置 IP 跟踪的信息，请参阅第 **2**-80 页上的 “跟踪 IP 地址”。*

范例 : 接口故障切换

在本例中，首先将 NetScreen-5GT 配置成 Dual Untrust 模式。随后将配置设备执行自动故障切换。主接口自动切换到备份接口后，备份接口将负责传送进出 Untrust 区段的所有信息流，直到主接口恢复正常。

对于主接口， NetScreen 设备监控三个 IP 地址以决定何时进行故障切换。每个被跟踪的 IP 地址的权重如下 :

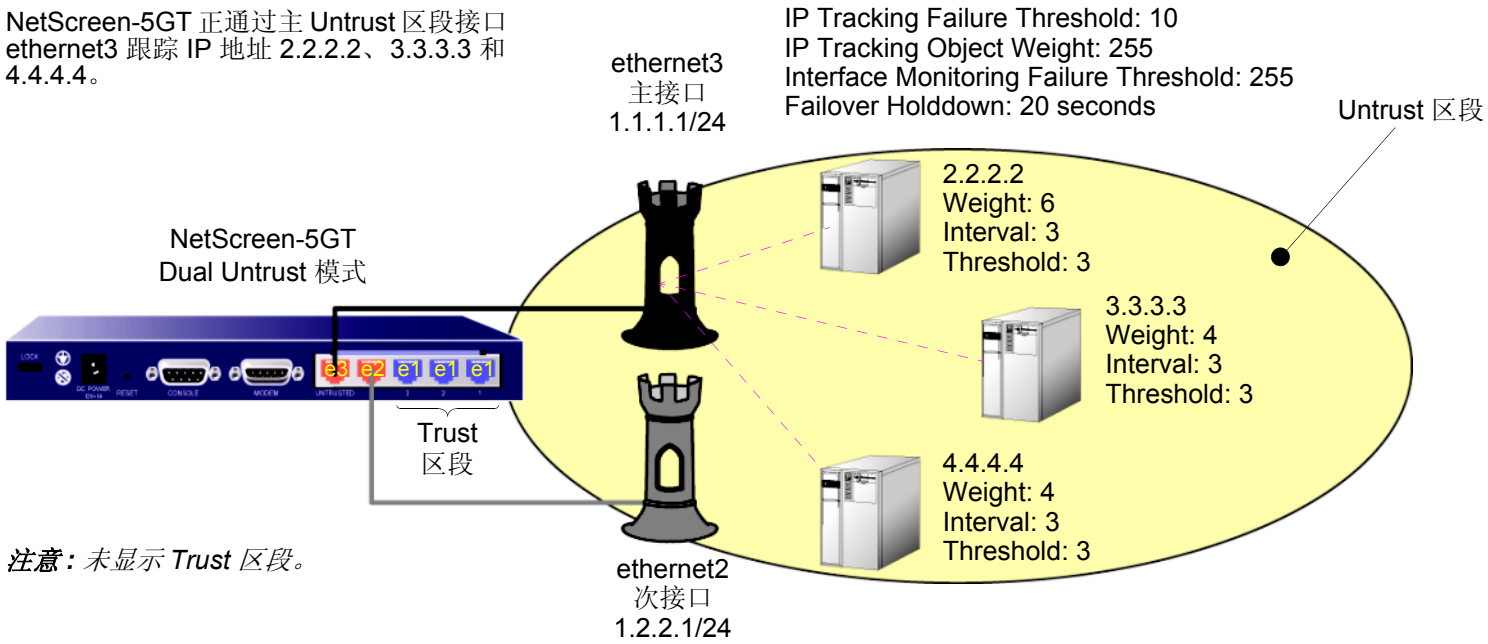
- 2.2.2.2 权重 = 6
- 3.3.3.3 权重 = 4
- 4.4.4.4 权重 = 3

对于上述每个被跟踪的 IP 地址，故障临界值为缺省值 3，并将 ICMP 回应请求间的时间间隔设置为 3 秒。如果 NetScreen 设备无法获取发往被跟踪的 IP 地址的 3 个连续 ICMP 请求 (各个请求间的时间间隔为 3 秒) 的响应，则设备将认为无法通过主接口到达该 IP 地址。

在 IP 跟踪失败时，NetScreen 设备会将已失败地址的权重计入所有 IP 跟踪失败的总权重中。如果总权重达到或超过 IP 跟踪对象临界值 (本例中将其设置为 10)，则 IP 跟踪会将其权重计入接口监控故障临界值。在本例中， IP 跟踪对象权重使用缺省值 255，接口监控故障临界值也使用缺省值 255。

因此，当 IP 跟踪失败的总权重达到 10 时将进行接口故障切换。只有均不能通过主接口到达 IP 地址 2.2.2.2 和 3.3.3.3 (或 2.2.2.2 和 4.4.4.4) 时才会发生此种情况。请注意，如果均不能通过主接口到达 IP 地址 3.3.3.3 和 4.4.4.4，则其故障累计权重将等于 7，将不会导致故障切换。

在本例中，将于 9 秒后达到接口监控故障临界值 (3 次间隔为 3 秒的失败 ICMP 请求)。但是，会将等待时间设置为 20 秒，以便在 IP 跟踪权重 (255) 达到接口监控故障临界值 (255) 时， NetScreen 设备在由主接口故障转换到备份接口前再加权 20 秒。



WebUI

1. 端口模式

Configuration > Port Mode: 从下拉列表中选择 **Dual-Untrust**，然后单击 **Apply**。

出现以下提示：

Operational mode change will erase current configuration and reset the device, continue?

单击 **OK**，随后 NetScreen 设备将重新启动。

2. 登录与接口

再次登录，并设置接口的 IP 地址。然后继续进行以下配置。

3. 自动故障切换和 IP 跟踪

Network > Untrust Failover: 选择以下内容，然后单击 **Apply**:

Track IP: (选择)

Automatic Failover: (选择)

Failover: (选择)

Failover Holddown Time: 20

Network > Interfaces > Edit (对于 ethernet3) > Monitor > Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)

Track IP: 2.2.2.2

Weight: 6

Interval: 3

Threshold: 3

> Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)

Track IP: 3.3.3.3

Weight: 4

Interval: 3

Threshold: 3

> Monitor Track IP ADD: 输入以下内容，然后单击 **Add**:

Static: (选择)

Track IP: 4.4.4.4

Weight: 4

Interval: 3

Threshold: 3

Network > Interface > Edit (对于 ethernet3) > Track IP Options: 输入以下内容，然后单击 **Apply**:

Monitor Option:

Enable Track IP: (选择)

Threshold: 10

Weight: 255

CLI

1. 端口模式

```
exec port-mode dual-untrust
```

出现以下提示：

```
Change port mode from <trust-untrust> to <dual-untrust> will erase system
    configuration and reboot box
Are you sure y/[n] ?
```

按 **Y** 键后， NetScreen 设备将重新启动。

2. 登录与接口

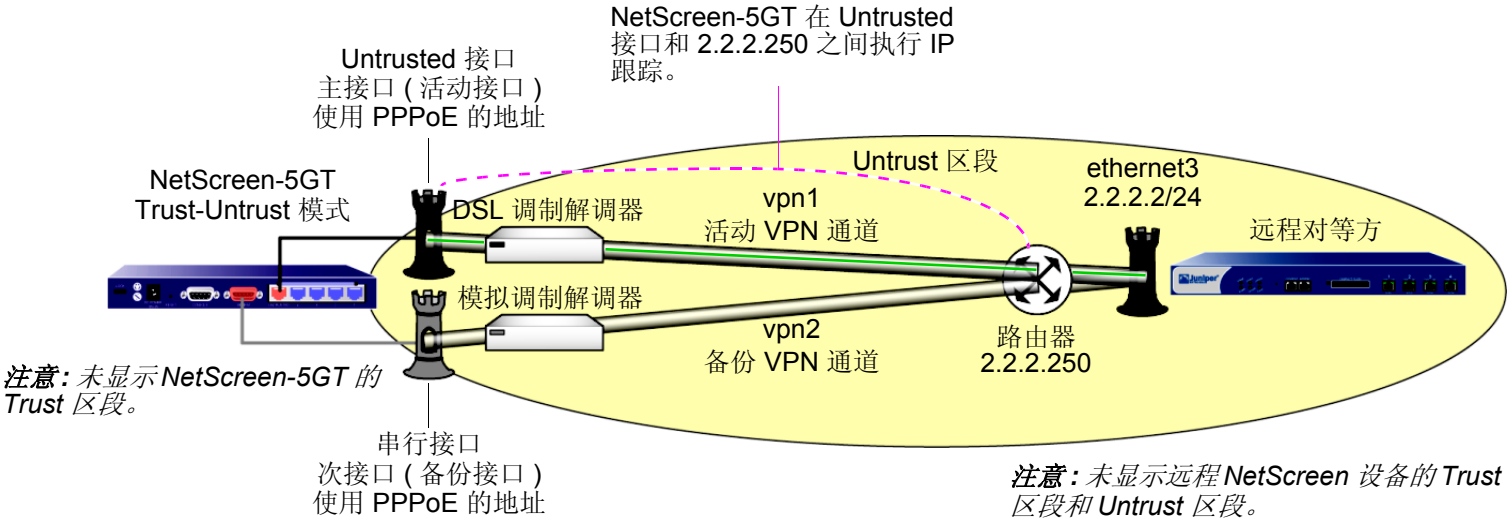
再次登录，并设置接口的 IP 地址。然后继续进行以下配置。

3. 自动故障切换和 IP 跟踪

```
set failover enable
set failover auto
set failover holddown 12
set failover type track-ip
set interface ethernet3 track-ip threshold 10

set interface ethernet3 track-ip ip 2.2.2.2 weight 6
set interface ethernet3 track-ip ip 2.2.2.2 interval 3
set interface ethernet3 track-ip ip 2.2.2.2 threshold 3

set interface ethernet3 track-ip ip 3.3.3.3 weight 4
set interface ethernet3 track-ip ip 3.3.3.3 interval 3
set interface ethernet3 track-ip ip 3.3.3.3 threshold 3

set interface ethernet3 track-ip ip 4.4.4.4 weight 4
set interface ethernet3 track-ip ip 4.4.4.4 interval 3
set interface ethernet3 track-ip ip 4.4.4.4 threshold 3
set interface ethernet3 track-ip
save
```

范例：由活动通道到备份通道的故障切换

在本例中，将在 NetScreen-5GT 设备上配置到远程 IKE 对等方的一对冗余双向 VPN 通道。在任一给定时刻只有一个通道处于活动状态。最初，经由主接口的 VPN 通道处于活动状态 (本例中为 vpn1)。如果该主通道出现了故障，则 NetScreen 设备会将发往远程对等方的 VPN 信息流转发到备份通道 (本例中为 vpn2)。



将仅在远程对等方站点配置一个 VPN 通道，因为从远程对等方的角度来讲只有一个源自 NetScreen-5GT 的 VPN 通道，从而导致了 Y 字形的 VPN 配置。

注意：设置 Y 字形 VPN 配置且备份接口为以太网接口时 (例如 Dual-Untrust 模式)，请勿对使用备份接口的任何 VPN 通道启用 VPN 监控重定密钥选项。如果启用了该选项，即使让该通道处于中断状态， NetScreen 设备仍将继续尝试启用该通道。如果备份接口为串行接口 (如本例中的接口)，则是否对备份接口上的 VPN 通道启用具有重定密钥选项的 VPN 监控将无关紧要。

NetScreen-5GT 处于 Trust-Untrust 模式[3]。 Untrusted 接口为主 Untrust 区段接口，而串行接口是其备份接口。每个 Untrust 区段接口均通过电缆与调制解调器相连。 Untrusted 接口与 DSL 调制解调器 (~1.5–8 Mbps) 相连，串行接口与模拟调制解调器 (~56–64 Kbps) 相连。

注意：*进行故障切换后，吞吐量会因调制解调器速度的差异而显著减少。*

将使用 IP 跟踪来确定是否有必要进行由 Untrusted 接口到串行接口的故障切换。将配置 IP 跟踪以便对位于 2.2.2.250 处的远程对等方的外部路由器执行 ping 操作。由于未配置远程站点的 NetScreen 设备对到达其 Untrust 区段接口的 ICMP 回应请求做出响应，因此将对该地址而不是远程对等方的 Untrust 区段接口的地址 (2.2.2.2) 进行跟踪。将设置以下 IP 跟踪值 :

- 跟踪 IP: 2.2.2.250
  - Weight: 255
  - Interval: 4
  - Threshold: 3
- Track IP failure threshold: 255
- Monitor failure threshold: 255
- Failover holddown: 16

若使用上面的设置，当 IP 跟踪开始失去与被跟踪 IP 地址 (2.2.2.250) 的连接后，由 vpn1 到 vpn2 的故障切换将大约需要花费 30 秒钟的时间 : 3 次间隔为 4 秒的失败 ICMP 回应请求 = 12 秒 + 16 秒的等待时间。在等待时间内，NetScreen-5GT 将以 4 秒为时间间隔不断地发送 ICMP 回应请求，所以故障切换总计需要 7 次连续的失败尝试才能得到来自 ICMP 回应请求的回复 (前 3 次 + 等待期间的另外 4 次)。

注意：*鉴于此范例较长，因此仅对 CLI 配置进行了完整介绍。 WebUI 部分仅列出了通向可在其中设置各个配置要素的各页面的导航路径。可通过查阅 CLI 命令来了解需要进行哪些设置。*

3. 使用任何端口模式均可进行此配置。有关每个端口模式的不同预设接口到区段绑定的说明，请参阅第 **2**-39 页上的 “端口模式”。

WebUI (NetScreen-5GT)

1. 端口模式

   Configuration > Port Mode

2. 登录与接口

   往回登录到 NetScreen 设备。然后继续进行以下配置 :

   Network > Interfaces > Edit (对于 Trust)

   Network > Interfaces > Edit (对于串行接口)

   Network > Interfaces > New Tunnel IF

3. 地址

   Objects > Addresses > List > New

4. PPPoE

   Network > PPPoE > New

5. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

6. 非对称 VPN

   Network > Zones > Edit (对于 Trust)

7. IP 跟踪

   Network > Interfaces > Edit (对于 Untrust) > Monitor

   Network > Interfaces > Edit (对于 Untrust) > Monitor > Monitor Track IP ADD

8. 通道故障切换

   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

9. 路由

   Network > Routing > Routing Entries > trust-vr New

10. 策略

    Policies > (From: Trust, To: Untrust) New

    Policies > (From: Untrust, To: Trust) New

WebUI (远程对等方)

1. 接口

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

4. 路由

   Network > Routing > Routing Entries > trust-vr New

5. 策略

   Policies > (From: Trust, To: Untrust) New

   Policies > (From: Untrust, To: Trust) New

CLI (NetScreen-5GT)

1. 端口模式

```
exec port-mode trust-untrust
```

出现以下提示：

```
Change port mode from <current_port-mode> to <trust-untrust> will erase system
    configuration and reboot box
Are you sure y/[n] ?
```

按 **Y** 键后， NetScreen 设备将重新启动。

2. 登录与接口

往回登录到 NetScreen 设备。然后继续进行以下配置：

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

set interface serial zone untrust

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface trust

set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface trust
```

3. 地址

```
set address untrust peer1 10.2.2.0/24
```

4. PPPoE

```
set pppoe name isp1a
set pppoe name isp1a username ns5gt password juniper
set pppoe name isp1a idle 0
set pppoe name isp1a interface untrust
exec pppoe name isp1a connect
```

5. VPN 通道

```
set ike gateway gw1 address 2.2.2.2 aggressive local-id ns5gt
    outgoing-interface untrust preshare netscreen1 sec-level compatible
set ike gateway gw2 address 2.2.2.2 aggressive local-id ns5gt
    outgoing-interface serial preshare netscreen1 sec-level compatible

set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

6. 非对称 VPN

```
set zone trust asymmetric-vpn
```

7. IP 跟踪

```
set interface untrust monitor track-ip ip
set interface untrust monitor track-ip ip 2.2.2.250 interval 4
set interface untrust monitor track-ip ip 2.2.2.250 threshold 3
set interface untrust monitor track-ip ip 2.2.2.250 weight 255
```

8. 通道故障切换

```
set failover enable
set failover auto
set failover holddown 16
set failover type track-ip
set interface untrust track-ip threshold 255
```

9. 路由

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
```

10. 策略

```
set policy from trust to untrust any any any permit
set policy from untrust to trust peer1 any any permit
save
```

CLI (远程对等方)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. 地址

```
set address untrust ns5gt 10.1.1.0/24
```

3. VPN 通道

```
set ike gateway ns5gt dynamic ns5gt aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible

set vpn vpn1 gateway ns5gt sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

```
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

5. 策略

```
set policy from untrust to trust ns5gt any any permit
set policy from trust to untrust any ns5gt any permit
save
```

使用 VPN 通道监控的接口故障切换

如果确定主接口上的某些 VPN 通道处于 “中断” 状态，则可指定接口故障切换。对于每个 VPN 通道，可以百分比形式指定故障切换权重。仅当一个或多个被监控通道处于 “中断” 状态时，分配的权重才会起作用。如果中断的 VPN 通道的累计权重达到或超过了 100%， ScreenOS 会自动切换到备份接口。

通过对 VPN 通道应用*权重*或权值，可以调整通道状态的重要程度 (与其它通道相比)。可以将较大的权重分配给相对重要的通道，将较小的权重分配给相对次要的通道。注意，*所有*被监控 VPN 通道的累计权重决定了发生接口故障切换的时机。例如，与权重为 10 的 VPN 通道的故障相比，权重为 50 的 VPN 通道的故障更容易导致主接口的故障切换。另请注意，处于 “非活动”、“就绪” 或待定状态的通道将按所分配权重的 50% 来计算。也就是说，如果您为某个处于非活动状态的通道所分配的权重为 50，则可导致接口故障切换的通道的权重将为 25。

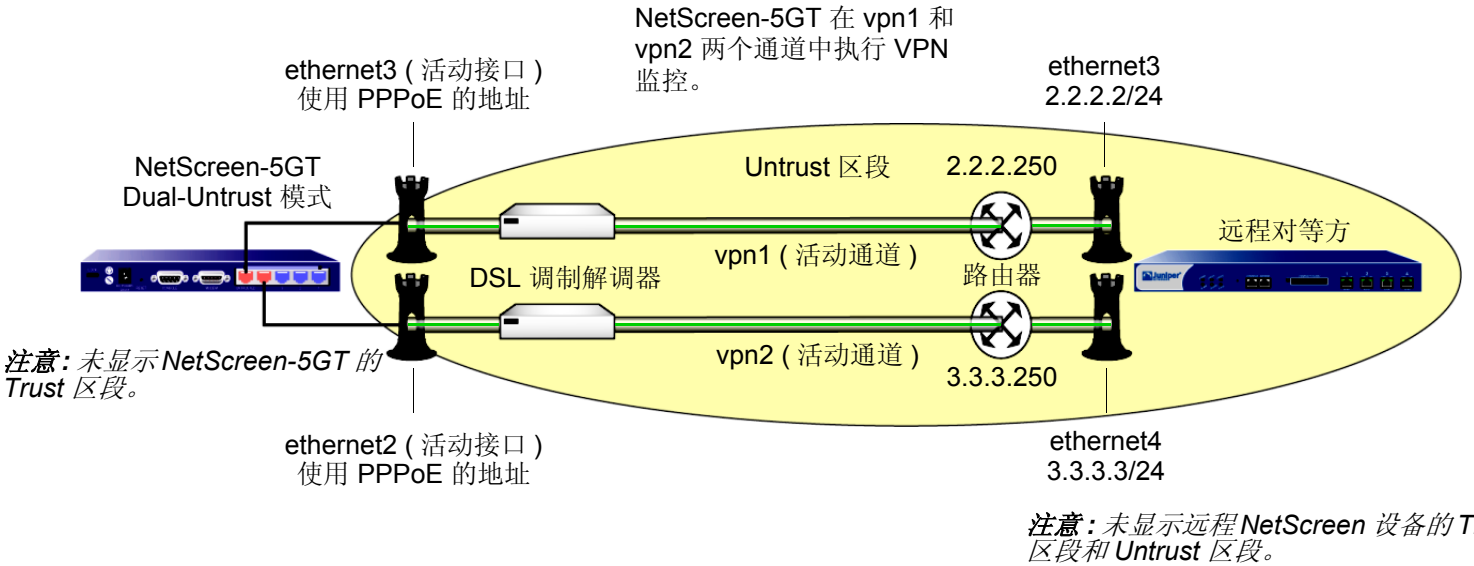
切换到备份接口后，即使启用了 VPN 监控重定密钥功能，ScreenOS 仍会尝试在主接口上建立新的 VPN 通道。如果主接口上的一个或多个 VPN 通道恢复为 “连接” 状态，从而导致累计故障切换权重小于 100%， ScreenOS 会将信息流重新转发到主接口。启用 VPN 监控重定密钥功能后， ScreenOS 可以将流向备份接口的信息流改发到主接口。

范例：双活动通道

此配置的目的是为了支持两个活动 VPN 通道间的 VPN 信息流故障切换。

将配置一对由 NetScreen-5GT 到远程 IKE 对等方的冗余双向 VPN 通道 (vpn1 和 vpn2)。两个通道将同时处于活动状态，而且 NetScreen-5GT 将执行基本形式的负载均衡，交替使用两个通道间的会话。(请注意，这不是真正的负载平衡，因为从一个会话转换到另外一个会话时信息流量会发生显著变化，从而导致非均衡的 “负载”。) 如果任一通道出现故障， NetScreen-5GT 会引导发往远程对等方的所有 VPN 信息流通过其它通道。

NetScreen-5GT 处于 Dual-Untrust 模式[4]。 ethernet3 和 ethernet2 均与 DSL 调制解调器相连。禁用故障切换选项后，它们均将成为活动接口。



在每个站点为 Trust 区段启用非对称 VPN 选项，以便在一个 VPN 通道上建立的现有会话变为另一个会话时，位于通道另一端的 NetScreen 设备不会拒绝此会话。

4. 也可使用 NetScreen-5XT 上的 “组合” 模式或 NetScreen-5GT Extended 平台上的 DMZ/DMZ/Dual Untrust 模式进行此配置。有关每个端口模式的不同预设接口到区段绑定的说明，请参阅第 **2**-39 页上的 “端口模式”。

注意：*鉴于此范例较长，因此仅对 CLI 配置进行了完整介绍。WebUI 部分仅列出了通向可在其中设置各个配置要素的各页面的导航路径。可通过查阅 CLI 命令来了解需要进行哪些设置。*

WebUI (NetScreen-5GT)

1. 端口模式

   Configuration > Port Mode

2. 登录与接口

   往回登录到 NetScreen 设备。然后继续进行以下配置 :

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > New Tunnel IF

3. 地址

   Objects > Addresses > List > New

4. PPPoE

   Network > PPPoE > New

5. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

6. 双通道

   Network > Untrust Failover

7. 非对称 VPN

   Network > Zones > Edit (对于 Trust)

8. 路由

   Network > Routing > Routing Entries > trust-vr New

9. 策略

   Policies > (From: Trust, To: Untrust) New
   Policies > (From: Untrust, To: Trust) New

WebUI (远程对等方)

1. 接口

   Network > Interfaces > Edit (对于 ethernet1)
   Network > Interfaces > Edit (对于 ethernet3)
   Network > Interfaces > Edit (对于 ethernet4)
   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New
   VPNs > Autokey IKE > New

4. 非对称 VPN

   Network > Zones > Edit (对于 Trust)

5. 路由

   Network > Routing > Routing Entries > trust-vr New

6. 策略

   Policies > (From: Trust, To: Untrust) New
   Policies > (From: Untrust, To: Trust) New

CLI (NetScreen-5GT)

1. 端口模式

```
exec port-mode dual-untrust
```

出现以下提示：

```
Change port mode from <trust-untrust> to <dual-untrust> will erase system
    configuration and reboot box
Are you sure y/[n] ?
```

按 **Y** 键后， NetScreen 设备将重新启动。

2. 登录与接口

往回登录到 NetScreen 设备。然后继续进行以下配置：

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

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1

set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
```

3. 地址

```
set address untrust peer1 10.2.2.0/24
```

4. PPPoE

```
set pppoe name isp1a
set pppoe name isp1a username ns5gt1a password juniper1a
set pppoe name isp1a idle 0
set pppoe name isp1a interface ethernet3
exec pppoe name isp1a connect
```

```
set pppoe name isp1b
set pppoe name isp1b username ns5gt1b password juniper1b
set pppoe name isp1b idle 0
set pppoe name isp1b interface ethernet2
exec pppoe name isp1b connect
```

5. VPN 通道

```
set ike gateway gw1 address 2.2.2.2 aggressive local-id 5gt-e3
    outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
set ike gateway gw2 address 3.3.3.3 aggressive local-id 5gt-e2
    outgoing-interface ethernet2 preshare netscreen2 sec-level compatible

set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 2.2.2.2 rekey

set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 monitor source-interface ethernet1 destination-ip 3.3.3.3 rekey
```

6. 双通道

```
unset failover enable
```

7. 非对称 VPN

```
set zone trust asymmetric-vpn
```

8. 路由

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
```

9. 策略

```
set policy from trust to untrust any any any permit
set policy from untrust to trust peer1 any any permit
save
```

CLI (远程对等方)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface ethernet4 zone untrust
set interface ethernet4 ip 3.3.3.3/24

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1

set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1
```

2. 地址

```
set address untrust ns5gt 10.1.1.0/24
```

3. VPN 通道

```
set ike gateway gw1 dynamic ns5gt-e3 aggressive outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface
    ethernet4 preshare netscreen2 sec-level compatible

set vpn vpn1 gateway gw1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any

set vpn vpn2 gateway gw2 sec-level compatible
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 非对称 VPN

```
set zone trust asymmetric-vpn
```

5. 路由

```
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.2
set vrouter trust-vr route 10.1.1.0/24 interface null metric 100
```

6. 策略

```
set policy from trust to untrust any any any permit
set policy from untrust to trust ns5gt any any permit
save
```

范例：对通道故障切换应用权重

在本例中，将创建三对单向 VPN 通道，其中每对通道均由一个主通道和一个备份通道组成。这些通道将分公司站点的 Trust 区段中的主机连接到企业站点的 Trust 区段中的 DNS、 SMTP 和 HTTP 服务器。每个站点的所有区段都在 trust-vr 路由选择域中。

首先配置 Dual Untrust 模式下的 NetScreen-5XT，它是用来保护分公司站点的 NetScreen 设备。然后配置将主 Untrust 区段接口 (ethernet3) 作为出接口的三个 VPN 通道以及将备份 Untrust 区段接口 (ethernet2) 作为出接口的三个备份 VPN 通道。 NetScreen 设备对主 VPN 通道进行监控以确定何时进行故障切换。每个 VPN 通道的故障切换权重如下：

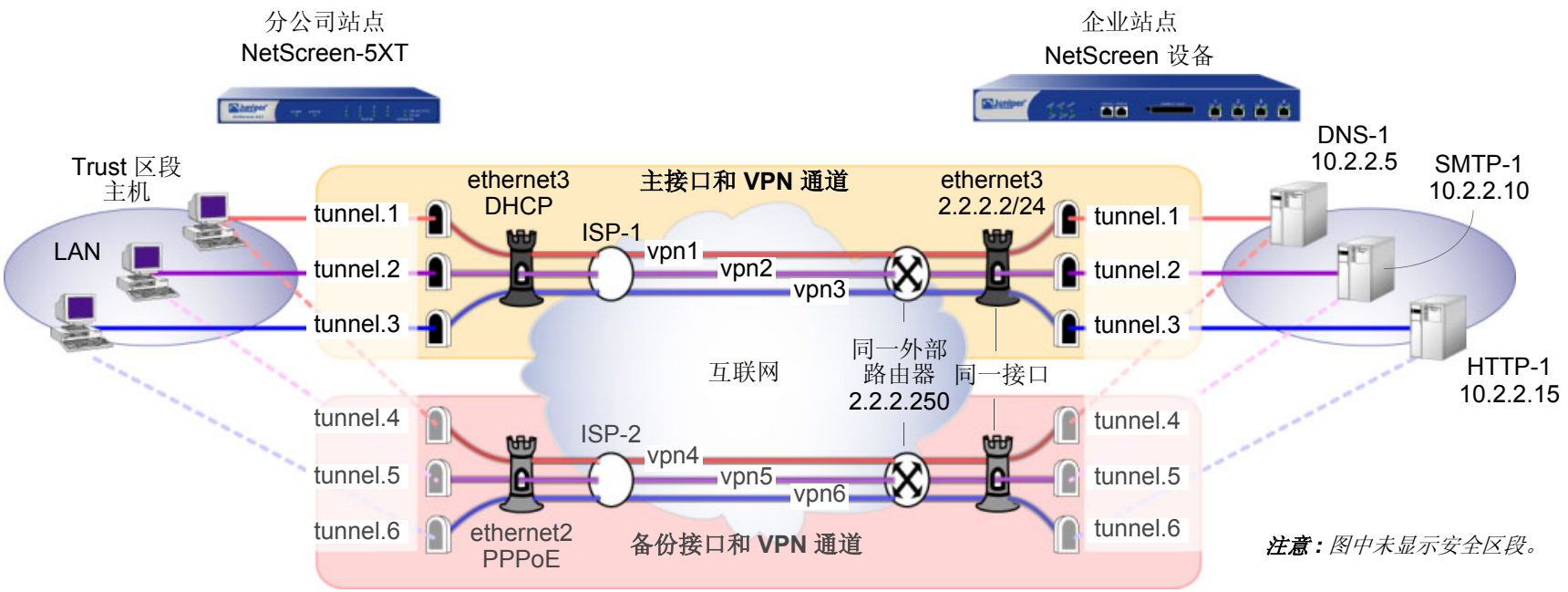
- vpn1 Weight: 60
- vpn2 Weight: 40
- vpn3 Weight: 40

将配置 NetScreen 设备使其可进行故障切换。主接口自动切换到备份接口后，备份接口将负责传送进出 Untrust 区段的所有信息流，直到主接口恢复正常。累计故障切换权重达到或超过 100% 时，主接口即会发生故障切换。也就是说，当 vpn1 和 vpn2 都处于中断状态时，累计故障权重将为 100%，这时将导致自动故障切换到备份接口。注意，当只有 vpn2 和 vpn3 处于中断状态，累计故障权重将为 80%，此时不会发生故障切换。

也可启用 VPN 监控重定密钥功能。发生故障切换后，当主接口的 VPN 通道的累计权重小于 100% 时，此功能允许 NetScreen 设备将流向备份设备的信息流重新转发到主接口。

最后，在每个站点为 Trust 区段启用非对称 VPN 选项，以便在一个 VPN 通道上建立的现有会话切换为另一个会话时，位于通道另一端的 NetScreen 设备不会拒绝此会话。

NetScreen-5XT 设备从两个不同的 ISP 动态接收其 Untrust 区段接口地址、缺省网关和 DNS 服务器地址。每个 ISP 使用不同的协议。 ISP-1 使用 DHCP 将地址分配给 ethernet3， ISP-2 使用 PPPoE 将地址分配给 ethernet2。企业站点的 NetScreen 设备拥有静态 IP 地址 (2.2.2.2)。其缺省网关的 IP 地址为 2.2.2.250。



VPN 监控的目标地址不是缺省地址 [远程网关 IP 地址 (2.2.2.2)]，而是三个服务器的地址 (10.2.2.5、 10.2.2.10、10.2.2.15)。若使用的是远程网关 IP 地址，且又无法到达该地址，则所有三个主通道将总是同时故障切换到备份通道。这将无法使用权重来执行这样的操作 : 只有当两个通道 (vpn1 + vpn2 或 vpn1 + vpn3) 同时出现故障时才进行故障切换。另一方面，如果 VPN 监控通过每个通道来监控不同的目标地址，且该功能无法再通过 vpn1 对 DNS-1 执行 ping 操作，则不会进行故障切换。如果，随后 NetScreen-5XT 无法再通过 vpn2 对 SMTP-1 执行 ping 操作，则相加后的权重总计为 100% (60 + 40)， vpn1 将故障切换到 vpn4， vpn2 将故障切换到 vpn5，而 vpn3 将处于活动状态。

注意： *鉴于此范例较长，因此仅对 CLI 配置进行了完整介绍。 WebUI 部分仅列出了通向可在其中设置各个配置要素的各页面的导航路径。可通过查阅 CLI 命令来了解需要进行哪些设置。*

WebUI (分公司)

1. 端口模式

   Configuration > Port Mode

2. 登录与接口

   往回登录到 NetScreen 设备。然后继续进行以下配置 :

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interfaces > Edit (对于 ethernet2)

   Network > Interfaces > New Tunnel IF

3. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

4. 通道故障切换

   Network > Untrust Failover

   Network > Untrust Failover > Edit Weight

5. 非对称 VPN

   Network > Zones > Edit (对于 Trust)

6. 路由

   Network > Routing > Routing Entries > trust-vr New

7. 策略

   Policies > (From: Trust, To: Untrust) New

WebUI (企业)

1. 接口

   Network > Interfaces > Edit (对于 ethernet1)

   Network > Interfaces > Edit (对于 ethernet3)

   Network > Interfaces > New Tunnel IF

2. 地址

   Objects > Addresses > List > New

3. 服务组

   Objects > Services > Groups > New

4. VPN 通道

   VPNs > AutoKey Advanced > Gateway > New

   VPNs > Autokey IKE > New

5. 非对称 VPN

   Network > Zones > Edit (对于 Trust)

6. 路由

   Network > Routing > Routing Entries > trust-vr New

7. 策略

   Policies > (From: Trust, To: Untrust) New

CLI (分公司)

1. 端口模式

```
exec port-mode dual-untrust
```

出现以下提示：

```
Change port mode from <trust-untrust> to <dual-untrust> will erase system
    configuration and reboot box
Are you sure y/[n] ?
```

按 **Y** 键后， NetScreen 设备将重新启动。

2. 登录与接口

往回登录到 NetScreen 设备。然后继续进行以下配置：

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

set interface ethernet3 dhcp client
exec dhcp client ethernet3 renew

set pppoe interface ethernet2
set pppoe username ns5gt password juniper

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1

set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1

set interface tunnel.3 zone trust
set interface tunnel.3 ip unnumbered interface ethernet1

set interface tunnel.4 zone trust
set interface tunnel.4 ip unnumbered interface ethernet1
```

```
set interface tunnel.5 zone trust
set interface tunnel.5 ip unnumbered interface ethernet1

set interface tunnel.6 zone trust
set interface tunnel.6 ip unnumbered interface ethernet1
```

3. VPN 通道

```
set ike gateway corp1 address 2.2.2.2 aggressive local-id 5gt-e3
    outgoing-interface ethernet3 preshare netscreen1 sec-level basic
set ike gateway corp2 address 2.2.2.2 aggressive local-id 5gt-e2
    outgoing-interface ethernet2 preshare netscreen2 sec-level basic

set vpn vpn1 gateway corp1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey

set vpn vpn2 gateway corp1 sec-level basic
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP[5]
set vpn vpn2 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey

set vpn vpn3 gateway corp1 sec-level basic
set vpn vpn3 bind interface tunnel.3
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn3 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey

set vpn vpn4 gateway corp2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS
set vpn vpn4 monitor source-interface ethernet1 destination-ip 10.2.2.5 rekey
```

5. 通常，代理 ID 可以为“local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any”。不过，此时每个通道的代理 ID 必须不同，以便可将一个通道与另一个通道区别开来。如果每个代理 ID 的服务均相同，则将导致配置冲突，且 NetScreen 设备将拒绝 vpn2 和 vpn3 (及 vpn5 和 vpn6) 的代理 ID。

```
set vpn vpn5 gateway corp2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP
set vpn vpn5 monitor source-interface ethernet1 destination-ip 10.2.2.10 rekey

set vpn vpn6 gateway corp2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
set vpn vpn6 monitor source-interface ethernet1 destination-ip 10.2.2.15 rekey
```

4. 通道故障切换

```
set failover type tunnel-if
set failover auto
set vpn vpn1 failover-weight 60
set vpn vpn2 failover-weight 40
set vpn vpn3 failover-weight 40
```

5. 非对称 VPN

```
set zone trust asymmetric-vpn
```

6. 路由

```
set vrouter trust-vr route 10.2.2.5/32 interface tunnel.1
set vrouter trust-vr route 10.2.2.10/32 interface tunnel.2
set vrouter trust-vr route 10.2.2.15/32 interface tunnel.3
set vrouter trust-vr route 10.2.2.5/32 interface tunnel.4
set vrouter trust-vr route 10.2.2.10/32 interface tunnel.5
set vrouter trust-vr route 10.2.2.15/32 interface tunnel.6
set vrouter trust-vr route 10.2.2.0/24 interface null metric 100
```

7. 策略

```
set policy from trust to untrust any any any permit
save
```

CLI (企业)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.2.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24

set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1

set interface tunnel.2 zone trust
set interface tunnel.2 ip unnumbered interface ethernet1

set interface tunnel.3 zone trust
set interface tunnel.3 ip unnumbered interface ethernet1

set interface tunnel.4 zone trust
set interface tunnel.4 ip unnumbered interface ethernet1

set interface tunnel.5 zone trust
set interface tunnel.5 ip unnumbered interface ethernet1

set interface tunnel.6 zone trust
set interface tunnel.6 ip unnumbered interface ethernet1
```

注意：*与创建六个通道接口相反 (为每个 VPN 通道各创建一个通道接口)，也可创建一个通道接口，然后将多个 VPN 通道绑定到该接口。 NetScreen 设备使用 “下一跳跃通道绑定” (NHTB) 表来区分各个通道。有关 NHTB 的信息，请参阅第* ***5****-374 页上的 “每个通道接口多个通道”。*

2. 地址

```
set address untrust branch 10.1.1.0/24
set address trust DNS-1 10.2.2.5/32
set address trust SMTP-1 10.2.2.10/32
set address trust HTTP-1 10.2.2.15/32
set group address trust servers add DNS-1
set group address trust servers add SMTP-1
set group address trust servers add HTTP-1
```

3. 服务组

```
set group service vpn-srv add DNS
set group service vpn-srv add SMTP
set group service vpn-srv add HTTP
set group service vpn-srv add ICMP
```

4. VPN 通道

```
set ike gateway branch1 dynamic ns5gt-e3 aggressive outgoing-interface
    ethernet3 preshare netscreen1 sec-level basic
set ike gateway branch2 dynamic ns5gt-e2 aggressive outgoing-interface
    ethernet3 preshare netscreen2 sec-level basic

set vpn vpn1 gateway branch1 sec-level basic
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn2 gateway branch1 sec-level basic
set vpn vpn2 bind interface tunnel.2
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn3 gateway branch1 sec-level basic
set vpn vpn3 bind interface tunnel.3
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
```

```
set vpn vpn4 gateway branch2 sec-level basic
set vpn vpn4 bind interface tunnel.4
set vpn vpn4 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 DNS

set vpn vpn5 gateway branch2 sec-level basic
set vpn vpn5 bind interface tunnel.5
set vpn vpn5 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 SMTP

set vpn vpn6 gateway branch2 sec-level basic
set vpn vpn6 bind interface tunnel.6
set vpn vpn6 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 HTTP
```

5. 非对称 VPN

```
set zone trust asymmetric-vpn
```

6. 路由

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

7. 策略

```
set policy from untrust to trust branch servers vpn-srv permit
save
```

串行接口

为了建立某些 NetScreen 设备与 ISP 之间的 PPP 连接，可以将外部调制解调器连接到这些设备的 RS-232 串行端口。这就为流向 Untrust 区段的信息流提供了一个拨号备份接口，当经过主接口的连接中断时将使用该接口。在缺省情况下， Trust-Untrust 和 Home-Work 端口模式启用拨号备份功能 (请参阅第 **2** -39 页上的 “端口模式”)。

拨号备份功能允许有两个接口绑定到 Untrust 区段 :

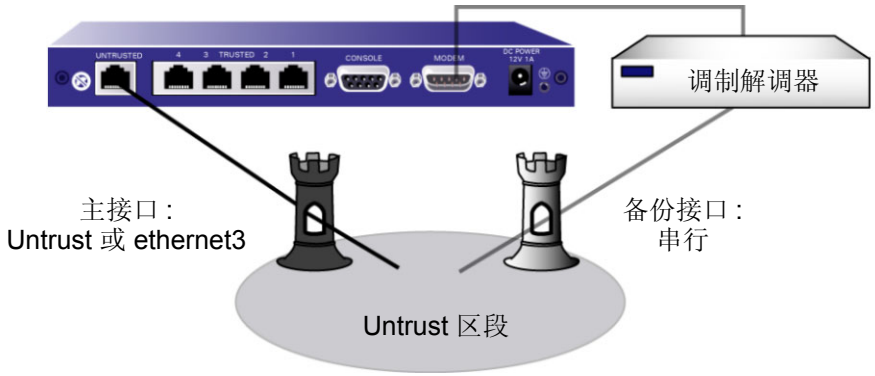
- 主物理接口是 Untrusted 以太网端口。在 ScreenOS 上，主逻辑接口为处于 Trust-Untrust 端口模式的 Untrust 接口和处于 Home-Work 端口模式的 ethernet3。
- 备份物理接口是调制解调器端口。在 ScreenOS 上，备份接口为处于 Trust-Untrust 或 Home-Work 端口模式的串行接口。在缺省情况下，串行接口绑定到 Null 区段。为了将串行接口用作备份接口，需要将其绑定到 Untrust 区段。

需要配置 ScreenOS，使得当信息流改发到串行接口时，通过调制解调器对现有 ISP 帐户进行拨号。切换到串行接口时，除非有要发送的信息流[6] 或调制解调器的空闲超时值设为 0，否则调制解调器不会拨号。拨号链接连通期间，ScreenOS 最多能在队列中放置 16 个数据包，这样即可在尽量不丢失数据的情况下，将信息流改发到串行接口。

在缺省情况下，需要在 NetScreen 设备上手动执行接口故障切换。手动执行故障切换时，需要使用 CLI 或 WebUI 来迫使 ScreenOS 将流向一个接口的信息流改发到另一个接口。当主接口再次可用后，需要使用 CLI 或 WebUI 指示 ScreenOS 将流向备份接口的信息流改发到主接口。

NetScreen 设备可以自动切换到串行接口，并会对先前存在的 ISP 帐户进行拨号和认证。经由主接口的连接一旦得到恢复， ScreenOS 会自动将流向串行接口的信息流改发到主接口。

6. 只有启用策略的直通 (用户生成的) 信息流才能促使调制解调器拨号。与管理或路由协议相关的消息 (例如 OSPF hello 消息) 不会促使调制解调器拨号。



调制解调器的设置

拨号连接所使用的调制解调器必须支持以下功能 :

- 硬件流控制
- 提供清除发送 (CTS) 信号
- 可以响应请求发送 (RTS) 信号
- 仅限于异步
- 支持 AT 命令集

可以在 ScreenOS 中配置以下串行链接参数 :

- ScreenOS 自动断开调制解调器前，串行链接的最长空闲时间 (缺省值为 10 分钟)
- 线路忙或无响应时， ScreenOS 重新尝试拨号连接的最大次数 (缺省值为 3 次)
- 重新尝试拨号的时间间隔，以秒为单位 (缺省值为 10 秒)
- 串行链接的最大波特率 (缺省值为 115200 bps)

ScreenOS 使用缺省的调制解调器初始化字符串。最多可以配置四个调制解调器初始化字符串，但一次只能激活一个配置的初始化字符串。调制解调器的初始化字符串必须符合以下要求：

- 建议使用硬件流控制，但不要求一定使用 (可以指定为无流控制)
- 不使用软件流控制
- 必须以 “逐字” 模式显示结果代码

范例：配置调制解调器的设置

在本例中，将调制解调器的空闲时间配置成 20 分钟。还将为新的调制解调器设置定义调制解调器初始化字符串 *mod1*，然后将其激活。

WebUI

Network > Interfaces > Edit (对于串行接口) > Modem: 输入以下内容，然后单击 **OK**:

Modem Name: mod1

Init String: AT&FS7=255S32=6

Status: Enable (选择)

Inactivity Timeout: 20

CLI

```
set modem idle-time 20
set modem settings mod1 init-strings AT&FS7=255S32=6
set modem settings mod1 active
save
```

ISP 配置

可以配置 NetScreen 设备，使得当切换到串行接口且存在待发信息流时，将对 ISP 帐户进行拨号。最多可配置四个 ISP 连接，可为它们分配不同的优先级号 (1 代表最高优先级)。优先级号决定了 ScreenOS 尝试拨号连接的顺序，ScreenOS 首先对优先级最高的 ISP 进行拨号。如果 ScreenOS 无法登录到优先级最高的 ISP 帐户，将对优先级第二高的 ISP 进行拨号，依此类推，直到用完所有的 ISP 配置。

注意：*在缺省情况下，ScreenOS 尝试对配置的 ISP 帐户最多可进行三次拨号 (有关调制解调器参数的信息，请参阅第 104 页上的 “调制解调器的设置”)。如果 ScreenOS 无法连接到配置的任何 ISP 帐户，则会发出连接失败消息，并保持等待直至主接口再次可用为止。*

对于每个 ISP 配置，请指定以下信息：

- 登录帐户和密码。[7]
- 主电话号码以及可选的备用电话号码。如果在缺省情况下调制解调器使用的是脉冲拨号，而您希望使用音频拨号，请在电话号码前加 **T**。如果在缺省情况下调制解调器使用的是音频拨号，而您希望使用脉冲拨号，请在电话号码前加 **P**。
- 此连接的优先级 (相对于所配置的其它 ISP 连接而言)。

7. ISP 帐户必须是标准的 Point-to-Point Protocol (PPP) 帐户，只需要登录时所用的用户名和密码。

范例：配置 ISP 信息

在本例中，将配置两个不同 ISP 帐户的信息：*isp1* 帐户的优先级为 1， *isp2* 帐户的优先级为 2。也就是说，切换到串行接口时， ScreenOS 始终首先对 isp1 帐户进行拨号。

WebUI

Network > Interfaces > Edit (对于串行接口) > ISP: 输入以下内容，然后单击 **OK**:

ISP Name: isp1

Primary Number: 4085551111

Alternative Number: 4085552222

Login Name: kgreen

Login Password: 98765432

Priority: 1

Network > Interfaces > Edit (对于串行接口) > ISP: 输入以下内容，然后单击 **OK**:

ISP Name: isp2

Primary Number: 4085551212

Alternative Number:

Login Name: kgreen

Login Password: 12345678

Priority: 2

CLI

```
set modem isp isp1 account login kgreen password 98765432
set modem isp isp1 primary-number 4085551111 alternative-number 4085552222
set modem isp isp1 priority 1
set modem isp isp2 account login kgreen password 12345678
set modem isp isp2 primary-number 4085551212
set modem isp isp2 priority 2
save
```

串行接口故障切换

在缺省情况下，主接口 (Untrust 或 ethernet3 接口) 连接中断时，必须使用 WebUI 或 CLI 促使 ScreenOS 切换到串行接口，并在主接口再次可用时使用 WebUI 或 CLI 促使 ScreenOS 切换回主接口。可以配置自动执行接口故障切换。还可以配置 IP 跟踪监控 Untrust 或 ethernet3 接口上的故障。有关详细信息，请参阅第 **2** -80 页上的 “跟踪 IP 地址”。

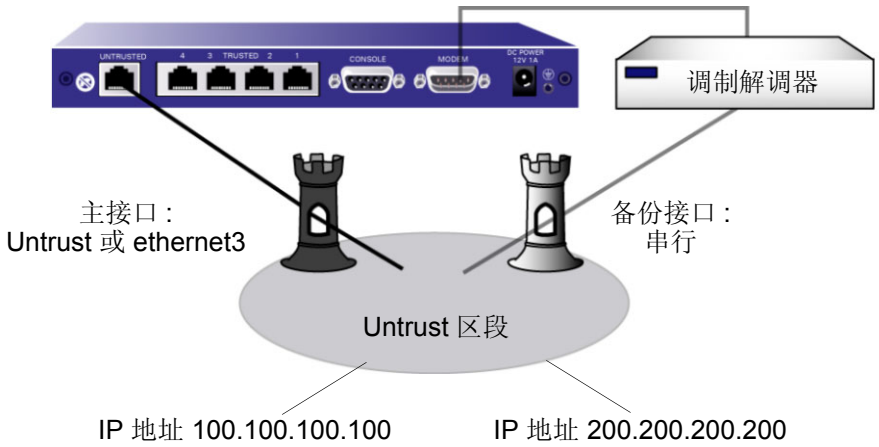
在缺省情况下，切换到串行接口后，允许信息流从 Trust 区段流向 Untrust 区段或允许信息流从 Untrust 区段流向 Trust 区段的策略仍处于活动状态。但是，流经主接口的信息流可能过多，以至于拨号链接无法对其进行处理。定义策略时，可以指定 ScreenOS 切换到串行接口后，该策略是否处于活动状态。有关如何使用 WebUI 和 CLI 配置上述内容的信息，请参阅第 113 页上的 “范例 : 指定策略在串行接口故障切换后处于非活动状态”。

在缺省情况下，串行接口绑定到 Null 区段。为了将串行接口用作备份接口，需要将其明确绑定到 Untrust 区段。如果使用 WebUI 将串行接口绑定到 Untrust 区段， ScreenOS 会自动为串行接口添加缺省路由。如果使用 CLI 将串行接口绑定到 Untrust 区段， ScreenOS *不会*向串行接口添加缺省路由。如果要经过串行接口传送信息流，则必须将缺省路由明确添加到串行接口。有关如何使用 WebUI 和 CLI 配置上述内容的信息，请参阅第 112 页上的 “范例 : 删除串行接口的缺省路由”。

范例：配置 Trust-Untrust 模式下的拨号备份

在本例中，首先将串行接口绑定到 Untrust 区段。串行接口将成为主接口 (Untrust 接口) 的备份接口。随后将配置 ScreenOS，使得当主接口连接中断时自动切换到串行接口。

还将配置 IP 跟踪来确定主接口发生了故障 — 若不能通过主接口到达 IP 地址 100.100.100.100 和 200.200.200.200，ScreenOS 将自动切换到备份接口。



WebUI

Network > Interfaces > Edit (对于串行接口): 输入以下内容，然后单击 **OK**:

Zone Name: (选择) Untrust

Network > Interfaces > Edit (对于串行接口) > Modem: 输入以下内容，然后单击 **OK**:

Modem Name: mod1

Init String: AT&FS7=255S32=6

Inactivity Timeout: 20

Network > Interfaces > Edit (对于串行接口) > ISP: 输入以下内容，然后单击 **OK**:

ISP Name: isp1

Primary Number: 4085551111

Alternative Number: 4085552222

Login Name: kgreen

Login Password: 98765432

Priority: 1

Network > Interfaces > Edit (对于串行接口) > ISP: 输入以下内容，然后单击 **OK**:

ISP Name: isp2

Primary Number: 4085551212

Alternative Number:

Login Name: kgreen

Login Password: 12345678

Priority: 2

Network > Untrust Failover > Automatic Failover: (选择)，然后单击 **Apply**。

Network > Interface > Edit (对于 ethernet3) > Track IP: 输入以下内容，然后单击 **Apply**:

Track IP: 100.100.100.100

Weight: 6

输入以下内容，然后单击 **Apply**:

Track IP: 200.200.200.200

Weight: 4

输入以下内容，然后单击 **Apply**:

Track IP: 210.210.210.210

Weight: 3

Network > Interface (ethernet3) > Edit > Track IP Options: 输入以下内容，然后单击 **OK**:

Enable Track IP: (选择)

Failover Threshold: 10

CLI

```
set interface serial zone untrust
set failover auto

set modem idle-time 20
set modem settings mod1 init-strings AT&FS7=255S32=6
set modem settings mod1 active
set modem isp isp1 account login kgreen password 98765432
set modem isp isp1 primary-number 4085551111 alternative-number 4085552222
set modem isp isp1 priority 1
set modem isp isp2 account login kgreen password 12345678
set modem isp isp2 primary-number 4085551212
set modem isp isp2 priority 2

set interface ethernet3 track-ip
set interface ethernet3 track-ip threshold 10
set interface ethernet3 track-ip ip 100.100.100.100 weight 6
set interface ethernet3 track-ip ip 200.200.200.200 weight 4
set interface ethernet3 track-ip ip 210.210.210.210 weight 3
save
```

范例：删除串行接口的缺省路由

如果使用 WebUI 将串行接口绑定到 Untrust 区段， ScreenOS 会自动为串行接口添加缺省路由。在本例中，将使用 WebUI 将串行接口绑定到 Untrust 区段。随后将删除为串行接口自动创建的缺省路由。

WebUI

Network > Interfaces > Edit (对于串行接口): 输入以下内容，然后单击 **OK**:

Zone Name: (选择) Untrust

Network > Routing > Routing Entries: 在 Configure 栏中，单击 **Remove**，删除经过串行接口到达 0.0.0.0/0 的缺省路由。

范例：为串行接口添加缺省路由

如果使用 CLI 将串行接口绑定到 Untrust 区段，ScreenOS *不会*向串行接口添加缺省路由。如果希望 NetScreen 设备经过串行接口传送信息流，则必须明确地向串行接口添加缺省路由。在本例中，将使用 CLI 将串行接口绑定到 Untrust 区段。随后，将向绑定到 Untrust 区段的串行接口添加缺省路由。

CLI

```
set interface serial zone untrust
set route 0.0.0.0/0 interface serial
save
```

范例：指定策略在串行接口故障切换后处于非活动状态

在本例中，经过主接口 (ethernet3) 流向 Untrust 区段的正常信息流包括通过 FTP 传输的大文件，这些文件从 Trust 区段的 host22 发往 Untrust 区段的 ftp_srv。切换到串行接口后，拨号链接有可能丢弃这类较大的 FTP 信息流。在每次切换到串行接口时，为串行接口配置的任何非活动策略都将失效，因此策略查找过程会继续查找下一策略。

WebUI

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

Source Address:

Address Book Entry: (选择), host22

Destination Address:

Address Book Entry: (选择), ftp_srv

Service: FTP

Action: Permit

> Advanced: 清除 **Valid for Serial**，然后单击 **Return** 设置高级选项并返回基本配置页。

CLI

```
set policy from trust to untrust host22 ftp_srv ftp permit no-session-backup
save
```

3

故障切换

通过冗余可以确保即使主组件不可用，仍可执行特定组件的功能。NetScreen 功能 (例如 NSRP) 提供了设备、VSD 组、 VPN 和接口中的冗余。存在冗余组件时，故障切换处于操作模式，即主组件不可用时，备份组件自动承担主组件的功能。

本章涵盖的具体主题如下：

- 第 116 页上的 “设备故障切换 (NSRP)”
- 第 117 页上的 “VSD 组故障切换 (NSRP)”
- 第 118 页上的 “为设备或 VSD 组故障切换配置对象监控”
  - 第 120 页上的 “配置被监控对象”
- 第 130 页上的 “虚拟系统故障切换”

设备故障切换 (NSRP)

在 NSRP 集群中配置两台 NetScreen 设备时，主设备会同步备份设备的所有配置和状态信息，以便备份设备能在需要时起到主设备的作用。例如，如果集群中的主设备发生故障，备份设备会升级为主设备并接管信息流处理。如果原主设备恢复到故障前的状态，还可以再次接管信息流处理。

导致 NSRP 集群中的主设备切换到备份设备的情况多种多样。这些情况包括主设备自身的物理故障，例如系统崩溃、电源断电、链接中断、设备中缺少 CPU 或内存板。此外，一些管理员定义的情况也能导致主设备切换到备份设备。例如，可以指定当与某些网关或服务器的连接中断时，将主设备切换到备份设备。

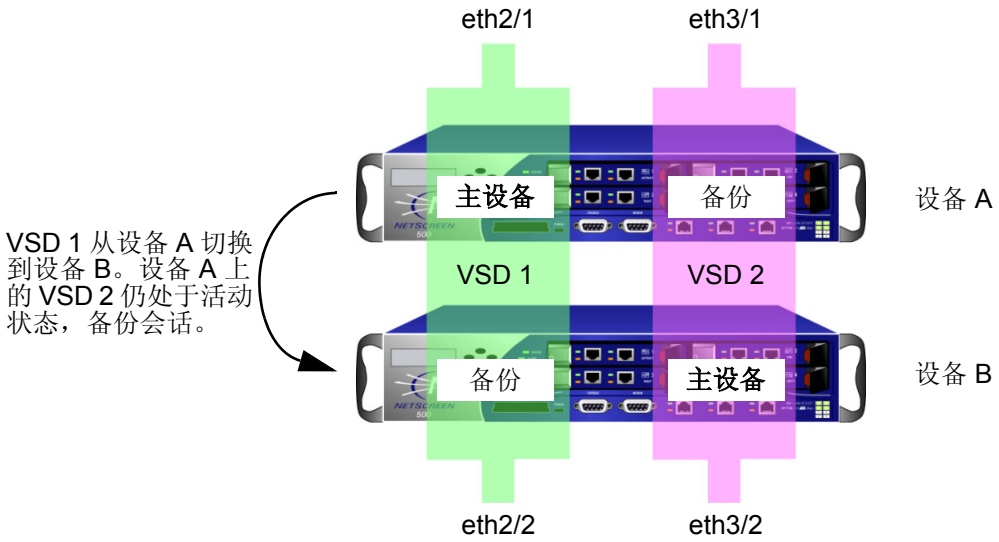
可以配置 NSRP 监控不同的对象，通过一个或多个被监控对象的故障引发主设备的故障切换。有关这些对象及其配置方法的详细信息，请参阅 “为设备或 VSD 组故障切换配置对象监控”。

集群中存在多次故障切换时，至少必须有一台设备充当主设备。如果某设备是集群中唯一一台无故障或无不符合成为主设备条件的设备，该设备会继续充当主设备。在某些情况下，被监控对象的故障可能导致集群中的两台设备同时不可用，以致造成信息流 “黑洞”。为确保一台设置仍能充当主设备并转发信息流，请发出 CLI 命令 **set nsrp vsd-group master-always-exist**。这样一来，即使根据 NSRP 对象监控的结果，集群中的所有设备均被视为有故障， NSRP 集群中的某个设备也能继续转发信息流。如果集群中的所有设备同时转入故障状态，系统会根据为设备预先配置的抢先值和优先值选择新的主设备。

VSD 组故障切换 (NSRP)

除设备故障切换外，还可以配置 NSRP 执行 VSD 组故障切换。与设备故障切换类似，一个或多个被监控对象的故障会导致 VSD 组中的主设备切换到该组的备份设备。有关这些对象及其配置方法的信息，请参阅 “为设备或 VSD 组故障切换配置对象监控”。您可以为 VSD 故障切换配置与设备故障切换相同的被监控对象。

下例说明，如果 VSD 组中的主设备的一个端口发生故障，不一定要将整个主设备切换到备份设备。在以下配置中，如果 ethernet 2/1 发生故障，VSD1 的主状态将由设备 A 切换到设备 B。VSD2 在设备 A 上仍处于活动状态，备份设备 A 上的会话。



为设备或 VSD 组故障切换配置对象监控

使用 NSRP 可监控某些对象，以决定是否对 NetScreen 设备或 VSD 组进行故障切换。 NSRP 被监控对象包括 :

- **物理接口** – NetScreen 设备使用 NSRP 检查物理端口是否处于活动状态以及是否与其它设备相连。
- **区段** – NetScreen 设备使用 NSRP 检查区段内的物理端口是否全部处于活动状态。
- **特定目标 IP 地址** – NetScreen 设备以指定时间间隔向指定 IP 地址 (每个监控对象最多 16 个) 发送 ping 或 ARP 请求，随后监控这些目标地址的响应[1]。为设备或指定 VSD 组配置的所有 IP 地址构成一个被监控对象。一个设备可以有一个被监控对象，每个 VSD 组可以有其自己的被监控对象。

使用被监控对象配置设备或 VSD 组故障切换包含以下设置 :

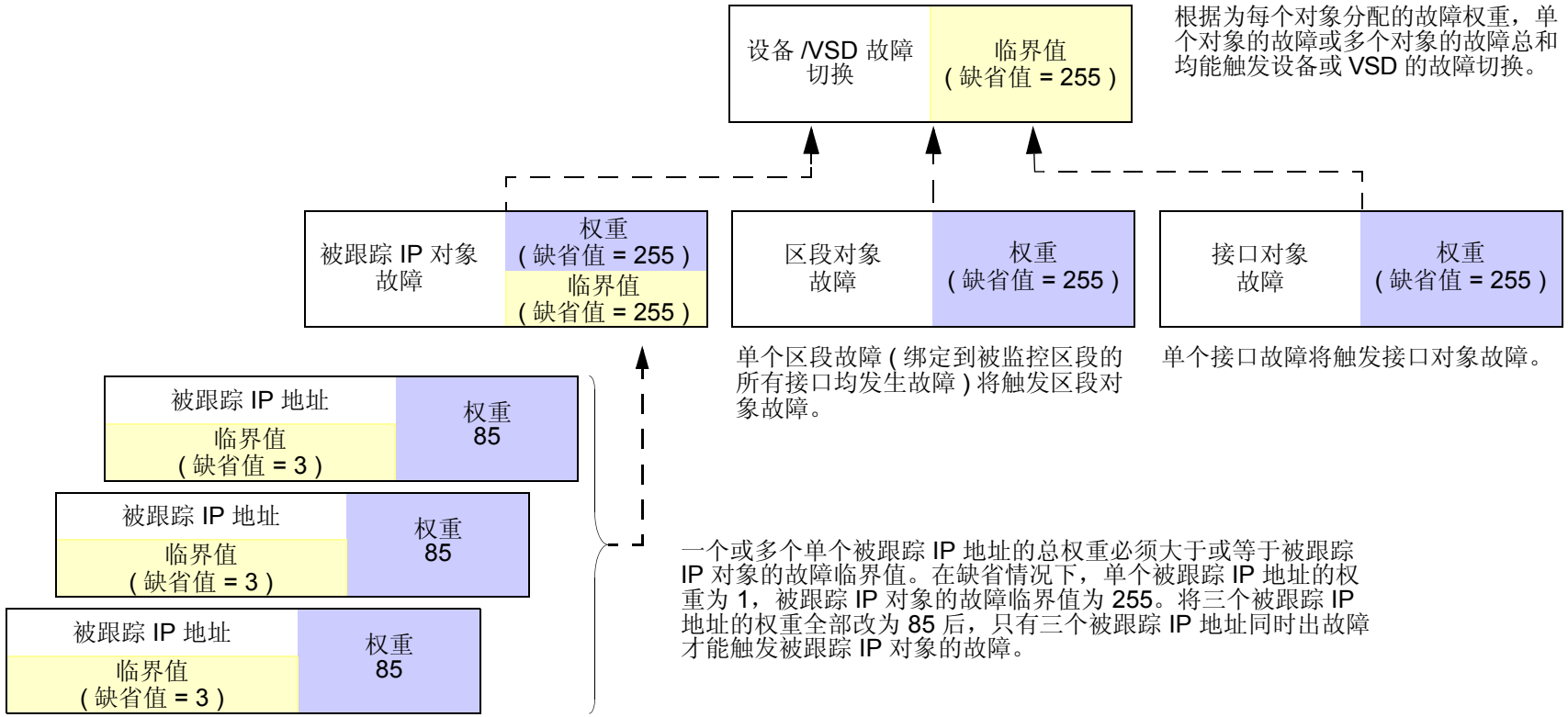
- **设备或 VSD 故障切换临界值** – 设备或 VSD 组故障切换临界值是所有发生故障的被监控对象的总权重，用作设备上的 VSD 组或 NSRP 集群中的设备失去主地位的决定条件。如果所有被监控对象的累计故障权重超过临界值，VSD 组或设备将被切换到备份 VSD 组或设备。设备或 VSD 的故障切换临界值可以设置为 1 到 255 之间的任意值。缺省临界值为 255。
- **每个被监控对象的故障权重** – 每个被监控对象都有一个可配置的故障权重，它是被监控对象的故障所占的权重，用于计算设备或 VSD 的故障切换临界值。对象故障权重可以设置为 1 到 255 间的任何值。

对于被跟踪的 IP 地址，需要逐个指定 IP 地址及其监控方法。还需要定义每个被跟踪 IP 地址 (临界值) 构成故障的条件以及故障 IP 地址附带的权重。对于被跟踪的 IP 对象，还可以指定故障临界值。此临界值是所有发生故障的被跟踪 IP 地址的权重之和，用于认定被跟踪 IP 对象是否出现故障。

注意， VSD 组的被监控对象独立于设备的被监控对象。也就是说，可以为 VSD 组和设备各配置一组不同的对象、权重和临界值。还可以为不同的 VSD 组配置独立的被监控对象组。例如，可以为两个 VSD 组配置相同的被监控对象，并为每个 VSD 组的同一对象指定不同的权重和临界值。

1. NetScreen 设备最多支持由 NSRP 使用的 32 个被监控对象和基于接口的监控，最多共支持 64 个被跟踪 IP 地址。

下图显示了一些被监控对象与设备 /VSD 组故障切换之间的关系。所有失败的被监控对象的权重均计入设备或 VSD 的故障切换临界值。如果不更改被监控对象的缺省权重或设备 /VSD 的故障切换临界值，任何被监控对象的故障都将导致设备或 VSD 的故障切换。对于被跟踪 IP 地址，所有失败的被跟踪 IP 地址的总权重均计入被跟踪 IP 对象的故障临界值。一旦达到被跟踪 IP 对象的故障临界值，系统会将被跟踪 IP 对象的故障权重与设备 /VSD 的故障切换临界值加以比较。



配置被监控对象

本节介绍如何配置被监控对象，其中包括故障权重的设置。

物理接口对象

第 2 层路径监控的功能是检查物理端口是否处于活动状态并连接到其它网络设备。当端口不再处于活动状态时，物理接口对象将发生故障。

范例：监控接口

在本例中，将启用对 ethernet2/1 的监控，以判断可能发生的设备故障切换。将该接口的故障权重设置为 100。

WebUI

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 输入以下内容，然后单击 **Apply**:

Interface Name: ethernet2/1 (选择)

Weight: 100

CLI

```
set nsrp monitor interface ethernet2/1 weight 100
save
```

区段对象

仅当被监控区段中的*所有*接口均发生故障时，区段对象才会发生故障。只要区段中仍存在活动端口，就不会发生区段故障。如果被监控区段未绑定任何接口，则区段对象不会发生故障。NetScreen 设备将始终认为其状态为已启用。如果故障接口是绑定到被监控区段的唯一接口，区段对象会发生故障；一旦解除接口与区段之间的绑定，区段对象将不再发生故障。如果解除某活动接口与被监控区段之间的绑定，而其余的接口都出现故障，则该区段对象将出现故障。

范例：监控接口

在本例中，将启用对 Trust 区段的监控，以判断可能发生的设备故障切换。将该区段的故障权重设置为 100。

WebUI

Network > NSRP > Monitor > Zone > VSD ID: Device Edit Zone: 输入以下内容，然后单击 **Apply**:

Zone Name: Trust (选择)

Weight: 100

CLI

```
set nsrp monitor zone trust weight 100
save
```

被跟踪 IP 对象

IP 跟踪功能以用户定义时间间隔向指定 IP 地址 (最多 16 个) 发送 ping 或 ARP 请求，随后监控目标地址是否响应。配置 IP 跟踪后，设备将从绑定到物理接口、冗余接口或子接口的管理 IP 地址发送 ping 或 ARP 请求。(管理 IP 地址必须与接口 IP 地址相异。) 请注意，不能用 VSI 进行 IP 跟踪，因为该地址可在多个设备中改变其绑定。

注意：*当使用 “虚拟路由器冗余协议 (VRRP)” 将路由器分组到冗余集群中时，如果该路由器不是虚拟 IP 地址的所有者 (故障切换后可能会出现此情况)，则作为主设备的路由器不会对该 IP 地址的 ping 请求做出响应。但是，主设备虚拟路由器一定会响应虚拟 MAC 地址的 ARP 请求，无论它是否是该 IP 地址的所有者。(有关详细信息，请参阅 RFC 2338。) 要在 IP 跟踪时使用 ARP，轮询设备必须与 NetScreen 管理 IP 地址处于同一物理子网中。*

为每个被跟踪 IP 地址指定以下信息 :

- **Tracked IP Failure Threshold** – 引发特定 IP 地址发出 ping 或 ARP 响应的连续失败次数，该失败次数构成一次失败的尝试。未超过临界值表示可以接受该地址的连通性；超过临界值则表示不可接受。可以将临界值设置为 1-200 之间的任意值，缺省值为 3。
- **Tracked IP Failure Weight** – 引发被跟踪 IP 地址响应失败的权重，用于计算被跟踪 IP 对象的故障权重。通过在被跟踪 IP 地址上应用权重，可以调整该地址连通性相对于其它被跟踪 IP 地址的重要程度。可以将较大的权重分配给相对重要的地址，将较小的权重分配给相对次要的地址。当达到跟踪的 IP 故障临界值时，所分配的权重开始起作用。例如，与权重为 1 的被跟踪 IP 地址的故障相比，超过权重为 10 的被跟踪 IP 地址的故障临界值占被跟踪 IP 对象的权重更大。可以在 1 到 255 之间分配权重，缺省值为 1。

还需要为被跟踪 IP 对象配置故障临界值，用于计算设备或 VSD 的故障切换临界值。如果一个或多个被跟踪 IP 地址超过其故障临界值，系统会对每个失败地址的权重求和。如果求和结果达到或超过被跟踪 IP 对象的故障临界值，被跟踪 IP 对象的故障权重即会计入设备或 VSD 的故障切换临界值。注意，只用被跟踪 IP 对象的故障权重计算设备或 VSD 的故障切换临界值，永远不会用单个被跟踪 IP 地址的故障权重计算设备或 VSD 的故障切换临界值。考虑以下示例：

被跟踪 IP 地址	故障权重			
10.10.10.250	100	被跟踪 IP 对象故障临界值	被跟踪 IP 对象故障权重	设备故障切换临界值
1.1.1.30	75	125	255	255
2.2.2.40	75			

如果被跟踪 IP 地址 10.10.10.250 失败，则会将被跟踪 IP 地址的故障权重 (100) 与被跟踪 IP 对象的故障临界值 (125) 加以比较。由于被跟踪 IP 地址的故障权重小于被跟踪 IP 对象的故障临界值，因此不认为被跟踪 IP 对象失败。如果被跟踪 IP 地址 1.1.1.30 和 2.2.2.40 均失败，则将相加后的故障权重 (150) 与被跟踪 IP 对象的故障临界值 (125) 加以比较。由于相加后的故障权重超过被跟踪 IP 对象的故障权重，因此认为被跟踪 IP 对象失败。随后，系统将被跟踪 IP 对象的故障权重 (255) 与设备的故障切换临界值 (255) 加以比较。由于被跟踪 IP 对象的故障权重等于设备的故障切换临界值，因此执行设备故障切换。

要将被跟踪 IP 地址 10.10.10.250 的故障权重设为 100，请输入以下内容：

WebUI

Network > NSRP > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.10.10.250

Weight: 100

CLI

```
set nsrp track-ip ip 10.10.10.250 weight 100
save
```

要将被跟踪 IP 对象的故障临界值设为 125，以判断可能发生的设备故障切换，请输入以下内容：

WebUI

Network > NSRP > Monitor > Track IP > VSD ID: Device Edit: 输入以下内容，然后单击 **Apply**:

Enable Track IP: (选择)

Failover Threshold: 125

CLI

```
set nsrp monitor track-ip threshold 125
save
```

范例：跟踪 IP 地址确定设备故障切换

两个 NetScreen 设备处于双主动配置。每隔 10 秒，对 Untrust 区段的冗余集群中运行 VRRP 的两个外部路由器，两个设备将向其物理 IP 地址[2] 发送 ARP 请求，对 Trust 区段中的两个 Web 服务器将发送 ping 请求。被跟踪 IP 对象的故障临界值为 51。被跟踪 IP 对象的权重和设备的故障切换临界值均为缺省值 (255)。被跟踪 IP 地址的权重和故障临界值如下：

- Untrust 区段中的冗余路由器
  - 210.1.1.250 – Weight: 16, threshold 5
  - 210.1.1.251 – Weight: 16, threshold 5
- Trust 区段中的 Web 服务器
  - 10.1.1.30 – Weight: 10, threshold 3
  - 10.1.1.40 – Weight: 10, threshold 3

向其中一个路由器发出 5 次连续尝试后，如果没有收到 ARP 响应，则认为尝试失败，并将其权重值 16 计入总故障切换临界值。向其中一个 Web 服务器发出 3 次连续尝试后，如果没有收到 ping 响应，则认为尝试失败，并将其权重值 10 计入总故障切换临界值。

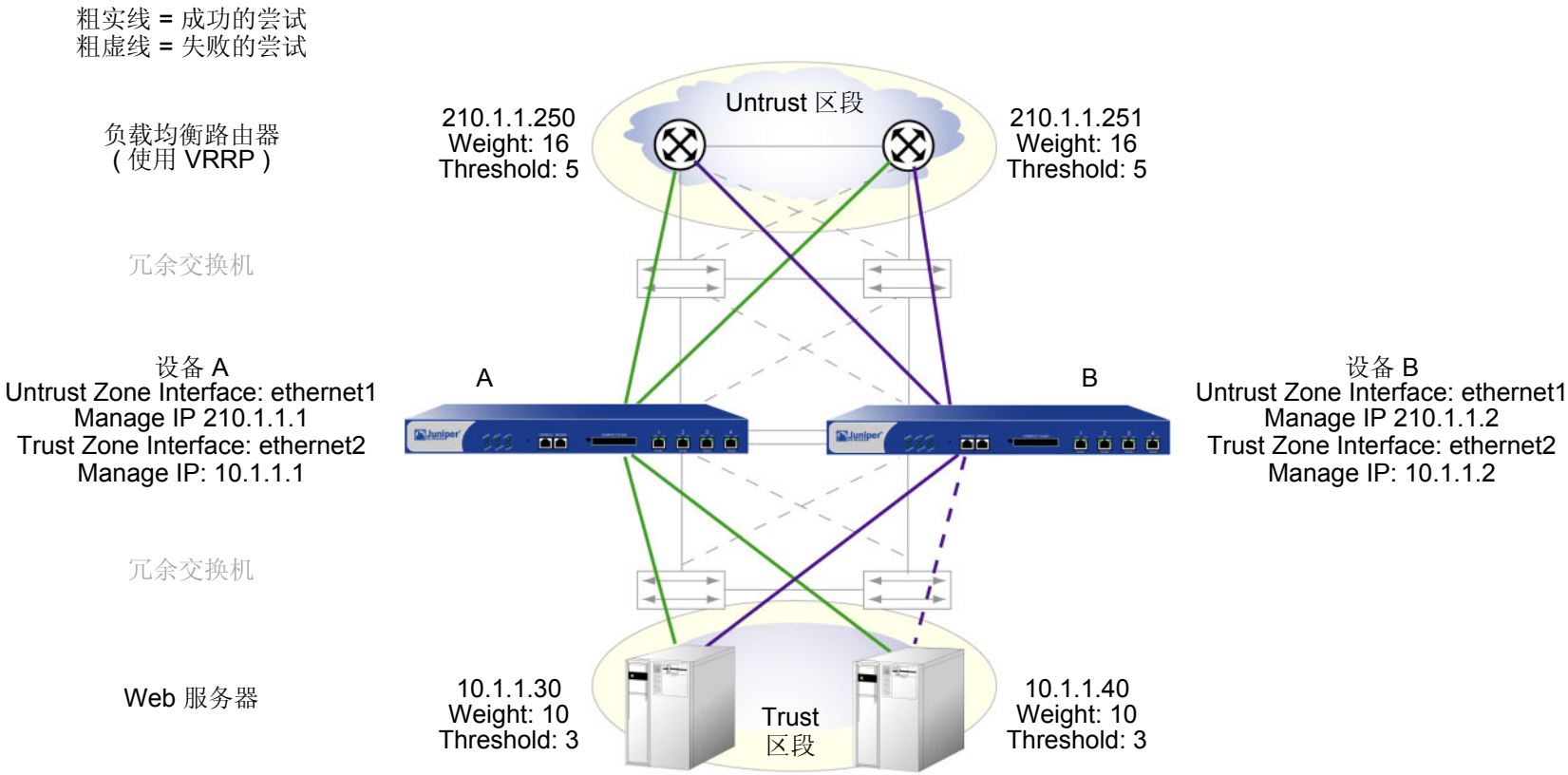
因为设备故障切换临界值为 51，所以发生设备切换前所有四个被跟踪 IP 地址必须都出现故障。如果不允许这样多的故障，您可以把临界值降低到一个更容易接受的级别。

在本例中，设备 A 的成功率为 100%，而设备 B 未能从 10.1.1.40 收到三个连续的响应，则将值 10 计入总故障临界值 51。

***注意：**所有 NSRP 监控设置只在本地设备上应用。IP 跟踪设置不会传播到 VSD 组中的其它设备。需要时，必须在该组的所有设备上输入相同的设置。*

在两个设备上， Untrust 区段接口为 ethernet1， Trust 区段接口为 ethernet2。在设备 A 上 ethernet1 的管理 IP 地址为 210.1.1.1，在设备 B 上为 210.1.1.2。在设备 A 上 ethernet2 的管理 IP 地址为 10.1.1.1，在设备 B 上为 10.1.1.2。所有的安全区段都在 trust-vr 路由选择域中。

2. 该物理 IP 地址为包含 VRRP 集群的物理路由器的专用地址。



WebUI

1. 跟踪 IP 地址

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 210.1.1.250

Method: ARP

Weight: 16

Interval (sec): 10

Threshold: 5

Interface: ethernet1

VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 210.1.1.251

Method: ARP

Weight: 16

Interval (sec): 10

Threshold: 5

Interface: ethernet1

VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.1.1.30

Method: Ping

Weight: 10

Interval (sec): 10

Threshold: 3

Interface: ethernet2

VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.1.1.40

Method: Ping

Weight: 10

Interval (sec): 10

Threshold: 3

Interface: ethernet2

VSD Group ID: Device

2. 跟踪 IP 对象故障临界值

Network > NSRP > Monitor > Track IP > Edit (对于 VSD: Device): 输入以下内容，然后单击 **Apply**:

Enable Track IP: (选择)

Failover Threshold: 51

CLI

1. 跟踪 IP 地址

```
set nsrp track-ip ip 210.1.1.250 interface ethernet1
set nsrp track-ip ip 210.1.1.250 interval 10
set nsrp track-ip ip 210.1.1.250 method arp
set nsrp track-ip ip 210.1.1.250 threshold 5
set nsrp track-ip ip 210.1.1.250 weight 16
set nsrp track-ip ip 210.1.1.251 interface ethernet1
set nsrp track-ip ip 210.1.1.251 interval 10
set nsrp track-ip ip 210.1.1.251 method arp
set nsrp track-ip ip 210.1.1.251 threshold 5
set nsrp track-ip ip 210.1.1.251 weight 16
set nsrp track-ip ip 10.1.1.30 interface ethernet2
set nsrp track-ip ip 10.1.1.30 interval 10
```

```
set nsrp track-ip ip 10.1.1.30 method ping[3]
set nsrp track-ip ip 10.1.1.30 threshold 3
set nsrp track-ip ip 10.1.1.30 weight 10
set nsrp track-ip ip 10.1.1.40 interface ethernet2
set nsrp track-ip ip 10.1.1.40 interval 10
set nsrp track-ip ip 10.1.1.40 method ping
set nsrp track-ip ip 10.1.1.40 threshold 3
set nsrp track-ip ip 10.1.1.40 weight 10
set nsrp track-ip
```

2. 跟踪 IP 对象故障临界值

```
set nsrp track-ip threshold 51
save
```

3. 在缺省情况下，IP 跟踪的方法是 ping 而被跟踪 IP 故障临界值为 3；所以，不需要指定它们。使用命令 **set nsrp track-ip ip 10.1.1.30** 和 **set nsrp track-ip ip 10.1.1.40** 就够了。

虚拟系统故障切换

虚拟系统要实现故障切换就必须位于 VSD 组中。要使 VSD 组支持虚拟系统，必须为每个虚拟系统创建 VSI。虚拟系统有自己的 Trust 区段 VSI，也可以拥有自己的 Untrust 区段 VSI。虚拟系统还可以与根级共享 Untrust 区段 VSI。当虚拟系统具有自己的 Untrust 区段 VSI 时，它们必须彼此在不同的子网中，它们与根级的 Untrust 区段 VSI 也应该在不同的子网中。所有 Trust 区段虚拟系统 VSI 也必须彼此在不同的子网中。

范例：虚拟系统间负载共享的 VSI

两台 NetScreen 设备 (设备 A 和设备 B) 处于双主动全网状配置中。您已经将设备 A 的根系统配置为 VSD 0 的主设备，设备 B 的根系统配置为 VSD 组 1 的主设备。根系统中的 VSD 0 和 1 的 Trust 和 Untrust 区段 VSI 如下所示：

VSD Group 0 的 VSI		VSD Group 1 的 VSI	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

(有关根系统 VSD 组的完全配置，请参阅第 50 页上的 “范例：双主动配置的 NSRP”。)

在本例中，为 NSRP 配置了两个虚拟系统 (vsys1 和 vsys2)。为向虚拟系统提供内向信息流的负载共享[4]，请对 VSD 成员关系进行如下分配：

- Vsys1 是 VSD 组 0 的成员。
- Vsys2 是 VSD 组 1 的成员。

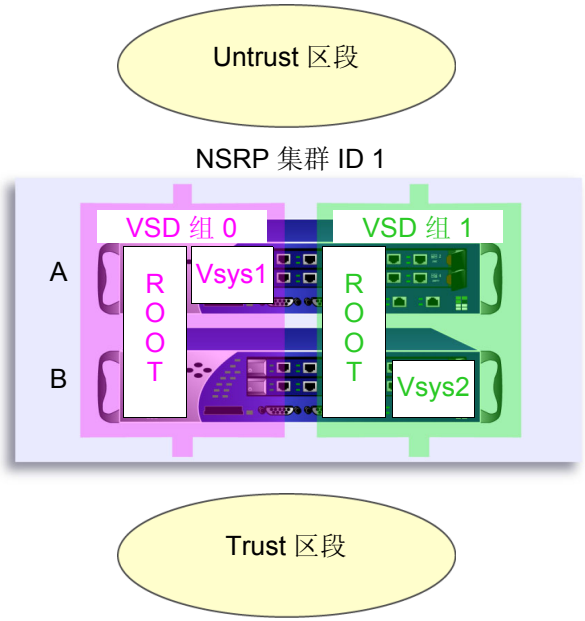
NetScreen 设备通过分配虚拟系统的 VSD 组来共享内向信息流负载。因为初始设计中将 vsys1 配置在设备 A 上，vsys2 配置在设备 B 上，所以向这些虚拟系统发送的内向流量被引导到含有它们的设备。

4. 请注意，在本例中，负载不是均匀分配的；即负载不均衡。两个 NetScreen 设备共享负载，设备 A 和 B 以动态变化的比例 (60/40%、70/30% 等等) 接收内向流量。

根系统在 VSD 组 0 和 1 中，且在两个 NetScreen 设备中是活动的。

Vsys1 在 VSD 组 0 中，且仅在设备 A 中是活动的。

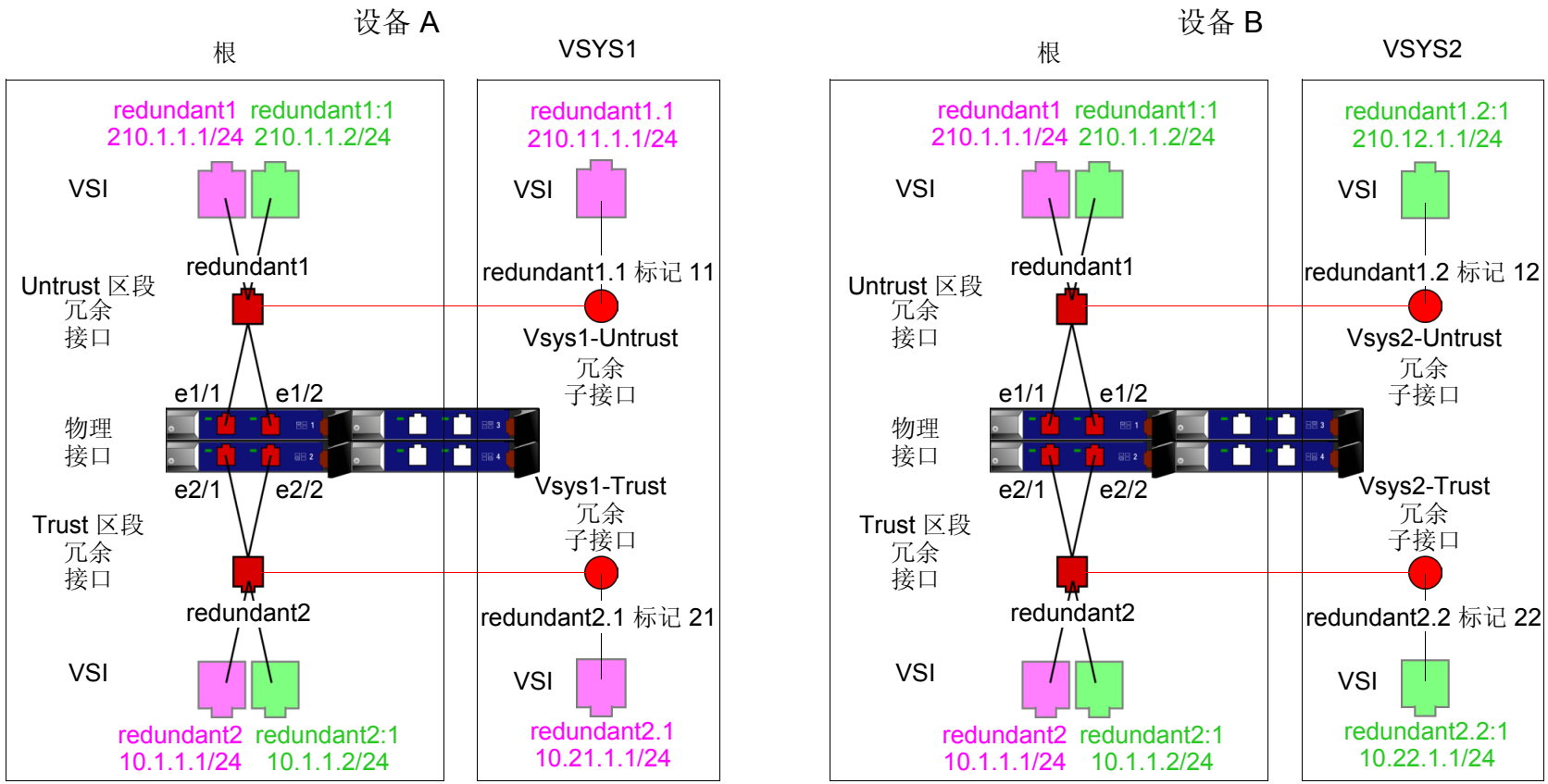
Vsys2 在 VSD 组 1 中，且仅在设备 B 中是活动的。



出站流量的缺省网关对于根系统和每个虚拟系统是不同的：

- 根：210.1.1.250
- Vsys1: 210.11.1.250
- Vsys2: 210.12.1.250

因为本例基于第 50 页上的 “范例：双主动配置的 NSRP”，其中建立了 VSD 组 0 和 1，同时设置了 NSRP 集群 ID 1 中的设备，并已启用 NSRP。所以，在设备 A 上配置的设置会自动传播给设备 B。



VSD 组 0 = 紫色 (注意 : VSD 0 的 VSI 不显示它们的 VSD ID 号。)
VSD 组 1 = 绿色 (注意 : VSD 1 的 VSI 用冒号 +1 表示它们的 VSD ID。)

WebUI

1. 设备 A: 根

注意 : *根系统的 NSRP 配置与第 50 页上的 “范例 : 双主动配置的 NSRP” 中的配置相同。*

2. 设备 A: Vsys1

Vsys > New: 输入以下内容，然后单击 **OK**:

VSYS Name: vsys1[5]

Vsys > 输入 (vsys1) > Network > Interface > New Sub-IF: 输入以下内容，然后单击 **OK**:

Interface Name: Redundant1.1

Zone Name: Untrust

VLAN Tag: 11

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

VSI Base: Redundant1.1

VSD Group: 0

IP Address / Netmask: 210.11.1.1/24

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

Interface Name: Redundant2.1

Zone Name: Trust-vsys-vsys1

VLAN Tag: 21

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

VSD Group ID: 0

IP Address / Netmask: 10.21.1.1/24

Interface Mode: Route[6]

5. 如果未定义 vsys admin， NetScreen 设备会自动创建一个，并在该 vsys 名称前加上 “vsys_”。在本例中， vsys1 的 vsys admin 为 vsys_vsys1。
6. 虚拟系统可以处于 “路由” 或 “NAT” 模式，而与您在根级设置的模式无关。

Network > Routing > Routing Entries > untrust-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: Redundant1

Gateway IP Address: 210.11.1.250

单击 **Exit Vsys** 以返回根级。

3. 设备 A: Vsys2

Vsys > New: 输入以下内容，然后单击 **OK**:

VSYS Name: vsys2

Vsys > 输入 (vsys2) > Network > Interface > New Sub-IF: 输入以下内容，然后单击 **OK**:

Interface Name: Redundant1.2

Zone Name: Untrust

VLAN Tag: 12

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

VSI Base: Redundant1.2

VSD Group: 1

IP Address / Netmask: 210.12.1.1

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

Interface Name: Redundant2.2

Zone Name: Trust-vsys-vsys2

VLAN Tag: 22

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

VSD Group ID: 1

IP Address / Netmask: 10.22.1.1/24

Interface Mode: Route

Network > Routing > Routing Entries > untrust-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: Redundant1

Gateway IP Address: 210.12.1.250

单击 **Exit Vsys** 以返回根级。

4. 设备 B

注意：*因为设备 A 会将其它配置的设置传播给设备 B，所有就不必在设备 B 中再次输入它们。*

CLI

1. 设备 A: 根

注意：*根系统的 NSRP 配置与*第 50 页上的 “范例 : 双主动配置的 NSRP”*中的配置是一样的。*

2. 设备 A: VSYS 1

```
set vsys vsys1
ns(vsys1)-> set interface redundant1.1 tag 11 zone untrust
ns(vsys1)-> set interface redundant1.1 ip 210.11.1.1/24
ns(vsys1)-> set interface redundant2.1 tag 21 zone trust-vsys1
ns(vsys1)-> set interface redundant2.1 ip 10.21.1.1/24
```

```
ns(vsys1)-> set interface redundant2.1 route[7]
ns(vsys1)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.11.1.250
ns(vsys1)-> save
ns(vsys1)-> exit
```

3. 设备 A: VSYS 2

```
set vsys vsys2
ns(vsys2)-> set interface redundant1.2 tag 12 zone untrust
ns(vsys2)-> set interface redundant1.2:1 ip 210.12.1.1/24
ns(vsys2)-> set interface redundant2.2 tag 22 zone trust-vsys2
ns(vsys2)-> set interface redundant2.2:1 ip 10.22.1.1/24
ns(vsys2)-> set interface redundant2.2:1 route
ns(vsys2)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway
    210.12.1.250
ns(vsys2)-> save
ns(vsys2)-> exit
```

4. 设备 B

注意：*因为设备 A 会将其它配置的设置传播给设备 B，所有就不必在设备 B 中再次输入它们。*

7. 虚拟系统可以处于 “路由” 或 “NAT” 模式，而与您在根级设置的模式无关。

4

NSRP-Lite

“NetScreen 冗余协议”(NSRP) 是一种在选定的 NetScreen 设备上支持的、可提供高可用性 (HA) 服务的专有协议。NSRP-Lite 是标准 NSRP 的简化版，只有某些 OSI 模型中第 3 层运行有 ScreenOS 的 NetScreen 设备支持它 (即接口必须处于 “路由”或 NAT 模式)。与 NSRP 的完全版不同， NSRP-Lite 仅支持 “主动 / 被动”配置，并可通过以下特点与完全版 NSRP 进一步加以区分 :

- NSRP-Lite 可支持配置同步 (缺省情况下不支持)。
- NSRP-Lite 不支持同步执行对象 (RTO)。
- 在 NSRP-Lite 中，如果发生由主设备到备份设备的故障切换，则会中断所有现有用户会话和 VPN 连接 (因为没有 RTO 同步)，必须重新建立会话和连接。因此， Juniper Networks 建议您对 VPN 通道启用带有重定密钥选项的 VPN 监控，以便它们自动对自身进行重建。

本章将解释 NSRP-Lite 的各个组件并将介绍如何为 HA 使用 NSRP-Lite 配置 NetScreen 设备。所涵盖的具体主题如下 :

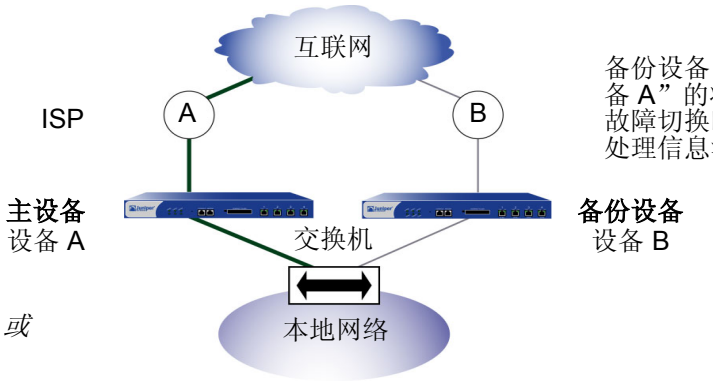
- 第 139 页上的 “NSRP-Lite 简介”
  - 第 140 页上的 “集群和 VSD 组”
  - 第 141 页上的 “缺省设置”
- 第 142 页上的 “集群”
  - 第 143 页上的 “集群名称”
  - 第 144 页上的 “认证和加密”
- 第 145 页上的 “VSD 组”
  - 第 145 页上的 “VSD 组成员状态”
  - 第 146 页上的 “心跳信号消息”
  - 第 147 页上的 “抢先选项”

- 第 148 页上的 “用电缆连接和配置 NSRP-Lite”
- 第 156 页上的 “配置和文件同步”
  - 第 156 页上的 “同步配置”
  - 第 157 页上的 “同步文件”
  - 第 158 页上的 “自动配置同步”
- 第 159 页上的 “路径监控”
  - 第 160 页上的 “设置临界值”
  - 第 160 页上的 “对被跟踪的 IP 地址加权”
  - 第 161 页上的 “VPN 通道故障切换的 IP 跟踪”

NSRP-Lite 简介

NSRP-Lite 在某些 NetScreen 设备上提供简单的高可用性 (HA) 解决方案。如果为 NSRP-Lite 用电缆连接和配置两台 NetScreen 设备，则一台充当主设备并积极处理网络信息流。另一台充当备份设备，被动等待以便在当前主设备无法执行其功能时成为主设备。通过将两台 NetScreen 设备连接到本地网络、为 NSRP-Lite 配置它们并且为每台设备使用不同的互联网服务提供商 (ISP)，可以避免本地网络出现设备故障和 ISP 故障。

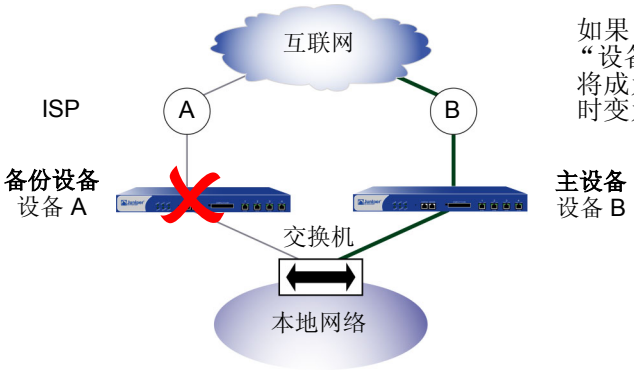
主设备 (“设备 A”) 积极处理穿越本地网络和互联网之间的防火墙的信息流。



备份设备 (“设备 B”) 接收来自 “设备 A” 的状态报告，并随时准备在发生故障切换时成为主设备。“设备 B” 不处理信息流。

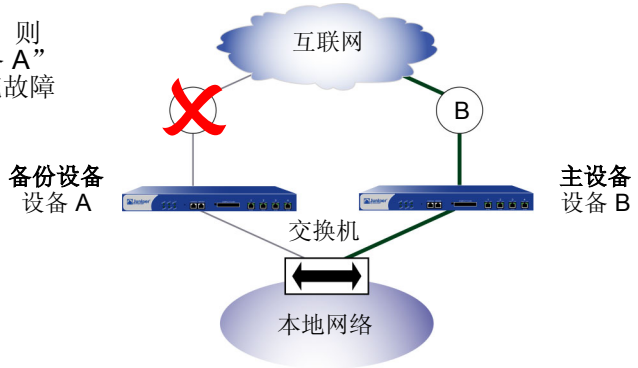
注意：NSRP-Lite 不支持 RTO 或会话同步。

设备 A 出现故障



如果 “设备 A” 或 ISP A 出现故障，则 “设备 B” 将成为主设备，而 “设备 A” 将成为备份设备 (或在出现内部系统故障时变为不可操作)。

ISP A 出现故障



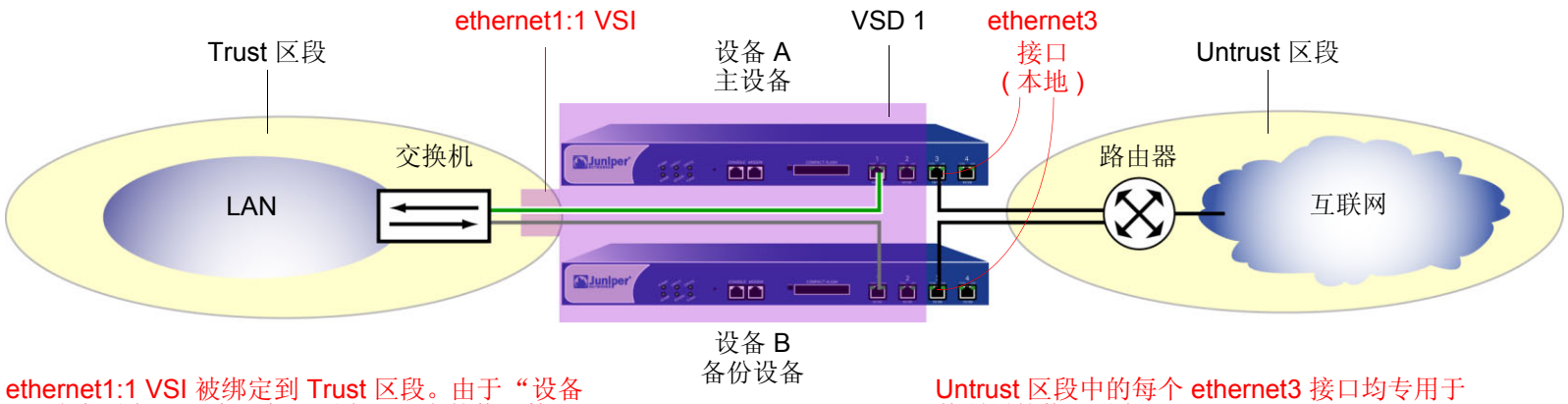
集群和 VSD 组

NSRP-Lite 集群由一对 NetScreen 设备组成，其中包括一台提供冗余网络连接的虚拟安全设备 (VSD)。一台物理设备充当 VSD 组的主设备，并处理全部发送到 VSD 的网络信息流。另一台设备充当主设备的备份设备，随时准备在当前主设备出现故障或性能降低时接手信息流的处理工作。

两台设备之间相互发送 VSD 心跳信号消息以提供状态报告。如果备份设备收到主设备遇到网络或系统故障并已更改其状态的消息，则备份设备将其状态更改为主设备并开始积极处理信息流。这一转变过程即构成故障切换。

在两台 NetScreen 设备能提供冗余服务前，必须通过指派介于 1 和 7 之间的集群 ID 来将这两台设备分组到同一 NSRP 集群中。当 NetScreen 设备成为集群的一个成员后，它将自动成为 VSD 组 0 的成员，且所有接口将成为 VSD 组 0 的虚拟安全接口 (VSI)。

VSI 绑定可以从一台物理设备切换到另一台设备，因为 VSD 组的主设备可进行切换并自称 VSI。要将 VSI (所有 VSD 成员可共享的虚拟接口) 恢复为其所属物理 NetScreen 设备专用的本地接口，必须取消设置 VSD 组 0。然后，可通过创建带有非零 ID 号 (如 VSD 1) 的 VSD 组以及将接口定义为该 VSD 的 VSI 来有选择性地创建本地接口 VSI。请参见下图 : Trust 区段中的 ethernet1:1 接口成为了 VSD 组 1 的 VSI，而 Untrust 区段中的 ethernet3 接口仍为本地接口。



缺省设置

基本 NSRP 配置使用以下缺省设置 :

- VSD 组信息
  - VSD group ID: 0
  - Device priority in the VSD group: 100
  - Preempt option: disabled
  - Preempt hold-down time: 0 seconds
  - Initial state hold-down time: 5 seconds
  - Heartbeat interval: 1000 milliseconds
  - Lost heartbeat threshold: 3
- NSRP 链接信息
  - Number of gratuitous ARPs: 4
  - NSRP encryption: disabled
  - NSRP authentication: disabled
  - Interfaces monitored: none
  - Secondary path: none

在 NSRP 集群中设置某个 NetScreen 设备时，该 NetScreen 设备将自动创建 “VSD 组 0”并将绑定到 Trust 区段的物理接口转换成 “VSD 组 0”的 “虚拟安全接口” (VSI)。

集群

NSRP 集群由一组实施相同的整体安全策略并且共享相同的配置设置的 NetScreen 设备组成。将 NetScreen 设备分配给 NSRP 集群时，对一个集群成员的配置所作的任何更改都将传播给其它成员[1]。同一 NSRP 集群成员的以下各项设置将保持相同：

- 策略和策略对象 (如地址、服务、 VPN、用户和时间表)
- 系统参数 (如认证服务器设置、 DNS、 SNMP、系统日志、 URL 阻塞、防火墙检测选项等等)

集群的成员不传播下列配置设置：

不传播的命令	
NSRP	• set/unset nsrp cluster id *number* • set/unset nsrp auth password *pswd_str* • set/unset nsrp encrypt password *pswd_str* • set/unset nsrp monitor interface *interface* • set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* } • set/unset nsrp rto-mirror …
Interface	• set/unset interface *interface* manage-ip *ip_addr* • set/unset interface *interface* phy … • set/unset interface *interface* bandwidth *number* • set/unset interface redundant *number* phy primary *interface* • 适用于本地接口的所有命令
Monitored Objects	• 所有 IP 跟踪、区段监控和接口监控命令
Console Settings	• 所有控制台命令 (set/unset console …)

1. 用户可以禁用配置和文件同步。有关信息，请参阅第 158 页上的 “自动配置同步”。

不传播的命令	
Hostname	• set/unset hostname *name_str*
SNMP	• set/unset snmp name *name_str*
Virtual Router	• set/unset vrouter *name_str* router-id *ip_addr*
Clear*	• 所有清除命令 (clear admin, clear dhcp, …)
Debug†	• 所有调试命令 (debug alarm, debug arp, …)

* 在缺省情况下，NSRP 集群成员不传播 **clear** 命令。要将一个 clear 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入命令中。例如 **clear cluster admin …**, **clear cluster dhcp …**

† 在缺省情况下，NSRP 集群成员不传播 **debug** 命令。要将一个 debug 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入 **debug** 命令中。例如 **debug cluster alarm …**, **debug cluster arp …**

集群名称

由于 NSRP 集群成员可以具有不同的主机名称，因此故障切换可破坏 SNMP 通信和数字证书的有效性，原因是 SNMP 通信和证书的正常工作依赖于设备的主机名称。

要为所有集群成员定义单个名称，请键入以下 CLI 命令：

```
set nsrp cluster name name_str
```

当为 NetScreen 设备配置 SNMP 主机名 (**set snmp name** *name_str*) 以及在 PKCS10 证书申请文件中定义通用名称时应使用集群名称。

通过为所有集群成员使用单个名称，可实现 SNMP 通信和数字证书在设备故障切换后继续使用而不中断。

认证和加密

由于 NSRP 通信的机密特性，可以通过加密和认证来确保所有 NSRP 信息流的安全。对于加密和认证， NSRP 分别支持 DES 和 MD5 算法。

***注意：**如果设备相互间是用电缆直接连接在一起的，则无需使用认证和加密。但是，如果设备相互间是通过交换机用电缆连接在一起的，则可能需要考虑执行这些额外的安全措施。*

要启用认证或加密，必须提供集群中每台设备的密码。

WebUI

Network > NSRP > Cluster: 输入以下内容，然后单击 **Apply**:

NSRP Authentication Password: (选择), *pswd_str*

NSRP Encryption Password: (选择), *pswd_str*

CLI

```
set nsrp auth password pswd_str
set nsrp encrypt password pswd_str
```

VSD 组

“虚拟安全设备”(VSD) 组是一对物理 NetScreen 设备，它们共同组成单个 VSD。一个物理设备充当 VSD 组的主设备。 VSD 的 “虚拟安全接口” (VSI) 被绑定到主设备的 Trust 区段物理接口上。另一个物理设备充当备份设备[2]。如果主设备出现故障，则 VSD 故障切换到备份设备，并且 VSI 绑定转移到备份设备的物理接口，该备份设备立即晋升为主设备[3]。

VSD 组成员状态

VSD 组的成员可以是以下六种状态之一：

- Master (主设备) – 处理发送到 VSI 的信息流的 VSD 组成员的状态。
- Primary Backup (主备份设备) – 当前主设备让位后将变成主设备的 VSD 组成员的状态。选择过程使用设备优先级来确定要晋升的成员。
- Backup (备份设备) – 监控主备份设备的状态并在当前主备份设备让位时将其中的一个备份设备选择为主备份设备的 VSD 组成员的状态。
- Initial (初始) – 启动设备或通过 **set nsrp vsd-group id** *id_num* 命令添加设备时， VSD 组成员加入 VSD 时的瞬间状态。

  使用 **set nsrp vsd-group init-hold** *number* 命令，可指定 VSD 组成员在初始状态中停留的时间。缺省 (最小) 设置为 5。要确定初始状态等待时间，将暂停初始化值乘以 VSD 心跳信号间隔 (暂停初始化 x 心跳信号间隔 = 初始状态等待时间)。例如，如果暂停初始化值为 5，心跳信号间隔为 1000 毫秒，则初始状态等待时间为 15,000 毫秒，或为 5 秒 (5 x 1000 = 5000)。

> ***注意：****如果减少 VSD 心跳信号间隔，则应增加暂停初始化值。有关配置心跳信号间隔的信息，请参阅**第 146 页上的 “心跳信号消息”**。*

2. 在当前版本中，一个 VSD 组可以有两个成员。在以后的版本中，可以有两个以上的成员。在这种情况下，一台设备充当主设备，另一台设备充当主备份设备，而其余的 VSD 组成员充当备份设备。
3. 如果使用了 BGP 且 Trust 和 Untrust 区段均处于同一虚拟路由选择域中，则 NetScreen 设备将通告与主设备 (主动) 和备份设备 (被动) VSD 组成员的 Trust 区段 VSI 相连接的子网。

- Ineligible (无资格) – 管理员有意指派一个 VSD 组成员，使其不能参与选择过程的状态。要做到这一点，请使用 **set nsrp vsd-group id** *id_num* **mode ineligible** 命令。
- Inoperable (不可操作) – 系统检查确定设备有内部问题 (如没有处理板) 或网络连接问题 (如接口链接失败) 后 VSD 组成员的状态。

> ***注意 :*** *设备从无资格状态 (使用* ***exec nsrp vsd-group id*** *id_num* ***mode { backup | init | master | pb }*** *命令) 或不可操作状态 (系统或网络问题已修正) 返回时，必须首先通过初始状态。*

心跳信号消息

心跳信号消息不断通告发送方成员的状态、其系统的使用状况以及网络的连通性。每个 VSD 组成员 (即使它处于初始、无资格或不可操作状态) 都可通过每隔一秒发送心跳信号消息与它的组成员进行通信。这些消息使每个成员知道其它每个成员当前的状态。心跳信号消息包括下列信息 :

- 设备的设备 ID
- VSD 组 ID
- VSD 组成员状态
- 设备优先级

可以对发送 VSD 心跳信号的间隔进行配置 (200、600、800 或 1000 毫秒，缺省值为 1000 毫秒)。可普遍应用到所有 VSD 组成员的 CLI 命令为 **set nsrp vsd-group hb-interval** *number*。也可配置失去心跳信号临界值，用于确定认为 VSD 组成员丢失的时间。可普遍应用到所有 VSD 组成员的 CLI 命令为 **set nsrp vsd hb-threshold** *number*。失去心跳信号临界值的最小值为 3。

抢先选项

通过将要成为主设备的设备设置为抢先模式，可以确定更好的优先级号 (接近零) 是否能发起故障切换。如果在该设备上启用抢先选项，则在当前主设备的优先级较低 (远离零) 时，该设备将变成 VSD 组的主设备。如果禁用此选项，则优先级比备份设备低的主设备可保持其位置 (除非某些其它因素，如内部问题或错误的网络连接方式，导致故障切换)。

要更改设备的优先级 (默认值为 100) 并启用或禁用抢先选项，请使用以下 CLI 命令 :

```
set nsrp vsd-group id number priority number
unset nsrp vsd-group id number priority[4]
set/unset nsrp vsd-group id number preempt
```

使用等待时间延迟故障切换，可防止在邻接的交换机端口忽隐忽现时快速故障切换造成的混乱，也可确保在新的主设备可用前，周围的网络设备有足够的时间协商新的链接。可以使用以下 CLI 命令将等待时间 (用于延迟抢先故障切换) 设置为介于 0 和 600 秒之间的任何时间长度 :

```
set nsrp vsd-group id number preempt hold-down number
```

4. 此命令可以将优先级恢复为默认值 100。

用电缆连接和配置 NSRP-LITE

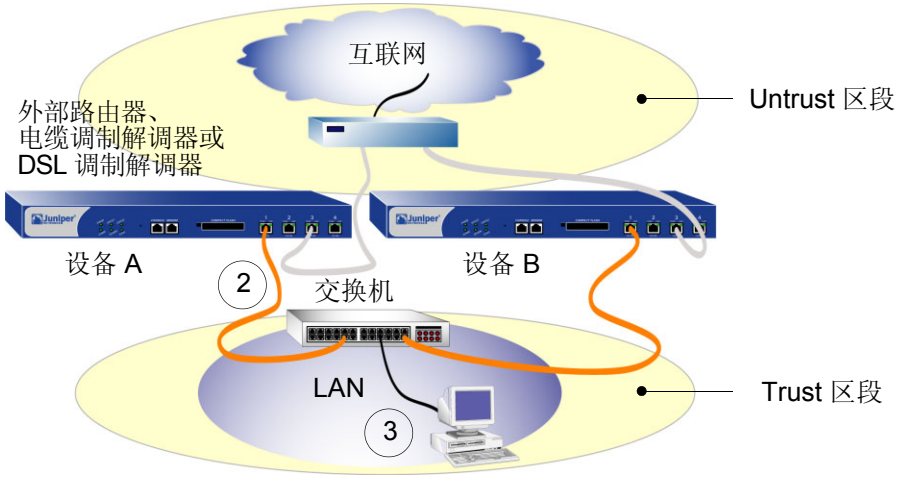
要设置两台 NetScreen 设备使其具有高可用性，必须用电缆将它们连接到网络并为 NSRP-Lite 配置它们。

使用一条 RJ-45 以太网电缆将两台 NetScreen 设备上的 Untrust 区段连接到外部路由器。使用另一条 RJ-45 以太网电缆将一个 Trust 区段端口连接到局域网 (LAN) 上的内部交换机。因为用于 NSRP 通信的心跳信号消息是一种专有协议，所以这些消息不能在 OSI 模型的第 3 层中进行发送。因此，只能使用第 2 层交换机或集线器连接 Trust 区段中的设备。

1. 将每台 NetScreen 设备上的 Untrust 区段端口用电缆连接到外部路由器。

2. 将每台 NetScreen 设备上的 Trust 区段端口连接到内部交换机。

3. 将内部 LAN 上的其它主机连接到交换机。



范例：配置 NSRP-Lite

在本例中，将使用 NSRP-Lite 配置两台 NetScreen 设备的高可用性。接口的 IP 地址如下：

- NetScreen-A
  - ethernet3 – Untrust 区段接口， 1.1.1.1/24，管理 IP: 1.1.1.2

    这是一个本地接口而不是 VSI。
  - ethernet1:1 – Trust 区段接口， 10.1.1.1/24， NAT 模式

    这是 VSD 组 1 的 VSI。
  - ethernet4 – HA 区段接口

    该接口用于两台设备之间的 HA 通信的控制链接。在 ethernet4 出现故障时，用户还将 ethernet1 设置为 VSD 心跳信号的二级路径接口。 (有关 VSD 心跳信号的详细信息，请参阅第 26 页上的 “心跳信号消息”。)
- NetScreen-B
  - ethernet3 – Untrust 区段接口， 1.1.2.1/24，管理 IP: 1.1.2.2

    这是一个本地接口而不是 VSI。
  - ethernet1 – Trust 区段接口， 10.1.1.1/24， NAT 模式

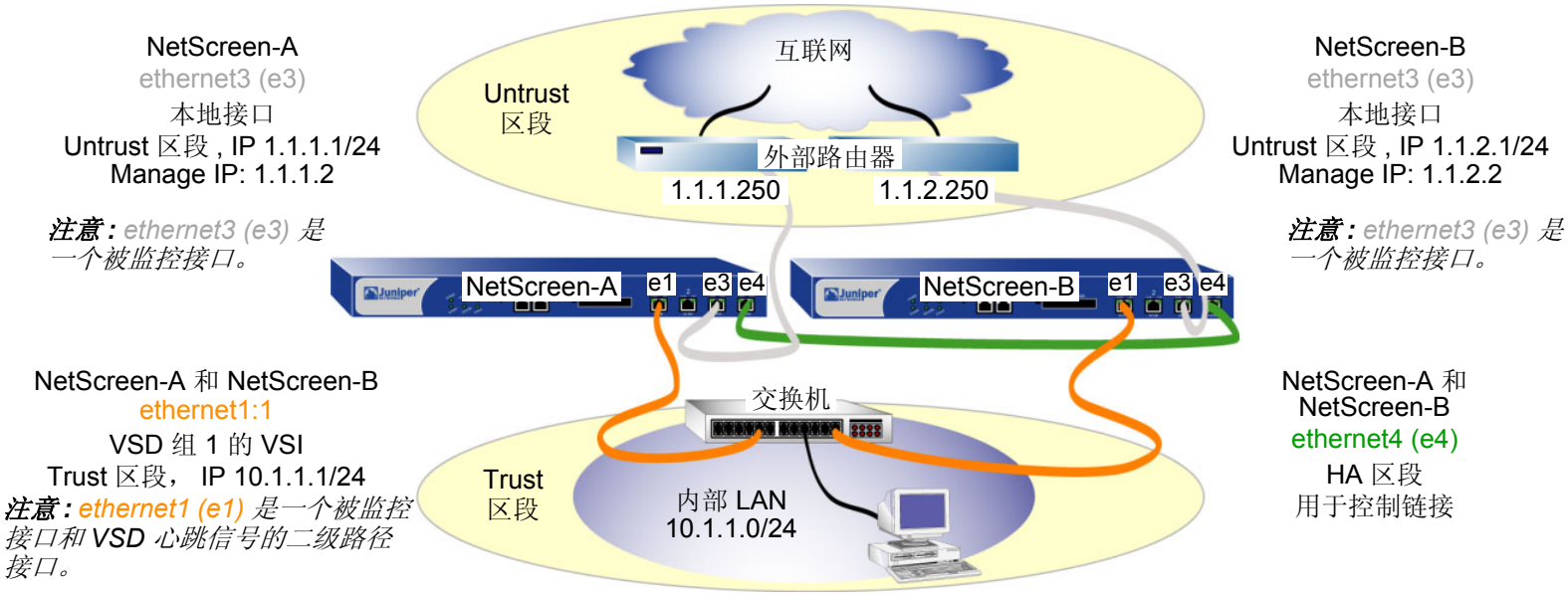
    这是 VSD 组 1 的 VSI。
  - ethernet4 – HA 区段接口

    该接口用于两台设备之间的 HA 通信的控制链接。在 ethernet4 出现故障时，用户还将 ethernet1 设置为 VSD 心跳信号的二级路径接口。

您希望将 NetScreen-A 充当 VSD 组 1 的主设备，因此将其优先级设置为 1 而将 NetScreen-B 的优先级保留其默认值 100 不变。将对 NetScreen-A 的抢先等待时间进行设置以便在 10 秒后其成为主设备。

将设置两台设备以监控接口 ethernet1 和 ethernet3，并为每台设备分配权重 255 (缺省值)。如果任何一个接口出现故障，都将发生设备级故障切换。

将为每个 Untrust 区段接口定义两个缺省路由。对于 NetScreen-A 上的 ethernet3，缺省路由指向 IP 地址为 1.1.1.250 的外部路由器。对于 NetScreen-B 上的 ethernet3，缺省路由指向 IP 地址为 1.1.2.250 的外部路由器。所有安全区段都在 trust-vr 路由选择域中。



WebUI (NetScreen-A)

1. 接口 (NetScreen-A)

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

Zone Name: Trust

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

Zone Name: Untrust

Static IP: (选择)

IP Address/Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

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

Zone Name: HA

2. NSRP (NetScreen-A)

Network > NSRP > Cluster: 输入以下内容，然后单击 **Apply**:

Cluster ID: (选择), 1

Network > NSRP > VSD Group: 单击 VSD group 0 的 **Remove**。当提示确认删除时，请单击 **OK**。

Network > NSRP > VSD Group > New: 输入以下内容，然后单击 **OK**:

Group ID: 1

Priority: 1

Enable Preempt: (选择)

Preempt Hold-Down Time (sec): 10

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

Interface Name:

VSI Base: ethernet1

VSD Group: 1

IP Address / Netmask: 10.1.1.1/24

Network > NSRP > Link: 从 Secondary Link 下拉列表中选择 **ethernet1**，然后单击 **Apply**。

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 输入以下内容，然后单击 **Apply**:

ethernet1: (选择), Weight: 255

ethernet3: (选择), Weight: 255

3. 路由 (NetScreen-A)

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

WebUI (NetScreen-B)

4. 接口 (NetScreen-B)

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

Zone Name: Untrust

Static IP: (选择)

IP Address/Netmask: 1.1.2.1/24

Manage IP: 1.1.2.2

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

Zone Name: HA

5. NSRP (NetScreen-B)

Network > NSRP > Cluster: 输入以下内容，然后单击 **Apply**:

Cluster ID: (选择), 1

Network > NSRP > VSD Group: 单击 VSD group 0 的 **Remove**。当提示确认删除时，请单击 **OK**。

Network > NSRP > VSD Group > New: 输入以下内容，然后单击 **OK**:

Group ID: 1

Priority: 100

Enable Preempt: (清除)

Preempt Hold-Down Time (sec): 0

***注意：**本版发行时，必须使用以下 CLI 命令将 NetScreen-A 与 NetScreen-B 的配置同步：**exec nsrp sync global-config save**。然后使用 **reset** 命令重置设备。*

Network > NSRP > Link: 从 Secondary Link 下拉列表中选择 **ethernet1**，然后单击 **Apply**。

Network > NSRP > Monitor > Interface > VSD ID: Device Edit Interface: 输入以下内容，然后单击 **Apply**:

ethernet1: (选择), Weight: 255

ethernet3: (选择), Weight: 255

6. 路由 (NetScreen-B)

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.2.250

CLI (NetScreen-A)

1. 接口 (NetScreen-A)

```
set interface ethernet1 zone trust
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface ethernet3 manage-ip 1.1.1.2
set interface ethernet4 zone ha
```

2. NSRP (NetScreen-A)

```
set nsrp cluster id 1
unset nsrp vsd-group id 0
set nsrp vsd-group id 1
set nsrp vsd-group id 1 priority 1
set nsrp vsd-group id 1 preempt hold-down 10
set nsrp vsd-group id 1 preempt
set interface ethernet1:1 ip 10.1.1.1/24
set nsrp secondary-path ethernet1
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
```

3. 路由 (NetScreen-A)

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

CLI (NetScreen-B)

4. 接口 (NetScreen-B)

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.2.1/24
set interface ethernet3 manage-ip 1.1.2.2
set interface ethernet4 zone ha
```

5. NSRP (NetScreen-B)

```
set nsrp cluster id 1
unset nsrp vsd-group id 0
set nsrp vsd-group id 1
save
exec nsrp sync global-config save
reset
```

出现以下提示：“Configuration modified, save?[y] / n”

按 **N** 键。

出现以下提示：“System reset, are you sure? y / [n]”

按 **Y** 键。

系统重新启动。

```
set nsrp secondary-path ethernet1
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet3
```

6. 路由 (NetScreen-B)

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.2.250
save
```

配置和文件同步

将新设备添加到活动 NSRP 集群中时，可以使 VSD 组主设备的配置和文件 (如 PKI 公开 / 私有密钥文件) 与新设备的配置和文件同步。在缺省情况下，在 NSRP-Lite 中，当两台设备第一次进入集群、开始 NSRP 通信并在 VSD 组 0 中建立主设备和备份设备角色时这两台设备不同步配置和文件。可以手动同步配置和文件，也可更改缺省行为以启用自动配置同步。

同步配置

在缺省情况下，在 NSRP-Lite 中将禁用自动配置同步。可通过输入 CLI 命令 **set nsrp config sync** 更改此行为。不过，即使启用了自动配置同步，配置设置仍可变得不同步。例如，假如当集群中的某台设备重新启动时，在另一台设备上进行了任何配置更改 (或者 NSRP 通信所使用的任一接口出现了故障)，配置设置可变得不同步。要了解某台设备的配置与另一台设备的配置是否同步，请使用 **exec nsrp sync global-config check-sum** 命令。输出结果将指出两台设备的配置是同步还是不同步，并可提供本地和远程设备的校验和。

如果配置不同步，请使用以下命令使其同步 : **exec nsrp sync global-config save**。在同步配置前，如果没有在本地设备上使用 **unset all** 命令，则本地设备将远程设备的设置附加到现有设置上。但是，在同步配置后，每个复制的设置都将生成一条错误消息。要避免在同步配置时生成错误消息，可执行以下操作 :

1. 将本地和远程配置下载到工作站。
2. 使用应用程序 (如 WinDiff) 识别文件间的差异。
3. 在本地设备上手动输入在远程设备上添加、修改或删除的设置。

注意 : *由于 NetScreen 设备使用 “NetScreen 可靠传输协议” (NRTP)，它与 TCP 非常类似 (只是更轻量)，因此集群中活动设备上的配置很少会变得不同步。*

同步文件

如果需要同步某个特定文件 (如本地证书)，请在要将文件同步到的设备上输入以下命令 : **exec nsrp sync file name** *name_str* **from peer**。如果要同步所有文件，请输入 **exec nsrp sync file from peer**。

范例 : 将设备添加到活动的 NSRP 集群

在本例中，将之前充当单一安全设备的设备 A 添加到 NSRP 集群中的 VSD 组 0 中，该集群的 ID 为 1，名称为“cluster1”。将取消设置设备 A 上以前的配置、对其进行重启，然后同步来自主设备 VSD 组 0 的配置和文件。然后将设备 A 指派为 VSD 组 0 的主设备。

WebUI

> ***注意 :*** *只能通过 CLI 来使用配置同步功能。*

CLI

设备 A

`unset all`[5]

出现以下提示 :“Erase all system config, are you sure y / [n]?”

按 **Y** 键。

系统配置将恢复为出厂缺省设置。

`reset`

系统重新启动。

5. 如果不首先使用 **unset all** 命令，则 **exec nsrp sync global-config** 命令可将新的配置设置附加到现有的设置上。(注意 : NetScreen 设备会为每个实现同步的复制设置生成一条错误消息。)

```
set nsrp cluster id 1
set nsrp cluster name cluster1
exec nsrp sync file
exec nsrp sync global-config
exec nsrp vsd-group id 0 mode master
save
```

自动配置同步

在缺省情况下， NSRP 集群中的设备不同步配置和文件。此设置十分有用，例如，当要通过 NetScreen-Security Manager 来进行所有配置更改时。

可通过 CLI 命令 **set nsrp config sync**[6] 来启用自动配置同步。请在集群中的所有成员上输入此命令。

启用自动配置同步前， Juniper Networks 建议您先手动在集群成员间同步文件 (如 PKI 对象)。可使用 **exec nsrp sync file from peer** 命令同步文件。如果同步了配置，但某个集群成员却丢失了配置中引用的某个文件，则该配置对于该成员来说将变为无效。为避免此情况的发生，请先同步文件，然后再同步配置。

6. WebUI 不支持此选项。

路径监控

路径监控将检查 NetScreen 接口和其它设备接口之间的第 2 层和第 3 层网络连接。冗余组中的设备可通过路径监控来确定设备的网络连接是否可以接受。如果连接不可接受且超出了已定义的临界值，则会发生 VSD 组级或设备级故障切换。有关上述两种故障切换级别的不同之处，请参阅第 115 页上的 “故障切换”。

第 2 层路径监控可检查物理端口是否处于活动状态以及是否与其它网络设备相连。可基于每个接口或每个区段对接口进行监控。每个接口：

- WebUI: 单击 **Network > NSRP > Monitor > Interface > VSD ID:** { **Device** | *number* } **Edit Interface**，然后选择希望 NetScreen 设备监控的接口。
- CLI: **set nsrp** [**vsd-group id** *number*] **monitor interface** *interface*

每个区段 (即 NetScreen 设备监控绑定到选定区段的所有接口):

- WebUI: 单击 **Network > NSRP > Monitor > Zone > VSD ID:** { **Device** | *number* } **Edit Zone**，然后选择希望 NetScreen 设备监控的区段。
- CLI: **set nsrp** [**vsd-group id** *number*] **monitor zone** *zone*

第 3 层路径监控，或 IP 跟踪的功能是向最多 16 个指定的 IP 地址以用户确定的间隔发送 ping 或 ARP 要求，然后监控目标是否响应。如果一个主设备 (不是其备份设备) 的跟踪 IP 总故障数超过设备的故障切换临界值，则备份设备将自动晋升为主设备，而让位的主设备将进入不可操作状态。(不可操作的 VSD 组成员将继续进行 IP 路径跟踪。当该结果不再超过故障切换临界值后，它会从不可操作状态转变为初始状态，然后再变为备份设备状态[7]。)

注意：*当使用 “虚拟路由器冗余协议” (VRRP) 将路由器分组到冗余集群中时，如果该路由器不是虚拟 IP 地址的所有者 (故障切换后可能会出现此情况)，则作为主设备的路由器不会对该 IP 地址的 ping 请求做出响应。但是，主设备虚拟路由器一定会响应虚拟 MAC 地址的 ARP 请求，无论它是否是该 IP 地址的所有者。(有关详细信息，请参阅 RFC 2338。) 要在 IP 跟踪时使用 ARP，则轮询设备必须与 NetScreen 管理 IP 地址处于同一物理子网中。*

在跟踪 IP 地址时，可以从发送来自接口上管理 IP 地址的 ping 或 ARP 请求。对于 VSI，管理 IP 地址必须不同于接口 IP 地址，并且对于每台设备都必须是唯一的。对于本地接口，管理 IP 地址可以和接口 IP 地址相同，也可以不相同。

7. 如果 VSD 组处于抢先模式且该设备的优先级高于当前主设备的优先级，则它会从不可操作状态转变为初始状态然后再变为主设备状态。

设置临界值

IP 路径跟踪涉及到两种临界值: 跟踪的 IP 故障临界值和设备故障切换临界值。

Tracked IP Failure Threshold – 引发特定 IP 地址发出 ping 或 ARP 响应的连续失败 (从而认为尝试失败) 次数。没有超过临界值表示该地址的连通性是可接受的；超过了临界值就表示不可接受。您可以为每个 IP 地址设置此临界值，它可以是 1 到 200 之间的任何值。缺省值是 3。

Device Failover Threshold – 导致 VSD 组主设备让位的累积失败尝试的总权重值。 (有关如何为被跟踪 IP 地址分配权重的信息，请参阅下一节，第 160 页上的 “对被跟踪的 IP 地址加权”。) 您可以将设备故障切换临界值设置为介于 1 和 255 之间的任何值。缺省值是 255。

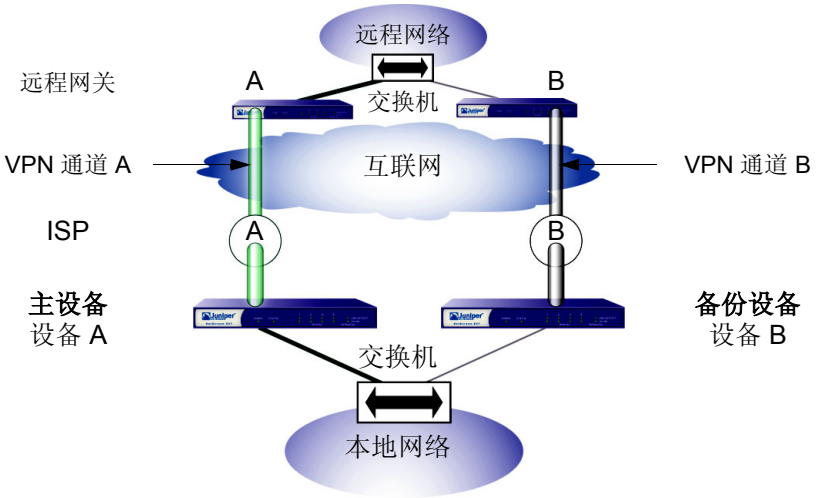
对被跟踪的 IP 地址加权

通过在被跟踪的 IP 地址上应用加权，或加权值，可以调整该地址连通性的重要性 (与其它被跟踪的地址相比)。您可以给相对较重要的地址分配相对较大的权重，而给相对不重要的地址分配相对较小的权重。当达到跟踪的 IP 故障临界值时，所分配的权重开始起作用。例如，超过权重为 10 的地址的 “跟踪的 IP 故障临界值”与超过权重为 1 的地址的 “跟踪的 IP 故障临界值”相比，前者更容易使主设备发生故障切换。可将权重的大小指配为介于 1 和 255 之间的数。缺省值为 255。

VPN 通道故障切换的 IP 跟踪

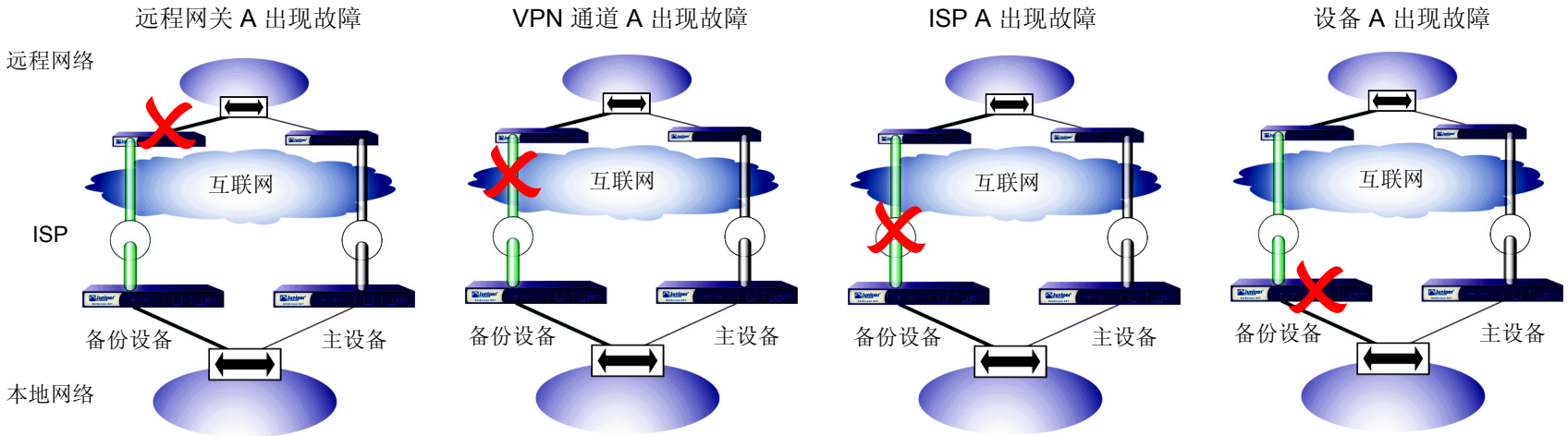
通过在每台设备上配置一个 VPN 通道以通过两个不同的远程 VPN 网关到达相同的远程网络，然后通过通道跟踪远程站点的 IP 地址，可以防止 VPN 信息流出现本地和远程网关设备故障、通道故障和 ISP 故障。

主设备（“设备 A”）积极通过 VPN 通道 A 处理本地和远程网络之间的 VPN 信息流。“设备 A”监控其系统的运行情况、网络连接和 VPN 通道 A。



备份设备（“设备 B”）接收来自“设备 A”的状态报告，并随时准备在发生故障切换时成为主设备。VPN 通道 B 处于连接、非活动状态。

如果发生下列任一事件，则“设备 B”将成为主设备，而“设备 A”将成为备份设备（或“设备 A”在出现内部系统故障时变为不可操作）。



范例 : 通过 VPN 通道的 IP 跟踪

在本例中，将配置两个 VPN 通道[8]，分别供 NSRP 集群中的两台 NetScreen 设备使用。然后将配置两台设备以跟踪通道远程端的两台服务器的 IP 地址 : 10.2.2.50 和 10.2.2.60。

注意 : *本例根据第 149 页上的 “范例 : 配置 NSRP-Lite”中的配置而建立。*

将每个 VPN 通道配置为基于路由，并将其绑定到名为 *tunnel.1* 的未编号通道接口。两条通道均使用预共享密钥 (在本例中两条通道的密钥是不相同的，但它们可以是相同的)。“阶段 1” 协商为 “主” 模式，并将启用 “阶段 2” 协商的回放攻击保护。为阶段 1 和阶段 2 提议使用预定义安全级别 “Compatible”[9]。还将启用带有重定密钥选项的 VPN 监控。 (有关基于路由的 VPN 通道的详细信息，请参阅第 5 卷，“VPN”。)

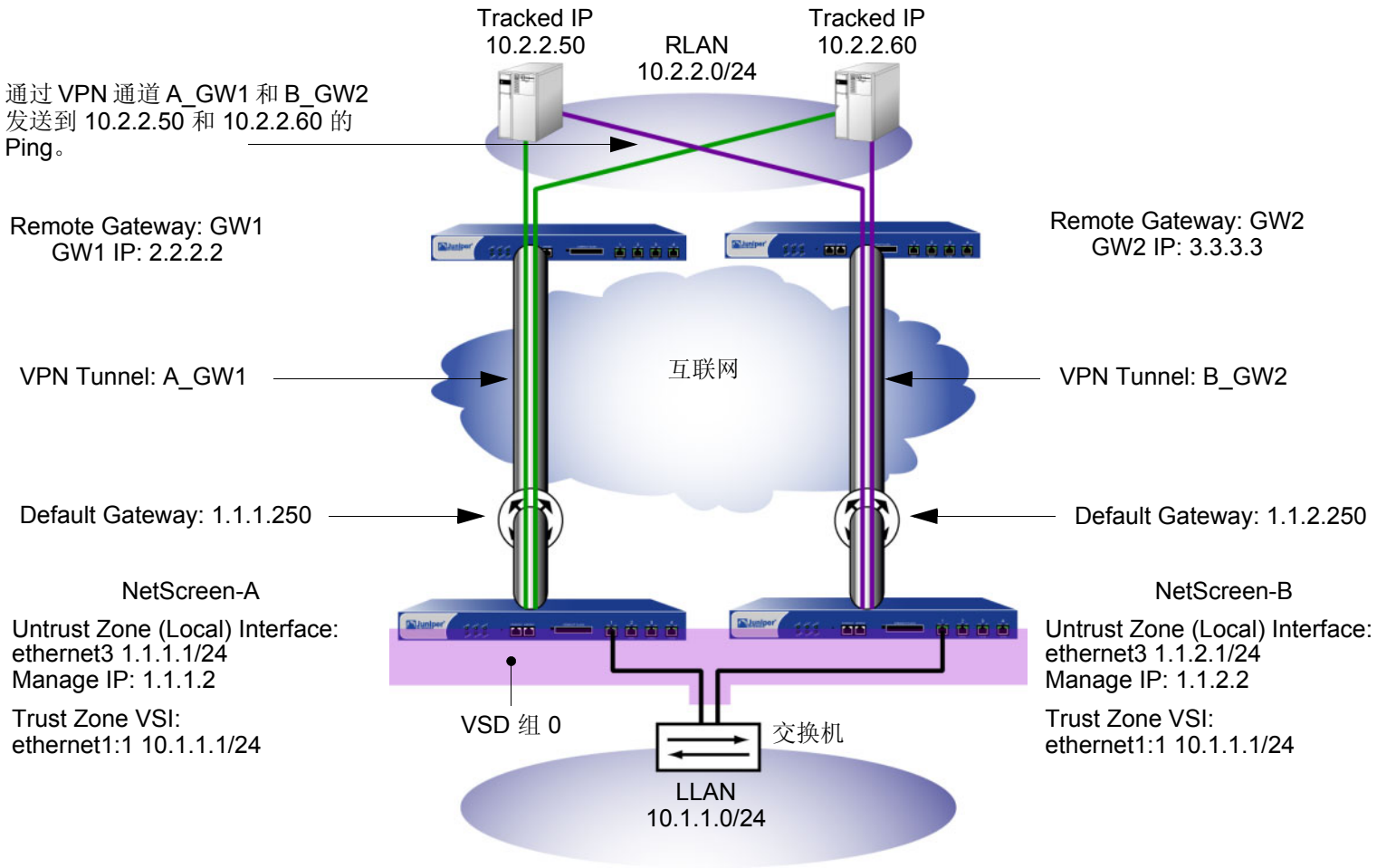
为每个被跟踪地址所定义的设置如下 :

- 10.2.2.50 处的服务器
  - Interval: 10
  - Threshold: 5
  - Weight: 16
- 10.2.2.60 处的服务器
  - Interval: 10
  - Threshold: 5
  - Weight: 16

向其中一个服务器连续发出 5 次尝试后，如果没有收到 ping 响应，即认为尝试失败，并将权重值 16 计入总故障切换临界值。

因为设备故障切换临界值为 31，所以只有两个被跟踪的 IP 地址都出现故障，才会发生设备切换。如果不允许这样多的故障，您可以把临界值降低到一个更容易接受的级别。

8. 本例中不包括远程站点设备上两个通道的配置。
9. 四个与 “阶段 1” 兼容的安全级别提议为 pre-g2-3des-sha、pre-g2-3des-md5、pre-g2-des-sha 和 pre-g2-des-md5。四个与 “阶段 2” 兼容的安全级别提议为 nopfs-esp-3des-sha、nopfs-esp-3des-md5、nopfs-esp-des-sha 和 nopfs-esp-des-md5。



WebUI (NetScreen-A)

1. VPN 通道 (NetScreen-A)

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

Address Name: LLAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

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

Address Name: RLAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)[10]

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

VPN Name: A_gw1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw1

Type: Static IP (选择), Address/Hostname: 2.2.2.2

Preshared Key: h1p8A24nG5

Security Level: Compatible

Outgoing Interface: ethernet3

10. 源接口所在的虚拟路由选择域必须与通道接口所绑定的虚拟路由选择域相同；本例中为 trust-vr。该未编号通道接口借用指定安全区段接口的 IP 地址。

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Security Level: Compatible

Replay Protection: (选择)

Bind To: Tunnel Interface: tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

VPN Monitor: (选择)

Source Interface: Default

Destination IP: 2.2.2.2

Optimization: (清除)

Rekey: (选择)

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

Network Address/Netmask: 10.2.2.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

Source Address:

Address Book Entry: (选择), LLAN

Destination Address:

Address Book Entry: (选择), RLAN

Service: ANY

Action: Permit

Position at Top: (选择)

2. IP 跟踪 (NetScreen A)

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.2.2.50

Method: Ping

Weight: 16

Interval (sec): 10

Threshold: 5

Interface: tunnel.1

VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.2.2.60

Method: Ping

Weight: 16

Interval (sec): 10

Threshold: 5

Interface: tunnel.1

VSD Group ID: Device

Network > NSRP > Monitor > Track IP > Edit (对于 VSD: Device): 选择 **Enable Track IP**，然后在 Failover Threshold 字段中输入 **31**。

3. VPN 通道 (NetScreen-B)

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

Address Name: LLAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

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

Address Name: RLAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)[11]

11. 源接口所在的虚拟路由选择域必须与通道接口所绑定的虚拟路由选择域相同；本例中为 trust-vr。该未编号通道接口借用指定安全区段接口的 IP 地址。

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

VPN Name: B_gw2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: gw2

Type: Static IP (选择), Address/Hostname: 3.3.3.3

Preshared Key: ih38CvE3g9

Security Level: Compatible

Outgoing Interface: ethernet3

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 AutoKey IKE 配置页：

Security Level: Compatible

Replay Protection: (选择)

Bind To: Tunnel Interface: tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

VPN Monitor: (选择)

Source Interface: Default

Destination IP: 3.3.3.3

Optimization: (清除)

Rekey: (选择)

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

Network Address/Netmask: 10.2.2.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.2.250

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

Source Address:

Address Book Entry: (选择), LLAN

Destination Address:

Address Book Entry: (选择), RLAN

Service: ANY

Action: Permit

Position at Top: (选择)

4. IP 跟踪 (NetScreen-B)

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.2.2.50
Method: Ping
Weight: 16
Interval (sec): 10
Threshold: 5
Interface: tunnel.1
VSD Group ID: Device

Network > NSRP > Monitor > Track IP > New: 输入以下内容，然后单击 **OK**:

Track IP: 10.2.2.60
Method: Ping
Weight: 16
Interval (sec): 10
Threshold: 5
Interface: tunnel.1
VSD Group ID: Device

Network > NSRP > Monitor > Track IP > Edit (对于 VSD: Device): 选择 **Enable Track IP**，然后在 Failover Threshold 字段中输入 **31**。

CLI

1. VPN 通道 (NetScreen-A)

```
set address trust LLAN 10.1.1.0/24
set address untrust RLAN 10.2.2.0/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set ike gateway gw1 ip 2.2.2.2 main outgoing-interface ethernet3 preshare
    h1p8A24nG5 sec-level compatible
set vpn A_gw1 gateway gw1 replay sec-level compatible
set vpn A_gw1 bind interface tunnel.1
set vpn A_gw1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
set vpn A_gw1 monitor source-interface ethernet3 destination-ip 2.2.2.2 rekey
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set policy top from trust to untrust LLAN RLAN any permit
```

2. IP 跟踪 (NetScreen-A)

```
set interface tunnel.1 track-ip ip 10.2.2.50
set interface tunnel.1 track-ip ip 10.2.2.50 interval 10
set interface tunnel.1 track-ip ip 10.2.2.50 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.50 weight 16
set interface tunnel.1 track-ip ip 10.2.2.60
set interface tunnel.1 track-ip ip 10.2.2.60 interval 10
set interface tunnel.1 track-ip ip 10.2.2.60 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.60 weight 16
set nsrp track-ip threshold 31
set nsrp track-ip
save
```

3. VPN 通道 (NetScreen-B)

```
unset nsrp config sync
set address trust LLAN 10.1.1.0/24
set address untrust RLAN 10.2.2.0/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set ike gateway gw2 ip 3.3.3.3 main outgoing-interface ethernet3 preshare
    ih38CvE3g9 sec-level compatible
set vpn B_gw2 gateway gw2 replay sec-level compatible
set vpn B_gw2 bind interface tunnel.1
set vpn B_gw2 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
set vpn B_gw2 monitor source-interface ethernet3 destination-ip 3.3.3.3 rekey
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.2.250
set policy top from trust to untrust LLAN RLAN any permit
```

4. IP 跟踪 (NetScreen-B)

```
set interface tunnel.1 track-ip ip 10.2.2.50
set interface tunnel.1 track-ip ip 10.2.2.50 interval 10
set interface tunnel.1 track-ip ip 10.2.2.50 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.50 weight 16
set interface tunnel.1 track-ip ip 10.2.2.60
set interface tunnel.1 track-ip ip 10.2.2.60 interval 10
set interface tunnel.1 track-ip ip 10.2.2.60 threshold 5
set interface tunnel.1 track-ip ip 10.2.2.60 weight 16
set nsrp track-ip threshold 31
set nsrp track-ip
save
```

索引

A

ARP 57, 122
  广播 19
  路径监控 159

C

CLI
  set arp always-on-dest 57
  约定 iv
插图
  约定 vii
串行接口 103
  故障切换 108
  ISP 配置 106
  调制解调器配置 104
串行接口的 ISP 配置 106
串行接口的调制解调器配置 104

D

端口
  端口故障切换 60
  二级可信和不可信 60
  监控 120, 159
  冗余 39
  主可信和不可信 60
对象监控 118

E

二级路径 19, 26

F

负载共享 130

G

高可用性
  请参阅 HA
故障切换
  串行接口 108
  对象监控器 118
  设备 116
  双 Untrust 接口 70, 72
  VSD 组 117
  虚拟系统 130
管理 IP
  VSD 组 0 8

H

HA
  串行接口 103
  电缆连接 46–49
  二级路径 26
  HA LED 26
  IP 跟踪 122, 159
  将网络接口作为 HA 链接连接 48
  聚合接口 67
  控制链接 39
  链接探查 43
  路径监控 159
  冗余接口 60
  数据链接 41
  双 Untrust 接口 69
  双主动故障切换 6
  消息 41
  主动 / 被动故障切换 4
  专用 HA 接口的电缆连接 46

I

IP 跟踪 122, 159
  device failover threshold 160
  跟踪的 IP 故障临界值 119
  ping 和 ARP 122, 159
  权重 160
  tracked IP failure threshold 160
  通道故障切换 161

J

集群 17–21, 50, 140–143
集群名称， NSRP 18, 143
加密
  NSRP 7, 19
  NSRP-Lite 144
接口
  串行 103
  HA 双端口 39–42
  监控 19
  聚合 67
  冗余 60
  双 Untrust 69
  VSI 29
  虚拟 HA 48
聚合接口 67

K

控制消息 39
  HA 物理链接心跳信号 40
  HA 消息 41
  RTO 心跳信号 41
  VSD 心跳信号 40

L

LED 指示器， HA 26
路径监控 159
  通道故障切换 161

M

名称
  约定 viii

N

NetScreen 可靠传输协议
  请参阅 NRTP

NetScreen 冗余协议
请参阅 NSRP
NRTP 34, 156
NSRP
ARP 57
ARP 广播 19
安全通信 7, 19
备份 4
clear 集群命令 17, 143
config sync 34
debug 集群命令 17, 143
电缆连接 46–49
端口故障切换 60
端口监控 120
二级路径 19, 26
负载共享 130
概述 3
管理 IP 122, 159
HA 电缆连接，网络接口 48
HA 电缆连接，专用接口 46
HA 端口，冗余接口 60
HA 会话备份 22
HA 接口 40
HA LED 26
集群 17–21, 50
集群名称 18, 143
接口监控 19
控制链接 39
控制消息 39, 40
NAT 和 “路由” 模式 8
NTP 同步 38
抢先模式 24
全网状配置 46, 130
缺省设置 9, 141
RTO 22–23, 50
RTO 状态 23
RTO，同步 35
冗余端口 39
数据包转发和动态路由选择 42
数据链接 41
数据消息 41
同步， PKI 35
透明模式 8
VSD 组 5, 24–28, 50, 159
VSI 5
VSI，静态路由 29, 65, 66
文件，同步 35
虚拟系统 130–136
抑制时间 52, 56
优先级编号 24
主设备 4
NSRP-Lite 137–158
安全通信 144
电缆连接 148
端口监控 159
集群 140–143
禁用同步 158
配置同步 156
抢先模式 147
VSD 组 145–147
文件同步 157
NTP
NSRP 同步 38

Q

抢先模式 24, 147
全网状配置 130

R

RFC
2338 122, 159
RTO 22–23
操作状态 23
RTO 对等方 25
认证
NSRP 7, 19
NSRP-Lite 144

S

设备故障切换 116
数据消息 41
双 Untrust 接口 69

T

同步
PKI 对象 35
配置 34
RTO 35
文件 35

V

VRRP 122, 159
VSD 组 5, 24–28, 145–147
成员状态 25, 145–146, 159
故障切换 117
心跳信号 19, 26, 146
抑制时间 52, 56
优先级编号 24
VSI 5, 24, 145
静态路由 29, 65, 66
每个 VSD 组有多个 VSI 130

W

WebUI
约定 v

X

协议
NRTP 34, 156
NSRP 1, 137
VRRP 122, 159
虚拟 HA 接口 48
虚拟安全接口
请参阅 VSI
虚拟安全设备组
请参阅 VSD 组
虚拟系统
负载共享 130
故障切换 130
NSRP 130

Y

约定
CLI iv
插图 vii
名称 viii
WebUI v

Z

执行对象
请参阅 RTO
字符类型， ScreenOS 支持的 viii