NetScreen 概念与范例

ScreenOS 参考指南

第 5 卷 : VPN

ScreenOS 5.1.0

编号 093-1370-000-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

虚拟专用网 (VPN) 是一种具有成本效益的安全方法，对于企业而言，可为用户提供对企业网的拨号访问，对于远程网络而言，可以实现互联网上的相互通信。通过互联网的安全专用连接比专用线路更具有成本效益。NetScreen 设备为安全的站点到站点以及拨号 VPN 应用程序提供了所有 VPN 功能。

第 5 卷中的 “VPN” 一节对 NetScreen 设备上可用的下列 VPN 概念和功能进行了介绍：

- 互联网密钥交换 (IKE) 和互联网协议安全性 (IPsec) 元素
- “公开密钥基础” (PKI) 环境下的证书及证书撤消列表 (CRL)
- 站点到站点 VPN
- 拨号 VPN
- “第 2 层通道协议” (L2TP) 及 IPSec 上的 L2TP
- 高级 VPN 功能，如 NAT 穿透、VPN 监控、将多个 VPN 通道绑定到单个通道接口、冗余 IKE 网关以及 VPN 通道故障切换行为等。

本卷中还提供了上述所有功能的大量示例。

约定

本文档包含几种类型的约定，以下各节将对其加以介绍：

CLI 约定

当出现命令行界面 (CLI) 命令的语法时，使用以下约定：

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

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

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

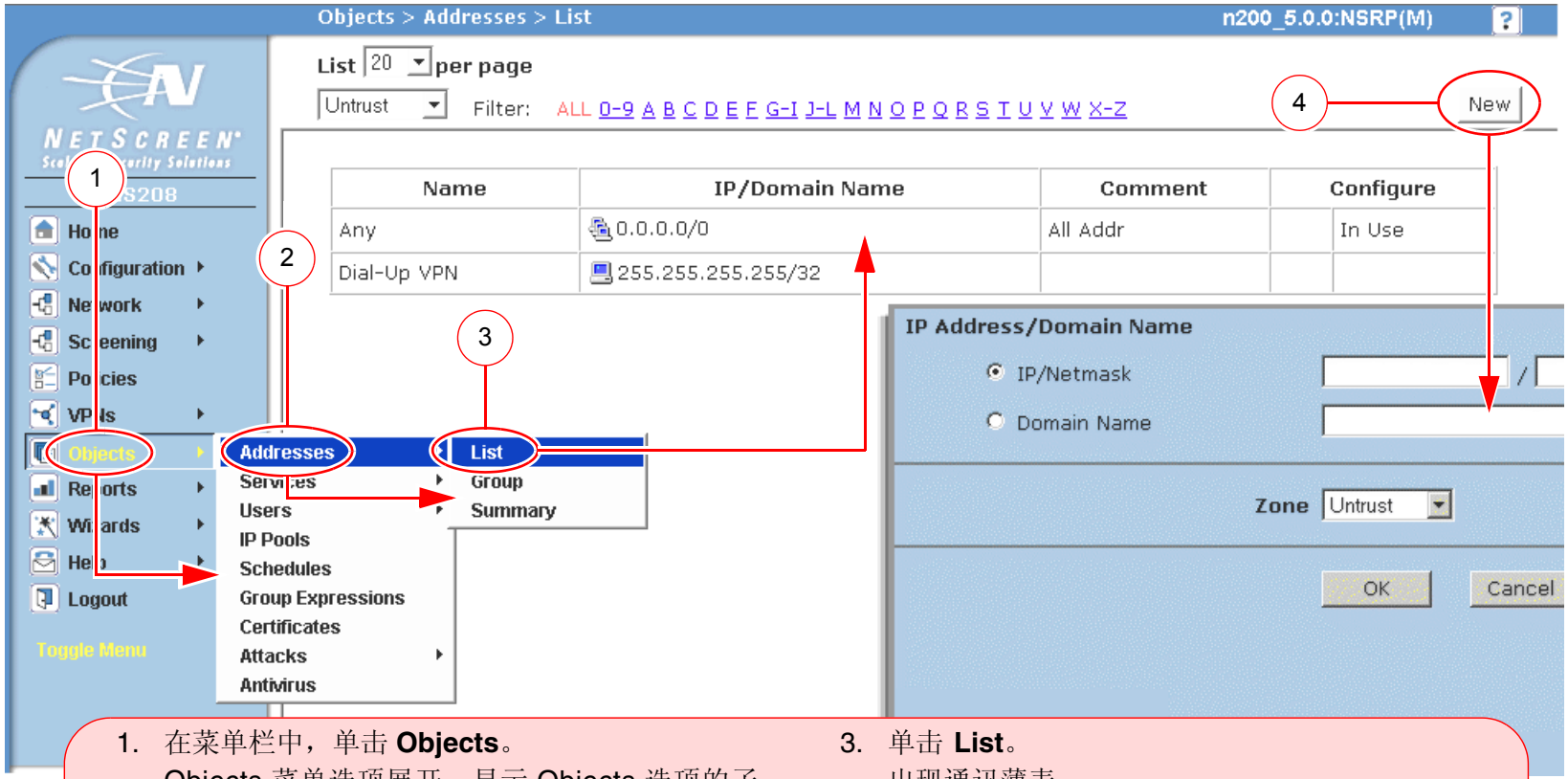
  ```
  set admin user name password
  ```

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

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

WebUI 约定

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



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

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

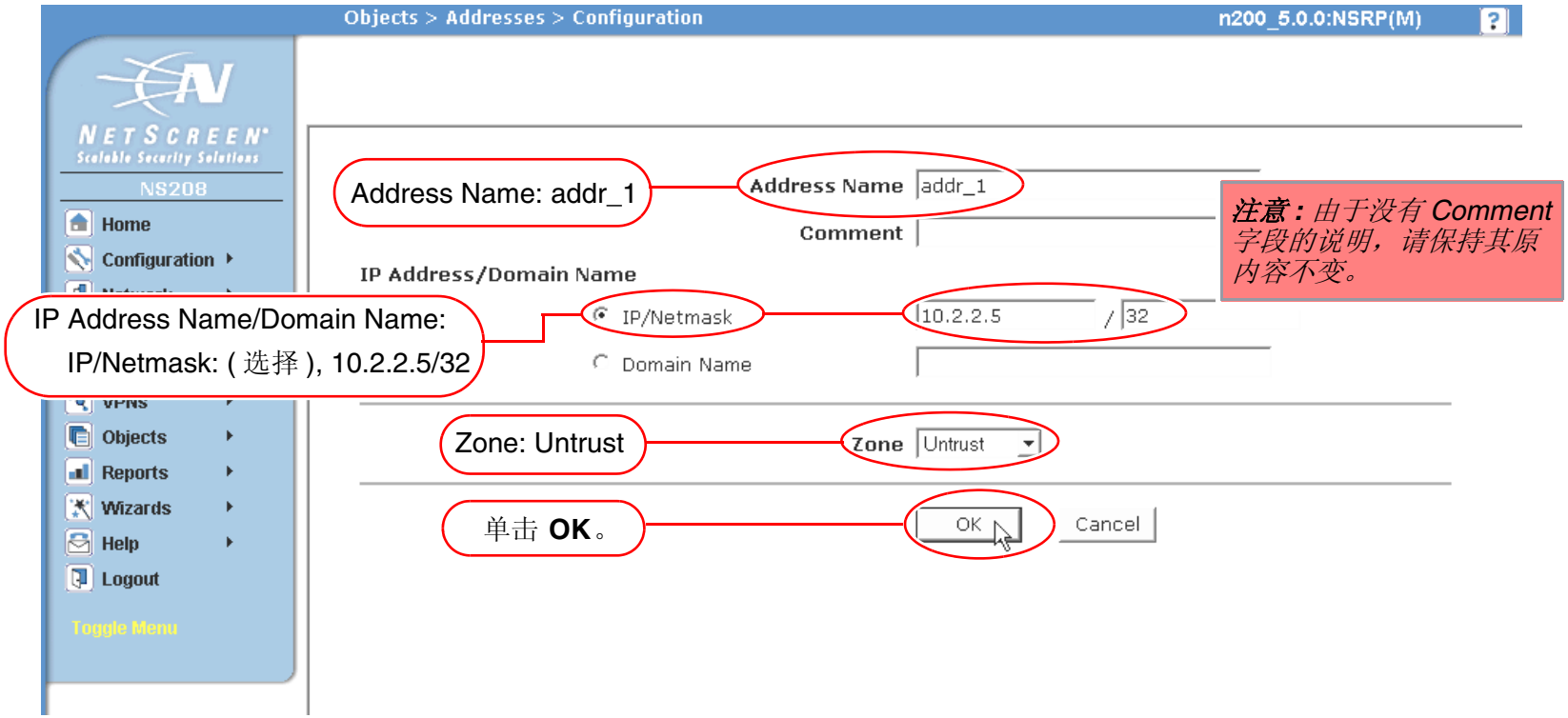
Objects > Addresses > List > New: 输入以下内容，然后单击 **OK**:

Address Name: addr_1

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.5/32

Zone: Untrust

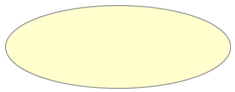


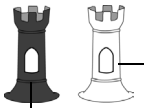
插图约定

下列图形构成了贯穿本书的插图所用的基本图像集：


通用 NetScreen 设备


虚拟路由选择域

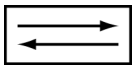

安全区段


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


通道接口

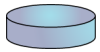

VPN 通道


路由器图标


交换机图标


包含单个子网的局域网 (LAN)
(例如 : 10.1.1.0/24)


互联网


动态 IP (DIP) 池


台式计算机


便携式计算机


通用网络设备
(例如： NAT 服务器，
接入集中器)


服务器

命名约定和字符类型

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

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

ScreenOS 支持以下字符类型 :

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

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

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

JUNIPER NETWORKS NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs-comments@juniper.net

1

IPSec

本章将介绍“互联网协议安全性” (IPSec) 的各种要素及其与虚拟专用网 (VPN) 通道相连的方式。作为第 2 页上的“VPN 简介”的后续内容，本章的其余部分将说明 IPSec 的以下各要素：

VPN 简介

虚拟专用网 (VPN) 提供了通过公用广域网 (WAN) (例如，互联网) 在远程计算机间实现安全通信的方法。

VPN 连接可以链接两个局域网 (LAN) 或一个远程拨号用户和一个 LAN。在这两点间流动的信息流流经共享的资源，例如，路由器、交换机以及其它组成公用 WAN 的网络设备。要在流经 WAN 时确保 VPN 通信的安全性，这两个参与者必须创建一个 “IP 安全性” (IPSec) 通道[1]。

IPSec 通道由一对指定安全参数索引 (SPI) 的单向 “安全联盟” (SA) (位于通道的两端)、目标 IP 地址以及所用的安全性协议 (“认证包头” 或 “封装安全性负荷”) 组成。

注意：*有关 SPI 的详细信息，请参阅**第 10 页上的 “安全联盟”**。有关 IPSec 安全性协议的详细信息，请参阅**第 7 页上的 “协议”**。*

通过 SA， IPSec 通道可以提供以下安全功能 :

- 私密性 (通过加密)
- 内容完整性 (通过数据认证)
- 发送方认证和 (如果使用证书) 认可 (通过数据初始认证)

根据需要采用相应的安全功能。如果仅需认证 IP 数据包来源和内容的完整性，您可以认证此数据包，而不应用任何加密。相反，如果仅想保护私密性，您可以对此数据包加密而不应用任何认证机制。还可同时加密和认证此数据包。大多数网络安全设计者都选择加密、认证 VPN 信息流，以及对 VPN 信息流进行回放保护。

NetScreen 支持 IPSec 技术，使用两种密钥创建机制创建 VPN 通道 :

- 手动密钥
- 具有预先共享密钥或证书的 “自动密钥 IKE”

1. 术语 “通道” 并不表示是 “传输” 模式或 “通道” 模式 (请参阅第 4 页上的 “模式”)。它仅指 IPSec 连接。

IPSEC 概念

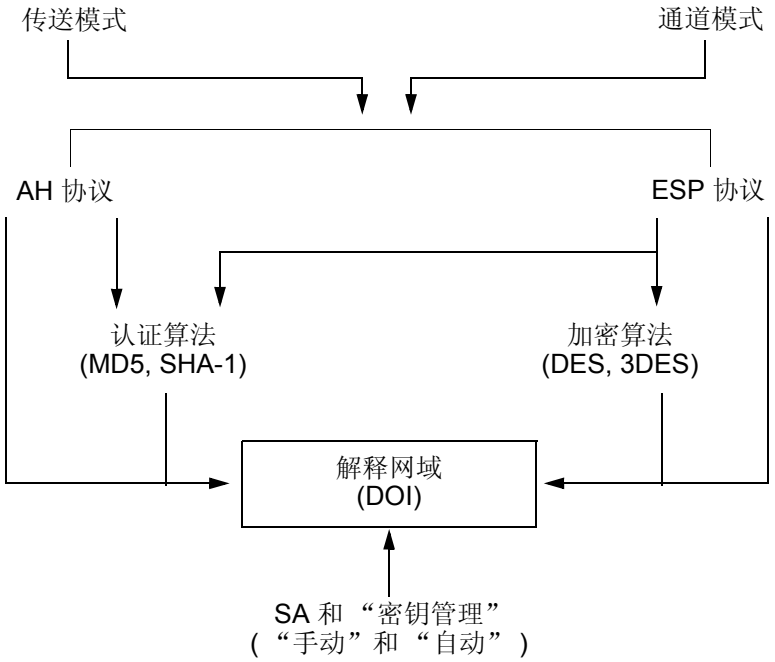
“IP 安全性” (IPSec) 是一系列用于在 IP 数据包层处用密码保护通信的相关协议。 IPSec 由两种模式和两种主要协议组成 :

- 传送模式和通道模式
- 用于认证的 “认证包头” (AH) 协议和用于加密 (和认证) 的 “封装安全性负荷” (ESP) 协议

IPSec 还提供用于 “安全联盟” (SA) 和密钥分配的手动和自动协商方法，包括在 “解释网域” (DOI) 中为其收集的所有属性。请参阅 RFC 2407 和 2408。

注意 : NetScreen 不支持带有 AH 的 “传送模式”。

IPSec 结构



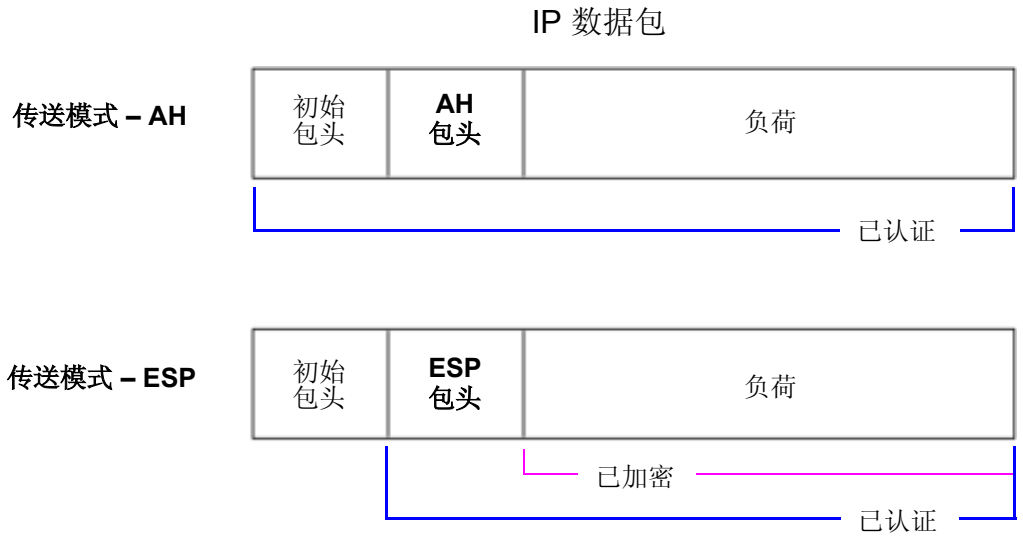
注意：IPSec “解释网域” (DOI) 是一个文档，该文档中包含 VPN 通道成功协商所需的所有安全性参数定义，特别是 SA 和 IKE 协商所需的所有属性。

模式

IPSec 在以下两种模式中的任一种模式下运行：传送模式和通道模式。当通道两端都是主机时，可以使用传送模式或通道模式。当至少有一个通道端点是安全网关 (例如，路由器或防火墙) 时，就必须使用通道模式。 NetScreen 设备总是对 IPSec 通道运行通道模式，对 IPSec 上的 L2TP 通道运行传送模式。

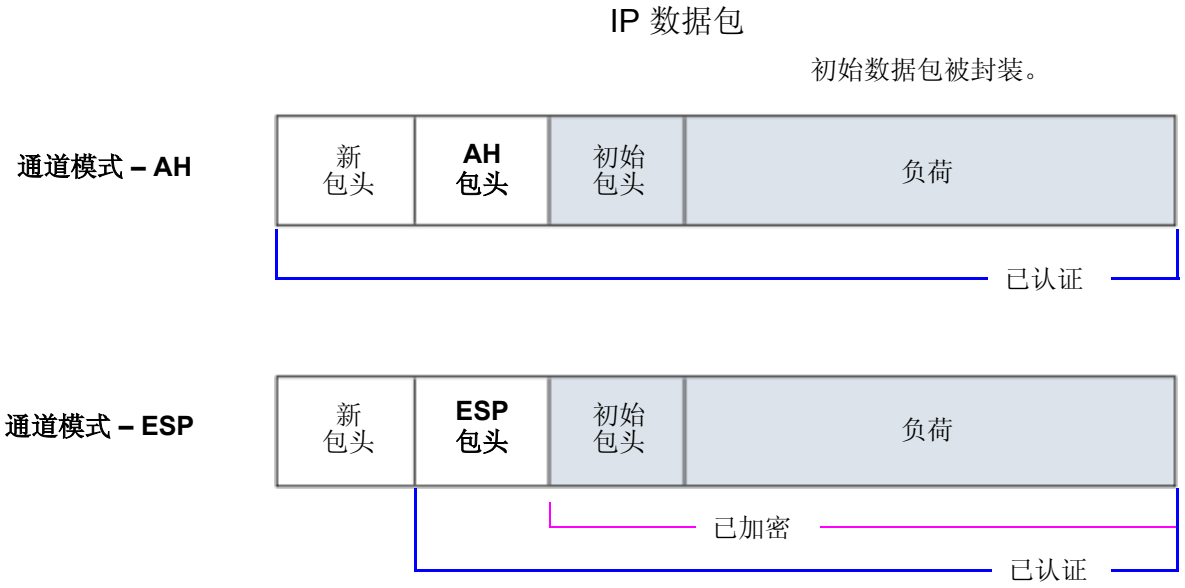
传送模式

初始 IP 数据包没有封装在另一个 IP 数据包中。整个数据包都可以认证 (使用 AH)，负荷可以加密 (使用 ESP)，初始包头仍保留明文的形式，就如同通过 WAN 发送一样。



通道模式

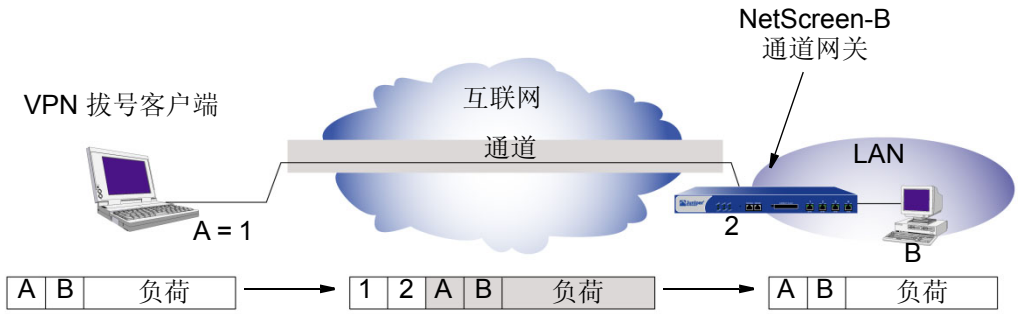
整个初始 IP 数据包 (负荷和包头) 都封装在另一个 IP 负荷中，并且附加了新包头。整个初始数据包可以被加密、被认证、或者既加密又认证。使用 AH， AH 和新包头也可以被认证。使用 ESP， ESP 包头也可以被认证。



在站点到站点的 VPN 中，新包头中使用的源地址和目标地址是出接口 (NAT 或 “路由” 模式下) 的 IP 地址，或是 VLAN1 IP 地址 (“透明” 模式下) ；已封装数据包的源地址和目标地址是该连接最终端点的地址。

通道模式下的站点到站点 VPN

在拨号 VPN 中，通道的 VPN 拨号客户端没有通道网关，通道直接延伸到客户端本身。这种情况下，在从拨号客户端发送的数据包上，新包头和已封装的初始包头具有相同的 IP 地址：即客户机的地址[2]。



通道模式下的拨号 VPN

2. 某些 VPN 客户端 (如 NetScreen-Remote) 允许定义虚拟内部 IP 地址。在这些情况下，虚拟内部 IP 地址是来自客户端的信息流的初始数据包包头中的源 IP 地址， ISP 动态分配给拨号客户端的 IP 地址是外部包头中的源 IP 地址。

协议

IPSec 使用两种协议来保护 IP 层的通信 :

- 认证包头 (AH) — 认证 IP 数据包来源和验证其内容完整性的安全协议
- 封装安全性负荷 (ESP) — 加密整个 IP 数据包 (以及认证其内容) 的安全协议

AH

“认证包头” (AH) 协议提供验证内容真实性 / 完整性以及数据包来源的方法。可以通过校验和来认证此数据包，该校验和是使用密钥和 MD5 或 SHA-1 散列功能通过基于散列的信息认证代码 (HMAC) 计算得出的。

“消息整理”版本 5 (MD5) — 从任意长度消息和 16 字节密钥生成 128 位散列 (也称作数字签名或消息整理) 的算法。所生成的散列 (如同输入的指印) 用于验证内容和来源的真实性及完整性。

安全散列算法 1 (SHA-1) — 从任意长度信息和 20 字节密钥生成 160 位散列的算法。通常认为它比 MD5 更安全，因为它生成的散列更大。由于是在 NetScreen ASIC 中执行运算处理的，所以执行成本可以忽略不计。

***注意：**有关 MD5 和 SHA-1 散列算法的详细信息，请参阅以下的 RFC: (MD5) 1321, 2403; (SHA-1) 2404。有关 HMAC 的信息，请参阅 RFC 2104。*

ESP

“封装安全性负荷” (ESP) 协议提供了确保私密性 (加密)、来源认证和内容完整性 (认证) 的方法。通道模式下的 ESP 封装整个 IP 数据包 (包头和负荷)，然后将新的 IP 包头附加到刚加密的数据包上。新 IP 包头中包含有需要通过网络发送受保护数据的目标地址。

利用 ESP，可以加密并认证、仅加密或仅认证。对于加密，可以选择下列加密算法中的一种 :

数据加密标准 (DES) — 带有 56 位密钥的密码块算法。

三重 DES (3DES) — 使用 168 位密钥的 DES 增强版本，在其中应用了三次初始 DES 算法。 DES 的性能更好，但并不适用于一些绝密或机密资料的传输。

高级加密标准 (AES) — 混合的加密标准，当全球的互联网基础设施都采用此标准时，它将提供与其它网络安全设备之间更强的互操作性。 NetScreen 支持带有 128 位、 192 位和 256 位密钥的 AES。

对于认证，可以使用 MD5 或 SHA-1 算法。

对于加密或认证算法，您可以选择 **NULL** ；但是，不能同时为两种算法选择 **NULL**。

密钥管理

密钥的分配和管理对于成功使用 VPN 很关键。 IPSec 支持手动和自动密钥分配方法。

手动密钥

利用 “手动密钥”，通道两端的管理员可以配置所有安全参数。对于小的、静态网络来说，这是可行的技术，在这种网络中，密钥的分配、维护和跟踪都不难。但是，在长距离内要安全地分配 “手动密钥” 配置会有安全问题。除了面对面传输密钥外，您不能完全保证在传输过程中不泄漏密钥。同时，每当要更改密钥时，象最初分配密钥时一样，需面对同样的安全问题。

自动密钥 IKE

当需要创建和管理多个通道时，就需要一种不必手动配置每一个元素的方法。 IPSec 使用 “互联网密钥交换” (IKE) 协议支持密钥的自动生成和协商以及安全联盟。 NetScreen 中将此自动通道协商称为 “自动密钥 IKE”，并支持带有预共享密钥的 “自动密钥 IKE” 和带有证书的 “自动密钥 IKE”。

具有预共享密钥的自动密钥 IKE

通过使用预共享密钥的 “自动密钥 IKE” 来认证 IKE 会话中的参与者时，各方都必须预先配置和安全地交换预共享密钥[3]。在此情况下，安全密钥分配问题就与使用 “手动密钥” 时的问题相同。但是，一旦分配了密钥，“自动密钥” 就可使用 IKE 协议，在预先确定的时间间隔内自动更改其密钥 (与 “手动密钥” 不同)。经常更改密钥会大大提高安全性，自动更改密钥会大大减少密钥管理任务。但是，由于更改密钥会增加流量开销，因此，过于频繁地更改密钥会降低数据传输效率。

3. 预共享密钥是用于加密和解密的密钥，参与者双方在开始通信前都必须拥有此密钥。

具有证书的自动密钥 IKE

当在 “自动密钥 IKE” 协商过程中使用证书对参与者认证时，双方都生成一个公用 / 私用密钥对 (请参阅第 2 章，第 23 页上的 “公开密钥密码术”) 并获得证书 (请参阅第 29 页上的 “证书和 CRL”)。只要双方都信任发行的证书授权机构 (CA)，参与者就可检索对等方的公用密钥并验证对等方的签名。没有必要对密钥和 SA 进行跟踪； IKE 将自动进行跟踪。

***注意：** 有关 “手动密钥” 和 “自动密钥 IKE” 通道的示例，请参阅第 4 章，第 99 页上的 “站点到站点 VPN”。*

安全联盟

安全联盟 (SA) 是 VPN 参与者之间用于确保信道安全有关方法和参数的单向协议。对于双向通信，至少需要有两个 SA，每个方向使用一个。

SA 将下列组件组合在一起用于确保通信安全 :

- 安全算法和密钥
- 协议模式 (传送或通道)
- 密钥管理方法 (“手动密钥” 或 “自动密钥 IKE”)
- SA 寿命

对于出站 VPN 信息流，策略将调用同 VPN 通道相关的 SA。对于入站信息流， NetScreen 设备通过使用以下的三元组来查找 SA: 目标 IP、安全协议 (AH 或 ESP) 以及安全参数索引 (SPI) 值。

通道协商

对于“手动密钥”IPSec 通道，由于已经预先定义了所有安全联盟 (SA) 参数，就不必协商要使用哪个 SA。事实上，已经建立了该通道。当信息流与使用该“手动密钥”通道的策略相匹配时，或当路由包含此通道时， NetScreen 设备将按所确定的方式仅加密和认证数据，并将其转发到目标网关。

要建立“自动密钥 IKE” IPSec 通道，需要进行两个阶段的协商：

- 在第 1 阶段，参与者要建立一个将在其中协商 IPSec SA 的安全通道。
- 在第 2 阶段，参与者协商用于加密和认证用户数据连续交换的 IPSec SA。

第 1 阶段

“自动密钥 IKE”通道协商的第 1 阶段由如何认证和保护通道的提议交换组成。交换可以在两种模式的其中一种模式下进行：Aggressive mode (主动模式) 或 Main mode (主模式) (如下所述)。使用任一种模式时，参与者将交换可接受的安全服务提议，例如：

- 加密算法 (DES 和 3DES) 和认证算法 (MD5 和 SHA-1)。有关这些算法的详细信息，请参阅第 7 页上的“协议”
- Diffie-Hellman 组 (请参阅第 13 页上的 “Diffie-Hellman 交换”。)
- 预共享密钥或 RSA/DSA 证书 (请参阅第 9 页上的 “自动密钥 IKE”)

当通道的两端都同意接受所提出的至少一组第 1 阶段安全参数，并处理该参数时，第 1 阶段协商将成功结束。NetScreen 设备最多支持四个第 1 阶段协商的提议，并允许您定义接受密钥协商的一系列安全参数的限制程度。

NetScreen 提供的预定义“第 1 阶段”提议如下：

- **Standard:** pre-g2-aes128-sha 和 pre-g2-3des-sha
- **Compatible:** pre-g2-3des-sha、 pre-g2-3des-md5、 pre-g2-des-sha 和 pre-g2-des-md5
- **Basic:** pre-g1-des-sha 和 pre-g1-des-md5

也可以定义自定义的“第 1 阶段”提议。

Main Mode / Aggressive Mode (主模式和主动模式)

第 1 阶段可能发生在 Main mode (主模式) 或 Aggressive mode (主动模式) 下。这两种模式如下所述。

Main mode (主模式): 发起方和接受方之间发送三个双向信息交换 (共六条消息) 以获取以下服务 :

- 第一次交换， (消息 1 和 2): 提出并接受加密和认证算法。
- 第二次交换， (消息 3 和 4): 执行 Diffie-Hellman 交换，发起方和接受方各提供一个当前数 (随机生成的号码)。
- 第三次交换， (消息 5 和 6): 发送并验证其身份。

在第三次交换消息时传输的信息由在前两次交换中建立的加密算法保护。因此，在明文中没有传输参与者的身份。

Aggressive mode (主动模式) : 发起方和接受方获取相同的对象，但仅进行两次交换，总共有三条消息 :

- 第 1 条消息 : 发起方建议 SA，启动 Diffie-Hellman 交换，发送一个当前数及其 IKE 身份。
- 第 2 条消息 : 接受方接受 SA，认证发起方，发送一个当前数及其 IKE 身份，以及发送接受方的证书 (如果使用证书)。
- 第 3 条消息 : 发起方认证接受方并确认交换，并发送发起方的证书 (若使用了证书)。

由于参与者的身份是在明文中交换的 (在前两条消息中)， Aggressive mode (主动模式) 不提供身份保护。

注意 : *当拨号 VPN 用户使用预共享密钥协商 “自动密钥 IKE” 通道时，必须使用 Aggressive mode (主动模式)。同时还要注意 : 拨号 VPN 用户可以使用电子邮件地址、完全合格的域名 (FQDN) 或 IP 地址作为其 IKE ID。动态对等方可以使用电子邮件地址或 FQDN，但不可以使用 IP 地址。*

Diffie-Hellman 交换

Diffie-Hellman 交换允许参与者生成一个共享的秘密值。该技术的优点在于它允许参与者在非安全媒体上创建秘密值，而不把此秘密值通过网线传输。有五个 Diffie-Hellman (DH) 组 (NetScreen 支持组 1、 2 和 5)。在各组计算中所使用主要模数的大小都不同，如下所述：

- DH 组 1: 768 位模数[4]
- DH 组 2: 1024 位模数
- DH 组 5: 1536 位模数

模数越大，就认为生成的密钥越安全；但是，模数越大，密钥生成过程就越长。由于每个 DH 组的模数都有不同的大小，因此参与者必须同意使用相同的组[5]。

第 2 阶段

当参与者建立了一个已认证的安全通道后，他们将继续执行 “第 2 阶段”。在此阶段中，他们将协商 SA 以保护要通过 IPSec 通道传输的数据。

与 “第 1 阶段”的过程相似，参与者交换提议以确定要在 SA 中应用的安全参数。“第 2 阶段”提议还包括一个安全协议 (“封装安全性负荷” (ESP) 或 “认证包头” (AH)) 及所选的加密和认证算法。如果需要 “完全正向保密” (PFS)，提议中还可以指定一个 Diffie-Hellman 组。

> ***注意：****有关 Diffie-Hellman 组的详细信息，请参阅上述 “Diffie-Hellman 交换”。有关 PFS 的详细信息，请参阅第 14 页上的 “完全正向保密”。*

不管在 “第 1 阶段”中使用何种模式，“第 2 阶段”总是在 “快速”模式中运行，并且包括三条消息的交换[5]。

NetScreen 设备最多支持四个 “第 2 阶段”协商的提议，允许您定义您可以接受的对一系列通道参数的限制程度。NetScreen 还提供回放攻击保护功能。使用此功能不需要协商，因为数据包总是和序列号一起发送。您仅有校验序列号或不校验序列号的选择权。 (有关回放攻击保护的详细信息，请参阅下文。)

4. “DH 组 1”安全性的优点已经下降，因此 Juniper Networks 建议您尽量不要使用它。
5. 如果配置有多个 (最多四个) “第 1 阶段”协商提议，请在所有的提议中使用相同的 Diffie-Hellman 组。将同样的准则应用于 “第 2 阶段”协商的多个提议中。

NetScreen 提供的预定义 “第 2 阶段” 提议如下 :

- **Standard:** g2-esp-3des-sha 和 g2-esp-aes128-sha
- **Compatible:** nopfs-esp-3des-sha、 nopfs-esp-3des-md5、 nopfs-esp-des-sha 和 nopfs-esp-des-md5
- **Basic:** nopfs-esp-des-sha 和 nopfs-esp-des-md5

也可以定义自定义的 “第 2 阶段” 提议。

在 “第 2 阶段” 中，对等方也交换代理 ID。代理 ID 是一个三方元组，由本地 IP 地址、远程 IP 地址和服务组成。两个对等方的代理 ID 必须匹配，这意味着两个对等方的代理 ID 中指定的服务必须相同，并且为一个对等方指定的本地 IP 地址必须与为另一个对等方指定的远程 IP 地址相同。

完全正向保密

“完全正向保密” (PFS) 是一种用于派生出与前述密钥无关的独立的 “第 2 阶段” 密钥的方法。此外，“第 1 阶段” 提议将创建一个密钥 (SKEYID_d 密钥)，所有 “第 2 阶段” 密钥都由该密钥派生而来。 SKEYID_d 密钥可以用最小的 CPU 处理过程生成 “第 2 阶段” 密钥。遗憾的是，如果某个未授权方获得 SKEYID_d 密钥的访问权，将泄漏所有的加密密钥。

PFS 通过对每个 “第 2 阶段” 通道强制执行新的 Diffie-Hellman 密钥交换来解决此安全风险。尽管在启用 PFS 后，“第 2 阶段” 中的重定密钥过程可能会需要稍长的时间，但使用 PFS 更安全。

回放攻击保护

当有人截取一系列数据包并在以后使用该数据包大量攻击系统 (将导致拒绝服务 (DoS)) 或获准进入可信任网络时会发生回放攻击。回放攻击保护功能将促使 NetScreen 设备对每一个 IPSec 数据包进行检查，以查看以前是否接收过此数据包。如果数据包在指定的序列范围外到达， NetScreen 设备将拒绝此数据包。

IKE 和 IPSEC 数据包

IPSec VPN 通道包含两个主要元素：

- **通道设置：** 对等方首先建立安全联盟 (SA)，以定义可确保它们之间信息流安全的参数。每端的管理员都可手动定义 SA，也可通过 IKE “阶段 1” 和 “阶段 2” 协商动态定义 SA。“阶段 1” 可以发生在 Main mode (主模式) 或 Aggressive mode (主动模式) 下。“阶段 2” 总是发生在 Quick mode (快速模式) 下。
- **应用的安全：** IPSec 通过使用在 SA (通道设置过程中已获得对等方的同意) 中定义的安全参数来保护两个通道端点之间发送的信息流。可将 IPSec 应用到以下两种模式 — 传送模式和通道模式。这两种模式均支持以下两种 IPSec 协议 — “封装安全性负荷 (ESP)” 和 “认证包头 (AH)”。

欲进一步了解在 VPN 通道的 IKE 和 IPSec 阶段所发生的数据包处理过程，请参阅涉及 IKE 和 IPSec 的数据包包头的以下各节。

IKE 数据包

当明文数据包到达要求通道的 NetScreen 设备，且不存在针对该通道的活动 “阶段 2” SA 时，NetScreen 设备将开始 IKE 协商 (并丢弃该数据包[6])。IP 数据包包头中的源地址和目标地址分别是本地和远程 IKE 网关的地址。在 IP 数据包负荷中，存在一个封装有 ISAKMP (IKE) 数据包的 UDP 段。IKE 数据包的格式在 “阶段 1” 和 “阶段 2” 中相同。

IKE 数据包
(对于 “阶段 1” 和 “阶段 2”)

注意：ISAKMP 是 IKE 所使用的数据包格式。

6. 当初始 IP 数据包被丢弃后，源主机将重新发送它。通常，当第二个数据包到达 NetScreen 设备时，IKE 协商已完成，且 NetScreen 设备会在转发该数据包之前使用 IPSec 对其进行保护，同时还将保护会话中的所有后续数据包。

IP 包头

版本	包头长度	服务类型	数据包长度总计 (以字节为单位)			
标识			0	D	M	片段偏移
活动时间 (TTL)		协议 (**对于 UDP，应为 17**)	包头校验和			
源地址 (本地对等方网关)						
目标地址 (远程对等方网关)						
IP 选项 (如果有)						扩展位
IP 负荷						

UDP 包头

源端口 (**对于 IKE，应为 500**)	目标端口 (**对于 IKE，应为 500**)
长度	校验和
UDP 负荷	

ISAKMP 包头 (对于 IKE)

发起方的 Cookie				
响应方的 Cookie (对于第一个数据包，应为				
下一个负荷	主要版本	次要版本	交换类型	标志
消息 ID				
消息长度				
ISAKMP 负荷				

“下一个负荷”字段中包含可表示以下任一负荷类型的号码：

- 0002 – SA 协商负荷；包含 “阶段 1” 和 “阶段 2” SA 的定义
- 0004 – 提议负荷；可以是 “阶段 1” 或 “阶段 2” 提议
- 0008 – 转换负荷；转换负荷在提议负荷中被封装，而提议负荷在 SA 负荷中被封装
- 0010 – 密钥交换 (KE) 负荷；包含执行密钥交换所必需的信息，例如 Diffie-Hellman 公开值
- 0020 – 标识 (IDx) 负荷
  - 在 “阶段 1” 中， IDii 表示发起方 ID，而 IDir 表示响应方 ID
  - 在 “阶段 2” 中， IDui 表示用户发起方，而 IDur 表示用户响应方

    ID 为 IKE ID 类型，例如 FQDN、 U-FQDN、 IP 地址以及 ASN.1_DN。
- 0040 – 证书 (CERT) 负荷
- 0080 – 证书申请 (CERT_REQ) 负荷
- 0100 – 散列 (HASH) 负荷；包含特定散列功能的摘要输出
- 0200 – 签名 (SIG) 负荷；包含数字签名
- 0400 – 当前数 (Nx) 负荷；包含交换必需的伪随机信息
- 0800 – 通知负荷
- 1000 – ISAKMP 删除负荷
- 2000 – 供应商 ID (VID) 负荷；可包含在 “阶段 1” 协商的任意位置。 NetScreen 用它来标记对 NAT-T 的支持。

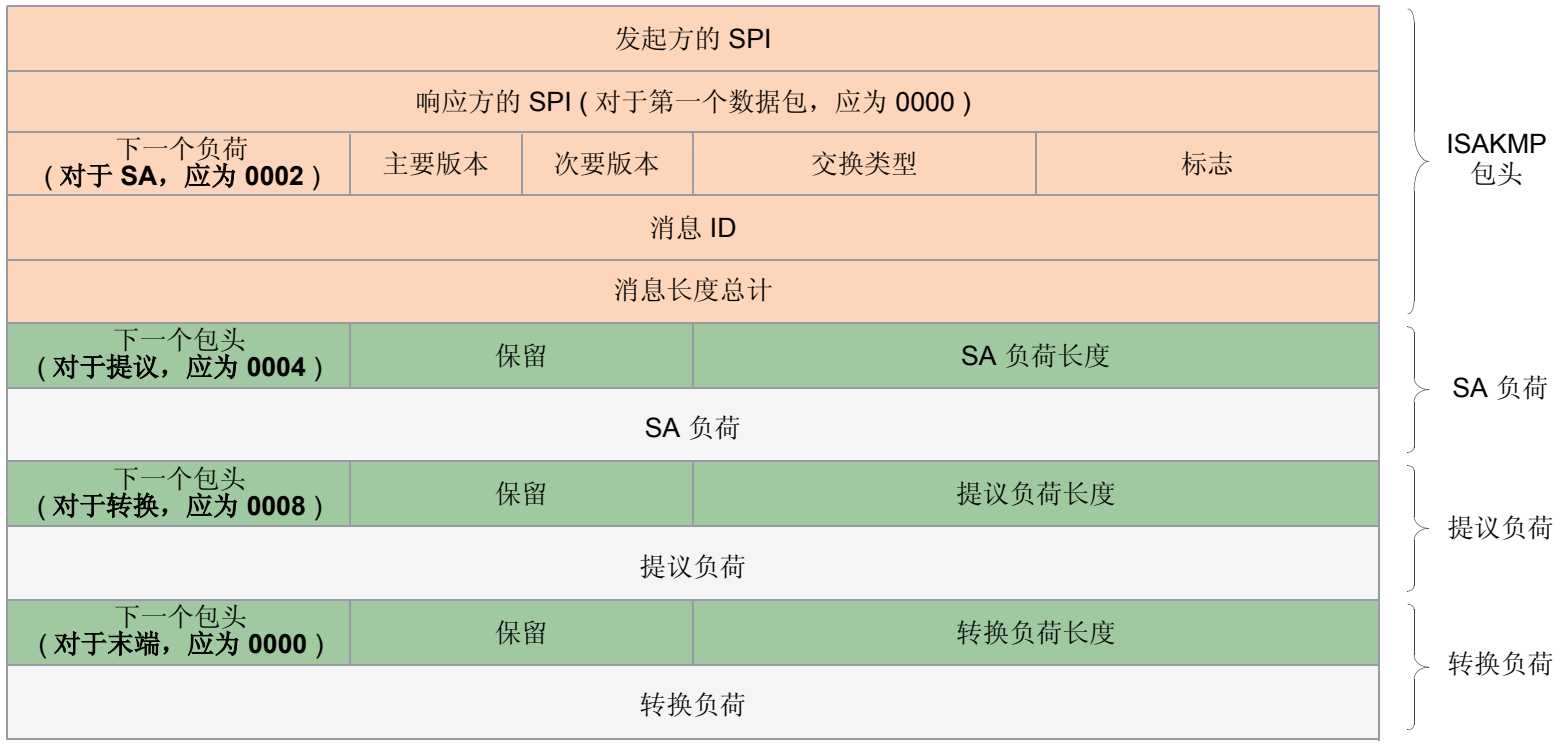
所有 ISAKMP 负荷均以相同的通用包头开始：

通用 ISAKMP 负荷包头

下一个包头	保留	负荷长度 (以字节为单位)
负荷		

可存在链接在一起的多个 ISAKMP 负荷，每个后续的负荷类型由 “下一个包头”字段中的值进行标明。值 0000 表示最后一个 ISAKMP 负荷。请参阅以下图表范例：

具有通用 ISAKMP 负荷的 ISAKMP 包头



IPSec 数据包

完成 IKE 协商且两个 IKE 网关已建立“阶段 1”和“阶段 2”安全联盟 (SA) 后，NetScreen 设备将 IPSec 保护应用到后续明文 IP 数据包 (即由位于一个 IKE 网关后面的主机发送给位于另外一个网关后面的主机的数据包) 中 (假设该策略允许信息流)。如果“阶段 2” SA 在通道模式下指定了“封装安全性协议 (ESP)”，则数据包如下所示[7]。请注意 : NetScreen 设备将两个附加包头添加到了由启动主机发送的初始数据包中。

IPSec 数据包 –
通道模式下的 “封装安全性负荷 (ESP)”

如上图所示，由启动主机构建的数据包包括负荷、 TCP 包头和内部 IP 包头 (IP1)。

由 NetScreen 设备添加的外部 IP 包头 (IP2) 中含有作为目标 IP 地址的远程网关的 IP 地址和作为源 IP 地址的本地 NetScreen 设备的 IP 地址。NetScreen 设备还在外部和内部 IP 包头之间添加了一个 ESP 包头。ESP 包头包含了有关允许远程对等方在接收到数据包时对其进行适当处理的信息。

7. 有关 ESP 的信息，请参阅第 8 页上的 “ESP”。有关通道模式的信息，请参阅第 5 页上的 “通道模式”。

外部 IP 包头 (IP2)

版本	包头长度	服务类型	数据包长度总计 (以字节为单位)			
标识			0	D	M	片段偏移
活动时间 (TTL)		协议 (**对于 UDP，应为 50**)	包头校验和			
源地址 (本地对等方的网关)						
目标地址 (远程对等方的网关)						
IP 选项 (如果有)						扩展位
负荷						

ESP 包头

* = 数据包的已认证部分
‡ = 数据包的已加密部分

“下一个包头”字段表明了负荷字段中的数据类型。在通道模式下，该值为 4，表示 IP-in-IP。如果将 ESP 应用于传送模式，则该值表示的是传输层协议，例如 : 6 表示 TCP， 17 表示 UDP。

内部 IP 包头 (IP1)

版本	包头长度	服务类型	数据包长度总计 (以字节为单位)			
标识			0	D	M	片段偏移
活动时间 (TTL)		协议 (**对于 TCP，应为 6**)	包头校验和			
源地址 (启动主机)						
目标地址 (接收主机)						
IP 选项 (如果有)						扩展位
负荷						

TCP 包头

源端口								目标端口
序列号								
确认编号								
包头长度	保留	URG	ACK	PSH	RST	SYN	FIN	窗口大小
校验和								紧急指针
选项 (如果有)								扩展位
数据								

2

公开密钥密码术

本章介绍了公开密钥密码术，并介绍了在 “公开密钥基础” (PKI) 的环境中如何使用证书和证书撤消列表 (CRL)。本章内容共分为以下几个部分：

公开密钥密码术简介

在公开密钥密码术中，使用公开 / 私有密钥对来加密和解密数据。用公开密钥 (所有者可将其公开使用) 加密的数据只能用相应的私有密钥 (所有者秘密持有并加以保护) 进行解密。例如，如果 Alice 想给 Bob 发送加密的消息，Alice 可用 Bob 的公开密钥来加密此消息，并发送给他。然后， Bob 用自己的私有密钥将此消息解密。

反之亦然。也就是说，用私有密钥加密数据，用相应的公开密钥将数据解密。这就是通常所说的创建数字签名。例如，如果 Alice 想以她本人的身份作为消息发送方，则可用她的私有密钥来加密消息并发送给 Bob。然后， Bob 用 Alice 的公开密钥将消息解密，从而验证了 Alice 确实是发送方。

公开 / 私有密钥对在数字证书的使用方面也起着重要作用。签署证书 (由证书授权机构执行)，然后验证签名 (由接收方执行) 的过程如下所述 :

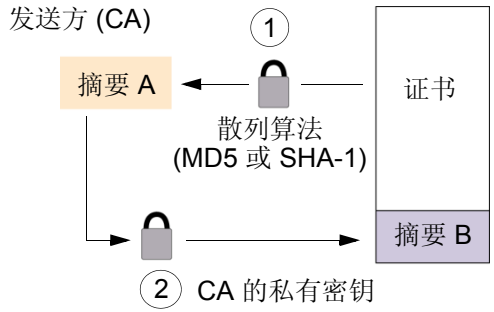
签署证书

1. 发布证书的 “证书授权机构” (CA) 用散列算法 (SHA-1 或 MD5) 来散列证书，以生成摘要。
2. 然后 CA “签署” 证书，方法是用其私有密钥加密摘要。结果即是数字签名。
3. 然后由 CA 为申请证书的用户发送经过数字签名的证书。

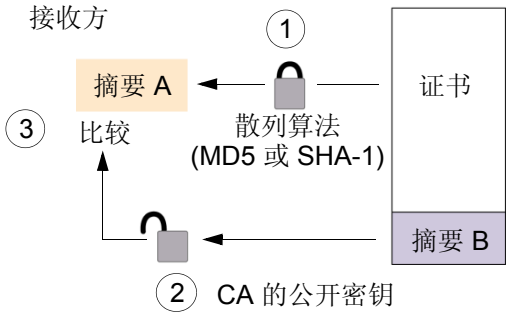
验证数字签名

1. 接收方获得证书后，还会生成另一摘要，方法是在证书文件中，应用同一散列算法 (SHA-1 或 MD5)。
2. 接收方使用 CA 的公开密钥将数字签名解密。
3. 接收方将解密的摘要和刚生成的摘要进行比较。如果这两个摘要匹配，接收方就能确认 CA 签名完整，进而确认了相应证书的完整性。

1. CA 使用 MD5 或 SHA-1 散列算法从该证书生成摘要。
2. CA 使用其私有密钥来加密摘要 A。结果即是数字签名摘要 B。
3. CA 为申请证书的用户发送经过数字签名的证书。



1. 接收方使用 MD5 或 SHA-1 从该证书生成摘要 A。
2. 接收方使用 CA 的公开密钥将摘要 B 解密。
3. 接收方将摘要 A 与摘要 B 进行比较。如果匹配，接收者即确认证书尚未被篡改。

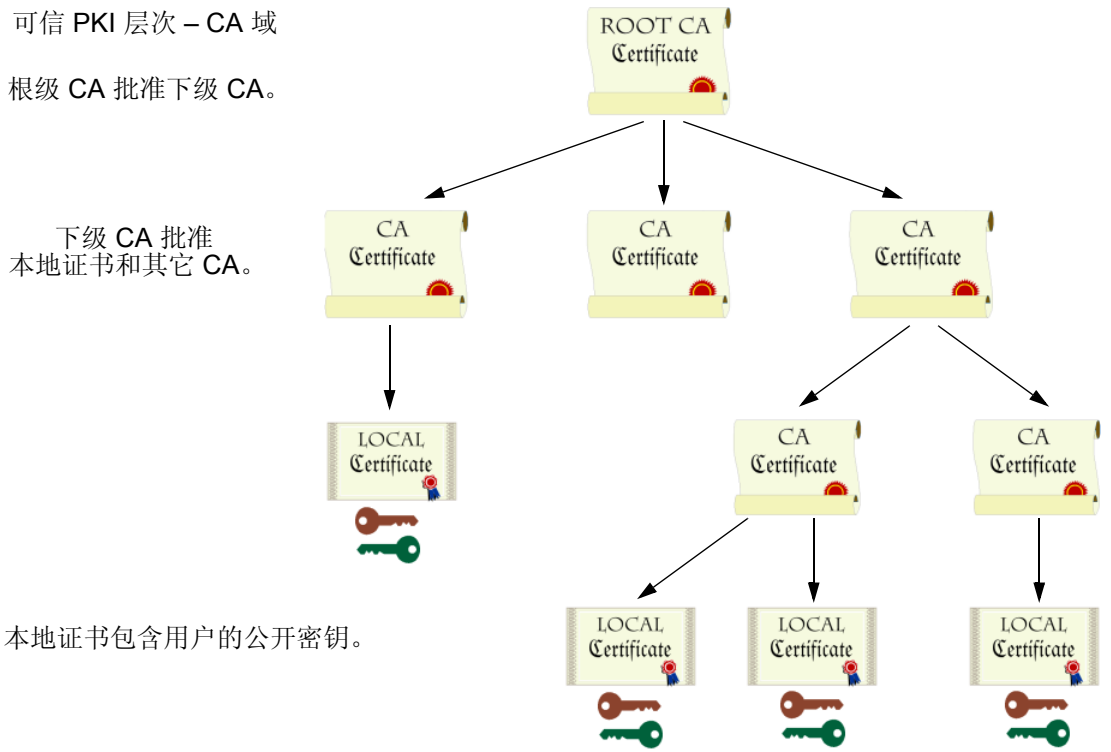


在 IKE 会话中，两个参与者之间发送数字签名消息的过程非常相似，以下为不同之处：

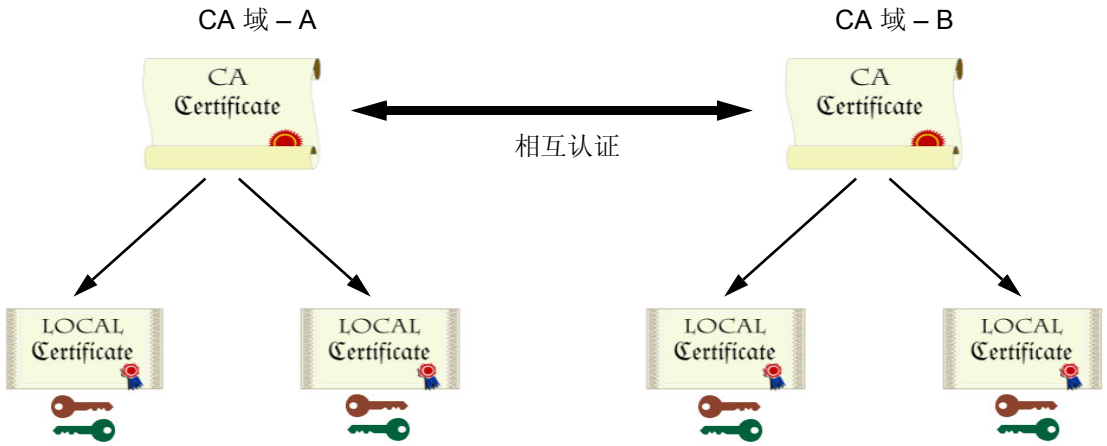
- 发送方不从 CA 证书生成摘要，而是从 IP 数据包负荷中的数据生成。
- 参与者不使用 CA 的公开 / 私有密钥对，而是使用发送方的公开 / 私有密钥对。

PKI

术语 “公开密钥基础” (PKI) 是指为成功执行公开密钥密码术所需的信任层次结构。要验证证书的可信度，必须能跟踪已认证的 CA 的路径 (从发布本地证书的 CA 回溯到 CA 域的根机构)。



如果仅将证书用于某个组织内，则该组织可拥有其自己的 CA 域，在该域内，公司 CA 在员工中发布并批准证书。如果该组织随后希望其员工能与另一 CA 域内的员工 (如，同样拥有其自己 CA 域的另一组织中的员工) 交换证书，则这两个 CA 可进行相互认证。即，他们同意彼此信任对方的权限。在此情况下， PKI 结构水平延伸而不垂直延伸。



由于这些 CA 彼此进行了相互认证，因此， CA 域 A 中的用户可与 CA 域 B 中的用户共同使用其证书和密钥对。

为了方便和实用起见，必须对 PKI 进行透明管理和实施。为达到此目标， NetScreen ScreenOS 做了以下工作 :

1. 创建证书申请时，生成公开 / 私有密钥对。
2. 提供了以文本文件形式存在的、作为证书申请一部分的公开密钥，以传输到 “证书认证机构” (CA) 进行证书注册 (PKCS10 文件)。

3. 支持将本地证书、 CA 证书以及证书撤消列表 (CRL)[1] 加载到设备中。

   也可指定在线刷新 CRL 的时间间隔。有关 CRL 的详细信息，请参阅第 29 页上的 “证书和 CRL”。

4. 建立 IPSec 通道时提供证书传输。
5. 支持在 PKI 层次结构中向上通过八级 CA 授权机构的证书路径验证。
6. 支持 PKCS #7 加密标准，表明 NetScreen 设备能接受 X.509 证书及 PKCS #7 封套内数据包的 CRL[2]。PKCS #7 支持在单个 PKI 请求内提交多个 X.509 证书。现在，可将 PKI 配置为从发布证书的 CA 一次批准提交的所有证书。
7. 支持通过 LDAP 或 HTTP 的在线 CRL 检索。

1. “证书授权机构”通常提供 CRL。尽管能将 CRL 加载到 NetScreen 设备中，但仍不能在加载后对其进行查看。
2. NetScreen 支持最多 7 千字节大小的 PKCS #7 文件。

证书和 CRL

数字证书是一种用来通过可信任第三方 (即通常所说的 “证书授权机构” (CA)) 来验证您的身份的方式。所用的 CA 服务器可由独立 CA[3] 或由您自己的组织 (在此情况下，您成为自己的 CA) 所拥有并对其进行操作。如果使用独立的 CA，必须与之联系以获取 CA 和 CRL 服务器的地址 (用于获取证书及证书撤消列表) 以及提交个人证书申请时所需的信息。当您是自己的 CA 时，由您自行确定此信息。

***注意：** ScreenOS 中含有一个 CA 证书，可使用该证书对从防病毒 (AV) 模式文件服务器和 “深入检查” (DI) 攻击对象数据库服务器下载进行认证。有关防病毒模式文件服务器的详细信息，请参阅第 **4**-81 页上的 “防病毒扫描”。有关 “深入检查” 攻击对象数据库服务器的详细信息，请参阅第 **4**-137 页上的 “攻击对象数据库服务器”。*

要在建立安全 VPN 连接时使用数字证书对您的身份进行认证，必须首先执行以下操作：

- 在 NetScreen 设备上生成密钥，将其发送给 CA 以获取个人证书 (即通常所说的*本地*证书)，并将此证书加载到 NetScreen 设备上。
- 为发布个人证书的 CA 获取 CA 证书 (主要用来验证可对您进行身份验证的 CA 的身份)，并将该证书加载到 NetScreen 设备中。可手动执行此任务，也可通过 “简单证书注册协议” (SCEP) 自动执行。
- 如果该证书不包含证书分布点 (CDP) 扩展名，并且不能通过 LDAP 或 HTTP 自动检索 CRL，则可手动检索 CRL，并将其加载到 NetScreen 设备中。

在交易过程中，有一些事件要求必须撤消证书。当怀疑证书已失效，或者当证书持有者离开公司时，您可能希望撤消证书。可在本地实现对证书撤消和验证的管理 (此为受限制的解决方案)，也可通过引用 CA 的 CRL (可按每天、每周或每月的时间间隔或按 CA 设置的缺省时间间隔自动在线访问此 CRL) 来进行管理。

3. NetScreen 支持以下 CA: Baltimore、 Entrust、 Microsoft、 Netscape、 RSA Keon 和 Verisign。

手动获取证书

要使用手动方法获取经过签名的数字证书，必须按以下顺序完成几项任务：

1. 生成公开 / 私有密钥对。
2. 填写证书申请。
3. 将申请提交给所选的 CA。
4. 收到经过签名的证书后，必须将其与 CA 证书一起加载到 NetScreen 设备中。

这样您就拥有了具有下列用途的相应证书：

- NetScreen 设备的本地证书，针对每个通道连接验证您的身份
- CA 证书 (其公开密钥)，用来验证对等方的证书
- 如果 CA 证书[4] 中含有 “证书撤消列表” (CRL)，则由 CRL 来确定无效的证书

收到这些文件 (证书文件通常具有扩展名 .cer，而 CRL 通常具有扩展名 .crl) 后，请按照下一小节所述步骤将它们加载到 NetScreen 中。

注意：*如果打算使用电子邮件来提交 PKCS10 文件，以获取证书，必须正确配置 NetScreen 设置，这样就能给系统管理员发送电子邮件。必须设置一级 DNS 服务器和二级 DNS 服务器，并指定 SMTP 服务器及电子邮件地址设置。*

4. CA 证书可能带有一个 CRL，并且被存储在 NetScreen 数据库中。或者，CA 证书可能包含存储在 CA 的数据库中的 CRL 的 CRL URL (LDAP 或 HTTP)。如果通过两种方法都无法获得 CRL，可在 NetScreen 设备中手动输入 CRL URL 的缺省服务器设置，如第 36 页上的 “范例：配置 CRL 设置”中所述。

范例 : 手动证书申请

申请证书时， NetScreen 设备将生成一个密钥对。公开密钥合并在申请中，并且最终合并在从 CA 收到的经过数字签名的本地证书中。

下例中，安全管理员为 Juniper Networks 开发部 (位于加利福尼亚 Sunnyvale) 的 Michael Zhang 生成证书申请。此证书将被 IP 地址为 10.10.5.44 的 NetScreen 设备使用。管理员指示 NetScreen 设备通过电子邮件将申请发送到安全管理员的邮箱 *admin@juniper.net*。然后，安全管理员再将此申请复制并粘贴到 CA 证书注册网站下的证书申请文本字段中。完成注册后， CA 往往会通过电子邮件将证书发送回安全管理员。

注意: *生成证书申请前，请确认已经设置了系统时钟，并已为 NetScreen 设备分配了主机名和域名。(如果 NetScreen 设备在 NSRP 集群中，则用集群名替换主机名。有关详细信息，请参阅第* ***10****-18 页上的 “集群名称”。)*

WebUI

1. 证书生成

Objects > Certificates > New: 输入以下内容，然后单击 **Generate**:

Name: Michael Zhang

Phone: 408-730-6000

Unit/Department: Development

Organization: Juniper Networks

County/Locality: Sunnyvale

State: CA

Country: US

E-mail: mzhang@juniper.net[5]

IP Address: 10.10.5.44

Write to file: (选择)

RSA: (选择)

Create new key pair of *1024*[6] length: (选择)

NetScreen 生成 PKCS #10 文件，并提示您通过电子邮件发送此文件，并将其保存到磁盘上，或通过 “简单证书注册协议” (SCEP) 自动注册。

选择 **E-mail to** 选项，键入 **admin@juniper.net**，然后单击 **OK**[7]。

2. 证书申请

安全管理员打开该文件并复制其内容 (必须复制整个文本内容，但不包括文本前后的任何空白)。 (开始于 “-----BEGIN CERTIFICATE REQUEST-----”，结束于 “-----END CERTIFICATE REQUEST-----”。)

然后，安全管理员按照 CA 网站上的证书申请说明将 PKCS #10 文件粘贴到相应的字段中 (需要时)。

3. 证书检索

安全管理员通过电子邮件接收到来自 CA 的证书后，随即将其转发给您。将其复制到文本文件，并保存到您的工作站 (随后将通过 WebUI 加载到 NetScreen 设备)，或保存到 TFTP 服务器 (随后将通过 CLI 进行加载)。

5. 某些 CA 不支持证书中的电子邮件地址。如果本地证书申请中不含有电子邮件地址，则作为动态对等方配置 NetScreen 设备时，就不能将电子邮件地址用作本地 IKE (因特网密钥交换) ID。而应使用完全合格的域名 (如果本地证书中存在)，或者使本地 ID 字段为空。缺省情况下， NetScreen 设备将发送其 hostname.domainname (主机名 . 域名)。如果未指定动态对等方的本地 ID，则应在对等方 ID 字段中输入位于 IPSec 通道另一端设备上的该对等方的 hostname.domainname。
6. 值 1024 表示密钥对的位长。如果使用 SSL 的证书 (请参阅第 **3**-7 页上的 “安全套接字层”)，请确保使用 Web 浏览器也同样支持的位长。
7. 使用电子邮件地址时，将假定您已经为 SMTP 服务器配置了 IP 地址 : **set admin mail server-name** { *ip_addr* **|** *dom_name* }。

CLI

1. 证书生成

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@juniper.net
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name "Santa Clara"
set pki x509 dn name "Michael Zhang"
set pki x509 dn org-name "Juniper Networks"
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
set pki x509 default send-to admin@juniper.net[8]
exec pki rsa new-key 1024
```

会通过电子邮件将证书申请发送到 admin@juniper.net。

2. 证书申请

安全管理员打开该文件并复制其内容 (必须复制整个文本内容，但不包括文本前后的任何空白)。(开始于 "-----BEGIN CERTIFICATE REQUEST-----"，结束于 "-----END CERTIFICATE REQUEST-----"。)

然后，安全管理员按照 CA 网站上的证书申请说明将 PKCS #10 文件粘贴到相应的字段中 (需要时)。

3. 证书检索

安全管理员通过电子邮件接收到来自 CA 的证书后，随即将其转发给您。将其复制到文本文件，并保存到您的工作站 (随后将通过 WebUI 加载到 NetScreen 设备)，或保存到 TFTP 服务器 (随后将通过 CLI 进行加载)。

8. 使用电子邮件地址时，将假定您已经为 SMTP 服务器配置了 IP 地址 : **set admin mail server-name** { *ip_addr* | *dom_name* }。

范例 : 加载证书和 CRL

CA 将返回以下三个文件，以便可将其加载到 NetScreen 设备 :

- CA 证书，该证书中含有 CA 的公开密钥
- 可标识本地机器的本地证书 (您的公开密钥)
- CRL，该列表中列有被 CA 撤消的所有证书

对于 WebUI 范例，已将这些文件下载到了管理员工作站上名为 C:\certs\ns 的目录。对于 CLI 范例，已下载了 IP 地址为 198.168.1.5 的 TFTP 服务器上的 TFTP 根目录。

注意 : *用 ScreenOS 2.5 或更新版本配置的 NetScreen 设备 (包括虚拟系统) 支持加载从不同的 CA 获取的多个本地证书。*

此例说明如何加载两个名为 auth.cer (CA 证书) 和 local.cer (您的公开密钥) 的证书文件，以及名为 distrust.crl 的 CRL 文件。

WebUI

1. Objects > Certificates: 选择 **Load Cert**，然后单击 **Browse**。
2. 找到 C:\certs 目录，选择 **auth.cer**，然后单击 **Open**。

   目录路径和文件名 (C:\certs\ns\auth.cer) 将显示在 File Browse 字段中。
3. 单击 **Load**。

   auth.cer 证书文件即被加载。
4. Objects > Certificates: 选择 **Load Cert**，然后单击 **Browse**。
5. 找到 C:\certs 目录，选择 **local.cer**，然后单击 **Open**。

   目录路径和文件名 (C:\certs\ns\local.cer) 将显示在 File Browse 字段中。

6. 单击 **Load**。

   local.cer 证书文件即被加载。

7. Objects > Certificates: 选择 **Load CRL**，然后单击 **Browse**。
8. 找到 C:\certs 目录，选择 **distrust.crl**，然后单击 **Open**。
9. 单击 **Load**。

   distrust.crl CRL 文件即被加载。

CLI

```
exec pki x509 tftp 198.168.1.5 cert-name auth.cer
exec pki x509 tftp 198.168.1.5 cert-name local.cer
exec pki x509 tftp 198.168.1.5 crl-name distrust.crl
```

范例 : 配置 CRL 设置

在第 1 阶段协商中，参与者检查 CRL 列表以查看 IKE 交换期间收到的证书是否仍然有效。如果 CA 证书没有随附 CRL，并且未将 CRL 加载到 NetScreen 数据库中，则 NetScreen 设备会尝试通过 LDAP 或 HTTP[9] CRL 位置 (在 CA 证书内定义) 来检索 CRL。如果未在 CA 证书内定义 URL 地址， NetScreen 设备会使用为该 CA 证书定义的服务器的 URL。如果没有为特定的 CA 证书定义 CRL URL， NetScreen 设备会引用缺省 CRL URL 地址处的 CRL 服务器。

注意 : *对于 ScreenOS 2.5 及更新版本，可以在加载 CRL 时禁止对 CRL 数字签名的检查。但是，禁止 CRL 证书检查会影响 NetScreen 设备的安全性。*

在本例中，先配置 Entrust CA 服务器，以每天检查 CRL，方法是连接到地址为 2.2.2.121 的 LDAP 服务器，并查找 CRL 文件。然后配置缺省证书验证设置，以便使用地址为 10.1.1.200 的公司的 LDAP 服务器，并每天检查 CRL。

注意 : *Entrust CA 证书的索引 (IDX) 号为 1。要查看加载到 NetScreen 设备上的所有 CA 证书的索引号列表，请使用以下 CLI 命令 :* ***get pki x509 list ca-cert****。*

WebUI

Objects > Certificates (Show: CA) > Server Settings (对于 NetScreen): 输入以下内容，然后单击 **OK**:

X509 Cert_Path Validation Level: Full

CRL Settings:

URL Address: ldap:///CN=Entrust,CN=en2001,CN=PublicKeyServices, CN=Services,CN=Configuration,DC=EN2001,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint

LDAP Server: 2.2.2.121

Refresh Frequency: Daily

9. X509 证书中的 CRL 分布点扩展名 (.cdp) 可以是 HTTP URL 或 LDAP URL。

Objects > Certificates > Default Cert Validation Settings: 输入以下内容，然后单击 **OK**:

X509 Certificate Path Validation Level: Full

Certificate Revocation Settings:

Check Method: CRL

URL Address: ldap:///CN=NetScreen,CN=safecert,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=SAFECERT,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint

LDAP Server: 10.1.1.200

CLI

```
set pki authority 1 cert-path full
set pki authority 1 cert-status crl url "ldap:///CN=Entrust,CN=en2001,
    CN=PublicKeyServices,CN=Services,CN=Configuration,DC=E
    N2000,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoin
    t"
set pki authority 1 cert-status crl server-name 2.2.2.121
set pki authority 1 cert-status crl refresh daily
set pki authority default cert-path full
set pki authority default cert-status crl url "ldap:///CN=NetScreen,
    CN=safecert,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=SAFECERT,
    DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint"
set pki authority default cert-status crl server-name 10.1.1.200
set pki authority default cert-status crl refresh daily
save
```

自动获取本地证书

要在建立安全 VPN 连接时使用数字证书来验证您的身份，必须先进行以下操作：

- 获取打算从中获得个人证书的证书授权机构 (CA) 证书，然后将该 CA 证书加载到 NetScreen 设备中。
- 从先前已经加载了其 CA 证书的 CA 中获取本地证书 (即通常所说的个人证书)，然后将该本地证书加载到 NetScreen 设备中。可手动执行此任务，或使用 “简单证书注册协议” (SCEP) 来自动执行。

由于手动申请本地证书的方法中具有要求您在证书间复制信息的步骤，因此其过程可能稍长。要绕过这些步骤，可使用自动方法。

注意：*使用 SCEP 之前，必须执行以下任务：*

- *配置并启用 DNS (请参阅第* ***2****-359 页上的 “域名系统支持”)。*
- *设置系统时钟 (请参阅第* ***2****-443 页上的 “系统时钟”)。*
- *为 NetScreen 设备分配主机名和域名。(如果 NetScreen 设备在 NSRP 集群中，则用集群名替换主机名。有关详细信息，请参阅第* ***10****-18 页上的 “集群名称”。)*

范例 : 自动证书申请

在本例中，将使用自动方法来申请本地证书。将使用带有 Verisign CA 的 “简单证书注册协议” (SCEP)。设置以下 CA 设置 :

- 完整证书路径验证
- RA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe[10]
- CA CGI: http://ipsec.verisign.com/cgi-bin/pkiclient.exe
- 自动确认 CA 证书的完整性
- CA ID，标识 SCEP 服务器，其中 Verisign SCEP 服务器使用域名，如 juniper.net 或 Verisign 为贵公司设置的域
- 质询密码
- 每隔三十分钟即进行一次自动证书轮询 (缺省为不轮询)

然后生成 RSA 密钥对，指定 1024 位的密钥长度，并启动 SCEP 操作，以便用上述 CA 设置从 Verisign CA 申请本地证书。

使用 WebUI 时，按名称引用 CA 证书。使用 CLI 时，按索引 (IDX) 号引用 CA 证书。在本例中， Verisign CA 的索引号为 “1”。要查看 CA 证书的索引号，请使用以下命令 : **get pki x509 list ca-cert**。输出内容显示每个证书的索引号和 ID 号。记下索引号，并且在命令中引用 CA 证书时使用该索引号。

10. 对于网络服务器来说，“通用网关接口” (CGI) 是将用户申请传递到应用程序并接收返回数据的标准方法。CGI 是 “超文本传输协议” (HTTP) 的一部分。即使不存在 RA，也必须指定 RA CGI 路径。如果 RA 不存在，使用为 CA CGI 指定的值。

WebUI

1. CA 服务器设置

Objects > Certificates > Show CA > Server Settings (对于 Verisign): 输入以下内容，然后单击 **OK**:

X509 certificate path validation level: Full

SCEP Settings:

RA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe

CA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 “CA 服务器设置”配置页：

Polling Interval: 30

Certificate Authentication: Auto

Certificate Renew: 14

2. 本地证书申请

Objects > Certificates > New: 输入以下内容，然后单击 **Generate**:

Name: Michael Zhang

Phone: 408-730-6000

Unit/Department: Development

Organization: Juniper Networks

County/Locality: Sunnyvale

State: CA

Country: US

Email: mzhang@juniper.net

IP Address: 10.10.5.44

Key Pair Information

RSA: (选择)

创建长度为 **1024**[11] 位的新密钥对。

发出 CLI 命令 **get pki x509 pkcs**，使 NetScreen 设备生成 PKCS #10 文件，然后执行以下操作之一：

- 发送 PKCS #10 证书申请文件到一个电子邮件地址
- 将其保存到磁盘
- 通过将该文件发送到支持 “简单证书注册协议” (SCEP) 的 CA 来自动注册

3. 自动注册

选择 **Automatically enroll to** 选项，选择 **Existing CA server settings** 选项，然后从下拉列表中选择 **Verisign**。

请与 Verisign 联系，将您的证书申请告知他们。只有在他们批准该证书申请后，您才能下载证书。

11. 值 1024 表示密钥对的位长度。如果使用 SSL 的证书，请确认使用 Web 浏览器支持的位长。

CLI

1. CA 服务器设置

```
set pki authority 1 cert-path full
set pki authority 1 scep ca-cgi "http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe"[12]
set pki authority 1 scep ra-cgi "http://ipsec.verisign.com/cgi-bin
    /pkiclient.exe"[13]
set pki authority 1 scep polling-int 30
set pki authority 1 scep renew-start 14
```

2. 本地证书申请

```
set pki x509 dn country-name US
set pki x509 dn email mzhang@juniper.net
set pki x509 dn ip 10.10.5.44
set pki x509 dn local-name "Santa Clara"
set pki x509 dn name "Michael Zhang"
set pki x509 dn org-name "Juniper Networks"
set pki x509 dn org-unit-name Development
set pki x509 phone 408-730-6000
set pki x509 dn state-name CA
exec pki rsa new 1024
```

3. 自动注册

```
exec pki x509 scep 1
```

如果该申请为来自该 CA 的第一个证书申请，则会出现一个提示，显示 CA 证书的指印值。必须与 CA 联系，以确认其为正确的 CA 证书。

请与 Verisign 联系，将您的证书申请告知他们。只有在他们批准该证书申请后，您才能下载证书。

12. 对于网络服务器来说，“通用网关接口” (CGI) 是将用户申请传递到应用程序并接收返回数据的标准方法。 CGI 是 “超文本传输协议” (HTTP) 的一部分。

13. 即使不存在 RA，也必须指定 RA CGI 路径。如果 RA 不存在，使用为 CA CGI 指定的值。

自动证书更新

可使 NetScreen 设备自动更新其通过 SCEP (简单证书注册协议) 获得的证书。此功能使您在 NetScreen 设备上的证书到期之前，不必记着要对证书进行更新。同时，通过同一标记，该功能可帮助您总是维持有效的证书。

缺省情况下，将禁用此功能。可以配置 NetScreen 设备，使其在证书到期之前自动发送更新证书的请求。可以使用日期数和分钟数来设置时间，让 NetScreen 设备在证书到期前发送证书更新请求。通过为每个证书设置不同的时间来防止 NetScreen 设备同时更新所有证书。

要让此功能正常运行， NetScreen 设备必须能够访问 SCEP 服务器，并且在更新时， NetScreen 设备上必须存在证书。而且，要让此功能正常运行，您还必须确保发布证书的 CA 可以执行以下操作 :

- 支持自动批准证书申请。
- 返回相同的 DN (域名)。换句话说， CA 不能修改新证书中的主题名称和 SubjectAltName 扩展名。

对所有 SCEP 证书或每个证书，您可以启用和禁用 SCEP 证书自动更新功能。

密钥对生成

NetScreen 设备将预先生成的密钥保存在内存中。预先生成的密钥的数量取决于设备型号。正常操作过程中，NetScreen 设备每次使用密钥时都会生成一个新密钥，从而保证有足够的密钥来更新证书。生成密钥的过程往往注意不到，因为在需要密钥前，设备已生成了一个新密钥。如果 NetScreen 设备一次更新大量的证书，从而很快用完密钥，则可能会用完预先生成的密钥，并且不得不为每个新的请求快速生成密钥。在这种情况下，密钥的生成过程可能会影响 NetScreen 设备的性能。尤其是在 HA (高可用性) 环境下更是如此，此时， NetScreen 设备性能的降低时间可能会持续长达数分钟。

NetScreen 设备上预先生成的密钥对的数量取决于设备型号。有关详细信息，请参阅 NetScreen 产品的说明书。

使用 OCSP 的状态检查

当 NetScreen 设备执行一项使用证书的操作时，验证该证书的有效性通常很重要。证书过期或撤消证书都可能会导致证书失效。检查证书状态的缺省方法是使用证书撤消列表 (CRL)。也可使用 “在线证书状态协议” (OCSP) 来检查证书状态。 OCSP 可提供有关证书的其它信息，并可更加及时地对证书状态进行检查。

使用 OCSP 的 NetScreen 设备称为 *OCSP 客户端* (或 *请求方*)。该客户端将验证请求发送到被称为 *OCSP 响应方*的服务器设备中。ScreenOS 支持 RSA Keon 和 Verisign 作为 OCSP 响应方[14]。客户端的请求包含要检查的证书标识。只有在将 NetScreen 设备配置为能够识别 OCSP 响应方的位置之后， NetScreen 设备才能执行任意 OCSP 操作。

收到请求后， OCSP 响应方确认证书的状态信息可用，然后会将当前状态返回给 NetScreen 设备。 OCSP 响应方的响应包括证书的撤消状态、响应方的名称以及该响应的有效时间间隔。除非响应是一条错误消息，否则，响应方将使用响应方私有密钥来对响应进行签名。NetScreen 设备通过使用响应方的证书来验证响应方签名的有效性。响应方的证书既可以嵌入在 OCSP 响应中，也可以进行本地存储并在 OCSP 配置中指定。如果证书在本地存储，请使用以下命令指定本地存储的证书 :

```
set pki authority id_num1 cert-status ocsp cert-verify id id_num2
```

id_num1 标识发布已验证证书的 CA 证书，而 *id_num2* 标识设备用来验证 OCSP 响应签名的本地存储证书。

如果响应方的证书未嵌入 OCSP 响应或没有在本地存储，则 NetScreen 设备通过使用发布审议中的证书的 CA 证书来验证签名。

14. 在过去大量的评价过程中， Juniper Networks 还成功测试了 Valicert OCSP 响应方。

配置 OCSP

可使用 CLI 命令为 OCSP 配置 NetScreen 设备。多数 CLI 命令使用识别号码将撤消引用 URL 与 CA 证书相关联。可使用以下 CLI 命令来获取此 ID 号：

```
get pki x509 list ca-cert
```

注意：列出 CA 证书时， NetScreen 设备将 ID 号动态分配给 CA 证书。修改证书存储器后，可更改此 ID 号。

指定 CRL 或 OCSP

要为特定 CA 的证书指定撤消检查方法 (CRL、 OCSP 或不进行指定)，请使用以下 CLI 语法：

```
set pki authority id_num cert-status revocation-check { CRL | OCSP | none }
```

其中， *id_num* 是证书的识别号码。

以下范例指定 OCSP 撤消检查。

```
set pki authority 3 cert-status revocation-check ocsp
```

ID 号 3 标识 CA 的证书。

查看状态检查属性

要显示特定 CA 的状态检查属性，请使用以下 CLI 语法：

```
get pki authority id_num cert-status
```

其中， *id_num* 是由 CA 发布的证书的识别号码。

要显示发布了证书 7 的 CA 的状态检查属性，请使用以下 CLI 语法：

```
get pki authority 7 cert-status
```

指定 OCSP 响应方 URL

要指定特定证书 OCSP 响应方的 URL 字符串，请使用以下 CLI 语法：

```
set pki authority id_num cert-status ocsp url url_str
```

要指定 CA (其证书索引号为 5) 的 OCSP 响应方 (http:\\192.168.10.10) 的 URL 字符串，请使用以下 CLI 语法：

```
set pki authority 5 cert-status ocsp url http:\\192.168.10.10
```

要删除证书 5 的 CRL 服务器的 URL (http:\\192.168.2.1)，请使用以下语法：

```
unset pki authority 5 cert-status ocsp url http:\\192.168.2.1
```

删除状态检查属性

要删除 CA (发布了特定证书) 的所有证书状态检查属性，请使用以下语法：

```
unset pki authority id_num cert-status
```

要删除与证书 1 相关的所有撤消属性，请使用以下语法：

```
unset pki authority 1 cert-status
```

自签证书

自签证书是一种由签名实体发布给自身的证书，即发布者和证书主体相同。例如，所有根证书授权机构 (CA) 的 CA 证书都是自签证书。

如果还没有已配置 “安全套接字层 (SSL)” 的证书 (即，第一次启动时)，则 NetScreen 设备会在启动时自动生成自签证书。创建自动生成的自签证书的 NetScreen 设备是使用该自签证书的唯一设备。该设备从不将此证书导出到其外部。当与集群的其它成员中的 PKI 对象同步时，即使 NetScreen 设备位于 “NetScreen 冗余协议” (NSRP) 集群内，它也不会在和 Cluster 里的其他成员进行 PKI 信息同步时将自动生成的自签证书和其他类型的证书一样同步过去。(NSRP 成员确实能交换手动生成的自签证书。有关手动生成自签证书的信息，请参阅第 51 页上的 “手动创建自签证书”。)

虽然无法导出自动生成的自签证书，但可复制其主题名称和指印。然后将主题名称和指印发送给远程管理员，他们随后会用此信息来验证在 SSL 协商过程中接收到的自签证书。检查主题名称和指印是防止中间人 (man-in-the-middle) 攻击的重要预防措施。在此攻击中，某些人截取 SSL 连接尝试并通过响应其自己的自签证书来伪装为目标 NetScreen 设备。(有关验证自签证书的详细信息，请参阅第 49 页上的 “证书验证”。)

用 SSL 保护管理信息流

当创建到 NetScreen 设备的“安全套接字层”(SSL) 连接时，可使用自签证书。通过 WebUI 管理设备时，SSL 可提供认证和加密以保护您的管理信息流。甚至可配置 NetScreen 设备，将使用 HTTP (缺省端口 80) 的管理连接尝试重新定向到 SSL (缺省端口 443)。

***注意：**有关 SSL 的详细信息 (包括 HTTP-to-SSL 重新定向机制)，请参阅第 **3**-7 页上的 “安全套接字层”。*

缺省情况下， NetScreen 设备使自动生成的自签证书供 SSL 协商使用。它是缺省的 SSL 证书。如果随后安装了经 CA 签名的证书或配置了 NetScreen 设备以生成另一个自签证书[15]，那么，您可将这些证书中的一种证书用于 SSL。如果删除了自动生成的自签证书，但未分配用于 SSL 的另一个证书，则 NetScreen 设备将在下次启动时自动生成另一个自签证书[16]。

15. 有关如何创建另一个自签证书的信息，请参阅第 51 页上的 “手动创建自签证书”。
16. 有关如何删除自动生成的自签证书的信息，请参阅第 59 页上的 “删除自签证书”。

证书验证

在 SSL 握手期间， NetScreen 设备通过向 SSL 客户端发送证书来验证该证书。当 NetScreen 设备发送自签证书时，SSL 客户端无法通过检查发布的 CA 的签名来对其进行验证，因为任何 CA 都未发布它。尽管如此，当 NetScreen 设备提供用于建立 SSL 会话的自签证书时，管理员计算机上的 Web 浏览器会尝试用其 CA 存储器中的 CA 证书来验证它。当浏览器无法找到这样的授权机构时，它会显示类似下面的消息，提示管理员接受或拒绝所提供的证书：

当浏览器接收到自签证书时可能会出现的两种类型的安全警告。

如果是在初始启动后第一次连接到 NetScreen 设备，则系统时钟可能会不准确。因而，证书的有效周期也可能会不准确。即使设置了系统时钟并重新生成了自签证书， Web 浏览器也无法找到认证 CA，因此每次 NetScreen 设备使用自签证书建立 SSL 连接时，管理员都必须随时准备查看以上消息。

在未使用公正的第三方 CA 进行证书验证的情况下，通过 SSL 登录的管理员可能想知道所收到的自签证书是否确实来自他试图连接到的 NetScreen 设备。(毕竟，证书有可能来自使用中间人 (man-in-the-middle) 攻击以试图伪装成 NetScreen 设备的非法入侵者。) 管理员可通过使用自签证书的主题名称和指印来验证他所接收到的证书。可将主题名称和指印发送给管理员，这样当 NetScreen 设备以后提供自签证书以验证其自身时，管理员就可验证该自签证书。

要查看自动生成的自签证书的主题名称和指印，请使用以下命令[17]：

```
ns-> get pki x509 cert system
. . .
    CN=0043022002000186,CN=system generated,CN=self-signed,
. . .
finger print (md5) <e801eae4 56699fbc 324e38f2 4cfa5d47>
finger print (sha) <0113f5ec 6bd6d32b 4ef6ead9 f809eead 3a71435b>
```

查看主题名称和指印后，可将它们复制并发送给管理员 (可选择使用安全的带外方法)，随后管理员将通过 SSL 连接到 NetScreen 设备。当管理员的 SSL 客户端在 SSL 握手期间接收到来自 NetScreen 设备的证书时，他会将接收到的证书中的主题名称和指印与先前带外接收到的主题名称和指印进行比较。若二者之间相互匹配，则可确定证书是可信的。由于没有可信任的第三方 CA 授权机构来认证证书，因此，如果没有可比较的主题名称和指印，远程管理员就无法确定证书的真伪。

17. 不能通过 WebUI 来查看自动生成的自签证书的详细信息。

手动创建自签证书

NetScreen 设备在第一次启动时自动生成自签证书，因此它支持使用 SSL 进行初始连接。但是，您可能希望通过 NetScreen 设备自动生成的自签证书来生成其它自签证书。以下是用管理员定义的自签证书替换自动生成的自签证书的一些可能原因：

- 自动生成的自签证书使用固定的密钥大小 (1024 位)。为了满足您的需要，可能要求使用更大或更小的密钥大小，当生成自己的自签密钥后即可对密钥大小进行控制。
- 您可能希望使用其主题名称不同于自动创建证书的主题名称的证书。
- 您可能需要使用多个自签证书。在支持虚拟系统的 NetScreen 设备上，根系统可与所有虚拟系统共享自动生成的自签证书。不过，虚拟系统管理员可能更喜欢生成他们自己的自签证书，然后要求他们的管理员检查这些特定证书的主题名称和指印，而不是共享证书的属性。

注意：*与自动生成的自签证书 (总是位于创建它的设备中) 不同，当 NSRP 集群中的 NetScreen 设备同步 PKI 对象与集群中的其它成员时，手动生成的自签证书可与其它证书一起使用。*

虽然可配置自签证书的各种组件，如识别名称 (DN) 字段、主题可选名称和密钥大小，但以下通用名称 (CN) 元素将始终出现在 DN 的末端：

“CN = *dev_serial_num*, CN = NetScreen self-signed”

虽然自签证书主要用于对创建到 NetScreen 设备的 “安全套接字层 (SSL)” 连接提供快捷而方便的支持，但您仍可像使用其它经 CA 签名的证书那样潜在地使用此证书。自签证书的用途如下：

- 创建 “安全套接字层 (SSL)” 连接以使管理信息流安全地到达 NetScreen 设备
- 确保 NetScreen-Security Manager (NSM) 与 NetScreen 设备之间信息流的安全
- 建立 VPN 通道时对 IKE 对等方进行认证

注意：*对于当前 ScreenOS 版本， NetScreen 支持仅供 SSL 使用的自签证书。*

范例 : 管理员定义的自签证书

在此示例中，定义供 SSL 使用的自签证书的以下组件 :

- Distinguished Name/Subject Name:
  - Name: 4ssl
  - Organization: jnpr
  - FQDN: www.juniper.net
- Key type and length: RSA, 1024 bits

完成定义后，即可生成证书并对其进行查看。然后复制主题名称和指印 (也称为 “指纹”)，将其分发给通过 SSL 进行登录以管理 NetScreen 设备的其它管理员。

当管理员试图使用 SSL 进行登录时， NetScreen 设备会向他发送此证书。管理员接收到该证书后，可打开该证书并将其中的主题名称和指印与先前接收到的信息进行比较。若二者之间相互匹配，则可确定证书是可信的。

WebUI

1. 定义证书属性

Objects > Certificates > New: 输入以下内容，然后单击 **Generate**:

Certificate Subject Information:

Name: 4ssl

Organization: jnpr

FQDN: www.juniper.net

Key Pair Information:

RSA: (选择)

创建长度为 **1024** 位的新密钥对。

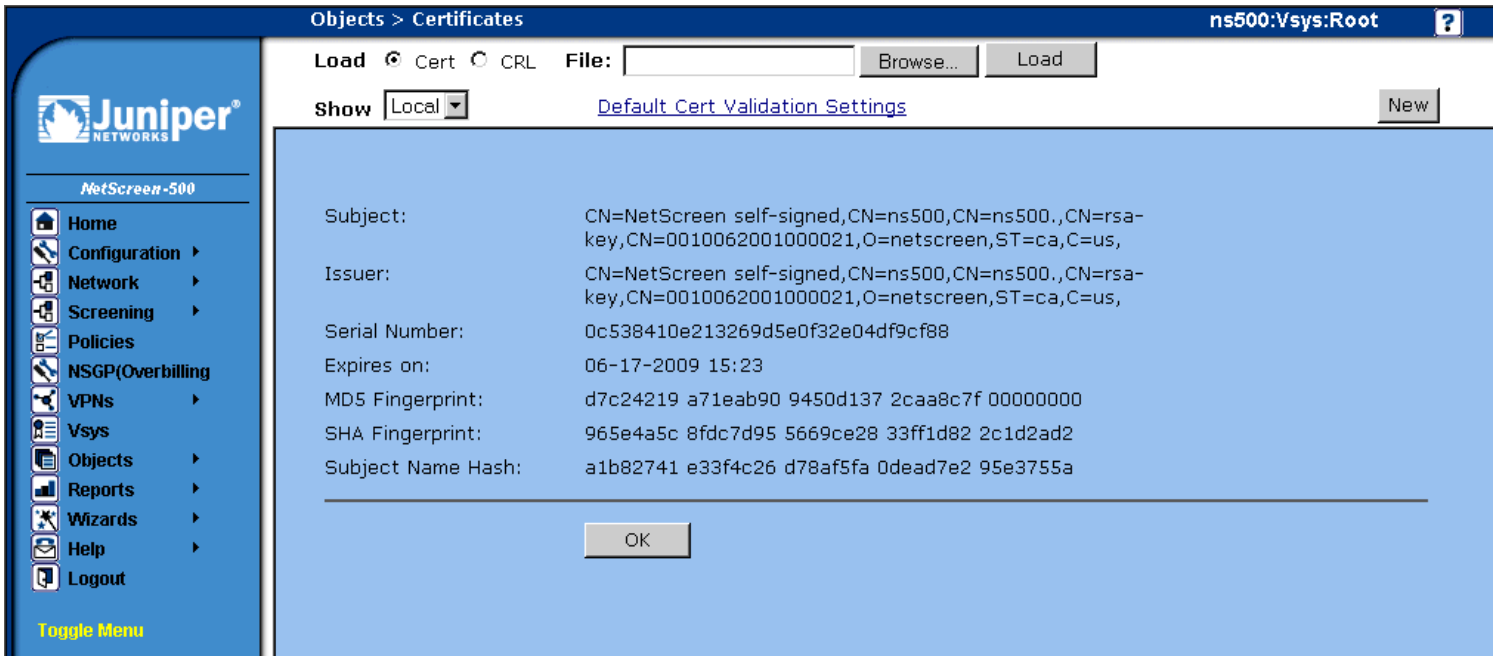
2. 生成自签证书

NetScreen 设备生成密钥后，开始编写证书申请。单击 **Generate Self-Signed Cert**。

3. 查看自签证书

Objects > Certificates > Show Local: 单击 **Detail**，查看刚刚创建的证书。

将出现以下页面，其中显示有证书的详细信息：



可复制此页面中的主题名称和指印并将其发送给要在管理 NetScreen 设备时使用 SSL 的其它管理员。启动 SSL 连接时，他们随后可使用此信息来确保他们所接收到的证书确实来自 NetScreen 设备。

CLI

1. 定义证书属性

```
set pki x509 dn name 4ssl
set pki x509 dn org-name jnpr
set pki x509 cert-fqdn www.juniper.net
save
```

2. 生成自签证书

要生成 NetScreen 设备在证书申请中所使用的公开 / 私有密钥对，请输入以下命令：

```
exec pki rsa new-key 1024
```

NetScreen 设备生成密钥对后，将编写以下证书申请：

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB0jCCATsCAQAwZTENMAsGA1UEChMESk5QUjEZMBcGA1UEAxMQMDA0MzAyMjAw
MjAwMDE4NjEQMA4GA1UEAxMHcnNhLWtleTEYMBYGA1UEAxMPd3d3Lmp1bmlwZXIu
bmV0MQ0wCwYDVQQDEwQ1c3NsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDP
aAtelkL4HxQmO1w1jv9NMmrWnzdVYnGrKrXnw2MaB3xEgouWrlymEkZetA2ouKeA
D24SL0h1YvJ7Sd9PvkhwHOnvP1zkOCWA84TgvxBzcAyeBnS1UpSwcC0admX0Da6T
80EUuGrmUWodddRFUc8o5d2VGTUOM7WgcFDZRSGQGwIDAQABoC0wKwYJKoZIhvcN
AQkOMR4wHDAaBgNVHREEEzARgg93d3cuanVuaXBlci5uZXQwDQYJKoZIhvcNAQEF
BQADgYEAgvDXI4H905y/2+k4omo9Y4XQrgq44Rj3jqXAYYMgQBd0Q8HoyL5NE3+i
QUkiYjMTWO2wIWzEr4u/tdAISEVTu03achZa3zIkUtn8sD/VYKhFlyPCBVvMiaHd
FzIHUgBuMrr+awowJDG6wARhR75w7pORXy7+aAmvIjew8YRre9s=
-----END CERTIFICATE REQUEST-----
```

要获取密钥对的 ID 号，请使用以下命令：

```
get pki x509 list key-pair
    Getting OTHER PKI OBJECT ...
    IDX   ID num      X509 Certificate Subject Distinguish Name
    ========================================================================
    0000 176095259 CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
         O=jnpr,
    ========================================================================
```

要生成自签证书，请输入以下命令，并引用通过上一个命令所获取的密钥对 ID 号：

```
exec pki x509 self-signed-cert key-pair 176095259
```

3. 查看自签证书

要查看您刚创建的自签证书，请输入以下命令：

```
get pki x509 list local-cert
    Getting LOCAL CERT ...
    IDX   ID num      X509 Certificate Subject Distinguish Name
    ========================================================================
    0000 176095261 LOCAL CERT friendly name <29>
    LOCAL CERT friendly name <29>
    CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
         O=jnpr,
    Expire on 10-19-2009 17:20, Issued By:
    CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
         O=jnpr,
    ========================================================================
```

要查看证书的详细信息，请使用证书的 ID 号输入以下命令：

```
get pki x509 cert 176095261
    -0001 176095261 LOCAL CERT friendly name <29>
    CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
        O=jnpr,
    Expire on 10-19-2009 17:20, Issued By:
    CN=self-signed,CN=4ssl,CN=www.juniper.net,CN=rsa-key,CN=0043022002000186,
        O=jnpr,
    Serial Number: <9d1c03365a5caa172ace4f82bb5ec9da>
    subject alt name extension:
    email(1): (空)
    fqdn(2): (www.juniper.net)
    ipaddr(7): (空)
    no renew
    finger print (md5) <be9e0280 02bdd9d1 175caf23 6345198e>
    finger print (sha) <87e0eee0 c06f9bac 9098bd02 0e631c1b 26e37e0e>
    subject name hash: <d82be8ae 4e71a576 2e3f06fc a98319a3 5c8c6c27>
    use count: <1>
    flag <00000000>
```

可从此输出信息中复制**主题名称**和**指印**并将其发送给要在管理 NetScreen 设备时使用 SSL 的其它管理员。启动 SSL 连接时，他们随后可使用此信息来确保他们所接收到的证书确实来自 NetScreen 设备。

证书自动生成

第一次启动 NetScreen 设备时，将自动生成自签证书。此证书的主要用途是在 NetScreen 设备初始启动后立即支持 SSL。要查看此证书，请使用以下 CLI 命令[18]：

```
get pki x509 cert system
    CN=0010062001000021,CN=system generated,CN=self-signed,
    Expire on 08- 3-2014 16:19, Issued By:
    CN=0010062001000021,CN=system generated,CN=self-signed,
    Serial Number: <c927f2044ee0cf8dc931cdb1fc363119>
    finger print (md5) <fd591375 83798574 88b3e698 62890b5d>
    finger print (sha) <40a1bda8 dcd628fe e9deaee1 92a2783c 817e26d9>
    subject name hash: <0324d38d 52f814fe 647aba3a 86eda7d4 a7834581>
```

缺省情况下，如果满足以下条件，则 NetScreen 设备在启动过程中将自动生成自签证书：

- 设备中不存在自动生成的自签证书。
- 未分配供 SSL 使用的证书。

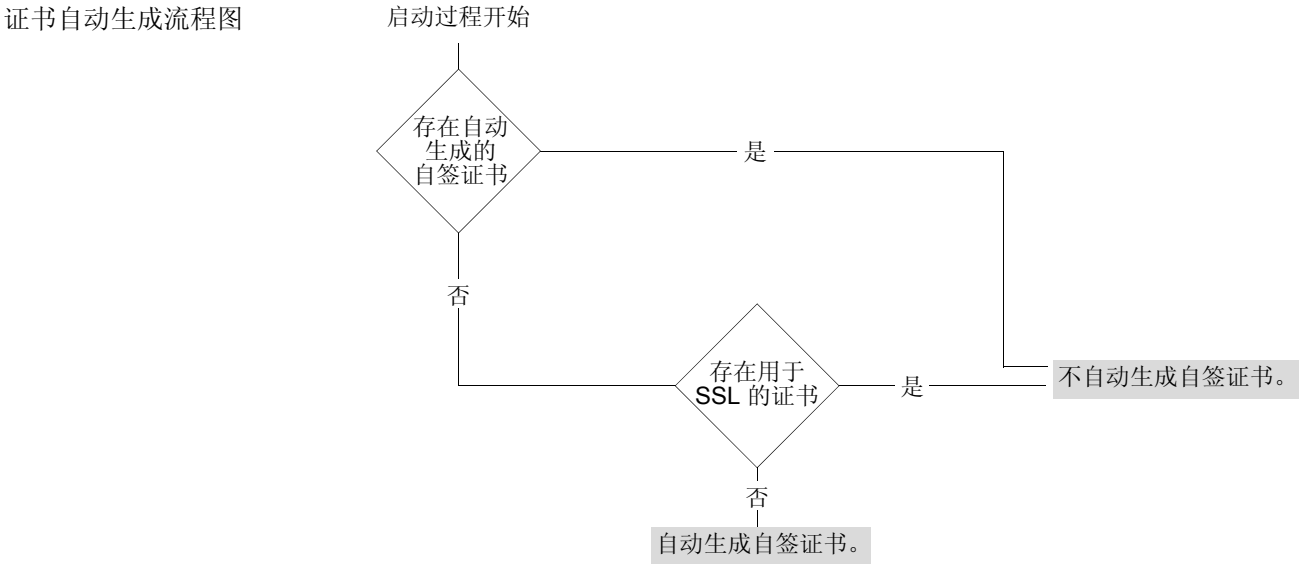
  可使用以下命令来查看是否已为 SSL 配置了证书：

  ```
  get ssl
  web SSL enable.
  web SSL port number(443).
  web SSL cert: Default - System Self-Signed Cert.
  web SSL cipher(RC4_MD5).
  ```

  在上面的输出信息中，可看到 SSL 正在使用自动生成的（“System”）自签证书。

18. 只能通过 CLI 来查看自动生成的自签证书。

下图为 NetScreen 设备启动时生成证书的流程图：



如果删除了自动生成的自签证书，并为 SSL 分配了另一个证书，然后对 NetScreen 设备进行了重置，则 NetScreen 设备在启动过程中将不会重新生成另一个自签证书。如果接下来更改了 SSL 配置，致使未向其分配任何证书，并重置了设备，则 NetScreen 设备将在下一个启动过程中自动重新生成新的自签证书。

删除自签证书

可用删除任一类型证书的方法来删除自动或手动生成的自签证书。可能您具有一份更希望将其用于 SSL 的经 CA 签名的证书，而不是自签证书。不管出于何种原因，当删除自动生成的自签证书时，都应使用以下 CLI 命令[19]：

```
delete pki object-id system
```

要删除管理员配置的自签证书，请使用以下命令，其中 *id_num* 是您要删除的证书的 ID 号[20]：

```
delete pki object-id id_num
```

如果删除了自动生成的自签证书，但之后想用 NetScreen 设备生成另一个自签证书，则请执行以下操作：

- 不要为 SSL 分配任何其它证书 (可使用以下命令 : **unset ssl cert**)。
- 重置 NetScreen 设备。

NetScreen 设备可将发送到其自身的 HTTP 信息流 (缺省端口 80) 重新定向到 SSL (缺省端口 443)[21]。因此，在启动过程中，要确保证书可用于 SSL， NetScreen 设备总是检查是否存在自动生成的自签证书，或者检查是否已分配了另一个可供 SSL 使用的证书。如果不存在自动生成的自签证书，并且也没有为 SSL 分配任何其它证书，则 NetScreen 设备将自动生成自签证书。

19. 只能通过 CLI 来删除自动生成的自签证书。

20. 要获取证书的 ID 号，请使用以下命令：**get pki x509 list local-cert**。

21. 有关将 HTTP 信息流重新定向到 SSL 的信息，请参阅第 **3**-11 页上的 “将 HTTP 重定向到 SSL”。

3

VPN 准则

配置 VPN 通道时， NetScreen 提供多种加密选项。即使配置简单的通道，也必须进行选择。本章前半部分对基本的站点到站点 VPN 和基本的拨号 VPN 的所有选项加以概述，并介绍选择一个选项或多个选项的一种或多种原因。

在本章的后半部分，我们将探讨基于策略和基于路由的 VPN 通道之间的差异。然后，我们将研究基于路由和基于策略的站点到站点 “自动密钥 IKE VPN” 通道的数据包流，以查看数据包所经历的出站和入站处理阶段。本章结束时介绍了配置通道时要记住的一些有用的 VPN 配置技巧。

本章的组织结构如下：

加密选项

配置 VPN 时，必须对要使用的密码术作出多种决定。会出现有关哪个 Diffie-Hellman 组适合选择、哪种加密算法能提供安全和性能之间的最佳平衡等问题。本节介绍配置基本的站点到站点 VPN 通道和基本的拨号 VPN 通道所需的全部加密选项，并说明每个选项的一个或多个优点，以帮助您作出决定。

您必须作出的第一个决定就是通道是针对站点到站点 VPN 通道 (两个 NetScreen 设备间)，还是针对拨号 VPN 通道 (从 NetScreen-Remote VPN 客户端到 NetScreen 设备)。尽管这是一个连网决定，但是两种通道间的差别还是会影响某些加密选项。因此，将以两种不同的决策树介绍各个选项 :

- 第 63 页上的 “站点到站点加密选项”
- 第 72 页上的 “拨号 VPN 选项”

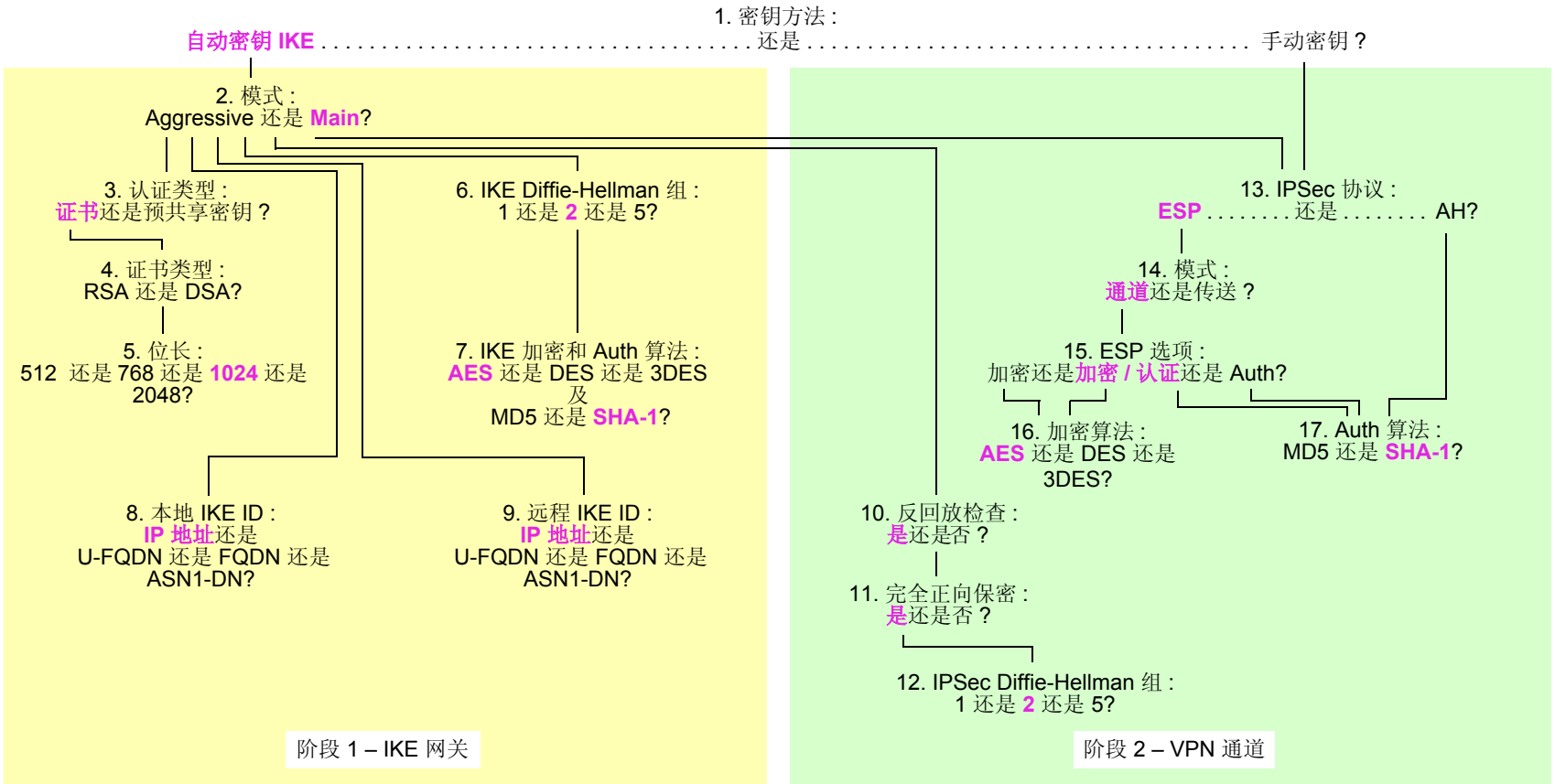
决定要配置站点到站点通道还是拨号通道之后，即可参考相应的决策树作为指导。每种决策树都介绍配置通道时必须作出的加密选择。每种决策树的后面是选择树中出现的每个选项的原因。

注意 : *配置两种通道的范例在第 4 章，“站点到站点 VPN”和第 5 章，“拨号 VPN”中。*

站点到站点加密选项

配置基本的站点到站点 VPN 通道时，必须在下面决策树的加密选项中进行选择。随后介绍每个选项的优点。

***注意：**用紫色突出显示的选项表示 Juniper Networks 建议的选项。有关不同的 IPSec 选项的背景信息，请参阅第 1 章，“IPSec”。*



1. 密钥方法：手动密钥还是自动密钥 IKE?

自动密钥 IKE

- 提供自动密钥更新和密钥刷新，因而增强了安全性

手动密钥

- 用于调试 IKE 问题
- 消除建立通道时的 IKE 协商延迟

2. 模式：Aggressive 模式还是 Main 模式？

Aggressive

- 其中一个 IPSec 对等方的 IP 地址被动态分配以及使用预共享密钥时，需要使用此模式

Main

- 提供身份保护
- 拨号用户拥有静态 IP 地址时或证书用于认证时，可使用此模式

3. 认证类型：预共享密钥还是证书？

证书

- 由于可以通过证书授权机构 (CA) 验证证书，因此提供比预共享密钥更高的安全级别。(有关详细信息，请参阅第 2 章，“公开密钥密码术”。)

预共享密钥

- 由于不需要 “公开密钥基础” (PKI)，因此使用更方便，设置更快速

4. 证书类型：RSA 还是 DSA?

具体取决于从其获得证书的 CA。两种证书类型没有优劣之分。

5. 位长 : 512 还是 768 还是 1024 还是 2048?

512

- 使处理开销最少

768

- 提供比 512 位更高的安全等级
- 使处理开销比 1024 和 2048 位的更少

1024

- 提供比 512 和 768 位更高的安全等级
- 使处理开销比 2048 位的更少

2048

- 提供最高的安全等级

6. IKE Diffie-Hellman 组 : 1 还是 2 还是 5?

Diffie-Hellman 组 1

- 使处理开销比 Diffie-Hellman 组 2 和 5 的更少
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 2

- 使处理开销比 Diffie-Hellman 组 5 的更少
- 提供比 Diffie-Hellman 组 1 更高的安全等级
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 5

- 提供最高的安全等级

7. IKE 加密和 Auth 算法 : AES 还是 DES 还是 3DES 及 MD5 还是 SHA-1?

AES

- 如果密钥长度全部相等，则比 DES 和 3DES 的加密性更强
- 在 NetScreen 硬件中提高处理速度
- 用于 “联邦信息处理标准” (FIPS) 和 “通用标准 EAL4” 标准的经核准加密算法

DES

- 使处理开销比 3DES 和 AES 的更少
- 在远程对等方不支持 AES 时非常有用

3DES

- 提供比 DES 更高的加密安全等级
- 在 NetScreen 硬件中提高处理速度

MD5

- 使处理开销比 SHA-1 的更少

SHA-1

- 提供比 MD5 更高的加密安全等级
- FIPS 接受的唯一认证算法

8. 本地 IKE ID : IP 地址 (缺省) 还是 U-FQDN 还是 FQDN 还是 ASN1-DN?

IP 地址

- 本地 NetScreen 设备具有静态 IP 地址时才能使用
- 使用预共享密钥认证时的缺省 IKE ID
- 如果 IP 地址出现在 SubjectAltName 字段中，则可与证书配合使用

U-FQDN

- 用户完全合格的域名 (U-FQDN — 电子邮件地址): 如果 U-FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

FQDN

- 完全合格的域名 (FQDN): 如果 FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用
- 针对具有动态 IP 地址的 VPN 网关使用
- 使用 RSA 或 DSA 证书认证时的缺省 IKE ID

ASN1-DN

- 只能与证书配合使用
- 当 CA 在其发布的证书中不支持 SubjectAltName 字段时使用

9. 远程 IKE ID : IP 地址 (缺省) 还是 U-FQDN 还是 FQDN 还是 ASN1-DN?

IP 地址

- 使用预共享密钥认证并且对等方是 NetScreen 设备时，不需要在静态 IP 地址处输入对等方的远程 IKE ID
- 可用于具有静态 IP 地址的设备
- 如果 IP 地址出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

U-FQDN

- 用户完全合格的域名 (U-FQDN — 电子邮件地址): 如果 U-FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

FQDN

- 完全合格的域名 (FQDN): 如果 FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用
- 用于具有动态 IP 地址的 VPN 网关
- 使用证书认证并且对等方是 NetScreen 设备时，不需要输入远程 IKE ID

ASN1-DN

- 只能与证书配合使用
- 当 CA 在其发布的证书中不支持 SubjectAltName 字段时使用

10. 反回放检查：否还是是？

是

- 允许收件人检查数据包包头中的序列号，以防止犯罪分子重新发送截取的 IPSec 数据包时导致的 “拒绝服务” (DoS) 攻击

否

- 禁用此项可能会解决与第三方对等方的兼容性问题

11. 完全正向保密：否还是是？

是

- 完全正向保密 (PFS): 由于对等方执行第二个 Diffie-Hellman 交换生成用于 IPSec 加密 / 解密的密钥，因此使安全性增强

否

- 提供更快的通道设置
- 使 “阶段 2” IPSec 协商期间处理开销更少

12. IPSec Diffie-Hellman 组：1 还是 2 还是 5?

Diffie-Hellman 组 1

- 使处理开销比 Diffie-Hellman 组 2 和 5 的更少
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman Group 2

- 使处理开销比 Diffie-Hellman 组 5 的更少
- 提供比 Diffie-Hellman 组 1 更高的安全等级
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 5

- 提供最高的安全等级

13. IPSec 协议：

ESP 还是 AH?

ESP

- 封装安全性负荷 (ESP): 通过加密和封装初始 IP 数据包可提供机密性，同时通过认证提供完整性
- 可提供单独加密或单独认证

AH

- 认证包头 (AH): 提供整个 IP 数据包的认证，包括 IPSec 包头和外部 IP 包头

14. 模式：通道模式还是传送模式？

通道

- 由于隐藏了初始 IP 包头，因此增加了私密性

传送

- 对于 L2TP-over-IPSec 通道支持，此模式是必需的

15. ESP 选项：加密还是加密 / 认证还是认证？

加密

- 提供比使用加密 / 认证更快的性能并使处理开销更少
- 用于要求机密性但不要求认证的情况

加密 / 认证

- 用于需要机密性和认证的情况

Auth

- 用于需要认证但不要求机密性的情况。也许信息不保密时，确定此信息确实来自声称发送它的人，以及在传输过程中没有任何人篡改内容是很重要的。

16. 加密算法：AES 还是 DES 还是 3DES?

AES

- 如果密钥长度全部相等，则比 DES 和 3DES 的加密性更强
- 在 NetScreen 硬件中提高处理速度
- 用于 (FIPS) 和 “通用标准 EAL4”标准的核准加密算法

DES

- 使处理开销比 3DES 和 AES 的更少
- 在远程对等方不支持 AES 时非常有用

3DES

- 提供比 DES 更高的加密安全等级
- 在 NetScreen 硬件中提高处理速度

17. Auth 算法 : MD5 还是 SHA-1?

MD5

– 使处理开销比 SHA-1 的更少

SHA-1

– 提供比 MD5 更高的加密安全等级

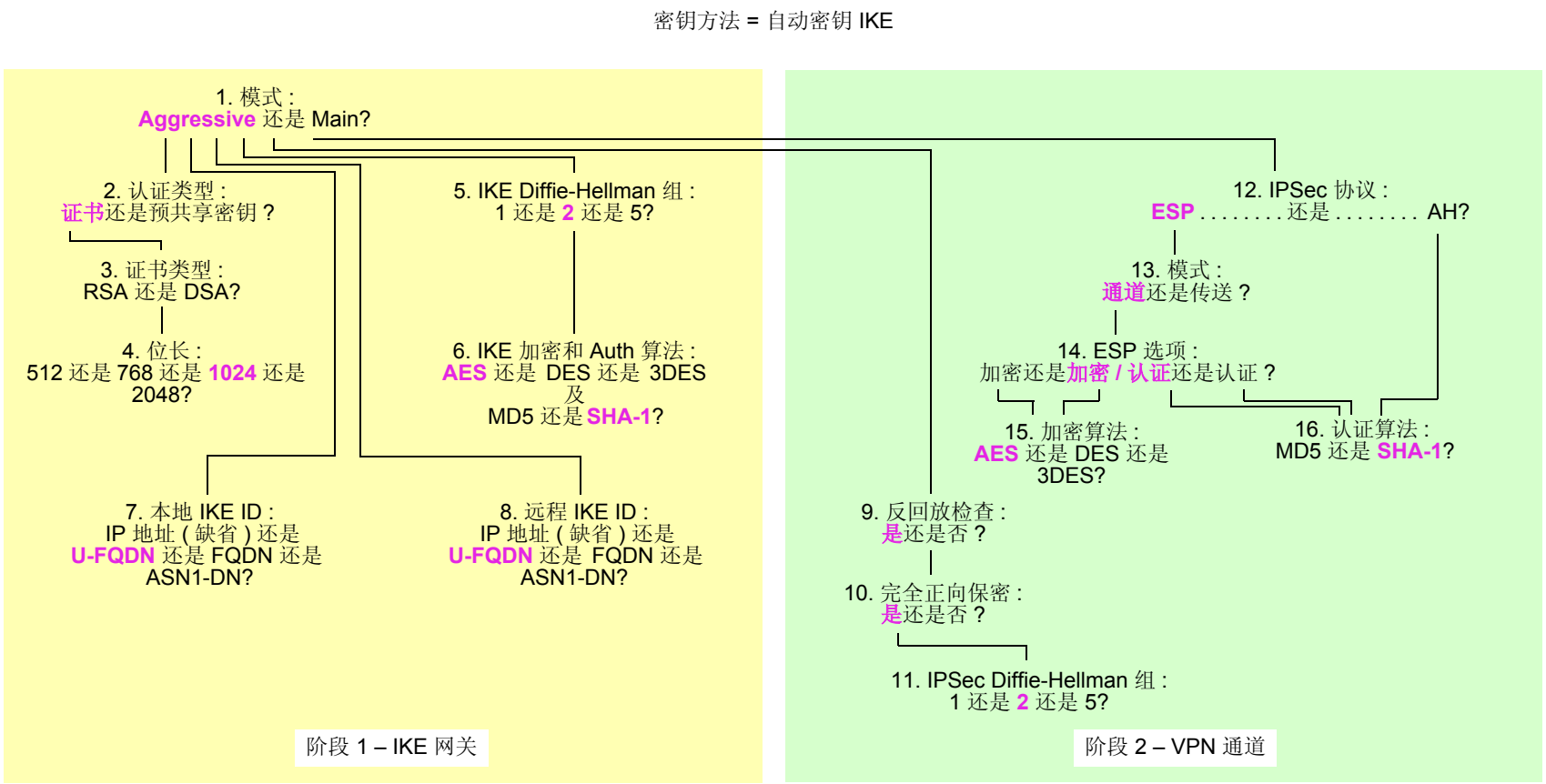
使用上述列表中建议的选项，具有静态 IP 地址的两台 NetScreen 设备间的通用站点到站点 VPN 配置的组成如下 :

- 自动密钥 IKE
- Main 模式
- 1024 位证书 (RSA 或 DSA)
- “阶段 1” Diffie-Hellman 组 2
- 加密 = AES
- 认证 = SHA-1
- IKE ID = IP 地址 (缺省)
- 反回放保护 = 是
- 完全正向保密 (PFS) = 是
- “阶段 2” Diffie-Hellman 组 2
- 封装安全性负荷 (ESP)
- 通道模式
- 加密 / 认证
- 加密 = AES
- 认证 = SHA-1

拨号 VPN 选项

配置基本的拨号 VPN 通道时，必须在下面决策树的加密选项中选择。随后介绍每个选项的优点。

***注意：**用紫色突出显示的选项表示 Juniper Networks 建议的选项。有关不同的 IPSec 选项的背景信息，请参阅第 1 章，“IPSec”。*



1. 模式 : Aggressive 模式还是 Main 模式 ?

   Aggressive

   – 其中一个 IPSec 对等方的 IP 地址被动态分配以及使用预共享密钥时，需要使用此模式
   – 可与证书或预共享密钥配合使用进行认证

   Main

   – 提供身份保护

2. 认证类型 : 预共享密钥还是证书 ?

   证书

   – 由于可以通过证书授权机构 (CA) 验证证书，因此提供比预共享密钥更高的安全级别。(有关详细信息，请参阅第 2 章，“公开密钥密码术”。)

   预共享密钥

   – 由于不需要 “公开密钥基础” (PKI)，因此使用更方便，设置更快速

3. 证书类型 : RSA 还是 DSA?

   具体取决于从其获得证书的 CA。两种证书类型没有优劣之分。

4. 位长 : 512 还是 768 还是 1024 还是 2048?

   512

   – 使处理开销最少

   768

   – 提供比 512 位更高的安全等级
   – 使处理开销比 1024 和 2048 位的更少

1024

- 提供比 512 和 768 位更高的安全等级
- 使处理开销比 2048 位的更少

2048

- 提供最高的安全等级

5. IKE Diffie-Hellman 组 : 1 还是 2 还是 5?

Diffie-Hellman 组 1

- 使处理开销比 Diffie-Hellman 组 2 和 5 的更少
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 2

- 使处理开销比 Diffie-Hellman 组 5 的更少
- 提供比 Diffie-Hellman 组 1 更高的安全等级
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 5

- 提供最高的安全等级

6. IKE 加密和 Auth 算法 : AES 还是 DES 还是 3DES 及 MD5 还是 SHA-1?

AES

- 如果密钥长度全部相等，则比 DES 和 3DES 的加密性更强
- 在 NetScreen 硬件中提高处理速度
- 用于 (FIPS) 和 “通用标准 EAL4”标准的核准加密算法

DES

- 使处理开销比 3DES 和 AES 的更少
- 在远程对等方不支持 AES 时非常有用

3DES

- 提供比 DES 更高的加密安全等级
- 在 NetScreen 硬件中提高处理速度

MD5

- 使处理开销比 SHA-1 的更少

SHA-1

- 提供比 MD5 更高的加密安全等级

7. 本地 IKE ID : IP 地址 (缺省) 还是 U-FQDN 还是 FQDN 还是 ASN1-DN?

IP 地址 (缺省)

- 不要求输入具有静态 IP 地址的设备的 IKE ID
- 可用于具有静态 IP 地址的设备
- 如果 IP 地址出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

U-FQDN

- 用户完全合格的域名 (U-FQDN — 电子邮件地址): 如果 U-FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

FQDN

- 完全合格的域名 (FQDN): 如果 FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用
- 用于具有动态 IP 地址的 VPN 网关

ASN1-DN

- 只能与证书配合使用
- 当 CA 在其发布的证书中不支持 SubjectAltName 字段时很有用

8. 远程 IKE ID：IP 地址 (缺省) 还是 U-FQDN 还是 FQDN 还是 ASN1-DN?

IP 地址 (缺省)

- 不要求输入具有静态 IP 地址的设备的 IKE ID
- 可用于具有静态 IP 地址的设备
- 如果 IP 地址出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

U-FQDN

- 用户完全合格的域名 (U-FQDN — 电子邮件地址): 如果 U-FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用

FQDN

- 完全合格的域名 (FQDN): 如果 FQDN 出现在 SubjectAltName 字段中，则可与预共享密钥或证书配合使用
- 用于具有动态 IP 地址的 VPN 网关

ASN1-DN

- 只能与证书配合使用
- 当 CA 在其发布的证书中不支持 SubjectAltName 字段时使用

9. 反回放检查：否还是是？

是

- 允许收件人检查数据包包头中的序列号，以防止犯罪分子重新发送截取的 IPSec 数据包时导致的 “拒绝服务” (DoS) 攻击

否

- 禁用此项可能会解决与第三方对等方的兼容性问题

10. 完全正向保密：否还是是？

是

- 完全正向保密 (PFS): 由于对等方执行第二个 Diffie-Hellman 交换生成用于 IPSec 加密 / 解密的密钥，因此使安全性增强

否

- 提供更快的通道设置
- 使 “阶段 2” IPSec 协商期间处理开销更少

11. IPSec Diffie-Hellman 组：1 还是 2 还是 5?

Diffie-Hellman 组 1

- 使处理开销比 Diffie-Hellman 组 2 和 5 的更少
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 2

- 使处理开销比 Diffie-Hellman 组 5 的更少
- 提供比 Diffie-Hellman 组 1 更高的安全等级
- 在 NetScreen 硬件中提高处理速度

Diffie-Hellman 组 5

- 提供最高的安全等级

12. IPSec 协议 : ESP 还是 AH?

ESP

- 封装安全性负荷 (ESP): 通过加密和封装初始 IP 数据包可提供机密性，同时通过认证提供完整性
- 可提供单独加密或单独认证

AH

- 认证包头 (AH): 提供整个 IP 数据包的认证，包括 IPSec 包头和外部 IP 包头

13. 模式 : 通道模式还是传送模式 ?

通道

- 由于隐藏了初始 IP 包头，因此增加了私密性

传送

- 对于 L2TP-over-IPSec 通道支持，此模式是必需的

14. ESP 选项 : 加密或加密 / 认证或认证 ?

加密

- 同使用加密 / 认证相比，具有更快的执行速度，且处理开销更少
- 用于要求机密性但不要求认证的情况

加密 / 认证

- 用于需要机密性和认证的情况

认证

- 用于需要认证但不要求机密性的情况。也许信息不保密时，确定此信息确实来自声称发送它的人，以及在传输过程中没有任何人篡改内容是很重要的。

15. 加密算法 : AES 或 DES 或 3DES?

AES

- 如果密钥长度全部相等，则比 DES 和 3DES 的加密性更强
- 加快 NetScreen 硬件中提供的处理速度
- 用于 (FIPS) 和 “通用标准 EAL4”标准的核准加密算法

DES

- 使处理开销比 3DES 和 AES 的更少
- 用于远程对等方不支持 AES 时的情况

3DES

- 提供比 DES 更高的加密安全等级
- 加快 NetScreen 硬件中提供的处理速度

16. 认证算法 : MD5 或 SHA-1?

MD5

- 使处理开销比 SHA-1 的更少

SHA-1

- 提供比 MD5 更高的加密安全等级

若使用了上述列表中建议的选项，则具有静态 IP 地址的两台 NetScreen 设备间的通用拨号 VPN 配置将由以下组件组成 :

- Aggressive 模式
- 1024 位证书 (RSA 或 DSA)
- “阶段 1” Diffie-Hellman 组 2
- 加密 = AES
- 认证 = SHA-1
- IKE ID = U-FQDN (电子邮件地址)
- 反回放保护 = 是
- 完全正向保密 (PFS) = 是
- “阶段 2” Diffie-Hellman 组 2
- 封装安全性负荷 (ESP)
- 通道模式
- 加密 / 认证
- 加密 = AES
- 认证 = SHA-1

基于路由和基于策略的通道

VPN 支持的 NetScreen 设备的配置非常灵活。可以创建基于路由和基于策略的 VPN 通道。另外，每种通道都可使用 “手动密钥” 或 “自动密钥 IKE” 来管理用于加密和认证的密钥。

对于基于策略的 VPN 通道而言，通道被视为对象 (或构件块)，其同源、目标、服务和动作一起共同构成允许 VPN 信息流的策略。(实际上， VPN 策略动作是 *tunnel*，但如果未申明，则暗指动作 *permit*。) 在基于策略的 VPN 配置中，策略专门按名称引用 VPN 通道。

对于基于路由的 VPN 而言，策略不专门引用 VPN 通道。而是引用目标地址。 NetScreen 设备进行路由查询以查找其发送流向该地址的信息流所必须经由的接口时，将通过通道接口来查找绑定到特定 VPN 通道的路由[1]。

因此，对于基于策略的 VPN 通道而言，可将通道视为策略结构中的一个元素。对于基于路由的 VPN 通道而言，可将通道视为传输信息流的一种方法，同时将策略视为允许或拒绝传送该信息流的方法。

可创建的基于策略的 VPN 通道的数量由设备所支持的策略数量决定。可创建的基于路由的 VPN 通道的数量由设备所支持的路由条目或通道接口的数量决定 (以较小的数值为准)。

当对 VPN 信息流设置了精确限制时，如果希望节约通道资源，建议使用基于路由的 VPN 通道配置。尽管可以创建引用同一 VPN 通道的多个策略，但是每个策略都将创建一个拥有远程对等方的单独的 IPSec 安全联盟 (SA)，每个联盟都被视为一个单独的 VPN 通道。对于基于路由的 VPN 方案，信息流的调整与其传输方式不成对。可配置多个策略以调整在两个站点间流过单个 VPN 通道的信息流，但只有一个 IPSec SA 在工作。另外，基于路由的 VPN 配置允许您创建引用经由 VPN 通道所到达目标的策略，其中的动作为 *deny*，与基于策略的 VPN 配置不同 (如前面所述)，其中的动作必须是 *tunnel*，暗指 *permit*。

基于路由的 VPN 提供的另一个优势就是可交换通过 VPN 通道的动态路由选择信息。可在绑定到 VPN 通道的通道接口上启用一个动态路由协议 (例如，“边界网关协议” (BGP)) 的实例。本地路由选择实例与绑定到另一端的通道接口上所启用的相邻方交换通过通道的路由选择信息。

当通道未连接运行动态路由协议的大型网络，以及不需要节约通道或定义各种策略来过滤经由通道的信息流时，建议使用基于策略的通道。另外，由于在拨号 VPN 客户端之外没有任何网络，因此对于拨号 VPN 配置来说，基于策略的 VPN 通道可能是一个很好的选择。

1. 通常，一个通道接口被绑定到一个单独通道。还可将一个通道接口绑定到多个通道。有关详细信息，请参阅第 374 页上的 “每个通道接口多个通道”。

也就是说，拨号客户端支持 NetScreen-Remote 所支持的虚拟内部 IP 地址时，还有使用基于路由的 VPN 配置的强制原因。基于路由的拨号 VPN 通道有以下优点：

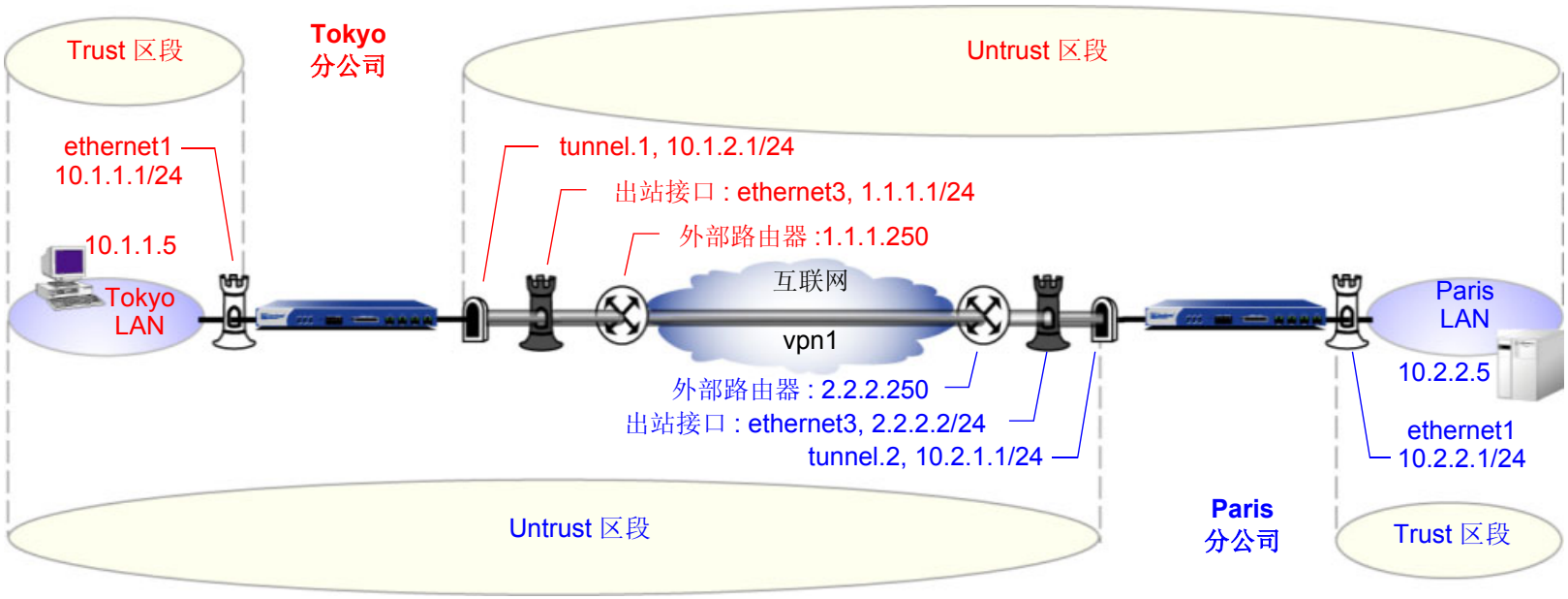
- 可将其通道接口绑定到要求或不要求策略执行的任何区段。
- 与基于策略的 VPN 配置不同，可定义路由强制信息流通过通道。
- 基于路由的 VPN 通道简化了向集中星型配置添加星型的操作 (请参阅第 464 页上的 “集中星型 VPN”)。
- 通过将远程客户端地址配置为 255.255.255.255/32，可调整代理 ID 以接受拨号 VPN 客户端的任何 IP 地址。
- 可在通道接口上定义一个或多个映射 IP (MIP) 地址。

注意：*有关拨号客户端的基于路由的 VPN 配置的范例，请参阅第 240 页上的 “范例：基于路由的拨号 VPN，动态对等方”。*

数据包流：站点到站点 VPN

为了更好地了解构成创建 IPSec 通道的各个组件相互间如何工作，本节将就通过通道的数据包流的处理过程 (NetScreen 设备发送出站 VPN 信息流及接收入站 VPN 信息流时) 进行介绍。先介绍基于路由的 VPN 的处理，紧接着是附录，该附录中记录有与基于策略的 VPN 不同的流动中的两个位置。

总部设在东京 (Tokyo) 的某公司不久前在巴黎 (Paris) 新开了一家分公司，需要通过 IPSec 通道将这两个站点连接起来。该通道使用 “手动密钥 IKE”、 ESP 协议、用于加密的 AES 以及用于通过预共享密钥进行认证的 SHA-1，并且启用反回放检查。保护每个站点的 NetScreen 设备处于 NAT 模式，并且所有区段都在 trust-vr 路由选择域中。地址如下：



数据包的路径为 : 起点是东京 LAN 中的 10.1.1.5/32，经由 IPSec 通道到达终点巴黎 LAN 中的 10.2.2.5/32，具体内容将在接下来的各个小节中进行阐述。

东京 (发起方)

1. 10.1.1.5 处的主机将目标为 10.2.2.5 的数据包发送到 10.1.1.1 (其为 ethernet1 的 IP 地址，并且是主机的 TCP/IP 设置中所配置的缺省网关)。
2. 数据包到达绑定到 Trust 区段的 ethernet1。
3. 此时，如果启用了 Trust 区段的 SCREEN 选项 (如 IP 欺骗检测)，则 NetScreen 设备将激活 SCREEN 模块。 SCREEN 检查可以生成下列三种结果之一：
   - 如果 SCREEN 机制检测到异常行为 (对此行为已配置 NetScreen 设备阻止该数据包)，则 NetScreen 设备会丢弃该数据包并在事件日志中生成一个条目。
   - 如果 SCREEN 机制检测到异常行为 (对此行为已配置 NetScreen 设备记录该事件但不阻止数据包)，则 NetScreen 设备会在 ethernet1 的 SCREEN 计数器列表中记录该事件并继续下一步骤。
   - 如果 SCREEN 机制没有检测到异常行为，则 NetScreen 设备将继续下一步骤。

   如果尚未启用 Trust 区段的任何 SCREEN 选项，则 NetScreen 设备将直接继续下一步骤。
4. 会话模块执行会话查找，尝试将数据包与现有会话进行匹配。

   如果该数据包与现有会话不匹配，则 NetScreen 设备将执行 “首包处理”，该过程包括其余的步骤。

   如果该数据包与现有会话匹配，则 NetScreen 设备将执行 “快速处理”，用现有会话条目中可用的信息来处理该数据包。“快速处理”会跳过路由和策略查找，因为在会话的首包处理期间已经获得了由这些跳过的步骤所生成的信息。
5. 地址映射模块检查映射 IP (MIP) 配置是否使用目标 IP 地址 10.2.2.5。由于 MIP 配置中未使用 10.2.2.5，因此 NetScreen 设备将继续下一步骤。 (有关涉及 MIP、 VIP 或目标地址转换 “NAT-dst” 时数据包处理的信息，请参阅第 **7**-36 页上的 “NAT-Dst 的数据包流”。)
6. 为了确定目标区段，路由模块将执行针对 10.2.2.5 的路由查找。 (路由模块使用入口接口来确定路由查找所使用的虚拟路由器。) 找到了一个路由条目：通过绑定到名为 “vpn1” 的 VPN 通道的 tunnel.1 接口，将信息流引向 10.2.2.5。此通道接口在 Untrust 区段中。通过确定入口接口和出口接口， NetScreen 设备从而确定了源区段和目标区段，因此现在即可进行策略查找。

7. 策略引擎在 Trust 和 Untrust 区段 (通过相应的入口接口和出口接口确定) 间进行策略查找。策略 (与源地址和源区段、目标地址和目标区段以及服务相匹配) 中所指定的动作为 “允许”。
8. IPSec 模块检查带有远程对等方的活动 “阶段 2” 安全联盟 (SA) 是否存在。“阶段 2” SA 检查可以生成下列结果之一：
   - 如果 IPSec 模块发现了带有对等方的活动 “阶段 2” SA，则将继续步骤 10.
   - 如果 IPSec 模块未发现带有对等方的活动 “阶段 2” SA，则将丢弃该数据包并触发 IKE 模块。
9. IKE 模块检查带有远程对等方的活动 “阶段 1” SA 是否存在。“阶段 1” SA 检查可以生成下列结果之一：
   - 如果 IKE 模块发现了带有对等方的活动 “阶段 1” SA，则将使用此 SA 来协商 “阶段 2” SA。
   - 如果 IKE 模块未发现带有对等方的活动 “阶段 1” SA，则将开始 Main 模式下的 “阶段 1” 协商，然后再进行 “阶段 2” 协商。
10. IPSec 模块先后将 ESP 包头和外部 IP 包头放在数据包上。使用指定为出接口的地址，将作为源 IP 地址的 1.1.1.1 放在外部包头中。使用为远程网关指定的地址，将作为目标 IP 地址的 2.2.2.2 放在外部包头中。接着，对从负荷到初始 IP 包头中的下一个包头字段的数据包进行加密。然后，对从 ESP 尾部到 ESP 包头的数据包进行认证。
11. NetScreen 设备通过出接口 (ethernet3) 将目标为 2.2.2.2 的已加密和已认证的数据包发送到 1.1.1.250 处的外部路由器。

巴黎 (接收方)

1. 数据包到达 2.2.2.2，它是绑定到 Untrust 区段的接口 ethernet3 的 IP 地址。
2. 通过使用外部数据包包头中的 SPI、目标 IP 地址以及 IPSec 协议， IPSec 模块尝试查找带有发起方的活动 “阶段 2” SA 和密钥，以便对该数据包进行认证和解密。“阶段 2” SA 检查可以生成下列三种结果之一：
   - 如果 IPSec 模块发现了带有对等方的活动 “阶段 2” SA，则将继续步骤 4.
   - 如果 IPSec 模块未发现带有对等方的活动 “阶段 2” SA (但可以使用源 IP 地址而不是 SPI 匹配非活动的 “阶段 2” SA)，则将丢弃该数据包，并生成一个事件日志条目，然后再将一个通知 (指出其收到了错误 SPI) 发送给发起方。
   - 如果 IPSec 模块未发现带有对等方的活动 “阶段 2” SA，则将丢弃该数据包并触发 IKE 模块。
3. IKE 模块检查带有远程对等方的活动 “阶段 1” SA 是否存在。“阶段 1” SA 检查可以生成下列结果之一：
   - 如果 IKE 模块发现了带有对等方的活动 “阶段 1” SA，则将使用此 SA 来协商 “阶段 2” SA。
   - 如果 IKE 模块未发现带有对等方的活动 “阶段 1” SA，则将开始 Main 模式下的 “阶段 1” 协商，然后再进行 “阶段 2” 协商。
4. IPSec 模块执行反回放检查。此检查可以生成下列两种结果之一：
   - 如果由于检测到 NetScreen 设备已经收到的序列号而导致该数据包未通过反回放检查，则 NetScreen 设备将丢弃该数据包。
   - 如果该数据包通过了反回放检查，则 NetScreen 设备将继续下一步骤。
5. IPSec 模块尝试对数据包进行认证。此认证检查可以生成下列两种结果之一：
   - 如果该数据包未通过认证检查，则 NetScreen 设备将丢弃该数据包。
   - 如果该数据包通过了认证检查，则 NetScreen 设备将继续下一步骤。
6. IPSec 模块使用 “阶段 2” SA 和密钥来解密该数据包，找出其初始源地址 (10.1.1.5) 和最终目标地址 (10.2.2.5)。获知该数据包来自绑定到 tunnel.1 的 vpn1。之后， NetScreen 设备对该数据包进行处理，就如同其入口接口是 tunnel.1 而非 ethernet3 一样。此时，还调整反回放滑动窗口。

7. 此时，如果启用了 Untrust 区段的 SCREEN 选项，则 NetScreen 设备将激活 SCREEN 模块。 SCREEN 检查可以生成下列三种结果之一：
   - 如果 SCREEN 机制检测到异常行为 (对此行为已配置 NetScreen 设备阻止该数据包)，则 NetScreen 设备会丢弃该数据包并在事件日志中生成一个条目。
   - 如果 SCREEN 机制检测到异常行为 (对此行为已配置 NetScreen 设备记录事件但不阻止该数据包)，则 NetScreen 设备会在 ethernet3 的 SCREEN 计数器列表中记录该事件并继续下一步骤。
   - 如果 SCREEN 机制没有检测到异常行为，则 NetScreen 设备将继续下一步骤。
8. 会话模块执行会话查找，尝试将数据包与现有会话进行匹配。然后执行 “首包处理”或 “快速处理”。

   如果该数据包与现有会话匹配，则 NetScreen 设备将执行 “快速处理”，用现有会话条目中可用的信息来处理该数据包。“快速处理”会跳过除最后两个步骤 (加密数据包和转发数据包) 之外的所有步骤，因为跳过的步骤所产生的信息已经在会话的首包处理期间获得。
9. 地址映射模块检查映射 IP (MIP) 或虚拟 IP (VIP) 配置是否使用目标 IP 地址 10.2.2.5。由于 MIP 或 VIP 配置中未使用 10.2.2.5，因此 NetScreen 设备将继续下一步骤。
10. 路由模块首先使用入口接口来确定进行路由查找所使用的虚拟路由器 (本例中为 trust-vr)。然后执行针对 trust-vr 中 10.2.2.5 的路由查找，并发现可通过 ethernet1 对该地址进行访问。通过确定入口接口 (tunnel.1) 和出口接口 (ethernet1)，从而 NetScreen 设备可以确定源区段和目标区段。 tunnel.1 接口被绑定到 Untrust 区段，而 ethernet1 被绑定到 Trust 区段。现在， NetScreen 设备即可进行策略查找。
11. 策略引擎从 Untrust 区段到 Trust 区段检查其策略列表，并找到准许访问的策略。
12. NetScreen 设备通过 ethernet1 将数据包转发到其目标 10.2.2.5。

附录：基于策略的 VPN

基于策略的 VPN 配置的数据包流与基于路由的 VPN 配置的数据包流有两点不同：路由查找和策略查找。

东京 (发起方)

在路由查找和随后的策略查找发生之前，出站数据包流的第一阶段与基于路由和基于策略的 VPN 配置相同：

路由查找：为确定目标区段，路由模块针对 10.2.2.5 执行路由查找。由于未找到与该特定地址相对应的条目，因此路由模块将该地址解析到一个通过 ethernet3 的路由， ethernet3 被绑定到 Untrust 区段。通过确定入口接口和出口接口，从而 NetScreen 设备确定了源区段和目标区段，因此现在即可执行策略查找。

策略查找：策略引擎在 Trust 和 Untrust 区段间执行策略查找。查找与源地址和源区段、目标地址和目标区段以及服务相匹配，并且找到了引用名为 vpn1 的 VPN 通道的策略。

然后， NetScreen 设备通过 ethernet1 将数据包转发到其目标 10.2.2.5。

巴黎 (接收方)

除了通道不是绑定到通道接口，而是绑定到通道区段之外，接收方一端的入站数据包流的大部分阶段都与基于路由和基于策略的 VPN 配置相同。 NetScreen 设备获知数据包来自绑定到 Untrust-Tun 通道区段的 vpn1，该通道区段的承载区段为 Untrust 区段。与基于路由的 VPN 不同， NetScreen 设备将 ethernet3 (而不是 tunnel.1) 视为解密数据包的入口接口。

数据包解密完成后数据包流将发生更改。此时，路由查找和策略查找的区别如下：

路由查找：路由模块对 10.2.2.5 执行路由查找，并发现可通过绑定到 Trust 区段的 ethernet1 对其进行访问。通过获知 Untrust 区段是源区段 (由于 vpn1 被绑定到了 Untrust-Tun 通道区段，该区段的承载区段为 Untrust 区段) 并根据出口接口确定了目标区段 (ethernet1 被绑定到 Trust 区段)，现在 NetScreen 设备可以从 Untrust 区段到 Trust 区段检查引用 vpn1 的策略。

策略查找：策略引擎从 Untrust 区段到 Trust 区段检查其策略列表，找到了一个引用名为 vpn1 的 VPN 通道并准许访问 10.2.2.5 的策略。

然后 NetScreen 设备将该数据包转发到其目标。

通道配置技巧

本节介绍配置 VPN 通道时要记住的一些准则或技巧。配置 IPSec VPN 通道时，请记住以下要点：

- NetScreen 最多支持四个 “阶段 1” 协商的提议及最多四个 “阶段 2” 协商的提议。必须配置对等方以接受由其它对等方提供的至少一个 “阶段 1” 提议和一个 “阶段 2” 提议。有关 “阶段 1” 和 “阶段 2” IKE 协商的信息，请参阅第 11 页上的 “通道协商”。
- 如果想使用证书进行认证，并且 NetScreen 设备上存在多个已加载的本地证书，则必须指定希望每个 VPN 通道配置使用的证书。有关证书的详细信息，请参阅第 2 章，第 23 页上的 “公开密钥密码术”。
- 对于基于策略的基本 VPN:
  - 使用策略中用户定义的地址，而不是预定义地址 “Any”。
  - 在 VPN 的两端配置的策略中所指定的地址和服务必须匹配。
  - 对双向 VPN 信息流使用对称策略。
- 两个对等方的代理 ID 必须匹配，这就意味着两个对等方的代理 ID 中所指定的服务相同，并且为一个对等方指定的本地 IP 地址与为另一个对等方指定的远程 IP 地址相同[2]。
  - 对于基于路由的 VPN 配置，用户可对代理 ID 进行配置。
  - 对于基于策略的 VPN 配置，在缺省情况下，NetScreen 设备从策略 (引用策略列表中的该 VPN 通道) 中指定的源地址、目标地址和服务中导出代理 ID。还可为基于策略的 VPN 定义代理 ID，该 ID 将取代导出的代理 ID。

  确保代理 ID 匹配的最简便方法就是使用 0.0.0.0/0 作为本地地址，使用 0.0.0.0/0 作为远程地址[3]，使用 “any” 作为服务。不是使用代理 ID 进行访问控制，而是使用策略对进出 VPN 的信息流进行控制。有关带有用户可配置的代理 ID 的 VPN 配置的范例，请参阅第 4 章，“站点到站点 VPN”中基于路由的 VPN 范例。

2. 代理 ID 是一个三方元组，由本地 IP 地址、远程 IP 地址和服务组成。
3. 当远程地址为拨号 VPN 客户端的虚拟内部地址时，请使用 255.255.255.255/32 作为代理 ID 中的远程 IP 地址 / 网络掩码。

- 如果对等方的代理 ID 设置相匹配，即使一个对等方定义了基于路由的 VPN 而另一个对等方定义了基于策略的 VPN 也无关紧要。如果对等方 1 使用基于策略的 VPN 配置而对等方 2 使用基于路由的 VPN 配置，则对等方 2 必须定义与从对等方 1 的策略导出的代理 ID 相匹配的代理 ID[4]。如果对等方 1 使用 DIP 池执行源网络地址转换 (NAT-src)，则应将该 DIP 池的地址和网络掩码用作对等方 2 的代理 ID 中的远程地址。例如：

DIP 池为：	在代理 ID 中使用：
1.1.1.8 – 1.1.1.8	1.1.1.8/32
1.1.1.20 – 1.1.1.50	1.1.1.20/26
1.1.1.100 – 1.1.1.200	1.1.1.100/25
1.1.1.0 – 1.1.1.255	1.1.1.0/24

  有关代理 ID 与 NAT-src 和 NAT-dst 配合使用的详细信息，请参阅第 199 页上的 “具有重叠地址的 VPN 站点”。
- 由于代理 ID 支持单个服务或所有服务，因此从引用服务组的基于策略的 VPN 导出的代理 ID 中的服务被认为是 “any”。
- 当两个对等方都具有静态 IP 地址时，他们都可使用缺省 IKE ID (其 IP 地址)。当一个对等方或拨号用户拥有动态分配的 IP 地址时，该对等方或用户必须使用另外一种 IKE ID。若为动态对等方，建议使用 FQDN；若为拨号用户，建议使用 U-FQDN (电子邮件地址)。可以使用具有预共享密钥和证书的 FQDN 和 U-FQDN IKE ID 类型 (如果 FQDN 或 U-FQDN 出现在证书的 SubjectAltName 字段中)。如果使用证书，则动态对等方或拨号用户也可使用 ASN1-DN 的全部或部分内容作为 IKE ID。

4. 对等方 1 还可定义与对等方 2 的代理 ID 相匹配的代理 ID。此时，对等方 1 的用户定义的代理 ID 将取代 NetScreen 设备从策略组件导出的代理 ID。

基于路由的 VPN 安全注意事项

虽然路由的变化不影响基于策略的 VPN，但却影响基于路由的 VPN。 NetScreen 设备使用静态和动态两种路由协议可通过基于路由的 VPN 通道来发送数据包。只要不发生路由更改， NetScreen 设备就会持续地加密和转发目标为绑定到基于路由的 VPN 通道的通道接口的数据包。

但是，当将 VPN 监控用于基于路由的 VPN 通道配置时，通道的状态可能会由连接变为中断。此时，引用绑定到该通道的通道接口的所有路由表条目都将变为非活动状态。然后，当对最初要加密及通过通道 (绑定到该通道接口) 发送的信息流进行路由查找时， NetScreen 设备将绕过引用该通道接口的路由，并搜索具有下一个最长匹配的路由。找到的路由可能是缺省路由。然后， NetScreen 设备使用此路由通过非通道接口将未加密的 (即 *明文*或*纯文本*格式) 信息流发送到公共 WAN。

为了避免将最初要发往 VPN 通道的信息流以明文格式重新路由到公共 WAN，可配置 NetScreen 设备，使其将这样的信息流重新路由到另一个通道或租用线路，或者干脆丢弃它，您可使用以下工作方式之一来实现这一操作：

- 第 91 页上的 “Null 路由”(当通向通道接口的路由变为非活动时丢弃信息流)
- 第 93 页上的 “拨号或租用线路”(当通向通道接口的路由变为非活动时将信息流重新路由到一个备用的安全路径)
- 第 97 页上的 “引诱通道接口”(当通向通道接口的路由变为非活动时丢弃信息流)
- 第 98 页上的 “通道接口的虚拟路由器”(当通向通道接口的路由变为非活动时丢弃信息流)
- 第 98 页上的 “重新路由到另一个通道”(当通向通道接口的路由变为非活动时将信息流重新路由到一个备用的 VPN 通道)

Null 路由

如果 VPN 通道的状态变为 “断开”，则 NetScreen 设备会将任何引用该通道接口的路由更改为 “非活动”。如果通向该通道接口的路由变为不可用，且下一可选路由为缺省路由 (举例)，则 NetScreen 设备将使用缺省路由来转发最初要发送给 VPN 通道的信息流。当发生路由更改时，为了避免将信息流以纯文本格式发送到公共 WAN，可使用 Null 路由。 Null 路由的目标地址与通过通道接口的路由的目标地址相同，不过 Null 路由将信息流引向 Null 接口。 Null 接口是丢弃发送给该接口的信息流的逻辑接口。为 Null 路由分配的度量 (远离零) 要高于使用通道接口的路由的度量，以使 Null 路由具有较低的优先级。

***注意：** ScreenOS 5.1.0 之前的版本不支持 Null 接口。但是，您可使用引诱通道接口来实现相同的目标。有关信息，请参阅第 97 页上的 “引诱通道接口”。*

例如，如果创建一个经由 tunnel.1 通向远程 LAN (IP 地址为 10.2.2.0/24) 的静态路由，则该路由将自动接受缺省值 1 作为其度量：

```
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
get route
…
Dest-Routes for <trust-vr> (4 entries)
```

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	3	0.0.0.0/0	eth3	1.1.1.250	S	20	1	Root
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	Root
*	1	10.1.1.0/24	eth1	0.0.0.0	C	0	0	Root
*	4	**10.2.2.0/24**	**tun.1**	0.0.0.0	S	20	**1**	Root

在上面的路由表中，星号 (*) 表示路由是活动的，“S” 表示 “静态路由”，而 “C” 则表示 “已连接路由”。在上面的路由表中， NetScreen 设备具有两个可到达 10.2.2.0/24 子网中的任意一个地址的路由。第一个可选路由是 4 号路由，因为它与该地址具有最长匹配。第二个可选路由是缺省路由 (0.0.0.0/0)。

如果随后添加了一个通过 Null 接口通向 10.2.2.0/24 的路由，并为其分配了一个大于 1 的值，则该路由将成为可到达 10.2.2.0/24 子网中任意一个地址的第二个可选路由。如果通过 tunnel.1 通向 10.2.2.0/24 的路由变为了非活动路由，则 NetScreen 设备将使用通向 Null 接口的路由。NetScreen 设备会将发往 10.2.2.0/24 的信息流转发给该接口，然后丢弃它。

```
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
get route
…
Dest-Routes for <trust-vr> (5 entries)
```

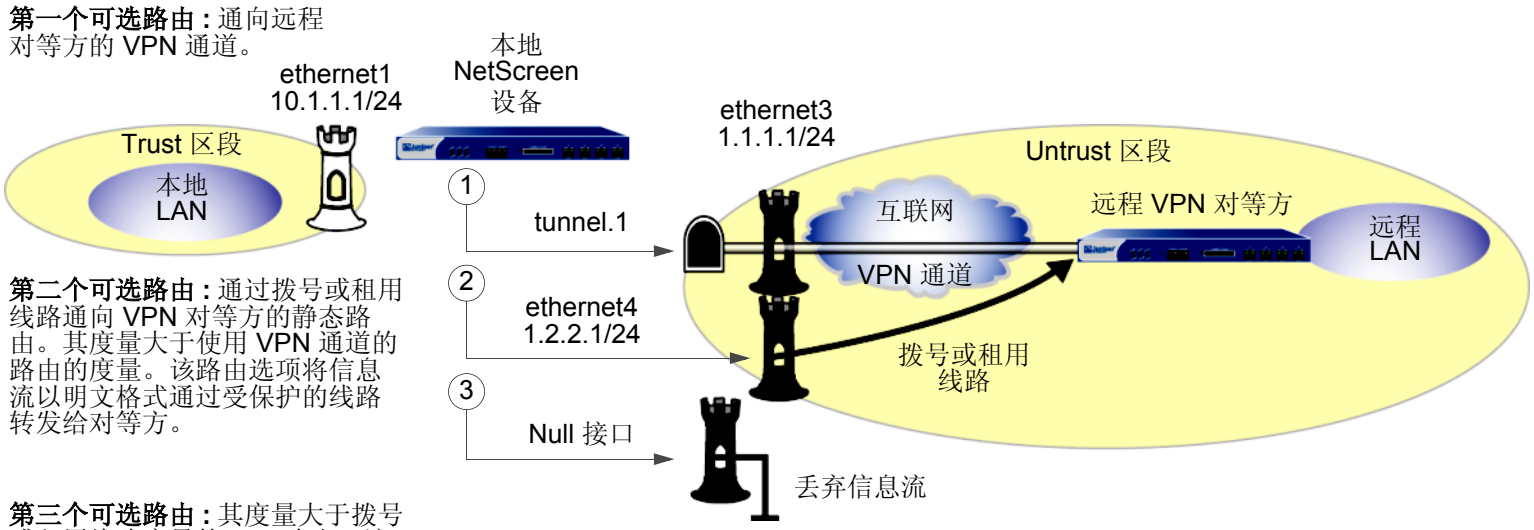
	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	3	0.0.0.0/0	eth3	1.1.1.250	S	20	1	Root
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	Root
*	1	10.1.1.0/24	eth1	0.0.0.0	C	0	0	Root
	4	**10.2.2.0/24**	**tun.1**	0.0.0.0	S	20	**1**	Root
*	5	**10.2.2.0/24**	**null**	0.0.0.0	S	20	**10**	Root

在上面的路由表中，通过 tunnel.1 通向 10.2.2.0/24 的路由是非活动的 (以左边第一列中无星号的方式进行标明)。因此， NetScreen 设备将搜索下一个与目标地址最长匹配的路由，并找到了 5 号路由。 (5 号路由之后的下一可选路由是 ID 号为 3 的缺省路由。) 随后， NetScreen 设备会将发往 10.2.2.0/24 的信息流转发给 Null 接口，并由该接口丢弃此信息流。因而，当使用 tunnel.1 的路由变为非活动时， NetScreen 设备将丢弃发往 10.2.2.0/24 的信息流，而不是使用 3 号路由将其以明文格式由 ethernet3 转发给 1.1.1.250 处的路由器。

拨号或租用线路

当通向远程对等方的通道变为非活动时，如果不想丢弃发送给该对等方的信息流，可为该对等方添加一个通过拨号或租用线路传送信息流的备用路由。该备用路由的目标 IP 地址与通过 VPN 通道的路由的目标 IP 地址相同，但该备用路由具有不同的出口接口和较低的优先级度量。如果通过 VPN 通道的路由变为非活动的，则 NetScreen 设备将通过拨号或租用线路将信息流重新路由到远程对等方。

当使用拨号或租用线路作为下一个可选路由时，第一个和第二个可选路由仍可能同时变为非活动的。此时，NetScreen 设备将使用第三个可选路由，该路由可能是缺省路由。由于预料到会发生这样的情况，您可将拨号或租用线路路由作为第二个可选路由，而将 Null 路由作为第三个可选路由 (请参阅第 91 页上的 “Null 路由”)。下图说明了这些处理路由故障切换的选项是如何协同工作的。



范例 : 租用线路或 Null 路由 VPN 故障切换

在本例中，您想让来自 NetScreen-A 后面的分公司的信息流通过安全的 VPN 连接到达 NetScreen-B 后面的企业网络。如果该通道出现故障，则让信息流通过租用线路流向企业办公室。如果 VPN 通道和租用线路都出现故障，则让 NetScreen-A 丢弃信息流，而不是将其以明文格式发送到互联网。

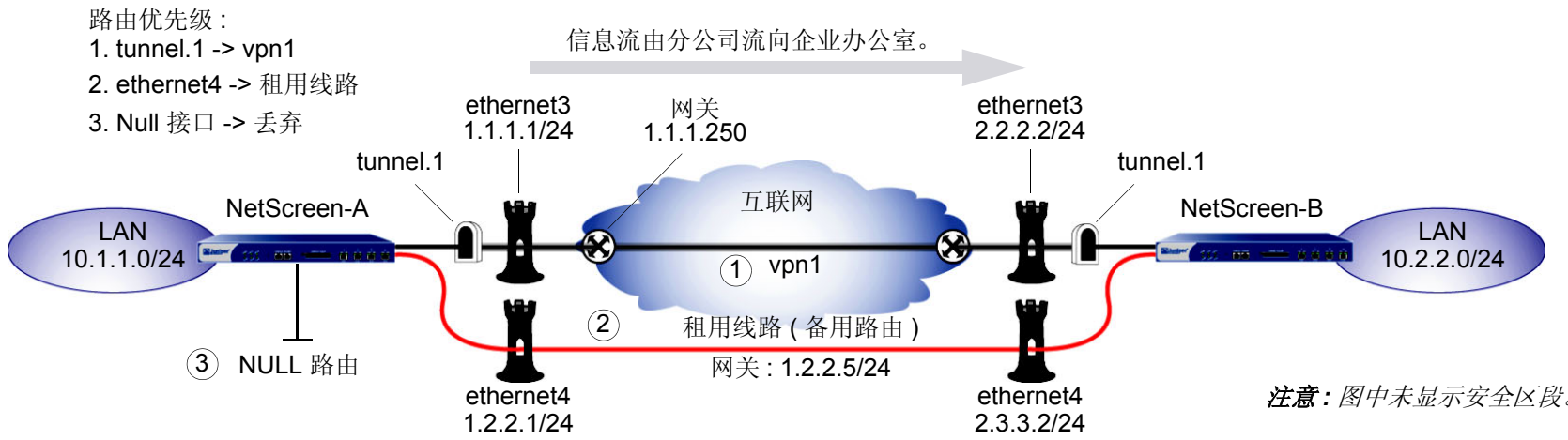
在 NetScreen-A 上创建三个到达 10.2.2.0/24 的路由并为它们分配不同的度量 :

- 首选路由 – 使用绑定到 vpn1 的 tunnel.1 (度量 = 1)
- 二级路由 – 使用 ethernet4 和 1.2.2.5 处的网关以使用租用线路 (度量 = 2)
- 三级路由 – 使用 Null 接口以丢弃信息流 (度量 = 10)

创建首选路由时，使用静态路由的缺省度量，即 1。为二级路由分配度量 2，即通过租用线路的备用路由 (如下图红线所示)。其度量大于通过 VPN 通道的首选路由的度量。 NetScreen 设备通常不使用二级路由，除非通过 VPN 通道的首选路由发生故障。

最后，添加一个度量为 10 的 NULL 路由。如果首选路由发生故障，且随后二级路由也发生故障，则 NetScreen 设备将丢弃所有数据包。所有安全区段都在 trust-vr 路由选择域中。

注意 : *本例仅介绍了 NetScreen-A 上四个路由的配置 — 用于故障切换的三个路由 + 缺省路由。但未介绍对其它必要元素 (例如接口和策略) 的配置。*



WebUI (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

Metric: 1

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

Metric: 1

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: ethernet4

Gateway IP Address: 1.2.2.5

Metric: 2

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: Null

Gateway IP Address: 0.0.0.0

Metric: 10

CLI (NetScreen-A)

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface ethernet4 gateway 1.2.2.5
    metric 2
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
save
```

可通过执行 **get route** 命令来检验新路由是否存在。

```
ns-> get route
…
Dest-Routes for <trust-vr> (7 entries)
```

	ID	IP-Prefix	Interface	Gateway	P	Pref	Mtr	Vsys
*	4	0.0.0.0/0	eth3	1.1.1.250	S	20	1	Root
*	2	1.1.1.0/24	eth3	0.0.0.0	C	0	0	Root
*	7	10.2.2.0/24	null	0.0.0.0	S	20	10	Root
*	5	10.2.2.0/24	tunnel.1	0.0.0.0	S	20	1	Root
*	6	10.2.2.0/24	eth4	1.2.2.5	S	20	2	Root
*	1	10.1.1.0/24	eth1	0.0.0.0	C	0	0	Root
*	3	1.2.2.0/24	eth4	0.0.0.0	C	0	0	Root

ID 号为 5 的路由表条目将目标为 10.2.2.0/24 的信息流引向 tunnel.1，然后再通过 VPN 通道。该路由是通向 10.2.2.0 网络的信息流的首选路由。如果该通道发生故障，则下一最佳路由是条目 6，即通过 1.2.2.5 处的网关的租用线路。如果路由条目 6 的连接发生故障，则路由条目 7 将成为下一最佳路由，而 NetScreen 设备会将目标为 10.2.2.0/24 的信息流引向 Null 接口，该接口随后丢弃此信息流。

引诱通道接口

除了将信息流从 VPN 通道改发到 Null 接口 (并随后丢弃它) 之外，还可通过非使用中的通道接口来实现同一目标。

***注意：** ScreenOS 5.1.0 之前的版本不支持 Null 接口 (请参阅第 91 页上的 “Null 路由”)。但是，您可使用引诱通道接口来实现相同的目标。*

要设置引诱通道接口，请执行以下操作：

1. 再创建一个通道接口，但不要将其绑定到 VPN 通道。而应将其绑定到一个通道区段，该通道区段与第一个通道接口所绑定到的区段位于同一虚拟路由选择域中[5]。
2. 使用第二个通道接口再定义一个通向同一目标的路由，并为该路由分配一个比首选路由的度量高的度量 (远离零)。

   当使用中的通道接口的状态由连接变为中断且引用该接口的路由表条目变成非活动时，所有的后续路由查找都可找到这个通往非使用中的通道接口的第二个路由。NetScreen 设备将信息流转发到第二个通道接口，由于该接口未绑定到 VPN 通道，因此设备将丢弃信息流。

5. 如果通道接口被绑定到通道区段，则其状态始终为连接。

通道接口的虚拟路由器

为了避免通过 VPN 通道的路由变为中断以及随后将最初要通过该通道的信息流改发到缺省路由，可为 VPN 信息流创建一个专用虚拟路由选择域。要完成此设置，请执行以下步骤：

1. 创建一个单独的虚拟路由器，用于指向通道接口的所有路由，并为该虚拟路由器命名，例如“VR-VPN”。
2. 创建一个安全区段 (例如，名为 “VPN zone”的安全区段)，并将其绑定到 VR-VPN。
3. 将所有通道接口绑定到该 VPN 区段，并将希望通过 VPN 通道到达的远程站点的所有地址放在此区段中。
4. 对于要加密并通过通道发送的信息流，配置通往 VR-VPN 的其它所有虚拟路由器中的静态路由。必要时，为从 VR-VPN 到其它虚拟路由器的已加密信息流定义静态路由。当从远程站点发起入站 VPN 信息流时，如果要允许该信息流通过通道，这些路由是必需的。

   如果通道接口的状态由连接变为中断，NetScreen 设备依然会将信息流转发到 VR-VPN。由于通往该接口的路由当前处于非活动状态，并且没有任何其它匹配路由，因此 NetScreen 设备将在 VR-VPN 上丢弃信息流。

重新路由到另一个通道

可为同一个远程对等方配置两个或多个 VPN 通道。如果其中的一个通道产生了中断， NetScreen 设备会通过另一个 VPN 通道重新路由信息流。有关配置冗余 VPN 通道的信息和范例，请参阅以下内容：

- 第 **10**-69 页上的 “Dual Untrust 接口”
- 第 **10**-78 页上的 “范例：由活动通道到备份通道的故障切换”
- 第 **10**-86 页上的 “范例：双活动通道”
- 第 **10**-93 页上的 “范例：对通道故障切换应用权重”

4

站点到站点 VPN

本章说明如何在两台 NetScreen 设备间配置站点到站点的虚拟专用网络 (VPN) 通道。阐述基于路由和基于策略的 VPN 通道，介绍设置通道时必须考虑的各种元素，并提供几个范例。

站点到站点 VPN 配置

IPSec VPN 通道存在于两个网关之间，同时每个网关都需要一个 IP 地址。当两个网关都拥有静态 IP 地址时，可配置以下种类的通道：

- 站点到站点 VPN，自动密钥 IKE 通道 (具有预共享密钥或证书)
- 站点到站点 VPN，手动密钥通道

当一个网关拥有静态地址，而另一个网关拥有动态分配的地址时，可配置以下种类的通道：

- 动态对等方站点到站点 VPN，自动密钥 IKE 通道 (具有预共享密钥或证书)

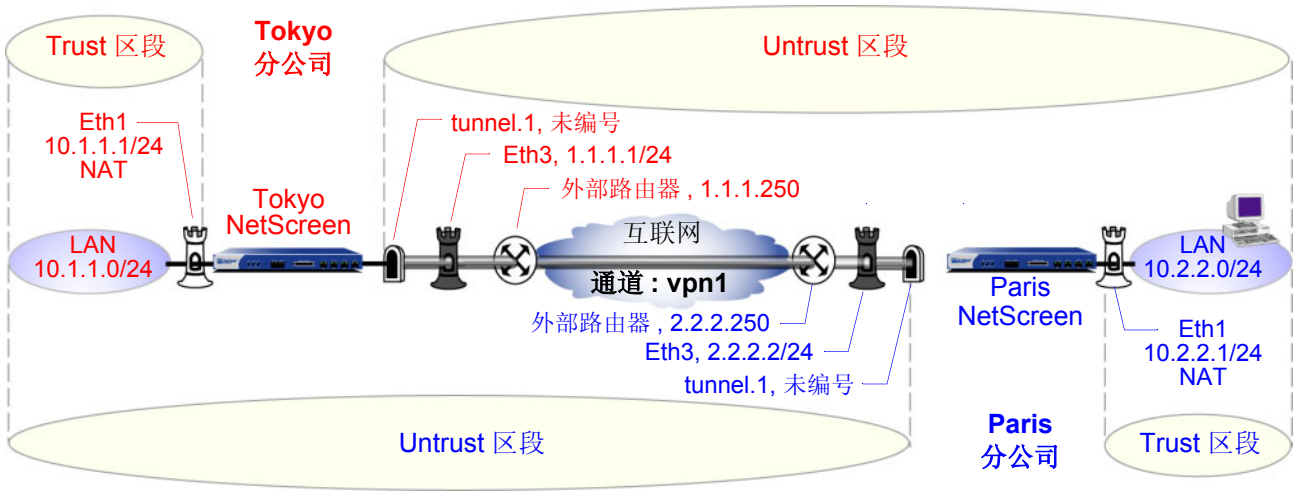
用于此处时，静态站点到站点 VPN 包括一个连接两个站点的 IPSec 通道，每个站点都拥有一个作为安全网关的 NetScreen 设备。在两个设备上用作出接口的物理接口或子接口都有一个固定的 IP 地址，同时内部主机也拥有静态 IP 地址。如果 NetScreen 设备处于 “透明” 模式下，则它将 VLAN1 地址当作出接口的 IP 地址使用。对于静态站点到站点 VPN，由于远程网关的 IP 地址保持不变而可以到达，因此，位于通道任一端的主机都可启动 VPN 通道设置。

如果其中一个 NetScreen 设备的出接口具有动态分配的 IP 地址，则该设备在术语上被称为 “动态对等方”，并且具有不同的 VPN 配置。对于动态对等方站点到站点 VPN，由于只有那些位于动态对等方后面的主机的远程网关才有固定的 IP 地址，并且可以从它们的本地网关到达，因此只有它们才能启动 VPN 通道设置。但是，当在动态对等方和静态对等方之间建立通道之后，如果目标主机有固定的 IP 地址，则在两个网关之中的任一个网关后面的主机均可发起 VPN 信息流。

注意：*有关可用 VPN 选项的背景信息，请参阅第 1 章，“IPSec”。有关从多种选项中进行选择的指导，请参阅第 3 章，“VPN 准则”。*

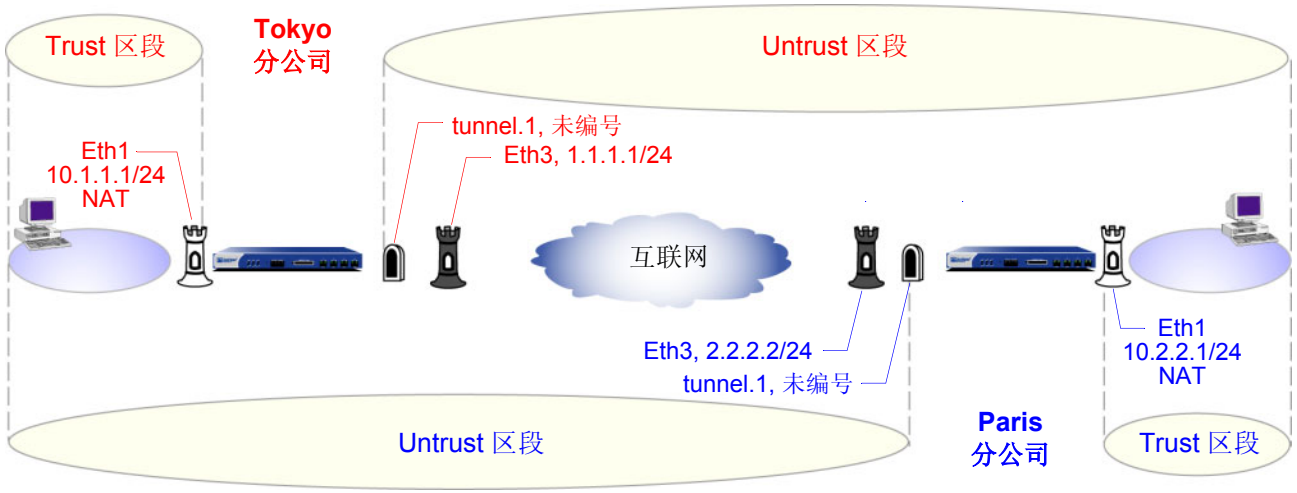
站点到站点通道的配置步骤

站点到站点 VPN 通道的配置需要协调通道配置以及其它设置 (接口、地址、路由和策略)。本节中三个 VPN 配置范例的环境如下 : 东京 (Tokyo) 分公司想通过 IPSec VPN 通道与巴黎 (Paris) 分公司进行安全通信。



两个分公司的管理员配置以下设置 :

- 接口 – 安全区段和通道
- 地址
- VPN (下列之一)
  - 自动密钥 IKE
  - 动态对等方
  - 手动密钥
- 路由
- 策略



1. 接口 – 安全区段和通道

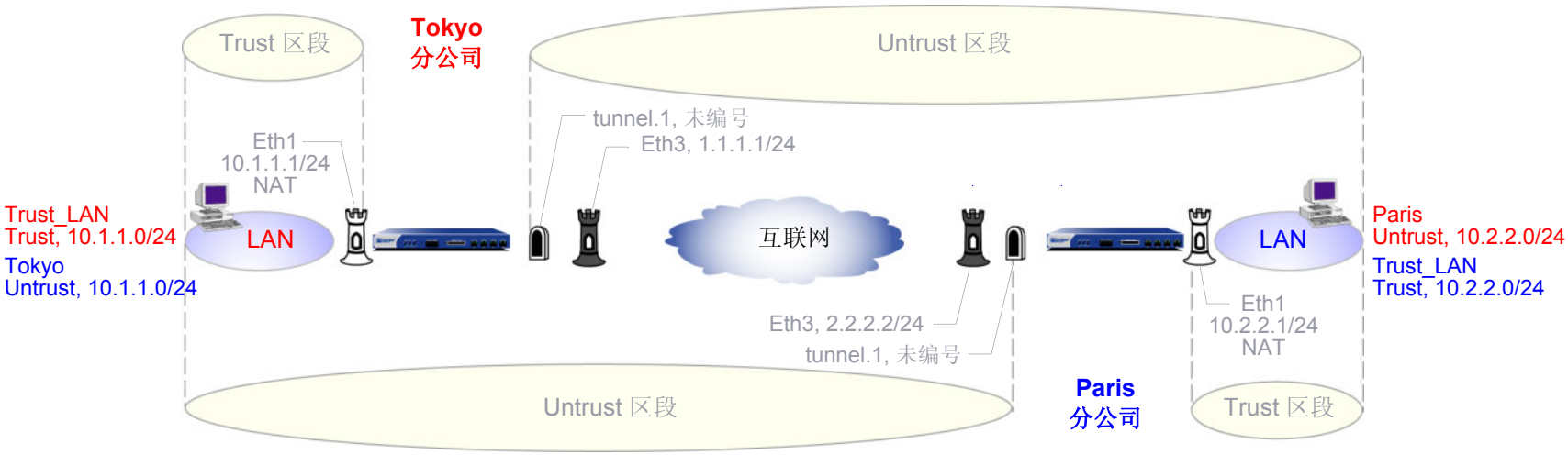
东京分公司的 admin 使用上图中以红色显示的设置来配置安全区段和通道接口。而巴黎分公司的 admin 使用以蓝色显示的设置来配置安全区段和通道接口。

Ethernet3 将成为 VPN 信息流的出接口及从通道另一端发送的 VPN 信息流的远程网关。

Ethernet1 处于 NAT 模式，因此每个 admin 都可以为所有内部主机分配 IP 地址，然而，当信息流从 Trust 区段传递到 Untrust 区段时， NetScreen 设备会将数据包包头中的源 IP 地址转换为 Untrust 区段接口 ethernet3 的地址 (东京为 1.1.1.1，巴黎为 2.2.2.2)。

对于基于路由的 VPN，每个 admin 都将通道接口 tunnel.1 绑定到 VPN 通道 vpn1。通过定义通向远程办公室 LAN 的地址空间的路由， NetScreen 设备可将为该 LAN 绑定的所有信息流引导到 tunnel.1 接口，从而可通过绑定了 tunnel.1 的通道。

由于不需要基于策略的 NAT 服务，因此，基于路由的 VPN 配置不要求 tunnel.1 具有 IP 地址 / 网络掩码，基于策略的 VPN 配置甚至不需要通道接口。



2. 地址

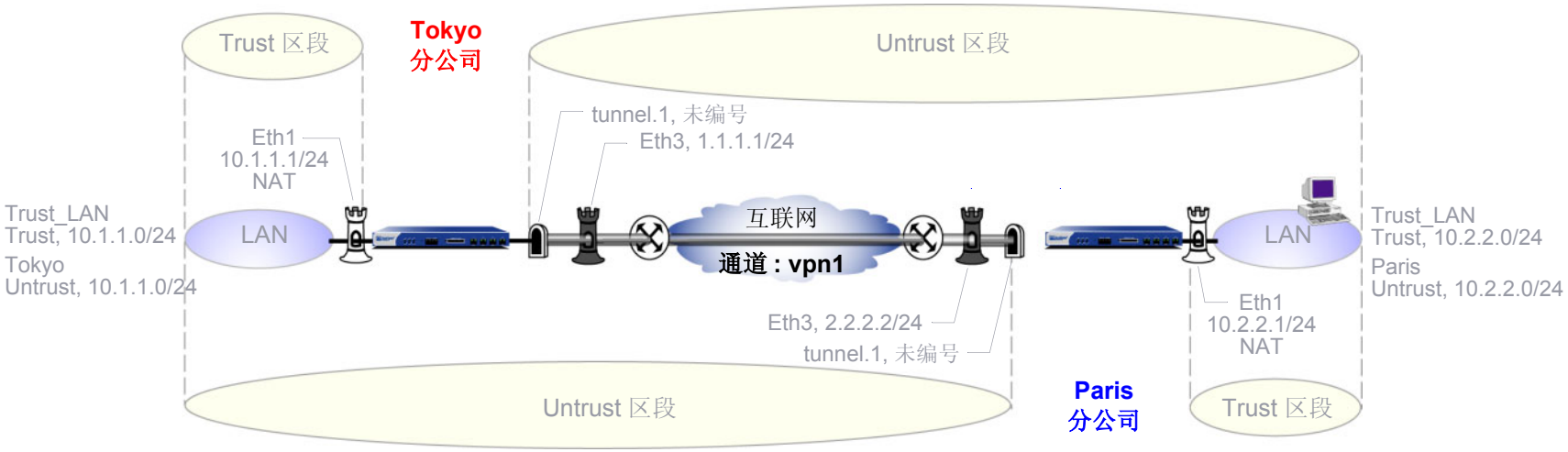
admin 定义地址，以备以后在入站和出站策略中使用。东京分公司的 admin 定义上图中以红色显示的地址。而巴黎分公司的 admin 定义上图中以蓝色显示的地址。

对于基于策略的 VPN， NetScreen 设备从策略导出代理 ID[1]。由于 VPN 通道两端的 NetScreen 设备使用的代理 ID 必须完全匹配，因此，如果在通道一端使用了较为具体的地址，则在通道另一端不能使用 IP 地址为 0.0.0.0/0 的预定义地址 “ANY”。例如，

如果东京的代理 ID 是 …		并且巴黎的代理 ID 是 …	则代理 ID 不匹配，并且 IKE 协商将失败。
From: 0.0.0.0/0	✗	To: 10.1.1.0/24	
To: 10.2.2.0/24	✓	From: 10.2.2.0/24	
Service: ANY	✓	Service: ANY	

对于基于路由的 VPN，可以使用 “0.0.0.0/0–0.0.0.0/0–any” 来定义代理 ID 的本地和远程 IP 地址及服务类型。然后可使用更为严格的策略，根据源地址、目标地址和服务类型来过滤入站和出站 VPN 信息流。

1. 在 ScreenOS 5.0.0 中，还可为基于策略的 VPN 配置中引用的 VPN 通道定义代理 ID。



3. VPN

可以配置下列三种 VPN 中的其中一种 :

– 自动密钥 IKE

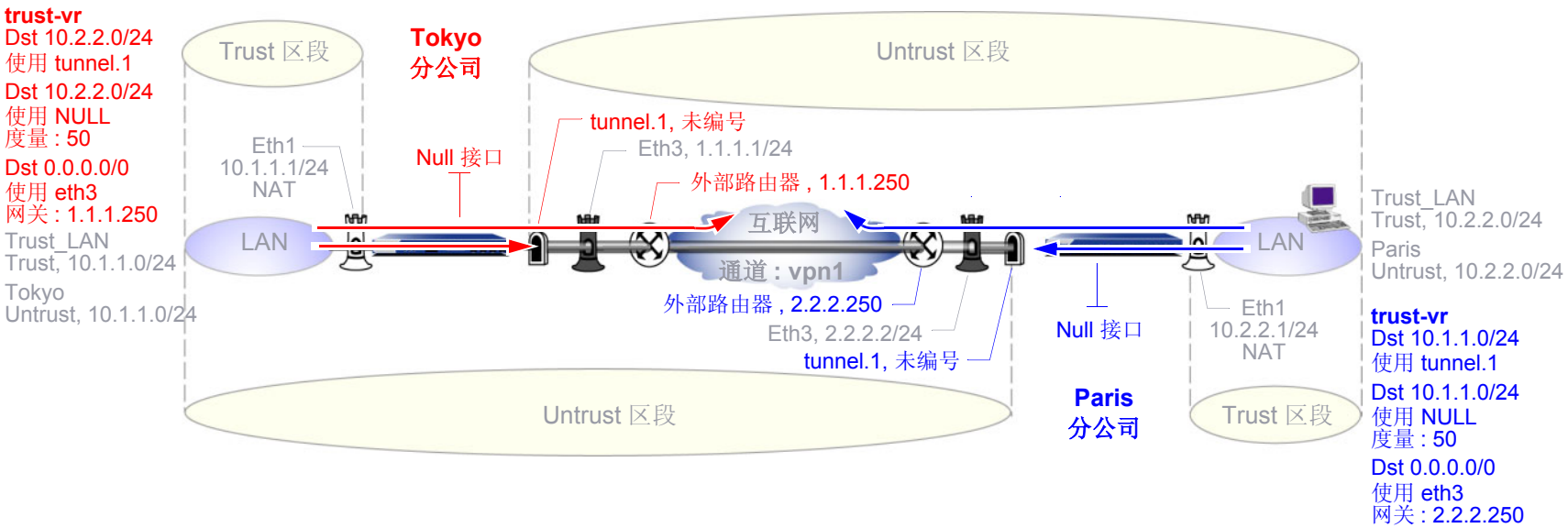
“自动密钥 IKE”方法使用预共享密钥或证书以用户定义的时间间隔 (称为密钥生存期) 自动刷新 (即更改) 加密和认证密钥。实际上，尽管生存期过短可能会降低整体性能，不过，经常更新这些密钥会加强安全。

– 动态对等方

动态对等方是具有动态分配的 IP 地址的远程网关。由于每次 IKE 协商开始时远程对等方的 IP 地址可能不同，因此对等方后面的主机必须发起 VPN 信息流。另外，如果使用预共享密钥进行认证，则在 Aggressive 模式下 “阶段 1”协商的第一条消息期间，对等方必须发送 IKE ID 以对自身进行识别。

– 手动密钥

“手动密钥”方法要求手动设置及更新加密和认证密钥。对于数量不多的一组 VPN 通道，此方法是一个可行的选项。

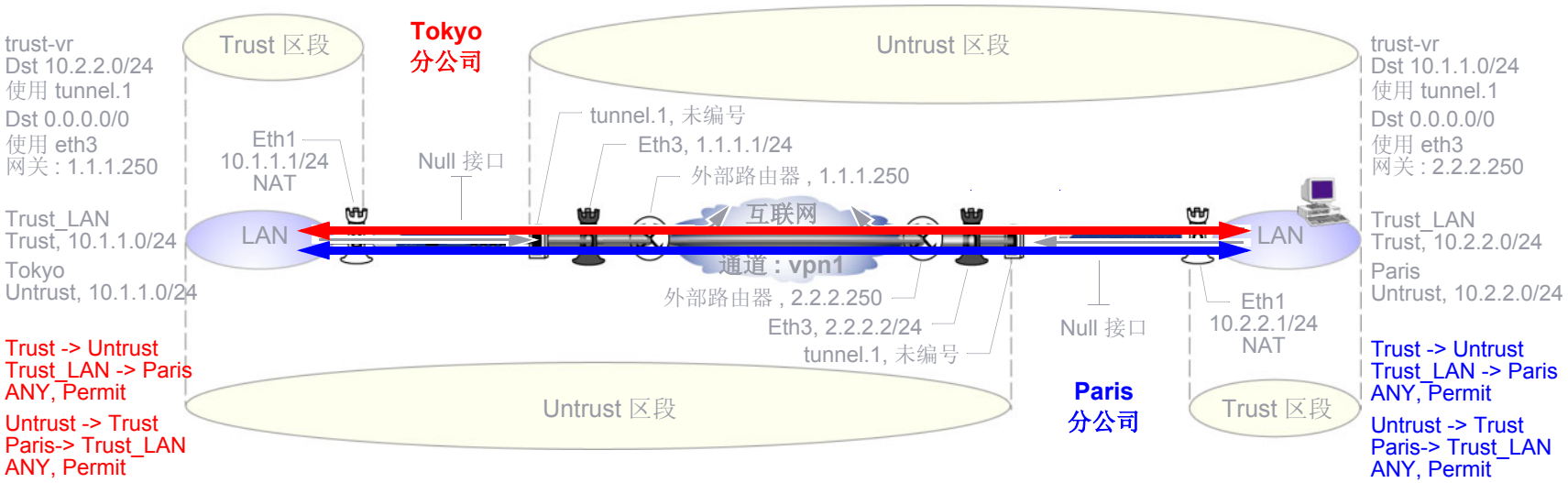


4. 路由

每个站点的 admin 至少应配置以下路由 :

- 可到达使用 tunnel.1 的远程 LAN 上的某个地址的信息流的路由
- 其它所有信息流的缺省路由，包括通过 ethernet3 然后再经由分公司地址 (东京分公司为 1.1.1.250，巴黎分公司为 2.2.2.250) 之外的外部路由器到达互联网的外部 VPN 通道信息流[2]。外部路由器是缺省网关， NetScreen 设备将其路由表中没有特定路由的任何信息流转发到该网关。
- Null 路由，若使用了该路由，如果 tunnel.1 的状态变为 “中断” 且任何引用 tunnel.1 的路由都被中断，则 NetScreen 设备将不使用缺省路由来转发通往远程 LAN 未经加密就发送出 ethernet3 的信息流。 Null 路由使用远程 LAN 作为其目标地址，但它将信息流指向 Null 接口，即丢弃发送给它的信息流的逻辑接口。为 Null 路由分配的度量 (远离零) 要高于通向远程 LAN 的路由 (使用 tunnel.1) 的度量，以使 Null 路由的优先级低于引用 tunnel.1 接口的路由。

2. 如果东京分公司的 NetScreen 设备收到了来自其 ISP 的动态分配的外部 IP 地址 (即，从巴黎分公司的角度来说，东京分公司的 NetScreen 设备是其动态对等方)，则 ISP 将为东京 NetScreen 自动提供缺省网关 IP 地址。



5. 策略

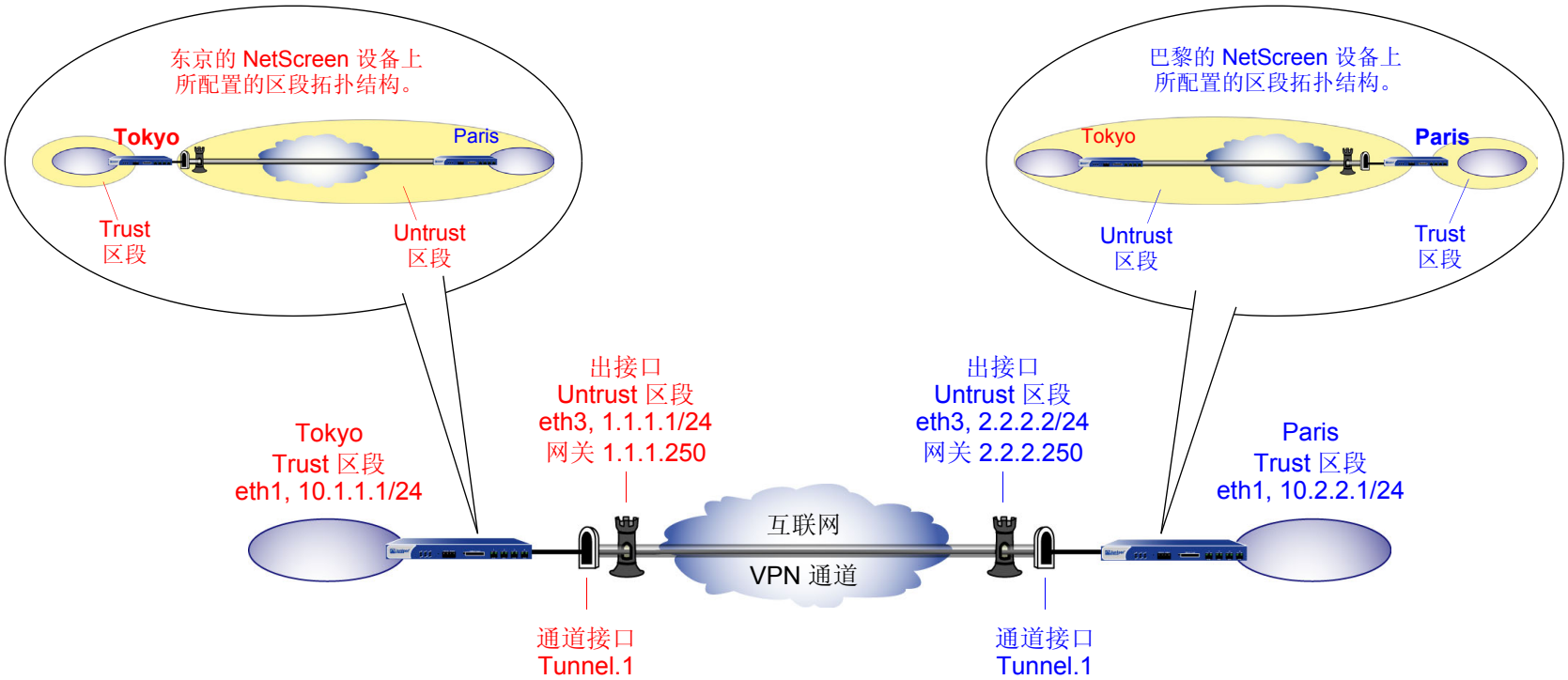
每个站点的 admin 定义允许这两个分公司间信息流的策略 :

- 允许从 Trust 区段中的 “Trust_LAN” 到 Untrust 区段中的 “Paris” 或 “Tokyo” 的任何种类的信息流的策略
- 允许从 Untrust 区段中的 “Paris” 或 “Tokyo” 到 Trust 区段中的 “Trust_LAN” 的任何种类的信息流的策略

由于通向远程站点的首选路由指定了绑定到 VPN 通道 vpn1 的 tunnel.1，因此，策略不需要引用 VPN 通道。

范例：基于路由的站点到站点 VPN，自动密钥 IKE

在本例中，“自动密钥 IKE”通道使用预共享密钥或一对证书 (通道两端各一个) 来提供东京 (Tokyo) 分公司与巴黎 (Paris) 分公司之间的安全连接。对于 “阶段 1”和 “阶段 2”安全级别，指定一个 “阶段 1”提议：为预共享密钥方法指定 pre-g2-3des-sha 或为证书指定 rsa-g2-3des-sha，并为 “阶段 2”选择预定义的 “Compatible”提议集。所有区段都在 trust-vr 中。



使用预共享密钥或证书来设置基于路由的 “自动密钥 IKE”通道，具体步骤如下：

1. 为绑定到安全区段和通道接口的物理接口分配 IP 地址。
2. 配置 VPN 通道，在 Untrust 区段内指定其出接口，将其绑定到通道接口，并配置其代理 ID。
3. 在 Trust 和 Untrust 区段的通讯簿中输入本地及远程端点的 IP 地址。

4. 输入通向 trust-vr 中外部路由器的缺省路由、通过通道接口通向目标的路由以及通向目标的 Null 路由。为 Null 路由分配较高的度量 (远离零)，以便其成为通向目标的下一个可选路由。那么，如果通道接口的状态变为 “中断”，且引用该接口的路由变为非活动，则 NetScreen 设备会使用 Null 路由 (即实质上丢弃了发送给它的任何信息流的路由)，而不使用缺省路由 (即转发未加密的信息流的路由)。
5. 为各个站点间通过的 VPN 信息流设置策略。

在下面的例子中，预共享密钥为 h1p8A24nG5。假定两个参与者都已有 RSA 证书，并将 Entrust 用作证书授权机构 (CA)。(有关获取和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。)

WebUI (东京)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

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

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

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

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Paris

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

Security Level: Compatible

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

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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: 10.2.2.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Name: To_Paris

Source Address: Trust_LAN

Destination Address: Paris_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From_Paris

Source Address: Paris_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

WebUI (巴黎)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP / Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

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

Name: Paris_Tokyo

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Tokyo

> 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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.2.2.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address/Netmask: 10.1.1.0/24

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: 10.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Name: To_Tokyo

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From_Tokyo

Source Address:

Address Book Entry: (选择), Tokyo_Office

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

CLI (东京)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

预共享密钥

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(或)

证书

```
set ike gateway To_Paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1[3]
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. 策略

```
set policy top name "To Paris" from trust to untrust Trust_LAN Paris_Office any
    permit
set policy top name "From Paris" from untrust to trust Paris_Office Trust_LAN
    any permit
save
```

3. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。

CLI (巴黎)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

预共享密钥

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(或)

证书

```
set ike gateway To_Tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

4. 路由

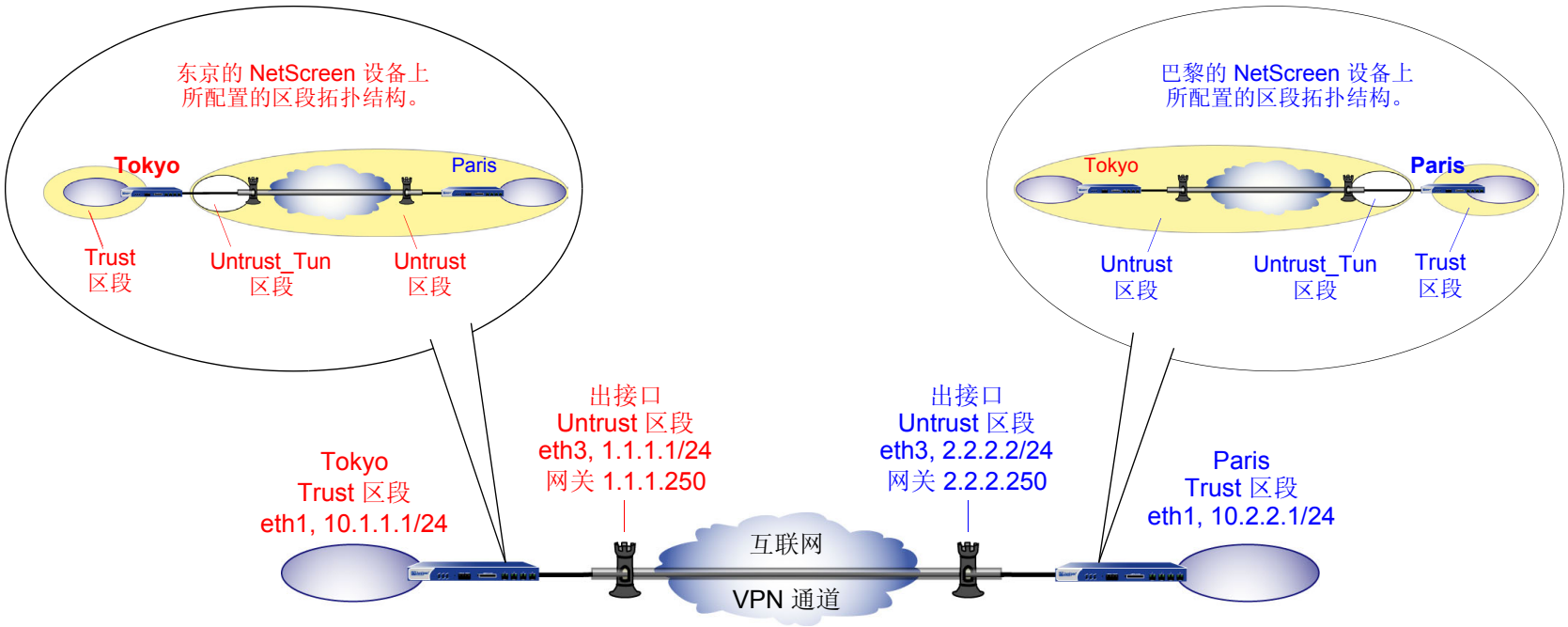
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.1.1.0/24 interface null metric 10
```

5. 策略

```
set policy top name “To Tokyo” from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name “From Tokyo” from untrust to trust Tokyo_Office Trust_LAN
    any permit
save
```

范例：基于策略的站点到站点 VPN，自动密钥 IKE

在本例中，“自动密钥 IKE”通道使用预共享密钥或一对证书 (通道两端各一个) 来提供东京 (Tokyo) 分公司与巴黎 (Paris) 分公司之间的安全连接。对于 “阶段 1”和 “阶段 2”安全级别，指定一个 “阶段 1”提议 : 为预共享密钥方法指定 pre-g2-3des-sha 或为证书指定 rsa-g2-3des-sha，并为 “阶段 2”选择预定义的 “Compatible”提议集。所有区段都在 trust-vr 中。



用带有预共享密钥或证书的 “自动密钥 IKE”设置 “自动密钥 IKE”通道，具体步骤如下 :

1. 定义安全区段接口 IP 地址。
2. 为本地及远程端实体生成通讯簿条目。
3. 定义远程网关和密钥交换模式，并指定预共享密钥或证书。

4. 创建 “自动密钥 IKE” VPN。
5. 设置到外部路由器的缺省路由。
6. 配置策略。

在下面的例子中，预共享密钥为 h1p8A24nG5。假定两个参与者都已有 RSA 证书，并将 Entrust 用作证书授权机构 (CA)。(有关获取和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。)

WebUI (东京)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP / Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

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

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Main (ID Protection)

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

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

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway: Predefined: (选择), To_Paris

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

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

Name: To/From Paris

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Paris_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Tokyo_Paris

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

WebUI (巴黎)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP / Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Tokyo
Security Level: Custom
Remote Gateway Type:
Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

预共享密钥

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本“网关”配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Main (ID Protection)
Preferred certificate (optional)
Peer CA: Entrust
Peer Type: X509-SIG

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

VPN Name: Paris_Tokyo

Security Level: Compatible

Remote Gateway: Predefined: (选择), To_Tokyo

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

5. 策略

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

Name: To/From Tokyo

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Tokyo_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Paris_Tokyo

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

CLI (东京)

1. 接口

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

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

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

预共享密钥

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
```

(或)

证书

```
set ike gateway to_paris address 2.2.2.2 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1[4]
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
```

4. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。

4. 路由

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

5. 策略

```
set policy top name "To/From Paris" from trust to untrust Trust_LAN
    paris_office any tunnel vpn tokyo_paris
set policy top name "To/From Paris" from untrust to trust paris_office
    Trust_LAN any tunnel vpn tokyo_paris
save
```

CLI (巴黎)

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
```

2. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

3. VPN

预共享密钥

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
```

(或)

证书

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo tunnel proposal nopfs-esp-3des-sha
```

4. 路由

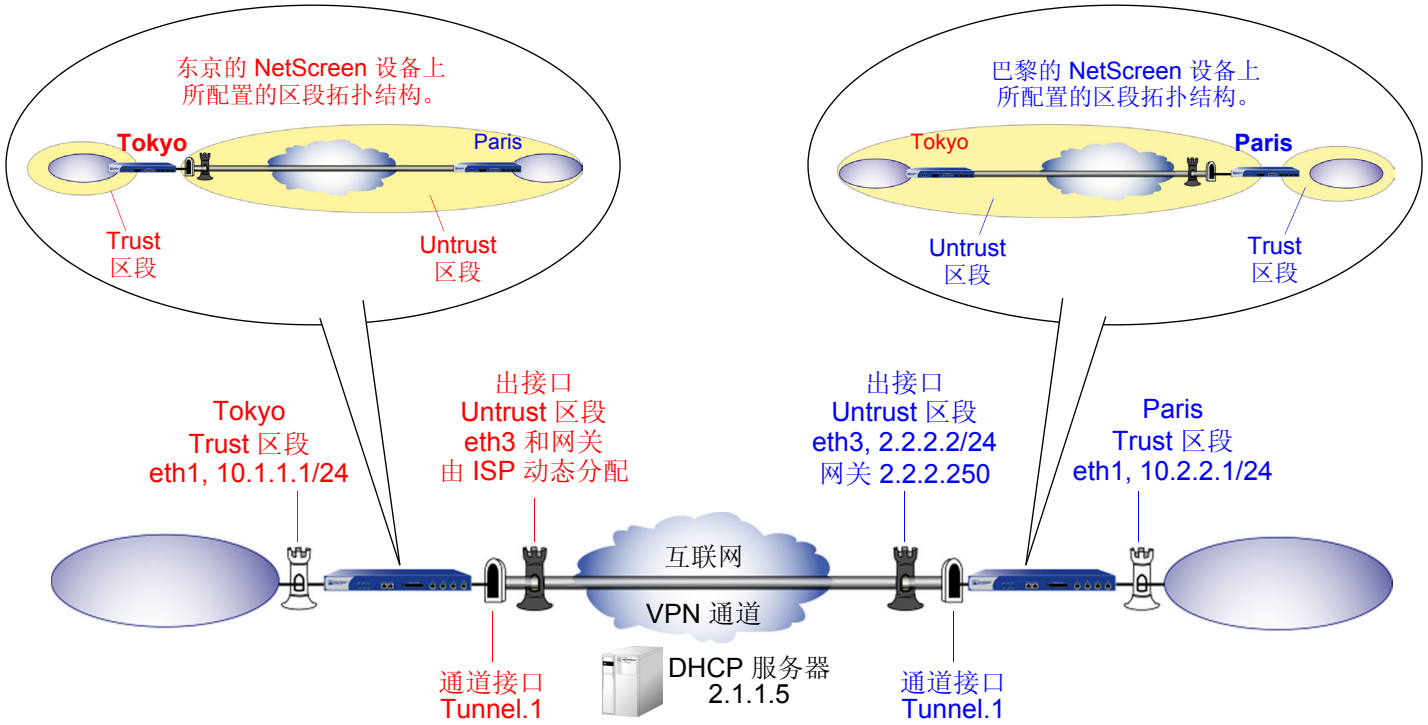
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
```

5. 策略

```
set policy top name “To/From Tokyo” from trust to untrust Trust_LAN
    tokyo_office any tunnel vpn paris_tokyo
set policy top name “To/From Tokyo” from untrust to trust tokyo_office
    Trust_LAN any tunnel vpn paris_tokyo
save
```

范例：基于路由的站点到站点 VPN，动态对等方

在本例中，“自动密钥 IKE” VPN 通道使用预共享密钥或一对证书 (通道两端各一个) 来提供可保护东京 (Tokyo) 分公司和巴黎 (Paris) 分公司的 NetScreen 设备之间的安全连接。巴黎分公司的 NetScreen 设备的 Untrust 区段接口具有静态 IP 地址。为东京分公司提供服务的 ISP 通过 DHCP 为 Untrust 区段接口动态分配 IP 地址。由于只有巴黎的 NetScreen 设备的 Untrust 区段具有固定地址，因此 VPN 信息流必须来自东京分公司的主机。建立通道后，通过该通道的信息流可以来自任意一端。所有安全区段和 Tunnel 区段都在 trust-vr 中。



预共享密钥为 h1p8A24nG5。假设两个参与者都已从证书授权机构 (CA) Verisign 获得了 RSA 证书，而且电子邮件地址 *pmason@abc.com* 出现在 NetScreen-A 上的本地证书中。(有关获取并加载证书的信息，请参阅第 29 页上的“证书和 CRL”。) 对于 “阶段 1” 和 “阶段 2” 安全级别，指定 “阶段 1” 提议 (对于预共享密钥方法，应为 pre-g2-3des-sha ；对于证书，应为 rsa-g2-3des-sha) 并为 “阶段 2” 选择 “Compatible” 提议集。

在 VPN 通道两端的 NetScreen 设备上输入三个路由 :

- 通向 trust-vr 中外部路由器的缺省路由
- 通过通道接口通向目标的路由
- 通向目标的 Null 路由。为 Null 路由分配较高的度量 (远离零)，以便其成为通向目标的下一个可选路由。那么，如果通道接口的状态变为 “中断”，且引用该接口的路由变为非活动，则 NetScreen 设备会使用 Null 路由 (即实质上丢弃了发送给它的任何信息流的路由)，而不使用缺省路由 (即转发未加密的信息流的路由)。

最后，配置允许两站点间双向信息流的策略。

WebUI (东京)

1. 接口

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

Zone Name: Trust
Static IP: (出现时选择此选项)
IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:
Interface Mode: NAT

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

Zone Name: Untrust

输入以下内容，然后单击 **OK**:
Obtain IP using DHCP: (选择)[5]

5. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址，但可通过 CLI 对其进行指定。

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

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

预共享密钥

Preshared Key: h1p8A24nG5
Local ID: pmason@abc.com
Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(或)

证书

Local ID: pmason@abc.com[6]
Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

6. U-FQDN “pmason@abc.com” 必须出现在证书的 SubjectAltName 字段中。

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

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Paris

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

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

Proxy-ID: (选择)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.2.0/24

Service: ANY

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[7]

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

7. ISP 通过 DHCP 动态提供网关 IP 地址。

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: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Paris_Office

Service: Any

Action: Permit

Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), Paris_Office

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: Any

Action: Permit

Position at Top: (选择)

WebUI (巴黎)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (选择), Peer ID: pmason@abc.com

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: Paris_Tokyo

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Tokyo

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

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

Proxy-ID: (选择)

Local IP / Netmask: 10.2.2.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: (选择), 2.2.2.250

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

Network Address/Netmask: 10.1.1.0/24

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: 10.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Tokyo_Office

Service: Any

Action: Permit

Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), Tokyo_Office

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: Any

Action: Permit

Position at Top: (选择)

CLI (东京)

1. 接口

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

set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

预共享密钥

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Tokyo_Paris gateway To_Paris tunnel sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(或)

证书

```
set ike gateway To_Paris address 2.2.2.2 aggressive local-id pmason@abc.com[8]
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Paris cert peer-ca 1[9]
set ike gateway To_Paris cert peer-cert-type x509-sig
set vpn Tokyo_Paris gateway To_Paris tunnel sec-level compatible
set vpn Tokyo_Paris bind interface tunnel.1
set vpn Tokyo_Paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[10]
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. 策略

```
set policy top from trust to untrust Trust_LAN Paris_Office any permit
set policy top from untrust to trust Paris_Office Trust_LAN any permit
save
```

8. U-FQDN “pmason@abc.com” 必须出现在证书的 SubjectAltName 字段中。
9. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。
10. ISP 通过 DHCP 动态提供网关 IP 地址，因而不能在此处指定。

CLI (巴黎)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

预共享密钥

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn Paris_Tokyo gateway To_Tokyo tunnel sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(或)

证书

```
set ike gateway To_Tokyo dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway To_Tokyo cert peer-ca 1[11]
set ike gateway To_Tokyo cert peer-cert-type x509-sig
set vpn Paris_Tokyo gateway To_Tokyo tunnel sec-level compatible
set vpn Paris_Tokyo bind interface tunnel.1
set vpn Paris_Tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
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 10
```

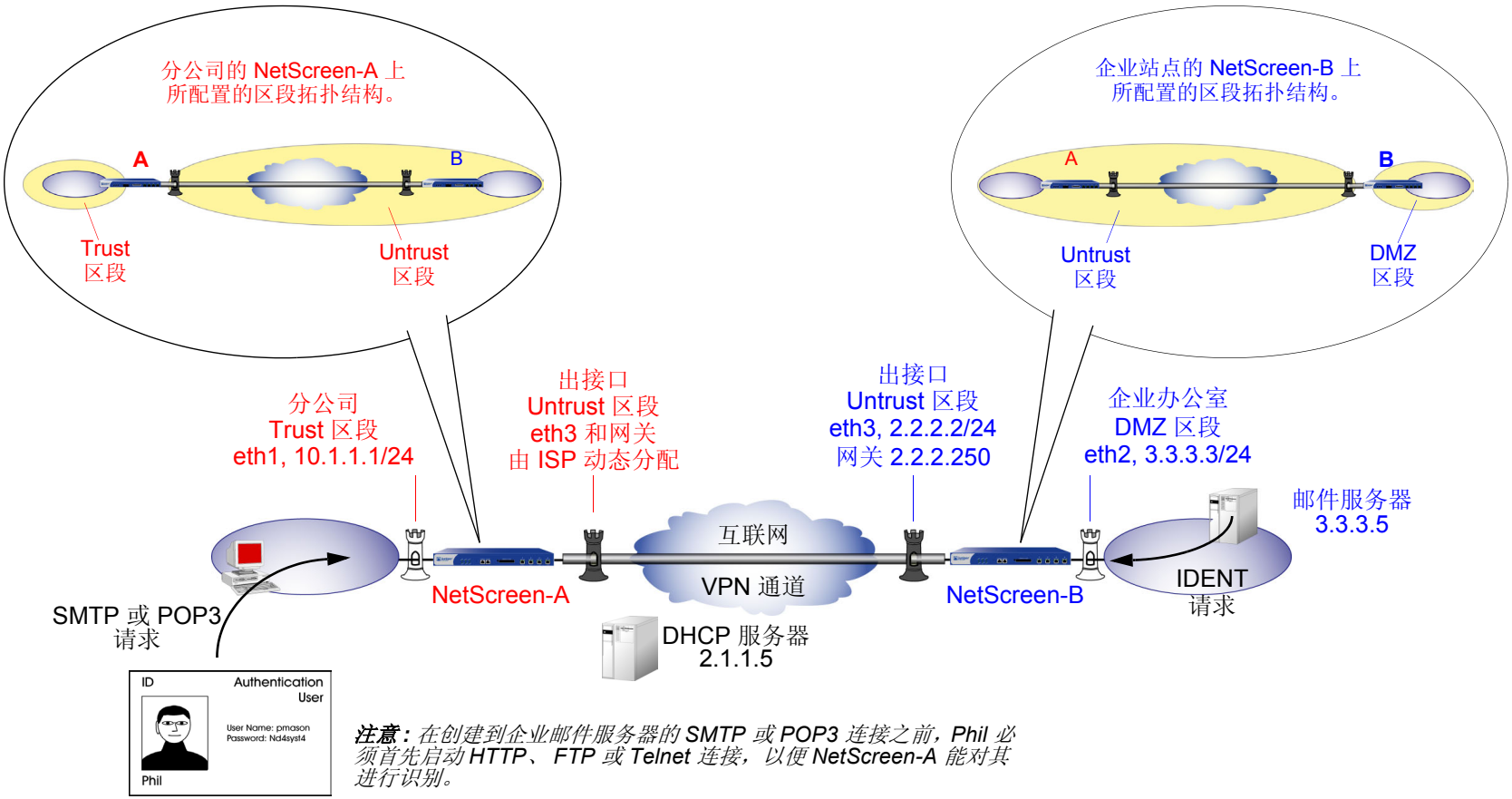
5. 策略

```
set policy top from trust to untrust Trust_LAN Tokyo_Office any permit
set policy top from untrust to trust Tokyo_Office Trust_LAN any permit
save
```

11. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。

范例：基于策略的站点到站点 VPN，动态对等方

在本例中， VPN 通道将 NetScreen-A 后面的 Trust 区段中的用户安全连接到邮件服务器，该服务器在企业 DMZ 区段，并被 NetScreen-B 保护。 NetScreen-B 的 Untrust 区段接口有一个静态 IP 地址。为 NetScreen-A 提供服务的 ISP，通过 DHCP 为其 Untrust 区段接口动态分配 IP 地址。因为只有 NetScreen-B 的 Untrust 区段具有固定地址，因此 VPN 信息流必须来自 NetScreen-A 后面的主机。 NetScreen-A 建立了通道之后，通过该通道的信息流可以来自任意一端。所有区段都在 trust-vr 路由选择域中。



***注意：**在创建到企业邮件服务器的 SMTP 或 POP3 连接之前，Phil 必须首先启动 HTTP、FTP 或 Telnet 连接，以便 NetScreen-A 能对其进行识别。*

在本例中，本地 auth 用户 Phil (登录名 : pmason ； 密码 : Nd4syst4) 要从企业站点上的邮件服务器获取他的电子邮件。当他试图执行此操作时，他将接受两次验证 : 第一次，在允许由他发出的信息流通过通道之前， NetScreen-A 在本地对其进行验证[12] ；第二次，邮件服务器程序通过发送经由通道的 IDENT 请求对他进行验证。

注意： *只有在 NetScreen-A 和 NetScreen-B 的管理员为其添加了定制服务 (TCP，端口 113)，并且设置了允许信息流通过通道到达 10.10.10.0/24 子网的策略时，邮件服务器才能通过该通道发送 IDENT 请求。*

预共享密钥为 h1p8A24nG5。假设两个参与者都已从证书授权机构 (CA) Verisign 获得了 RSA 证书，而且电子邮件地址 *pmason@abc.com* 出现在 NetScreen-A 上的本地证书中。(有关获取并加载证书的信息，请参阅第 29 页上的“证书和 CRL”。) 对于 “阶段 1”和 “阶段 2”安全级别，指定 “阶段 1”提议 (对于预共享密钥方法，应为 pre-g2-3des-sha ；对于证书，应为 rsa-g2-3des-sha) 并为 “阶段 2”选择预定义的 “Compatible”提议集。

WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Obtain IP using DHCP: (选择)[13]

12. 由于 Phil 是一个认证用户，因此，在他能提出 SMTP 或 POP3 请求之前，必须首先启动 HTTP、FTP 或 Telnet 连接，这样， NetScreen-A 就能用一个防火墙用户 / 注册提示来进行响应以对其进行认证。 NetScreen-A 对他进行认证后，就允许他通过 VPN 通道与企业邮件服务器进行通信。

13. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址，但可通过 CLI 对其进行指定。

2. 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: pmason

Status: Enable

Authentication User: (选择)

User Password: Nd4syst4

Confirm Password: Nd4syst4

3. 地址

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

Address Name: Trusted_network

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: Mail_Server

IP Address/Domain Name:

IP / Netmask: (选择), 3.3.3.5/32

Zone: Untrust

4. 服务

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (选择)

Transport Protocol: TCP (选择)

Source Port: Low 0, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: 输入以下内容，移动以下服务，然后单击 **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

HTTP
FTP
Telnet
Ident
MAIL
POP3

5. VPN

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

Gateway Name: To_Mail

Security Level: Custom

Remote Gateway Type:

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

预共享密钥

Preshared Key: h1p8A24nG5

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(或)

证书

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

Name: branch_corp

Security Level: Compatible

Remote Gateway Tunnel: To_Mail

6. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[14]

7. 策略

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

Source Address:

Address Book Entry: (选择), Trusted network

Destination Address:

Address Book Entry: (选择), Mail Server

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: branch_corp

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

14. ISP 通过 DHCP 动态提供网关 IP 地址。

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

Authentication: (选择)

Auth Server: Local

User: (选择), Local Auth User - pmason

WebUI (NetScreen-B)

1. 接口

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

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

2. 地址

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

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (选择), 3.3.3.5/32

Zone: DMZ

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

Address Name: branch office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. 服务

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (选择)

Transport Protocol: TCP (选择)

Source Port: Low 0, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: 输入以下内容，移动以下服务，然后单击 **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident

MAIL

POP3

4. VPN

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

Gateway Name: To_branch
Security Level: Custom
Remote Gateway Type:
Dynamic IP Address: (选择), Peer ID: pmason@abc.com

预共享密钥

Preshared Key: h1p8A24nG5
Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha
Mode (Initiator): Aggressive

(或)

证书

Outgoing Interface: ethernet3
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Gateway 配置页 :
Security Level: Custom
Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha
Mode (Initiator): Aggressive
Preferred Certificate (optional):
Peer CA: Verisign
Peer Type: X509-SIG

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

VPN Name: corp_branch

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_branch

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: ethernet3

Gateway IP Address: 2.2.2.250

6. 策略

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

Source Address:

Address Book Entry: (选择), Mail Server

Destination Address:

Address Book Entry: (选择), branch office

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: corp_branch

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

CLI (NetScreen-A)

1. 接口

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

set interface ethernet3 zone untrust
set interface ethernet3 dhcp client
set interface ethernet3 dhcp client settings server 1.1.1.5
```

2. 用户

```
set user pmason password Nd4syst4
```

3. 地址

```
set address trust "trusted network" 10.1.1.0/24
set address untrust "mail server" 3.3.3.5/32
```

4. 服务

```
set service ident protocol tcp src-port 0-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add http
set group service remote_mail add ftp
set group service remote_mail add telnet
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

5. VPN

预共享密钥

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com
    outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn branch_corp gateway to_mail sec-level compatible
```

(或)

证书

```
set ike gateway to_mail address 2.2.2.2 aggressive local-id pmason@abc.com[15]
    outgoing-interface ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_mail cert peer-ca 1[16]
set ike gateway to_mail cert peer-cert-type x509-sig
set vpn branch_corp gateway to_mail sec-level compatible
```

6. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[17]
```

7. 策略

```
set policy top from trust to untrust "trusted network" "mail server"
    remote_mail tunnel vpn branch_corp auth server Local user pmason
set policy top from untrust to trust "mail server" "trusted network"
    remote_mail tunnel vpn branch_corp
save
```

15. U-FQDN "pmason@abc.com" 必须出现在证书的 SubjectAltName 字段中。
16. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。
17. ISP 通过 DHCP 动态提供网关 IP 地址。

CLI (NetScreen-B)

1. 接口

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 3.3.3.3/24

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

2. 地址

```
set address dmz "mail server" 3.3.3.5/32
set address untrust "branch office" 10.1.1.0/24
```

3. 服务

```
set service ident protocol tcp src-port 0-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

预共享密钥

```
set ike gateway to_branch dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_branch gateway to_branch tunnel sec-level compatible
```

(或)

证书

```
set ike gateway to_branch dynamic pmason@abc.com aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_branch cert peer-ca 1[18]
set ike gateway to_branch cert peer-cert-type x509-sig
set vpn corp_branch gateway to_branch sec-level compatible
```

5. 路由

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

6. 策略

```
set policy top from dmz to untrust "mail server" "branch office" remote_mail
    tunnel vpn corp_branch
set policy top from untrust to dmz "branch office" "mail server" remote_mail
    tunnel vpn corp_branch
save
```

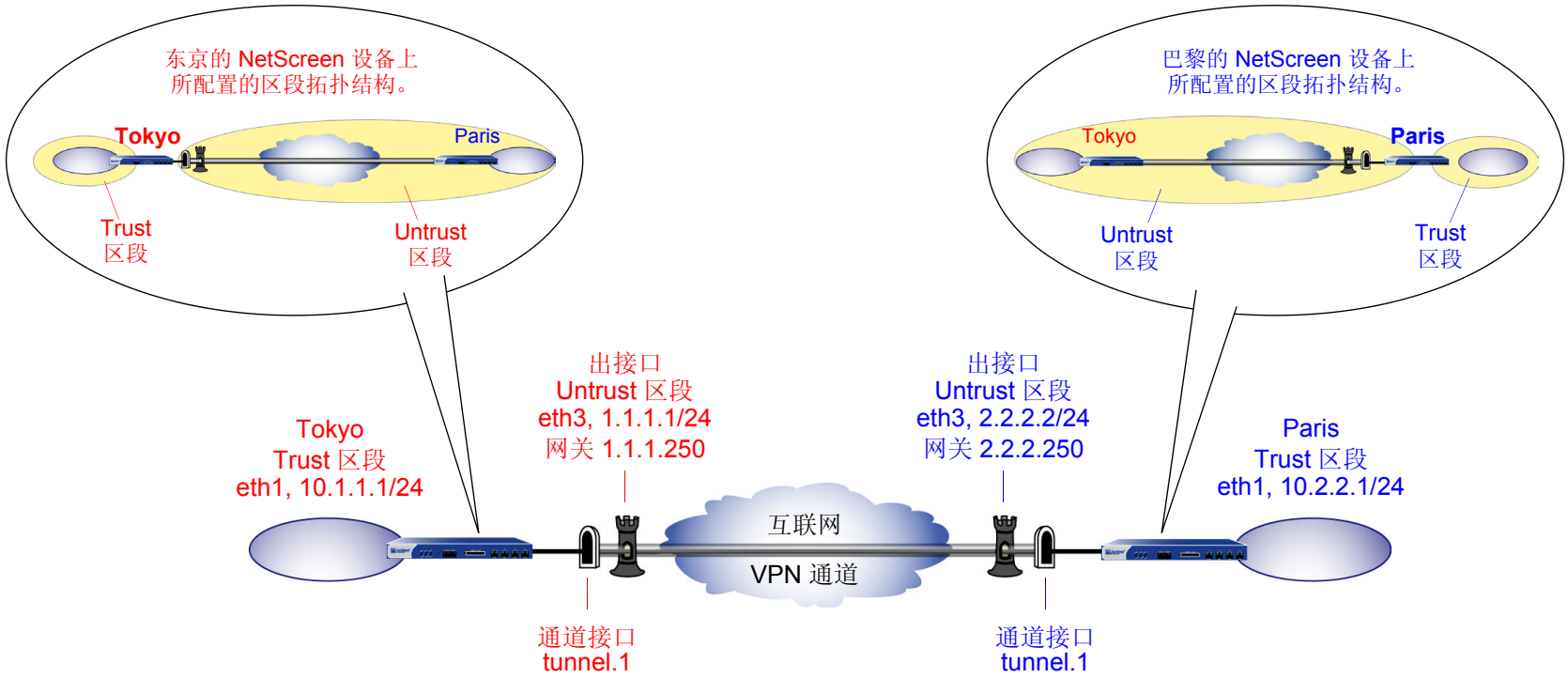
18. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。

范例：基于路由的站点到站点 VPN，手动密钥

在本例中，“手动密钥”通道在东京 (Tokyo) 分公司与巴黎 (Paris) 分公司之间提供了一个安全信道。每个站点的 Trust 区段都处于 NAT 模式。地址如下：

- 东京：
  - Trust 区段接口 (ethernet1): 10.1.1.1/24
  - Untrust 区段接口 (ethernet3): 1.1.1.1/24
- 巴黎：
  - Trust 区段接口 (ethernet1): 10.2.2.1/24
  - Untrust 区段接口 (ethernet3): 2.2.2.2/24

Trust 和 Untrust 安全区段都在 trust-vr 路由选择域中。 Untrust 区段接口 (ethernet3) 作为 VPN 通道的出接口。



要设置通道，请在通道两端的 NetScreen 设备上执行以下步骤 :

1. 为绑定到安全区段和通道接口的物理接口分配 IP 地址。
2. 配置 VPN 通道，在 Untrust 区段内指定其出接口，并将其绑定到通道接口。
3. 在 Trust 和 Untrust 区段的通讯簿中输入本地及远程端点的 IP 地址。
4. 输入通向 trust-vr 中外部路由器的缺省路由、通过通道接口通向目标的路由以及通向目标的 Null 路由。为 Null 路由分配较高的度量 (远离零)，以便其成为通向目标的下一个可选路由。那么，如果通道接口的状态变为 “中断”，且引用该接口的路由变为非活动，则 NetScreen 设备会使用 Null 路由 (即实质上丢弃了发送给它的任何信息流的路由)，而不使用缺省路由 (即转发未加密的信息流的路由)。
5. 为各个站点间通过的 VPN 信息流设置策略。

WebUI (东京)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

VPN Tunnel Name: Tokyo_Paris

Gateway IP: 2.2.2.2

Security Index: 3020 (Local), 3030 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (选择)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Manual Key 通道配置页：

Bind to: Tunnel Interface, tunnel.1

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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: 10.2.2.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Name: To Paris

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Paris_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From Paris

Source Address:

Address Book Entry: (选择), Paris_Office

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

WebUI (巴黎)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

VPN Tunnel Name: Paris_Tokyo

Gateway IP: 1.1.1.1

Security Index: 3030 (Local), 3020 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (选择)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Manual Key 通道配置页：

Bind to: Tunnel Interface, tunnel.1

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address/Netmask: 10.1.1.0/24

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: 10.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Name: To Tokyo

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From Tokyo

Source Address:

Address Book Entry: (选择), Tokyo_Office

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

CLI (东京)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Paris_Office 10.2.2.0/24
```

3. VPN

```
set vpn Tokyo_Paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Tokyo_Paris bind interface tunnel.1
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. 策略

```
set policy top name "To Paris" from trust to untrust Trust_LAN Paris_Office any
    permit
set policy top name "From Paris" from untrust to trust Paris_Office Trust_LAN
    any permit
save
```

CLI (巴黎)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust Tokyo_Office 10.1.1.0/24
```

3. VPN

```
set vpn Paris_Tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn Paris_Tokyo bind interface tunnel.1
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
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 10
```

5. 策略

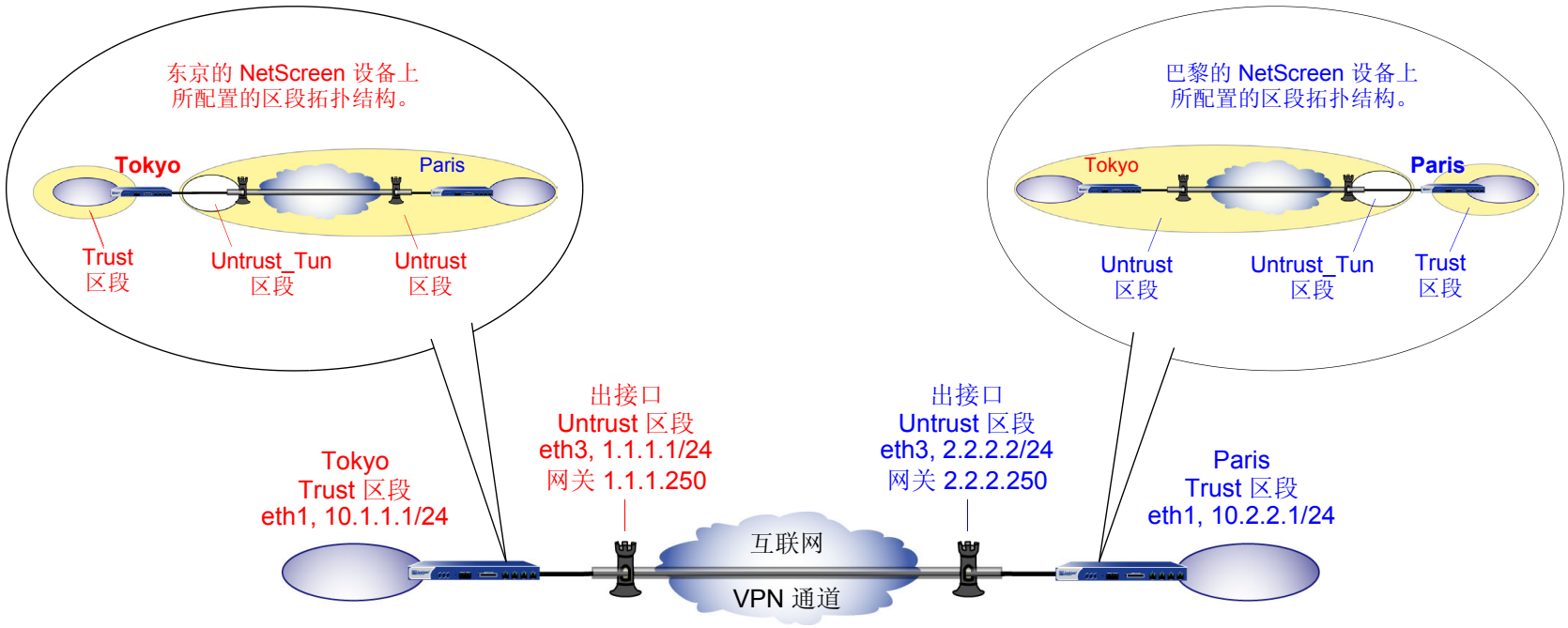
```
set policy top name “To Tokyo” from trust to untrust Trust_LAN Tokyo_Office any
    permit
set policy top name “From Tokyo” from untrust to trust Tokyo_Office Trust_LAN
    any permit
save
```

范例：基于策略的站点到站点 VPN，手动密钥

在本例中，通过使用具有 3DES 加密和 SHA-1 认证的 ESP，“手动密钥”通道在东京 (Tokyo) 分公司和巴黎 (Paris) 分公司之间提供了一个安全信道。每个站点的 Trust 区段都处于 NAT 模式。地址如下：

- 东京：
  - Trust 接口 (ethernet1): 10.1.1.1/24
  - Untrust 接口 (ethernet3): 1.1.1.1/24
- 巴黎：
  - Trust 接口 (ethernet1): 10.2.2.1/24
  - Untrust 接口 (ethernet3): 2.2.2.2/24

Trust 安全区段、 Untrust 安全区段以及 Untrust_Tun 通道区段都在 trust-vr 路由选择域中。 Untrust 区段接口 (ethernet3) 作为 VPN 通道的出接口。



要设置通道，需在通道两端的 NetScreen 设备上执行以下五个步骤：

1. 将 IP 地址分配给绑定到安全区段的物理接口。
2. 配置 VPN 通道，并在 Untrust 区段中指定其出接口。
3. 在 Trust 和 Untrust 通讯簿中输入本地及远程端点的 IP 地址。
4. 输入到外部路由器的缺省路由。
5. 为 VPN 信息流设置策略，使其可通过该通道双向流动。

WebUI (东京)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP / Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

VPN Tunnel Name: Tokyo_Paris

Gateway IP: 2.2.2.2

Security Index: 3020 (Local), 3030 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (选择)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Manual Key 通道配置页：

Bind to: Tunnel Zone, Untrust-Tun

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

5. 策略

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

Name: To/From Paris

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Paris_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Tokyo_Paris

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

WebUI (巴黎)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

VPN Tunnel Name: Paris_Tokyo

Gateway IP: 1.1.1.1

Security Index (HEX Number): 3030 (Local), 3020 (Remote)

Outgoing Interface: ethernet3

ESP-CBC: (选择)

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Manual Key 通道配置页：

Bind to: Tunnel Zone, Untrust-Tun

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

5. 策略

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

Name: To/From Tokyo

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Tokyo_Office

Service: ANY

Action: Tunnel

Tunnel VPN: Paris_Tokyo

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

CLI (东京)

1. 接口

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

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

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

```
set vpn tokyo_paris manual 3020 3030 gateway 2.2.2.2 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn tokyo_paris bind zone untrust-tun
```

4. 路由

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

5. 策略

```
set policy top name "To/From Paris" from trust to untrust Trust_LAN
    paris_office any tunnel vpn tokyo_paris
set policy top name "To/From Paris" from untrust to trust paris_office
    Trust_LAN any tunnel vpn tokyo_paris
save
```

CLI (巴黎)

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
```

2. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

3. VPN

```
set vpn paris_tokyo manual 3030 3020 gateway 1.1.1.1 outgoing-interface
    ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
set vpn paris_tokyo bind zone untrust-tun
```

4. 路由

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

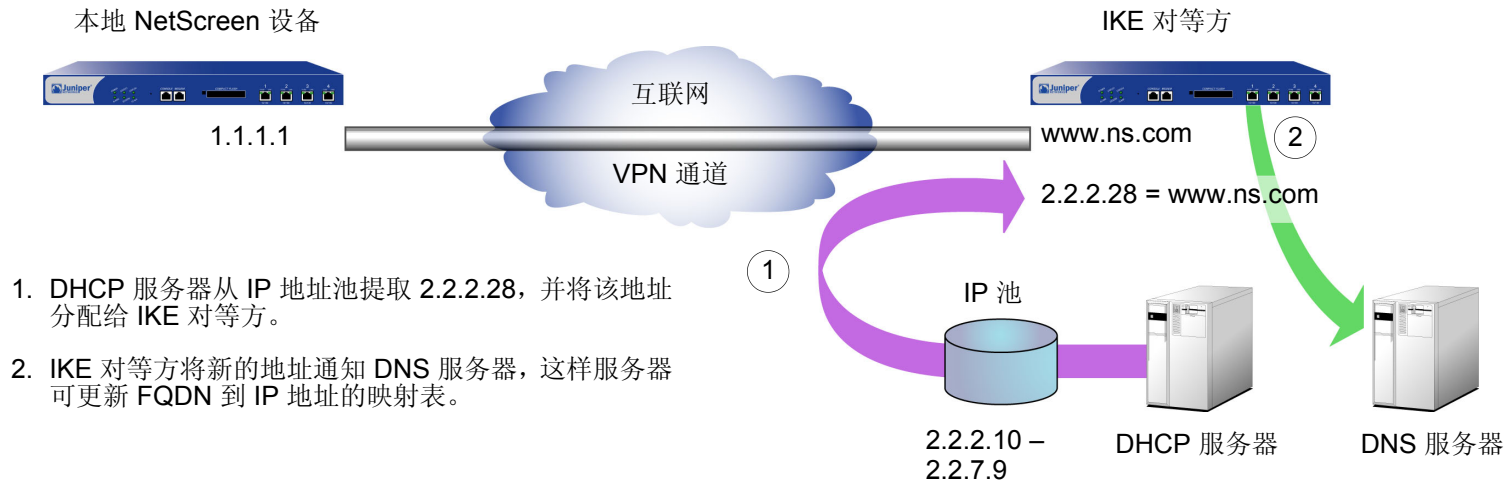
5. 策略

```
set policy top name "To/From Tokyo" from trust to untrust Trust_LAN
    tokyo_office any tunnel vpn paris_tokyo
set policy top name "To/From Tokyo" from untrust to trust tokyo_office
    Trust_LAN any tunnel vpn paris_tokyo
save
```

使用 FQDN 的动态 IKE 网关

对于动态获取 IP 地址的 IKE 对等方，可在远程网关的本地配置中指定完全合格的域名 (FQDN)。例如，互联网服务提供商 (ISP) 有可能通过 DHCP 将 IP 地址分配给客户。 ISP 从大型地址池提取地址，并在客户联机时分配这些地址。尽管 IKE 对等方拥有不变的 FQDN，但其 IP 地址的更改无法预测。IKE 对等方可使用三种方法维护从 FQDN 到动态分配的 IP 地址的 “域名服务” (DNS) 映射 (此过程称为动态 DNS)。

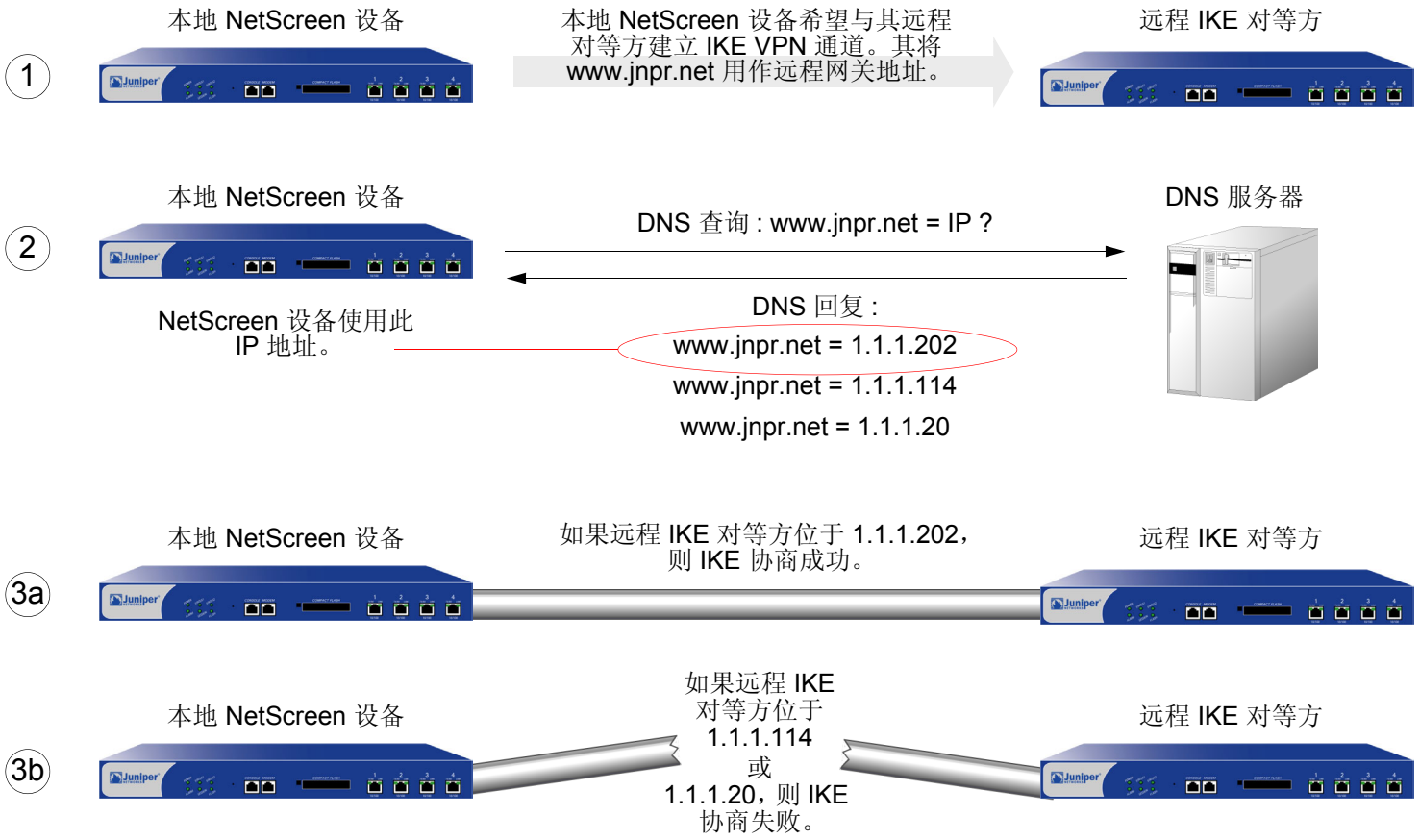
- 如果远程 IKE 对等方是 NetScreen 设备，则 NetScreen 设备每次从 ISP 收到新的 IP 地址时， admin 都可手动通知 DNS 服务器更新其从 FQDN 到 IP 地址的映射。
- 如果远程 IKE 对等方是另一种 VPN 终端设备，其上运行有动态 DNS 软件，则该软件可自动将其地址更改通知 DNS 服务器，这样服务器可更新 FQDN 到 IP 地址的映射表。
- 如果远程 IKE 对等方是 NetScreen 设备或其它任何种类的 VPN 终端设备，则其后面的主机可运行 FQDN 到 IP 地址自动更新程序，提醒 DNS 服务器 : 地址已更改。



现在无需知道远程 IKE 对等方的当前 IP 地址即可使用其 FQDN (而不是 IP 地址) 为该对等方配置 “自动密钥 IKE” VPN 通道。

别名

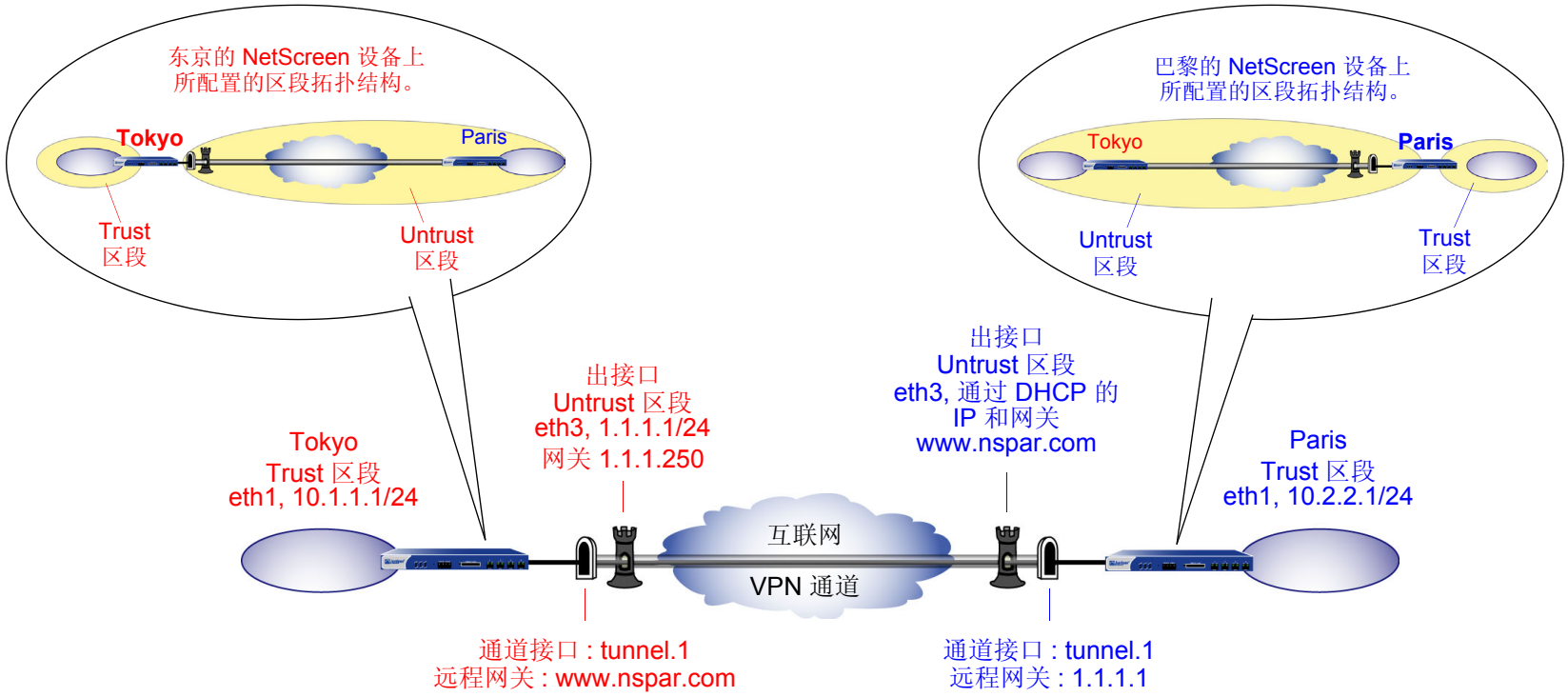
如果本地 NetScreen 设备查询的 DNS 服务器只返回一个 IP 地址，则还可使用远程 IKE 对等方的 FQDN 的别名。如果 DNS 服务器返回多个 IP 地址，则本地设备使用接收到的第一个地址。由于对 DNS 服务器的响应中地址的顺序没有保证，因此本地 NetScreen 设备可能使用错误的 IP 地址，并且 IKE 协商可能会失败。



范例：具有 FQDN 的自动密钥 IKE 对等方

在本例中，“自动密钥 IKE” VPN 通道使用预共享密钥或一对证书 (通道两端各一个) 来提供东京 (Tokyo) 分公司与巴黎 (Paris) 分公司之间的安全连接。巴黎分公司拥有动态分配的 IP 地址，因此东京分公司将远程对等方的 FQDN (www.nspar.com) 用作其 VPN 通道配置中远程网关的地址。

以下配置针对基于路由的 VPN 通道。对于 “阶段 1” 和 “阶段 2” 安全级别，指定 “阶段 1” 提议 (对于预共享密钥方法，应为 pre-g2-3des-sha ；对于证书，应为 rsa-g2-3des-sha) 并为 “阶段 2” 选择预定义的 “Compatible” 提议集。所有区段都位于 trust-vr 中。



使用预共享密钥或证书来设置基于路由的 “自动密钥 IKE” 通道，具体步骤如下 :

1. 为绑定到安全区段和通道接口的物理接口分配 IP 地址。
2. 定义远程网关和密钥交换模式，并指定预共享密钥或证书。
3. 配置 VPN 通道，在 Untrust 区段内指定其出接口，将其绑定到通道接口，并配置其代理 ID。
4. 在 Trust 和 Untrust 通讯簿中输入本地及远程端点的 IP 地址。
5. 输入通向 trust-vr 中外部路由器的缺省路由、通过通道接口通向目标的路由以及通向目标的 Null 路由。为 Null 路由分配较高的度量 (远离零)，以便其成为通向目标的下一个可选路由。那么，如果通道接口的状态变为 “中断”，且引用该接口的路由变为非活动，则 NetScreen 设备会使用 Null 路由 (即实质上丢弃了发送给它的任何信息流的路由)，而不使用缺省路由 (即转发未加密的信息流的路由)。
6. 为各个站点间通过的信息流设置策略。

在下面的例子中，预共享密钥为 h1p8A24nG5。假定两个参与者都已有 RSA 证书，并将 Entrust 用作证书授权机构 (CA)。(有关获取和加载证书的信息，请参阅 *NetScreen 概念与范例 ScreenOS 参考指南，第 4 卷， VPN*。)

WebUI (东京)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Trust_LAN

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: Paris_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

3. VPN

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

Gateway Name: To_Paris

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: www.nspar.com

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

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

VPN Name: Tokyo_Paris

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Paris

> 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

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

4. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 0.0.0.0[19]

19. ISP 通过 DHCP 动态提供网关 IP 地址。

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: 10.2.2.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Name: To_Paris

Source Address: Trust_LAN

Destination Address: Paris_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From_Paris

Source Address: Paris_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

WebUI (巴黎)

1. 主机名和域名

Network > DNS: 输入以下内容，然后单击 **Apply**:

Host Name: www

Domain Name: nspar.com

2. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Obtain IP using DHCP: (选择)

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

3. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Trust

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

Address Name: Tokyo_Office

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

4. VPN

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

Gateway Name: To_Tokyo

Security Level: Custom

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Main (ID Protection)

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Preferred certificate (optional)

Peer CA: Entrust

Peer Type: X509-SIG

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

Name: Paris_Tokyo

Security Level: Custom

Remote Gateway:

Predefined: (选择), To_Tokyo

> 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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP/Netmask: 10.2.2.0/24

Remote IP/Netmask: 10.1.1.0/24

Service: ANY

5. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address/Netmask: 10.1.1.0/24

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: 10.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

6. 策略

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

Name: To Tokyo

Source Address: Trust_LAN

Destination Address: Tokyo_Office

Service: ANY

Action: Permit

Position at Top: (选择)

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

Name: From Tokyo

Source Address: Tokyo_Office

Destination Address: Trust_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

CLI (东京)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust paris_office 10.2.2.0/24
```

3. VPN

预共享密钥

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

(或)

证书

```
set ike gateway to_paris address www.nspar.com main outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_paris cert peer-ca 1[20]
set ike gateway to_paris cert peer-cert-type x509-sig
set vpn tokyo_paris gateway to_paris sec-level compatible
set vpn tokyo_paris bind interface tunnel.1
set vpn tokyo_paris proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.2.0/24 any
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.2.0/24 interface null metric 10
```

5. 策略

```
set policy top name “To Paris” from trust to untrust Trust_LAN paris_office any
    permit
set policy top name “From Paris” from untrust to trust paris_office Trust_LAN
    any permit
save
```

20. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get ike ca**。

CLI (巴黎)

1. 主机名和域名

```
set hostname www
set domain nspar.com
```

2. 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 dhcp-client enable

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. 地址

```
set address trust Trust_LAN 10.2.2.0/24
set address untrust tokyo_office 10.1.1.0/24
```

4. VPN

预共享密钥

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

(或)

证书

```
set ike gateway to_tokyo address 1.1.1.1 main outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway to_tokyo cert peer-ca 1
set ike gateway to_tokyo cert peer-cert-type x509-sig
set vpn paris_tokyo gateway to_tokyo sec-level compatible
set vpn paris_tokyo bind interface tunnel.1
set vpn paris_tokyo proxy-id local-ip 10.2.2.0/24 remote-ip 10.1.1.0/24 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
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 10
```

6. 策略

```
set policy top name “To Tokyo” from trust to untrust Trust_LAN tokyo_office any
    permit
set policy top name “From Tokyo” from untrust to trust tokyo_office Trust_LAN
    any permit
save
```

具有重叠地址的 VPN 站点

由于私有 IP 地址的范围相对较小，因此两个 VPN 对等方的受保护网络的地址很可能重叠[21]。对于具有重叠地址的两端实体间的双向 VPN 信息流，通道两端的 NetScreen 设备必须将源和目标网络地址转换 (NAT-src 和 NAT-dst) 应用于通过它们的 VPN 信息流。

对于 NAT-src，通道两端的接口在互为唯一的子网中必须具有 IP 地址，每个子网都具有动态 IP (DIP) 池[22]。然后，控制出站 VPN 信息流的策略可以应用使用 DIP 池地址的 NAT-src，将初始源地址转换为中性地址空间中的地址。

要对入站 VPN 信息流执行 NAT-dst，可使用以下两种方式 :

- 基于策略的 NAT-dst: 策略可应用 NAT-dst，将入站 VPN 信息流转换为一个地址，该地址可以位于通道接口所在的子网中 (但不在出站 VPN 信息流所使用的本地 DIP 池的范围内)，还可以是 NetScreen 设备的路由表中拥有的另一个子网中的地址。 (有关配置 NAT-dst 时需要注意的路由注意事项的信息，请参阅第 **7**-40 页上的 “NAT-Dst 的路由选择”。)
- 映射 IP (MIP): 策略可以将 MIP 引用为目标地址。 MIP 地址与通道接口地址位于同一个子网中，但不在出站 VPN 信息流所用的本地 DIP 池的范围内。 (有关 MIP 的信息，请参阅第 **7**-90 页上的 “映射 IP 地址”。)

具有重叠地址的站点间的 VPN 信息流在两个方向都要求进行地址转换。由于出站信息流的源地址与入站信息流的目标地址不能相同 (NAT-dst 地址或 MIP 不能在 DIP 池中)，因此入站和出站策略中引用的地址不能对称。

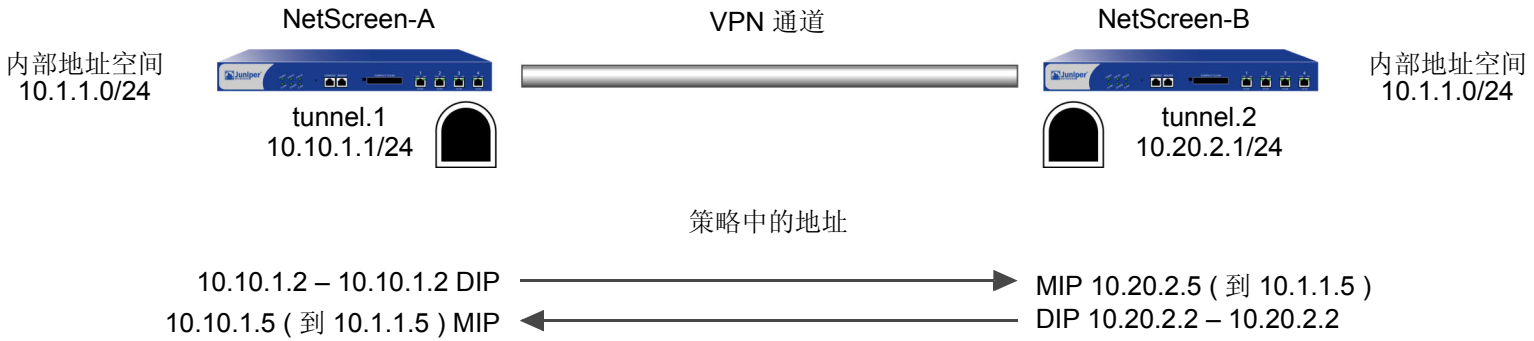
21. 重叠地址空间就是当两个网络中 IP 地址范围部分或全部相同时的空间。

22. DIP 池中的地址范围必须处于通道接口所在的子网内，但是该池中不允许包括可能也位于此子网中的接口 IP 地址、任何 MIP 或 VIP 地址。对于安全区段接口，还可以在接口 IP 地址所在子网之外的其它子网中定义一个扩展的 IP 地址和一个伴随的 DIP 池。有关详细信息，请参阅第 **2**-271 页上的 “扩展接口和 DIP”。

当希望 NetScreen 设备对通过同一通道的双向 VPN 信息流执行源和目标地址转换时，有以下两种选择：

- 可为基于策略的 VPN 配置定义代理 ID[23]。在策略中明确引用 VPN 通道时， NetScreen 设备从引用该通道的策略组件中导出代理 ID。首次创建策略以及此后每次重新启动设备时， NetScreen 设备都将导出代理 ID。不过，如果以手动方式为策略中引用的 VPN 通道定义了代理 ID，则 NetScreen 设备将应用用户定义的代理 ID，而不应用从该策略导出的代理 ID。
- 可使用基于路由的 VPN 通道配置，该配置必须具有用户定义的代理 ID。具有基于路由的 VPN 通道配置后，不能在策略中明确引用 VPN 通道。取而代之的是，策略将控制对特定目标的访问 (允许或拒绝)。到该目标的路由指向依次绑定到 VPN 通道的通道接口。由于 VPN 通道不直接与可从源地址、目标地址和服务导出代理 ID 的策略相关联，因此必须手动为其定义代理 ID。 (注意，基于路由的 VPN 配置还允许使用单个 VPN 通道 — 即单个 “阶段 2” SA — 来创建多个策略。)

在以下插图中，考虑具有重叠地址空间的两个站点间 VPN 通道的地址：



23. 代理 ID 是 IKE 对等方之间的一种协议，如果信息流与本地地址、远程地址和服务的一个指定元组匹配，则将允许信息流通过通道。

如果前面插图中的 NetScreen 设备从策略导出代理 ID (如在基于策略的 VPN 配置中的那样)，则入站和出站策略生成以下代理 ID:

NetScreen-A			
	本地	远程	服务
出站	10.10.1.2/32	10.20.2.5/32	Any
入站	10.10.1.5/32	10.20.2.2/32	Any

NetScreen-B			
	本地	远程	服务
入站	10.20.2.5/32	10.10.1.2/32	Any
出站	10.20.2.2/32	10.10.1.5/32	Any

正如表中所示，存在两个代理 ID: 一个是由出站 VPN 信息流导出的，而另一个则是由入站 VPN 信息流导出的。NetScreen-A 首次将信息流从 10.10.1.2/32 发送到 10.20.2.5/32 时，两个对等方执行 IKE 协商，并生成 “阶段 1” 和 “阶段 2” 安全联盟 (SA)。“阶段 2” SA 为 NetScreen-A 生成上面的出站代理 ID，为 NetScreen-B 生成入站代理 ID。

然后，当 NetScreen-B 将信息流发送到 NetScreen-A 时，从 10.20.2.2/32 到 10.10.1.5/32 的信息流的策略查找会指出没有可产生这种代理 ID 的活动 “阶段 2” SA。因此，两个对等方将使用现有的 “阶段 1” SA (假如其生存期还没有到期) 与不同的 “阶段 2” SA 进行协商。生成的代理 ID 在上面显示为 NetScreen-A 的入站代理 ID 及 NetScreen-B 的出站代理 ID。由于地址不对称并且需要不同的代理 ID，因此有两个 “阶段 2” SA (两个 VPN 通道)。

要为双向 VPN 信息流只创建一个通道，可以定义以下具有地址的代理 ID，该地址范围包括通道两端已转换的源地址和目标地址 :

NetScreen-A		
本地	远程	服务
10.10.1.0/24	10.20.2.0/24	Any
或		
0.0.0.0/0	0.0.0.0/0	Any

NetScreen-B		
本地	远程	服务
10.20.2.0/24	10.10.1.0/24	Any
或		
0.0.0.0/0	0.0.0.0/0	Any

上面的代理 ID 包括在两个站点间的入站和出站 VPN 信息流中出现的地址。地址 10.10.1.0/24 包括 DIP 池 10.10.1.2 – 10.10.1.2 及 MIP 10.10.1.5。同样，地址 10.20.2.0/24 包括 DIP 池 10.20.2.2 -10.20.2.2 及 MIP 10.20.2.5[24]。上面的代理 ID 是对称的，即 NetScreen-A 的本地地址是 NetScreen-B 的远程地址，反之亦然。如果 NetScreen-A 将信

24. 地址 0.0.0.0/0 包括所有 IP 地址，从而也包括 DIP 池及 MIP 的地址。

息流发送到 NetScreen-B，则 “阶段 2” SA 及代理 ID 还适用于从 NetScreen-B 发送到 NetScreen-A 的信息流。因此，两个站点间双向信息流仅需要单个 “阶段 2” SA (即单个 VPN 通道)。

当同一设备上所配置的 NAT-src 和 NAT-dst 的地址位于不同的子网中时，要为具有重叠地址空间的两个站点间的双向信息流创建一个 VPN 通道，该通道的代理 ID 必须是 (本地 IP) 0.0.0.0/0 – (远程 IP) 0.0.0.0/0 – *服务类型*。如果要在代理 ID 中使用更为严格的地址，则 NAT-src 和 NAT-dst 的地址必须在相同的子网中。

范例 : 具有 NAT-Src 和 NAT-Dst 的通道接口

在本例中，将在某个企业站点的 “NetScreen-A” 与某个分公司的 “NetScreen-B” 之间配置一个 VPN 通道。 VPN 端实体的地址空间重叠，它们都使用 10.1.1.0/24 子网中的地址。要解决此冲突，可使用 NAT-src 转换出站 VPN 信息流的源地址以及用 NAT-dst 转换入站 VPN 信息流的目标地址。策略允许企业 LAN 中的所有地址到达分公司站点的 FTP 服务器，并且允许分公司站点的所有地址到达企业站点的 FTP 服务器。

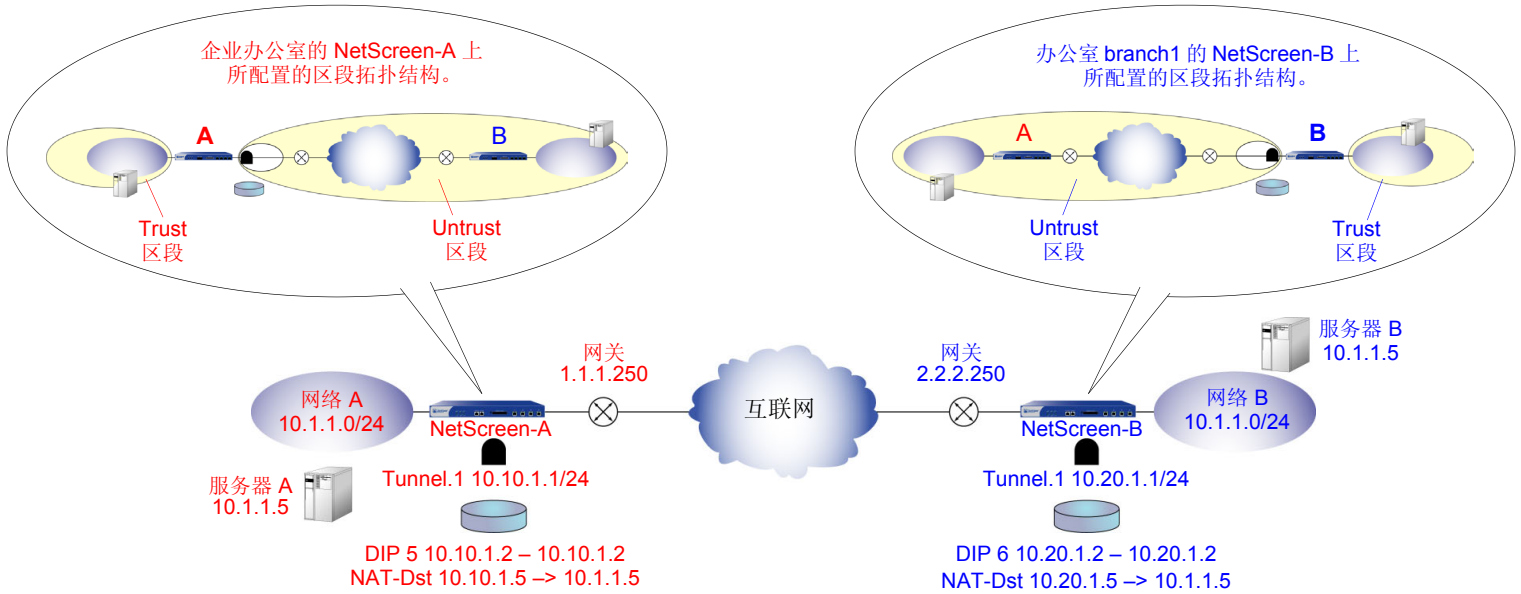
注意：*有关源和目标网络地址转换 (NAT-src 和 NAT-dst) 的详细信息，请参阅第 7 卷，“地址转换”。*

通道两端的通道配置使用以下参数 : 自动密钥 IKE、预共享密钥 (“netscreen1”) 以及为 “阶段 1” 和 “阶段 2” 提议预定义的安全级别 “Compatible”。 (有关这些提议的详细信息，请参阅第 11 页上的 “通道协商”。)

企业站点的 NetScreen-A 上的出接口为 ethernet3，其 IP 地址为 1.1.1.1/24，并绑定到 Untrust 区段上。分公司的 NetScreen-B 将该地址用作远程 IKE 网关。

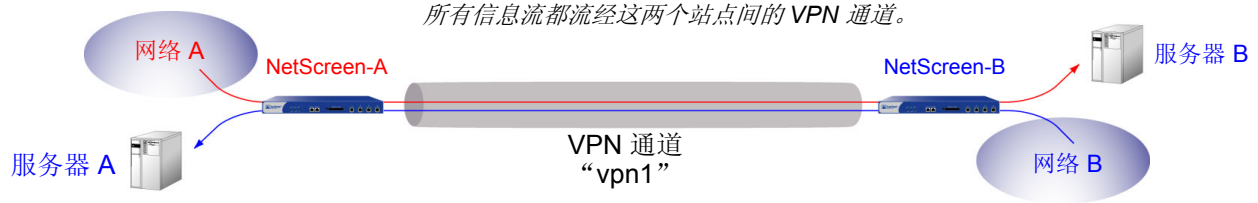
分公司的 NetScreen-B 上的出接口为 ethernet3，其 IP 地址为 2.2.2.2/24，并绑定到 Untrust 区段上。企业站点的 NetScreen-A 将该地址用作远程 IKE 网关。

两个 NetScreen 设备上的 Trust 区段接口为 ethernet1，其 IP 地址为 10.1.1.1/24。两个 NetScreen 设备上的所有区段都位于 trust-vr 路由选择域中。



网络 A 上的用户可以访问服务器 B。网络 B 上的用户也可以访问服务器 A。

所有信息流都流经这两个站点间的 VPN 通道。



WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.10.1.1/24

2. DIP

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

ID: 5

IP Address Range: (选择), 10.10.1.2 ~ 10.10.1.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 地址

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

Address Name: corp

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: virtualA

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.5/32

Zone: Trust

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

Address Name: branch1

IP Address/Domain Name:

IP/Netmask: (选择), 10.20.1.2/32

Zone: Untrust

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

Address Name: serverB

IP Address/Domain Name:

IP/Netmask: (选择), 10.20.1.5/32

Zone: Untrust

4. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: branch1

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

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3[25]

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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.10.1.0/24

Remote IP / Netmask: 10.20.1.0/24

Service: ANY

25. 出接口不一定非要位于通道接口绑定到的区段中，但在本例中二者位于同一区段。

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: ethernet3

Gateway IP Address: 1.1.1.250

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

Network Address/Netmask: 10.20.1.0/24

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: 10.20.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

6. 策略

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

Source Address:

Address Book Entry: (选择), corp

Destination Address:

Address Book Entry: (选择), serverB

Service: FTP

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP On: 5 (10.10.1.2–10.10.1.2)/X-late

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

Source Address:

Address Book Entry: (选择), branch1

Destination Address:

Address Book Entry: (选择), virtualA

Service: FTP

Action: Permit

Position at Top: (选择)

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

NAT:

Destination Translation: (选择)

Translate to IP: (选择), 10.1.1.5

Map to Port: (清除)

WebUI (NetScreen-B)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.20.1.1/24

2. DIP

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

ID: 6

IP Address Range: (选择), 10.20.1.2 ~ 10.20.1.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

3. 地址

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

Address Name: branch1

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: virtualB

IP Address/Domain Name:

IP/Netmask: (选择), 10.20.1.5/32

Zone: Trust

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

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.2/32

Zone: Untrust

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

Address Name: serverA

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.5/32

Zone: Untrust

4. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3[26]

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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.20.1.0/24

Remote IP / Netmask: 10.10.1.0/24

Service: ANY

26. 出接口不一定非要位于通道接口绑定到的区段中，但在本例中二者位于同一区段。

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: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address/Netmask: 10.10.1.0/24

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: 10.10.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

6. 策略

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

Source Address:

Address Book Entry: (选择), corp

Destination Address:

Address Book Entry: (选择), serverA

Service: FTP

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP on: 6 (10.20.1.2–10.20.1.2)/X-late

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

Source Address:

Address Book Entry: (选择), corp

Destination Address:

Address Book Entry: (选择), virtualB

Service: FTP

Action: Permit

Position at Top: (选择)

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

NAT:

Destination Translation: (选择)

Translate to IP: 10.1.1.5

Map to Port: (清除)

CLI (NetScreen-A)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.10.1.1/24
```

2. DIP

```
set interface tunnel.1 dip 5 10.10.1.2 10.10.1.2
```

3. 地址

```
set address trust corp 10.1.1.0/24
set address trust virtualA 10.10.1.5/32
set address untrust branch1 10.20.1.2/32
set address untrust serverB 10.20.1.5/32
```

4. VPN

```
set ike gateway branch1 address 2.2.2.2 outgoing-interface ethernet3[27] preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway branch1 sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any
```

27. 出接口不一定非要位于通道接口绑定到的区段中，但在本例中二者位于同一区段。

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.20.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.20.1.0/24 interface null metric 10
```

6. 策略

```
set policy top from trust to untrust corp serverB ftp nat src dip-id 5 permit
set policy top from untrust to trust branch1 virtualA ftp nat dst ip 10.1.1.5
    permit
save
```

CLI (NetScreen-B)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.20.1.1/24
```

2. DIP

```
set interface tunnel.1 dip 6 10.20.1.2 10.20.1.2
```

3. 地址

```
set address trust branch1 10.1.1.0/24
set address trust virtualB 10.20.1.5/32
set address untrust corp 10.10.1.2/32
set address untrust serverA 10.10.1.5/32
```

4. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3[28] preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.1
set vpn vpn1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter trust-vr route 10.10.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.10.1.0/24 interface null metric 10
```

6. 策略

```
set policy top from trust to untrust branch1 serverA ftp nat src dip-id 6
    permit
set policy top from untrust to trust corp virtualB ftp nat dst ip 10.1.1.5
    permit
save
```

28. 出接口不一定非要位于通道接口绑定到的区段中，但在本例中二者位于同一区段。

透明模式 VPN

当 NetScreen 设备接口处于 “透明” 模式时 (即，这些接口无 IP 地址并且在 OSI 模型[29] 中的 “第二层” 运行)，可将 VLAN1 IP 地址用作 VPN 终止点。 VPN 通道将引用外向区段而不是出接口，当接口处于 “路由” 或 NAT 模式时 (即，这些接口具有 IP 地址并且在 “第三层” 运行) 将引用后者。缺省情况下，通道将 V1-Untrust 区段用作外向区段。如果有多个接口绑定到同一个外向区段，则 VPN 通道可使用其中的任意一个接口。

***注意：** 本版发行时，接口处于 “透明” 模式的 NetScreen 设备仅支持基于策略的 VPN。有关 “透明” 模式的详细信息，请参阅第 **2** -104 页上的 “透明模式”。*

29. OSI 模型是网络协议体系结构的网络行业标准模型。 OSI 模型由七个层构成，其中第二层是数据链路层，第三层是网络层。

范例：透明模式，基于策略的自动密钥 IKE VPN

在本例中，将在其接口处于 “透明” 模式下的两台 NetScreen 设备间设置一个基于策略的 “自动密钥 IKE” VPN 通道。

***注意：**两台 NetScreen 设备的接口不必都处于 “透明” 模式。通道一端的设备的接口可以处于 “透明” 模式，而另一台设备的接口可以处于 “路由” 或 NAT 模式。*

通道两端的 NetScreen 设备的主要配置元素如下：

配置元素	NetScreen-A	NetScreen-B
V1-Trust 区段	Interface: ethernet1, 0.0.0.0/0 (为本地 admin 启用管理)	Interface: ethernet1, 0.0.0.0/0 (为本地 admin 启用管理)
V1-Untrust 区段	Interface: ethernet3, 0.0.0.0/0	Interface: ethernet3, 0.0.0.0/0
VLAN1 接口	IP Address: 1.1.1.1/24 Manage IP: 1.1.1.2*	IP Address: 2.2.2.2/24 Manage IP: 2.2.2.3
地址	local_lan: 1.1.1.0/24 in V1-Trust peer_lan: 2.2.2.0/24 in V1-Untrust	local_lan: 2.2.2.0/24 in V1-Trust peer_lan: 1.1.1.0/24 in V1-Untrust
IKE 网关	gw1, 2.2.2.2, preshared key h1p8A24nG5, security: compatible	gw1, 1.1.1.1, preshared key h1p8A24nG5, security: compatible
VPN 通道	security: compatible	security: compatible
策略	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1
外部路由器	IP Address: 1.1.1.250	IP Address: 2.2.2.250
路由	0.0.0.0/0，使用通向网关 1.1.1.250 的 VLAN1 接口	0.0.0.0/0，使用通向网关 2.2.2.250 的 VLAN1 接口

* 通过使用管理 IP 地址接收管理信息流及使用 VLAN1 地址终止 VPN 信息流，可从 VPN 信息流分离管理信息流。

为接口处于 “透明”模式的 NetScreen 设备配置基于策略的 “自动密钥 IKE”通道包括以下步骤 :

1. 从物理接口删除所有 IP 地址，并将接口绑定到第 2 层安全区段。
2. 为 VLAN1 接口分配并管理 IP 地址。
3. 在 V1-Trust 和 V1-Untrust 区段的通讯簿中输入本地及远程端点的 IP 地址。
4. 配置 VPN 通道，并将其外向区段指定为 V1-Untrust 区段。
5. 输入通向 trust-vr 中外部路由器的缺省路由。
6. 为各个站点间通过的 VPN 信息流设置策略。

WebUI (NetScreen-A)

1. 接口

注意 : *将 VLAN1 IP 地址移动到不同的子网会使 NetScreen 设备删除与前一个 VLAN1 接口相关的所有路由。通过 WebUI 配置 NetScreen 设备时，工作站必须能访问第一个 VLAN1 地址，其次必须与新地址位于同一子网中。更改 VLAN1 地址后，必须更改工作站的 IP 地址，以便使工作站的 IP 地址与新的 VLAN1 地址位于同一子网中。还可能需要将工作站重新定位到物理上与 NetScreen 设备相邻的子网中。*

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

IP Address / Netmask: 1.1.1.1/24

Manage IP: 1.1.1.2

Management Services: WebUI, Telnet, Ping[30]

30. 为 V1-Trust 区段和 VLAN1 接口上的 WebUI、Telnet 和 Ping 启用管理选项，以便 V1-Trust 区段中的本地 admin 可以访问 VLAN1 管理 IP 地址。如果尚未在 VLAN1 和 V1-Trust 区段接口上启用通过 WebUI 的管理，则将无法通过 WebUI 访问 NetScreen 设备以进行这些设置。必须首先通过控制台连接在这些接口上设置 WebUI 可管理性。

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

Management Services: WebUI, Telnet

Other Services: Ping

选择以下内容，然后单击 **OK**:

Zone Name: V1-Trust

IP Address/Netmask: 0.0.0.0/0

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

Zone Name: V1-Untrust

IP Address/Netmask: 0.0.0.0/0

2. 地址

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

Address Name: local_lan

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.0/24

Zone: V1-Trust

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

Address Name: peer_lan

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.0/24

Zone: V1-Untrust

3. VPN

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

Gateway Name: gw1

Security Level: Compatible

Remote Gateway Type:

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

Preshared Key: h1p8A24nG5

Outgoing Zone: V1-Untrust

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (选择), gw1

4. 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: VLAN1 (VLAN)

Gateway IP Address: 1.1.1.250

5. 策略

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

Source Address:

Address Book Entry: (选择), local_lan

Destination Address:

Address Book Entry: (选择), peer_lan

Service: ANY

Action: Tunnel

Tunnel VPN: vpn1

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

WebUI (NetScreen-B)

1. 接口

***注意：**将 VLAN1 IP 地址移动到不同的子网会使 NetScreen 设备删除与前一个 VLAN1 接口相关的所有路由。通过 WebUI 配置 NetScreen 设备时，工作站必须能访问第一个 VLAN1 地址，其次必须与新地址位于同一子网中。更改 VLAN1 地址后，必须更改工作站的 IP 地址，以便使工作站的 IP 地址与新的 VLAN1 地址位于同一子网中。还可能需要将工作站重新定位到物理上与 NetScreen 设备相邻的子网中。*

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

IP Address/Netmask: 2.2.2.2/24

Manage IP: 2.2.2.3

Management Services: WebUI[31] , Telnet, Ping

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

Management Services: WebUI, Telnet

Other Services: Ping

选择以下内容，然后单击 **OK**:

Zone Name: V1-Trust

IP Address/Netmask: 0.0.0.0/0

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

Zone Name: V1-Untrust

IP Address/Netmask: 0.0.0.0/0

31. 如果尚未在 VLAN1 和 V1-Trust 区段接口上启用通过 WebUI 的管理，则将无法通过 WebUI 访问 NetScreen 设备以进行这些设置。必须首先通过控制台连接在这些接口上设置 WebUI 可管理性。

2. 地址

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

Address Name: local_lan

IP Address/Domain Name:

IP/Netmask: (选择), 2.2.2.0/24

Zone: V1-Trust

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

Address Name: peer_lan

IP Address/Domain Name:

IP/Netmask: (选择), 1.1.1.0/24

Zone: V1-Untrust

3. VPN

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

Gateway Name: gw1

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

Preshared Key: h1p8A24nG5

Outgoing Zone: V1-Untrust

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Predefined: (选择), gw1

4. 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: VLAN1 (VLAN)

Gateway IP Address: 2.2.2.250

5. 策略

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

Source Address:

Address Book Entry: (选择), local_lan

Destination Address:

Address Book Entry: (选择), peer_lan

Service: ANY

Action: Tunnel

Tunnel VPN: vpn1

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

CLI (NetScreen-A)

1. 接口和区段

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage web
set zone v1-trust manage telnet
set zone v1-trust manage ping[32]

unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust

set interface vlan1 ip 1.1.1.1/24
set interface vlan1 manage-ip 1.1.1.2
set interface vlan1 manage web
set interface vlan1 manage telnet
set interface vlan1 manage ping
```

2. 地址

```
set address v1-trust local_lan 1.1.1.0/24
set address v1-untrust peer_lan 2.2.2.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface v1-untrust preshare
    h1p8A24nG5 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
```

32. 为 V1-Trust 区段和 VLAN1 接口上的 WebUI、 Telnet 和 Ping 启用管理选项，以便 V1-Trust 区段中的本地 admin 可以访问 VLAN1 管理 IP 地址。

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 1.1.1.250
```

5. 策略

```
set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn
    vpn1
set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn
    vpn1
save
```

CLI (NetScreen-B)

1. 接口和区段

```
unset interface ethernet1 ip
unset interface ethernet1 zone
set interface ethernet1 zone v1-trust
set zone v1-trust manage

unset interface ethernet3 ip
unset interface ethernet3 zone
set interface ethernet3 zone v1-untrust

set interface vlan1 ip 2.2.2.2/24
set interface vlan1 manage-ip 2.2.2.3
set interface vlan1 manage
```

2. 地址

```
set address v1-trust local_lan 2.2.2.0/24
set address v1-untrust peer_lan 1.1.1.0/24
```

3. VPN

```
set ike gateway gw1 address 1.1.1.1 main outgoing-interface v1-untrust preshare
    h1p8A24nG5 sec-level compatible
set vpn vpn1 gateway gw1 sec-level compatible
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface vlan1 gateway 2.2.2.250
```

5. 策略

```
set policy top from v1-trust to v1-untrust local_lan peer_lan any tunnel vpn
    vpn1
set policy top from v1-untrust to v1-trust peer_lan local_lan any tunnel vpn
    vpn1
save
```

5

拨号 VPN

NetScreen 设备支持拨号 VPN 连接。可以配置具有静态 IP 地址的 NetScreen 设备，从而确保具有 NetScreen-Remote 客户端或具有动态 IP 地址的其它 NetScreen 设备的 IPSec 通道安全。

本章提供以下拨号 VPN 概念的范例：

拨号 VPN

可以为单个 VPN 拨号用户配置通道，也可以将用户组成 VPN 拨号组，从而只需为该组配置一个通道。还可创建组 IKE ID 用户，它允许定义一位用户，该用户的 IKE ID 作为各个拨号 IKE 用户的 IKE ID 的一部分。在有大型拨号用户组时，此方案特别节省时间，因为不必单独配置每个 IKE 用户。

***注意：**有关创建 IKE 用户组的详细信息，请参阅第 **8**-76 页上的 “IKE 用户和用户组”。有关 “组 IKE ID” 功能的详细信息，请参阅第 270 页上的 “组 IKE ID”。*

如果拨号客户端能支持虚拟内部 IP 地址 (NetScreen-Remote 即支持)，还可创建动态对等方拨号 VPN、“自动密钥 IKE” 通道 (具有预共享密钥或证书)。可以用静态 IP 地址配置 NetScreen 安全网关，从而确保具有 NetScreen-Remote 客户端或具有动态 IP 地址的其它 NetScreen 设备的 IPSec 通道安全。

***注意：**有关可用 VPN 选项的背景信息，请参阅第 1 章，“IPSec”。有关从多种选项中进行选择的指导，请参阅第 3 章，“VPN 准则”。*

可为 VPN 拨号用户配置基于策略的 VPN 通道。对于拨号动态对等方客户端[1]，可配置基于策略或基于路由的 VPN。由于拨号动态对等方客户端可支持虚拟内部 IP 地址 (NetScreen-Remote 即支持)，因此可通过指定的通道接口配置该虚拟内部地址的路由表条目。这样允许在 NetScreen 设备和该对等方之间配置基于路由的 VPN 通道。

***注意：**除拨号客户端的内部 IP 地址为虚拟地址外，拨号动态对等方与站点到站点动态对等方几乎一样。*

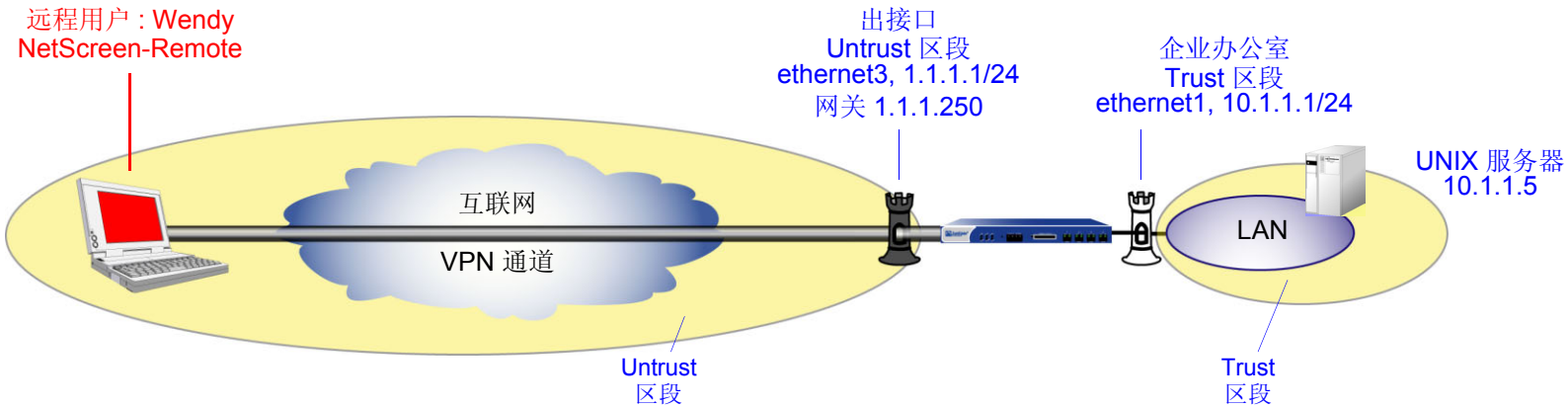
1. 拨号动态对等方客户端是拨号客户端，它支持虚拟内部 IP 地址。

范例：基于策略的拨号 VPN，自动密钥 IKE

在本范例中，“自动密钥 IKE”通道使用预共享密钥或使用一对证书 (通道[2] 的每端各一个)，提供 IKE 用户 Wendy 和 UNIX 服务器之间的安全信道。通道再次使用由 3DES 加密并且由 SHA-1 认证的 ESP。

用具有预共享密钥或证书的 “自动密钥 IKE”设置 “自动密钥 IKE”通道，要求在企业站点进行以下配置：

1. 为 Trust 和 Untrust 区段配置接口，两个区段都在 trust-vr 路由选择域中。
2. 在 Trust 区段通讯簿中输入 UNIX 服务器的地址。
3. 将 Wendy 定义为 IKE 用户。
4. 配置远程网关和 “自动密钥 IKE VPN”。
5. 设置缺省路由。
6. 创建从 Untrust 区段到 Trust 区段、允许拨号用户访问 UNIX 的策略。



2. 预共享密钥为 h1p8A24nG5。假定两个参与者都已经有证书。有关证书的详细信息，请参阅第 29 页上的 “证书和 CRL”。

预共享密钥为 h1p8A24nG5。本范例假定两个参与者都已经具有 Verisign 发布的 RSA 证书，并且 NetScreen-Remote 上的本地证书包含 U-FQDN wparker@email.com。(有关获取和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。) 对于 “阶段 1” 和 “阶段 2” 安全级别，指定 “阶段 1” 提议 (对预共享密钥方法为 pre-g2-3des-sha，对证书为 rsa-g2-3des-sha) 并对 “阶段 2” 选择预定义的 “Compatible (兼容)” 提议集。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: UNIX

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Wendy

Status: Enable (选择)

IKE User: (选择)

Simple Identity: (选择)

IKE Identity: wparker@email.com

4. VPN

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

Gateway Name: Wendy_NSR

Security Level: Custom

Remote Gateway Type:

Dialup User: (选择), User: Wendy

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: Wendy_UNIX

Security Level: Compatible

Remote Gateway:

Predefined: (选择), Wendy_NSR

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: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), UNIX

Service: ANY

Action: Tunnel

Tunnel VPN: Wendy_UNIX

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. 接口

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

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

2. 地址

```
set address trust unix 10.1.1.5/32
```

3. 用户

```
set user wendy ike-id u-fqdn wparker@email.com
```

4. VPN

预共享密钥

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

(或)

证书

```
set ike gateway wendy_nsr dialup wendy aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway wendy_nsr cert peer-ca 1[3]
set ike gateway wendy_nsr cert peer-cert-type x509-sig
set vpn wendy_unix gateway wendy_nsr sec-level compatible
```

5. 路由

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

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" unix any tunnel vpn
    wendy_unix
save
```

3. 数字 1 为 CA ID 号。要了解 CA 的 ID 号，请使用以下命令 : **get pki x509 list ca-cert**。

NetScreen-Remote 安全策略编辑器

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

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 10.1.1.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 1.1.1.1

4. 单击位于 UNIX 图标左边的加号，展开连接策略。
5. 单击 **My Identity**: 执行以下任一操作：

   单击 **Pre-shared Key** > **Enter Key**: 键入 **h1p8A24nG5**，然后单击 **OK**。

   ID Type: (选择 **E-mail Address**)，然后键入 **wparker@email.com**。

   (或)

   从 “Select Certificate” 下拉列表中选择一个证书。

   ID Type: (选择 **E-mail Address**)[4]

6. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
7. 单击位于 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。

4. 来自证书的电子邮件地址自动出现在标识符字段中。

8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法 :

   Authentication Method: Pre-Shared Key

   (或)

   Authentication Method: RSA Signatures

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :

   Encapsulation Protocol (ESP): (选择)

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Tunnel

10. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Tunnel

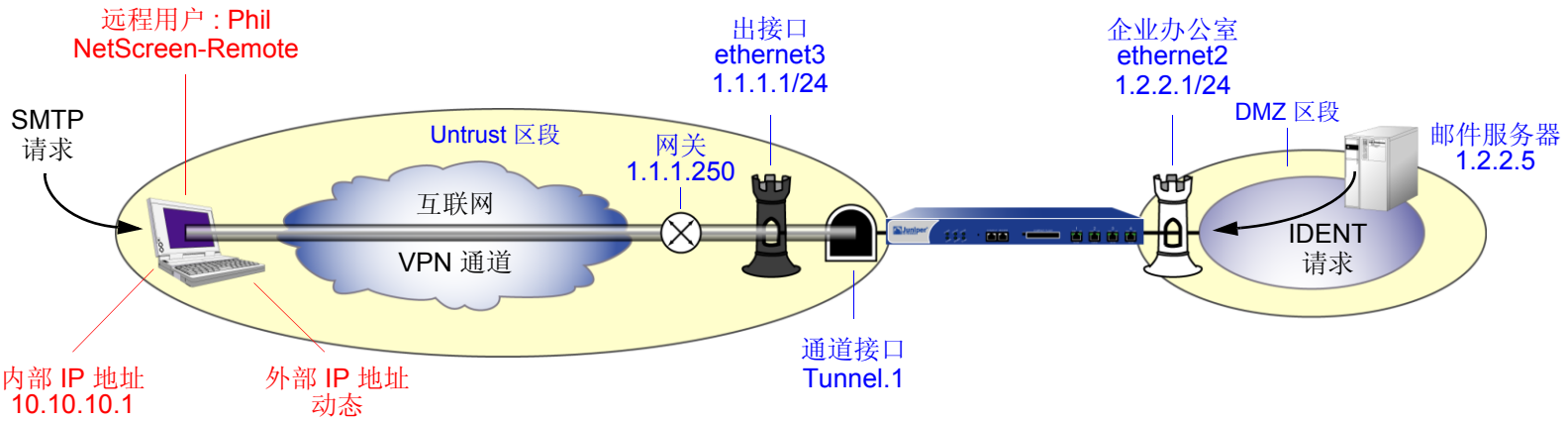
13. 单击 **File > Save Changes**。

范例：基于路由的拨号 VPN，动态对等方

在本例中， VPN 通道将 NetScreen-Remote 后面的用户安全连接到 NetScreen 设备的 Untrust 区段接口，以保护 DMZ 区段中的邮件服务器。 Untrust 区段接口具有静态 IP 地址。 NetScreen-Remote 客户端具有一个动态分配的外部 IP 地址和一个静态 (虚拟) 的内部 IP 地址。NetScreen 设备的管理员必须知道对等方的内部 IP 地址，目的有以下两个：

- 管理员可在策略中使用它。
- 管理员可创建路由，将地址与绑定到相应通道的通道接口相关联。

NetScreen-Remote 客户端建立通道后，信息流即可从该通道的任一端通过。 NetScreen 设备的所有区段都在 trust-vr 路由域中。



在本例中， Phil 要从公司网站的邮件服务器取得他的电子邮件。当他尝试这样做时，邮件服务器程序对他进行认证，通过通道向他发送一条 IDENT 请求。

注意： *只有在 NetScreen 管理员为邮件服务器 (TCP，端口 113) 添加了定制服务，并且设置了允许信息流通过通道到达 10.10.10.1 的外向策略时，邮件服务器才能通过通道发送 IDENT 请求。*

预共享密钥为 h1p8A24nG5。本例假定两个参与者都已获得 Verisign 发布的 RSA 证书，并且 NetScreen-Remote 上的本地证书包含 U-FQDN *pm@juniper.net*。(有关获取和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。) 对于 “阶段 1” 和 “阶段 2” 安全级别，指定 “阶段 1” 提议 (对预共享密钥方法为 pre-g2-3des-sha，对证书为 rsa-g2-3des-sha) 并对 “阶段 2” 选择预定义的 “Compatible (兼容)” 提议集。

可在 NetScreen 设备上输入以下三个路由 :

- 通向 trust-vr 中外部路由器的缺省路由
- 通过通道接口通向目标的路由
- 通向目标的 Null 路由。为 Null 路由分配较高的度量 (远离零)，以便其成为通向目标的下一个可选路由。接着，如果通道接口的状态变为 “中断”，且引用该接口的路由变为非活动，则 NetScreen 设备会使用 Null 路由 (即实质上丢弃了发送给它的任何信息流)，而不使用缺省路由 (即转发未加密的信息流)。

最后，创建允许信息流在 Phil 和邮件服务器之间的双向流动的策略。

WebUI

1. 接口

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

Zone Name: DMZ

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.2.2.1/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Unnumbered: (选择)

Interface: ethernet3 (trust-vr)

2. 地址

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

Address Name: Mail Server

IP Address/Domain Name:

IP/Netmask: (选择), 1.2.2.5/32

Zone: DMZ

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

Address Name: Phil

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.10.1/32

Zone: Untrust

3. 服务

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (选择)

Transport Protocol: TCP (选择)

Source Port: Low 1, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: 输入以下内容，移动以下服务，然后单击 **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident
MAIL
POP3

4. VPN

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

Gateway Name: To_Phil

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (选择), Peer ID: pm@juniper.net

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: corp_Phil

Security Level: Compatible

Remote Gateway:

Predefined: (选择), To_Phil

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

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

Proxy-ID: (选择)

Local IP / Netmask: 1.2.2.5/32

Remote IP / Netmask: 10.10.10.1/32

Service: Any

5. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

Network Address/Netmask: 10.10.10.1/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

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

Network Address/Netmask: 10.10.10.1/32

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

6. 策略

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

Source Address:

Address Book Entry: (选择), Phil

Destination Address:

Address Book Entry: (选择), Mail Server

Service: Remote_Mail

Action: Permit

Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), Mail Server

Destination Address:

Address Book Entry: (选择), Phil

Service: Remote_Mail

Action: Permit

Position at Top: (选择)

CLI

1. 接口

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

2. 地址

```
set address dmz "Mail Server" 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. 服务

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

预共享密钥

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

(或)

证书

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1[5]
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
set vpn corp_phil bind interface tunnel.1
set vpn corp_phil proxy-id local-ip 1.2.2.5/32 remote-ip 10.10.10.1/32 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1
set vrouter trust-vr route 10.10.10.1/32 interface null metric 10
```

6. 策略

```
set policy top from dmz to untrust "Mail Server" phil remote_mail permit
set policy top from untrust to dmz phil "Mail Server" remote_mail permit
save
```

5. 数字 1 是 CA ID 号。要了解 CA 的 ID 号，请使用以下命令 : **get pki x509 list ca-cert**。

NetScreen-Remote

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

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 1.2.2.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 1.1.1.1

5. 单击 unix 图标左侧的加号，展开连接策略。
6. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
7. 单击 **My Identity**，并执行下列任一操作：

   单击 **Pre-shared Key** > **Enter Key**: 键入 **h1p8A24nG5**，然后单击 **OK**。

   ID Type: E-mail Address; pm@juniper.net

   Internal Network IP Address: 10.10.10.1

   (或)

   从 Select Certificate 下拉列表中，选择包含电子邮件地址“pm@juniper.net”的证书。

   ID Type: E-mail Address; pm@juniper.net

   Internal Network IP Address: 10.10.10.1

8. 单击 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。
9. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法 :

   Authentication Method: Pre-Shared Key

   (或)

   Authentication Method: RSA Signatures

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2
10. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel
11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel
12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

13. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

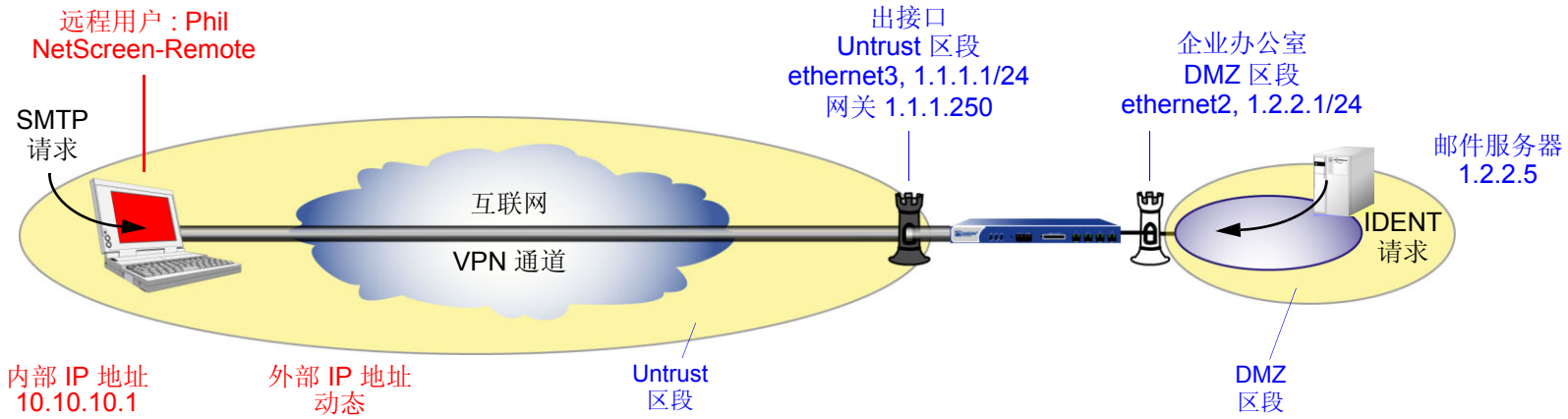
    Hash Alg: MD5

    Encapsulation: Tunnel

14. 单击 **File > Save Changes**。

范例：基于策略的拨号 VPN，动态对等方

在本例中， VPN 通道将 NetScreen-Remote 后面的用户安全连接到 NetScreen 设备的 Untrust 区段接口，以保护 DMZ 区段中的邮件服务器。 Untrust 区段接口具有静态 IP 地址。 NetScreen-Remote 客户端具有一个动态分配的外部 IP 地址和一个静态 (虚拟) 的内部 IP 地址。NetScreen 设备的管理员必须知道客户端的内部 IP 地址，以便能将它添加到 Untrust 通讯薄中，以用于为来自该来源的信息流建立通道的策略。 NetScreen-Remote 客户端建立通道后，信息流可从该通道的任一端通过。



在本例中， Phil 要从公司网站的邮件服务器取得他的电子邮件。当他尝试这样做时，邮件服务器程序对他进行认证，通过通道向他发送一条 IDENT 请求。

注意： *只有在 NetScreen 管理员为邮件服务器 (TCP，端口 113) 添加了定制服务，并且设置了允许信息流通过通道到达 10.10.10.1 的外向策略时，邮件服务器才能通过通道发送 IDENT 请求。*

预共享密钥为 h1p8A24nG5。本范例假定两个参与者都已经具有 Verisign 发布的 RSA 证书，并且 NetScreen-Remote 上的本地证书包含 U-FQDN *pm@juniper.net*。(有关获得和加载证书的详细信息，请参阅第 29 页上的 “证书和 CRL”。) 对于 “阶段 1” 和 “阶段 2” 安全级别，指定 “阶段 1” 提议 (对预共享密钥方法为 pre-g2-3des-sha，对证书为 rsa-g2-3des-sha) 并对 “阶段 2” 选择预定义的 “Compatible (兼容)” 提议集。

WebUI

1. 接口

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

   Zone Name: DMZ

   Static IP: (出现时选择此选项)

   IP Address/Netmask: 1.2.2.1/24

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

   Zone Name: Untrust

   Static IP: (出现时选择此选项)

   IP Address/Netmask: 1.1.1.1/24

2. 地址

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

   Address Name: Mail Server

   IP Address/Domain Name:

   IP/Netmask: (选择), 1.2.2.5/32

   Zone: DMZ

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

Address Name: Phil

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.10.1/32

Zone: Untrust

3. 服务

Objects > Services > Custom > New: 输入以下内容，然后单击 **OK**:

Service Name: Ident

Service Timeout:

Use protocol default: (选择)

Transport Protocol: TCP (选择)

Source Port: Low 1, High 65535

Destination Port: Low 113, High 113

Objects > Services > Group > New: 输入以下内容，移动以下服务，然后单击 **OK**:

Group Name: Remote_Mail

Group Members << Available Members:

Ident
MAIL
POP3

4. VPN

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

Gateway Name: To_Phil

Security Level: Custom

Remote Gateway Type:

Dynamic IP Address: (选择), Peer ID: pm@juniper.net

预共享密钥

Preshared Key: h1p8A24nG5

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

(或)

证书

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: corp_Phil
Security Level: Compatible
Remote Gateway:
Predefined: (选择), To_Phil

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: ethernet3
Gateway IP Address: 1.1.1.250

6. 策略

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

Source Address:
Address Book Entry: (选择), Phil
Destination Address:
Address Book Entry: (选择), Mail Server
Service: Remote_Mail
Action: Tunnel
VPN Tunnel: corp_Phil
Modify matching bidirectional VPN policy: (选择)
Position at Top: (选择)

CLI

1. 接口

```
set interface ethernet2 zone dmz
set interface ethernet2 ip 1.2.2.1/24

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

2. 地址

```
set address dmz "mail server" 1.2.2.5/32
set address untrust phil 10.10.10.1/32
```

3. 服务

```
set service ident protocol tcp src-port 1-65535 dst-port 113-113
set group service remote_mail
set group service remote_mail add ident
set group service remote_mail add mail
set group service remote_mail add pop3
```

4. VPN

预共享密钥

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
set vpn corp_phil gateway to_phil sec-level compatible
```

(或)

证书

```
set ike gateway to_phil dynamic pm@juniper.net aggressive outgoing-interface
    ethernet3 proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1[6]
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
```

5. 路由

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

6. 策略

```
set policy top from untrust to dmz phil "mail server" remote_mail tunnel vpn
    corp_phil
set policy top from dmz to untrust "mail server" phil remote_mail tunnel vpn
    corp_phil
save
```

6. 数字 1 为 CA ID 号。要了解 CA 的 ID 号，请使用以下命令 : **get pki x509 list ca-cert**。

NetScreen-Remote

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

   Connection Security: Secure

   Remote Party Identity and Addressing:

   ID Type: IP Address, 1.2.2.5

   Protocol: All

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 1.1.1.1

5. 单击 unix 图标左侧的加号，展开连接策略。
6. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
7. 单击 **My Identity**，并执行下列任一操作：

   单击 **Pre-shared Key** > **Enter Key**: 键入 **h1p8A24nG5**，然后单击 **OK**。

   Internal Network IP Address: 10.10.10.1

   ID Type: E-mail Address; pm@juniper.net

   (或)

   从 Select Certificate 下拉列表中，选择包含电子邮件地址“pmason@email.com”的证书。

   Internal Network IP Address: 10.10.10.1

   ID Type: E-mail Address; pm@juniper.net

8. 单击位于 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。

9. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法 :

   Authentication Method: Pre-Shared Key

   (或)

   Authentication Method: RSA Signatures

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

10. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: SHA-1

    Encapsulation: Tunnel

11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Tunnel

12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

Hash Alg: SHA-1

Encapsulation: Tunnel

13. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Tunnel

14. 单击 **File > Save Changes**。

用于拨号 VPN 用户的双向策略

可以为拨号 VPN 创建双向策略。此配置提供的功能与动态对等 VPN 配置类似。但是，使用动态对等 VPN 配置，NetScreen 设备管理员必须知道拨号用户的内部 IP 地址空间，以便在配置外向策略时，管理员可将其用作目标地址 (请参阅第 252 页上的 “范例 : 基于策略的拨号 VPN，动态对等方”)。使用拨号 VPN 用户配置， LAN 网站的管理员不需要知道拨号用户的内部地址空间。保护 LAN 的 NetScreen 设备使用预定义的地址 “Dial-Up VPN” 作为内向策略中的源地址及外向策略中的目标地址。

此项为拨号 VPN 通道创建双向策略的功能，在建立连接后允许信息流从 VPN 连接的 LAN 端发起。 (远程端必须首先启动通道创建。) 请注意，与拨号动态对等 VPN 通道不同，此功能要求内向和外向策略上的服务相同。

***注意 :** NetScreen 不支持引用拨号 VPN 配置的双向策略中的服务组和地址组。*

请注意，两个或多个同时连接的拨号 VPN 用户的内部地址空间可能会重叠。例如，拨号用户 A 和 B 可能都具有内部 IP 地址空间 10.2.2.0/24。如果出现这种情况，NetScreen 设备会通过在策略列表中找到的第一个策略中引用的 VPN 向用户 A 和用户 B 发送所有出站 VPN 信息流。例如，如果将 VPN 引用到用户 A 的出站策略首先出现在策略列表中，则 NetScreen 设备就会将预定给用户 A 和 B 的所有出站 VPN 信息流发送到用户 A。

同样，拨号用户的内部地址可能与其它任何策略中的地址重叠，无论其它策略是否引用 VPN 通道。如果出现这种情况， NetScreen 设备会应用与源地址、目标地址、源端口号、目标端口号及服务的基本信息流属性匹配的第一个策略。为避免具有动态产生的地址的双向拨号 VPN 策略取代具有静态地址的另一个策略， Juniper Networks 建议将双向拨号 VPN 策略放在策略列表中较低的位置。

范例 : 双向拨号 VPN 策略

在本例中，为具有 IKE ID *jf@ns.com* 的 IKE 用户 *dialup-j* 配置名为 *VPN_dial* 的拨号 “自动密钥 IKE VPN” 通道的双向策略。对于 “阶段 1” 协商，使用提议 *pre-g2-3des-sha* 以及预共享密钥 *Jf11d7uU*。为 “阶段 2” 协商选择预定义的 “Compatible (兼容)” 提议集。

IKE 用户从 Untrust 区段的 NetScreen 设备发起到 VPN 连接，以访问 Trust 区段中的企业服务器。 IKE 用户建立 VPN 连接后，信息流可从通道的任一端发起。

Trust 区段接口为 ethernet1，其 IP 地址为 10.1.1.1/24，并且处于 NAT 模式。 Untrust 区段接口为 ethernet3，其 IP 地址为 1.1.1.1/24。缺省路由指向 1.1.1.250 处的外部路由器。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 对象

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

Address Name: trust_net

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: dialup-j

Status: Enable

IKE User: (选择)

Simple Identity: (选择); jf@ns.com

3. VPN

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

Gateway Name: dialup1

Security Level: Custom

Remote Gateway Type:

Dialup User: (选择); dialup-j

Preshared Key: Jf11d7uU

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): pre-g2-3des-sha

Mode (Initiator): Aggressive

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

VPN Name: VPN_dial

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (选择)

Gateway Name: dialup1

Type:

Dialup User: (选择); dialup-j

Preshared Key: Jf11d7uU

Security Level: Compatible

Outgoing Interface: ethernet3

4. 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: ethernet1

Gateway IP Address: 1.1.1.250

5. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), trust_net

Service: ANY

Action: Tunnel

VPN Tunnel: VPN_dial

Modify matching bidirectional VPN policy: (选择)

CLI

1. 接口

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

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

2. 对象

```
set address trust trust_net 10.1.1.0/24
set user dialup-j ike-id u-fqdn jf@ns.com
```

3. VPN

```
set ike gateway dialup1 dialup dialup-j aggressive outgoing-interface ethernet3
    preshare Jf11d7uU proposal pre-g2-3des-sha
set vpn VPN_dial gateway dialup1 sec-level compatible
```

4. 路由

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

5. 策略

```
set policy from untrust to trust "Dial-Up VPN" trust_net any tunnel vpn
    VPN_dial
set policy from trust to untrust trust_net "Dial-Up VPN" any tunnel vpn
    VPN_dial
save
```

NetScreen-Remote 安全策略编辑器

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

   Connection Security: Secure

   Remote Party Identity and Addressing

   ID Type: IP Subnet

   Subnet: 10.1.1.0

   Mask: 255.255.255.0

   Protocol: All

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 1.1.1.1
4. 单击位于 UNIX 图标左边的加号，展开连接策略。
5. 单击 **My Identity**: 执行以下任一操作：

   单击 **Pre-shared Key** > **Enter Key**: 键入 **Jf11d7uU**，然后单击 **OK**。

   ID Type: (选择 **E-mail Address**)，然后键入 **jf@ns.com**。
6. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
7. 单击位于 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。
8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法：

   Authentication Method: Pre-Shared Key

   (或)

Authentication Method: RSA Signatures
Encrypt Alg: Triple DES
Hash Alg: SHA-1
Key Group: Diffie-Hellman Group 2

9. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel
10. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel
11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel
12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel
13. 单击 **File > Save Changes**。

组 IKE ID

某些组织拥有许多拨号 VPN 用户。例如，一个销售部门可能拥有几百个用户，其中许多用户在远离网站时要求保证拨号通信的安全。对于数量如此之多的用户，为每位用户分别创建单独的用户定义、拨号 VPN 配置以及策略是不切实际的。

为了消除这种麻烦，“组 IKE ID”方法使一个用户定义可用于多个用户。组 IKE ID 用户定义适用于以下两类用户，即具有在识别名称 (dn) 中有指定值的证书的所有用户，或者全部 IKE ID 和 VPN 客户端上的预共享密钥与 NetScreen 设备上的部分 IKE ID 和预共享密钥匹配的所有用户。

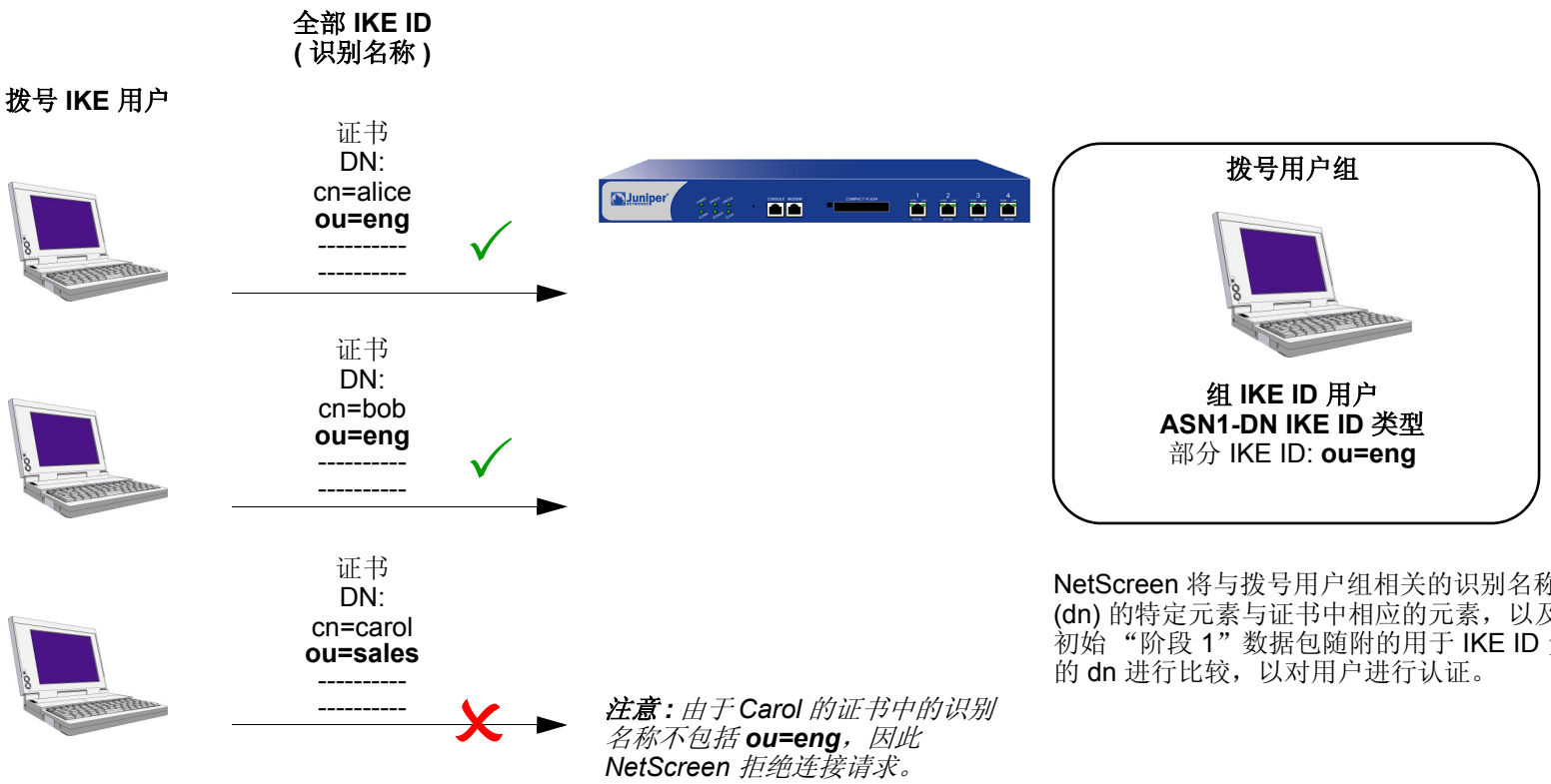
***注意：**拨号 IKE 用户连接到 NetScreen 设备时，NetScreen 设备首先提取并使用全部 IKE ID，搜索其对等方网关记录以防用户不属于组 IKE ID 用户组。如果全部 IKE ID 搜索过程没有匹配条目， NetScreen 设备则检查内向的嵌入 IKE ID 和配置的组 IKE ID 用户之间是否有部分 IKE ID 匹配。*

将单个组 IKE ID 用户添加到一个 IKE 拨号 VPN 用户组中，并指定该组支持的并发连接的最大数量。并发会话的最大数量不能超过允许的 “第 1 阶段” SA 的最大数量，或 NetScreen 平台上允许的 VPN 通道最大数量。

具有证书的组 IKE ID

具有证书的 “组 IKE ID” 是一项认证技术，用于对一组拨号 IKE 用户执行 IKE 认证，而不必为每个用户配置单独的用户配置文件。NetScreen 设备使用包含部分 IKE ID 的单个组 IKE ID 用户配置文件。一个拨号 IKE 用户可成功建立通向 NetScreen 设备的 VPN 通道，前提是在他的 VPN 客户端上的 VPN 配置指定了一个包含识别名称元素的证书，而这些元素与那些配置为 NetScreen 设备上的组 IKE ID 用户配置文件中的部分 IKE ID 定义的元素相匹配。

具有证书的组 IKE ID



可设置具有证书的组 IKE ID，方法如下：

在 NetScreen 设备上：

1. 创建一个新的具有部分 IKE 标识 (如 *ou=sales，o=netscreen*) 的组 IKE ID 用户，并指定可使用组 IKE ID 配置文件进行登录的拨号用户数量。
2. 将新的组 IKE ID 用户分配到一个拨号用户组[7]，并命名该组。
3. 在拨号 “自动密钥 IKE VPN” 配置中，指定拨号用户组的名称、“阶段 1” 协商处于 Aggressive mode (主动模式) 以及使用证书 (具体是 RSA 还是 DSA，要取决于在拨号 VPN 客户端加载的证书的类型) 进行认证。
4. 创建允许入站信息流通过指定的拨号 VPN 的策略。

在 VPN 客户端上：

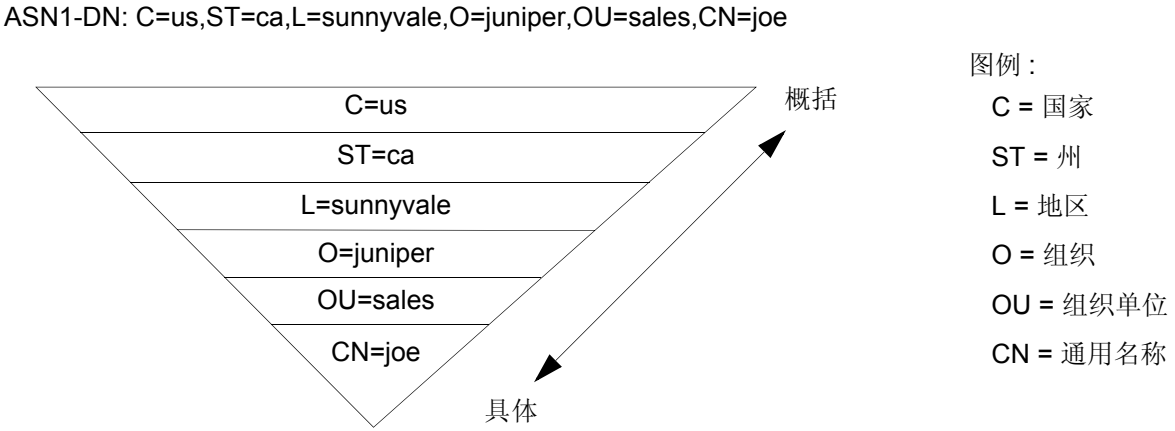
1. 获得并加载特定证书，该证书的识别名称所包含的信息要与在 NetScreen 设备上部分 IKE ID 中定义的信息相同。
2. 对于 “阶段 1” 协商，使用 Aggressive mode (主动模式) 配置通向 NetScreen 设备的 VPN 通道，指定之前已经加载的证书，并为本地 IKE ID 类型选择 *Distinguished Name*。

此后，每个具有特定证书 (即识别名称元素与组 IKE ID 用户配置文件中定义的部分 IKE ID 匹配的证书) 的拨号 IKE 用户都可以成功建立通向 NetScreen 设备的 VPN 通道。例如，如果组 IKE ID 用户的 IKE ID 为 *OU=sales，O=netscreen*，则 NetScreen 设备接受来自任何特定用户 (该用户拥有的证书在其识别名称中包含这些元素) 的 “阶段 1” 协商。可连接到 NetScreen 设备的此类拨号 IKE 用户的最大数量，要取决于在组 IKE ID 用户配置文件中指定的并发会话的最大数量。

7. 在 IKE 用户组中只能放置一组 IKE ID 用户。

通配符和容器 ASN1-DN IKE ID 类型

为组 IKE 用户定义 IKE ID 时，必须使用版本 1 的 “抽象语法表示法”，识别名称 (ASN1-DN) 作为标识配置的 IKE ID 类型。此表示法是一连串的值，其顺序通常为 (但并非总是) 从概括到具体。例如 :



配置组 IKE ID 用户时，必须将对等方的 ASN1-DN ID 指定为以下两种类型之一 :

- **通配符 :** 如果拨号 IKE 用户的 ASN1-DN 标识字段中的值与组 IKE 用户的 ASN1-DN 标识字段中的值匹配，则 NetScreen 认证拨号 IKE 用户的 ID 有效。对于每个标识字段，通配符 ID 类型仅支持一个值 (例如，支持 “ou=eng” 或 “ou=sw”，但不支持 “ou=eng, ou=sw”)。两个 ASN1-DN 字符串中标识字段的顺序无关紧要。
- **容器 :** 如果拨号 IKE 用户的 ASN1-DN 标识字段中的值与组 IKE 用户的 ASN1-DN 标识字段中的值完全匹配，则 NetScreen 认证拨号 IKE 用户的 ID 有效。对于每个标识字段，容器 ID 类型支持多个条目 (例如，“ou=eng, ou=sw, ou=screenos”)。两个 ASN1-DN 字符串在标识字段中的值的排序必须一样。

为远程 IKE 用户配置 ASN1-DN ID 时，指定类型为 “通配符” 或 “容器”，并定义期望在对等方的证书中收到的 ASN1-DN ID (例如，“c=us, st=ca, cn=jrogers”)。为本地 IKE ID 配置 ASN1-DN ID 时，使用以下关键字 : [DistinguishedName]。包含括号而且拼写应完全如前所示。

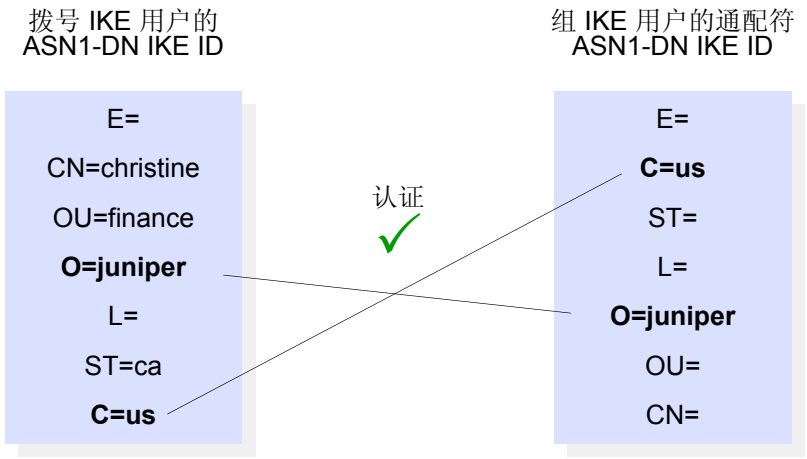
通配符 ASN1-DN IKE ID

通配符 ASN1-DN 要求远程对等方的识别名称 IKE ID 中的值与组 IKE 用户的部分 ASN1-DN IKE ID 中的值匹配，这些值在 ASN1-DN 字符串中的先后顺序无关紧要。例如，如果拨号 IKE 用户的 ID 和组 IKE 用户的 ID 如下：

- 拨号 IKE 用户的全部 ASN1-DN IKE ID: CN=christine,OU=finance,**O=netscreen**,ST=ca,**C=us**
- 组 IKE 用户的部分 ASN1-DN IKE ID: **C=us**,**O=netscreen**

则一个通配符 ASN1-DN IKE ID 成功匹配两个 IKE ID，即使两个 ID 中值的顺序不同。

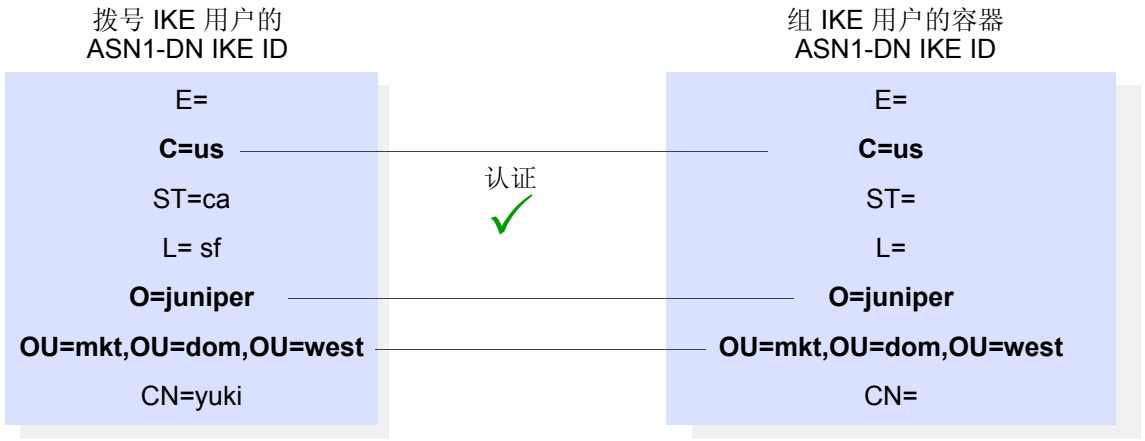
拨号 IKE 用户的 ASN1-DN 包含在组 IKE 用户的 ASN1-DN 中指定的值。值的顺序并不重要。



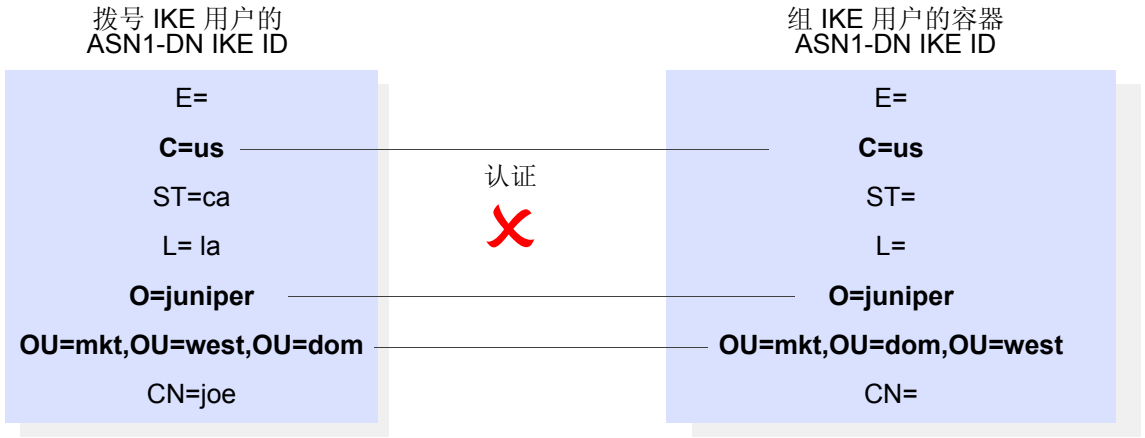
容器 ASN1-DN IKE ID

容器 ASN1-DN ID 允许组 IKE 用户的 ID 在每个标识字段中拥有多个条目。如果拨号用户的 ID 包含的值与组 IKE 用户 ID 中的值完全匹配，则 NetScreen 认证拨号 IKE 用户有效。与通配符类型不同的是，在拨号 IKE 用户和组 IKE 用户的 ID 中， ASN1-DN 字段的顺序必须相同，并且这些字段中多个值的顺序也必须相同。

第一个拨号 IKE 用户的 ASN1-DN 包含与组 IKE 用户的 ASN1-DN 完全匹配的值。OU ID 字段中多个条目的顺序也相同。

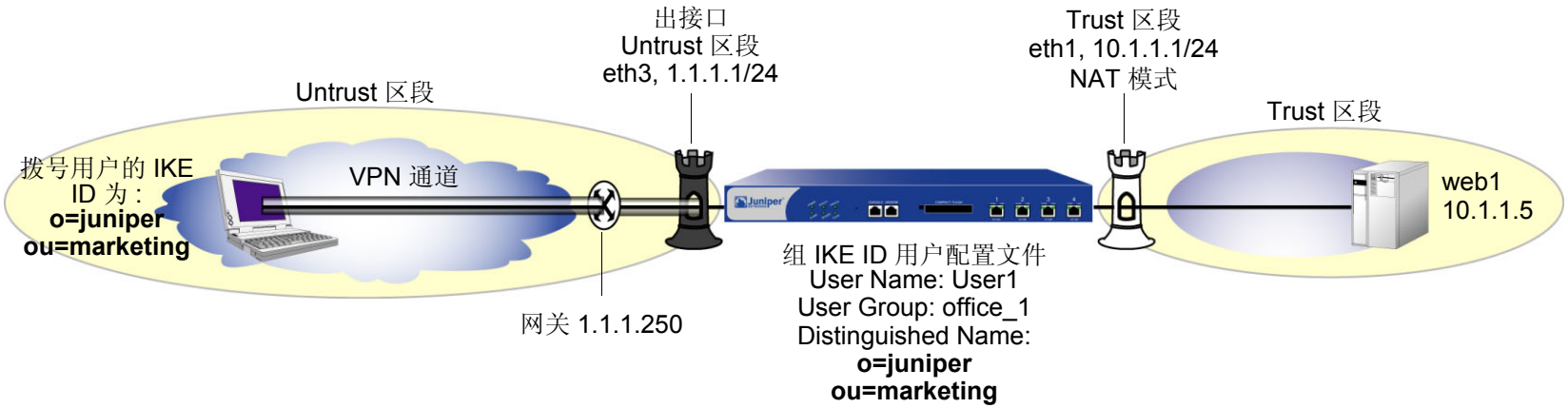


第二个拨号 IKE 用户的 ASN1-DN 包含与组 IKE 用户的 ASN1-DN 完全匹配的值。但是， OU ID 字段中多个条目的顺序不一样。



范例 : 组 IKE ID (证书)

在本范例中，创建名为 *User1* 的新的组 IKE ID 用户定义。将其配置为可接受同时来自具有特定 RSA 证书 (该证书包含 *O=netscreen* 和 *OU=marketing*) 的 VPN 客户端的数量多达 10 个的 “阶段 1” 协商。证书授权机构 (CA) 为 Verisign。将拨号 IKE 用户组命名为 *office_1*。



拨号 IKE 用户发送一个识别名称作为他们的 IKE ID。此组中拨号 IKE 用户的证书中的识别名称 (dn) 可能以下列连在一起的字符串方式出现 :

C=us,ST=ca,L=sunnyvale,**O=netscreen**,**OU=marketing**,CN=michael zhang,CN=a2010002,CN=ns500, CN=4085557800,CN=rsa-key,CN=10.10.5.44

由于值 *O=netscreen* 和 *OU=marketing* 出现在对等方的证书中，并且该用户使用该识别名称作为其 IKE ID 类型，因此 NetScreen 设备会认证该用户有效。

对于 “阶段 1” 和 “阶段 2” 安全级别，指定一个 “阶段 1” 提议 (对证书为 rsa-g2-3des-sha)，并为 “阶段 2” 选择预定义的 “Compatible (兼容)” 提议集。

配置拨号 VPN 和允许 HTTP 信息流通过 VPN 通道到达 Web 服务器 *Web1* 的策略。其中也包括远程 VPN 客户端 (使用 NetScreen-Remote) 的配置。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: User1

Status Enable: (选择)

IKE User: (选择)

Number of Multiple Logins with same ID: 10

Use Distinguished Name For ID: (选择)

OU: marketing

Organization: juniper

Objects > User Groups > Local > New: 在 Group Name 字段中键入 **office_1**，执行以下操作，然后单击 **OK**:

选择 **User1**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

4. VPN

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

Gateway Name: Corp_GW

Security Level: Custom

Remote Gateway Type: Dialup User Group: (选择), Group: office_1

Outgoing Interface: ethernet3

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

Security Level: Custom

Phase 1 Proposal (for Custom Security Level): rsa-g2-3des-sha

Mode (Initiator): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: Corp_VPN

Security Level: Compatible

Remote Gateway: Predefined: (选择), Corp_GW

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: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Corp_VPN

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. 接口

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

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

2. 地址

```
set address trust web1 10.1.1.5/32
```

3. 用户

```
set user User1 ike-id asn1-dn wildcard o=juniper,ou=marketing share-limit 10
set user-group office_1 user User1
```

4. VPN

```
set ike gateway Corp_GW dialup office_1 aggressive outgoing-interface ethernet3
    proposal rsa-g2-3des-sha
set ike gateway Corp_GW cert peer-ca 1[8]
set ike gateway Corp_GW cert peer-cert-type x509-sig
set vpn Corp_VPN gateway Corp_GW sec-level compatible
```

5. 路由

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

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" web1 http tunnel vpn Corp_VPN
save
```

8. 数字 1 是 CA ID 号。要了解 CA 的 ID 号，请使用以下命令 : **get pki x509 list ca-cert**。

NetScreen-Remote 安全策略编辑器

1. 单击 **Options > Secure > Specified Connections**。
2. 单击 **Add a new connection**，在出现的新连接图标旁键入 **web1**。
3. 配置连接选项：

   Connection Security: Secure
   Remote Party Identity and Addressing
   ID Type: IP Address, 10.1.1.5
   Protocol: 突出显示 **All**，键入 **HTTP**，按下 **Tab** 键，然后键入 **80**。
   Connect using Secure Gateway Tunnel: (选择)
   ID Type: IP Address, 1.1.1.1

4. 单击位于 web1 图标左边的加号，展开连接策略。
5. 单击 **My Identity**: 从 Select Certificate 下拉列表[9] 中，选择在识别名称中将 *o=netscreen,ou=marketing* 作为元素的证书。

   ID Type: 从下拉列表中选择 **Distinguished Name**。

6. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
7. 单击 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。
8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择下列 “加密” 和 “数据完整性” 算法：

   Authentication Method: RSA Signatures
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2

9. 本范例假定在 NetScreen-Remote 客户端上已经加载了适当的证书。有关在 NetScreen-Remote 上加载证书的信息，请参阅 NetScreen-Remote 文档。

9. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel
10. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Encapsulation: Tunnel
11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel
12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: DES
   Hash Alg: MD5
   Encapsulation: Tunnel
13. 单击 **File > Save Changes**。

具有预共享密钥的组 IKE ID

具有预共享密钥的 “组 IKE ID” 是一项技术，用于对一组拨号 IKE 用户执行 IKE 认证，而不必为每个用户配置单独的用户配置文件。NetScreen 设备使用包含部分 IKE ID 的单组 IKE ID 用户配置文件。一个拨号 IKE 用户可成功建立通向 NetScreen 设备的 VPN 通道，前提是如果在他的 VPN 客户端上的 VPN 配置具有正确的预共享密钥，并且用户的全部 IKE ID 的最靠右侧部分与组 IKE ID 用户配置文件的部分 IKE ID 定义相匹配。

IKE 用户发送全部 IKE ID 时， NetScreen 会实时生成预共享密钥。

(每个 IKE 用户的预共享密钥 = 预共享密钥种子值 x 全部 IKE ID。)

NetScreen 将其产生的密钥与初始 “第 1 阶段” 数据包随附的预共享密钥进行比较，以便认证用户。

可用于具有预共享密钥功能的组 IKE ID 的 IKE ID 类型，可以是一个电子邮件地址，也可以是一个完全合格的域名 (FQDN)。

可设置具有预共享密钥的组 IKE ID，方法如下：

在 NetScreen 设备上：

1. 创建一个新的具有部分 IKE 标识的组 IKE ID 用户 (如 **juniper.net**)，并指定可使用组 IKE ID 配置文件进行登录的拨号用户的数量。
2. 将新的组 IKE ID 用户分配给拨号用户组。
3. 在拨号 “自动密钥 IKE VPN” 配置中，为远程网关指派一个名称 (如 **road1**)，指定拨号用户组，并输入一个预共享密钥种子值。
4. 使用下列 CLI 命令，用预共享密钥种子值和完整用户 IKE ID (如 **joe@juniper.net**) 生成单个拨号用户的预共享密钥：

   exec ike preshare-gen *name_str usr_name_str*

   (例如) **exec ike preshare-gen road1 joe@juniper.net**
5. 记录配置远程 VPN 客户端时所使用的预共享密钥。

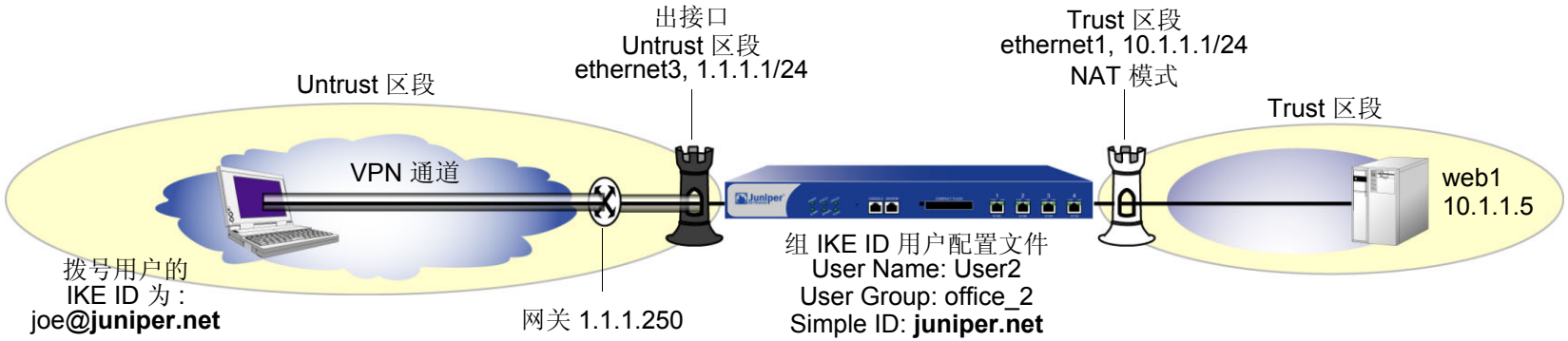
在 VPN 客户端上：

对于 “阶段 1” 协商，使用 Aggressive mode (主动模式) 配置通向 NetScreen 设备的 VPN 通道，并输入之前在 NetScreen 设备上生成的预共享密钥。

此后，NetScreen 设备可成功认证每个特定的单独用户，该用户的全部 IKE ID 包含一部分与部分组 IKE ID 用户配置文件相匹配的内容。例如，如果组 IKE ID 用户具有 IKE 标识 **juniper.net**，则在 IKE ID 中具有该域名的任何用户都能以 Aggressive mode (主动模式) 在 NetScreen 设备上发起 “阶段 1” IKE 协商。例如：**alice@juniper.net**、**bob@juniper.net** 和 **carol@juniper.net**。可登录的此类用户数量取决于在组 IKE ID 用户配置文件中指定的最大并发会话数量。

范例 : 组 IKE ID (预共享密钥)

在本范例中，创建命名为 *User2* 的新的组 IKE ID 用户。将其配置为接受同时来自具有预共享密钥的 VPN 客户端的数量多达 10 个的 “阶段 1” 协商，该预共享密钥包含由字符串 *juniper.net* 结尾的 IKE ID。预共享密钥的种子值为 *jk930k*。将拨号 IKE 用户组命名为 *office_2*。



对于 “阶段 1” 和 “阶段 2” 协商，选择预定义为 “Compatible (兼容)” 的安全级别。所有安全区段都在 trust-vr 路由域中。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: User2

Status: Enable

IKE User: (选择)

Number of Multiple Logins with same ID: 10

Simple Identity: (选择)

IKE Identity: juniper.net

Objects > User Groups > Local > New: 在 Group Name 字段中键入 **office_2**，执行以下操作，然后单击 **OK**:

选择 **User2**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

4. VPN

> ***注意：****WebUI 仅允许输入一个预共享密钥值，而不是从 NetScreen 设备衍生的预共享密钥所使用的种子值。要在配置 IKE 网关时输入预共享密钥种子值，必须使用 CLI。*

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

VPN Name: Corp_VPN

Security Level: Compatible

Remote Gateway: Predefined: (选择), Corp_GW

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: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Corp_VPN

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. 接口

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

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

2. 地址

```
set address trust web1 10.1.1.5/32
```

3. 用户

```
set user User2 ike-id u-fqdn juniper.net share-limit 10
set user-group office_2 user User2
```

4. VPN

```
set ike gateway Corp_GW dialup office_2 aggressive seed-preshare jk930k
    sec-level compatible
set vpn Corp_VPN gateway Corp_GW sec-level compatible
```

5. 路由

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

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" web1 http tunnel vpn
    Corp_VPN
save
```

获得预共享密钥

只能通过使用以下 CLI 命令获得预共享密钥 :

exec ike preshare-gen *name_str usr_name_str*

基于预共享密钥种子值 *jk930k* (在名为 *Corp_GW* 的远程网关的配置中指定)，以及单个用户的全部标识 *joe@juniper.net* 预共享密钥为 *11ccce1d396f8f29ffa93d11257f691af96916f2*。

NetScreen-Remote 安全策略编辑器

1. 单击 **Options > Secure > Specified Connections**。
2. 单击 **Add a new connection**，在出现的新连接图标旁键入 **web1**。
3. 配置连接选项 :

   Connection Security: Secure

   Remote Party Identity and Addressing

   ID Type: IP Address, 10.1.1.5

   Protocol: 突出显示 **All**，键入 **HTTP**，按下 **Tab** 键，然后键入 **80**。

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address, 1.1.1.1
4. 单击位于 web1 图标左边的加号，展开连接策略。
5. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
6. 单击 **My Identity**: 单击 **Pre-shared Key** > **Enter Key**: 键入 **11ccce1d396f8f29ffa93d11257f691af96916f2**，然后单击 **OK**。

   ID Type: (选择 **E-mail Address**)，然后键入 **joe@juniper.net**。
7. 单击位于 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。

8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择下列 “加密” 和 “数据完整性” 算法 :
   Authentication Method: Pre-Shared Key
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2
9. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Authentication Method: Pre-Shared Key
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2
10. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Authentication Method: Pre-Shared Key
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Key Group: Diffie-Hellman Group 2
11. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Authentication Method: Pre-Shared Key
    Encrypt Alg: DES
    Hash Alg: MD5
    Key Group: Diffie-Hellman Group 2

12. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: Triple DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel
13. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: Triple DES
    Hash Alg: MD5
    Encapsulation: Tunnel
14. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel
15. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: DES
    Hash Alg: MD5
    Encapsulation: Tunnel
16. 单击 **File > Save Changes**。

共享 IKE ID

共享 IKE ID 功能使得部署大量的拨号用户很方便。利用此功能， NetScreen 设备使用单个组 IKE ID 和预共享密钥可以对多个拨号 VPN 用户进行认证。这样，它即可通过通用 VPN 配置为大型远程用户组提供 IPSec 保护。

此功能与具有预共享密钥的 “组 IKE ID”的功能类似，其不同之处如下 :

- 对于组 IKE ID 功能，IKE ID 可以是电子邮件地址或 FQDN (完全合格的域名)。对于此功能， IKE ID 必须是电子邮件地址。
- 为组中的所有用户指定单个预共享密钥，而不是使用预共享密钥种子值和完全用户 IKE ID 为每个用户生成一个预共享密钥。
- 必须使用 XAuth 对单个用户进行认证。

在 NetScreen 设备上设置共享 IKE ID 和预共享密钥 :

1. 创建一个新的组 IKE ID 用户，并指定可使用组 IKE ID 进行登录的拨号用户数量。对于此功能，使用电子邮件地址作为 IKE ID。
2. 将新的组 IKE ID 分配给拨号用户组。
3. 在拨号到 LAN 自动密钥 IKE VPN 配置中，创建预共享 IKE ID 网关。
4. 定义 XAuth 用户，并在远程 IKE 网关上启用 XAuth。

在 VPN 客户端上 :

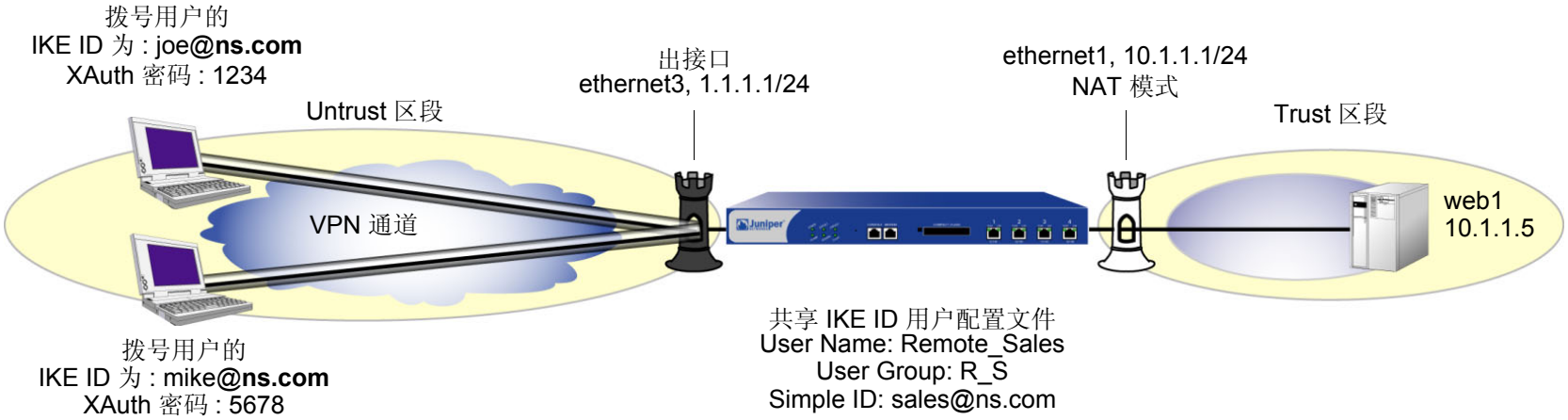
对于 “阶段 1 ”协商，使用 Aggressive mode (主动模式) 配置通向 NetScreen 设备的 VPN 通道，并输入之前在 NetScreen 设备上定义的预共享密钥。此后， NetScreen 设备对每个远程用户如下进行认证 :

在 “阶段 1”协商过程中， NetScreen 设备首先认证 VPN 客户端，方法是将客户端发送的 IKE ID 和预共享密钥与 NetScreen 设备上的 IKE ID 和预共享密钥相匹配。如果有匹配项，则 NetScreen 设备使用 XAuth 对单个用户进行认证。向 “阶段 1”和 “阶段 2” IKE 协商之间的远程站点的用户发送登录提示。如果远程用户使用正确的用户名和密码成功登录，则 “阶段 2”协商将开始。

范例：共享 IKE ID (预共享密钥)

在本例中，创建名为 Remote_Sales 的新的组 IKE ID 用户。它可接受来自具有相同预共享密钥 (abcd1234) 的 VPN 客户端的多达 250 个 “阶段 1” 协商。将拨号 IKE 用户组命名为 *R_S*。另外，配置两个 XAuth 用户， Joe 和 Mike。

对于 “阶段 1” 和 “阶段 2” 协商，选择预定义为 “Compatible (兼容)” 的安全级别。所有安全区段都在 trust-vr 路由域中。



WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: web1

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.5/32

Zone: Trust

3. 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Remote_Sales

Status: Enable

IKE User: (选择)

Number of Multiple Logins with same ID: 250

Simple Identity: (选择)

IKE Identity: sales@ns.com

Objects > User Groups > Local > New: 在 Group Name 字段中键入 **R_S**，执行以下操作，然后单击 **OK**:

选择 **Remote_sales**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Joe

Status: Enable

XAuth User: (选择)

Password: 1234

Confirm Password: 1234

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Mike

Status: Enable

XAuth User: (选择)

Password: 5678

Confirm Password: 5678

4. VPN

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

Gateway Name: sales_gateway

Security Level: Compatible (选择)

Remote Gateway Type: Dialup Group (选择), R_S

Preshared Key: abcd1234

Outgoing Interface: ethernet3

> Advanced: 输入以下内容，然后单击 **Return**，返回基本 Gateway 配置页 :

Enable XAuth: (选择)

Local Authentication: (选择)

Allow Any: (选择)

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

VPN Name: Sales_VPN

Security Level: Compatible

Remote Gateway: Predefined: (选择) sales_gateway

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

Bind to: Tunnel Zone, Untrust-Tun

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: ethernet3

Gateway IP Address: 1.1.1.250

6. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Sales_VPN

Modify matching bidirectional VPN policy: (清除)

Position at Top: (选择)

CLI

1. 接口

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

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

2. 地址

```
set address trust web1 10.1.1.5/32
```

3. 用户

```
set user Remote_Sales ike-id sales@ns.com share-limit 250
set user-group R_S user Remote_Sales
set user Joe password 1234
set user Joe type xauth
set user Mike password 5678
set user Mike type xauth
```

4. VPN

```
set ike gateway sales_gateway dialup R_S aggressive outgoing-interface
    ethernet3 preshare abcd1234 sec-level compatible
set ike gateway sales_gateway xauth
set vpn sales_vpn gateway sales_gateway sec-level compatible
set vpn sales_vpn bind zone untrust-tun
```

5. 路由

```
set route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
```

6. 策略

```
set policy top from untrust to trust "Dial-Up VPN" web1 http tunnel vpn sales_vpn
save
```

NetScreen-Remote 安全策略编辑器

本例说明用户 Joe 的配置。

1. 单击 **Options > Secure > Specified Connections**。
2. 单击 **Add a new connection**，在出现的新连接图标旁键入 **web1**。
3. 配置连接选项：

   Connection Security: Secure

   Remote Party ID Type: IP Address

   IP Address: 10.1.1.5

   Connect using Secure Gateway Tunnel: (选择)

   ID Type: IP Address; 1.1.1.1

4. 单击位于 web1 图标左边的加号，展开连接策略。
5. 单击 **Security Policy** 图标，并选择 **Aggressive Mode**，然后清除 **Enable Perfect Forward Secrecy (PFS)**。
6. 单击 **My Identity**: 单击 **Pre-shared Key** > **Enter Key**: 键入 **abcd1234**，然后单击 **OK**。

   ID Type: (选择 **E-mail Address**)，然后键入 **sales@ns.com**。
7. 单击位于 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。
8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择下列 “加密” 和 “数据完整性” 算法：

   Authentication Method: Pre-Shared Key; Extended Authentication

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Authentication Method: Pre-Shared Key; Extended Authentication
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2
10. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Authentication Method: Pre-Shared Key; Extended Authentication
   Encrypt Alg: DES
   Hash Alg: SHA-1
   Key Group: Diffie-Hellman Group 2
11. 单击 **Authentication (Phase 1)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Authentication Method: Pre-Shared Key; Extended Authentication
   Encrypt Alg: DES
   Hash Alg: MD5
   Key Group: Diffie-Hellman Group 2
12. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: Triple DES
   Hash Alg: SHA-1
   Encapsulation: Tunnel
13. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :
   Encapsulation Protocol (ESP): (选择)
   Encrypt Alg: Triple DES
   Hash Alg: MD5
   Encapsulation: Tunnel

14. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)
    Encrypt Alg: DES
    Hash Alg: SHA-1
    Encapsulation: Tunnel

15. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

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

16. 单击 **File > Save Changes**。

6

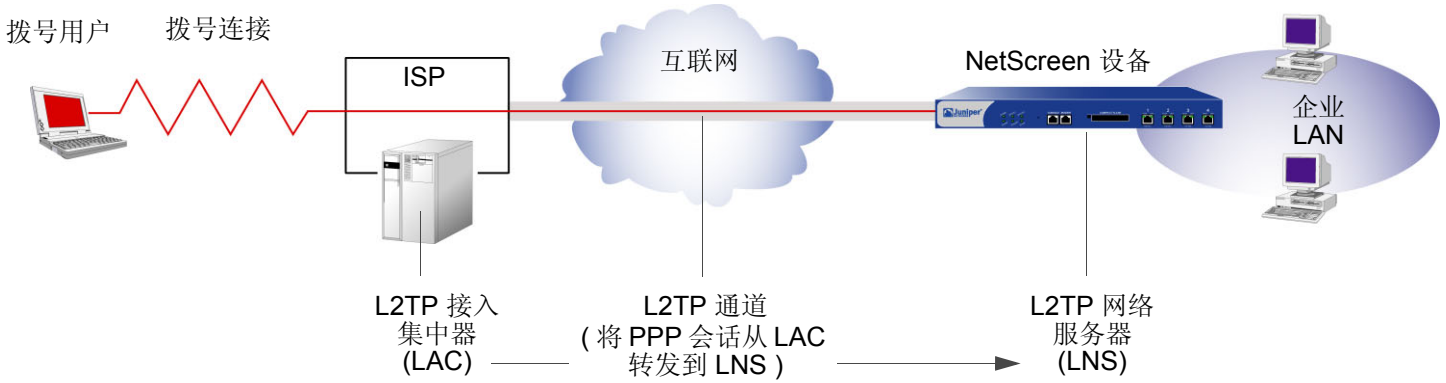
L2TP

本章将对 “第 2 层通道协议” (L2TP) 进行介绍，并说明单独使用它时的使用方法以及同 IPSec (Internet Protocol Security，互联网协议安全性) 支持一起使用时的使用方法，此外还针对 L2TP 和 IPSec 上的 L2TP 给出了一些配置范例 :

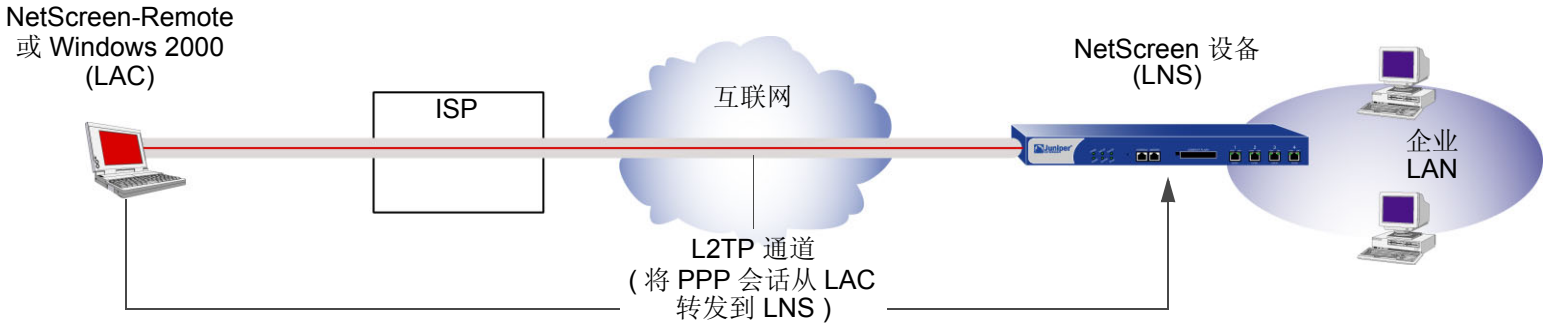
L2TP 简介

通过使用 “第 2 层通道协议” (L2TP)，拨号用户可以创建到 “L2TP 网络服务器” (LNS) 的虚拟 “点对点协议” (PPP) 连接，而该服务器可以是一台 NetScreen 设备。L2TP 通过 “L2TP 接入集中器” (LAC) 与 LNS 之间的通道来发送 PPP 帧。

最初设计 L2TP 的目的，是在某个 ISP 站点上的 LAC 与另一 ISP 站点或企业站点上的 LNS 之间建立通道连接。L2TP 通道未能完全延伸到拨号用户的计算机上，而只是延伸到了拨号用户本地 ISP 的 LAC 上。(有时将其称为强制的 L2TP 配置。)

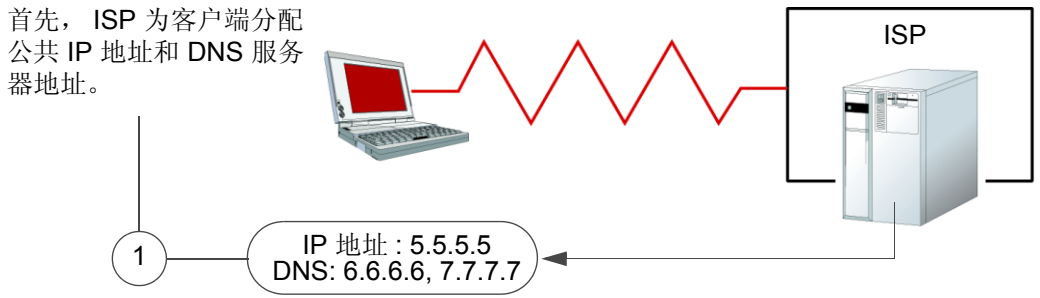


Windows 2000 或 Windows NT 的 NetScreen-Remote 客户端或 Windows 2000 客户端本身均可充当 LAC。L2TP 通道可以直接延伸到拨号用户的计算机上，从而提供端到端通道。(这种方法有时被称为自愿的 L2TP 配置。)

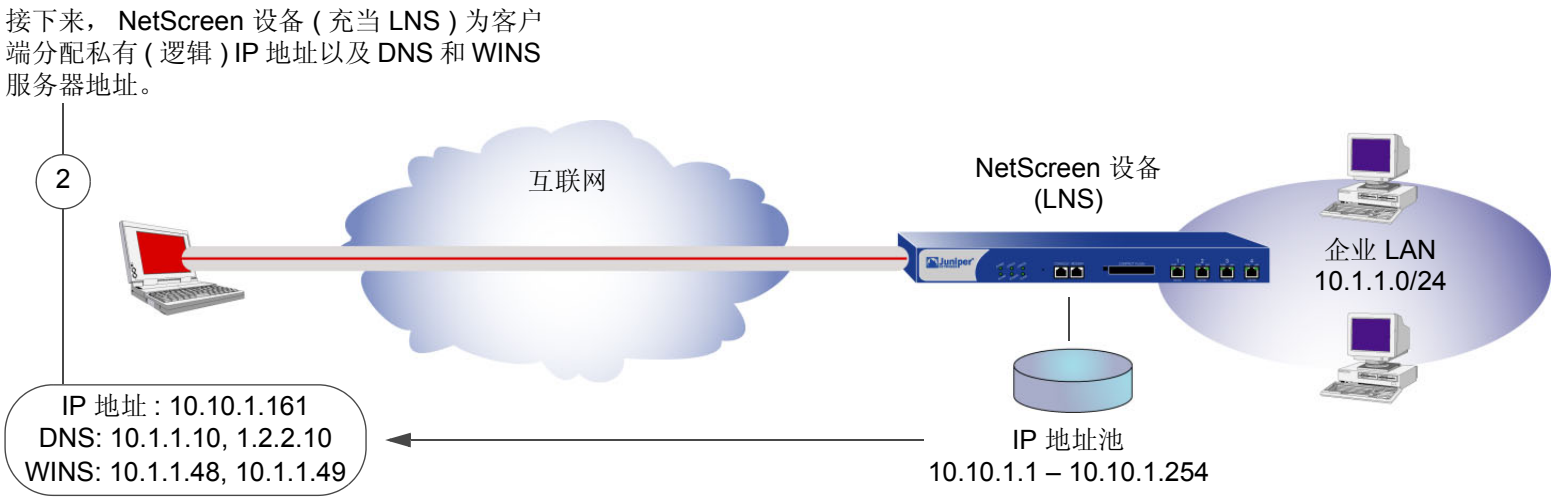


因为 PPP 链接通过互联网从拨号用户延伸到 NetScreen 设备 (LNS)，所以是由 NetScreen 设备而不是由 ISP 来分配客户端的 IP 地址、DNS 和 WINS 服务器地址的，由 NetScreen 设备通过本地数据库或外部 auth 服务器 (RADIUS、SecurID 或 LDAP) 对用户进行认证的。

实际上，客户端会收到两个 IP 地址，一个用于它和 ISP 之间的物理连接，另一个用于它与 LNS 之间的逻辑连接。当客户端与其 ISP 联系时 (可能使用 PPP)， ISP 将分配 IP 地址和 DNS 地址，并对客户端进行认证。这样用户就可通过公共 IP 地址连接到互联网，该 IP 地址成为了 L2TP 通道的外部 IP 地址。



然后，当 L2TP 通道向 NetScreen 设备转发封装的 PPP 帧时，该 NetScreen 设备将为客户端分配 IP 地址以及 DNS 和 WINS 设置。 IP 地址可能来自互联网中未使用的私有地址集。该地址将成为 L2TP 通道的内部 IP 地址。



注意 : *分配给 L2TP 客户端的 IP 地址与企业 LAN 中的 IP 地址必须处于不同的子网中。*

当前版本的 ScreenOS 提供了以下 L2TP 支持 :

- 来自运行 Windows 2000 的主机的 L2TP 通道[1]
- 传送模式下的 L2TP 和 IPSec 的组合 (IPSec 上的 L2TP)
  - 对于 NetScreen-Remote: 在 Main mode (主模式) 协商时使用证书以及在 Aggressive mode (主动模式) 协商时使用预共享密钥或证书的 IPSec 上的 L2TP
  - 对于 Windows 2000: 在 Main mode (主模式) 协商时使用证书的 IPSec 上的 L2TP
- L2TP 通道与 IPSec 上的 L2TP 通道的外向拨号策略。可将外向拨号策略与内向策略相结合，从而提供双向通道。
- 使用 “密码认证协议” (PAP) 或 “质询握手认证协议” (CHAP) 通过本地数据库或外部 auth 服务器 (RADIUS、 SecurID 或 LDAP) 对用户进行认证

  注意 : *本地数据库和 RADIUS 服务器均支持 PAP 和 CHAP。 SecurID 和 LDAP 服务器仅支持 PAP。*

- 通过本地数据库或 RADIUS 服务器分配拨号用户 IP 地址、“域名系统 (DNS)” 服务器和 “Windows 互联网命名服务 (WINS)” 服务器
- 用于根系统和虚拟系统的 L2TP 通道和 IPSec 上的 L2TP 通道

  注意 : *要使用 L2TP， NetScreen 设备必须在第 3 层运行，并且安全区段接口处于 NAT 或 “路由” 模式。当 NetScreen 设备在第 2 层运行且安全区段接口处于 “透明” 模式时，在 WebUI 中不会出现与 L2TP 相关的信息，并且与 L2TP 相关的 CLI 命令会引发错误消息。*

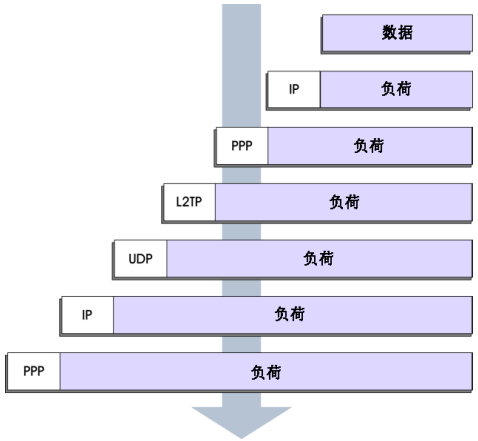
1. 缺省情况下，Windows 2000 将执行 IPSec 上的 L2TP。要强制其仅使用 L2TP，必须在注册表中找到 ProhibitIPSec 密钥并将 **0** (IPSec 上的 L2TP) 更改为 **1** (仅 L2TP)。(Juniper Networks 建议您在执行此操作前对注册表进行备份。) 单击**开始** > **运行** : 键入 **regedit**。双击 **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Services** > **RasMan** > **Parameters**。双击 **ProhibitIPSec**: 在 “数值” 数据字段中键入 **1**，选择**十六进制**作为基值，然后单击**确定**。重新启动计算机。 (如果注册表中没有类似条目，请参阅 Microsoft WIndows 文档以获得如何创建该条目的信息。)

数据包的封装和解封

L2TP 使用封装数据包的方法将 PPP 帧从 LAC 传送到 LNS。在查看有关设置 L2TP 和 IPSec 上的 L2TP 的具体范例之前，首先简要介绍一下 L2TP 过程中所涉及到的封装和解封操作。

封装

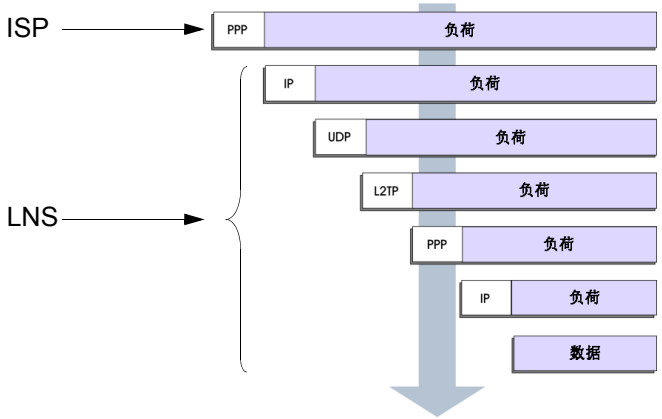
当一个 IP 网络上的拨号用户通过 L2TP 通道发送数据时， LAC 将 IP 数据包封装在一系列第 2 层帧、第 3 层数据包和第 4 层段中。假设该拨号用户通过 PPP 链接连接到本地 ISP，则封装过程如下：



1. 数据放置于 IP 负荷中。
2. 该 IP 数据包封装在 PPP 帧中。
3. 该 PPP 帧封装在 L2TP 帧中。
4. 该 L2TP 帧封装在 UDP 段中。
5. 该 UDP 段封装在 IP 数据包中。
6. 该 IP 数据包封装在 PPP 帧中，以便在拨号用户和 ISP 之间建立物理连接。

解封

当 LAC 发起到 ISP 的 PPP 链接时，解封和嵌套内容的转发过程如下：



1. ISP 完成 PPP 链接并为用户计算机分配一个 IP 地址。
   在 PPP 负荷中是一个 IP 数据包。
2. ISP 移除 PPP 包头并将 IP 数据包转发给 LNS。
3. LNS 移除该 IP 包头。
   在 IP 负荷中是一个指定端口 1701 的 UDP 段，该端口号为 L2TP 保留。
4. LNS 移除该 UDP 包头。
   在 UDP 负荷中是一个 L2TP 帧。
5. LNS 对 L2TP 帧进行处理，使用 L2TP 包头中的通道 ID 和呼叫 ID 来识别特定的 L2TP 通道。然后 LNS 移除该 L2TP 包头。
   在 L2TP 负荷中是一个 PPP 帧。
6. LNS 对 PPP 帧进行处理，为用户计算机分配一个逻辑 IP 地址。
   在 PPP 负荷中是一个 IP 数据包。
7. LNS 将该 IP 数据包路由到其最终目标，在那里移除 IP 包头并提取出 IP 数据包中的数据。

L2TP 参数

LNS 使用 L2TP 为通常来自 ISP 的拨号用户提供 PPP 设置。这些设置如下：

- IP 地址 – NetScreen 设备从 IP 地址池中选择一个地址，并将它分配给拨号用户的计算机。该选择过程在 IP 地址池中循环进行；即，在从 10.10.1.1 到 10.10.1.3 的地址池中，该地址的选择按下面的循环方式进行：10.10.1.1 – 10.10.1.2 – 10.10.1.3 – 10.10.1.1 – 10.10.1.2 …
- DNS 一级和二级服务器 IP 地址 – NetScreen 设备提供这些地址供拨号用户的计算机使用。
- WINS 一级和二级服务器 IP 地址 – NetScreen 设备也提供这些地址供拨号用户的计算机使用。

LNS 也通过用户名和密码认证用户。可以在本地数据库或外部 auth 服务器 (RADIUS、 SecurID 或 LDAP) 中输入用户。

注意：*用于认证 L2TP 用户的 RADIUS 或 SecurID 服务器可以和用于网络用户的服务器相同，也可是其它的服务器。*

另外，可以为 PPP 认证指定下列方案之一：

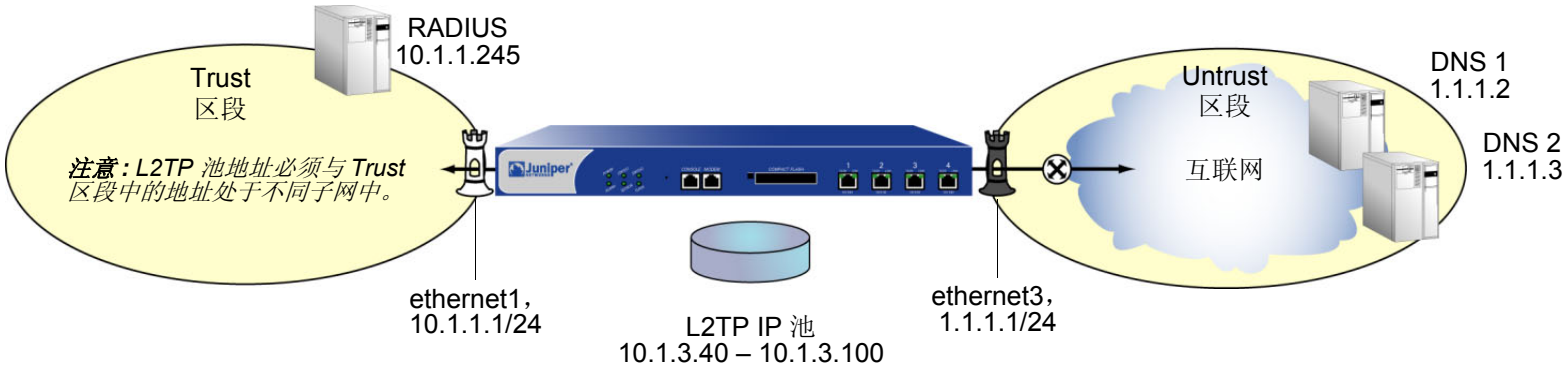
- “质询握手认证协议” (CHAP)；在拨号用户发出 PPP 链接请求后， NetScreen 设备向用户发送质询 (加密密钥)，然后用户使用该密钥加密自己的登录名称和密码。本地数据库和 RADIUS 服务器支持 CHAP。
- “密码认证协议” (PAP)；以明文方式发送拨号用户的密码，并一同发送 PPP 链接请求。本地数据库和 RADIUS、 SecurID 和 LDAP 服务器均支持 PAP。
- “ANY”；意味着 NetScreen 设备协商 CHAP，如果它出现故障，则使用 PAP。

您可以将通过“L2TP 缺省配置”页 (VPNs > L2TP > Default Settings) 所配置的缺省 L2TP 参数应用于拨号用户和拨号用户组，也可通过 **set l2tp default** 命令来执行这一操作。您也可以在 “用户配置”页 (Users > Users > Local > New) 中特别对 L2TP 用户进行配置或使用 **set user** *name_str* **remote-settings** 命令来应用 L2TP 参数。用户指定的 L2TP 设置会替代缺省的 L2TP 设置。

范例 : 配置 IP 池和 L2TP 缺省设置

在本范例中，将定义一个地址范围介于 10.1.3.40 与 10.1.3.100 之间的 IP 地址池。指定 DNS 服务器的 IP 地址为 1.1.1.2 (一级) 和 1.1.1.3 (二级)。 NetScreen 设备使用 CHAP 执行 PPP 认证。

注意 : *以每个 L2TP 通道为基础指定 auth 服务器。*



WebUI

1. IP 池

   Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

   IP Pool Name: Sutro

   Start IP: 10.1.3.40

   End IP: 10.1.3.100

2. 缺省 L2TP 设置

VPNs > L2TP > Default Settings: 输入以下内容，然后单击 **Apply**:

IP Pool Name: Sutro

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

CLI

1. IP 池

```
set ippool sutro 10.1.3.40 10.1.3.100
```

2. 缺省 L2TP 设置

```
set l2tp default ippool sutro
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
save
```

L2TP 和 IPSEC 上的 L2TP

尽管可以使用 CHAP 或 PAP 认证拨号用户，但是 L2TP 通道没有加密，因此它不是一个真正的 VPN 通道。L2TP 的作用只是允许本地 NetScreen 设备的管理员为远程拨号用户分配 IP 地址。然后这些地址可以被引用到策略中。

要加密一个 L2TP 通道，需要为该 L2TP 通道应用一个加密方案。因为 L2TP 假设 LAC 与 LNS 之间的网络为 IP，因此可以使用 IPSec 来提供加密。这种组合称为 IPSec 上的 L2TP。IPSec 上的 L2TP 要求为同一个端点既设置 L2TP 通道又设置 IPSec 通道，然后在策略中将它们链接到一起。 IPSec 上的 L2TP 要求 IPSec 通道处于传送模式，以便该通道端点的地址保持明文状态。 (有关传送模式和通道模式的信息，请参阅第 4 页上的 “模式”。)

如果更改了 Windows 2000 的注册表设置，就可以在 NetScreen 设备和一台运行 Windows 2000 的主机之间创建 L2TP 通道。 (有关如何更改注册表的信息，请参阅第 305 页上的脚注。)

可以在 NetScreen 设备和下列任意一个 VPN 客户端之间创建一个 IPSec 上的 L2TP 通道 :

- 在 Windows 2000 或 Windows NT 操作系统上运行 NetScreen-Remote 的主机
- 运行 Windows 2000 (没有 NetScreen-Remote) 的主机[2]

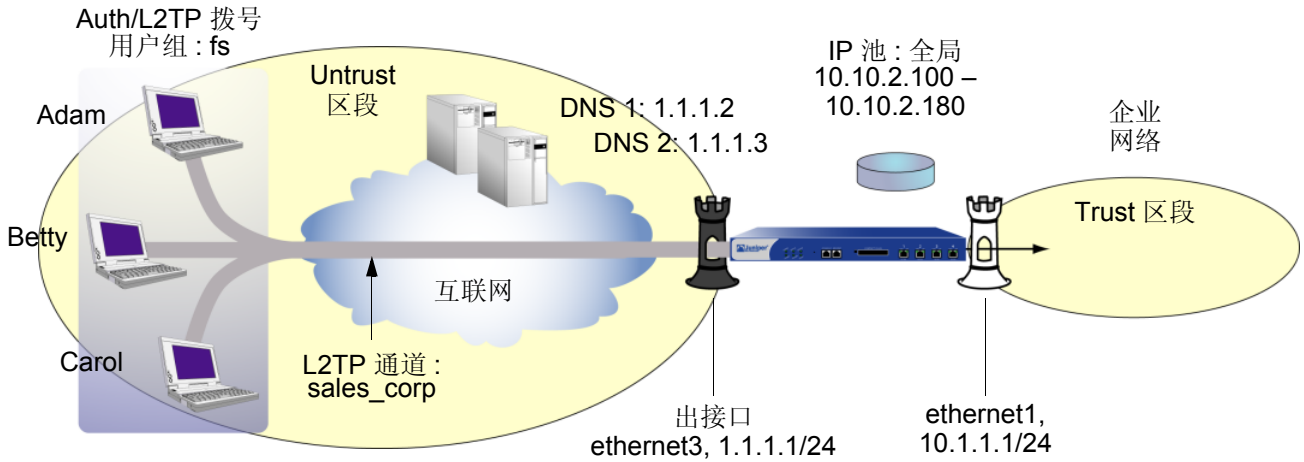
2. 要在使用没有 NetScreen-Remote 的 Windows 2000 时提供认证，就必须使用证书。

范例：配置 L2TP

在本范例中，创建一个名为 “fs”（代表 “field-sales”）的拨号用户组，并配置一个名为 “sales_corp” 的 L2TP 通道，使用 ethernet3（Untrust 区段）作为 L2TP 通道的出接口。 NetScreen 设备将下列缺省 L2TP 通道设置应用于拨号用户组：

- 通过本地数据库对 L2TP 用户进行认证。
- PPP 认证使用 CHAP。
- IP 池（名为 “global”）的地址范围介于 10.10.2.100 和 10.10.2.180 之间[3]。
- DNS 服务器为 1.1.1.2（一级）和 1.1.1.3（二级）。

注意： *一个只有 L2TP 的配置并不安全。建议仅用于调试。*



远程 L2TP 客户端使用 Windows 2000 操作系统。有关如何在远程客户端上配置 L2TP 的信息，请参阅 Windows 2000 文档。下面仅提供 L2TP 通道末端 NetScreen 设备的配置。

3. L2TP IP 池中的地址必须与企业网络中的地址处于不同子网中。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. L2TP 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Adam

Status: Enable

L2TP User: (选择)

User Password: AJbioJ15

Confirm Password: AJbioJ15

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Betty

Status: Enable

L2TP User: (选择)

User Password: BviPsoJ1

Confirm Password: BviPsoJ1

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Carol

Status: Enable

L2TP User: (选择)

User Password: Cs10kdD3

Confirm Password: Cs10kdD3

3. L2TP 用户组

Objects > User Groups > Local > New: 在“Group Name”字段中，键入 **fs**，执行以下操作，然后单击 **OK**:

选择 **Adam**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Betty**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Carol**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

4. 缺省 L2TP 设置

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: global

Start IP: 10.10.2.100

End IP: 10.10.2.180

VPNs > L2TP > Default Settings: 输入以下内容，然后单击 **OK**:

IP Pool Name: global

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

5. L2TP 通道

VPNs > L2TP > Tunnel > New: 输入以下内容，然后单击 **OK**:

Name: sales_corp

Use Custom Settings: (选择)

Authentication Server: Local

Dialup Group: Local Dialup Group - fs

Outgoing Interface: ethernet3

Peer IP: 0.0.0.0[4]

Host Name (optional): 输入充当 LAC 的计算机名称[5]。

Secret (optional): 输入一个在 LAC 和 LNS 之间共享的机密。

注意：*要将一个机密添加到 LAC 以认证 L2TP 通道，必须按如下步骤修改 Windows 2000 注册表：*

*(1) 单击**开始 > 运行**，然后键入 **regedit**。将打开“注册表编辑器”。*

*(2) 单击 **HKEY_LOCAL_MACHINE**。*

*(3) 右键单击 **SYSTEM**，然后从弹出的菜单中选择**查找**。*

*(4) 键入 **ms_l2tpminiport**，然后单击**查找下一个**。*

*(5) 在“编辑”菜单中，突出显示**新建**，然后选择**字串值**。*

*(6) 键入 **Password**。*

*(7) 双击 **Password**。出现“编辑字符串”对话框。*

(8) 在“数值数据”字段中键入密码。此密码必须与 NetScreen 设备上的 L2TP Tunnel Configuration Secret 字段中的密码相同。

(9) 重新启动运行 Windows 2000 的计算机。

当使用 IPSec 上的 L2TP 时 (它是 Windows 2000 缺省设置)，不需要进行通道认证；所有 L2TP 消息在 IPSec 内部加密和认证。

Keep Alive: 60[6]

4. 因为对等方的 ISP 会动态分配给它一个 IP 地址，所以请在此处输入 **0.0.0.0**。
5. 要找到运行 Windows 2000 的计算机的名称，请执行以下步骤：单击**开始 > 设置 > 控制面板 > 系统**。出现“系统特性”对话框。单击**网络标识**选项卡，并查看**完整的计算机名称**后面的条目。
6. 激活值是在 NetScreen 设备向 LAC 发送 L2TP hello 信号前静止的秒数。

6. 路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

7. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), Any

NAT: Off

Service: ANY

Action: Tunnel

Tunnel L2TP: sales_corp

Position at Top: (选择)

CLI

1. 拨号用户

```
set user adam type l2tp
set user adam password AJbioJ15
unset user adam type auth[7]

set user betty type l2tp
set user betty password BviPsoJ1
unset user betty type auth

set user carol type l2tp
set user carol password Cs10kdD3
unset user carol type auth
```

2. L2TP 用户组

```
set user-group fs location local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

3. 缺省 L2TP 设置

```
set ippool global 10.10.2.100 10.10.2.180
set l2tp default ippool global
set l2tp default auth server Local
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

7. 自动为用户定义密码可将该用户分类为 auth 用户。所以，要将用户类型严格地定义为 L2TP，就必须撤消该 auth 用户类型。

4. L2TP 通道

```
set l2tp sales_corp outgoing-interface ethernet3
set l2tp sales_corp auth server Local user-group fs
```

5. 路由

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

6. 策略

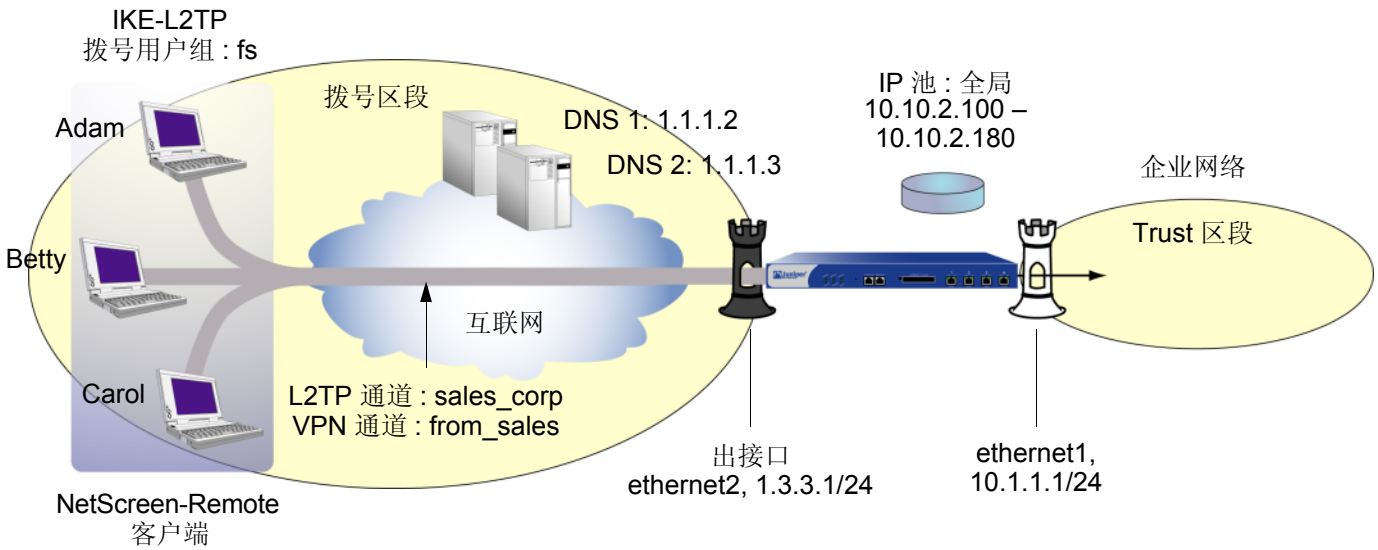
```
set policy top from untrust to trust "Dial-Up VPN" any any tunnel l2tp
    sales_corp
save
```

范例 : 配置 IPSec 上的 L2TP

本范例中使用的 L2TP 通道与上例中 (第 312 页上的 “范例 : 配置 L2TP”) 所创建的 L2TP 通道相同。另外，将一个 IPSec 通道覆盖到 L2TP 通道上以提供加密。IPSec 通道使用之前加载的 RSA 证书、3DES 加密和 SHA-1 认证来协商 Aggressive mode (主动模式) 下的 “阶段 1”。证书授权机构 (CA) 为 Verisign。 (有关获取和加载证书的信息，请参阅第 2 章，第 23 页上的 “公开密钥密码术”。) “阶段 2”协商使用为 “阶段 2”提议预定义的安全级别 “Compatible”。 IPSec 通道处于传送模式。

预定义的 Trust 区段和用户定义的 “拨号”区段都在 trust-vr 路由选择域中。用于 “拨号”和 Trust 区段的接口分别为 ethernet2 (1.3.3.1/24) 和 ethernet1 (10.1.1.1/24)。 Trust 区段处于 NAT 模式。

拨号用户 Adam、Betty 和 Carol 使用 Windows 2000 操作系统上的 NetScreen-Remote 客户端[8]。拨号用户 Adam 的 NetScreen-Remote 配置也包括在下面。 (其他两位拨号用户的 NetScreen-Remote 配置与 Adam 的相同。)



8. 要为 (没有 NetScreen-Remote 的) Windows 2000 配置 IPSec 上的 L2TP 通道，第 1 阶段协商必须处于 Main mode (主模式) 下，且 IKE ID 类型必须为 ASN1-DN。

WebUI

1. 用户定义的区段

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

Zone Name: Dialup

Virtual Router Name: trust-vr

Zone Type: Layer 3 (选择)

Block Intra-Zone Traffic: (选择)

TCP/IP Reassembly for ALG: (清除)

***注意：** Trust 区段预先进行了配置。无需对其进行创建。*

2. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Dialup

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.3.3.1/24

3. IKE/L2TP 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Adam

Status: Enable

IKE User: (选择)

Simple Identity: (选择)[9]

IKE Identity: ajackson@abc.com

L2TP User: (选择)

User Password: AJbioJ15

Confirm Password: AJbioJ15

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Betty

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE Identity: bdavis@abc.com

L2TP User: (选择)

User Password: BviPsoJ1

Confirm Password: BviPsoJ1

9. 输入的 IKE ID 必须与 NetScreen-Remote 客户端发送的相同，它是客户端认证时使用的证书中所显示的电子邮件地址。

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: Carol

Status: Enable

IKE User: (选择)

Simple Identity: (选择)

IKE Identity: cburnet@abc.com

L2TP User: (选择)

User Password: Cs10kdD3

Confirm Password: Cs10kdD3

4. IKE/L2TP 用户组

Objects > User Groups > Local > New: 在 “Group Name” 字段中，键入 **fs**，执行以下操作，然后单击 **OK**:

选择 **Adam**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Betty**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

选择 **Carol**，并使用 **<<** 按钮将其从 Available Members 栏移动到 Group Members 栏中。

5. IP 池

Objects > IP Pools > New: 输入以下内容，然后单击 **OK**:

IP Pool Name: global

Start IP: 10.10.2.100

End IP: 10.10.2.180

6. 缺省 L2TP 设置

VPNs > L2TP > Default Settings: 输入以下内容，然后单击 **Apply**:

IP Pool Name: global

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.2

DNS Secondary Server IP: 1.1.1.3

WINS Primary Server IP: 0.0.0.0

WINS Secondary Server IP: 0.0.0.0

7. L2TP 通道

VPNs > L2TP > Tunnel > New: 输入以下内容，然后单击 **OK**:

Name: sales_corp

Dialup Group: (选择), Local Dialup Group - fs

Authentication Server: Local

Outgoing Interface: ethernet2

Peer IP: 0.0.0.0[10]

Host Name (optional): 如果要将 L2TP 通道限定到某台特定的主机，请输入充当 LAC 的计算机名称[11]。

Secret (optional): 输入一个在 LAC 和 LNS 之间共享的机密[12]

注意：*通常可以忽略主机名称和机密设置。建议只有高级用户才可使用这些设置。*

Keep Alive: 60[13]

10. 因为对等方的 IP 地址是动态的，所以请在此处输入 **0.0.0.0**。
11. 要找到运行 Windows 2000 的计算机的名称，请执行以下步骤：单击**开始 > 设置 > 控制面板 > 系统**。出现“系统特性”对话框。单击**网络标识**选项卡，并查看**完整的计算机名称**后面的条目。
12. 要将一个机密添加到 LAC 以认证 L2TP 通道，必须修改 Windows 2000 的注册表。请参阅上一范例中的注意事项。
13. 激活值是在 NetScreen 设备向 LAC 发送 L2TP hello 信号前静止的秒数。

8. VPN 通道

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

Gateway Name: field

Security Level: Custom

Remote Gateway Type:

Dialup User Group: (选择), Group: fs

Outgoing Interface: ethernet2

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

Security Level: User Defined: Custom

Phase 1 Proposal: rsa-g2-3des-sha

Mode (Initiator): Aggressive[14]

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

Name: from_sales

Security Level: Compatible

Remote Gateway: Predefined: field

> 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

Transport Mode: (选择)

14. Windows 2000 (没有 NetScreen-Remote) 仅支持 Main mode (主模式) 协商。

9. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Tunnel

Tunnel VPN: from_sales

Modify matching bidirectional VPN policy: (清除)

L2TP: sales_corp

Position at Top: (选择)

CLI

1. 用户定义的区段

```
set zone name dialup
set zone dialup vrouter trust-vr
set zone dialup block
```

2. 接口

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

set interface ethernet2 zone dialup
set interface ethernet2 ip 1.3.3.1/24
```

3. L2TP/IKE 用户

```
set user adam type ike l2tp
set user adam password AJbioJ15
unset user adam type auth
set user adam ike-id u-fqdn ajackson@abc.com

set user betty type ike l2tp
set user betty password BviPsoJ1
unset user betty type auth
set user betty ike-id u-fqdn bdavis@abc.com

set user carol type ike l2tp
set user carol password Cs10kdD3
unset user carol type auth
set user carol ike-id u-fqdn cburnet@abc.com
```

4. IKE/L2TP 用户组

```
set user-group fs location Local
set user-group fs user adam
set user-group fs user betty
set user-group fs user carol
```

5. IP 池

```
set ippool global 10.10.2.100 10.10.2.180
```

6. 缺省 L2TP 设置

```
set l2tp default ippool global
set l2tp default ppp-auth chap
set l2tp default dns1 1.1.1.2
set l2tp default dns2 1.1.1.3
```

7. L2TP 通道

```
set l2tp sales_corp outgoing-interface ethernet2
set l2tp sales_corp auth server Local user-group fs
```

8. VPN 通道

```
set ike gateway field dialup fs aggressive[15] outgoing-interface ethernet2
    proposal rsa-g2-3des-sha
set ike gateway field cert peer-ca1[16]
set ike gateway field cert peer-cert-type x509-sig
set vpn from_sales gateway field transport sec-level compatible
```

9. 策略

```
set policy top from dialup to trust "Dial-Up VPN" any any tunnel vpn from_sales
    l2tp sales_corp
save
```

15. Windows 2000 (没有 NetScreen-Remote) 仅支持 Main mode (主模式) 协商。

16. 数字 1 为 CA ID 号。要获取 CA 的 ID 号，请使用以下命令 : **get pki x509 list ca-cert**。

NetScreen-Remote 安全策略编辑器 (Adam[17])

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

   Connection Security: Secure

   Remote Party ID Type: IP Address

   IP Address: 1.3.3.1

   Protocol: UDP

   Port: L2TP

   Connect using Secure Gateway Tunnel: (清除)
4. 单击位于 AJ 图标左边的加号，展开连接策略。
5. 单击 **My Identity**，并配置以下设置：

   从 “Select Certificate” 下拉列表中，选择其中含有在 NetScreen 设备上被指定为用户 IKE ID 的电子邮件地址的证书

   ID Type: E-mail Address[18]

   Port: L2TP
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
7. 单击 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。

17. 要为 Betty 和 Carol 的 NetScreen-Remote 客户端配置 IPSec 上的 L2TP 通道，请按照与此处针对 Adam 所介绍的配置过程相同的步骤执行操作。
18. 证书中的电子邮件地址将自动出现在标识符字段中。

8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法 :

   Authentication Method: Pre-Shared Key

   (或)

   Authentication Method: RSA Signatures

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2

9. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :

   Encapsulation Protocol (ESP): (选择)

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Transport

10. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Transport

11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Transport

12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Transport

13. 单击 **File > Save Changes**。
14. 还需使用 “网络连接向导” 为 Windows 2000 操作系统设置网络连接。

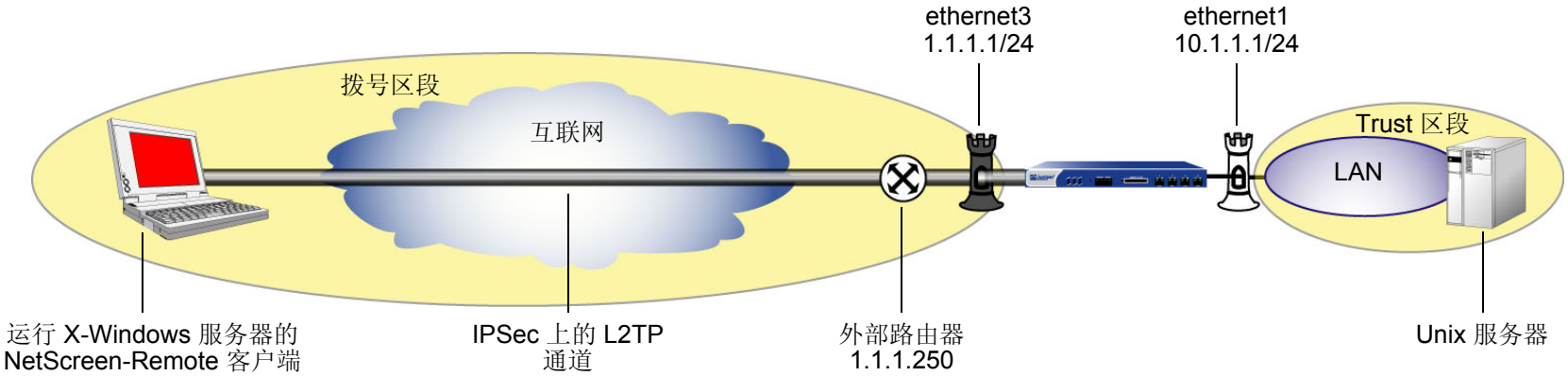
注意 : *配置 “网络连接向导” 时，必须输入一个目标主机名或 IP 地址。输入 1.3.3.1。以后在启动连接时，会提示输入用户名和密码，请输入 adam， AJbioJ15。有关详细信息，请参阅 Microsoft Windows 2000 文档。*

范例：双向的 IPSec 上的 L2TP

在本例中， ethernet1 (10.1.1.1/24) 是 Trust 区段接口且处于 NAT 模式，而 ethernet3 (1.1.1.1/24) 是 Untrust 区段接口。在 NetScreen-Remote 拨号用户与企业 LAN 之间创建 IPSec 上的 L2TP 通道。远程用户正在运行要求双向策略的 X-Windows 应用程序。

为名为 *VPN_dial* 的拨号 “自动密钥 IKE” VPN 通道 (其归 IKE ID 为 *jf@ns.com.* 的 IKE 用户 *dialup-j* 所有) 以及名为 tun1 的 L2TP 通道配置内向和外向策略。 IKE 用户从 Untrust 区段启用到 NetScreen 设备的 IPSec 连接，以访问 Trust 区段中的企业服务器。此时，仅允许 L2TP 通信。L2TP/PPP 协商后，即可建立 L2TP 通道。配置双向策略后，可从通道的任一端发起信息流。

拨号用户 *dialup-j* 使用 Windows 2000 操作系统上的 NetScreen-Remote 客户端[19]。拨号用户 *dialup-j* 的 NetScreen-Remote 配置将在本例之后进行介绍。



19. 要为 (没有 NetScreen-Remote 的) Windows 2000 配置 IPSec 上的 L2TP 通道，第 1 阶段协商必须处于 Main mode (主模式) 下，且 IKE ID 类型必须为 ASN1-DN。

WebUI

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: trust_net

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Trust

3. L2TP/IKE 用户

Objects > Users > Local > New: 输入以下内容，然后单击 **OK**:

User Name: dialup-j

Status: Enable

IKE User: (选择)

Simple Identity: (选择)[20]

IKE Identity: jf@ns.com

Authentication User: (选择)

L2TP User: (选择)

User Password: abc123

Confirm Password: abc123

4. L2TP

VPNs > L2TP > Tunnel > New: 输入以下内容，然后单击 **OK**:

Name: tun1

Use Default Settings: (选择)

Secret: netscreen

Keepalive: 60

20. 输入的 IKE ID 必须与 NetScreen-Remote 客户端发送的相同，它是客户端认证时使用的证书中所显示的电子邮件地址。

5. VPN

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

Gateway Name: dialup1

Security Level: (选择); Standard

Remote Gateway Type: Dialup User; (选择), dialup-j

Preshared Key: n3TsCr33N

Outgoing Interface: (选择) ethernet3

> Advanced: 输入以下内容，然后单击 **Return**，返回基本 AutoKey IKE Gateway 配置页 :

Mode (Initiator): Aggressive

Enable NAT-Traversal: (选择)

UDP Checksum: (选择)

Keepalive Frequency: 5

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

VPN Name: VPN_dial

Remote Gateway: Predefined: (选择), dialup1

> Advanced: 输入以下内容，然后单击 **Return**，返回基本 AutoKey IKE 配置页 :

Security Level: Standard (选择)

Transport Mode (仅对于 IPSec 上的 L2TP): (选择)

6. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

7. 策略

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

Source Address:

Address Book Entry: (选择), Dial-Up VPN

Destination Address:

Address Book Entry: (选择), trust_net

Service: ANY

Action: Tunnel

Tunnel VPN: VPN_dial

Modify matching bidirectional VPN policy: (选择)

L2TP: (选择) tun1

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

Source Address:

Address Book Entry: (选择), trust_net

Destination Address:

Address Book Entry: (选择), Dial-Up VPN

Service: ANY

Action: Tunnel

Tunnel VPN: VPN_dial

Modify matching bidirectional VPN policy: (选择)

L2TP: tun1

CLI

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
```

2. 地址

```
set address trust trust_net 10.1.1.0/24
```

3. L2TP/IKE 用户

```
set user dialup-j ike-id u-fqdn jf@ns.com
set user dialup-j type auth ike l2tp
set user dialup-j password abc123
```

4. L2TP

```
set l2tp tun1 outgoing-interface ethernet3 secret "netscreen" keepalive 60
```

5. VPN

```
set ike gateway dialup1 dialup "dialup-j" aggressive outgoing-interface
    ethernet3 preshare n3TsCr33N sec-level standard
set ike gateway dialup1 nat-traversal udp-checksum
set ike gateway dialup1 nat-traversal keepalive-frequency 5
set vpn VPN_dial gateway dialup1 no-replay transport idletime 0 sec-level
    standard
```

6. 路由

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

7. 策略

```
set policy from untrust to trust “Dial-Up VPN” “trust_net” any tunnel vpn
    VPN_dial tun1
set policy from trust to untrust trust_net “Dial-Up VPN” any tunnel vpn
    VPN_dial l2tp tun1
save
```

NetScreen-Remote 安全策略编辑器 (对于用户 dialup-j)

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

   Connection Security: Secure

   Remote Party ID Type: IP Address

   IP Address: 1.1.1.1

   Protocol: UDP

   Port: L2TP

   Connect using Secure Gateway Tunnel: (清除)
4. 单击 dialup-j 图标左侧的加号，展开连接策略。
5. 单击 **My Identity**，并配置以下设置 :

   从 “Select Certificate” 下拉列表中，选择其中含有在 NetScreen 设备上被指定为用户 IKE ID 的电子邮件地址的证书

   ID Type: E-mail Address[21]

   Port: L2TP
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
7. 单击 Security Policy 图标左边的加号，然后单击 Authentication (Phase 1) 和 Key Exchange (Phase 2) 左边的加号，进一步展开策略。

21. 证书中的电子邮件地址将自动出现在标识符字段中。

8. 单击 **Authentication (Phase 1)** > **Proposal 1**: 选择以下认证方法和算法 :

   Authentication Method: Pre-Shared Key

   (或)

   Authentication Method: RSA Signatures

   Hash Alg: SHA-1

   Key Group: Diffie-Hellman Group 2[22]

9. 单击 **Key Exchange (Phase 2)** > **Proposal 1**: 选择以下 IPSec 协议 :

   Encapsulation Protocol (ESP): (选择)

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Transport

10. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: Triple DES

    Hash Alg: MD5

    Encapsulation: Transport

11. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: SHA-1

    Encapsulation: Transport

22. 在 NetScreen 设备 (DF 组 1、 2 或 5) 上启用 “完全正向保密” (PFS) 时，必须同时为 NetScreen-Remote 下的 VPN 客户端启用它。

12. 单击 **Key Exchange (Phase 2)** > **Create New Proposal**: 选择以下 IPSec 协议 :

    Encapsulation Protocol (ESP): (选择)

    Encrypt Alg: DES

    Hash Alg: MD5

    Encapsulation: Transport

13. 单击 **File > Save Changes**。

还需使用 “网络连接向导” 为 Windows 2000 操作系统设置网络连接。

注意：*配置 “网络连接向导” 时，必须输入一个目标主机名或 IP 地址。输入 1.1.1.1。以后在启动连接时，会提示输入用户名和密码，请输入 dialup-j, abc123。有关详细信息，请参阅 Microsoft Windows 2000 文档。*

7

高级 VPN 功能

本章内容介绍 VPN 技术的下列更高级用途：

NAT 穿透

“网络地址转换” (NAT) 和 “网络地址端口转换” (NAPT) 为互联网标准，它允许局域网 (LAN) 将一组 IP 地址用于内部信息流，将第二组地址用于外部信息流。 NAT 设备从预定义的 IP 地址池中生成这些外部地址。

在设置 IPSec 通道时，沿着数据路径出现 NAT 设备不影响 “阶段 1” 和 “阶段 2” 的 IKE 协商，它通常将 IKE 数据包封装在 “用户数据包协议 (UDP)” 片段中。但是，在完成 “阶段 2” 协商后，对 IPSec 数据包执行 NAT 会导致通道失败。在 NAT 导致 IPSec 发生中断的众多原因中[1]，其中之一在于对 “封装安全性协议 (ESP)” 而言， NAT 设备不能识别端口转换的 “第 4 层” 包头的位置 (因为它已被加密)。对于 “认证包头” (AH) 协议， NAT 设备可以修改端口号，但不能修改认证检查，因而会导致对整个 IPSec 数据包的认证检查失败。

要解决这些问题，NetScreen 设备和 NetScreen-Remote 客户端 (6.0 版或更高[2]) 可应用 NAT 穿透 (NAT-T) 功能。在 “阶段 1” 交换过程中，当 NAT-T 沿数据路径检测完一个或多个 NAT 设备后，将为 IPSec 数据包添加一层 UDP 封装，如 IETF 草案 *draft-ietf-ipsec-nat-t-ike-00.txt* 和 *draft-ietf-ipsec-udp-encaps-00.txt* 及更高版本中所规定。

如果 NAT 设备同时是 IKE/IPSec 感知设备，则当其试图处理 IKE 端口号为 500 或 IPSec 协议号为 50 (对于 ESP) 和 51 (对于 AH) 的数据包时会产生其它问题。为了避免此类 IKE 数据包中间处理，上文提及的 IETF 草案版本 2 建议将 IKE 的 UDP 端口号从 500 变换 (或浮动) 为 4500。为了避免 IPSec 数据包的中间处理，草案 0 和 2 都将在外部 IP 包头与 ESP 或 AH 包头之间插入一个 UDP 包头，从而使得 Protocol 字段中的值从 50 或 51 (分别对于 ESP 或 AH 而言) 变为 17 (对于 UDP)。此外，插入的 UDP 包头也使用端口 4500。 ScreenOS 的当前版本支持基于 *draft-ietf-ipsec-nat-t-ike-02.txt* 和 *draft-ietf-ipsec-udp-encaps-02.txt* 及这些草案的版本 0 所述的 NAT-T。

***注意：** NetScreen 不支持 “手动密钥” 通道的 NAT-T，也不支持使用 AH 的 IPSec 信息流。 NetScreen 仅支持使用 ESP 的 “自动密钥” IKE 通道的 NAT-T。*

1. 有关 IPSec/NAT 不兼容性列表，请参阅 Bernard Aboba 所撰写的 *draft-ietf-ipsec-nat-regts-00.txt*。
2. NetScreen-Remote 6 和 7 支持 NAT-T，如 *draft-ietf-ipsec-nat-t-ike-00.txt* 和 *draft-ietf-ipsec-udp-encaps-00.txt* 中所述。NetScreen-Remote 8.2 支持草案 02。

探查 NAT

为了核对 VPN 通道的两端是否都支持 NAT-T， NetScreen 会在 “阶段 1” 协商的前两次交换过程中在供应商 ID 负荷中发送两个 MD-5 散列，一个散列用于草案 0 的标题，另一个用于草案 2 的标题 :

- “4485152d 18b6bbcd 0be8a846 9579ddcc” — 是 “draft-ietf-ipsec-nat-t-ike-00” 的一个 MD-5 散列
- “90cb8091 3ebb696e 086381b5 ec427b1f” — 是 “draft-ietf-ipsec-nat-t-ike-02” 的一个 MD-5 散列

两个对等方都必须至少发送和接收一次供应商负荷 ID 中的这些值， NAT-T 探查才能继续进行。如果它们为两个草案都发送了散列，则 NetScreen 将对草案 2 使用 NAT-T 实现方案。

如果每个端点的设备都支持 NAT-T，它们将在第三次和第四次 “阶段 1” 交换 [Main mode (主模式)] 或第二次和第三次交换 [Aggressive mode (主动模式)] 过程中彼此发送 “NAT 发现 (NAT-D)” 负荷[3]。NAT-D 负荷包含经协商的有关下列信息的散列 :

- 目标 NAT-D 散列 :
  - 发起方 Cookie (CKY-I)
  - 响应方 Cookie (CKY-R)
  - 远程 (目标) IKE 对等方 IP 地址
  - 目标端口号
- 源 NAT-D 散列 (一个或多个[4]):
  - 发起方 Cookie (CKY-I)
  - 响应方 Cookie (CKY-R)
  - 本地 (源) IKE 对等方 IP 地址
  - 源端口号

3. “NAT 发现 (NAT-D)” 负荷是新引入的用于 NAT-T 的 IKE 负荷类型。 NAT-D 负荷类型编号为 0130。有关其它 IKE 负荷类型的列表，请参阅第 15 页上的 “IKE 数据包”。

4. 对于未指定出接口的具有多个接口和实现方案的设备而言， NAT-T 支持多个源 NAT-D 散列。

当各个对等方将接收的散列与发送的散列进行比较时，它们能够确定两个散列间是否发生了地址转换。通过判断哪个数据包已被修改也可指示 NAT 设备的位置：

如果	匹配	则
本地对等方的目标散列	至少为远程对等方源散列之一	未发生地址转换。
至少为本地对等方源散列之一	远程对等方的目标散列	未发生地址转换。

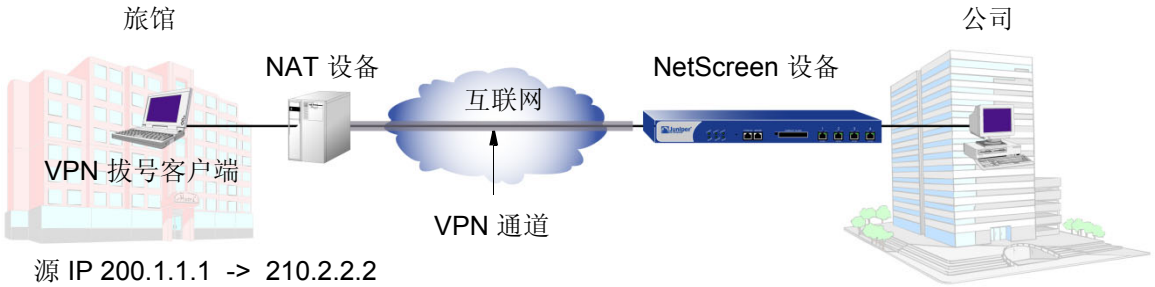
如果	不匹配	则
本地对等方的目标散列	至少为远程对等方源散列之一	NAT 设备在远程对等方之前。
至少为本地对等方源散列之一	远程对等方的目标散列	NAT 设备在本地对等方之前。

了解 NAT 设备的位置至关重要，因为 IKE 激活必须由 NAT 设备后面的对等方发起。请参阅第 351 页上的 “激活数据包”。

如果两个对等方都支持 IETF 草案 2，则当其在 “阶段 1” 协商期间检测到彼此之间存在 NAT 设备时，它们也会将 IKE 端口号从 500 浮动为 4500。在 Main mode (主模式) 下，端口号将在 “阶段 1” 的第五次和第六次交换过程中浮动为 4500，随后在 “阶段 2” 的所有交换过程中都保持此值。在 Aggressive mode (主动模式) 下，端口号将在 “阶段 1” 的第三次和最后一次交换过程中浮动为 4500，随后在 “阶段 2” 的所有交换过程中都保持此值。对于所有后继信息流，对等方也将使用 4500 作为 UDP 端口号。

穿透 NAT 设备

在以下图例中，某旅馆 LAN 周围的 NAT 设备将接收一个来自 VPN 拨号客户端的数据包，其 IP 地址为 2.1.1.5 (由旅馆指定)。对于所有出站信息流， NAT 设备都将用新地址 2.2.2.2 替换外部包头中的初始源 IP 地址。在 “阶段 1” 协商过程中， VPN 客户端和 NetScreen 设备将检测是否 VPN 参与双方都支持 NAT-T、 NAT 设备是否沿数据路径出现以及它是否位于 VPN 客户端之前。

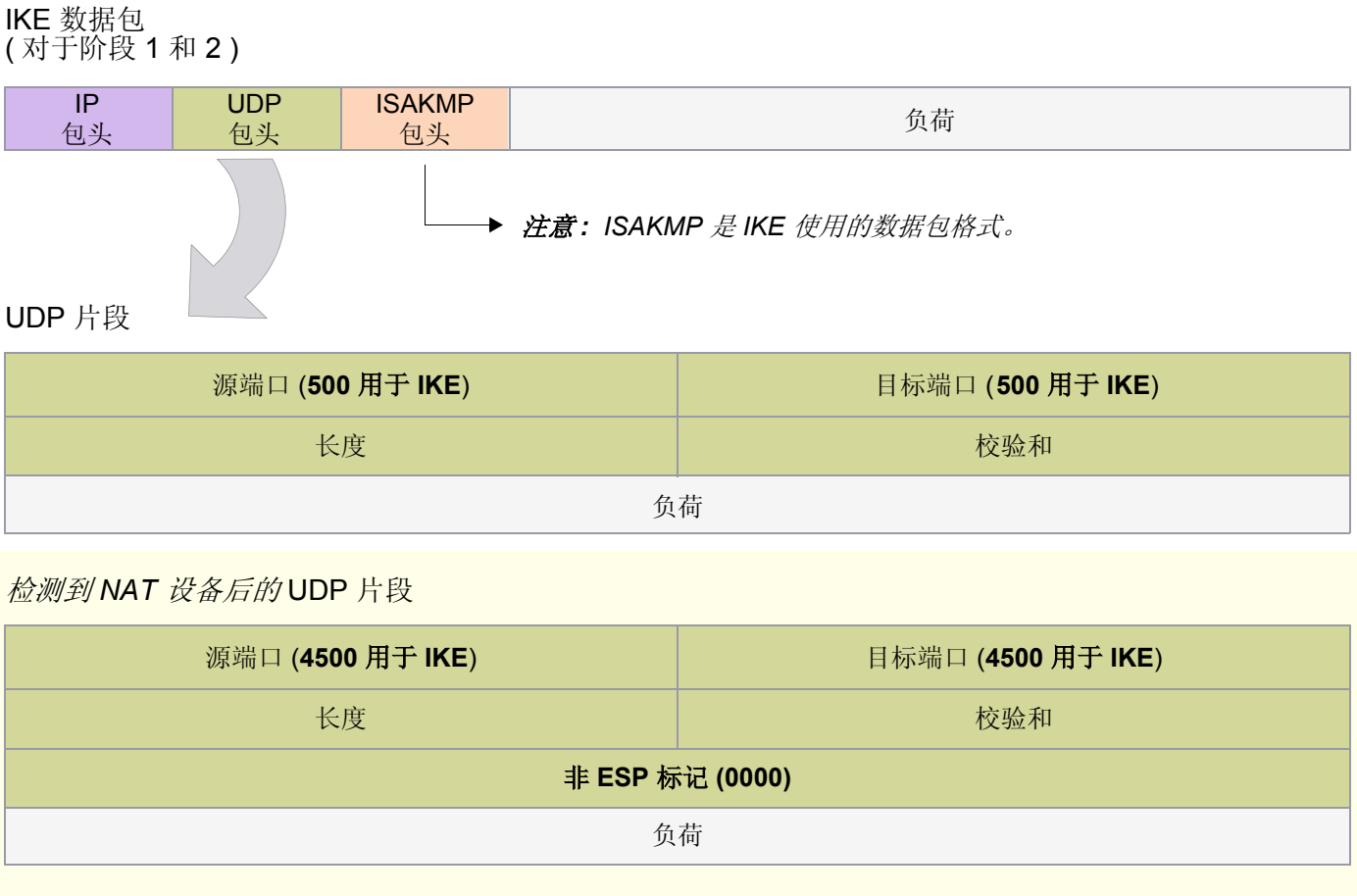


将 IPSec 数据包封装在 UDP 数据包中 (VPN 客户端和 NetScreen 设备都会执行) 可以解决认证检查失败问题。NAT 设备将其作为 UDP 数据包处理，只更改 UDP 包头中的源端口而不修改 AH 或 ESP 包头中的 SPI。VPN 参与者将剥开 UDP 层来处理 IPSec 数据包，这样处理可以通过认证检查，因为对认证过的内容并未做任何更改。

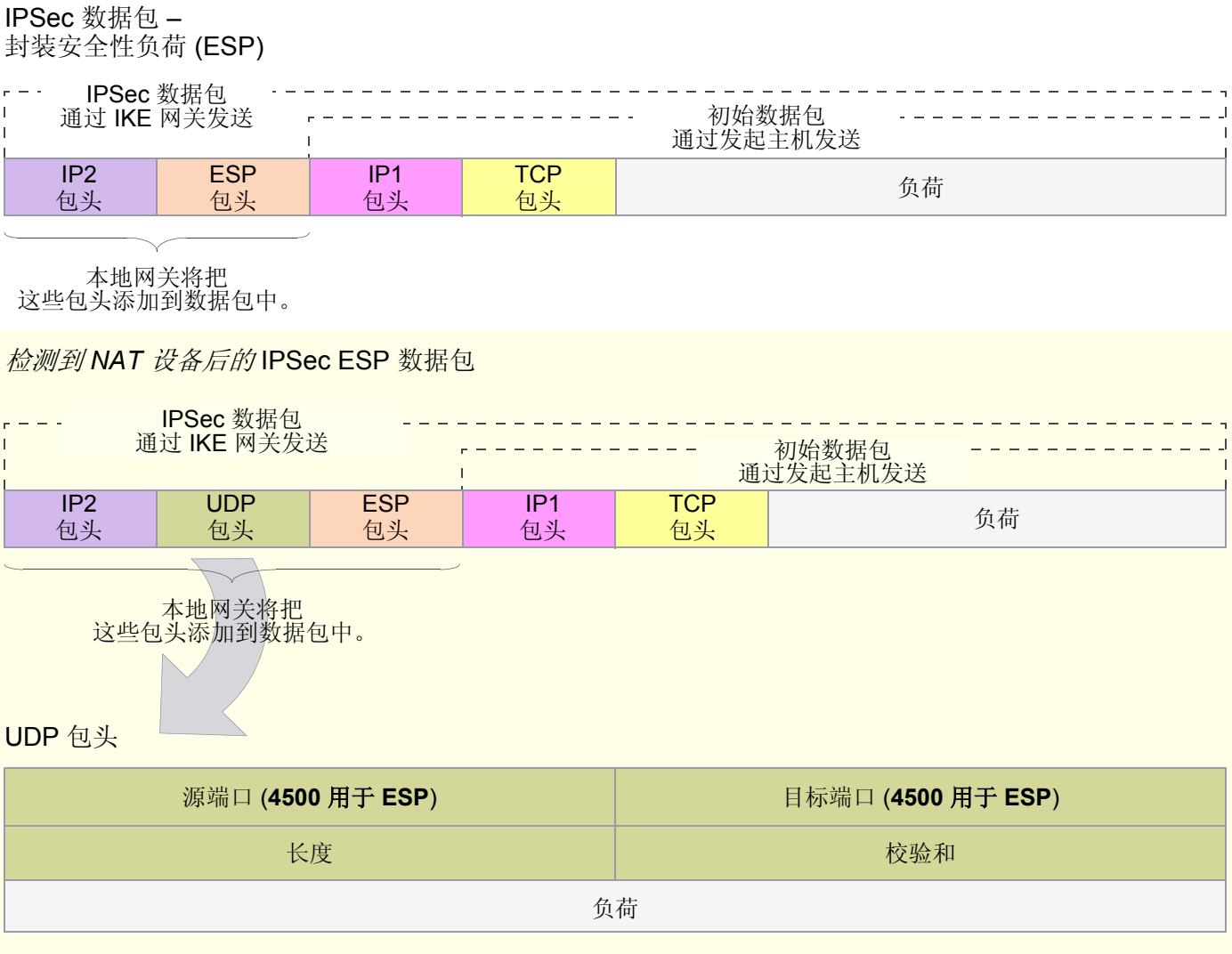
如果 NAT 设备是 IKE/IPSec 感知设备，则可能会出现其它问题。IKE/IPSec 感知 NAT 设备可能试图处理 IKE/IPSec 信息流而不是转发它。为防止此类中间处理， NAT-T (v2) 将把 IKE 源和目标 UDP 端口号从 500 变为 4500。NAT-T 还将在 UDP 包头的负荷之前插入一个非 ESP 标记。对于 IPSec 信息流，NAT-T (v0 和 v2) 将在外部 IP 包头和 ESP 包头之间插入一个 UDP 包头。 UDP 数据包也将使用 4500 作为源和目标端口号。

如上所述， NAT-T (v2) 将在封装有 ISAKMP 数据包的 UDP 片段包头和负荷之间添加一个非 ESP 标记。非 ESP 标记由 4 个字节的 0 构成 (0000)，它将被添加到 UDP 片段以区分封装的 ISAKMP 数据包与无此标记的封装 ESP 数据包。如果没有非 ESP 标记，接受方将无法确认封装的数据包是 ISAKMP 数据包还是 ESP 数据包，因为对这两种类型 UDP 包头均使用 4500。使用此标记可指出所封装数据包的正确类型，以便接收方能够正确地多路分离它。

如下图所示，在数据路径中检测到 NAT 设备后， IKE 数据包中 UDP 包头的源和目标端口号将从 500 变为 4500。并且， VPN 通道端点将在 UDP 包头和负荷之间插入一个非 ESP 标记以区分封装的 ISAKMP 数据包和 ESP 数据包。接收方可使用此标记来区分封装的 ISAKMP 数据包和 ESP 数据包并正确地多路分离它。



如下图所示，在数据路径中检测到 NAT 设备后，VPN 通道端点将在外部 IP 包头和 IPSec 数据包的 ESP 包头之间插入一个附加的 UDP 包头。由于没有非 ESP 标记，接收方可区分封装的 ESP 数据包和 ISAKMP 数据包并正确地多路分离 ESP 数据包。



UDP 校验和

所有 UDP 数据包都包含一个 UDP 校验和、一个用来确保 UDP 数据包没有传输错误的计算值。NetScreen 设备不要求对 NAT-T 使用 UDP 校验和，因此，WebUI 和 CLI 将校验和作为可选设置。即使如此，某些 NAT 设备仍要求校验和，所以您可能必须启用或禁用此设置。缺省情况下，当您启用 NAT-T 时也将同时包括 UDP 校验和。

WebUI

VPNs > AutoKey Advanced > Gateway > New: 输入在第 4 章，第 99 页上的 “站点到站点 VPN”或第 5 章，第 229 页上的 “拨号 VPN”中所述的新通道网关的必要参数，输入以下内容，然后单击 **OK**:

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

启用 NAT 穿透 : (选择)

UDP Checksum: Enable

CLI

```
set ike gateway name nat-traversal udp-checksum
unset ike gateway name nat-traversal udp-checksum
```

激活数据包

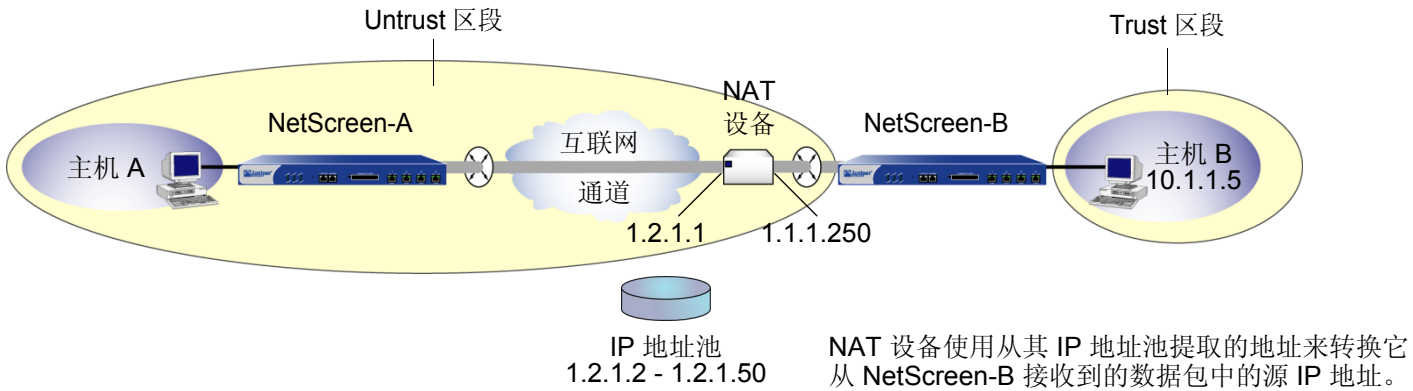
当 NAT 设备将 IP 地址分配给主机时，NAT 设备将确定在没有信息流发生时这个新地址可以保持有效的期限。例如，NAT 设备可能会使任何已生成但连续 20 秒未使用的 IP 地址无效。因此，IPSec 参与者通常需要通过 NAT 设备发送定期激活数据包 (空的 UDP 数据包)，以便在 “阶段 1”和 “阶段 2”的 SA 过期前无需更改 NAT 映射。

注意：*NAT 设备的会话超时间隔可能会随制造商和型号的不同而异。确定 NAT 设备的间隔以及在该间隔内设置激活频率值非常重要。*

发起方 / 响应方对称

当两个 NetScreen 设备在没有 NAT 设备的情况下建立通道时，任一设备都可作为发起方或响应方。但是，如果其中一个主机在 NAT 设备之后，则此类发起方 / 响应方可能无法对称。当 NAT 设备动态生成 IP 地址时会出现这种情况。

注意：*以下描述的安全区段是通过 NetScreen-B 观察所得。*



在上图中， NetScreen-B 驻留在 NAT 设备后面的子网中。如果 NAT 设备为从 NetScreen-B 中接收到的数据包生成新的源 IP 地址 (从 IP 地址池中动态提取)， NetScreen-A 将无法明确地识别出 NetScreen-B。因此， NetScreen-A 不能成功地发起与 NetScreen-B 之间的通道。 NetScreen-A 必须是响应方， NetScreen-B 必须是发起方，双方必须在 Aggressive mode (主动模式) 下执行 “阶段 1” 协商。

但是，如果 NAT 设备使用映射 IP 地址 (MIP) 或其它一对一寻址方法生成新 IP 地址， NetScreen-A 则可以明确识别出 NetScreen-B。因此， NetScreen-A 或 NetScreen-B 都可以是发起方，而且双方都可以使用 “阶段 1” 的 Main mode (主模式) 或 Aggressive mode (主动模式) 。

注意：*如果在充当响应方的 NetScreen 设备上启用 NAT-T 并对其进行配置，以便在 Main mode (主模式) 下执行 IKE 协商，则该设备及其以下类型的所有对等方 (在相同出接口上配置) 都必须使用相同的 “阶段 1” 提议 (彼此以相同顺序出现)。*

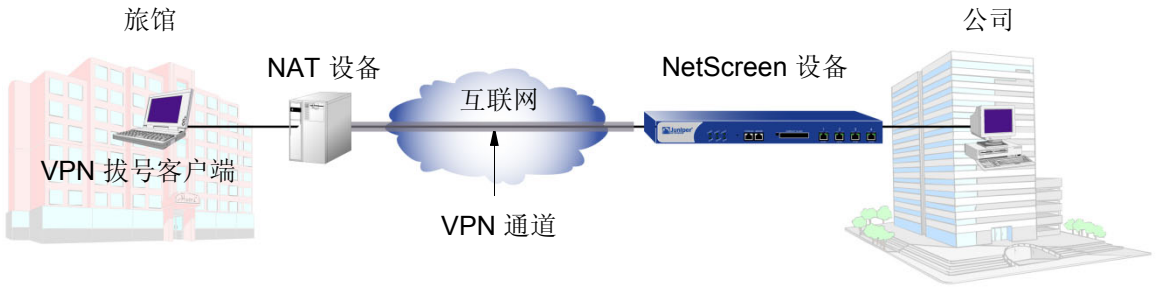
- *动态对等方 (具有动态分配 IP 地址的对等方)*
- *拨号 VPN 用户*
- *NAT 设备后面具有静态 IP 地址的对等方*

由于在最后两条消息之前，在 Main mode (主模式) 下与 “阶段 1” 协商时不可能知道对等方身份，因此 “阶段 1” 提议必须完全相同 IKE 协商才能够继续。

在相同出接口上为上述某一对等方类型在 Main mode (主模式) 下配置 IKE 时，NetScreen 设备将自动检查 “阶段 1” 的所有提议是否都相同以及顺序是否相同。如果提议不同，则 NetScreen 设备会生成一条错误消息。

范例 : 启用 NAT 穿透

在以下示例中，某旅馆 LAN 周围的 NAT 设备将把一个地址分配给由 Michael Smith (参加会议的销售员) 使用的 VPN 拨号客户端。要想通过拨号 VPN 通道接入公司的 LAN，Michael Smith 必须启用 NAT-T，以用于在 NetScreen 设备上配置的远程网关 “msmith” 以及在 VPN 拨号客户端配置的远程网关。您还必须使 NetScreen 设备在传输中包括 UDP 校验和并将激活频率设置为 8 秒。



WebUI

VPNs > AutoKey Advanced > Gateway > New: 输入在第 4 章，第 100 页上的 “站点到站点 VPN 配置”或第 5 章，第 230 页上的 “拨号 VPN”中所述的新通道网关的必要参数，输入以下内容，然后单击 **OK**:

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

启用 NAT 穿透 : (选择)

UDP Checksum: Enable

Keepalive Frequency: 8 Seconds (0~300 Sec)

注意：*通过 CLI 配置拨号 VPN 时， NetScreen 设备将自动启用 “NAT 穿透”。*

CLI

```
set ike gateway msmith nat-traversal
set ike gateway msmith nat-traversal udp-checksum
set ike gateway msmith nat-traversal keepalive-frequency 8
save
```

VPN 监控

为特定通道启用 VPN 监控时，NetScreen 设备将在指定时间间隔 (可按秒配置) 内通过通道发送 ICMP 回应请求 (或“pings”)，以监控通过通道的网络连接性能。[5] 如果 ping 动作指出 VPN 监控状态已改变，则 NetScreen 设备将触发以下“简单网络管理协议” (SNMP) 陷阱之一 :

- **连接转为中断 :** 通道的 VPN 监控处于连接状态时会发生此陷阱，但指定数目的连续 ICMP 回应请求并不引起回复，并且没有其它任何内向 VPN 信息流。[6] 然后，状态更改为中断。
- **中断转为连接 :** 如果通道的 VPN 监控处于中断状态，而 ICMP 回应请求引起单个响应，则状态更改为连接。仅当 ICMP 回应请求通过通道引起回复时禁用了重定密钥选项并且“阶段 2” SA 仍处于活动状态时，中断才会转为连接陷阱。

注意 : *有关 VPN 监控提供的 SNMP 数据的详细信息，请参阅**第 373 页上的 “SNMP VPN 监控对象和陷阱”**。*

可按每个 VPN 对象来应用 VPN 监控，而不必必须按每个 VPN 通道来应用。VPN 对象是通过 **set vpn** 命令或相应的 WebUI 命令定义的。定义了一个 VPN 对象后，接下来即可在一个或多个策略中引用它 (创建基于策略的 VPN)。由于 ScreenOS 从 VPN 对象及其它策略参数中得到基于策略的 VPN 通道，因此单个 VPN 对象可以是多个 VPN 通道中的一个元素。由于在未启用优化的情况下，Juniper Networks 建议对 IPSec VPN 通道应用 VPN 监控时的通道数量不要超过 100，因此了解 VPN 对象与 VPN 通道之间的区别非常重要。如果确定启用了优化，则对能够应用 VPN 监控的 VPN 通道数量无任何限制。要了解有关优化选项的信息，请参阅第 356 页上的 “重定密钥和优化选项”。

注意 : *VPN 监控优化以单个对象为基础运行。可对所有 VPN 对象启用它，也可以只对部分启用或对所有均不启用。*

5. 要更改 ping 时间间隔，可使用以下 CLI 命令 : **set vpnmonitor interval** *number*。缺省值为 10 秒。
6. 要更改连续的未成功 ICMP 回应请求数临界值，可使用以下 CLI 命令 : **set vpnmonitor threshold** *number*。缺省值为 10 个连续请求。

重定密钥和优化选项

如果启用重定密钥选项，则 NetScreen 设备将在完成通道配置后立即开始发送 ICMP 回应请求，并一直发送下去。回应请求将触发启动 IKE 协商来建立 VPN 通道，直到通道的 VPN 监控处于连接状态。然后 NetScreen 设备使用 ping 进行 VPN 监控。如果通道的 VPN 监控状态从连接变为中断，则 NetScreen 设备将为对等方禁用 “阶段 2” 安全联盟 (SA)。 NetScreen 设备按定义的时间间隔继续向其对等方发送回应请求，触发重新启动 IKE “阶段 2” 协商 (必要时启动 “阶段 1” 协商) 的尝试，直到成功为止。此时， NetScreen 设备将重新激活 “阶段 2” SA、生成新密钥并重新建立通道。在事件日志中会出现一条消息，声明已成功完成重定密钥操作[7]。

可使用重定密钥选项来确保 “自动密钥 IKE” 通道始终处于连接状态，以监控远程站点的设备，或使动态路由协议能够知道远程站点的路由并通过通道传送消息。应用带有重定密钥选项的 VPN 监控的另一个用途是，在多个 VPN 通道绑定到单个通道接口的情况下自动填充下一跳跃通道绑定表 (NHTB 表) 和路由表。有关最后一个用途的范例，请参阅第 374 页上的 “每个通道接口多个通道”。

如果禁用重定密钥选项，仅当使用用户生成的信息流激活通道时， NetScreen 设备才会执行 VPN 监控。

7. 如果 NetScreen 设备是一个 DHCP 客户端，则不同地址的 DHCP 更新会使 IKE 重定密钥。但是，同一地址的 DHCP 更新不会引发 IKE 重定密钥操作。

缺省情况下禁用 VPN 监控优化。如果启用它 (**set vpn** *name* **monitor optimized**)，则 VPN 监控行为将更改如下：

- NetScreen 设备将把通过 VPN 通道的内向信息流视为 ICMP 回应回复。如果将内向信息流作为 ICMP 回应回复的替代物，则当通过通道的信息流很大而回应回复未通过时可以减少可能发生的错误警报。
- 如果同时存在通过 VPN 通道的内向和外向信息流，则 NetScreen 设备将彻底抑制 VPN 监控 ping。这样有助于减少网络信息流。

尽管 VPN 监控优化具有某些优点，但是应注意当优化选项激活时， VPN 监控不再提供精确的 SNMP 统计信息，如 VPN 网络延迟时间。另外，如果使用 VPN 监控跟踪通道远程端特定目标 IP 地址的可用性，则优化功能会产生容易造成误解的结果。

源接口和目标地址

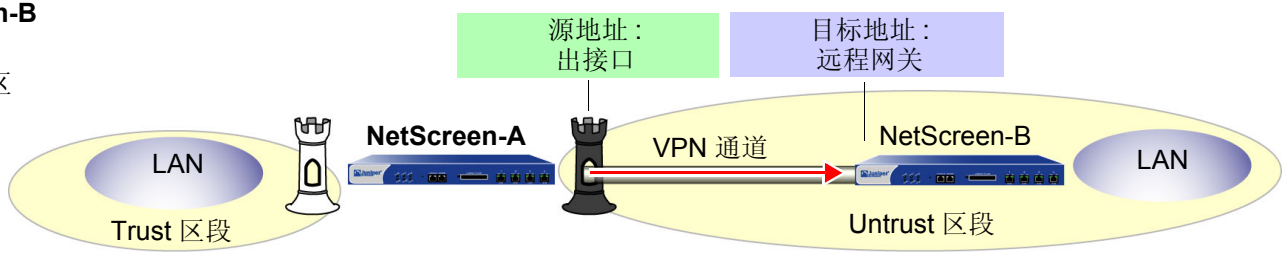
在缺省情况下， VPN 监控功能将本地出接口的 IP 地址用作源地址，将远程网关的 IP 地址用作目标地址。如果远程对等方是拥有内部 IP 地址的 VPN 拨号客户端 (如 NetScreen-Remote)，则 NetScreen 设备会自动检测内部地址并将其用作目标地址。VPN 客户端可以是拥有已分配内部 IP 地址的 XAuth 用户，或拥有内部 IP 地址的拨号 VPN 组的拨号 VPN 用户或成员。也可指定 VPN 监控使用其它源和目标 IP 地址，主要用于当 VPN 通道的另一端为非 NetScreen 设备时为 VPN 监控提供支持。

由于 VPN 监控是在本地和远程站点独立运行的，因此在通道一端的设备上配置的源地址可以不必是在另一端设备上配置的目标地址。实际上，可以在通道的两端或仅在一端启用 VPN 监控。

NetScreen-A –> NetScreen-B

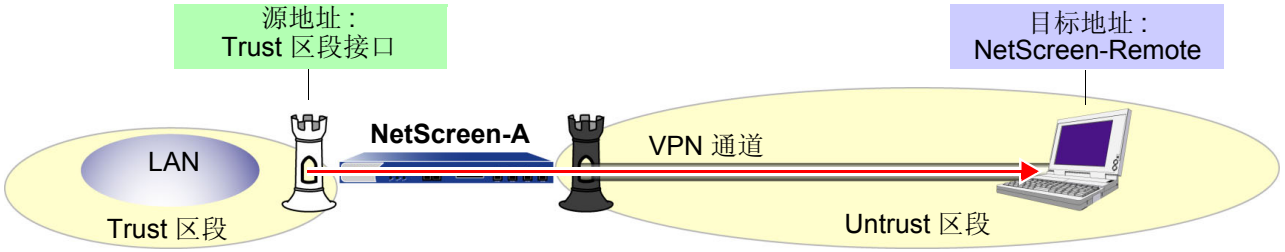
从出接口到远程网关 (即从 NetScreen-A 上的 Untrust 区段接口到 NetScreen-B 上的 Untrust 区段接口) 的 NetScreen-A ping。

(缺省行为)



NetScreen-A –> NetScreen-Remote

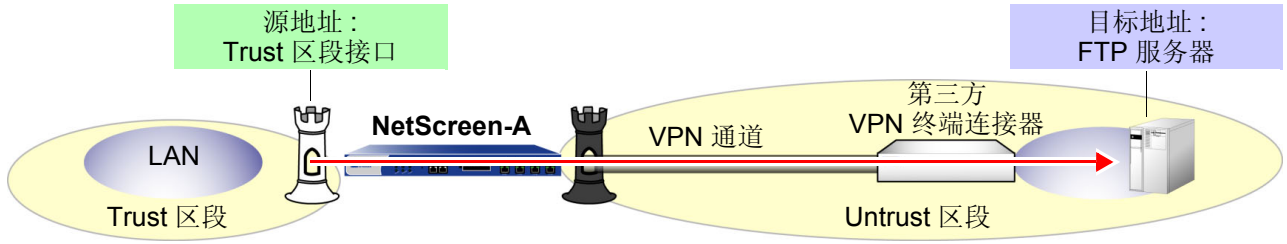
从 Trust 区段接口到 NetScreen-Remote 的 NetScreen-A ping。NetScreen-Remote 需要一个策略，以允许来自远程网关之外地址 (即 NetScreen-A 的 Untrust 区段接口之外) 的入站 ICMP 信息流。



注意 : *NetScreen-A 需要一个策略，以允许从 Trust 到 Untrust 区段的 ping 信息流。*

NetScreen-A –> 第三方 VPN 终端连接器

从 Trust 区段接口到远程网关之外设备的 NetScreen-A ping。如果远程对等方不响应 ping 但支持允许入站 ping 信息流的策略，则此操作可能是必要的。



注意 : *NetScreen-A 需要一个策略，以允许从 Trust 到 Untrust 区段的 ping 信息流。*

注意 : *如果通道的另一端是可通过 XAuth 来接收地址的 NetScreen-Remote VPN 客户端，则在缺省情况下，NetScreen 设备将把 XAuth 分配的 IP 地址用作目标地址进行 VPN 监控。有关 XAuth 的信息，请参阅第* ***8*** *-81 页上的 “XAuth 用户和用户组”。*

策略注意事项

必须在发送设备上创建一个策略，以便在下列情况下允许来自包含源接口区段的 ping 通过 VPN 通道到达包含目标地址的区段：

- 源接口位于与目标地址不同的区段中。
- 源接口与目标地址在相同的区段中，并且启用了内部区段阻塞。

同样，必须在接收设备上创建一个策略，以便在下列情况下允许来自包含源地址区段的 ping 通过 VPN 通道到达包含目标地址的区段：

- 目标地址位于与源地址不同的区段中。
- 目标地址与源地址在相同的区段中，并且启用了内部区段阻塞。

注意：*如果接收设备是不响应 ICMP 回应请求的第三方产品，请将目标更改为可以响应的远程对等方 LAN 中的内部主机。远程对等方的防火墙必须具有允许 ICMP 回应请求通过的策略。*

配置 VPN 监控功能

要启用 VPN 监控，请执行以下操作：

WebUI

VPNs > AutoKey IKE > New: 配置 VPN，单击 **Advanced**，输入下列信息，单击 **Return** 以返回基本 VPN 配置页，然后单击 **OK**:

VPN Monitor: 选择以启用对此 VPN 通道的 VPN 监控。

Source Interface: 从下拉列表中选择接口。如果选择 “default”， NetScreen 设备将使用出接口。

Destination IP: 输入目标 IP 地址。如果不输入任何内容， NetScreen 设备将使用远程网关 IP 地址。

Rekey: 如果希望 NetScreen 设备在通道状态从连接变为中断时尝试 IKE “阶段 2” 协商 (必要时尝试 IKE “阶段 1” 协商)，请选择此选项。选择此选项后， NetScreen 设备将尝试 IKE 协商以建立通道，并在完成配置通道后立即启动 VPN 监控。

如果不希望 NetScreen 设备在通道状态从连接变为中断时尝试 IKE 协商，请清除此选项。禁用重定密钥选项时， VPN 监控将在用户生成的信息流触发 IKE 协商后启动，并在通道状态从连接变为中断时停止。

(或)

VPNs > Manual Key > New: 配置 VPN，单击 **Advanced**，输入下列信息，单击 **Return** 以返回基本 VPN 配置页，然后单击 **OK**:

VPN Monitor: 选择以启用对此 VPN 通道的 VPN 监控。

Source Interface: 从下拉列表中选择接口。如果选择 “default”， NetScreen 设备将使用出接口。

Destination IP: 输入目标 IP 地址。如果不输入任何内容， NetScreen 设备将使用远程网关 IP 地址。

CLI

```
set vpnmonitor frequency number[8]
set vpnmonitor threshold number[9]
set vpn name_str monitor [ source-interface interface[10] [ destination-ip
    ip_addr[11] ] ] [optimized] [ rekey[12] ]
save
```

8. VPN 监控频率以秒为单位。缺省设置间隔为 10 秒。
9. VPN 监控临界值数是指连续的成功或未成功 ICMP 回应请求数，它可确定能否通过 VPN 通道到达远程网关。缺省临界值是 10 个连续的成功 ICMP 回应请求或 10 个连续的未成功 ICMP 回应请求。
10. 如果不选择源接口， NetScreen 设备将使用出接口作为缺省接口。
11. 如果不选择目标 IP 地址， NetScreen 设备将使用远程网关的 IP 地址。
12. 重定密钥选项不适用于 “手动密钥 VPN” 通道。

范例：为 VPN 监控指定源和目标地址

在本例中，将在两台 NetScreen 设备 (NetScreen-A 和 NetScreen-B) 之间配置“自动密钥 IKE VPN”通道。对设备 A，将设置从 Trust 区段接口 (ethernet1) 到 NetScreen-B 上 Trust 区段接口 (10.2.1.1/24) 的 VPN 监控。对 NetScreen-B，将设置从 Trust 区段接口 (ethernet1) 到 NetScreen-A 后面企业内部网服务器 (10.1.1.5) 的 VPN 监控。

NetScreen-A	NetScreen-B
区段和接口	
• ethernet1 - Zone: Trust - IP address: 10.1.1.1/24 - Interface mode: NAT	• ethernet1 - Zone: Trust - IP address: 10.2.1.1/24 - Interface mode: NAT
• ethernet3 - Zone: Untrust - IP address: 1.1.1.1/24	• ethernet3 - Zone: Untrust - IP address: 2.2.2.2/24
基于路由的自动密钥 IKE 通道参数	
• 阶段 1 - Gateway name: gw1 - Gateway static IP address: 2.2.2.2 - Security level: Compatible* - Preshared Key: Ti82g4aX - Outgoing interface: ethernet3 - Mode: Main	• 阶段 1 - Gateway name: gw1 - Gateway static IP address: 1.1.1.1 - Proposals: Compatible - Preshared Key: Ti82g4aX - Outgoing interface: ethernet3 - Mode: Main
• 阶段 2 - VPN tunnel name: vpn1 - Security level: Compatible† - VPN Monitoring: src = ethernet1; dst = 10.2.1.1 - Bound to interface: tunnel.1	• 阶段 2 - VPN tunnel name: vpn1 - Security level: Compatible - VPN Monitoring: src = ethernet1; dst = 10.1.1.5 - Bound to interface: tunnel.1

* Compatible 的“阶段 1”安全级别包括以下提议：pre-g2-3des-sha、pre-g2-3des-md5、pre-g2-des-sha 和 pre-g2-des-md5。

† Compatible 的“阶段 2”安全级别包括以下提议：nopfs-esp-3des-sha、nopfs-esp-3des-md5、nopfs-esp-des-sha 和 nopfs-esp-des-md5。

NetScreen-A	NetScreen-B
路由	
通往 0.0.0.0/0，使用 ethernet3，网关为 1.1.1.250 通往 10.2.1.0/24，使用 tunnel.1，无网关 (Null 路由 – 如果 tunnel.1 中断则将信息流丢弃在 10.2.1.0/24) 通往 10.2.1.0/24，使用 Null 接口，度量值 : 10	通往 0.0.0.0/0，使用 ethernet3，网关为 2.2.2.250 通往 10.1.1.0/24，使用 tunnel.1，无网关 (Null 路由 – 如果 tunnel.1 中断则将信息流丢弃在 10.1.1.0/24) 通往 10.1.1.0/24，使用 Null 接口，度量值 : 10

由于两台设备的 ping 操作都从 Trust 区段的接口到 Untrust 区段的地址，因此 VPN 通道两端的 admin 必须定义策略以允许 ping 在区段间传递。

注意：*由于本例中两个 VPN 终端连接器都是 NetScreen 设备，因此可使用缺省源和目标地址进行 VPN 监控。本例所包括的其它选项用途只是为了说明如何配置 NetScreen 设备以供使用。*

WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Unnumbered: (选择)

Interface: ethernet1(trust-vr)

2. 地址

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

Address Name: Trust_LAN

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: Remote_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.1.0/24

Zone: Untrust

3. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (选择)

Gateway Name: gw1

Type:

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

Preshared Key: Ti82g4aX

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：

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.1.1.0/24

Remote IP / Netmask: 10.2.1.0/24

Service: ANY

VPN Monitor: (选择)

Source Interface: ethernet1

Destination IP: 10.2.1.1

Rekey: (清除)

4. 路由

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:
Network Address/Netmask: 0.0.0.0/0
Gateway: (选择)
Interface: ethernet3
Gateway IP Address: 1.1.1.250

Network > Routing > Routing Entries > trust-vr New: 输入以下内容，然后单击 **OK**:
Network Address/Netmask: 10.2.1.0/24
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: 10.2.1.0/24
Gateway: (选择)
Interface: Null
Gateway IP Address: 0.0.0.0
Metric: 10

5. 策略

Policies > (From: Trust, To: Untrust) New: 输入以下内容，然后单击 **OK**:
Source Address:
Address Book Entry: (选择), Trust_LAN
Destination Address:
Address Book Entry: (选择), Remote_LAN
Service: ANY
Action: Permit
Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), Remote_LAN

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: Any

Action: Permit

Position at Top: (选择)

WebUI (NetScreen-B)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Trust (trust-vr)

Unnumbered: (选择)

Interface: ethernet1(trust-vr)

2. 地址

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

Address Name: Trust_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.1.0/24

Zone: Trust

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

Address Name: Remote_LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway:

Create a Simple Gateway: (选择)

Gateway Name: gw1

Type:

Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: Ti82g4aX

Security Level: Compatible

Outgoing Interface: ethernet3

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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 10.2.1.0/24

Remote IP / Netmask: 10.1.1.0/24

Service: ANY

VPN Monitor: (选择)

Source Interface: ethernet1

Destination IP: 10.1.1.5

Rekey: (清除)

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address / Netmask: 10.1.1.0/24

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: 10.1.1.0/24

Gateway: (选择)

Interface: Null

Gateway IP Address: 0.0.0.0

Metric: 10

5. 策略

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

Source Address:

Address Book Entry: (选择), Trust_LAN

Destination Address:

Address Book Entry: (选择), Remote_LAN

Service: ANY

Action: Permit

Position at Top: (选择)

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

Source Address:

Address Book Entry: (选择), Remote_LAN

Destination Address:

Address Book Entry: (选择), Trust_LAN

Service: Any

Action: Permit

Position at Top: (选择)

CLI (NetScreen-A)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet1 nat
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone trust
set interface tunnel.1 ip unnumbered interface ethernet1
```

2. 地址

```
set address trust Trust_LAN 10.1.1.0/24
set address untrust Remote_LAN 10.2.1.0/24
```

3. VPN

```
set ike gateway gw1 address 2.2.2.2 main outgoing-interface ethernet3 preshare
    Ti82g4aX 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 10.1.1.0/24 remote-ip 10.2.1.0/24 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.2.1.1
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.2.1.0/24 interface tunnel.1
set vrouter trust-vr route 10.2.1.0/24 interface null metric 10
```

5. 策略

```
set policy top from trust to untrust Trust_LAN Remote_LAN any permit
set policy top from untrust to trust Remote_LAN Trust_LAN any permit
save
```

CLI (NetScreen-B)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.2.1.1/24
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 trust Trust_LAN 10.2.1.0/24
set address untrust Remote_LAN 10.1.1.0/24
```

3. VPN

```
set ike gateway gw1 address 1.1.1.1 main outgoing-interface ethernet3 preshare
    Ti82g4aX 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 10.2.1.0/24 remote-ip 10.1.1.0/24 any
set vpn vpn1 monitor source-interface ethernet1 destination-ip 10.1.1.5
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
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 10
```

5. 策略

```
set policy top from trust to untrust Trust_LAN Remote_LAN any permit
set policy top from untrust to trust Remote_LAN Trust_LAN any permit
save
```

SNMP VPN 监控对象和陷阱

ScreenOS 可以使用 “简单网络管理协议” (SNMP) VPN 监控对象和陷阱来确定活动 VPN 的状态和条件。 VPN 监控 MIB 时，将记录每个 ICMP 回应请求是否引发回复、连续的平均成功回复、回复等待时间以及最后 30 次尝试的平均回复等待时间。

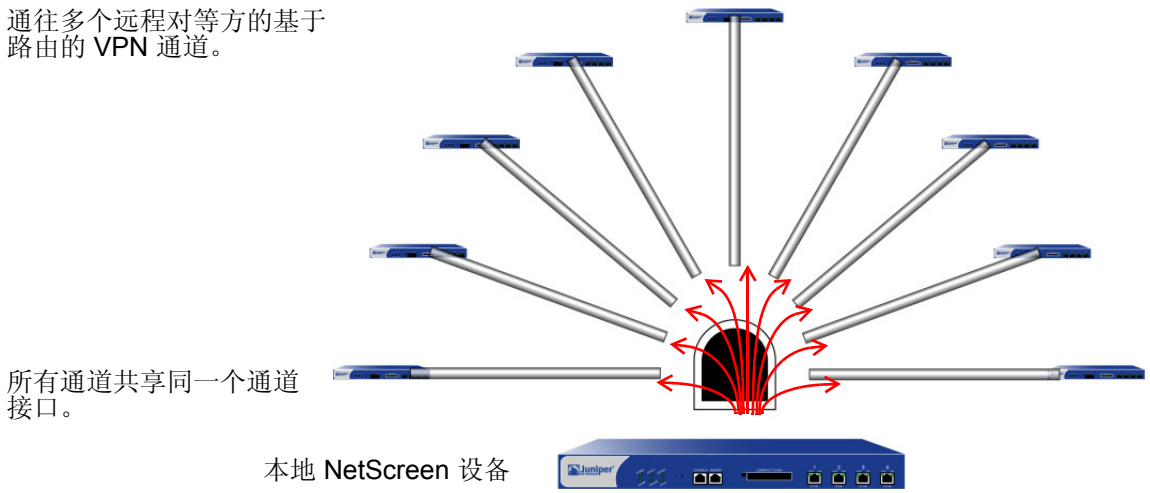
***注意：**为使 SNMP 管理器应用程序能够识别 VPN 监控 MIB (管理信息库)，必须将 NetScreen 专用的 MIB 扩展文件导入到应用程序中。可在随 NetScreen 设备发运的 NetScreen 文档 CD 中找到 MIB 扩展文件。*

在 “自动密钥 IKE” 或 “手动密钥 VPN” 通道中启用 VPN 监控功能后， NetScreen 设备将激活其 SNMP VPN 监控对象，其中包含以下数据 :

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

每个通道接口多个通道

可将多个 IPSec VPN 通道绑定到单个通道接口。要将特定目标链接到绑定到同一通道接口的多个 VPN 通道中的某个通道， NetScreen 设备需要使用两个表 : 路由表和下一跳跃通道绑定 (NHTB) 表。 NetScreen 设备将路由表条目中指定的下一跳跃网关 IP 地址映射到 NHTB 表中指定的特定 VPN 通道。利用此技术，单个通道接口可支持多个 VPN 通道。 (请参阅第 375 页上的 “路由到通道的映射”。)



对于通过单个通道接口发送到路由表或 VPN 通道容量最多可支持的 VPN 通道 (取数量较少者) 的 VPN 信息流， NetScreen 设备可对其进行分类。

VPN 通道的最大数量不是由可创建的通道接口数来限制，而是由路由表容量或专用 VPN 通道所允许的最大数量来限制 (取数量较少者)。例如，如果 NetScreen 设备支持 4000 个路由和 1000 个专用 VPN 通道，则可创建 1000 个 VPN 通道并将其绑定到单个通道接口。如果 NetScreen 设备支持 8192 个路由和 10,000 个专用 VPN 通道，则可创建 8000 多个 VPN 通道并将其绑定到单个通道接口[13]。要查看 NetScreen 设备的最大路由容量和通道容量，请参阅相关的产品数据表。

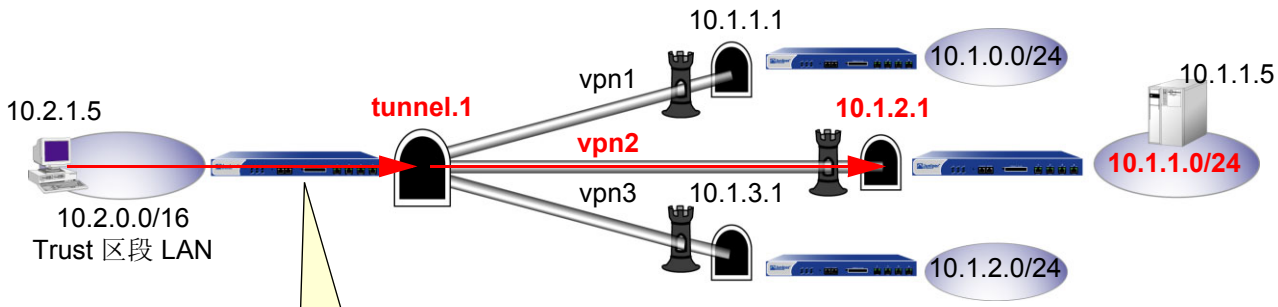
13. 如果路由表容量是限制因素，则必须减去由安全区段接口自动生成的路由及其它所有静态路由 (如通往缺省网关的路由)，这些路由可能需要通过基于路由的 VPN 通道总数来定义。

路由到通道的映射

要对绑定到相同通道接口的多个 VPN 通道中的信息流进行分类，NetScreen 设备将把在路由中指定的下一跳跃网关 IP 地址映射到特定的 VPN 通道名称。路由表条目到 NHTB 表条目的映射关系如下所示。在下图中，本地 NetScreen 设备先后通过 tunnel.1 接口和 vpn2 将从 10.2.1.5 发送到 10.1.1.5 的信息流进行了路由。

本地 NetScreen 设备，具有多个绑定到 tunnel.1 接口的通道

远程 VPN 对等方 (具有动态分配的外部 IP 地址和固定的通道接口 IP 地址) 及其受保护的 LAN



路由表

ID	IP 前缀 (Dst)	接口	网关
1	10.1.0.0/24	tunnel.1	**10.1.1.1**
2	**10.1.1.0/24**	**tunnel.1**	**10.1.2.1**
3	10.1.2.0/24	tunnel.1	**10.1.3.1**

下一跳跃通道绑定表

下一跳跃	VPN	标志
10.1.1.1	vpn1	static
10.1.2.1	**vpn2**	static
10.1.3.1	vpn3	static

可采用动态路由协议 [如边界网关协议 (BGP)] 来自动传送路由表，也可手动输入这些路由。网关的 IP 地址是远程对等方站点的通道接口地址。

在 “阶段 2” 协商过程中，两个 IKE 对等方将交换通道接口地址，并自动输入这些 “下一跳跃到通道” 绑定。另外，也可手动输入这些绑定。下一跳跃 IP 地址是远程对等方的通道接口 IP 地址。

在上述条目中，路由表中网关的 IP 地址 (也是 NHTB 表中下一跳跃 IP 地址) 是远程对等方站点的通道接口。此 IP 地址将把路由 (进而将路由中指定的通道接口) 链接到目的地为指定 IP 前缀的信息流的特定 VPN 通道。

NetScreen 设备将远程对等方的通道接口 IP 地址用作网关和下一跳跃 IP 地址。可手动输入路由，也可通过动态路由协议输入，该路由将把对等方的通道接口 IP 地址自动引用为路由表中的网关。同时还必须在 NHTB 表中输入与下一跳跃相同的 IP 地址及相应 VPN 通道名称。它们也有两种选择 : 可手动输入或者在“阶段 2”协商期间使 NetScreen 设备从远程对等方获取并自动输入。

NetScreen 设备将路由表条目中的网关 IP 地址和 NHTB 表条目中的下一跳跃 IP 地址用作通用元素，并将通道接口与相应的 VPN 通道相链接。然后， NetScreen 设备即可用 NHTB 表中指定的正确 VPN 通道来引导目的地为路由中指定的 IP 前缀的信息流。

远程对等方的地址

对所有通过基于路由的 VPN 而到达的远程对等方而言，其内部寻址方案彼此必须唯一。要实现此目的，一种方法是使每个远程对等方都执行源和目标地址的网络地址转换 (NAT)。此外，通道接口 IP 地址在所有远程对等方中也必须唯一。如果要与大量远程站点相连，则使用寻址方案是必要的。以下是针对最多 1000 个 VPN 通道的一个可能寻址方案 :

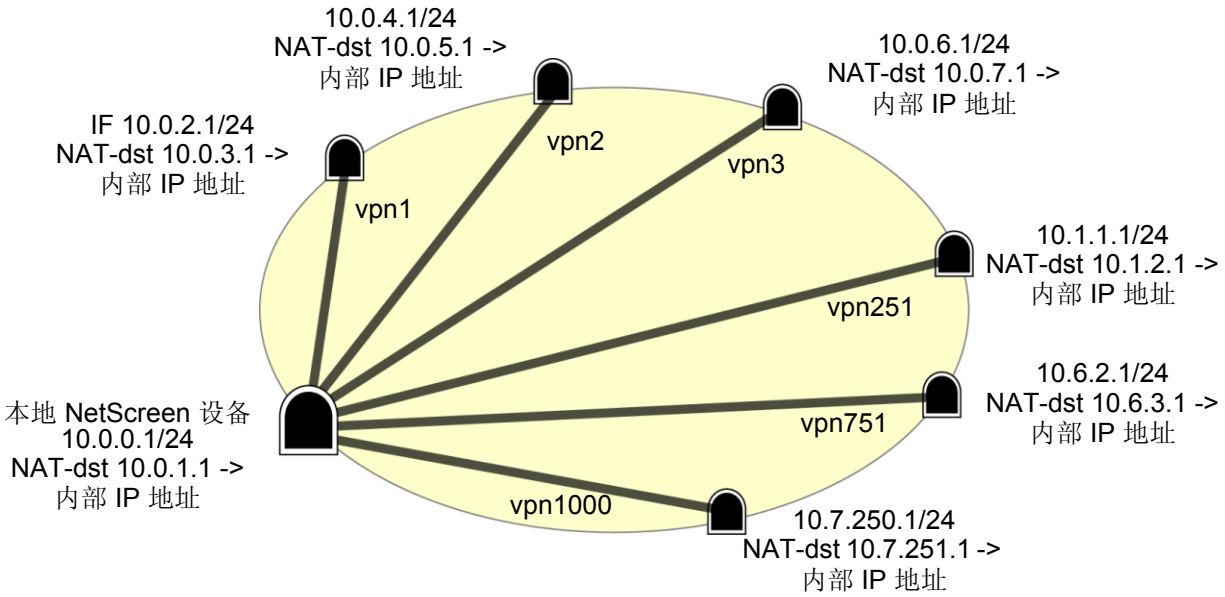
本地路由表中的目标	本地通道接口	网关 / 下一跳跃 (对等方的通道接口)	VPN 通道
10.0.3.0/24	tunnel.1	10.0.2.1/24	vpn1
10.0.5.0/24	tunnel.1	10.0.4.1/24	vpn2
10.0.7.0/24	tunnel.1	10.0.6.1/24	vpn3
…	…	…	…
10.0.251.0/24	tunnel.1	10.0.250.1/24	vpn125
10.1.3.0/24	tunnel.1	10.1.2.1/24	vpn126
10.1.5.0/24	tunnel.1	10.1.4.1/24	vpn127
10.1.7.0/24	tunnel.1	10.1.6.1/24	vpn128
…	…	…	…
10.1.251.0/24	tunnel.1	10.1.250.1/24	vpn250

本地路由表中的目标	本地通道接口	网关 / 下一跳跃 (对等方的通道接口)	VPN 通道
10.2.3.0/24	tunnel.1	10.2.2.1/24	vpn251
…	…	…	…
10.2.251.0/24	tunnel.1	10.2.250.1/24	vpn375
…	…	…	…
10.7.3.0/24	tunnel.1	10.7.2.1/24	vpn876
…	…	…	…
10.7.251.0/24	tunnel.1	10.7.250.1/24	vpn1000

本地 NetScreen 设备上的通道接口 10.0.0.1/24。在所有远程主机上，都存在具有 IP 地址的通道接口，该地址显示为本地路由表和 NHTB 表中的网关 / 下一跳跃 IP 地址。

有关说明绑定到具有地址转换的单个通道接口的多通道范例，请参阅第 381 页上的 “范例 : 重叠子网的一个通道接口上的多个 VPN”。

本地 NetScreen 设备及其所有对等方都对入站 VPN 信息流执行具有 IP 变换的 NAT-dst，对出站 VPN 信息流执行来自具有端口转换的出口通道接口 IP 地址的 NAT-src。有关 NAT-src 和 NAT-dst 的详细信息，请参阅第 7 卷，“地址转换”。



手动和自动表条目

可在 NHTB 和路由表中手动创建条目。也可自动填充 NHTB 和路由表。对于绑定到单个通道接口的少数通道，手动方法比较好。对于大量通道，自动方法可以减少管理设置和维护工作，因为当通道或接口在中心站点的通道接口上不可用时，路由会动态自我调整。

手动表条目

可将 VPN 通道手动映射到下一跳跃通道绑定 (NHTB) 表中远程对等方通道接口的 IP 地址。首先，必须联系远程 admin 以获悉用于该通道端通道接口的 IP 地址。然后，可使用以下命令将该地址与 NHTB 表中的 VPN 通道名称相关联：

set interface tunnel.1 nhtb *peer's_tunnel_interface_addr* **vpn** *name_str*

此后，可在路由表中输入静态路由，路由表将把该通道接口 IP 地址用作网关。可通过 WebUI 或以下 CLI 命令输入路由：

set vrouter *name-str* **route** *dst_addr* **interface tunnel.1 gateway** *peer's_tunnel_interface_addr*

自动表条目

要自动填充 NHTB 和路由表，必须满足以下条件：

- 所有绑定到单个本地通道接口的 VPN 通道的远程对等方必须是运行 ScreenOS 5.0.0 的 NetScreen 设备。
- 每个远程对等方必须将其通道绑定到通道接口，并且该接口在所有对等方通道接口地址中必须具有唯一的 IP 地址。
- 在每个 VPN 通道的两端，启用带有重定密钥选项的 VPN 监控或启用各个远程网关的 IKE 心跳信号重新连接选项[14]。
- 本地和远程对等方必须拥有在连接通道接口时启用的动态路由协议[15] 的实例。

利用带有重定密钥选项的 VPN 监控，通道两端的 NetScreen 设备无需等待用户发起 VPN 信息流[16] 即可建立通道。在 VPN 通道两端启用带有重定密钥选项的 VPN 监控后，两台 NetScreen 设备将执行 “阶段 1” 和 “阶段 2” IKE 协商以建立通道。(有关详细信息，请参阅第 355 页上的 “VPN 监控”。)

在 “阶段 2” 协商期间， NetScreen 设备会互相交换通道接口 IP 地址。然后，每个 IKE 模块都可在 NHTB 表中自动输入通道接口 IP 地址及相应的 VPN 通道名称。

14. 在通道接口上运行动态路由协议时，即使不启用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控，由协议生成的信息流也会触发 IKE 协商。但 Juniper Networks 仍建议不要依赖动态路由信息流来触发 IKE 协商。应使用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控。

15. 对于 “开放式最短路径优先 (OSPF)”，在本地对等方的通道接口上启用路由协议之前，必须将该接口配置为 “点对多点” 接口。

16. 对于具有动态分配的外部 IP 地址的远程对等方，或是对具有映射到动态 IP 地址的完全合格域名 (FQDN) 的远程对等方，它们必须首先发起 IKE 协商。但是，由于本地 NetScreen 设备上的 “阶段 2” SA 缓存远程对等方的动态分配 IP 地址，因此任何一个对等方都可以重新发起 IKE 协商，重新建立 VPN 监控状态已从连接变为中断的通道。

要使本地 NetScreen 设备在其路由表中自动输入通往远程目标的路由，必须在本地和远程通道接口上启用 BGP 实例。基本步骤如下：

1. 在虚拟路由器上创建 BGP 路由实例，该路由器包含已绑定多个 VPN 通道的通道接口。
2. 在虚拟路由器上启用路由实例。
3. 在通向 BGP 对等方的通道接口上启用路由实例。

远程对等方也将执行这些步骤。

在本地 (或中心) 设备上，也必须定义通往每个对等方通道接口 IP 地址的缺省路由和静态路由。中心设备需要通往对等方通道接口的静态路由，以便最初能够通过正确的 VPN 通道到达 BGP 邻接设备。

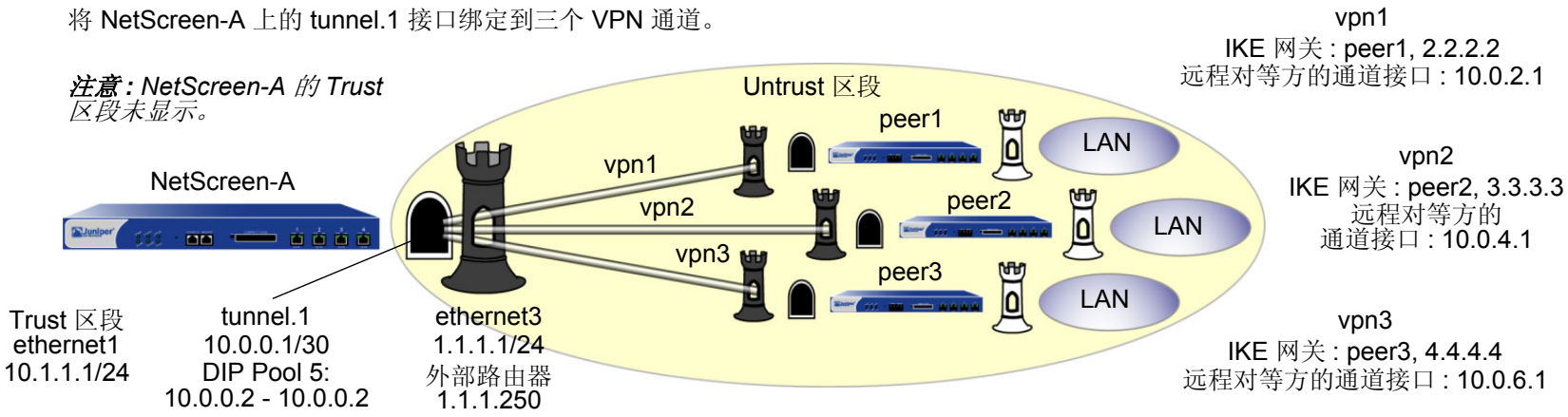
建立通信之后，BGP 邻接设备将交换路由信息，以便能够自动填充其路由表。两个对等方在彼此间建立了 VPN 通道后，远程对等方即可向本地设备发送路由信息或从本地设备接收路由信息。本地 NetScreen 设备上的动态路由实例通过本地通道接口获悉了到对等方的路由后，即可将作为网关的远程对等方通道接口的 IP 地址加入路由。

有关说明绑定到单个通道接口 (其中 “中心” 设备自动填充其 NHTB 和路由表) 的多个通道的范例，请参阅第 413 页上的 “范例 : 自动路由表和 NHTB 表条目”。

范例：重叠子网的一个通道接口上的多个 VPN

在本例中，将把三个基于路由的“自动密钥 IKE VPN”通道 (vpn1、vpn2 和 vpn3) 绑定到单个通道接口 (tunnel.1)。通道从 NetScreen-A 通向三个远程对等方 (对等方 1、对等方 2 和 对等方 3)。在 NetScreen-A 上，为三个对等方手动添加路由表和 NHTB 表条目。

将 NetScreen-A 上的 tunnel.1 接口绑定到三个 VPN 通道。



每个通道两端的 VPN 通道配置对 “阶段 1”和 “阶段 2”提议均使用下列参数：自动密钥 IKE、预共享密钥 (peer1: “netscreen1”、peer2: “netscreen2”、peer3: “netscreen3”) 以及预定义为 “Compatible” 的安全级别。(有关这些提议的详细信息，请参阅第 11 页上的 “通道协商”。)

每台设备上的所有安全区段和接口都在该设备的 trust-vr 虚拟路由选择域中。

本例对每个 LAN 都使用相同的地址空间 (10.1.1.0/24)，以说明如何使用源和目标网络地址转换 (NAT-src 和 NAT-dst) 来解决 IPSec 对等方之间的寻址冲突。有关 NAT-src 和 NAT-dst 的详细信息，请参阅第 7 卷，“地址转换”。

WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.0.0.1/30

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

ID: 5

IP Address Range: (选择), 10.0.0.2 ~ 10.0.0.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

2. 地址

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

Address Name: corp

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: oda1

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.1.0/24

Zone: Trust

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

Address Name: peers

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.0.0/16

Zone: Untrust

3. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: peer1

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

Preshared Key: netscreen1

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：

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

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

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: peer2

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

Preshared Key: netscreen2

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：

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

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

VPN Name: vpn3

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: peer3

Type: Static IP: (选择), Address/Hostname: 4.4.4.4

Preshared Key: netscreen3

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 :

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

Network Address / Netmask: 10.0.1.0/24

Gateway: (选择)

Interface: ethernet1

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: 10.0.3.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.2.1

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

Network Address / Netmask: 10.0.2.2/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.2.1

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

Network Address / Netmask: 10.0.5.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.4.1

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

Network Address / Netmask: 10.0.4.2/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.4.1

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

Network Address / Netmask: 10.0.7.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.6.1

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

Network Address / Netmask: 10.0.6.2/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 10.0.6.1

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

Network Address / Netmask: 10.0.0.0/16

Gateway: (选择)

Interface: null

Gateway IP Address: 0.0.0.0

Metric: 10

Network > Interfaces > Edit (对于 tunnel.1) > NHTB > New: 输入以下内容，然后单击 **Add**:

New Next Hop Entry:

IP Address: 10.0.2.1

VPN: vpn1

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

New Next Hop Entry:

IP Address: 10.0.4.1

VPN: vpn2

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

New Next Hop Entry:

IP Address: 10.0.6.1

VPN: vpn3

5. 策略

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

Source Address:

Address Book: (选择), corp

Destination Address:

Address Book: (选择), peers

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP On: 5 (10.0.0.2–10.0.0.2)/X-late

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

Source Address:

Address Book Entry: (选择), peers

Destination Address:

Address Book Entry: (选择), oda1

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.1.1.0 - 10.1.1.254

CLI (NetScreen-A)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
set interface tunnel.1 dip 5 10.0.0.2 10.0.0.2
```

2. 地址

```
set address trust corp 10.1.1.0/24
set address trust oda1 10.0.1.0/24
set address untrust peers 10.0.0.0/16
```

3. VPN

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 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 ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set ike gateway peer3 address 4.4.4.4 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway peer3 sec-level compatible
set vpn vpn3 bind interface tunnel.1
set vpn vpn3 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

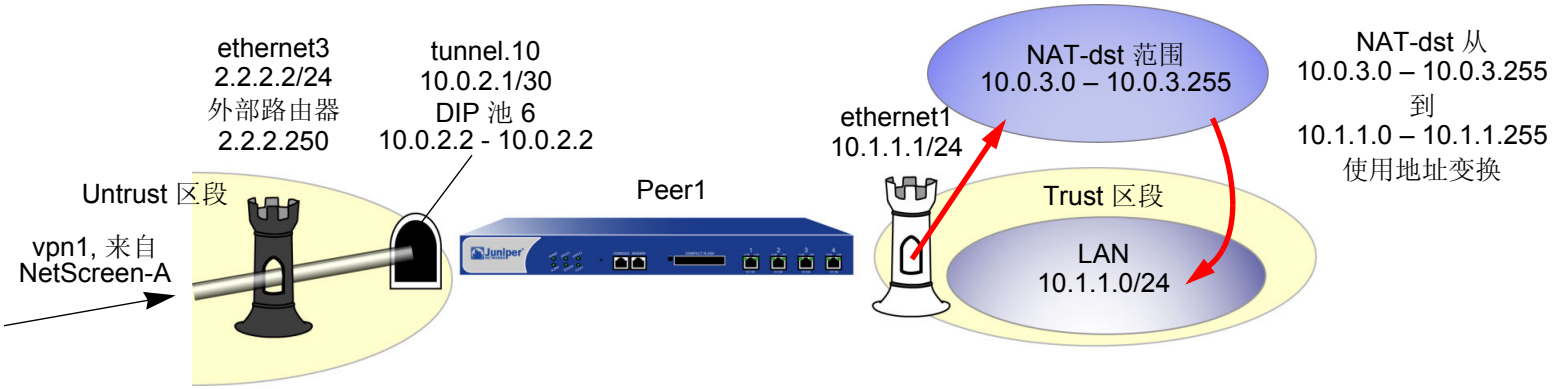
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 10.0.1.0/24 interface ethernet1
set vrouter trust-vr route 10.0.3.0/24 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.2.2/32 interface tunnel.1 gateway 10.0.2.1
set vrouter trust-vr route 10.0.5.0/24 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.4.2/32 interface tunnel.1 gateway 10.0.4.1
set vrouter trust-vr route 10.0.7.0/24 interface tunnel.1 gateway 10.0.6.1
set vrouter trust-vr route 10.0.6.2/32 interface tunnel.1 gateway 10.0.6.1
set vrouter trust-vr route 10.0.0.0/16 interface null metric 10
set interface tunnel.1 nhtb 10.0.2.1 vpn vpn1
set interface tunnel.1 nhtb 10.0.4.1 vpn vpn2
set interface tunnel.1 nhtb 10.0.6.1 vpn vpn3
```

5. 策略

```
set policy from trust to untrust corp peers any nat src dip-id 5 permit
set policy from untrust to trust peers oda1 any nat dst ip 10.1.1.0 10.1.1.254
    permit
save
```

Peer1

以下配置是创建到企业站点 NetScreen-A 的 VPN 通道时， NetScreen 设备的远程 admin 在 peer1 站点中必须输入的内容。由于内部地址与企业 LAN 的地址均位于地址空间 10.1.1.0/24 内，因此远程 admin 需要配置 NetScreen 设备以执行源和目标 NAT (NAT-src 和 NAT-dst)。 Peer1 通过 VPN1 将信息流发送到 NetScreen-A 时，使用 DIP 池 6 来执行 NAT-src 以将所有内部源地址转换为 10.0.2.2。 Peer1 将对从 NetScreen-A 发来的 VPN 信息流执行 NAT-dst，使用生效的地址变换将地址从 10.0.3.0/24 转换为 10.1.1.0/24。



***注意：**有关 NAT-src 和 NAT-dst 的详细信息，请参阅第 7 卷，“地址转换”。*

WebUI (Peer1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.10

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.0.2.1/30

Network > Interfaces > Edit (对于 tunnel.10) > DIP > New: 输入以下内容，然后单击 **OK**:

ID: 6

IP Address Range: (选择), 10.0.2.2 ~ 10.0.2.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

2. 地址

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

Address Name: lan

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: oda2

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.3.0/24

Zone: Trust

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

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.1.0/24

Zone: Untrust

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

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.0.2/32

Zone: Untrust

3. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

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：

Bind to: Tunnel Interface, tunnel.10

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.250

Metric: 1

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

Network Address / Netmask: 10.0.3.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

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

Network Address / Netmask: 10.0.0.0/8

Gateway: (选择)

Interface: tunnel.10

Gateway IP Address: 0.0.0.0

Metric: 10

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

Network Address / Netmask: 10.0.0.0/8

Gateway: (选择)

Interface: null

Gateway IP Address: 0.0.0.0

Metric: 12

5. 策略

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

Source Address:

Address Book Entry: (选择), fr_corp

Destination Address:

Address Book Entry: (选择), oda2

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.1.1.0 - 10.1.1.254

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

Source Address:

Address Book Entry: (选择), lan

Destination Address:

Address Book Entry: (选择), to_corp

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP On: 6 (10.0.2.2–10.0.2.2)/X-late

CLI (Peer1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.2/24
set interface tunnel.10 zone untrust
set interface tunnel.10 ip 10.0.2.1/30
set interface tunnel.10 dip 6 10.0.2.2 10.0.2.2
```

2. 地址

```
set address trust lan 10.1.1.0/24
set address trust oda2 10.0.3.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

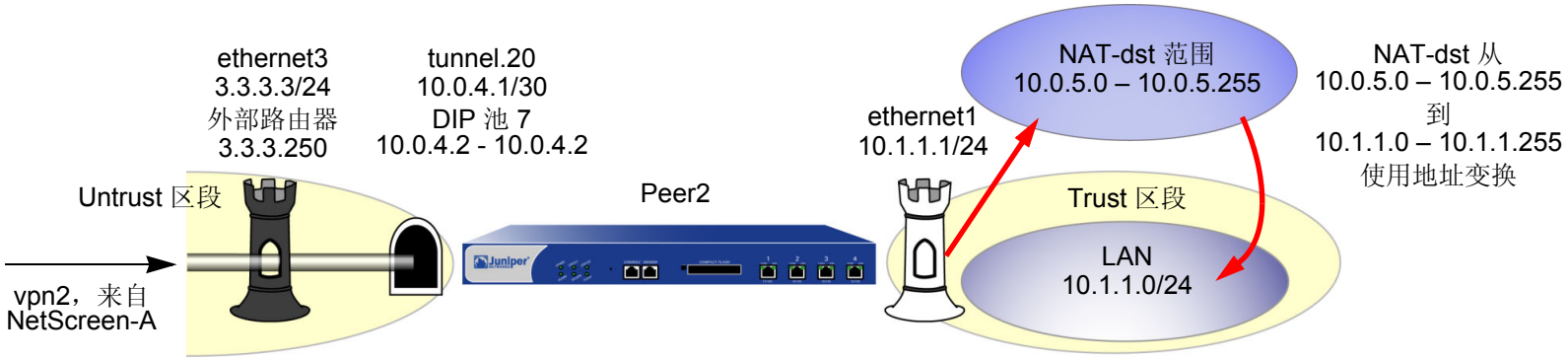
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250 metric 1
set vrouter trust-vr route 10.0.3.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.10 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

5. 策略

```
set policy from trust to untrust lan to_corp any nat src dip-id 6 permit
set policy from untrust to trust fr_corp oda2 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

Peer2

以下配置是创建到企业站点 NetScreen-A 的 VPN 通道时，NetScreen 设备的远程 admin 在 peer2 站点中必须输入的内容。由于内部地址与企业 LAN 的地址均位于地址空间 10.1.1.0/24 内，因此远程 admin 需要配置 NetScreen 设备以执行源和目标 NAT (NAT-src 和 NAT-dst)。 Peer2 通过 VPN2 将信息流发送到 NetScreen-A 时，使用 DIP 池 7 来执行 NAT-src 以将所有内部源地址转换为 10.0.4.2。 Peer2 将对从 NetScreen-A 发来的 VPN 信息流执行 NAT-dst，使用生效的地址变换将地址从 10.0.5.0/24 转换为 10.1.1.0/24。



注意：有关 NAT-src 和 NAT-dst 的详细信息，请参阅第 7 卷，“地址转换”。

WebUI (Peer2)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

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

Tunnel Interface Name: tunnel.20

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.0.4.1/30

Network > Interfaces > Edit (对于 tunnel.20) > DIP > New: 输入以下内容，然后单击 **OK**:

ID: 7

IP Address Range: (选择), 10.0.4.2 ~ 10.0.4.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

2. 地址

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

Address Name: lan

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: oda3

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.5.0/24

Zone: Trust

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

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.1.0/24

Zone: Untrust

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

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.0.2/32

Zone: Untrust

3. VPN

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

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

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：

Bind to: Tunnel Interface, tunnel.20

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Metric: 1

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

Network Address / Netmask: 10.0.5.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

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

Network Address / Netmask: 10.0.1.0/24

Gateway: (选择)

Interface: tunnel.20

Gateway IP Address: 0.0.0.0

Metric: 10

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

Network Address / Netmask: 10.0.1.0/24

Gateway: (选择)

Interface: null

Gateway IP Address: 0.0.0.0

Metric: 12

5. 策略

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

Source Address:

Address Book Entry: (选择), lan

Destination Address:

Address Book Entry: (选择), to_corp

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Source Translation: (选择)

DIP On: 7 (10.0.4.2–10.0.4.2)/X-late

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

Source Address:

Address Book Entry: (选择), fr_corp

Destination Address:

Address Book Entry: (选择), oda3

Service: Any

Action: Permit

Position at Top: (选择)

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

NAT:

Destination Translation: (选择)

Translate to IP Range: (选择), 10.1.1.0 - 10.1.1.254

CLI (Peer2)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24
set interface tunnel.20 zone untrust
set interface tunnel.20 ip 10.0.4.1/30
set interface tunnel.20 dip 7 10.0.4.2 10.0.4.2
```

2. 地址

```
set address trust lan 10.1.1.0/24
set address trust oda3 10.0.5.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway corp sec-level compatible
set vpn vpn2 bind interface tunnel.20
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 路由

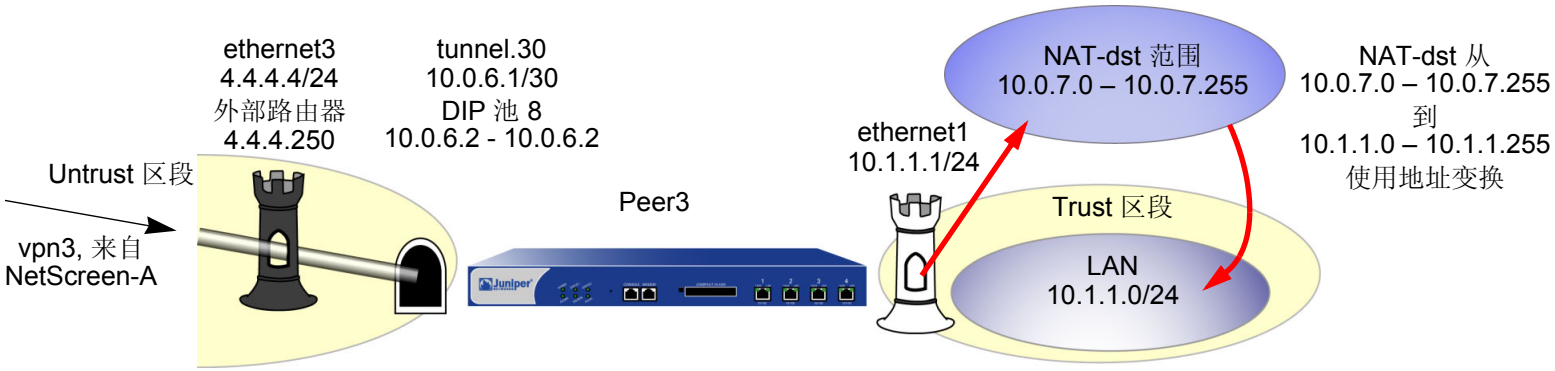
```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.0.5.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.20 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

5. 策略

```
set policy from trust to untrust lan to_corp any nat src dip-id 7 permit
set policy from untrust to trust fr_corp oda3 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

Peer3

以下配置是创建到企业站点 NetScreen-A 的 VPN 通道时， NetScreen 设备的远程 admin 在 peer3 站点中必须输入的内容。由于内部地址与企业 LAN 的地址均位于地址空间 10.1.1.0/24 内，因此远程 admin 需要配置 NetScreen 设备以执行源和目标 NAT (NAT-src 和 NAT-dst)。Peer3 通过 VPN3 将信息流发送到 NetScreen-A 时，使用 DIP 池 8 来执行 NAT-src 以将所有内部源地址转换为 10.0.6.2。 Peer3 将对从 NetScreen-A 发来的 VPN 信息流执行 NAT-dst，使用生效的地址变换将地址从 10.0.7.0/24 转换为 10.1.1.0/24。



***注意：**有关 NAT-dst 的详细信息，请参阅第 7 卷，“地址转换”。*

WebUI (Peer3)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 4.4.4.4/24

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

Tunnel Interface Name: tunnel.30

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.0.6.1/30

Network > Interfaces > Edit (对于 tunnel.30) > DIP > New: 输入以下内容，然后单击 **OK**:

ID: 7

IP Address Range: (选择), 10.0.6.2 ~ 10.0.6.2

Port Translation: (选择)

In the same subnet as the interface IP or its secondary IPs: (选择)

2. 地址

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

Address Name: lan

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: oda4

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.7.0/24

Zone: Trust

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

Address Name: to_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.1.0/24

Zone: Untrust

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

Address Name: fr_corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.0.0.2/32

Zone: Untrust

3. VPN

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

VPN Name: vpn3

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen3

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：

Bind to: Tunnel Interface, tunnel.30

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 4.4.4.250

Metric: 1

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

Network Address / Netmask: 10.0.7.0/24

Gateway: (选择)

Interface: ethernet1

Gateway IP Address: 0.0.0.0

Metric: 1

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

Network Address / Netmask: 10.0.0.0/8

Gateway: (选择)

Interface: tunnel.30

Gateway IP Address: 10.0.0.1

Metric: 10

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

Network Address / Netmask: 10.0.0.0/8

Gateway: (选择)

Interface: null

Gateway IP Address: 10.0.0.1

Metric: 12

5. 策略

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

Source Address:

Address Book Entry: (选择), lan

Destination Address:

Address Book Entry: (选择), to_corp

Service: Any

Action: Permit

Position at Top: (选择)

> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：
NAT:
Source Translation: (选择)
DIP On: 8 (10.0.6.2–10.0.6.2)/X-late

Policies > (From: Untrust, To: Trust) New: 输入以下内容，然后单击 **OK**:
Source Address:
Address Book Entry: (选择), fr_corp
Destination Address:
Address Book Entry: (选择), oda4
Service: Any
Action: Permit
Position at Top: (选择)
> Advanced: 输入以下高级设置，然后单击 **Return**，返回基本 Policy 配置页：
NAT:
Destination Translation: (选择)
Translate to IP Range: (选择), 10.1.1.0 - 10.1.1.254

CLI (Peer3)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/24
set interface ethernet3 zone untrust
set interface ethernet3 ip 4.4.4.4/24
set interface tunnel.30 zone untrust
set interface tunnel.30 ip 10.0.6.1/30
set interface tunnel.30 dip 8 10.0.6.2 10.0.6.2
```

2. 地址

```
set address trust lan 10.1.1.0/24
set address trust oda4 10.0.7.0/24
set address untrust to_corp 10.0.1.0/24
set address untrust fr_corp 10.0.0.2/32
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen3 sec-level compatible
set vpn vpn3 gateway corp sec-level compatible
set vpn vpn3 bind interface tunnel.30
set vpn vpn3 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 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.0.7.0/24 interface ethernet1 metric 1
set vrouter trust-vr route 10.0.0.0/8 interface tunnel.30 metric 10
set vrouter trust-vr route 10.0.0.0/8 interface null metric 12
```

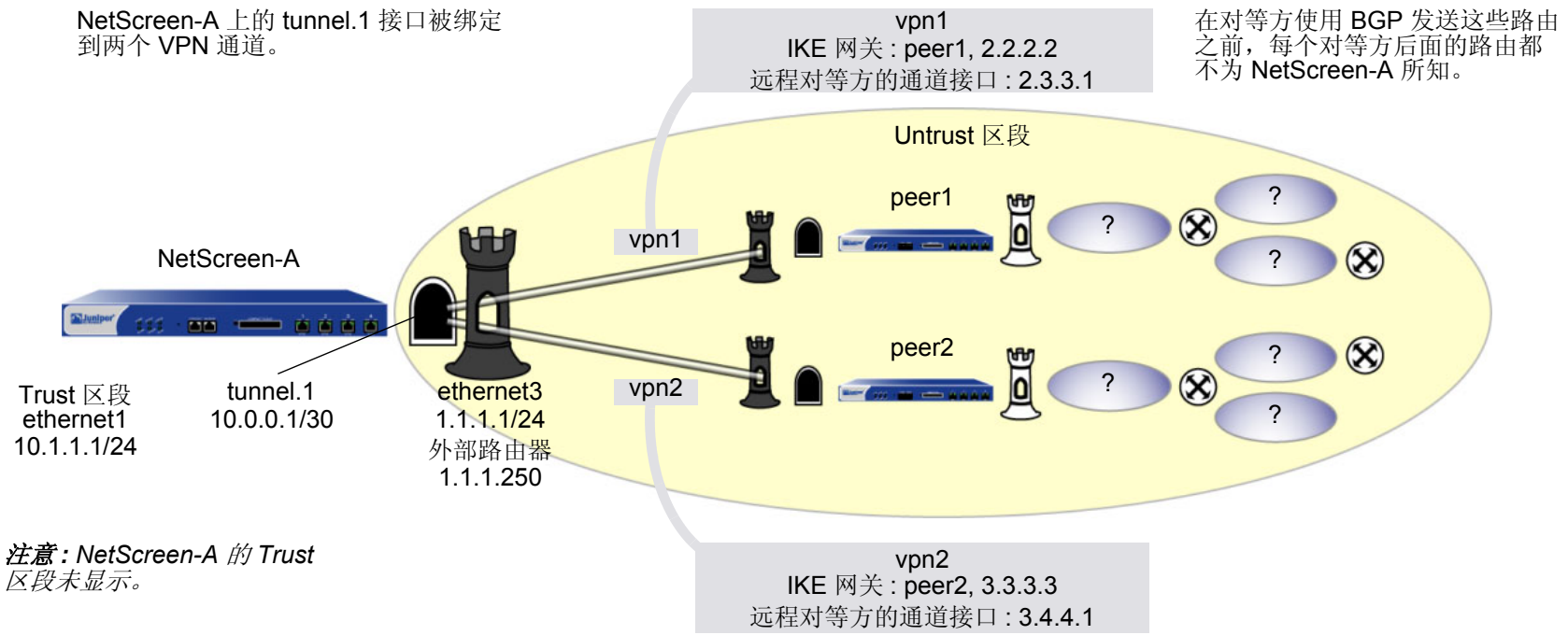
5. 策略

```
set policy from trust to untrust lan to_corp any nat src dip-id 8 permit
set policy from untrust to trust fr_corp oda4 any nat dst ip 10.1.1.0
    10.1.1.254 permit
save
```

范例：自动路由表和 NHTB 表条目

在本例中，将把两个基于路由的 “自动密钥 IKE VPN” 通道 (vpn1、 vpn2) 绑定到企业站点 NetScreen-A 上的单个通道接口 tunnel.1。在已连接路由的后面，每个远程对等方保护的网络都有多个路由。对等方利用 “边界网关协议” (BGP) 将路由传给 NetScreen-A。本例允许 VPN 信息流从 NetScreen-A 后的企业站点流向对等方站点。

***注意：** 在此例中，也可使用 “开放式最短路径优先 (OSPF)” 替代 BGP 作为路由协议。有关 OSPF 配置的信息，请参阅第 431 页上的 “范例附录：自动路由表条目的 OSPF”。*



***注意：** NetScreen-A 的 Trust 区段未显示。*

每个通道两端的 VPN 通道配置对 “阶段 1” 和 “阶段 2” 提议均使用下列参数 : 自动密钥 IKE、预共享密钥 (peer1: “netscreen1”、peer2: “netscreen2”) 以及预定义为 “Compatible” 的安全级别。(有关这些提议的详细信息，请参阅第 11 页上的 “通道协商”。)

通过配置以下两个功能，即可使 NetScreen-A 自动填充 NHTB 表和路由表[17] :

- 带有重定密钥选项 (或 IKE 心跳信号重新连接选项) 的 VPN 监控[18]
- tunnel.1 上的 BGP 动态路由

为 “自动密钥 IKE VPN” 通道启用带有重定密钥选项的 VPN 监控后，当您和远程站点的 admin 完成对通道的配置后， NetScreen-A 即建立与远程对等方的 VPN 连接。设备并不等待用户生成的 VPN 信息流来执行 IKE 协商。在 “阶段 2” 协商期间，NetScreen 设备交换通道接口 IP 地址，这样 NetScreen-A 即可自动在 NHTB 表中生成 VPN 到下一跳跃的映射。

重定密钥选项会确保当 “阶段 1” 和 “阶段 2” 生存期到期时，设备自动协商新密钥的生成程序，而无需他人干预。实际上，启用重定密钥的 VPN 监控提供了一种方法，使 VPN 通道即使在没有用户生成信息流的情况下也能连续保持连接状态。这一点非常必要，因为这可使您和远程 admin 在通道两端创建并启用的 BGP 动态路由实例将路由信息发送给 NetScreen-A 并使用路由自动填充路由表。在用户生成的信息流需要这些路由之前， NetScreen-A 需要使用这些路由来引导通过 VPN 通道的信息流。 (对等方站点的 admin 仍需要通过各自站点的通道接口输入通往虚拟专用网其余部分的单个静态路由。)

在 NetScreen-A 上输入缺省路由和静态路由，以通过正确的 VPN 通道到达其 BGP 邻接设备。每台设备上的所有安全区段和接口都在该设备的 trust-vr 虚拟路由选择域中。

17. 在通道接口上运行动态路由协议时，即使不启用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控，由协议生成的信息流也会触发 IKE 协商。但 Juniper Networks 仍建议不要依赖动态路由信息流来触发 IKE 协商。应使用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控。

18. 在通道接口上运行 BGP 时，即使不启用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控， BGP 生成的信息流也会触发 IKE 协商。但 Juniper Networks 仍建议不要依赖 BGP 信息流来触发 IKE 协商。而应使用带有重定密钥选项或 IKE 心跳信号重新连接选项的 VPN 监控。

WebUI (NetScreen-A)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.0.0.1/30

2. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: peer1

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

Preshared Key: netscreen1

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：

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPN Monitor[19] : (选择)

Rekey: (选择)

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

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: peer2

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

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

19. 保留 Source Interface 和 Destination IP 选项的缺省设置。有关这些选项的信息，请参阅第 355 页上的 “VPN 监控”。

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

Bind to: Tunnel Interface, tunnel.1

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

VPN Monitor[20] : (选择)

Rekey: (选择)

3. 静态路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.250

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

Network Address / Netmask: 2.3.3.1/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 2.3.3.1

20. 保留 Source Interface 和 Destination IP 选项的缺省设置。有关这些选项的信息，请参阅 第 355 页上的 “VPN 监控”。

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

Network Address / Netmask: 3.4.4.1/32

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 3.4.4.1

4. 动态路由

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create BGP Instance: 输入以下内容，然后单击 **OK**:

AS Number (必需): 99

BGP Enabled: (选择)

Network > Interfaces > Edit (对于 tunnel.1) > BGP: 选中 **Protocol BGP** 复选框，然后单击 **OK**。

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 99

Remote IP: 2.3.3.1

Outgoing Interface: tunnel.1

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 99

Remote IP: 3.4.4.1

Outgoing Interface: tunnel.1

5. 策略

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

Source Address:

Address Book: (选择), Any

Destination Address:

Address Book: (选择), Any

Service: ANY

Action: Permit

CLI (NetScreen-A)

1. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip 10.0.0.1/30
```

2. VPN

```
set ike gateway peer1 address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway peer1 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 rekey
```

```
set ike gateway peer2 address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn2 gateway peer2 sec-level compatible
set vpn vpn2 bind interface tunnel.1
set vpn vpn2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
set vpn vpn2 monitor rekey
```

3. 静态路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
set vrouter trust-vr route 2.3.3.1/32 interface tunnel.1 gateway 2.3.3.1
set vrouter trust-vr route 2.4.4.1/32 interface tunnel.1 gateway 2.4.4.1
```

4. 动态路由

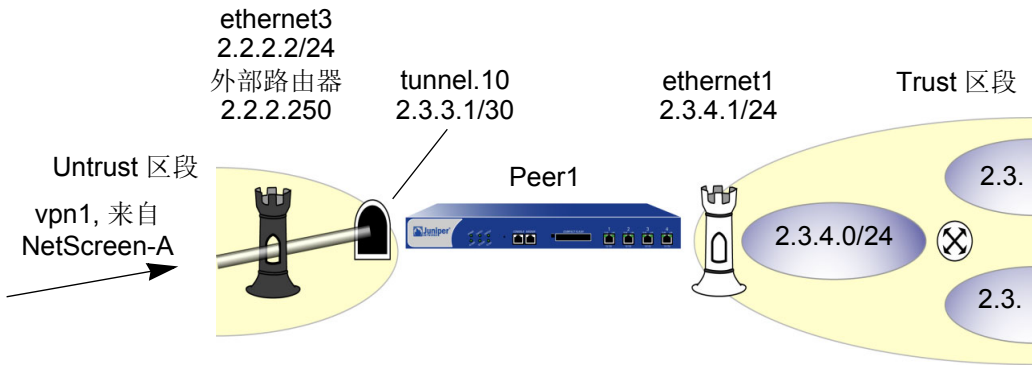
```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.1 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 2.3.3.1 remote-as 99 outgoing interface
    tunnel.1
ns(trust-vr/bgp)-> set neighbor 2.3.3.1 enable
ns(trust-vr/bgp)-> set neighbor 3.4.4.1 remote-as 99 outgoing interface
    tunnel.1
ns(trust-vr/bgp)-> set neighbor 3.4.4.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

5. 策略

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

Peer1

以下配置是创建到企业站点 NetScreen-A 的 VPN 通道时， NetScreen 设备的远程 admin 在 peer1 站点中必须输入的内容。远程 admin 配置 NetScreen 设备，以允许企业站点的入站信息流。还需要配置 NetScreen 设备，以便与通过 vpn1 到 BGP 邻接设备的内部路由进行通信。



WebUI (Peer1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.3.4.1/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.10

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 2.3.3.1/30

2. 地址

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

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

VPN Name: vpn1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

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：

Bind to: Tunnel Interface, tunnel.10

Proxy-ID: (选择)
Local IP / Netmask: 0.0.0.0/0
Remote IP / Netmask: 0.0.0.0/0
Service: ANY

4. 静态路由

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

Network Address / Netmask: 0.0.0.0/0
Gateway: (选择)
Interface: ethernet3
Gateway IP Address: 2.2.2.250
Metric: 1

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

Network Address / Netmask: 10.1.1.0/24
Gateway: (选择)
Interface: tunnel.10
Gateway IP Address: 0.0.0.0
Metric: 1

5. 动态路由

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create BGP Instance: 输入以下内容，然后单击 **OK**:

AS Number (必需): 99
BGP Enabled: (选择)

Network > Interfaces > Edit (对于 tunnel.10) > BGP: 选中 **Protocol BGP** 复选框，然后单击 **OK**。

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 99

Remote IP: 10.0.0.1

Outgoing Interface: tunnel.10

6. 策略

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

Source Address:

Address Book Entry: (选择), corp

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

CLI (Peer1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 2.3.4.1/24

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

set interface tunnel.10 zone untrust
set interface tunnel.10 ip 2.3.3.1/30
```

2. 地址

```
set address untrust corp 10.1.1.0/24
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.10
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 静态路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250 metric 1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.10 metric 1
```

5. 动态路由

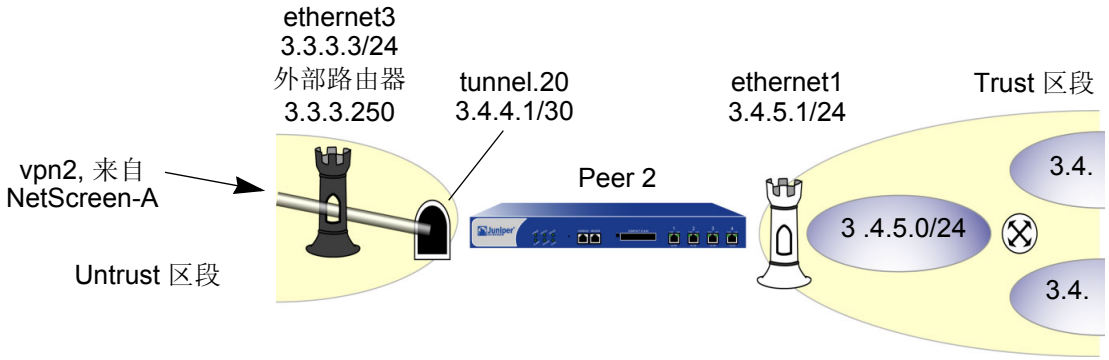
```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.10 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface
    tunnel.10
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

6. 策略

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

Peer2

以下配置是创建到企业站点 NetScreen-A 的 VPN 通道时， NetScreen 设备的远程 admin 在 peer2 站点中必须输入的内容。远程 admin 配置 NetScreen 设备，以允许企业站点的入站信息流。还需要配置 NetScreen 设备，以便与通过 vpn2 到 BGP 邻接设备的内部路由进行通信。



WebUI (Peer2)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.3.4.1/24

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

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

Tunnel Interface Name: tunnel.20

Zone (VR): Untrust (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 3.4.4.1/30

2. 地址

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

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.1.0/24

Zone: Untrust

3. VPN

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

VPN Name: vpn2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: corp

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

Security Level: Compatible

Outgoing Interface: ethernet3

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

Bind to: Tunnel Interface, tunnel.20

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 静态路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 3.3.3.250

Metric: 1

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

Network Address / Netmask: 10.1.1.0/24

Gateway: (选择)

Interface: tunnel.20

Gateway IP Address: 0.0.0.0

Metric: 1

5. 动态路由

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create BGP Instance: 输入以下内容，然后单击 **OK**:

AS Number (必需): 99

BGP Enabled: (选择)

Network > Interfaces > Edit (对于 tunnel.20) > BGP: 选中 **Protocol BGP** 复选框，然后单击 **OK**。

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Edit BGP Instance > Neighbors: 输入以下内容，然后单击 **Add**:

AS Number: 99

Remote IP: 10.0.0.1

Outgoing Interface: tunnel.20

6. 策略

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

Source Address:

Address Book Entry: (选择), corp

Destination Address:

Address Book Entry: (选择), Any

Service: ANY

Action: Permit

CLI (Peer2)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 3.4.5.1/24
```

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24

set interface tunnel.20 zone untrust
set interface tunnel.20 ip 3.4.4.1/30
```

2. 地址

```
set address untrust corp 10.1.1.0/24
```

3. VPN

```
set ike gateway corp address 1.1.1.1 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn vpn1 gateway corp sec-level compatible
set vpn vpn1 bind interface tunnel.20
set vpn vpn1 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

4. 静态路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250 metric 1
set vrouter trust-vr route 10.1.1.0/24 interface tunnel.20 metric 1
```

5. 动态路由

```
ns-> set vrouter trust-vr protocol bgp 99
ns-> set vrouter trust-vr protocol bgp enable
ns-> set interface tunnel.20 protocol bgp
ns-> set vrouter trust-vr
ns(trust-vr)-> set protocol bgp
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 remote-as 99 outgoing interface
    tunnel.20
ns(trust-vr/bgp)-> set neighbor 10.0.0.1 enable
ns(trust-vr/bgp)-> exit
ns(trust-vr)-> exit
```

6. 策略

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

范例附录：自动路由表条目的 OSPF

也可使用 OSPF 来替代 BGP 动态路由，使对等方将路由信息传达给 NetScreen-A。要允许 NetScreen-A 上的 tunnel.1 与其对等方形成 OSPF 邻接，必须将通道接口配置为 “点对多点” 接口。每个设备的 OSPF 动态路由配置如下所示。

WebUI (NetScreen-A)

动态路由 (OSPF)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create OSPF Instance: 选择 **OSPF Enabled**，然后单击 **Apply**。

Area > Configure (对于区域 0.0.0.0): 单击 **<< Add** 将 tunnel.1 接口从 Available Interface(s) 列表移动到 Selected Interface(s) 列表，然后单击 **OK**。

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

Bind to Area: (选择), 从下拉列表选择 0.0.0.0

Protocol OSPF: Enable

Link Type: Point-to-Multipoint (选择)

CLI (NetScreen-A)

动态路由 (OSPF)

```
ns-> set vrouter trust-vr protocol ospf
ns-> set vrouter trust-vr protocol ospf enable
ns-> set interface tunnel.1 protocol ospf area 0
ns-> set interface tunnel.1 protocol ospf link-type p2mp
ns-> set interface tunnel.1 protocol ospf enable
ns-> save
```

WebUI (Peer1)

动态路由 (OSPF)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create OSPF Instance: 选择 **OSPF Enabled**，然后单击 **Apply**。

Area > Configure (对于区域 0.0.0.0): 单击 **<< Add** 将 tunnel.1 接口从 Available Interface(s) 列表移动到 Selected Interface(s) 列表，然后单击 **OK**。

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

Bind to Area: (选择), 从下拉列表选择 0.0.0.0

Protocol OSPF: Enable

CLI (Peer1)

动态路由 (OSPF)

```
ns-> set vrouter trust-vr protocol ospf
ns-> set vrouter trust-vr protocol ospf enable
ns-> set interface tunnel.1 protocol ospf area 0
ns-> set interface tunnel.1 protocol ospf enable
ns-> save
```

WebUI (Peer2)

动态路由 (OSPF)

Network > Routing > Virtual Routers > Edit (对于 trust-vr) > Create OSPF Instance: 选择 **OSPF Enabled**，然后单击 **Apply**。

Area > Configure (对于区域 0.0.0.0): 单击 **<< Add** 将 tunnel.1 接口从 Available Interface(s) 列表移动到 Selected Interface(s) 列表，然后单击 **OK**。

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

Bind to Area: (选择), 从下拉列表选择 0.0.0.0

Protocol OSPF: Enable

CLI (Peer2)

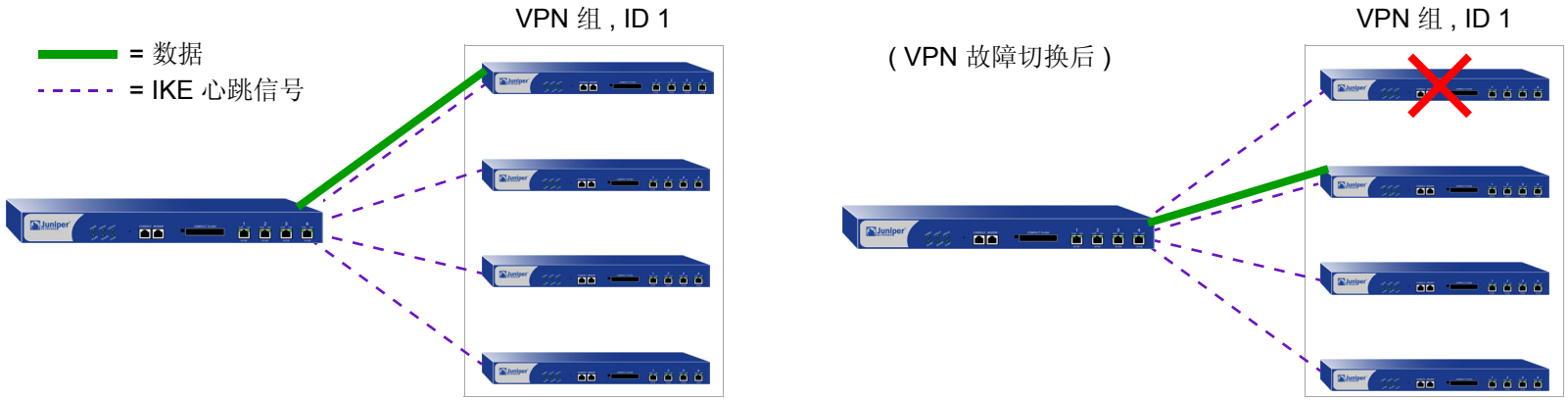
动态路由 (OSPF)

```
ns-> set vrouter trust-vr protocol ospf
ns-> set vrouter trust-vr protocol ospf enable
ns-> set interface tunnel.1 protocol ospf area 0
ns-> set interface tunnel.1 protocol ospf enable
ns-> save
```

冗余 VPN 网关

NetScreen 冗余网关功能可提供一种解决方案，它能够在站点到站点故障切换期间及故障后保证不间断的 VPN 连接。可以创建一个 VPN 组以提供一组 (最多四个) 冗余网关，基于策略的站点到站点或站点到站点动态对等方自动密钥 IKE IPSec[21] VPN 通道可连接到这些冗余网关上。当 NetScreen 设备首次接收到与引用 VPN 组的策略相匹配的信息流时，它将与该组中的所有成员执行 “阶段 1” 和 “阶段 2” IKE 协商。 NetScreen 设备通过 VPN 通道将数据发送到组中具有最高优先权的网关或 “加权” 网关。对于组中的其它所有网关， NetScreen 设备将保持 “阶段 1” 和 “阶段 2” 的 SA 并通过经这些通道发送 IKE 激活数据包来使其保持活动状态。如果活动的 VPN 通道失败，此通道可以故障切换到组中具有第二高优先权的通道和网关。

***注意：** 此方案假设已与冗余网关后的站点建立连接，因而数据在所有站点的主机中均有镜像。此外，每个站点 (专门针对高可用性 (HA)) 都有一个在 HA 模式下运行的 NetScreen 设备冗余集群。因此，设置的 VPN 故障切换临界值必须高于设备故障切换临界值，否则可能会发生不必要的 VPN 故障切换。*

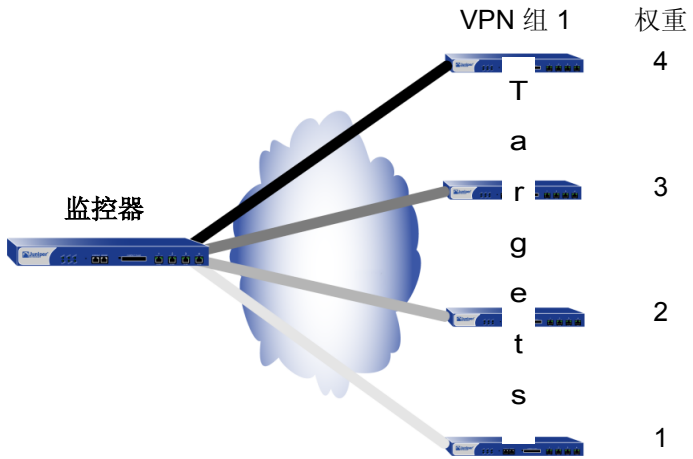


21. VPN 组不支持 L2TP、IPSec 上的 L2TP、拨号、手动密钥或基于路由的 VPN 通道类型。在 “站点对站点动态对等方” 配置中，监视 VPN 组的 NetScreen 设备其不可信 IP 地址必须是动态指定的，而 VPN 组成员的不可信 IP 地址必须是静态的。

VPN 组

VPN 组是一组 VPN 通道配置，最多可包括四个目标远程网关。组中各通道的 “阶段 1” 和 “阶段 2” 安全联盟 (SA) 参数可以不同，也可以相同 (当然远程网关的 IP 地址不能相同)。VPN 组具有唯一的 ID 号，并且组中的各成员都被指定一个唯一的权重以确定其在要成为活动通道的优先队列中的位置。数值 1 是最低的或最不优先的队列。

注意：在此图例中，底纹代表各通道的权重。通道遮蔽得越暗，其优先权越高。



NetScreen 设备与 VPN 组成员进行通信，各成员之间也具有监控器与目标关系。监控设备连续监控各目标设备的连通性和运行状态。监控器用来执行此操作的工具如下：

- IKE 心跳信号
- IKE 恢复尝试

这两种工具将在下一部分第 436 页上的 “监控机制”中加以介绍。

***注意：**监控器到目标关系不必是单向的。监控设备也可以是 VPN 组的一个成员，因而也可以是其它监控设备的目标。*

监控机制

NetScreen 使用两种机制来监控 VPN 组的成员以确定其终止 VPN 信息流的能力：

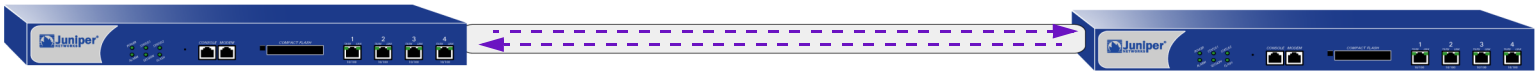
- IKE 心跳信号
- IKE 恢复尝试

使用这两种工具及 TCP 应用程序故障切换选项 (请参阅第 440 页上的 “TCP SYN 标记检查”)， NetScreen 设备即可判断何时需要 VPN 故障切换以及何时不必中断 VPN 设备而将信息流切换到新通道。

IKE 心跳信号

IKE 心跳信号是 IKE 对等方在 “阶段 1” 安全联盟 (SA) 保护下相互发送的 hello 消息，用以确认另一方的连通性和运行状态。例如，如果 device_m (监控器) 未收到来自 device_t (目标) 的指定数量的心跳信号 (缺省值是 5)，device_m 即认为 device_t 已经中断。 Device_m 将从 SA 高速缓存中清除相应的 “阶段 1” 和 “阶段 2” 安全联盟 (SA) 并开始 IKE 恢复过程。 (请参阅第 437 页上的 “IKE 恢复过程”。) Device_t 也将清除自己的 SA。

注意：*在 VPN 组中， VPN 通道两端的设备必须启用 IKE 心跳信号功能。如果在 device_m 上启用该功能而在 device_t 上未启用， device_m 将禁止 IKE 心跳信号传输并在事件日志中生成以下消息：“Heartbeats have been disabled because the peer is not sending them.”*



“IKE 心跳信号” 必须通过 VPN 通道进行双向流动。

要定义特定 VPN 通道的 IKE 心跳信号间隔和临界值 (缺省值是 5)，请执行以下操作 :

WebUI

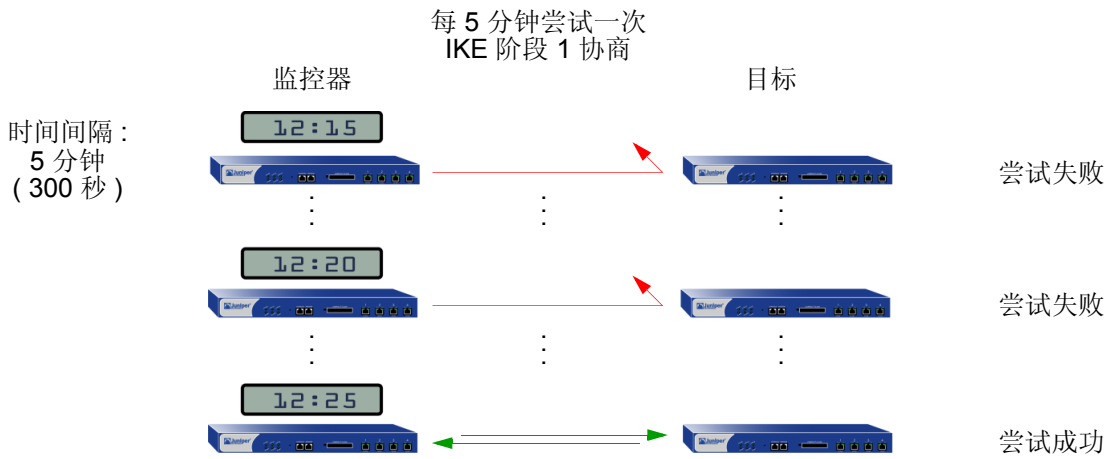
VPNs > AutoKey Advanced > Gateway > Edit (对于希望修改其 IKE 心跳信号临界值的网关) > Advanced: 在 Heartbeat Hello 和 Heartbeat Threshold 字段中输入新值，然后单击 **OK**。

CLI

```
set ike gateway name_str heartbeat hello number
set ike gateway name_str heartbeat threshold number
```

IKE 恢复过程

NetScreen 监控设备确定目标设备已中断后，监控器将停止发送 IKE 心跳信号，并从其 SA 高速缓存中清除该对等方的 SA。经过定义的时间间隔后，监控器会尝试启动与失败对等方的 “阶段 1” 协商。如果第一次尝试不成功，监控器将继续以固定时间间隔尝试 “阶段 1” 协商，直到协商成功为止。



要定义特定 VPN 通道的 IKE 恢复时间间隔 (最小设置是 60 秒)，请执行以下任一操作：

WebUI

VPNs > AutoKey Advanced > Gateway > Edit (对于希望修改其 IKE 重新连接时间间隔的网关) > Advanced: 在 Heartbeat Reconnect 字段中输入秒数，然后单击 **OK**。

CLI

```
set ike gateway name_str heartbeat reconnect number
```

当具有最大权重的 VPN 组成员将通道故障切换到其它组成员，然后重新连接监控设备时，该通道将在故障恢复后自动切换回第一个成员。加权系统总是使用组中最好的网关来处理 VPN 数据 (只要该网关可以执行此操作)。

以下图例介绍了当来自目标网关丢失的心跳信号超过故障临界值时， VPN 组成员经历的过程。

TCP SYN 标记检查

要使 VPN 故障切换顺利执行，必须进行 TCP 会话的处理。故障切换后，如果新活动网关在现有 TCP 会话中接收到一个数据包，新网关将把它作为新 TCP 会话中的第一个数据包进行处理，同时检查数据包包头中是否设置了 SYN 标记。由于此数据包确实是现有会话的组成部分，因而它未设置 SYN 标记。新网关将因此拒绝此数据包。启用 TCP SYN 标记检查时，如果发生故障切换，所有 TCP 应用程序都必须进行重新连接。

要解决此问题，可禁用 VPN 通道中 TCP 会话的 SYN 标记检查，如下所述：

WebUI

不能通过 WebUI 禁用 SYN 标记检查。

CLI

```
unset flow tcp-syn-check-in-tunnel
```

注意：*缺省情况下 SYN 标记检查是启用的。*

范例 : 冗余 VPN 网关

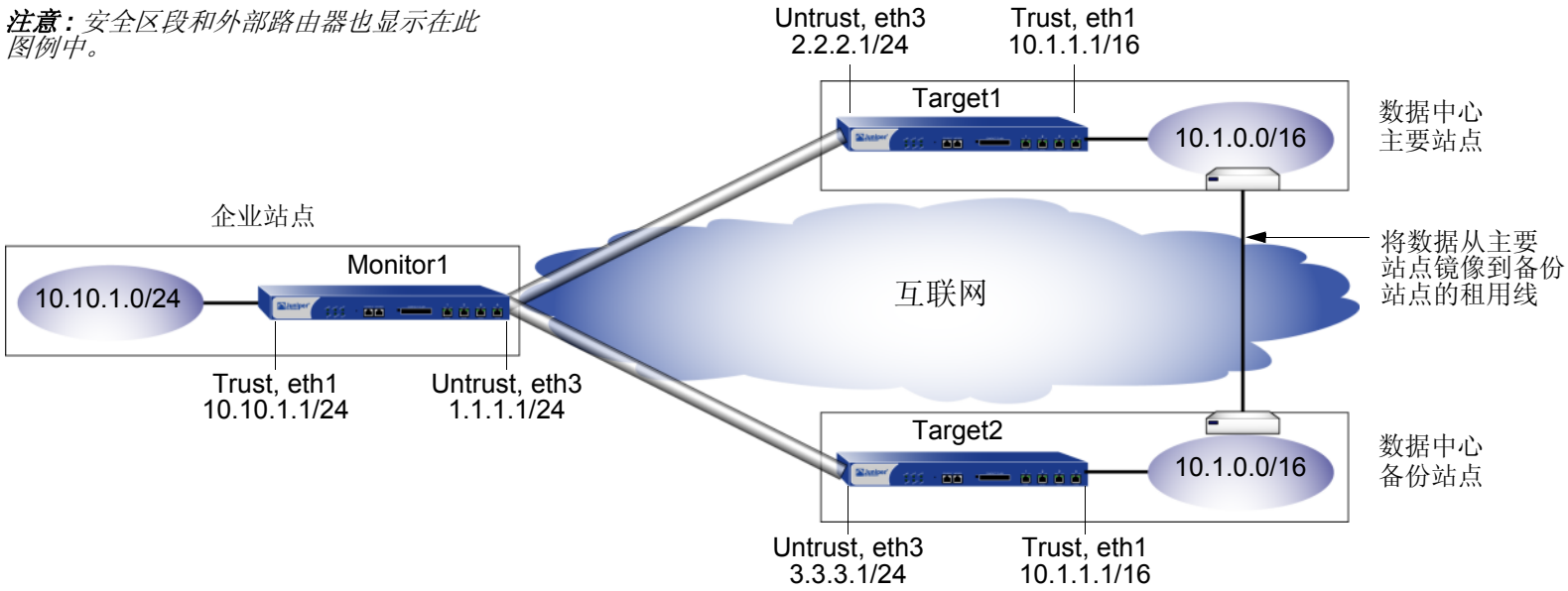
在此例中，企业站点具有一个通往数据中心的 VPN 通道和通往备份数据中心的第二通道。所有数据都通过这两个数据中心站点间的租用线连接加以镜像。数据中心是独立的，即使在发生灾难性故障 (例如全天断电或发生自然灾害) 时，也可以提供连续的服务。

设备的位置和名称、物理接口及其 Trust 和 Untrust 区段的 IP 地址、各个 NetScreen 设备的 VPN 组 ID 和权重，如下所示 :

设备位置	设备名称	物理接口和 IP 地址 (Trust 区段)	物理接口 IP 地址、缺省网关 (Untrust 区段)	VPN 组 ID 和权重
公司	Monitor1	ethernet1, 10.10.1.1/24	ethernet3, 1.1.1.1/24, (GW) 1.1.1.2	– –
数据中心 (主要)	Target1	ethernet1, 10.1.1.1/16	ethernet3, 2.2.2.1/24, (GW) 2.2.2.2	ID = 1，权重 = 2
数据中心 (备份)	Target2	ethernet1, 10.1.1.1/16	ethernet3, 3.3.3.1/24, (GW) 3.3.3.2	ID = 1，权重 = 1

注意 : *两个数据中心站点的内部地址空间必须一致。*

所有安全区域都在 trust-vr 路由选择域中。所有 “站点到站点自动密钥 IKE VPN” 通道对 “阶段 1” 和 “阶段 2” 提议都使用预定义为 “Compatible” 的安全级别。预共享密钥认证参与者。



WebUI (Monitor1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.10.1.1/24

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

2. 地址

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

Address Name: in_trust

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.0/24

Zone: Trust

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

Address Name: data_ctr

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.0.0/16

Zone: Untrust

3. VPN

VPNs > AutoKey Advanced > VPN Group: 在 VPN Group ID 字段中输入 1，然后单击 **Add**。

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

Gateway Name: target1

Security Level: Compatible

Remote Gateway Type: Static IP Address: (选择), IP Address: 2.2.2.1

Preshared Key: SLi1yoo129

Outgoing Interface: ethernet3

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

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 seconds

Threshold: 5

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

VPN Name: to_target1

Security Level: Compatible

Remote Gateway: Predefined: (选择), target1

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

VPN Group: VPN Group-1

Weight: 2

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

Gateway Name: target2

Security Level: Compatible

Remote Gateway Type: Static IP Address: (选择), IP Address: 3.3.3.1

Preshared Key: CMFwb7oN23

Outgoing Interface: ethernet3

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

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 seconds

Threshold: 5

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

VPN Name: to_target2

Security Level: Compatible

Remote Gateway: Predefined: (选择), target2

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

VPN Group: VPN Group -1

Weight: 1

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 1.1.1.2(untrust)

5. 策略

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

Source Address:

Address Book Entry: (选择), in_trust

Destination Address:

Address Book Entry: (选择), data_ctr

Service: ANY

Action: Tunnel

VPN: VPN Group -1

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

WebUI (Target1)

1. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.1.1.1/16

输入以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.1/24

2. 地址

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

Address Name: in_trust

IP Address/Domain Name:

IP/Netmask: (选择), 10.1.0.0/16

Zone: Trust

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

Address Name: corp

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.0/24

Zone: Untrust

3. VPN

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

Gateway Name: monitor1

Security Level: Compatible

Remote Gateway Type:

Static IP Address: (选择), IP Address/Hostname: 1.1.1.1

Preshared Key: SLi1yoo129

Outgoing Interface: ethernet3

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

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 0 seconds

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

Name: to_monitor1

Security Level: Compatible

Remote Gateway: Predefined: (选择), monitor1

4. 路由

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

Network Address / Netmask: 0.0.0.0/0

Gateway: (选择)

Interface: ethernet3

Gateway IP Address: 2.2.2.2

5. 策略

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

Source Address:

Address Book Entry: (选择), in_trust

Destination Address:

Address Book Entry: (选择), corp

Service: ANY

Action: Tunnel

Tunnel VPN: monitor1

Modify matching bidirectional VPN policy: (选择)

Position at Top: (选择)

WebUI (Target2)

注意：*按照 Target1 配置步骤配置 Target2，但必须将 Untrust 区段接口 IP 地址定义为 3.3.3.1/24，缺省网关 IP 地址定义为 3.3.3.2，并使用 CMFwb7oN23 生成预共享密钥。*

CLI (Monitor1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.10.1.1/24
set interface ethernet1 nat

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

2. 地址

```
set address trust in_trust 10.10.1.0/24
set address untrust data_ctr 10.1.0.0/16
```

3. VPN

```
set ike gateway target1 address 2.2.2.1 main outgoing-interface ethernet3
    preshare SLi1yoo129 sec-level compatible
set ike gateway target1 heartbeat hello 3
set ike gateway target1 heartbeat reconnect 60
set ike gateway target1 heartbeat threshold 5
set vpn to_target1 gateway target1 sec-level compatible
set ike gateway target2 address 3.3.3.1 main outgoing-interface ethernet3
    preshare CMFwb7oN23 sec-level compatible
set ike gateway target2 heartbeat hello 3
set ike gateway target2 heartbeat reconnect 60
set ike gateway target2 heartbeat threshold 5
set vpn to_target2 gateway target2 sec-level compatible
set vpn-group id 1 vpn to_target1 weight 2
set vpn-group id 1 vpn to_target2 weight 1
unset flow tcp-syn-check-in-tunnel
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.2
```

5. 策略

```
set policy top from trust to untrust in_trust data_ctr any tunnel “vpn-group 1”
set policy top from untrust to trust data_ctr in_trust any tunnel “vpn-group 1”
save
```

CLI (Target1)

1. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.1.1.1/16
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 2.2.2.1/24
```

2. 地址

```
set address trust in_trust 10.1.0.0/16
set address untrust corp 10.10.1.0/24
```

3. VPN

```
set ike gateway monitor1 address 1.1.1.1 main outgoing-interface ethernet3
    preshare SLi1yoo129 sec-level compatible
set ike gateway monitor1 heartbeat hello 3
set ike gateway monitor1 heartbeat threshold 5
set vpn to_monitor1 gateway monitor1 sec-level compatible
```

4. 路由

```
set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2
```

5. 策略

```
set policy top from trust to untrust in_trust corp any tunnel vpn to_monitor
set policy top from untrust to trust corp in_trust any tunnel vpn to_monitor
save
```

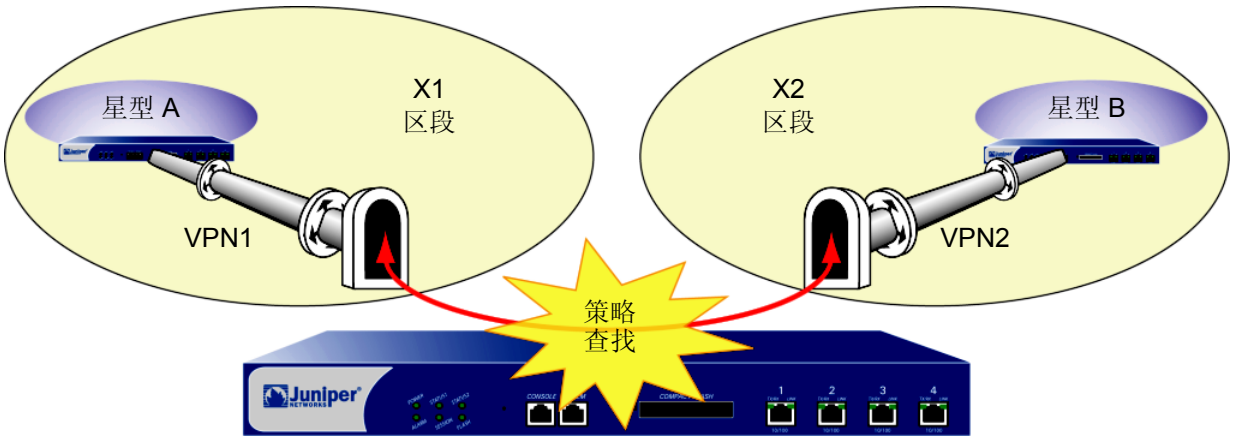
CLI (Target2)

注意：*按照 Target1 配置步骤配置 Target2，但必须将 Untrust 区段接口 IP 地址定义为 3.3.3.1/24，缺省网关 IP 地址定义为 3.3.3.2，并使用 CMFwb7oN23 生成预共享密钥。*

背对背的 VPN

可在中心站点强制执行区段间策略，使信息流能从一个 VPN 通道到达另一通道，方法是将星型站点置于不同区段内[22]。由于它们处于不同区段，在将信息流从一个通道发送到另一通道之前，位于网络中心处的 NetScreen 设备必须执行策略查找。这样才能控制通过星型站点间 VPN 通道的信息流。这样的布置称为背对背 VPN。

背对背的 VPN



22. 也可选择启用内部区段阻塞并定义一个内部区段策略，以控制同一区段内两个通道接口间的信息流。

背对背 VPN 的几个优点：

- 可保持需要创建的 VPN 的数量。例如，周边站点 A 可链接到网络中心以及周边站点 B、C、D...，但是，A 只需建立一个 VPN 通道。特别是对于可同时使用最多十个 VPN 通道的 NetScreen-5XP 用户，应用集中星型方法可显著增加其 VPN 选项和功能。
- 位于中心设备的管理员可完全控制周边站点间的 VPN 信息流。例如，
  - 可以只允许 HTTP 信息流从站点 A 流向站点 B，但允许任意类型的信息流从站点 B 流向站点 A。
  - 可允许起始于 A 的信息流到达 C，但拒绝起始于 C 的信息流到达 A。
  - 允许 A 处的特定主机连接整个 D 网络，而只允许 D 处的主机连接 A 处的不同主机。
- 位于中心设备处的管理员能完全控制起始于所有周边网络的出站信息流。在每个周边站点必须先有一个策略，以引导所有出站信息流通过星型 VPN 到达网络中心，例如：**set policy top from trust to untrust any any any tunnel vpn** *name_str*（其中 *name_str* 定义从每个周边站点到达网络中心的特定 VPN 通道）。在网络中心，管理员可控制互联网访问、允许某些类型的信息流（如只允许 HTTP）、在不符合需要的网站执行 URL 阻塞等等。
- 可使用区域内的网络中心并通过星型通道互连，以允许某一区域内的星型站点连接另一区域内的星型站点。

范例：背对背的 VPN

下例与第 465 页上的 “范例：集中星型 VPN”非常相似，不同之处在于位于纽约中心站点处的 NetScreen 设备需要对东京和巴黎办事处两个通道间发送的信息流执行策略检测。将每个远程站点置于不同区段，即可控制网络中心处的 VPN 信息流。

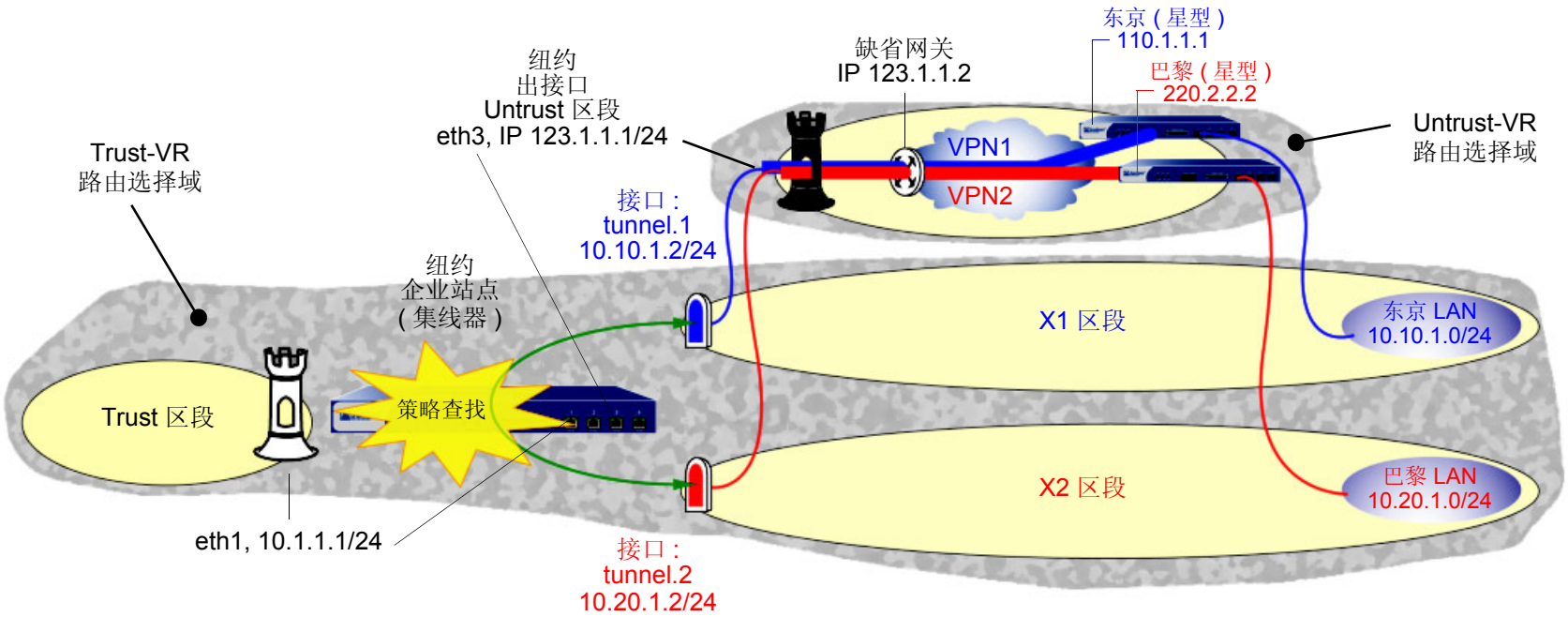
东京 LAN 地址在用户定义的 X1 区段内，巴黎 LAN 地址在用户定义的 X2 区段内。这两个区段都在 Trust-VR 路由选择域中。

注意：*要创建用户定义的区段，必须先获取区段授权数字串并加载到 NetScreen 设备上。*

将 VPN1 通道绑定到 tunnel.1 接口，将 VPN2 通道绑定到 tunnel.2 接口。尽管没有为 X1 和 X2 区段接口分配 IP 地址，但是却为两个通道接口分配了地址。这些接口的路由会自动出现在 Trust-VR 路由表中。将一个通道接口的 IP 地址置于同一目标子网中，即可将流向这个子网的信息流发送到该通道接口。

ethernet3 是出接口，被绑定到 Untrust 区段。从以下图例可以看出，两个通道都终止于 Untrust 区段；但是，使用这两个通道的信息流的终点均位于 X1 和 X2 区段。这两个通道使用 “自动密钥 IKE” 并带有预共享密钥。为阶段 1 和阶段 2 提议选择预定义为 “Compatible” 的安全级别。将 Untrust 区段绑定到 untrust-vr。由于通道是基于路由的 (即，正确的通道由路由确定，而不是由策略中指定的通道名确定)，因此代理 ID 将被包括在每个通道的配置中。

***注意：** 以下只提供了中心站点处 NetScreen 设备的配置。*



WebUI

1. 安全区段和虚拟路由器

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

IP Address / Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

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

Zone Name: Null

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

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (选择)

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

Zone Name: X1

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (选择)

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

Zone Name: X2

Virtual Router Name: trust-vr

Block Intra-Zone Traffic: (选择)

2. 接口

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 123.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): X1 (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.10.1.2/24

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

Tunnel Interface Name: tunnel.2

Zone (VR): X2 (trust-vr)

Fixed IP: (选择)

IP Address / Netmask: 10.20.1.2/24

3. 东京办事处的 VPN

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

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: Tokyo

Type: Static IP: (选择), Address/Hostname: 110.1.1.1

Preshared Key: netscreen1

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：

Proxy-ID: (选择)[23]

Local IP / Netmask: 10.20.1.0/24

Remote IP / Netmask: 10.10.1.0/24

Service: ANY

23. 在 NetScreen 设备上配置用以保护东京和巴黎办事处的 VPN 通道时，请执行以下操作之一：
(基于路由的 VPN) 选中 **Enable Proxy-ID** 复选框，并为 Local IP 和 Netmask 输入 **10.10.1.0/24** (东京) 和 **10.20.1.0/24** (巴黎)，为 Remote IP 和 Netmask 输入 **10.20.1.0/24** (东京) 和 **10.10.1.0/24** (巴黎)。
(基于策略的 VPN) 在 Trust 区段通讯簿中生成 10.10.1.0/24 (东京) 和 10.20.1.0/24 (巴黎) 的条目，在 Untrust 区段通讯簿中生成 10.20.1.0/24 (东京) 和 10.10.1.0/24 (巴黎) 的条目。将这些地址用作策略中的源和目标地址，该策略将引用到中心站点的 VPN 通道。

4. 巴黎办事处的 VPN

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

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: Paris

Type: Static IP: (选择), Address/Hostname: 220.2.2.2

Preshared Key: netscreen2

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：

Proxy-ID: (选择)

Local IP / Netmask: 10.10.1.0/24

Remote IP / Netmask: 10.20.1.0/24

Service: ANY

5. 路由

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

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (选择), untrust-vr

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: ethernet3

Gateway IP Address: 123.1.1.2

6. 地址

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

Address Name: Tokyo LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.10.1.0/24

Zone: X1

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

Address Name: Paris LAN

IP Address/Domain Name:

IP/Netmask: (选择), 10.20.1.0/24

Zone: X2

7. 策略

Policy > (From: X1, To: X2) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Tokyo LAN

Destination Address:

Address Book Entry: (选择), Paris LAN

Service: ANY

Action: Permit

Position at Top: (选择)

Policy > (From: X2, To: X1) New: 输入以下内容，然后单击 **OK**:

Source Address:

Address Book Entry: (选择), Paris LAN

Destination Address:

Address Book Entry: (选择), Tokyo LAN

Service: ANY

Action: Permit

Position at Top: (选择)

CLI

1. 安全区段和虚拟路由器

```
unset interface ethernet3 ip
unset interface ethernet3 zone

set zone untrust vrouter untrust-vr
set zone untrust block

set zone name x1
set zone x1 vrouter trust-vr
set zone x1 block

set zone name x2
set zone x2 vrouter trust-vr
set zone x2 block
```

2. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 123.1.1.1/24

set interface tunnel.1 zone x1
set interface tunnel.1 ip 10.10.1.2/24

set interface tunnel.2 zone x2
set interface tunnel.2 ip 10.20.1.2/24
```

3. 东京办事处的 VPN

```
set ike gateway Tokyo address 110.1.1.1 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn VPN1 gateway Tokyo sec-level compatible
set vpn VPN1 bind interface tunnel.1
set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any[24]
```

4. 巴黎办事处的 VPN

```
set ike gateway Paris address 220.2.2.2 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn VPN2 gateway Paris sec-level compatible
set vpn VPN2 bind interface tunnel.2
set vpn VPN2 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 123.1.1.2
```

6. 地址

```
set address x1 "Tokyo LAN" 10.10.1.0/24
set address x2 "Paris LAN" 10.20.1.0/24
```

7. 策略

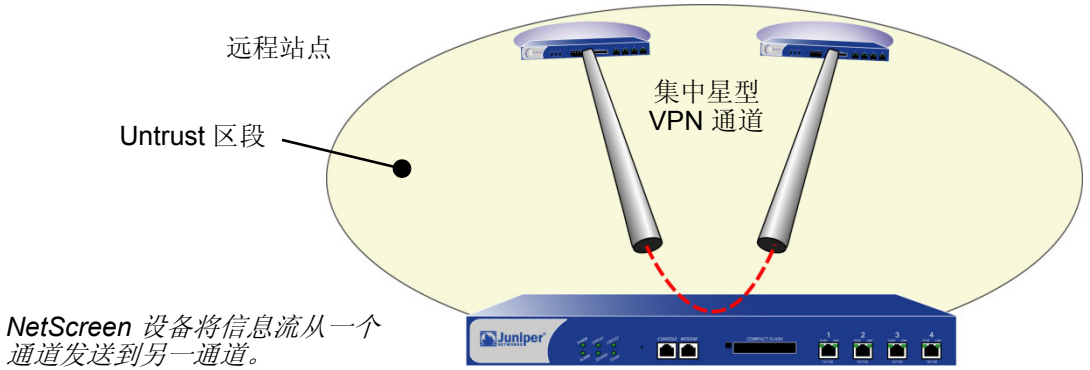
```
set policy top from x1 to x2 "Tokyo LAN" "Paris LAN" any permit[25]
set policy top from x2 to x1 "Paris LAN" "Tokyo LAN" any permit
save
```

24. 在 NetScreen 设备上配置用以保护东京和巴黎办事处的 VPN 通道时，请执行以下操作之一：
(基于路由的 VPN) 输入以下命令：**set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24** (东京) 和 **set vpn VPN1 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24** (巴黎)。
(基于策略的 VPN) 在 Trust 区段通讯簿中生成 10.10.1.0/24 (东京) 和 10.20.1.0/24 (巴黎) 的条目，在 Untrust 区段通讯簿中生成 10.20.1.0/24 (东京) 和 10.10.1.0/24 (巴黎) 的条目。使用它们作为策略中的源和目标地址，这些策略将引用到中心站点的 VPN 通道。

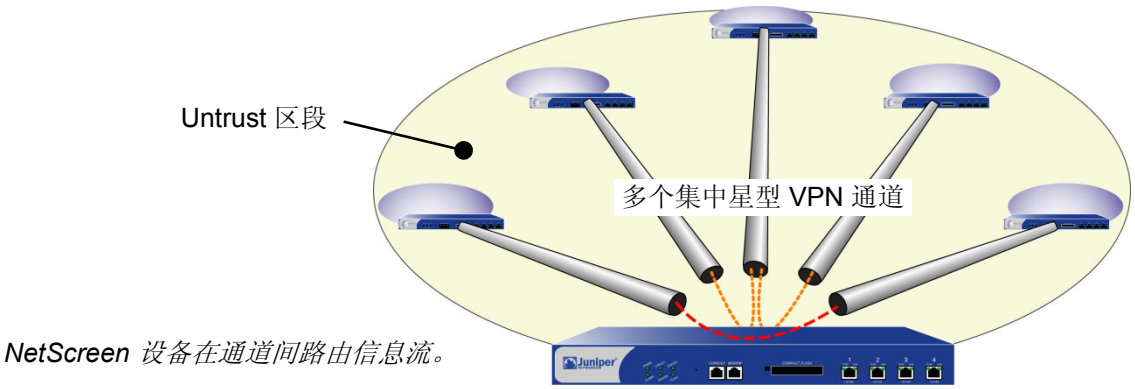
25. 以下消息可以忽略，该消息是由于通道接口处于 NAT 模式才出现的：*Warning: Some interfaces in the <zone_name> zone are in NAT mode. Traffic might not pass through them!*

集中星型 VPN

如果创建两个在 NetScreen 设备处终止的 VPN 通道，则可设置一对路由，这样， NetScreen 设备即可引导信息流离开一个通道而到达另一通道。如果两个通道都包含在一个单独区段内，则无需创建允许信息流从一个通道到达另一通道的策略。只需定义路由。这种布置就是通常所说的集中星型 VPN。



也可在一个区段内配置多个 VPN，并在任意两个通道之间路由信息流。



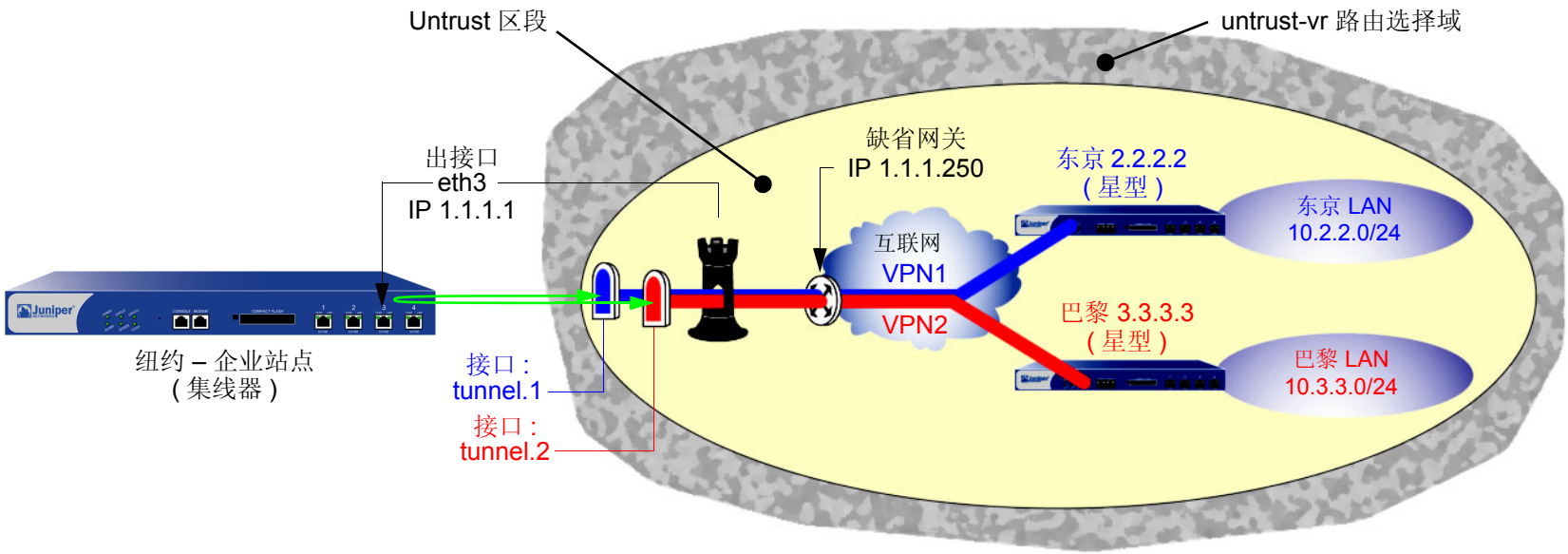
范例：集中星型 VPN

在本例中，东京和巴黎的两个办事处之间通过一对 VPN 通道 VPN1 和 VPN2 进行通信。每个通道都起始于远程站点，终止于纽约的企业站点。位于企业站点的 NetScreen 设备引导信息流离开一个通道而进入另一通道。

在通道间引导信息流时，由于两个远程端点都位于同一区段 (Untrust 区段) 中[26]，因此，通过禁用内部区段阻塞，位于企业站点的 NetScreen 只需进行路由查找，而不必进行策略查找。

将通道绑定到通道接口 tunnel.1 和 tunnel.2，这两个通道均未编号。它们使用 “自动密钥 IKE” 并带有预共享密钥。为阶段 1 和阶段 2 提议选择预定义为 “Compatible” 的安全级别。将 Untrust 区段绑定到 untrust-vr。 Untrust 区段接口为 ethernet3。

注意：*以下配置针对基于路由的 VPN。如果配置基于策略的集中星型 VPN，必须在策略中使用 Trust 和 Untrust 区段而不能使用用户定义的安全区段。*



26. (可选) 也可保留内部区段阻塞处于启用状态，然后定义一个内部区段策略以允许两个通道接口间的信息流。

WebUI (纽约)

1. 安全区段和虚拟路由器

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

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

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

Zone Name: Null

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

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (清除)

2. 接口

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 1.1.1.1/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (选择)

Interface: ethernet3 (untrust-vr)

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

Tunnel Interface Name: tunnel.2

Zone (VR): Untrust (untrust-vr)

Unnumbered: (选择)

Interface: ethernet3 (untrust-vr)

3. 东京办事处的 VPN

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

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: Tokyo

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

Preshared Key: netscreen1

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：

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

4. 巴黎办事处的 VPN

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

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: Paris

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

Preshared Key: netscreen2

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：

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. 路由

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

Network Address / Netmask: 10.3.3.0/24

Gateway: (选择)

Interface: tunnel.2

Gateway IP Address: 0.0.0.0

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: ethernet3

Gateway IP Address: 1.1.1.250

WebUI (东京)

1. 安全区段和虚拟路由器

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

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

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

Zone Name: Null

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

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (选择)

2. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.2.2.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 2.2.2.2/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (选择)

Interface: ethernet3 (untrust-vr)

3. 地址

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

Address Name: Paris

IP Address/Domain Name:

IP/Netmask: (选择), 10.3.3.0/24

Zone: Untrust

4. VPN

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

VPN Name: VPN1

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: New York

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen1

Security Level: Compatible

Outgoing Interface: ethernet3

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

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. 路由

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

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (选择); untrust-vr

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: ethernet3

Gateway IP Address: 2.2.2.250

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

Network Address / Netmask: 10.3.3.0/24

Gateway: (选择)

Interface: tunnel.1

Gateway IP Address: 0.0.0.0

6. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Paris

Service: ANY

Action: Permit

WebUI (巴黎)

1. 安全区段和虚拟路由器

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

IP Address/Netmask: 0.0.0.0/0

Manage IP: 0.0.0.0

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

Zone Name: Null

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

Virtual Router Name: untrust-vr

Block Intra-Zone Traffic: (选择)

2. 接口

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

Zone Name: Trust

Static IP: (出现时选择此选项)

IP Address/Netmask: 10.3.3.1/24

选择以下内容，然后单击 **OK**:

Interface Mode: NAT

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

Zone Name: Untrust

Static IP: (出现时选择此选项)

IP Address/Netmask: 3.3.3.3/24

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

Tunnel Interface Name: tunnel.1

Zone (VR): Untrust (untrust-vr)

Unnumbered: (选择)

Interface: ethernet3 (untrust-vr)

3. 地址

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

Address Name: Tokyo

IP Address/Domain Name:

IP/Netmask: (选择), 10.2.2.0/24

Zone: Untrust

4. VPN

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

VPN Name: VPN2

Security Level: Compatible

Remote Gateway: Create a Simple Gateway: (选择)

Gateway Name: New York

Type: Static IP: (选择), Address/Hostname: 1.1.1.1

Preshared Key: netscreen2

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：

Proxy-ID: (选择)

Local IP / Netmask: 0.0.0.0/0

Remote IP / Netmask: 0.0.0.0/0

Service: ANY

5. 路由

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

Network Address / Netmask: 0.0.0.0/0

Next Hop Virtual Router Name: (选择); untrust-vr

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: ethernet3

Gateway IP Address: 3.3.3.250

Network > Routing > Routing Entries > untrust-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

6. 策略

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

Source Address:

Address Book Entry: (选择), Any

Destination Address:

Address Book Entry: (选择), Tokyo

Service: ANY

Action: Permit

CLI (纽约)

1. 安全区段和虚拟路由器

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
unset zone untrust block
```

2. 接口

```
set interface ethernet3 zone untrust
set interface ethernet3 ip 1.1.1.1/24
set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set interface tunnel.2 zone untrust
set interface tunnel.2 ip unnumbered interface ethernet3
```

3. 东京办事处的 VPN

```
set ike gateway Tokyo address 2.2.2.2 outgoing-interface ethernet3 preshare
    netscreen1 sec-level compatible
set vpn VPN1 gateway Tokyo 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. 巴黎办事处的 VPN

```
set ike gateway Paris address 3.3.3.3 outgoing-interface ethernet3 preshare
    netscreen2 sec-level compatible
set vpn VPN2 gateway Paris 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
```

5. 路由

```
set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.2
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250
save
```

CLI (东京)

1. 安全区段和虚拟路由器

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
```

2. 接口

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

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

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. 地址

```
set address untrust Paris 10.3.3.0/24
```

4. VPN

```
set ike gateway "New York" address 1.1.1.1 outgoing-interface ethernet3
    preshare netscreen1 sec-level compatible
set vpn VPN1 gateway "New York" 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
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.250
set vrouter untrust-vr route 10.3.3.0/24 interface tunnel.1
```

6. 策略

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

CLI (巴黎)

1. 安全区段和虚拟路由器

```
unset interface ethernet3 ip
unset interface ethernet3 zone
set zone untrust vrouter untrust-vr
```

2. 接口

```
set interface ethernet1 zone trust
set interface ethernet1 ip 10.3.3.1/24
set interface ethernet1 nat

set interface ethernet3 zone untrust
set interface ethernet3 ip 3.3.3.3/24

set interface tunnel.1 zone untrust
set interface tunnel.1 ip unnumbered interface ethernet3
```

3. 地址

```
set address untrust Tokyo 10.2.2.0/24
```

4. VPN

```
set ike gateway "New York" address 1.1.1.1 outgoing-interface ethernet3
    preshare netscreen2 sec-level compatible
set vpn VPN2 gateway "New York" sec-level compatible
set vpn VPN2 bind interface tunnel.1
set vpn VPN2 proxy-id local-ip 0.0.0.0/0 remote-ip 0.0.0.0/0 any
```

5. 路由

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 3.3.3.250
set vrouter untrust-vr route 10.2.2.0/24 interface tunnel.1
```

6. 策略

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

索引

J

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z