NetScreen 概念与范例

ScreenOS 参考指南

第 4 卷 : VPN

ScreenOS 4.0.0

编号 093-0522-000-SC

版本 F

Copyright Notice

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

FCC Statement

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

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

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

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

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

Disclaimer

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

目录

前言

对企业来说，虚拟专用网 (VPN) 是一种具有成本效益的安全方法，它为用户提供对企业网的拨号访问，以及远程网在互联网上的互相通信。通过 “互联网” 的安全秘密连接比专线连接更具有成本效益。 NetScreen 设备为安全的 LAN 到 LAN，以及为拨号到 LAN 的 VPN 应用程序提供了所有 VPN 功能。

第 4 卷，“VPN” 说明在 NetScreen 设备上可用的 VPN 功能，包括与 VPN 通道有关的 “互联网协议安全性 (IPsec)” 、“公开密钥基础 (PKI)” 环境下的证书及证书撤消列表 (CRLs)、基于路由的 VPN、基于策略的 VPN 以及 “Layer 2 （第 2 层）通道协议 (L2TP)” 等。本卷还有一些例子，其中包括配置通道接口、基于路由的 VPN、基于策略的 VPN、 L2TP，以及 IPSec 上的 L2TP。

约定

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

WebUI 导航约定

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

范例：Objects > Addresses > List > New

要访问 new address configuration 对话框，请执行以下操作：

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

CLI 约定

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

相关性定义符

每个语法说明中将介绍使用特殊字符来显示命令功能之间的相关性。

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

嵌套的相关性

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

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

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

以下例子说明一些 **set interface** 命令功能的相关性。

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

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

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

CLI 命令及功能的可用性

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

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

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

NETSCREEN 文档

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

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

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

1

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 的简介”的后续内容，本章的其余部分将说明 IPSec 的以下各要素：

VPN 的简介

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。在这两点间流动的流量流经共享的资源，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，则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 地址以及使用的安全协议 （“认证包头 (AH)” 或 “封装安全性负荷 (ESP)”）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）
- 发送方认证和认可 （如果使用证书）（通过数据初始认证）

根据所需采用安全功能。如果仅需认证 IP 封包来源和内容的完整性，您可以不申请任何密码而认证此封包。但是，如果仅想保护私密性，您可以不申请任何认证机制而对此封包加密。如果您愿意，您可以同时加密和认证此封包。大多数网络安全设计者都选择加密、认证，以及对其 VPN 流量进行回放攻击保护。

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
- 使用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”）。它仅是指 IPSec 连接。

IPSEC 概念

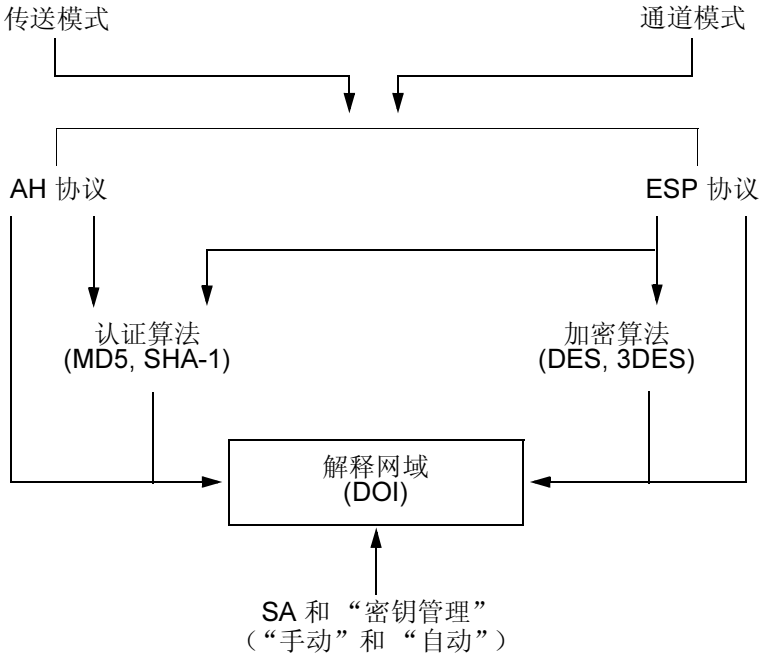
“IP 安全性 (IPSec)”是一系列用于在 IP 封包层处用密码保护通信的相关协议。 IPSec 由两种模式和两种主要协议组成：

- 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



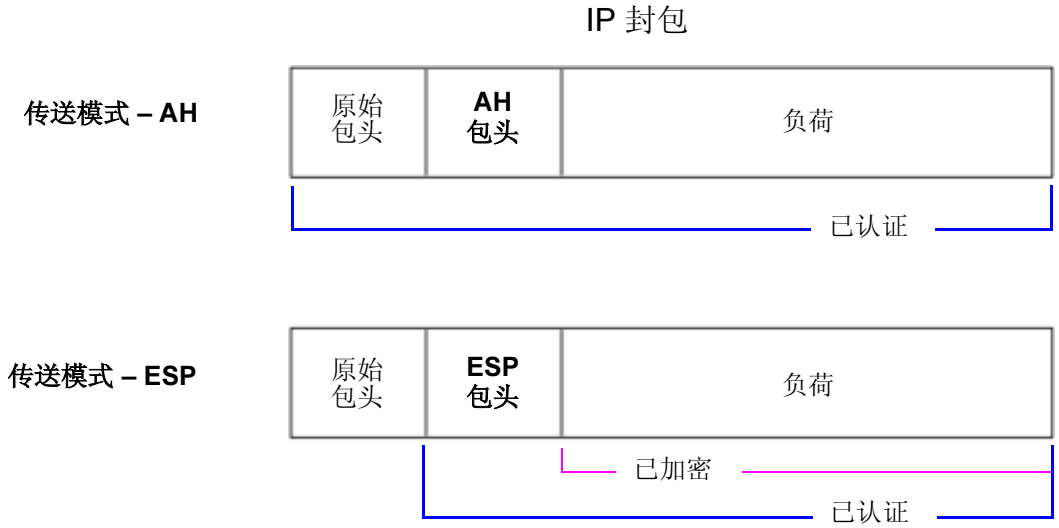
注意：IPSec “解释网域 (DOI)” 是一个文档，该文档中包含要求用于 VPN 通道成功协商的所有安全性参数定义，特别是要求用于 SA 和 IKE 协商的所有属性。

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。

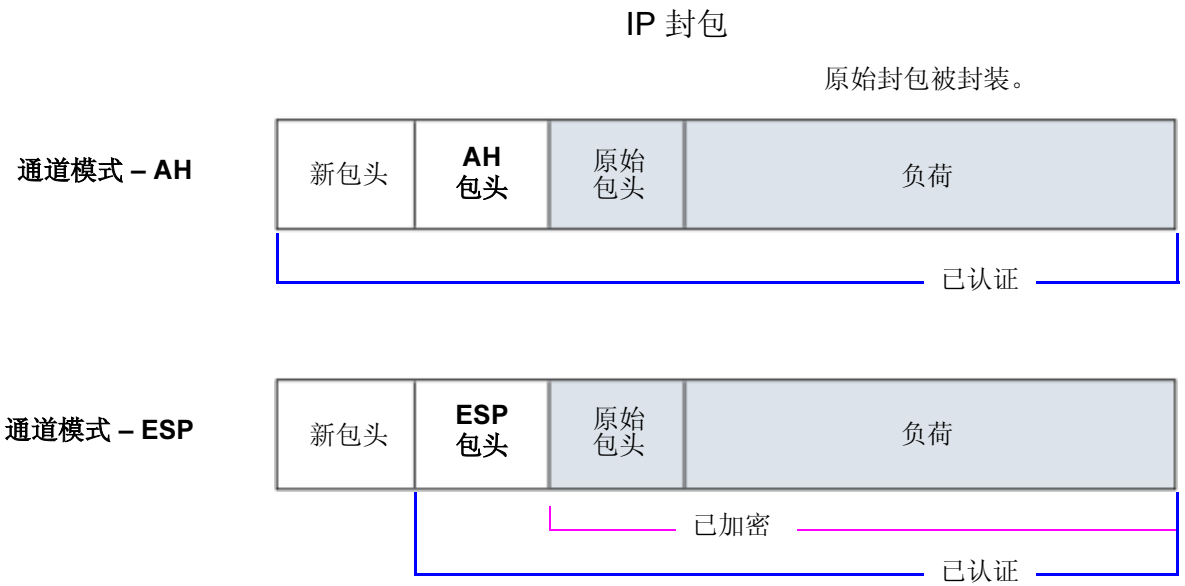
传送模式

原始 IP 封包没有封装在另一个 IP 封包中。整个封包都可以认证 （使用 AH），负荷可以加密 （使用 ESP），原始包头仍保留通过 WAN 发送的明文。



通道模式

整个原始 IP 封包 （负荷和包头）都封装在另一个 IP 负荷中，并且附加了新包头。整个原始封包可以被加密、被认证、或者既加密又认证。利用 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 LAN 到 LAN 的 VPN 中，新包头中使用的源地址和目标地址是外向接口（NAT 或“路由器”模式下）的 IP 地址，或是 VLAN1 IP 地址 （“透明”模式下）；已封装封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 LAN 到 LAN VPN

在拨号到 LAN 的 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本身。在这种情况下，在发送到拨号客户端的封包上，新包头和已封装的原始包头具有相同的 IP 地址：即客户的计算机的地址。

通道模式下拨号到 LAN 的 VPN

协议

IPSec 使用两种协议以保护 IP 层的通信：

- 认证包头 (AH) — 认证 IP 封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 封包 （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 / 完整性以及封包来源的方法。可以通过校验和来认证此封包，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。

“信息整理”版本 5 (MD5) — 从任意长度信息和 16 字节密钥生成 128 位散列（也称作数字签名或信息整理）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和完整性。

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 封包 （包头和负荷），然后将新的 IP 包头附加到刚加密的封包上。新 IP 包头中包含有需要通过网络路由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，在其中应用了三次原始 DES 算法。 DES 的性能更好，但是对于许多绝密或机密资料传输却认为它不可接受。

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。 AES 版本使用 128 位密钥。

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[2]。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，一旦分配密钥后，“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，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。

2. 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”）同时获得证书 （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)，参与者就可检索对方的公用密钥并验证对方的签名。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 3 章，第 47 页上的 “基于路由的 VPN” 和第 4 章，第 123 页上的 “基于策略的 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，至少必须有两个 SA，每个方向使用一个。

SA 将下列组件组合在一起用于保证通信安全：

- 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 流量，策略将调用有关 VPN 通道的 SA。对于入站流量， NetScreen 设备通过使用以下的三个一组来检查 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。当流量与使用该“手动密钥”通道的策略相匹配时，或当路由器包含此通道时， 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，一个成功的第 1 阶段协商将结束。NetScreen 设备最多支持四个第 1 阶段协商的提议，允许您定义对一系列安全参数的限制程度，从而您才会接受密钥协商。

NetScreen 提供的预定义的第 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进行三个双向信息交换 （总共六条信息）以获取以下服务：

- 第一次交换，（信息 1 和 2）：提出并接受加密和认证算法。
- 第二次交换，（信息 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，（信息 5 和 6）：发送并验证其身份。

在第三次交换信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，发起 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，确认交换，发送发起方的证书 （如果使用证书）。

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 用户使用预定义密钥协商 “自动密钥 IKE” 通道时，必须使用 Aggressive mode （主动模式）。*
注意：拨号 VPN 用户也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[3]
- 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[4]。

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)”）和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，请参阅第 13 页上的“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[4]。

3. “DH 组 1”安全性的优点已经下降， NetScreen 建议不使用它。
4. 如果配置多个（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 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安全参数的限制程度。NetScreen 还提供回放攻击保护功能。使用此功能不需要协商，因为封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）

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。

完全正向保密

“完全正向保密 (PFS)”是一种用于派生出第 2 阶段密钥并与前述密钥无关的方法。此外，第 1 阶段提议将创建密钥（SKEYID_d 密钥），从该密钥中将派生出所有的第 2 阶段密钥。SKEYID_d 密钥可以用最小的 CPU 处理过程生成第 2 阶段密钥。可惜的是，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 阶段通道强制产生新的 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

当有人截取一系列封包并在以后使用该封包大量攻击系统、导致拒绝服务 (DoS)、或获准进入可信任网络时会发生回复攻击。回放攻击保护功能将使 NetScreen 设备检查每一个 IPSec 封包，以查看以前是否接受过此封包。如果封包到达指定的序列范围外， NetScreen 设备将拒绝此封包。

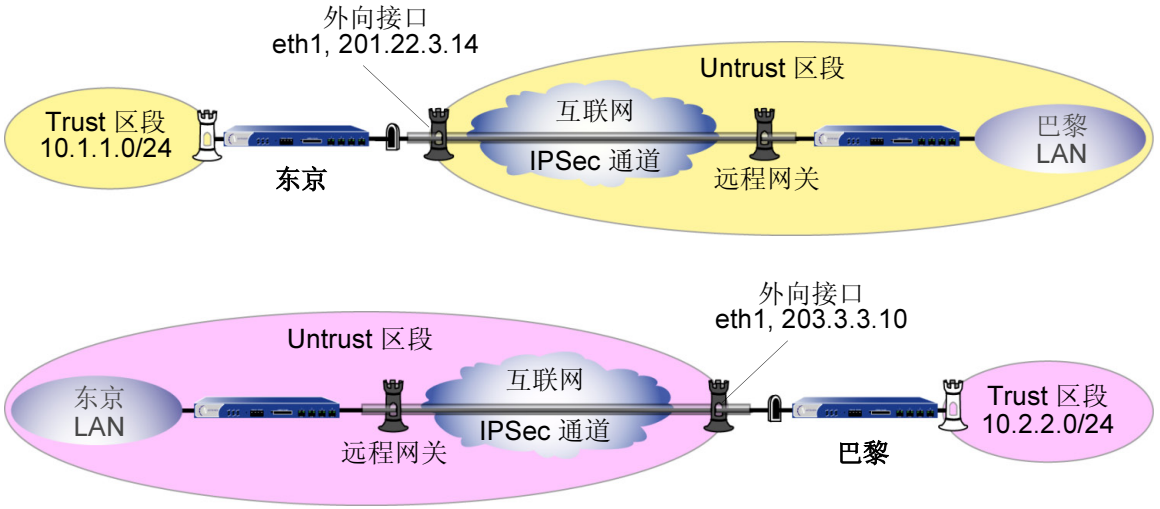
封包流：基于策略的 LAN 到 LAN VPN

要查看各种组件，这些组件彼此相关创建出 IPSec 通道，下列示例将演示封包流过通道的方式。

总部在东京的公司在巴黎新开了一个分部，需要通过 IPSec 通道来连接这两个站点。该通道使用“手动密钥”、ESP 协议、用 3DES 加密以及用 SHA-1 认证。

NetScreen 设备保护的各个站点处于 NAT 模式下。地址如下：

- 东京：
  - 外向接口 （ethernet1， Untrust 区段）：201.22.3.14
  - Trust 区段：10.1.1.0/24
- 巴黎：
  - 外向接口 （ethernet1， Untrust 区段）：203.3.3.10
  - Trust 区段：10.2.2.0/24



封包的路径来自 10.1.1.10，发往 10.2.2.20，通过 IPSec 通道传送，如下所述：

1. 在 10.1.1.0/24 子网上的主机将封包发送到 10.2.2.0/24 子网上的服务器。
2. 封包到达其网关，也就是东京的 Netscreen 设备。
3. 东京的 Netscreen 设备执行以下操作：
   - 它将检查其 “访问控制列表 (ACL)” 并 （使用源地址和目标地址）决定通过 VPN 通道将此封包发送到巴黎的办公室。
   - 它将加密整个封包 （包括原始包头）并赋予此封包新的包头。在外部包头中，源 IP 地址是 201.22.3.14，目标 IP 地址是 203.3.3.10。
   - 它将该封包发送到 203.3.3.10，也就是在巴黎 NetScreen 设备的外向接口 IP 地址。
4. 巴黎的 Netscreen 设备执行以下操作：
   - 使用 SPI、目标 IP 地址、包含在外部封包包头中的 IPSec 协议，它将找到 SA 和密钥。
   - 它将解密此封包，找出其最终目的地。
   - 它将检查 “访问控制列表 (ACL)”，查找准予访问的策略，将此封包转发到其目的地。

IPSec 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 地址用于内部流量，将第二组地址用于外部流量。 NAT 设备从预定义的 IP 地址池中生成这些外部地址。

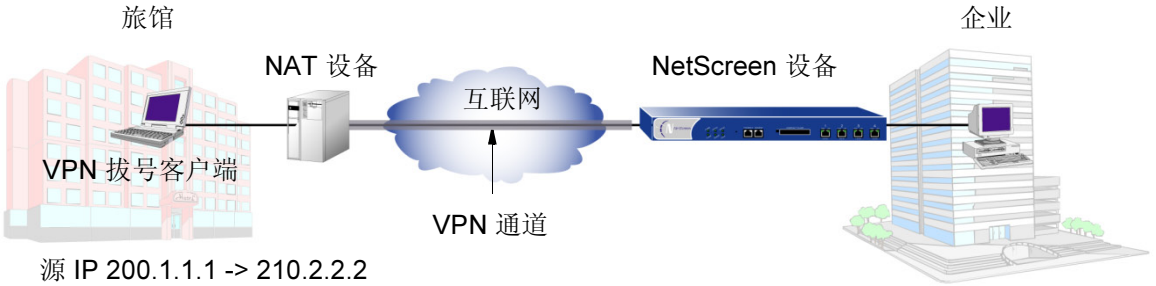
在设置 IPSec 通道时，沿着数据路径出现 NAT 设备不影响第 1 阶段和第 2 阶段的 IKE 协商，它通常将 IKE 封包封装在 “用户数据报协议 (UDP)”封包中。但是，在完成第 2 阶段协商后，执行 IPSec 封包上的 NAT 会导致通道失败。在 NAT 对 IPSec 造成中断的众多原因中[5]，其中一个原因就是，对于 “封装安全性协议 (ESP)”来说， NAT 设备不能识别端口转换的 Layer 4 （第 4 层）包头的位置 （因为它已被加密）。对于 “认证包头 (AH)”协议， NAT 设备可以修改端口号，但不可以修改认证检查，于是对整个 IPSec 封包的认证检查就会失败。

要解决此问题，NetScreen 设备（使用 ScreenOS 3.0.0 或更高版本）和 NetScreen-Remote 客户端（6.0 版本或更高版本）可以应用 NAT 穿透 (NAT-T) 功能。NAT-T 在第 1 阶段交换过程中，沿着数据路径检测完一个或多个 NAT 设备后，将添加一层 UDP 封装。

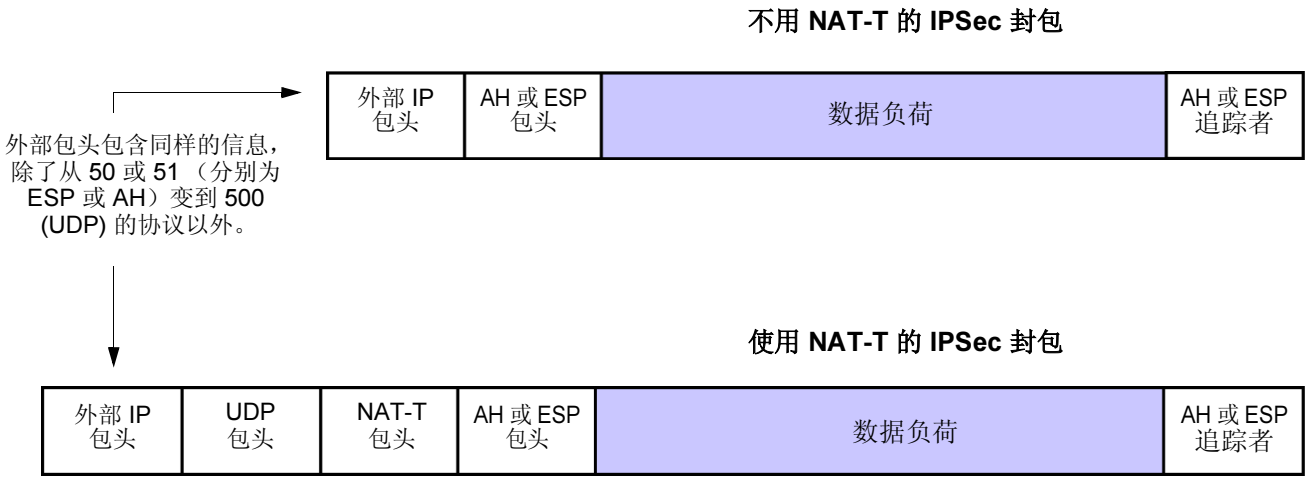
5. 有关 IPSec/NAT 不兼容性的列表，请参阅 Bernard Aboba 所写的 *draft-ietf-ipsec-nat-regts-00.txt*。

穿透 NAT 设备

在以下的图例中，在某旅馆 LAN 周围的 NAT 设备将接收一个来自 VPN 拨号客户的封包，其 IP 地址为 200.1.1.1（由该客户的 ISP 指定）。对于所有出站流量，NAT 设备用新地址 210.2.2.2 替换外部包头中的初始 IP 源地址。在第 1 阶段协商过程中， VPN 客户端和 NetScreen 设备检测是否 VPN 参与者双方都支持 NAT-T， NAT 是否沿着数据路径出现以及它是否位于 VPN 客户端的前部。



将 IPSec 封包封装在 UDP 封包中 （VPN 客户端和 NetScreen 设备都会执行）可以解决认证检查失败的问题。 NAT 设备将其作为 UDP 封包处理，更改 UDP 包头中的源端口，不修改 AH 或 ESP 中的 SPI 包头。 VPN 参与者将剥开 UDP 层并处理 IPSec 封包，这样处理就会通过认证检查，因为对认证过的内容并没有做任何更改。



注意：*启用 NAT-T 时，NetScreen 设备仅在需要时才应用它，也就是当它检测远程主机和 NetScreen 设备间的 NAT 设备存在时才应用它。*

UDP 校验和

所有 UDP 封包都包含一个 UDP 校验和，一个确保 UDP 封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，所以您可能不得不启用此设置。

激活频率值

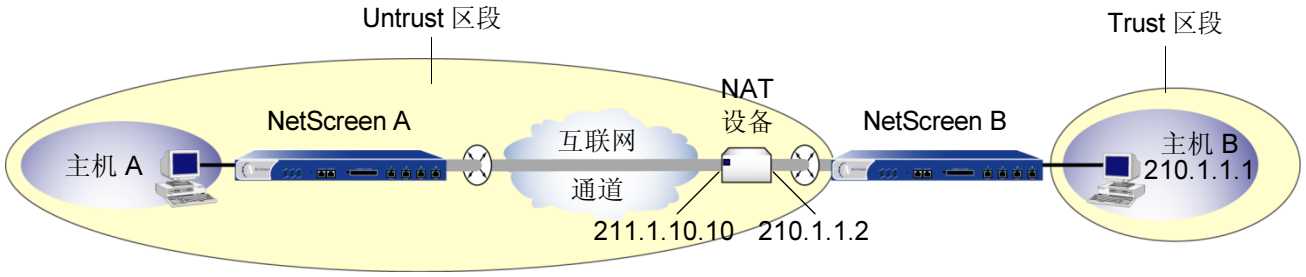
当 NAT 设备将 IP 地址分配给主机时， NAT 设备将确定在没有流量发生时这个新地址可以保持有效的期限。例如，NAT 设备可能会使任何已生成的，保留 20 秒而未使用的 IP 地址无效。因此， IPSec 参与者通常需要通过向 NAT 设备发送定期激活封包 （UDP 封包），这样就不需要更改 NAT 映射，直到第 1 阶段和第 2 阶段的 SA 过期。

注意：*NAT 设备根据制造商和型号的不同，具有不同的会话超时间隔。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。*

IPSec NAT 穿透和发起方 / 响应方对称

当两个 NetScreen 设备在没有 NAT 设备的情况下建立一个通道时，任一个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 设备的后面，就不可能使此类发起方 / 响应方对称。每当 NAT 设备动态生成 IP 地址时就会发生这种情况。

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 在位于 NAT 设备后面的子网中。如果 NAT 设备从 IP 地址池中动态生成新 IP 地址 (210.1.1.1)，NetScreen A 就不能明确地识别出 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）下执行第 1 阶段协商。

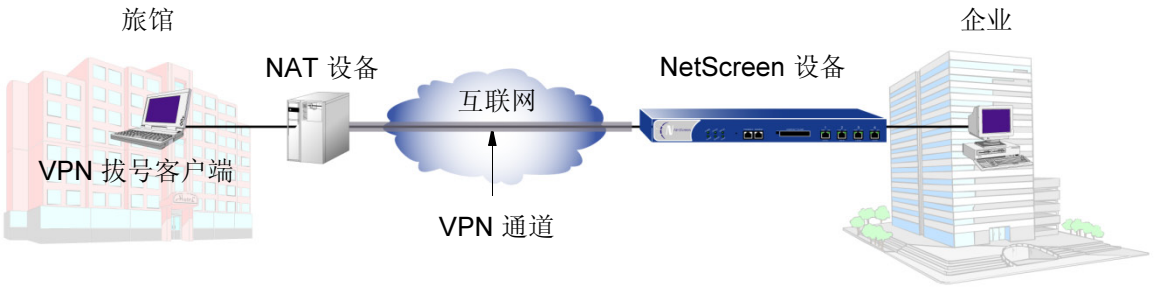
但是，如果 NAT 设备使用映射 IP (MIP) 地址或其它一对一寻址方法生成新的 IP 地址，NetScreen A 就可以明确地识别出 NetScreen B。因此， NetScreen A 或 NetScreen B 都可以是发起方，而且双方都可以使用第 1 阶段的 Main mode （主模式）或 Aggressive mode （主动模式）。

注意：如果在响应方启用 NAT-T 并对其进行配置，以静态对等方身份查看发起方，那么以下类型的对等方就必须使用相同的 P1 提议：

- *具有动态分配 IP 地址的对等方*
- *拨号 VPN 用户*
- *具有静态 IP 地址、已启用了 NAT-T 的对等方*

范例：启用 NAT 穿透

在以下示例中，某旅馆 LAN 周围的 NAT 设备将把一个地址赋给由 Michael Smith （参加会议的销售员）使用的 VPN 拨号客户端。 Michael Smith 要想通过拨号 VPN 通道接入公司的 LAN，就必须启用 NAT-T，以用于在 NetScreen 设备上所配置远程网关 (msmith)，以及在 VPN 拨号客户端配置的远程网关。您还必须启用 NetScreen 设备使传输中包括 UDP 校验和，以及将激活频率设置为 8 秒。



WebUI

VPNs > AutoKey Advanced > Gateway > New：输入在第 3 章，第 47 页上的“基于路由的 VPN”或第 4 章，第 123 页上的“基于策略的 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 **OK** 返回基本 “网关”配置页：

Enable Nat-Traversal: （选择）

UDP Checksum: Enable

Keepalive Frequency: 8

注意：*NetScreen 设备为拨号 VPN 自动启用 NAT 穿透。*

CLI

1. set ike gateway msmith nat-traversal
2. set ike gateway msmith nat-traversal enable-udp-checksum
3. set ike gateway msmith nat-traversal keepalive-frequency 8
4. save

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)。内容分为以下部分：

公开密钥密码术简介

在公开密钥密码术中，公开 / 私有密钥对用来对数据进行加密和解密。用公开密钥 （所有者使其可公开使用）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 想以她的标识来作为消息发送方，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），然后验证签署（由接收方）的过程如下所述：

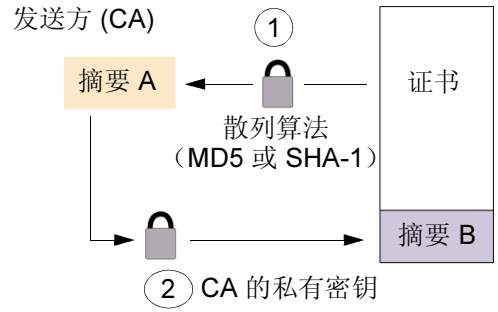
签署证书

1. 发布证书的“证书授权机构 (CA)”用散列算法（SHA-1 或 MD5）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. CA 于是给申请的个人发送数字签署的证书。

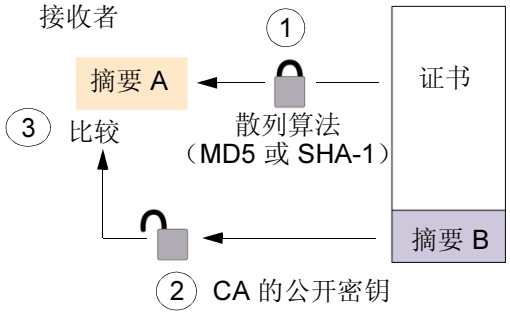
验证数字签名

1. 接收者获得证书后，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. 接收者使用 CA 的公开密钥将数字签名解密。
3. 接收者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，接收者就能确认 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 给申请证书的个人发送数字签署的证书。



1. 接收者使用 MD5 或 SHA-1 从该证书生成摘要 A。
2. 接收者使用 CA 的公开密钥将摘要 B 解密。
3. 接收者将摘要 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。

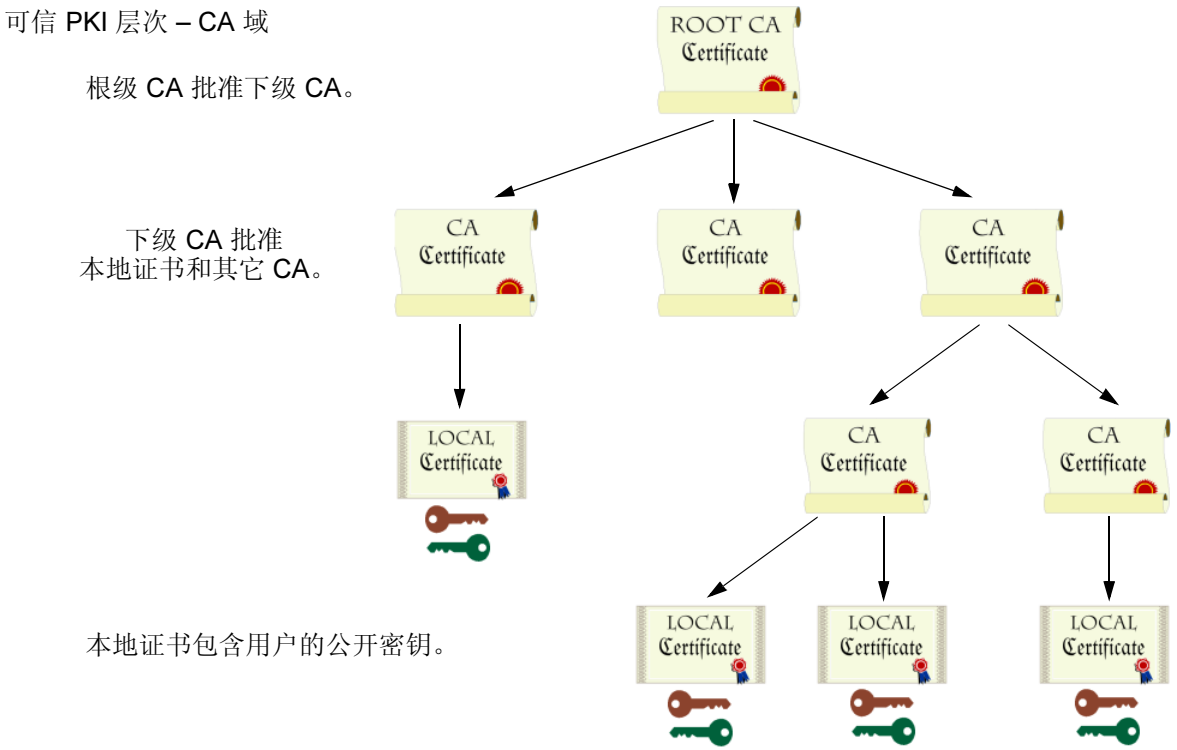


在 IPSec 会话中，两个参与者之间发送数字签署的消息的过程非常相似，以下为不同之处：

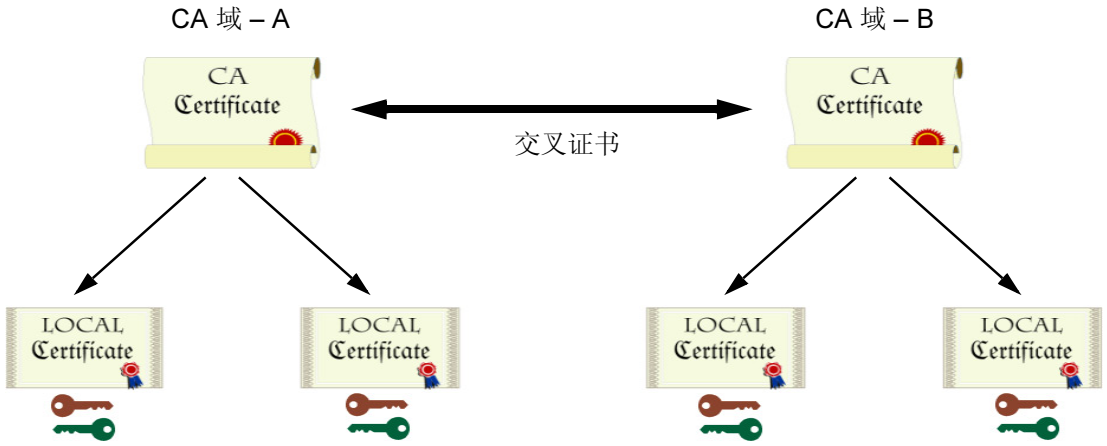
- 发送方不从 CA 证书生成摘要，而是从 IP 封包负荷中的数据生成。
- 参与者不使用 CA 的公开 / 私有密钥对，而是使用发送方的公开 / 私有密钥对。

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 （从将本地证书发回给 CA 域的根权限的 CA 开始）。



如果在一组织内单独使用证书，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 能开发交叉证书。即，他们同意信任对方的权限。在此情况下， PKI 结构水平延伸而不垂直延伸。



由于这些 CA 相互间进行了交叉认证， CA 域 A 中的用户可与 CA 域 B 中的用户一起使用其证书和密钥对。

为方便和实用，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. 提供了文本文件形式的、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）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。关于 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 封套内封包的 CRL[2]。 PKCS #7 支持在单独 PKI 请求内，允许提交多个 X.509 证书。现在，可将 PKI 配置为同时批准所有从发布的 CA 提交的证书。
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

数字证书是一种电子方式，用来通过可信任第三方来验证您的标识，即通常所说的“证书授权机构 (CA)”。使用的 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）拥有并操作。如果使用独立的 CA，必须与之联系，获取 CA 和 CRL 服务器的地址（以便获得证书及证书撤消列表），并获取提交个人证书申请时所需的信息。您即是自己的 CA 时，由您自行确定此信息。

要在建立安全 VPN 连接时使用数字证书来鉴别您的标识，必须先进行以下操作：

- 从 CA 获取个人证书（也即通常所说的*本地*证书），并将此证书加载到 NetScreen 设备上。
- 获取发布个人证书的 CA 的 CA 证书 （主要用来检查验证您的 CA 的身份），并将其加载到 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。
- 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，有几个事件必须能够撤消证书。如果怀疑证书被破坏，或当证书持有者离开公司时，可能希望撤消证书。可在本地完成证书撤消和验证的管理（此为受限制的解决方案），或者参考 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）。

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签署的数字证书，必须按以下顺序完成几项任务：

1. 配置缺省服务器设置。
2. 生成公开 / 私有密钥对。
3. 填写证书申请。
4. 将申请提交到所选 CA。
5. 收到签署的证书后，必须将其与 CA 证书一起加载到 NetScreen 设备中。

现在您拥有用于下列用途中的以下项目：

- NetScreen 设备的本地证书，对每个通道连接验证您的标识
- CA 证书 （其公开密钥），用来验证对等方的证书
- 如果 “证书撤消列表 (CRL)” 包括在 CA 证书[4] 中，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，用以下部分叙述的过程将它们加载到 NetScreen 中。

注意：*如果打算使用电子邮件来提交 PKCS10 文件，以获得证书，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。必须设置主 DNS 服务器和次 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。换句话说， 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：为 CA 证书配置 CRL 设置”中所述。

范例：手动申请证书

申请证书时， NetScreen 设备生成密钥对。公开密钥合并在申请中，并且最终合并在从 CA 收到的数字签署的本地证书中。

下例中，安全管理员为加利福尼亚 Santa Clara 的 NetScreen Technologies 开发部的 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 设备将申请写入一个文件，然后将此文件复制并粘贴到 CA 的证书注册网站中的证书申请文本字段中。完成注册过程后， CA 通常使用电子邮件将证书发送到安全管理员。

注意：*生成证书申请前，请确认已经设置了系统时钟，并将主机名和域名分配给了 NetScreen 设备。（如果 NetScreen 设备在 NSRP 集群中，则用集群名替换主机名。详细信息，请参阅第* ***7****-17 页上的 “集群名称”。）*

WebUI

1. 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: NetScreen Technologies
   County/Locality: Santa Clara
   State: CA
   Country: US
   E-mail: mzhang@netscreen.com[5]

5. 有些 CA 不支持证书中的电子邮件地址。如果在本地证书申请中不包括电子邮件地址，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。可改为使用完全合格的域名 （如果在本地证书中），或者使本地 ID 字段为空。 NetScreen 设备缺省状态下发送其 hostname.domainname （主机名 . 域名）。如果不指定动态对等方的本地 ID，则在对等方 ID 字段中，输入 IPSec 通道另一端设备上的对等方 hostname.domainname。

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，并提示您打开该文件或保存到磁盘上。

2. 打开该文件并复制其内容，小心复制整个文本内容，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-----”。）
3. 按 CA 网站上的证书申请说明，需要时，将 PKCS #10 文件粘贴到适当的字段。
4. 通过电子邮件从 CA 收到证书时，将其复制到文本文件，并保存到您的工作站（随后会通过 WebUI 加载到 NetScreen 设备），或保存到 TFTP 服务器（随后通过 CLI 加载）。

CLI

1. set pki x509 dn country-name US
2. set pki x509 dn email mzhang@netscreen.com
3. set pki x509 dn ip 10.10.5.44
4. set pki x509 dn local-name “Santa Clara”
5. set pki x509 dn name “Michael Zhang”
6. set pki x509 dn org-name “NetScreen Technologies”
7. set pki x509 dn org-unit-name Development
8. set pki x509 phone 408-730-6000
9. set pki x509 dn state-name CA

6. 值 1024 指出密钥对的位长度。如果使用 SSL 的证书 （参阅第 **3**-9 页上的 “安全套接字层”），请确认使用 Web 浏览器支持的位长。

10. set pki x509 default send-to admin@netscreen.com[7]
11. exec pki rsa new-key 1024

    通过电子邮件将证书申请发送到 admin@netscreen.com。

12. 复制申请的内容，小心复制整个文本内容，但不复制文本前后的任何空白。（开始于 “-----BEGIN CERTIFICATE REQUEST-----”，结束于 “-----END CERTIFICATE REQUEST-----”。）
13. 按 CA 网站上的证书申请说明，需要时，将 PKCS #10 文件粘贴到适当的字段。

通过电子邮件从 CA 收到证书时，将其复制到文本文件，并保存到您的工作站（随后会通过 WebUI 加载到 NetScreen 设备），或保存到 TFTP 服务器 （随后通过 CLI 加载）。

7. 使用电子邮件地址，假定已经为 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 为您返回以下三个文件，以加载到 NetScreen 设备：

- CA 证书，包含 CA 的公开密钥
- 确定本地机器的本地证书 （您的公开密钥）
- CRL，列出被 CA 撤消的所有证书

对 WebUI 范例，将文件下载到了管理员工作站上名为 C:\certs\ns 的目录。对 CLI 范例，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）支持从不同的 CA 加载多个本地证书。*

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) 显示在 File Browse 字段中。
3. 单击 **Load**。

   加载了 auth.cer 证书文件。
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) 显示在 File Browse 字段中。

6. 单击 **Load**。

   加载了 auth.cer 证书文件。

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**。

   加载了 distrust.crl CRL 文件。

CLI

1. exec pki x509 tftp 198.168.1.5 cert-name auth.cer
2. exec pki x509 tftp 198.168.1.5 cert-name local.cer
3. exec pki x509 tftp 198.168.1.5 crl-name distrust.crl

范例：为 CA 证书配置 CRL 设置

在阶段 1 协商中，参与者检查 CRL 列表，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，并且未加载到 NetScreen 数据库中，则 NetScreen 设备会尝试通过 LDAP 或 HTTP[8] CRL 位置（在 CA 证书内定义）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。如果没有为特殊的 CA 证书定义 CRL URL， NetScreen 设备会引用缺省 CRL URL 地址的 CRL 服务器。

注意：*加载 CRL 时，可使用 ScreenOS 2.5 及更新版本来禁止对 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

1. Objects > Certificates (Show: CA) > Server Settings（对 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

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

2. 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

1. set pki authority 1 cert-path full
2. set pki authority 1 cert-status crl url “ldap:///CN=Entrust,CN=en2001,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=EN2000,DC=com?CertificateRevocationList?base?objectclass=CRLDistributionPoint”
3. set pki authority 1 cert-status crl server-name 2.2.2.121
4. set pki authority 1 cert-status crl refresh daily
5. set pki authority default cert-path full
6. 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”
7. set pki authority default cert-status crl server-name 10.1.1.200
8. set pki authority default cert-status crl refresh daily
9. 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鉴别您的标识，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 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有要求您在证书间复制信息的步骤，因而其过程可能稍长。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（参阅第* ***2****-370 页上的“域名系统支持”）。*
- *设置系统时钟（参阅第* ***2****-403 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。详细信息，请参阅第* ***7****-17 页上的“集群名称”。）*

范例：自动申请本地证书

在本例中，用自动方法使用 SCEP 从 Verisign CA 申请证书。设置以下 CA 设置：

- 完整证书路径验证
- RA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe[9]
- CA CGI: http://ipsec.verisigncom/cgi-bin/pkiclient.exe
- 三十分钟的轮询时间间隔来检查挂起的证书地址是否就绪
- 自动确认从该 CA 通过 SCEP 收到的证书的完整性
- 过期前十四天通知更新本地证书

然后生成 RSA 密钥对，指定 1024 位的密钥长度，并初始化 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。

9. 对网络服务器来说，“通用网关接口 (CGI)”是将用户申请传递到应用程序和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

CA 服务器设置

1. Objects > Certificates > Show CA > Server Settings（对 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

本地证书申请

2. 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: NetScreen Technologies

   County/Locality: Santa Clara

   State: CA

   Country: US

   Email: mzhang@netscreen.com

   IP Address: 10.10.5.44

   Create new key pair of *1024*[10] length: （选择）

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

NetScreen 设备生成 PKCS #10 文件，并提示执行以下操作之一：

- 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
- 发送该文件到支持 “简单证书注册协议 (SCEP)” 的 CA，以自动注册。

3. 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**。
4. 请与 Verisign 联系，将您的证书申请告知他们。必须在他们授权此证书申请后，您才能下载证书。

CLI

CA 服务器设置

1. set pki authority 1 cert-path full
2. set pki authority 1 scep ca-cgi “http://ipsec.verisign.com/cgi-bin/pkiclient.exe”[11]
3. set pki authority 1 scep ra-cgi “http://ipsec.verisign.com/cgi-bin/pkiclient.exe”[12]
4. set pki authority 1 scep polling-int 30
5. set pki authority 1 scep renew-start 14

本地证书申请

1. set pki x509 dn country-name US
2. set pki x509 dn email mzhang@netscreen.com
3. set pki x509 dn ip 10.10.5.44
4. set pki x509 dn local-name “Santa Clara”
5. set pki x509 dn name “Michael Zhang”
6. set pki x509 dn org-name “NetScreen Technologies”
7. set pki x509 dn org-unit-name Development
8. set pki x509 phone 408-730-6000
9. set pki x509 dn state-name CA
10. exec pki rsa new 1024
11. exec pki x509 scep 1

    如果是从该 CA 申请的第一个证书，会出现一个提示，显示 CA 证书的指纹值。必须与 CA 联系，以确认其为正确的 CA 证书。
12. 请与 Verisign 联系，将您的证书申请告知他们。必须在他们授权此证书申请后，您才能下载证书。

11. 对网络服务器来说，“通用网关接口 (CGI)”是将用户申请传递到应用程序和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。

12. 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。

使用 OCSP 检查撤消

当 NetScreen 设备执行一个使用证书的操作时，可能需要检查过早撤消的证书。检查数字证书撤消状态的缺省方法是使用 CRL。

“在线证书状态协议 (OCSP)”是一种检查数字证书状态的替换方法。 OCSP 能提供关于证书的其它信息。还以更适时的方式提供证书状态。

NetScreen 设备使用 OCSP 时，被称为 *OCSP 客户机*（或*请求方*）。该客户机发送验证请求到称为 *OCSP 响应方*的服务器设备中。客户机的请求包含要检查的证书标识。必须在将其配置为能够识别 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，然会将当前状态返回给客户机。除了证书的撤消状态之外，生成的响应还包括响应方的名称，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，响应方使用响应方私有密钥来签署响应。 OCSP 客户机验证响应信号的正确性。

配置 OCSP

可使用 CLI 命令来配置 NetScreen 设备，使其支持 OCSP 操作。多数 CLI 命令使用识别号码，将撤消参考 URL 与 CA 证书关联。可使用以下 CLI 命令来获取此 ID 号：

```
ns-> 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，可更改此号码。*

指定 CRL 或 OCSP 以用于撤消检查

要为特殊 CA 的证书指定撤消检查方法 （CRL、 OCSP、使用这两种方法或不使用这两种方法），请使用以下 CLI 语法：

ns-> **set pki authority** *id_num* **cert-status revoc { CRL | OCSP | all | none }**

其中， *id_num* 是证书的识别号码。

以下范例指定 OCSP 撤消检查。

ns-> **set pki authority 3 cert-status revocation-check ocsp**

ID 号 3 识别该 CA 的证书。

显示证书撤消状态属性

要显示特殊 CA 的撤消检查属性，请使用以下 CLI 语法：

ns-> **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 的撤消状态属性，请使用以下语法：

ns-> **get pki authority 7 cert-status**

指定证书的 “OCSP 响应方” URL

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

ns-> **set pki authority** *id_num* **cert-status ocsp url** *url_str*

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

ns-> **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：

ns-> **unset pki authority 5 cert-status ocsp url http:\\192.168.2.1**

删除证书撤消检查属性

要删除 CA （发布了特殊证书）的所有与证书撤消检查相关的属性，请使用以下语法：

ns-> **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：

ns-> **unset pki authority 1 cert-status**

3

基于路由的 VPN

虚拟专用网 (VPN) 支持的 NetScreen 设备的配置非常灵活。在 3.1.0 之前的 ScreenOS 版本中， VPN 通道被当作对象 （或构件块），与源、目标、服务和动作一起，组成允许 VPN 流量的策略。（实际上， VPN 策略动作是 **tunnel（通道）**，但如果未申明，则暗指动作 **permit（允许）**。）在 ScreenOS 3.1.0 中， VPN 通道的概念发生了变化。除[1]之前作为对象来构建策略的通道概念外 （请参阅第 4 章，第 123 页上的 “基于策略的 VPN”），也可将通道作为用来传送流量的网络资源。因此，可将一个通道当作在点 A 和点 B 之间传输流量的方法，同时将一个策略当作允许或拒绝传送该流量的方法。简单地说， ScreenOS 给了您消除流量与其传输方式间的相互影响的自由。

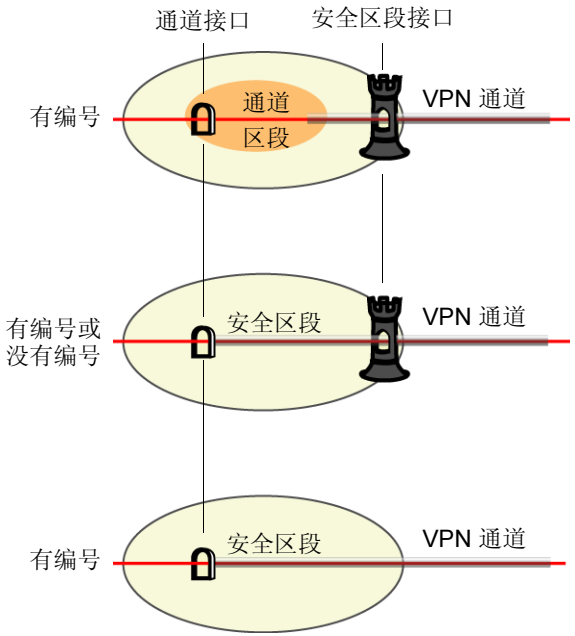
本章概述并提供以下基于路由的 VPN 概念的范例：

1. 3.1.0 之后的 ScreenOS 版本继续支持 ScreenOS 3.1.0 之前的 VPN 配置概念和方法。

通道接口

配置 VPN 通道的远程网关的同时，还必须将一个安全区段接口指定为本地网关[2]。在 VPN 通道终止点（本地和远程网关）上，也可在安全区段或 Tunnel 区段中配置通道接口，NetScreen 设备通过该接口引导流量出入 VPN 通道[3]。在安全区段内，可将 VPN 通道绑定到一个有具体编号（具有 IP 地址 / 网络掩码）或没有编号（没有 IP 地址 / 网络掩码）的通道接口。如果通道接口没有编号，它从安全区段（在其中创建了它）接口借用 IP 地址。现在，就拥有了同时绑定到通道接口和本地安全区段接口的 VPN 通道。

从概念上讲，可将 VPN 通道当作铺设的管道。它们从本地设备延伸到远程网关，而通道接口就是这些管道的开口。管道始终存在，只要路由引擎将流量引导到接口之一就可随时使用。



当有编号的通道接口在 Tunnel 区段内时，则不能将 VPN 通道绑定到该通道接口。只能将一个通道绑定到该 Tunnel 区段。这就允许将多个通道接口链接到一个单独通道，或将多个通道链接到一个单独通道接口。在这种情况下，必须创建一个基于策略的 VPN 配置。

当通道接口在一个安全区段内时，必须将一个 VPN 通道绑定到该通道接口。这样就允许创建基于路由的 VPN 配置。

通道接口有无编号均可。如果没有编号，则通道接口从安全区段接口借用 IP 地址。注意：只有带编号的通道接口（即具有 IP 地址和网络掩码的接口）才能支持基于策略的 NAT。

当有编号的通道接口在安全区段内并且是该区段内的唯一接口时，就不需要创建安全区段接口。在此情况下，安全区段支持通过通道接口的 VPN 流量，但不支持其它类型的流量。

2. 在 IKE 对等方的 NetScreen 设备上配置远程网关时，对等方使用本地网关接口（或外向接口）的 IP 地址。
3. 如果没有指定一个通道接口，则通道为安全区段使用缺省接口。

通常，如果希望接口支持基于策略的 NAT，请为该通道接口指派一个 IP 地址。有关 VPN 和基于策略的 NAT 的详细信息，请参阅第 202 页上的 “Tunnel 区段和基于策略的 NAT”。可以在 Tunnel 区段或安全区段内创建一个有编号的通道接口。

如果通道接口不需要支持基于策略的 NAT，并且配置不要求将通道接口绑定到一个 Tunnel 区段，则可以将该接口指定为无编号 (Unnumbered)。必须将一个没有编号的通道接口绑定到安全区段；同时不能将其绑定到 Tunnel 区段。还必须指定一个绑定到该安全区段 （其 IP 地址被无编号 (Unnumbered) 的通道接口借用）的接口。

注意：*指定的安全区段接口必须位于已将通道接口绑定到其中的同一区段中。*

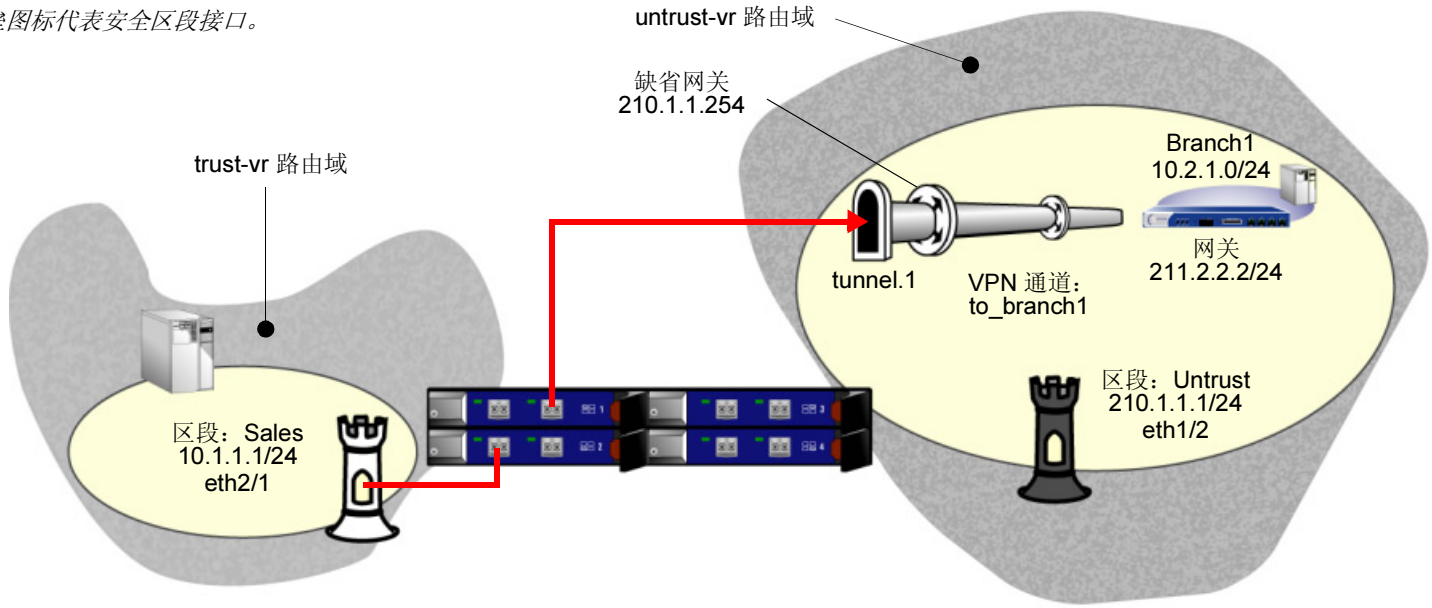
范例：绑定到通道接口的通道

在本范例中配置一个企业网站和分公司之间的 VPN 通道。该通道具有以下特征：

- 该 VPN 通道被绑定到一个命名为 *tunnel.1 的通道接口。*
- Untrust 区段被绑定到 untrust-vr，而非 trust-vr。
- 自动密钥 IKE VPN 使用预共享密钥 (netscreen1)、Main mode （主模式），并且建议将 “阶段 1” 和 “阶段 2” 的安全级别预定义为 “Compatible”。
- 企业网站上指定为本地网关的接口为 210.1.1.1。（分公司将该地址用作其 IKE 配置中的远程网关。）
- 企业网站上的 NetScreen 设备运行 ScreenOS 4.0.0。
- 远程站点上的 NetScreen 设备运行早于 3.1.0 版本的 ScreenOS。

注意：*下面仅提供通道的企业端配置。有关配置运行 USGA 之前 ScreenOS 的 NetScreen 设备的详细信息，请参阅* NetScreen 概念与范例 ScreenOS *参考指南，了解适合设备使用的 ScreenOS 版本。*

注意：堡垒图标代表安全区段接口。



NetScreen 设备将封装 VPN 流量
发送到充当缺省网关的外部路由器。

WebUI

安全区段和虚拟路由器

1. Network > Interfaces > Edit（对 ethernet1/2）：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

2. Network > Interfaces > Edit（对 ethernet1/2）：输入以下内容，然后单击 **OK**：

   Zone Name: Null

3. Network > Zones > Edit（对 Untrust）：在 Virtual Routers Name 下拉列表中，选择 **untrust-vr**，然后单击 **OK**。

4. Network > Interfaces > Edit（对 ethernet1/2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
5. Network > Zones > New：输入以下内容，然后单击 **OK**：
   Name: Sales
   Virtual Router Name: trust-vr

接口 – 区段和通道

6. Network > Interfaces > Edit（对于 ethernet2/1）：输入以下内容，然后单击 **OK**：
   Zone Name: Sales
   IP Address/Netmask：10.1.1.1/24
7. Network > Interfaces > Edit（对于 ethernet1/2）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24
8. Network > Interfaces > Tunnel IF New：输入以下内容，然后单击 **OK**：
   Interface Name: tunnel.1
   Zone: Untrust
   Unnumbered: （选择）
   Interface: ethernet1/2(Untrust)[4]

4. 源接口必须处于绑定通道接口的同一区段内；在本例中为 Untrust 区段。没有编号的通道接口借用指定安全区段接口的 IP 地址。

VPN

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

   VPN Name: to_branch1

   Security Level: Compatible

   Remote Gateway: Create a Simple Gateway: （选择）

   Gateway Name: branch1

   Type: Static IP （选择）, IP Address: 211.2.2.2

   Preshared Key: netscreen1

   Security Level: Compatible

   Outgoing Interface: ethernet1/2[5]

   > 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

   Replay Protection: （选择）

   Bind To: Tunnel Interface: tunnel.1

   Proxy-ID: （选择）

   Local IP/Netmask: 10.1.1.0/24

   Remote IP/Netmask: 10.2.1.0/24

   Service: ANY

5. 外向接口不必位于绑定通道接口的同一区段内。

地址

10. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
    Address Name: sales-any
    IP Address/Domain Name:
    IP/Netmask: （选择）, 10.1.1.0/24
    Zone:Sales
11. 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）, 10.2.1.0/24
    Zone: Untrust

路由

12. Network > Routing > Route Table > 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
13. Network > Routing > Route Table > untrust-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

14. Network > Routing > Route Table > 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: ethernet1/2(untrust-vr)

    Gateway IP Address: 210.1.1.254[6]

注意：由于 Sales 区段 (eth2/1) 的接口处于“路由”模式， NetScreen 设备将在 untrust-vr 路由表中自动为其建立一个条目。因此不必手动输入一个条目。

策略

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

    Source Address: Address Book: sales-any

    Destination Address: Address Book: branch1

    Service: ANY

    Action: Permit

    Position at Top: （选择）

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

    Source Address: Address Book: branch1

    Destination Address: Address Book: sales-any

    Service: ANY

    Action: Permit

    Position at Top: （选择）

6. 对于出站 VPN 和网络流量，设置到指定为缺省网关的外部路由器的路由至关重要。在本范例中， NetScreen 设备将封装 VPN 流量发送到此路由器，作为它到远程对等方网关的第一次跳跃。在本范例的图解中，通过对经过该路由器的通道的描述介绍此概念。

CLI

安全区段和虚拟路由器

1. unset interface ethernet1/2 ip
2. unset interface ethernet1/2 zone
3. set zone untrust vrouter untrust-vr
4. set zone name sales trust-vr

接口 – 区段和通道

5. set interface ethernet2/1 zone sales
6. set interface ethernet2/1 ip 10.1.1.1/24
7. set interface ethernet1/2 zone untrust
8. set interface ethernet1/2 ip 210.1.1.1/24
9. set interface tunnel.1 zone untrust
10. set interface tunnel.1 ip unnumbered interface eth1/2

VPN

11. set ike gateway branch1 ip 211.2.2.2 outgoing-interface ethernet1/2 preshare netscreen1 sec-level compatible
12. set vpn to_branch1 gateway branch1 replay sec-level compatible
13. set vpn to_branch1 bind interface tunnel.1
14. set vpn to_branch1 proxy-id local-ip 10.1.1.0/24 remote-ip 10.2.1.0/24 any

地址

15. set address sales sales-any 10.1.1.0/24
16. set address untrust branch1 10.2.1.0/24

路由

17. set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
18. set vrouter untrust-vr route 10.2.1.0/24 interface tunnel.1
19. set vrouter untrust-vr route 0.0.0.0/0 interface ethernet1/2 gateway 210.1.1.254

> ***注意：****由于 Sales 区段 (ethernet2/1) 的接口处于“路由”模式， NetScreen 设备将在 untrust-vr 路由表中自动为其建立一个条目。因此不必手动输入一个条目。*

策略

20. set policy top from sales to untrust sales-any branch1 any permit
21. set policy top from untrust to sales branch1 sales-any any permit
22. save

删除通道接口

不能立即删除拥有映射 IP 地址 (MIP)、虚拟 IP 地址 (VIP) 或 “动态 IP (DIP)” 地址池的通道接口。删除拥有这些特征的通道接口前，必须首先删除引用它们的所有策略。然后必须删除通道接口上的 MIP、VIP 和 DIP 池。如果基于路由的 VPN 配置引用一个通道接口，则必须首先删除 VPN 配置，再删除通道接口。

范例：删除通道接口

在本范例中，通道接口 tunnel.2 被链接到 DIP 池 8。从 Trust 区段到 Untrust 区段的 VPN 流量的策略引用 DIP 池 8。要删除该通道接口，必须首先删除该策略 （或从该策略中删除引用的 DIP 池 8），然后依次删除 DIP 池和接口。

WebUI

1. Policies (From: Trust, To: Untrust): 单击策略 ID 10 的 **Remove**。
2. Network > Interfaces > Edit（对于 tunnel.2）> DIP: 单击 DIP ID 8 的 **Remove**。
3. Network > Interfaces: 单击 tunnel.2 的 **Remove**。

CLI

1. unset policy 10
2. unset interface tunnel.2 dip 8
3. unset interface tunnel.2
4. save

LAN 到 LAN 的 VPN

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，可配置以下各种通道：

- LAN 到 LAN 的 VPN，手动密钥通道
- LAN 到 LAN 的 VPN，自动密钥 IKE 通道 （具有预共享密钥或证书）

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，可配置以下各种通道：

- 动态对等 LAN 到 LAN 的 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 LAN 到 LAN 的 VPN 包括一个连接两个 LAN 的 IPSec 通道，每个 LAN 都拥有一个作为安全网关的 NetScreen 设备。在两个设备上用作外向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，则使用 VLAN1 地址。（请参阅第 59 页上的“范例：基于路由的 LAN 到 LAN 的 VPN，手动密钥”和第 70 页上的“范例：基于路由的 LAN 到 LAN 的 VPN，自动密钥 IKE”。）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可使用静态 LAN 到 LAN 的 VPN 发起 VPN 通道设置。

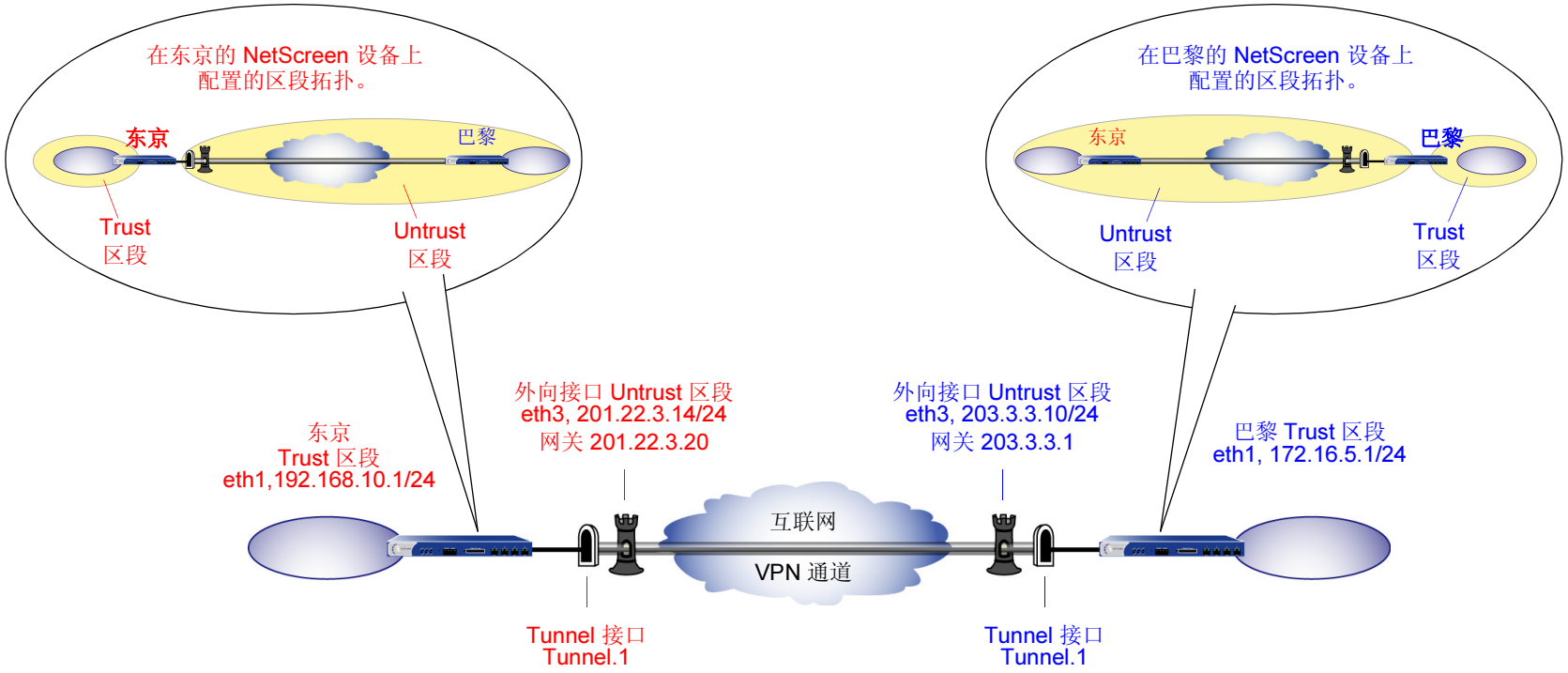
如果其中一个 NetScreen 设备的外向接口具有动态分配的 IP 地址，则该设备在术语上被称为“动态对等方”，并且具有不同的 VPN 配置。（请参阅第 76 页上的“范例：基于路由的 LAN 到 LAN 的 VPN，动态对等方”。）由于只有那些位于动态对等方后面的主机的远程网关才有固定的 IP 地址，并且可以从它们的本地网关到达，因此只有它们才能使用动态对等 LAN 到 LAN 的 VPN 发起 VPN 通道设置。但是，当在动态对等方和静态对等方之间的一个通道设置完成后，如果目标主机有固定的 IP 地址，则任一网关后面的主机都可以发起 VPN 流量。

范例：基于路由的 LAN 到 LAN 的 VPN，手动密钥

在本例中，使用建议将阶段 1 和阶段 2 的安全级别预定义为 “Compatible” 的方法，“手动密钥” 通道在东京和巴黎的分公司之间提供了安全信道。每个站点的 Trust 区段都处于 NAT 模式。地址如下：

- 东京：
  - Trust 接口 (ethernet1)：192.168.10.1/24
  - Untrust 接口 (ethernet3)：201.22.3.14/24
- 巴黎：
  - Trust 接口 (ethernet1)：172.16.5.1/24
  - Untrust 接口 (ethernet3)：203.3.3.10/24

Trust 和 Untrust 安全区段，以及 “Untrust_Tun” 通道区段都在 trust-vr 路由域中。 Untrust 区段接口 (ethernet3) 作为 VPN 通道的外向接口。



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 区段内指定其外向接口，将其绑定到通道接口，并配置其 Proxy ID。
3. 在 Trust 和 Untrust 地址通讯簿中输入本地及远程端点的 IP 地址。
4. 输入从 Trust-VR 到 Untrust-VR 的缺省路由、到 Untrust-VR 中外部路由器的缺省路由以及通过通道接口到达目的地的路由。
5. 为每个站点间通过的 VPN 流量设置策略。

WebUI (东京)

接口 – 安全区段和通道

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

   Zone Name: Trust

   IP Address/Netmask: 192.168.10.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 201.22.3.14/24

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

   Interface Name: tunnel.1

   Zone: Untrust

   Unnumbered: （选择）

   Interface: ethernet3(Untrust)

地址

4. 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: 192.168.10.0/24
   Zone: Trust
5. 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: 172.16.5.0/24
   Zone: Untrust

VPN

6. VPNs > Manual Key > New：输入以下内容，然后单击 **OK**：
   VPN Tunnel Name: Tokyo_Paris
   Gateway IP: 203.3.3.10
   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 “手动密钥” 通道配置页：
   Bind to Tunnel Interface: （选择）, tunnel.1

路由

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3

   Gateway IP Address: 201.22.3.20

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

   Network Address/Netmask: 172.16.5.0/24

   Gateway: （选择）

   Interface: Tunnel.1

   Gateway IP Address: 0.0.0.0

策略

9. 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）

10. 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)

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 172.16.5.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 203.3.3.10/24
3. Network > Interfaces > Tunnel IF New：输入以下内容，然后单击 **OK**：
   Interface Name: tunnel.1
   Zone: Untrust
   Unnumbered: （选择）
   Interface: ethernet3(Untrust)

地址

4. 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）, 172.16.5.0/24
   Zone: Trust

5. 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）, 192.168.10.0/24

   Zone: Untrust

VPN

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

   VPN Tunnel Name: Paris_Tokyo

   Gateway IP: 201.22.3.14

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

   Outgoing Interface: ethernet3(Untrust)

   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 “手动密钥” 通道配置页：

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

路由

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3

   Gateway IP Address: 203.3.3.1

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

   Network Address/Netmask: 192.168.10.0/24

   Gateway: （选择）

   Interface: Tunnel.1

   Gateway IP Address: 0.0.0.0

策略

9. 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）

10. 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)

接口 – 区段和通道

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 192.168.10.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 201.22.3.14/24
5. set interface tunnel.1 zone untrust
6. set interface tunnel.1 ip unnumbered interface ethernet3

地址

7. set address trust Trust_LAN 192.168.10.0/24
8. set address untrust paris_office 172.16.5.0/24

VPN

9. set vpn tokyo_paris manual 3020 3030 gateway 203.3.3.10 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
10. set vpn tokyo_paris bind interface tunnel.1

路由

11. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.22.3.20
12. set vrouter trust-vr route 172.16.5.0/24 interface tunnel.1

策略

13. set policy top name “To Paris” from trust to untrust Trust_LAN paris_office any permit
14. set policy top name “From Paris” from untrust to trust paris_office Trust_LAN any permit
15. save

CLI (巴黎)

接口 – 区段和通道

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.16.5.1/24
3. set interface ethernet1 nat
4. set interface ethernet3 zone untrust
5. set interface ethernet3 ip 203.3.3.10/24
6. set interface tunnel.1 zone untrust
7. set interface tunnel.1 ip unnumbered interface ethernet3

地址

8. set address trust Trust_LAN 172.16.5.0/24
9. set address untrust tokyo_office 192.168.10.0/24

VPN

10. set vpn paris_tokyo manual 3030 3020 gateway 201.22.3.14 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a
11. set vpn paris_tokyo bind interface tunnel.1

路由

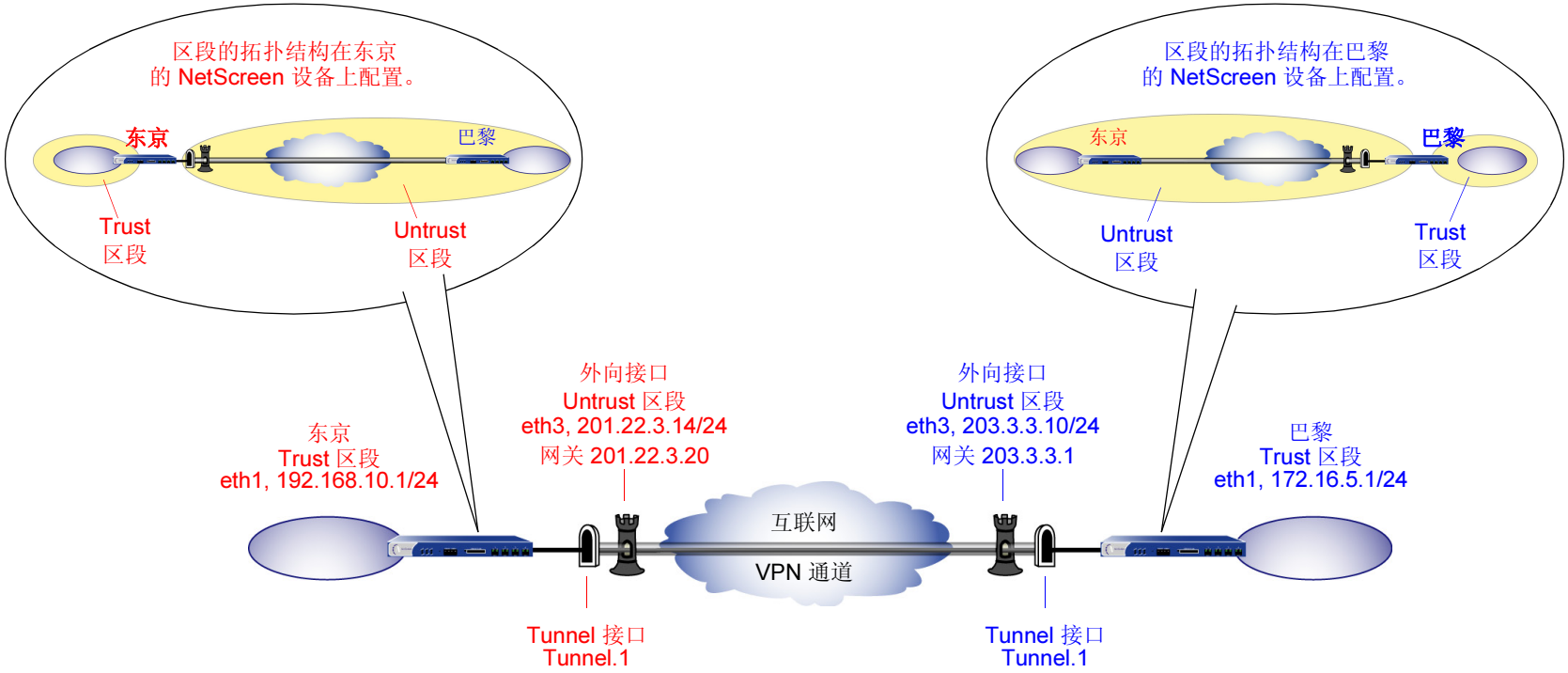
12. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.3.3.1
13. set vrouter trust-vr route 192.168.10.0/24 interface tunnel.1

策略

14. set policy top name “To Tokyo” from trust to untrust Trust_LAN tokyo_office any permit
15. set policy top name “from Tokyo” from untrust to trust tokyo_office Trust_LAN any permit
16. save

范例：基于路由的 LAN 到 LAN 的 VPN，自动密钥 IKE

在本例中，“自动密钥 IKE”通道使用预共享机密或一对证书（通道两端各一个），提供东京和巴黎分公司之间的安全连接。对于阶段 1 和阶段 2 安全级别，为阶段 1 提案指定 pre-g2-3des-sha 预共享密钥方法或 rsa-g2-3des-sha 证书，并为阶段 2 提案选择预定义的 “Compatible”设置。所有区域都在 trust-vr 中。



使用预共享机密或证书来设置基于路由的 “自动密钥 IKE”通道，包括以下步骤：

1. 定义远程网关和密钥交换模式，并指定预共享机密或证书
2. 创建“自动密钥 IKE VPN”条目，将通道绑定到通道接口，并配置 Proxy ID

注意：*完整的“自动密钥 IKE”配置还包括以下步骤：*

- *定义安全区段接口 IP 地址*
- *创建无编号 (Unnumbered) 通道接口*
- *为本地及远程端实体生成通讯簿条目*
- *设置路由*
- *配置策略*

*但由于这些步骤与*第 59 页上的 “范例：基于路由的 LAN 到 LAN 的 VPN，手动密钥”*中介绍的步骤相同，因此不再赘述。*

在以下例子中，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. 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：203.3.3.10

   （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)

（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

2. 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: （选择）, tunnel.1

Proxy-ID: （选择）

Local IP/Netmask: 192.168.10.0/24

Remote IP/Netmask: 172.16.5.0/24

Service: ANY

WebUI (巴黎)

1. 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：201.22.3.14

   （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)

   （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

2. 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 “自动密钥 IKE”配置页：

   Security Level: Compatible

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

   Proxy-ID: （选择）

   Local IP/Netmask: 172.16.5.0/24

   Remote IP/Netmask: 192.168.10.0/24

   Service: ANY

CLI (东京)

预共享密钥

1. set ike gateway to_paris ip 203.3.3.10 main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
2. set vpn tokyo_paris gateway to_paris sec-level compatible
3. set vpn tokyo_paris bind interface tunnel.1
4. set vpn tokyo_paris proxy-id local-ip 192.168.10.0/24 remote-ip 172.16.5.0/24 any
5. save

证书

1. set ike gateway to_paris ip 203.3.3.10 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
2. set ike gateway to_paris cert peer-ca 1[7]
3. set ike gateway to_paris cert peer-cert-type x509-sig
4. set vpn tokyo_paris gateway to_paris sec-level compatible
5. set vpn tokyo_paris bind interface tunnel.1
6. set vpn tokyo_paris proxy-id local-ip 192.168.10.0/24 remote-ip 172.16.5.0/24 any
7. save

CLI (巴黎)

预共享密钥

1. set ike gateway to_tokyo ip 201.22.3.14 main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha
2. set vpn paris_tokyo gateway to_tokyo sec-level compatible
3. set vpn paris_tokyo bind interface tunnel.1
4. set vpn paris_tokyo proxy-id local-ip 172.16.5.0/24 remote-ip 192.168.10.0/24 any
5. save

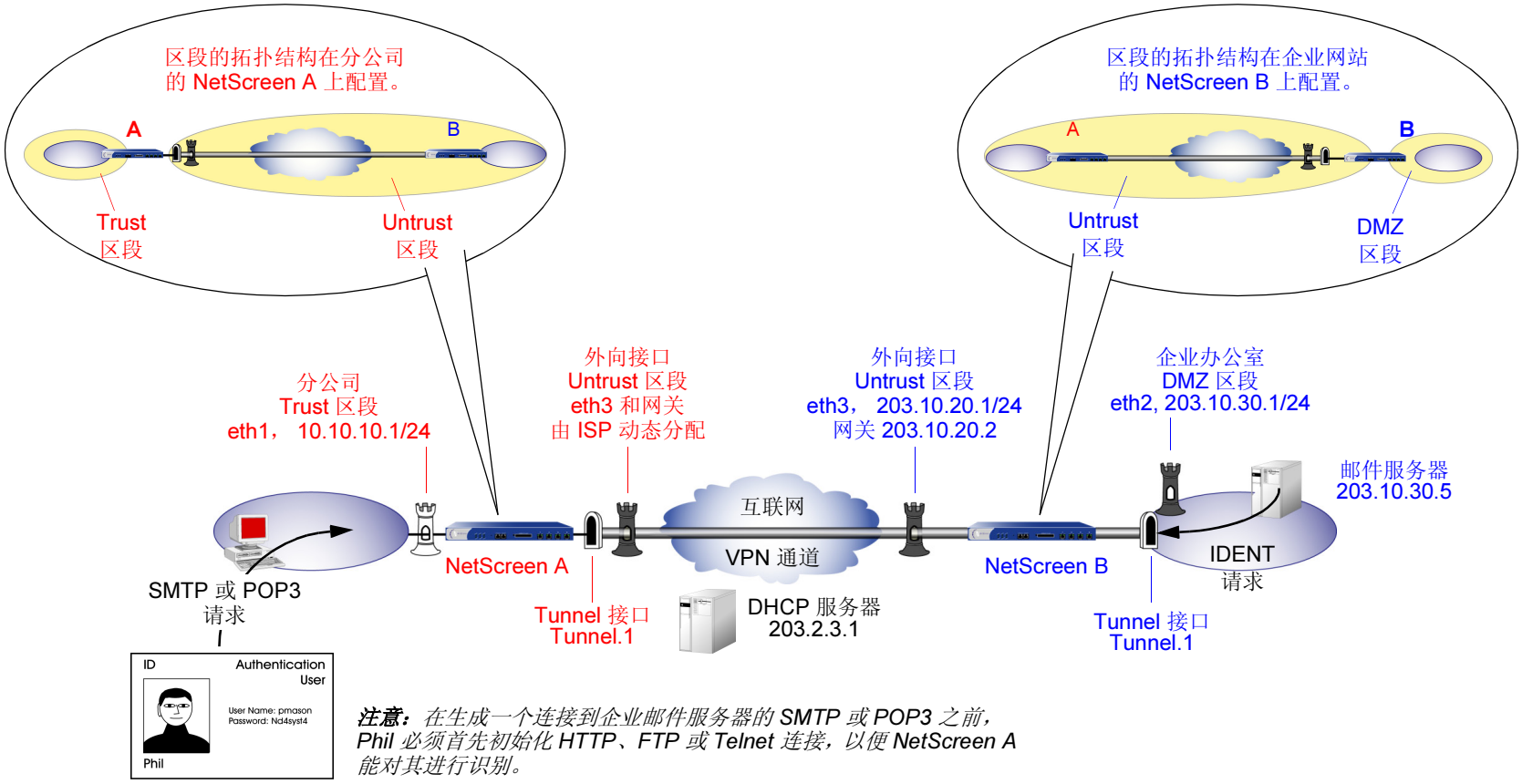
证书

1. set ike gateway to_tokyo ip 201.22.3.14 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
2. set ike gateway to_tokyo cert peer-ca 1[7]
3. set ike gateway to_tokyo cert peer-cert-type x509-sig
4. set vpn paris_tokyo gateway to_tokyo sec-level compatible
5. set vpn paris_tokyo bind interface tunnel.1
6. set vpn paris_tokyo proxy-id local-ip 172.16.5.0/24 remote-ip 192.168.10.0/24 any
7. save

7. 数字 1 是 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。

范例：基于路由的 LAN 到 LAN 的 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 具有其 Untrust 区段的固定地址， VPN 流量必须来自 NetScreen A 后面的主机。 NetScreen A 建立了通道之后，流量可从该通道的任一端通过。所有安全和 Tunnel 区段都在 trust-vr 中。



注意：*在生成一个连接到企业邮件服务器的 SMTP 或 POP3 之前，Phil 必须首先初始化 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）要从企业网站上的邮件服务器获得他的电子邮件。当他试图这样做时，对他进行两次验证：第一次，在允许流量从他那里通过通道[8] 之前， NetScreen A 在本地对他进行验证；第二次，邮件服务器程序对他进行验证，并通过该通道发送 IDENT 请求。

注意：*只有在 NetScreen A 和 NetScreen B 的管理员为其 （TCP，端口 113）添加了定制服务，并且设置了策略，允许流量通过通道到达 10.10.10.0/24 子网时，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。（有关获取并下载证书的详细信息，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，为阶段 1 提案指定 pre-g2-3des-sha 预共享密钥方法或 rsa-g2-3des-sha 证书，并为阶段 2 提案选择预定义的 “Compatible”设置。

WebUI (NetScreen A)

接口 – 安全区段和通道

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.10.1/24

2. 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）

8. 由于 Phil 是一个认证用户，在他能提出一个 POP3 的 SMTP 请求之前，必须先初始化 HTTP、FTP 或 Telnet 连接，这样， NetScreen A 就能作出用一个防火墙用户 / 注册提示来对他进行认证的响应。 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联系。

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

   Interface Name: tunnel.1

   Zone: Untrust

   Unnumbered: （选择）

   Interface: ethernet3(Untrust)

用户

4. 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

地址

5. 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:10.10.10.0/24

   Zone: Trust

6. 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: 203.10.30.5/32

   Zone: Untrust

服务

7. 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

8. 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

   选择以下服务，然后使用 **<<** 按钮将它们从 “Available members” 栏中移动到 “Group members” 栏中：

   FTP
   HTTP
   MAIL
   POP3
   Telnet
   Ident

VPN

9. 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: 203.10.20.1

（预共享密钥）

Preshared Key: h1p8A24nG5

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，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): Aggressive

（证书）

Local ID: pmason@abc.com

Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，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): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

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

VPN Name: branch_corp

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“自动密钥 IKE”配置页：

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

Proxy-ID: （选择）

Local IP/Netmask: 10.10.10.0/24

Remote IP/Netmask: 203.10.30.5/32

Service: Remote_Mail

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(Untrust)

Gateway IP Address: 0.0.0.0[9]

9. ISP 通过 DHCP 动态提供网关 IP 地址。

12. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
    Network Address/Netmask: 203.10.30.5/32
    Gateway: （选择）
    Interface: Tunnel.1
    Gateway IP Address: 0.0.0.0

策略

13. Policies > (From: Trust, To: Untrust) New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Trusted network
    Destination Address:
    Address Book: （选择） , Mail Server
    Service: Remote_Mail
    Action: Permit
    Position at Top: （选择）
14. Policies > (From: Untrust, To: Trust) New：输入以下内容，然后单击 **OK**：
    Source Address:
    Address Book: （选择） , Mail Server
    Destination Address:
    Address Book: （选择） , Trusted network
    Service: Remote_Mail
    Action: Permit
    Position at Top: （选择）

WebUI (NetScreen B)

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet2）：输入以下内容，然后单击 **OK**：
   Zone Name: DMZ
   IP Address/Netmask: 203.10.30.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address: 203.10.20.1/24
3. Network > Interfaces > Tunnel IF New：输入以下内容，然后单击 **OK**：
   Tunnel Interface Name: tunnel.1
   Zone: DMZ
   Unnumbered: （选择）
   Interface: ethernet2(DMZ)

地址

4. 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: 203.10.30.5/32
   Zone: DMZ

5. 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: 10.10.10.0/24

   Zone: Untrust

服务

6. 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

7. Objects > Services > Group > New：输入以下内容，运行以下服务，然后单击 **OK**：

   Group Name: Remote_Mail

   选择以下服务，然后使用 **<<** 按钮将它们从“Available members”栏中移动到“Group members”栏中：

   Ident
   MAIL
   POP3

VPN

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

Gateway Name: to_branch1

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：输入下列高级设置，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): Aggressive

（证书）

Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，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): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

9. 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

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

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

   Proxy-ID: （选择）

   Local IP/Netmask: 203.10.30.5/32

   Remote IP/Netmask: 10.10.10.0/24

   Service: Remote_Mail

路由

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

    Network Address/Netmask: 0.0.0.0/0

    Gateway: （选择）

    Interface: ethernet3(untrust)

    Gateway IP Address: （选择）, 203.10.20.2

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

    Network Address/Netmask: 10.10.10.0/24

    Gateway: （选择）

    Interface: Tunnel.1

    Gateway IP Address: 0.0.0.0

策略

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

    Source Address:

    Address Book: （选择） , Mail Server

    Destination Address:

    Address Book: （选择） , branch office

    Service: Remote_Mail

    Action: Permit

    Position at Top: （选择）

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

    Source Address:

    Address Book: （选择） , branch office

    Destination Address:

    Address Book: （选择） , Mail Server

    Service: Remote_Mail

    Action: Permit

    Position at Top: （选择）

CLI (NetScreen A)

接口 – 安全区段和通道

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.10.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 dhcp
5. set dhcp client server 201.2.3.1
6. set interface tunnel.1 zone untrust
7. set interface tunnel.1 ip unnumbered interface ethernet3

用户

8. set user pmason password Nd4syst4

地址

9. set address trust “trusted network” 10.10.10.0/24
10. set address untrust “mail server” 203.10.30.5/32

服务

11. set service ident protocol tcp src-port 0-65535 dst-port 113-113
12. set group service remote_mail
13. set group service remote_mail add http
14. set group service remote_mail add ftp
15. set group service remote_mail add telnet
16. set group service remote_mail add ident
17. set group service remote_mail add mail
18. set group service remote_mail add pop3

VPN

19. 预共享密钥：

```
set ike gateway to_mail ip 203.10.20.1 aggressive outgoing-interface ethernet3 local-id
pmason@abc.com preshare h1p8A24nG5 proposal pre-g2-3des-sha-1
set vpn branch_corp gateway to_mail tunnel proposal nopfs-esp-3des-sha
set vpn branch_corp bind interface tunnel.1
set vpn branch_corp proxy-id local-ip 10.10.10.0/24 remote-ip 203.10.30.5/32 remote_mail
```

（或）

证书：

```
set ike gateway to_mail ip 203.10.20.1 aggressive outgoing-interface ethernet3 local-id
pmason@abc.com proposal rsa-g2-3des-sha
set ike gateway to_mail cert peer-ca 1[10]
set ike gateway to_mail cert peer-cert-type x509-sig
set vpn branch_corp gateway to_mail tunnel proposal nopfs-esp-3des-sha
set vpn branch_corp bind interface tunnel.1
set vpn branch_corp proxy-id local-ip 10.10.10.0/24 remote-ip 203.10.30.5/32 remote_mail
```

路由

20. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[11]
21. set vrouter trust-vr route 203.10.30.5/32 interface tunnel.1

10. 数字 1 为 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。
11. ISP 通过 DHCP 动态提供网关 IP 地址，因而不能在此处指定。

策略

22. set policy top from trust to untrust “trusted network” “mail server” remote_mail permit auth server Local user pmason
23. set policy top from untrust to trust “mail server” “trusted network” remote_mail permit
24. save

CLI (NetScreen B)

接口 – 安全区段

1. set interface ethernet2 zone dmz
2. set interface ethernet2 ip 203.10.30.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24
5. set interface tunnel.1 zone dmz
6. set interface tunnel.1 ip unnumbered interface ethernet2

地址

7. set address dmz “mail server” 203.10.30.5/32
8. set address untrust “branch office” 10.10.10.0/24

服务

9. set service ident protocol tcp src-port 0-65535 dst-port 113-113
10. set group service remote_mail
11. set group service remote_mail add ident
12. set group service remote_mail add mail
13. set group service remote_mail add pop3

VPN

14. 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 proposal nopfs-esp-3des-sha

    set vpn to_branch bind interface tunnel.1

    set vpn to_branch proxy-id local-ip 203.10.30.5/32 remote-ip 10.10.10.0/24 remote_mail

    （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[12]

    set ike gateway to_branch cert peer-cert-type x509-sig

    set vpn corp_branch gateway to_branch tunnel proposal nopfs-esp-3des-sha

    set vpn to_branch bind interface tunnel.1

    set vpn to_branch proxy-id local-ip 203.10.30.5/32 remote-ip 10.10.10.0/24 remote_mail

路由

15. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2
16. set vrouter trust-vr route 10.10.10.0/24 interface tunnel.1

策略

17. set policy top from dmz to untrust “mail server” “branch office” remote_mail permit
18. set policy top from untrust to dmz “branch office” “mail server” remote_mail permit
19. save

12. 数字 1 为 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。

拨号到 LAN 的 VPN，动态对等方

NetScreen 设备也支持 VPN 拨号连接。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。

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[13]，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互联网 IP 地址（NetScreen-Remote 也支持），因此可通过指定的通道接口配置该虚拟互联网地址的路由表条目。这样允许配置 NetScreen 设备和该对等方之间基于路由的 VPN 通道。

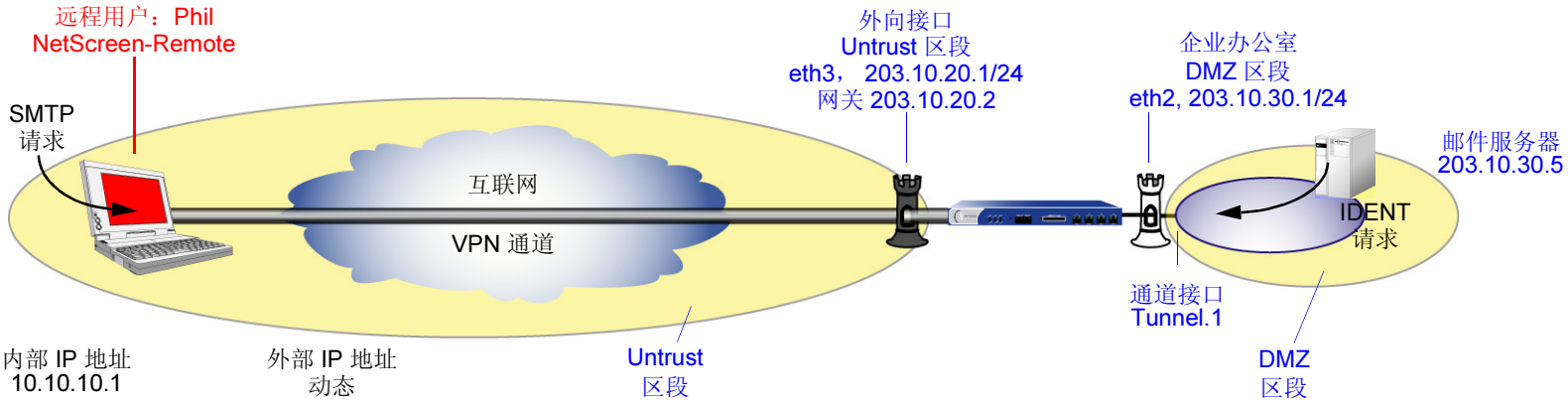
注意：*除拨号客户端的内部 IP 地址为虚拟地址外，拨号到 LAN 的动态对等方与 LAN 到 LAN 动态对等方几乎一样。*

13. 拨号动态对等方客户端是拨号客户端，它支持虚拟互联网 IP 地址。

范例：基于路由的拨号到 LAN 的 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这两个地址，以便能将它们添加到 Untrust 通讯薄中，用于来自该地址通道流量的策略中。 NetScreen-Remote 客户端建立通道后，流量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，并且设置了外向策略，允许流量通过通道到达 10.10.10.1 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@netscreen.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” 提议集。

WebUI

接口 – 安全区段和通道

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

   Zone Name: DMZ

   IP Address/Netmask: 203.10.30.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 203.10.20.1/24

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

   Interface Name: tunnel.1

   Zone: DMZ

   Unnumbered: （选择）

   Interface: ethernet2(DMZ)

地址

4. 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: 203.10.30.5/32

   Zone: DMZ

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

   Address Name: Phil

   IP Address/Domain Name:

   IP/Netmask: 10.10.10.1/32

   Zone: Untrust

服务

6. 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

7. 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

VPN

8. 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@netscreen.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 “网关” 配置页：

Security Level: Custom

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

Mode (Initiator): Aggressive

（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): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

9. 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“自动密钥 IKE”配置页：

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

Proxy-ID: （选择）

Local IP/Netmask: 203.10.30.5/32

Remote IP/Netmask: 10.10.10.1/32

Service：Remote_Mail

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 203.10.20.2

11. Network > Routing > Routing Table > 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(untrust)

    Gateway IP Address: 0.0.0.0

策略

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

    Source Address：

    Address Book: （选择） , Phil

    Destination Address：

    Address Book: （选择） , Mail Server

    Service：Remote_Mail

    Action：Permit

    Position at Top: （选择）

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

    Source Address:

    Address Book: （选择） , Mail Server

    Destination Address:

    Address Book: （选择） , Phil

    Service: Remote_Mail

    Action: Permit

    Position at Top: （选择）

CLI

接口 – 安全区段和通道

1. set interface ethernet2 zone dmz
2. set interface ethernet2 ip 203.10.30.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24
5. set interface tunnel.1 zone dmz
6. set interface tunnel.1 ip unnumbered interface ethernet2

地址

7. set address dmz “mail server” 203.10.30.5/32
8. set address untrust phil 10.10.10.1/32

服务

9. set service ident protocol tcp src-port 0-65535 dst-port 113-113
10. set group service remote_mail
11. set group service remote_mail add ident
12. set group service remote_mail add mail
13. set group service remote_mail add pop3

VPN

14. 预共享密钥：

    set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha

    set vpn corp_phil gateway to_phil sec-level compatible

    set vpn to_branch bind interface tunnel.1

    set vpn to_branch proxy-id local-ip 203.10.30.5/32 remote-ip 10.10.10.1/32 remote_mail

（或）

证书：

```
set ike gateway to_phil dynamic pm@netscreen.com aggressive outgoing-interface ethernet3
proposal rsa-g2-3des-sha
set ike gateway to_phil cert peer-ca 1[14]
set ike gateway to_phil cert peer-cert-type x509-sig
set vpn corp_phil gateway to_phil sec-level compatible
set vpn to_branch bind interface tunnel.1
set vpn to_branch proxy-id local-ip 203.10.30.5/32 remote-ip 10.10.10.1/32 remote_mail
```

路由

15. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2
16. set vrouter trust-vr route 10.10.10.1/32 interface tunnel.1

策略

17. set policy top from dmz to untrust “mail server” phil remote_mail permit
18. set policy top from untrust to dmz phil “mail server” remote_mail permit
19. save

14. 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 ID Type: IP Address

   IP Address: 203.10.30.5

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 203.10.20.1

5. 单击 unix 图标左侧的加号“**+**”，展开连接策略。
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
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@netscreen.com

   或

   从 Select Certificate 下拉列表中，选择包含电子邮件地址“pm@netscreen.com”的证书。

   Internal Network IP Address: 10.10.10.1

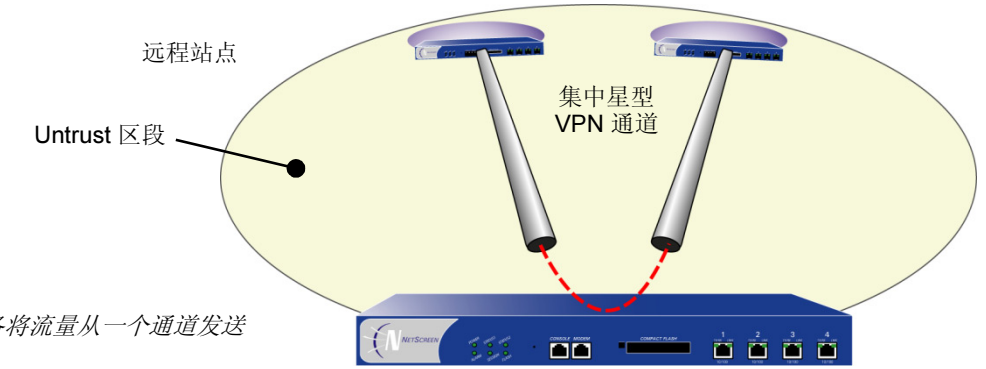
   ID Type: E-mail Address; pm@netscreen.com

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**：选择下列“加密”和“数据完整性算法”：
   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 **Save** 按钮。

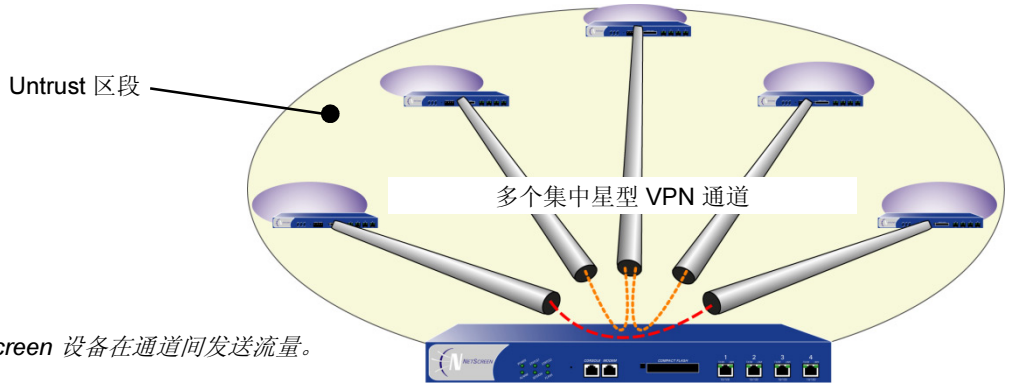
集中星型 VPN

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 设备就能引导流量离开一个通道，到达另一通道。如果两个通道都包含在一个单独区段内，则不需创建允许流量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。



NetScreen 设备将流量从一个通道发送到另一通道。

也可在一个区段内配置多个 VPN，并在任意两个通道之间发送流量。



NetScreen 设备在通道间发送流量。

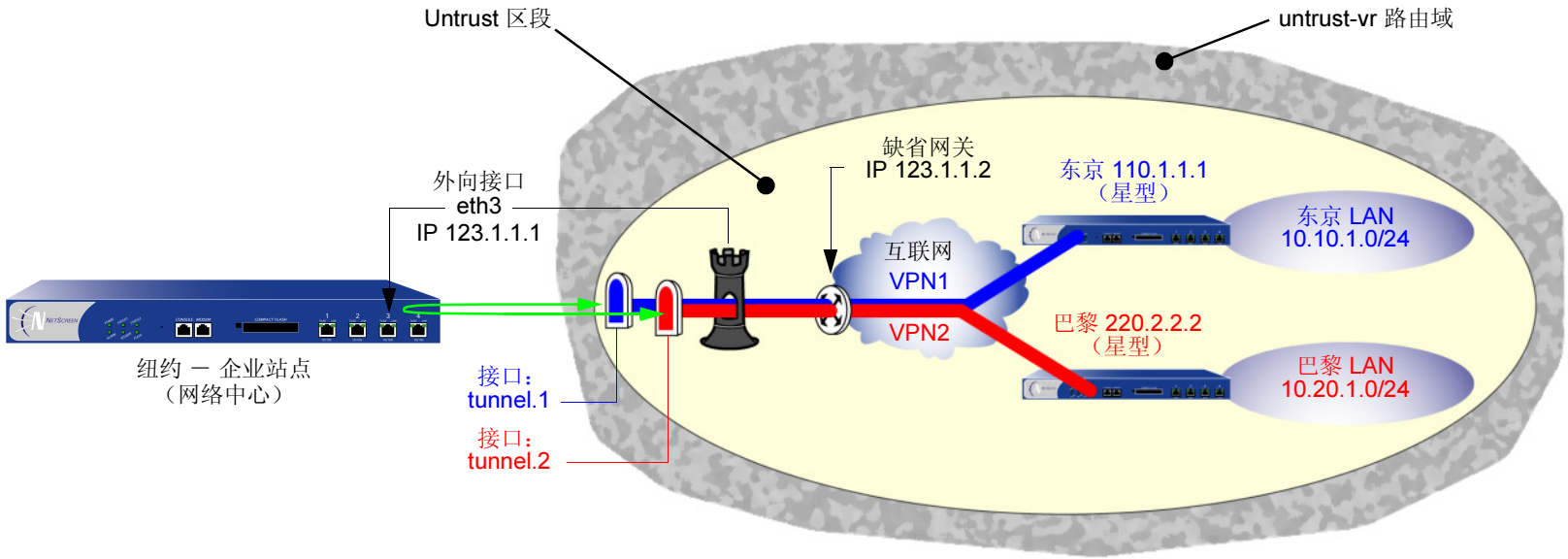
范例：集中星型 VPN

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 设备引导流量离开一个通道，而进入另一通道。

在通道间引导流量时，由于两个远程端点都在同一区段 （Untrust Zone）中[15]，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.2，二者均无编号。这两个通道使用“自动密钥 IKE”，并带有预共享密钥。选择与阶段 1 和阶段 2 提议都“Compatible”的预定义安全级别。将 Untrust 区段绑定到 untrust-vr。Untrust 区段接口为 ethernet3。

注意： *下面只提供了位于企业站点的 NetScreen 设备的配置。*



15. 也可选择启用内部区段阻塞，并定义内部区段策略，允许两个通道接口间的流量。

WebUI

安全区段和虚拟路由器

1. 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
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Null
3. 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）

接口 – 区段和通道

4. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 123.1.1.1/24
5. Network > Interfaces > Tunnel IF New：输入以下内容，然后单击 **OK**：
   Interface Name: tunnel.1
   Unnumbered: （选择）
   Interface: ethernet3(Untrust)
6. Network > Interfaces > Tunnel IF New：输入以下内容，然后单击 **OK**：
   Interface Name: tunnel.2
   Unnumbered: （选择）
   Interface: ethernet3(untrust)

东京办事处的 VPN

7. 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）, IP Address: 110.1.1.1

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）[16]

Local IP/Netmask: 10.0.0.0/8

Remote IP/Netmask: 10.10.1.0/24

Service: ANY

16. 在 NetScreen 设备上配置 VPN 通道，以保护东京和巴黎办事处时，请执行以下操作之一：
（基于路由的 VPN）选中 **Proxy-ID** 复选框，并为 **Local IP/Netmask** 输入 **10.10.1.0/24**（东京）和 **10.20.1.0/24**（巴黎），为**Remote IP/Netmask** 输入 **10.0.0.0/8**。
（基于策略的 VPN）在 Trust 区段地址本中为 10.10.1.0/24 （东京）和 10.20.1.0/24 （巴黎）生成一个条目，在 Untrust 区段地址本中为 10.0.0.0/8 生成另一条目，并在将 VPN 通道引用到中心站点的策略中，将这些地址作为源和目标地址。

巴黎办事处的 VPN

8. 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）, IP Address：220.2.2.2

   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：

   Proxy-ID: （选择）

   Local IP/Netmask: 10.0.0.0/8

   Remote IP/Netmask: 10.20.1.0/24

   Service: ANY

路由

9. Network > Routing > Routing Table > untrust-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(untrust-vr)

   Gateway IP Address: 0.0.0.0

10. Network > Routing > Routing Table > untrust-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.2(untrust-vr)

    Gateway IP Address: 0.0.0.0

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

    Virtual Router Name: untrust_vr

    Network Address: 0.0.0.0/0

    Gateway: （选择）

    Interface: ethernet3(untrust-vr)

    Gateway IP Address: 123.1.1.2

CLI

安全区段和虚拟路由器

1. unset interface ethernet3 ip
2. unset interface ethernet3 zone
3. set zone untrust vrouter untrust-vr
4. unset zone untrust block

接口 – 区段和通道

5. set interface ethernet3 zone untrust
6. set interface ethernet3 ip 123.1.1.1/24
7. set interface tunnel.1 zone untrust
8. set interface tunnel.1 ip unnumbered interface ethernet3
9. set interface tunnel.2 zone untrust
10. set interface tunnel.2 ip unnumbered interface ethernet3

东京办事处的 VPN

11. set ike gateway Tokyo ip 110.1.1.1 outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
12. set vpn VPN1 gateway Tokyo sec-level compatible
13. set vpn VPN1 bind interface tunnel.1
14. set vpn VPN1 proxy-id local-ip 10.0.0.0/8 remote-ip 10.10.1.0/24 any[17]

17. 在 NetScreen 设备上配置 VPN 通道，保护东京和巴黎办事处时，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 10.10.1.0/24 remote-ip 10.0.0.0/8**（东京）和 **set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.0.0.0/8**（巴黎）。
（基于策略的 VPN）在 Trust 区段地址本中为 10.10.1.0/24（东京）和 10.20.1.0/24（巴黎）生成一个条目，在 Untrust 区段地址本中为 10.0.0.0/8 生成另一条目，并在将 VPN 通道引用到中心站点的策略中，将这些地址作为源和目标地址。

巴黎办事处的 VPN

15. set ike gateway Paris ip 220.2.2.2 outgoing-interface ethernet3 preshare netscreen2 sec-level compatible
16. set vpn VPN2 gateway Paris sec-level compatible
17. set vpn VPN2 bind interface tunnel.2
18. set vpn VPN2 proxy-id local-ip 10.0.0.0/8 remote-ip 10.20.1.0/24 any

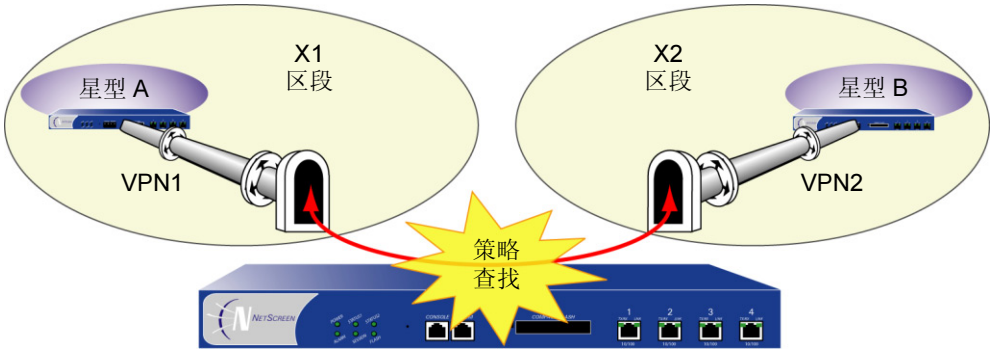
路由

19. set vrouter untrust-vr route 10.10.1.0/24 interface tunnel.1
20. set vrouter untrust-vr route 10.20.1.0/24 interface tunnel.2
21. set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 123.1.1.2
22. save

背对背的 VPN

可在中心站点强制执行区段间策略，使流量能从一个 VPN 通道到达另一通道，方法是将星型站点置于不同区段内[18]。由于它们处于不同区段，在将流量从一个通道发送另一通道之前，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 通道的流量。这样的布置称为背对背 VPN。

背对背的 VPN



18. 也可选择启用内部区段阻塞，并定义内部区段策略，控制同一区段内两个通道接口间的流量。

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，以及链接到周边站点 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，可应用集中星型方法，显著增加它们的 VPN 选项和功能。
- 位于中心设备的管理员能完全控制周边站点间的 VPN 流量。例如，
  - 可能只允许 HTTP 流量从站点 A 流向 站点 B，但允许任意类型的流量从站点 B 流向站点 A。
  - 可允许起始于 A 的流量到达 C，但拒绝起始于 C 的流量到达 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流量。在每个周边站点，必须先有一个策略，引导所有出站流量通过星型 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，管理员能控制互联网访问、允许某些类型的流量 （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，并通过星型通道互联，允许一个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

除了纽约中心站点处的 NetScreen 设备对东京和巴黎办事处两个通道间发送的流量执行策略检测以外，下例与第 104 页上的 “范例：集中星型 VPN”非常相似。将每个远程站点置于不同区段，即可控制网络中心处的 VPN 流量。

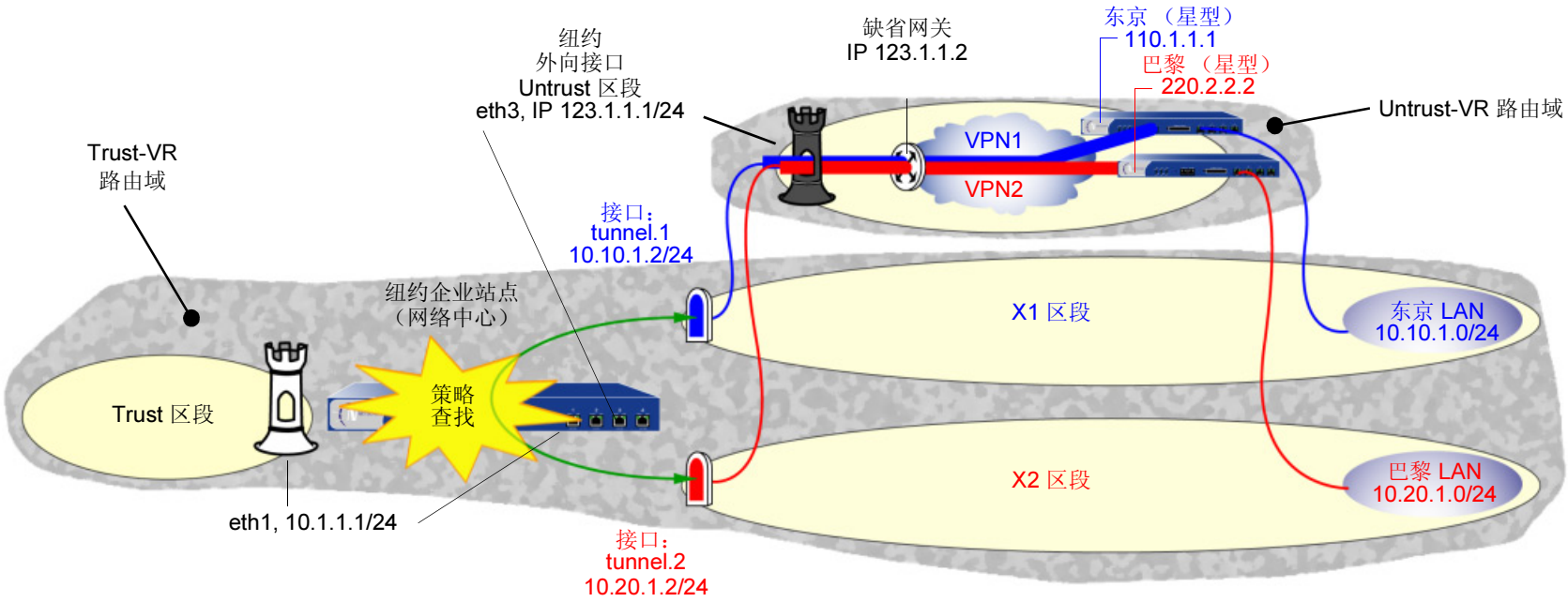
东京 LAN 地址在用户定义的 X1 区段内，巴黎 LAN 地址在用户定义的 X2 区段内。这两个区段都在 Trust-VR 路由域中。

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，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流量发送到该通道接口。

ethernet3 是外向接口，它被绑定到 Untrust 区段。从以下说明可以看出，两个通道都终止于 Untrust 区段。但是，使用这两个通道的流量的终点位于 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。选择与阶段 1 和阶段 2 提议都“Compatible”的预定义安全级别。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）， Proxy ID 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

安全区段和虚拟路由器

1. 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
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Null
3. 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）
4. 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）
5. Network > Zones > New：输入以下内容，然后单击 **OK**：
   Name: X2
   Virtual Router Name: trust-vr
   Block Intra-Zone Traffic: （选择）

接口 – Untrust 区段和通道

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

   Zone Name: Untrust

   IP Address/Netmask: 123.1.1.1/24

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

   Interface Name: tunnel.1

   Zone: X1

   Fixed IP: （选择）

   IP Address/Netmask: 10.10.1.2/24

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

   Interface Name: tunnel.2

   Zone: X2

   Fixed IP: （选择）

   IP Address/Netmask: 10.20.1.2/24

东京办事处的 VPN

9. 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）. IP Address: 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 “自动密钥 IKE” 配置页：

   Proxy-ID: （选择）[19]

   Local IP/Netmask: 10.20.1.0/24

   Remote IP/Netmask: 10.10.1.0/24

   Service: ANY

19. 在 NetScreen 设备上配置 VPN 通道，以保护东京和巴黎办事处时，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 “本地 IP” 和 “网络掩码” 输入 **10.10.1.0/24**（东京）和 **10.20.1.0/24**（巴黎），为 “远程 IP” 和 “网络掩码” 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 区段地址本中生成 10.10.1.0/24 （东京）和 10.20.1.0/24 （巴黎）的条目，在 Untrust 区段地址本生成 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 VPN 通道引用到中心站点。

巴黎办事处的 VPN

10. 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）, IP Address: 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 “自动密钥 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

路由

11. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
    Network Address/Netmask: 0.0.0.0/0
    Next Hop Virtual Router Name: （选择）, untrust-vr
12. Network > Routing > Routing Table > 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(untrust-vr)
    Gateway IP Address: 123.1.1.2

地址

13. 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: 10.10.1.0/24
    Zone: X1
14. 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: 10.20.1.0/24
    Zone: X2

策略

15. Policy (From: X1, To: X2) > New：输入以下内容，然后单击 **OK**：

    Source Address:

    Address Book: （选择） , Tokyo LAN

    Destination Address:

    Address Book: （选择） , Paris LAN

    Service: ANY

    Action: Permit

    Position at Top: （选择）

16. Policy (From: X2, To: X1) > New：输入以下内容，然后单击 **OK**：

    Source Address:

    Address Book: （选择） , Paris LAN

    Destination Address:

    Address Book: （选择） , Tokyo LAN

    Service: ANY

    Action: Permit

    Position at Top: （选择）

CLI

安全区段和虚拟路由器

1. unset interface ethernet3 ip
2. unset interface ethernet3 zone
3. set zone untrust vrouter untrust-vr
4. set zone untrust block
5. set zone name X1
6. set zone x1 vrouter trust-vr
7. set zone x1 block
8. set zone name x2
9. set zone x2 vrouter trust-vr
10. set zone x2 block

接口 – Untrust 区段和通道

11. set interface ethernet3 zone untrust
12. set interface ethernet3 ip 123.1.1.1/24
13. set interface tunnel.1 zone x1
14. set interface tunnel.1 ip 10.10.1.2/24
15. set interface tunnel.2 zone x2
16. set interface tunnel.2 ip 10.20.1.2/24

东京办事处的 VPN

17. set ike gateway Tokyo ip 110.1.1.1 outgoing-interface ethernet3 preshare netscreen1 sec-level compatible
18. set vpn VPN1 gateway Tokyo sec-level compatible
19. set vpn VPN1 bind interface tunnel.1
20. set vpn VPN1 proxy-id local-ip 10.20.1.0/24 remote-ip 10.10.1.0/24 any[20]

巴黎办事处的 VPN

21. set ike gateway Paris ip 220.2.2.2 outgoing-interface ethernet3 preshare netscreen2 sec-level compatible
22. set vpn VPN2 gateway Paris sec-level compatible
23. set vpn VPN2 bind interface tunnel.2
24. set vpn VPN2 proxy-id local-ip 10.10.1.0/24 remote-ip 10.20.1.0/24 any

路由

25. set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
26. set vrouter untrust-vr route 0.0.0.0/0 interface ethernet3 gateway 123.1.1.2

地址

27. set address x1 “Tokyo LAN” 10.10.1.0/24
28. set address x2 “Tokyo LAN” 10.20.1.0/24

策略

29. set policy top from x1 to x2 “Tokyo LAN” “Paris LAN” any permit[21]
30. set policy top from x2 to x1 “Paris LAN” “Tokyo LAN” any permit
31. save

---

20. 在 NetScreen 设备上配置 VPN 通道，以保护东京和巴黎办事处时，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 区段地址本中生成 10.10.1.0/24（东京）和 10.20.1.0/24（巴黎）的条目，在 Untrust 区段地址本生成 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，这些策略将 VPN 通道引用到中心站点。

21. 可忽略以下消息（由于通道接口在 NAT 模式下，所有出现该消息）：*Warning: Some interfaces in the <zone_name> zone are in NAT mode. Traffic might not pass through them!*

4

基于策略的 VPN

基于策略的 VPN 是一种配置，在该配置中，特定的 VPN 通道在策略中被引用，该策略的动作被设置为 tunnel。基于策略的 VPN 与基于路由的 VPN 配置相比，后者的策略不引用特定的 VPN 通道。VPN 通道被指向特定通道接口的路由间接引用。通道接口可被绑定到 VPN 通道或 Tunnel 区段。

注意：*有关基于路由的 VPN 的例子，请参阅第 3 章，第 47 页上的“基于路由的 VPN”。有关将通道接口绑定到 VPN 通道的信息，请参阅第 125 页上的“通道接口”。*

本章只做简要介绍，并提供以下基于策略的 VPN 概念的例子：

- 第 124 页上的“LAN 到 LAN 的 VPN”
  - 第 127 页上的“范例：基于策略的 LAN 到 LAN 的 VPN，手动密钥”
  - 第 136 页上的“范例：基于策略的 LAN 到 LAN 的 VPN，自动密钥 IKE”
  - 第 142 页上的“范例：基于策略的 LAN 到 LAN 的 VPN，动态对等方”
- 第 156 页上的“拨号到 LAN 的 VPN”
  - 第 157 页上的“范例：基于策略的拨号到 LAN 的 VPN，手动密钥”
  - 第 163 页上的“范例：基于策略的拨号到 LAN 的 VPN，自动密钥 IKE”
  - 第 171 页上的“范例：基于策略的拨号到 LAN 的 VPN，动态对等”
- 第 180 页上的“组 IKE ID”
  - 第 186 页上的“范例：组 IKE ID （证书）”
  - 第 195 页上的“范例：组 IKE ID （预共享密钥）”
- 第 202 页上的“Tunnel 区段和基于策略的 NAT”
  - 第 204 页上的“范例：具有 MIP 和 DIP 的 Tunnel 接口”
- 第 213 页上的“冗余 VPN 网关”
  - 第 220 页上的“范例：冗余 VPN 网关”

LAN 到 LAN 的 VPN

IPSec VPN 通道存在于两个网关之间，而且每个网关需要一个 IP 地址。当两个网关都有静态的 IP 地址时，可配置以下各种通道：

- LAN 到 LAN 的 VPN、手动密钥通道
- LAN 到 LAN 的 VPN、自动密钥 IKE 通道 （具有预共享密钥或证书）

当一个网关具有一个静态地址，而另一个具有动态分配的地址时，可配置以下各种通道：

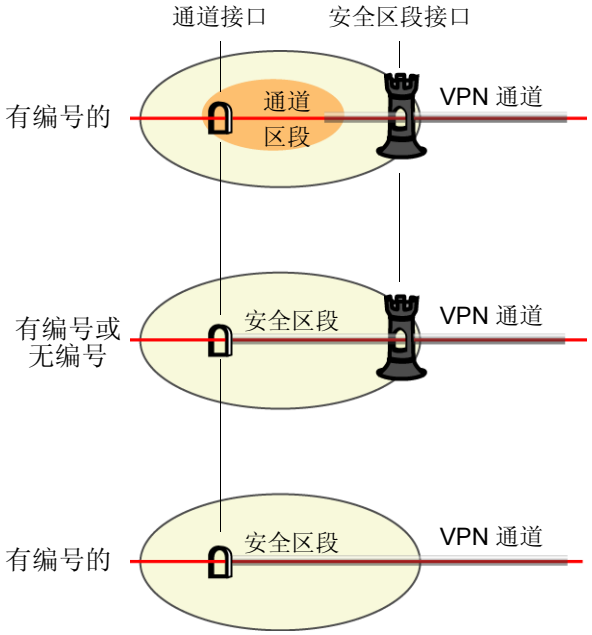
- 动态对等 LAN 到 LAN 的 VPN、自动密钥 IKE 通道 （具有预共享密钥或证书）

在此处，静态 LAN 到 LAN 的 VPN 包括 IPSec 通道，该通道连接两个 LAN，每个 LAN 都有一个 NetScreen 设备，而该设备是作为安全网关来运行的。在两个设备上用作外向接口的物理接口或子接口，有一个固定的 IP 地址，而且内部主机也有静态 IP 地址。如果 NetScreen 设备在 “透明” 模式下，它将 VLAN1 地址当作外向接口的 IP 地址使用。（请参阅第 127 页上的 “范例：基于策略的 LAN 到 LAN 的 VPN，手动密钥”，和第 136 页上的 “范例：基于策略的 LAN 到 LAN 的 VPN，自动密钥 IKE” 。）对于静态 LAN 到 LAN 的 VPN，处于其通道两端的主机，可发起 VPN 通道设置，因为远程网关的 IP 地址保持不变因而可以访问。

如果其中一个 NetScreen 设备的外向接口有动态分配的 IP 地址，该设备被称为动态的对等方，并且 VPN 的配置是不同的。（请参阅第 142 页上的 “范例：基于策略的 LAN 到 LAN 的 VPN，动态对等方”。）对于动态对等 LAN 到 LAN 的 VPN，只有在动态对等方后面的主机，才可发起 VPN 通道设置，因为只有它们的远程网关有一个固定的 IP 地址，因而可从它们的本地网关访问。但是，当在动态对等方和静态对等方之间建立通道之后，如果目的主机有固定的 IP 地址，在两个网关之中的任一个网关后面的主机，可发起 VPN 流量。

通道接口

在通道终点（本地和远程网关）以外，还可在安全区段或 Tunnel 区段配置通道接口，通过它， NetScreen 设备引导流量出入 VPN 通道[1]。在安全区段，可将 VPN 通道绑定到有特定编号的（有 IP 地址 / 网络掩码）或无编号的（没有 IP 地址 / 网络掩码）安全区段中的通道接口。如果通道接口是无编号的，它从安全区段中的接口借用 IP 地址，该通道就是在这个安全区段中创建的。



当有编号的通道接口在一个 Tunnel 区段中时，不能将 VPN 通道绑定到该通道接口。只可将一个通道绑定到该 Tunnel 区段。这就允许将多个通道接口链接到一个单一通道，或将多个通道链接到一个单一通道接口。在这些例子中，必须创建一个基于策略的 VPN 配置。

当通道接口在安全区段中时，可将一个 VPN 通道绑定到该通道接口。这样做，允许创建一个基于路由的 VPN 配置。

通道接口可以是有编号的，也可以是无编号的。如果它是无编号的，通道接口从安全区段接口借用 IP 地址。注意：只有一个有编号的通道接口（也就是说，具有一个 IP 地址和网络掩码的一个接口）才支持基于策略的 NAT。

当一个有编号的通道接口在一个安全区段中，而且它是该区段唯一的接口时，则无需创建一个安全区段接口。在这种情况下，安全区段支持通过通道接口的 VPN 流量，但不支持其它类型的流量。

一般来说，如果想让一个接口支持基于策略的 NAT，就应当给该通道接口分配一个 IP 地址。有关基于策略的 NAT 的详细信息，请参阅第 202 页上的“Tunnel 区段和基于策略的 NAT”。在 Tunnel 区段或安全区段中，可创建一个有编号的通道接口。

1. 如果不指定一个通道接口，通道对安全区段使用默认的接口。

如果通道接口无需支持基于策略的 NAT，而且其配置不需要将通道接口绑定到一个 Tunnel 区段，则可以指定该接口为无编号的。必须将一个无编号的通道接口绑定到一个安全区段，而不可将它绑定到一个 Tunnel 区段。还必须指定绑定到安全区段的接口，此安全区段的 IP 地址被无编号的通道接口借用。

注意：*指定的安全区段接口与已经绑定的通道接口必须在同一个区段中。*

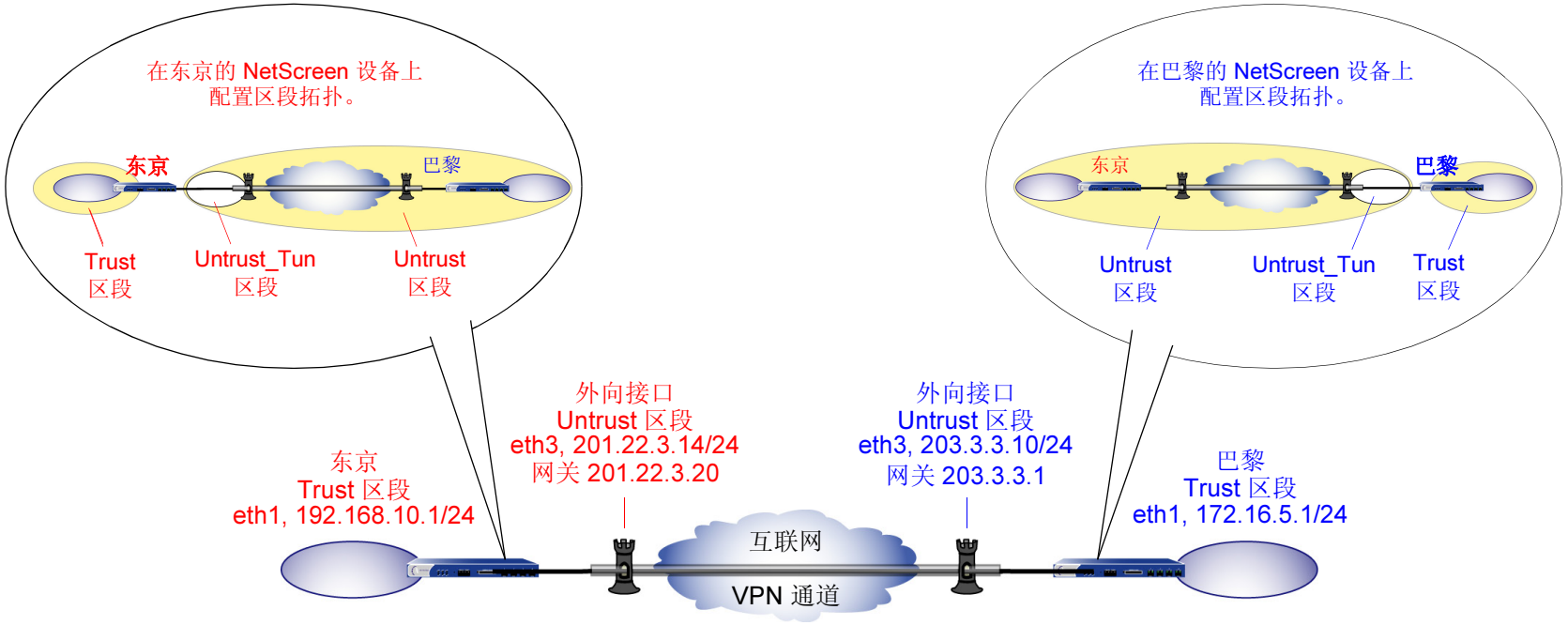
范例：基于策略的 LAN 到 LAN 的 VPN，手动密钥

在本例中，通过使用以 3DES 加密并经 SHA-1 认证的 ESP，手动密钥提供一个在东京和巴黎办公室之间的安全信道。在各个站点中的 Trust 区段都处于 NAT 模式下。地址如下：

- 东京：
  - Trust 接口 (ethernet1)：192.168.10.1/24
  - Untrust 接口 (ethernet3)：201.22.3.14/24
- 巴黎：
  - Trust 接口 (ethernet1)：172.16.5.1/24
  - Untrust 接口 (ethernet3)：203.3.3.10/24

Trust 和 Untrust 安全区段，以及 “Untrust_Tun” 通道区段，都在 trust-vr 路由域中。 Untrust 区段接口 (ethernet3) 作为 VPN 通道的外向接口。

注意：*缺省情况下， VPN 通道将绑定到 “Untrust_Tun” 通道区段，即使选择了* ***Bind to: None*** *选项（在 WebUI 中 VPN > Manual Key > New > 高级配置页上）。*



要建立通道，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，并指定其在 Untrust 区段中的外向接口。
3. 在 Trust 及 Untrust 区段地址本中，输入有关本地及远程端点的 IP 地址。
4. 输入到外部路由器的默认路由。
5. 设置有关 VPN 流量的策略，双向使用此通道。

WebUI (东京)

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击**OK**：
   Zone Name: Trust
   IP Address/Netmask: 192.168.10.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击**OK**：
   Zone Name: Untrust
   IP Address/Netmask: 201.22.3.14/24

地址

3. 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）, 192.168.10.0/24
   Zone: Trust

4. 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）, 172.16.5.0/24
   Zone: Untrust

VPN

5. VPNs > Manual Key > New：输入以下内容，然后单击 **OK**：
   VPN Tunnel Name: Tokyo_Paris
   Gateway IP: 203.3.3.10
   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

路由

6. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
   Network Address/Netmask: 0.0.0.0/0
   Gateway: （选择）
   Gateway IP Address: 201.22.3.20
   Interface: ethernet3(untrust)

策略

7. 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: （选择）, Trust_LAN

Destination Address：

Address Book: （选择）, Paris_office

Service: ANY

Action: Tunnel

Tunnel VPN: Tokyo_Paris

Modify matching VPN policy: （选择）

Position at Top: （选择）

WebUI (巴黎)

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 172.16.5.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 203.3.3.10/24

地址

3. 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）, 172.16.5.0/24
   Zone: Trust
4. 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）, 192.168.10.0/24
   Zone: Untrust

VPN

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

VPN Tunnel Name: Paris_Tokyo

Gateway IP: 201.22.3.14

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

Outgoing Interface: ethernet3(Untrust)

Bind to Tunnel Zone: （选择）, Untrust-Tun

ESP-CBC: （选择）

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password: PNas134a

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Gateway IP Address: 203.3.3.1

Interface: ethernet3(untrust)

策略

7. 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: （选择）, Trust_LAN

Destination Address：

Address Book: （选择）, Tokyo_office

Service: ANY

Action: Tunnel

Tunnel VPN: Paris_Tokyo

Modify matching VPN policy: （选择）

Position at Top: （选择）

CLI (东京)

接口 – 区段和通道

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 192.168.10.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 201.22.3.14/24

地址

5. set address trust Trust_LAN 192.168.10.0/24
6. set address untrust paris_office 172.16.5.0/24

VPN

7. set vpn tokyo_paris manual 3020 3030 gateway 203.3.3.10 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a

路由

8. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 201.22.3.20

策略

9. set policy top name “To/From Paris” from trust to untrust Trust_LAN paris_office any tunnel vpn tokyo_paris
10. set policy top name “To/From Paris” from untrust to trust paris_office Trust_LAN any tunnel vpn tokyo_paris
11. save

CLI (巴黎)

接口 – 区段和通道

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.16.5.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.3.3.10/24

地址

5. set address trust Trust_LAN 172.16.5.0/24
6. set address untrust tokyo_office 192.168.10.0/24

VPN

7. set vpn paris_tokyo manual 3030 3020 gateway 201.22.3.14 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a

路由

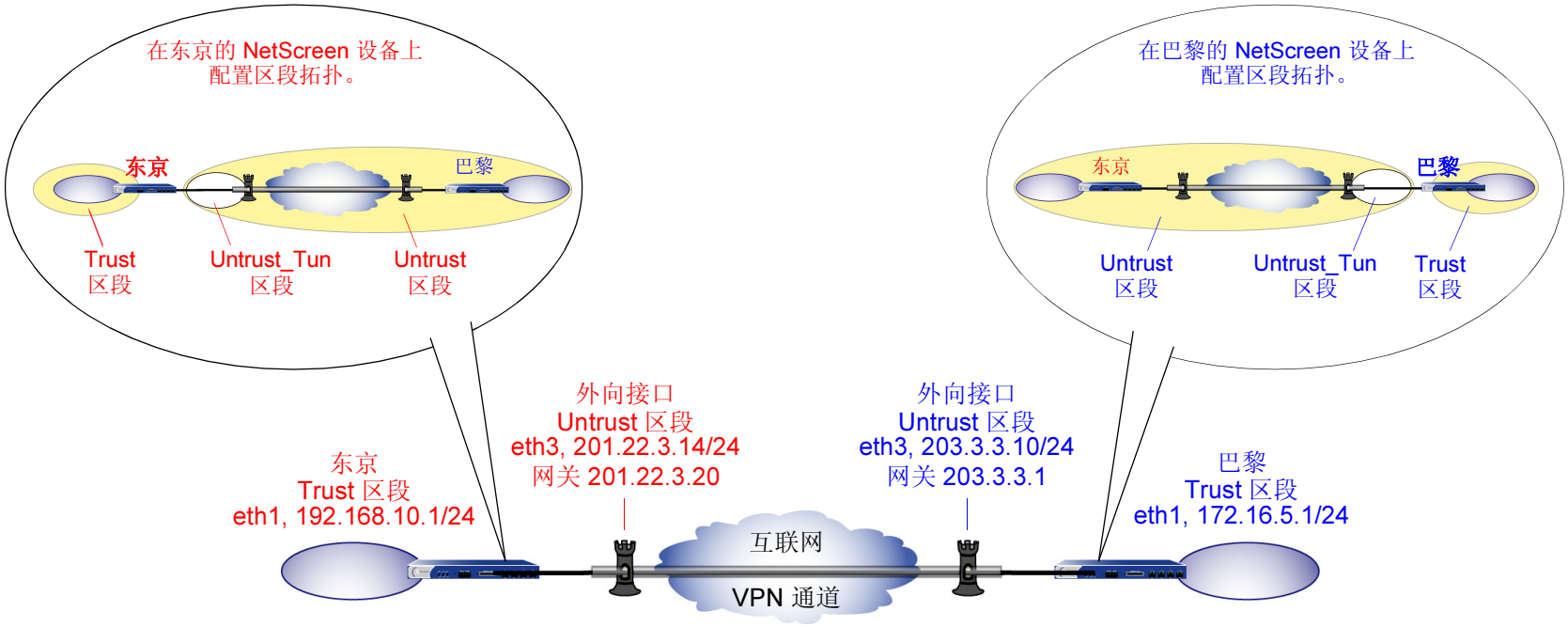
8. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.3.3.1

策略

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

范例：基于策略的 LAN 到 LAN 的 VPN，自动密钥 IKE

在本例中，“自动密钥 IKE”通道使用预共享机密或一对证书（每个通道端一个），提供东京和巴黎之间的安全通信连接。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”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，包括以下两个步骤：

1. 定义远程网关和密钥交换模式，并指定预共享密钥或证书。
2. 创建“自动密钥 IKE VPN”条目。

注意：完整的 “自动密钥 IKE” 配置还包括以下程序：

- *定义安全区段接口 IP 地址*
- *为本地及远程端实体生成通讯簿条目*
- *设置缺省路由*
- *策略配置*

因为这些步骤与在第 127 页上的 “范例：基于策略的 LAN 到 LAN 的 VPN，手动密钥”中的说明是相同的，因而在此忽略它们。

在以下例子中，预共享密钥为 h1p8A24nG5。假定两个参与者都已有 RSA 证书，并将 Entrust 作为证书授权机构 (CA)。（有关获得和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。）

WebUI (东京)

1. 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: 203.3.3.10

   （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 “网关” 配置页：

   Security Level: Custom

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

Mode (Initiator): Main (ID Protection)

（证书）

Outgoing Interface: ethernet3

> Advanced：输入以下高级设置，然后单击 OK，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

2. 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

WebUI (巴黎)

1. 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: 201.22.3.14

   （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)

   （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

2. 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

CLI (东京)

预共享密钥

1. set ike gateway to_paris ip 203.3.3.10 main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha-1
2. set vpn tokyo_paris gateway to_paris sec-level compatible
3. save

证书

1. set ike gateway to_paris ip 203.3.3.10 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
2. set ike gateway to_paris cert peer-ca 1[2]
3. set ike gateway to_paris cert peer-cert-type x509-sig
4. set vpn tokyo_paris gateway to_paris sec-level compatible
5. save

2. 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**。

CLI (巴黎)

预共享密钥

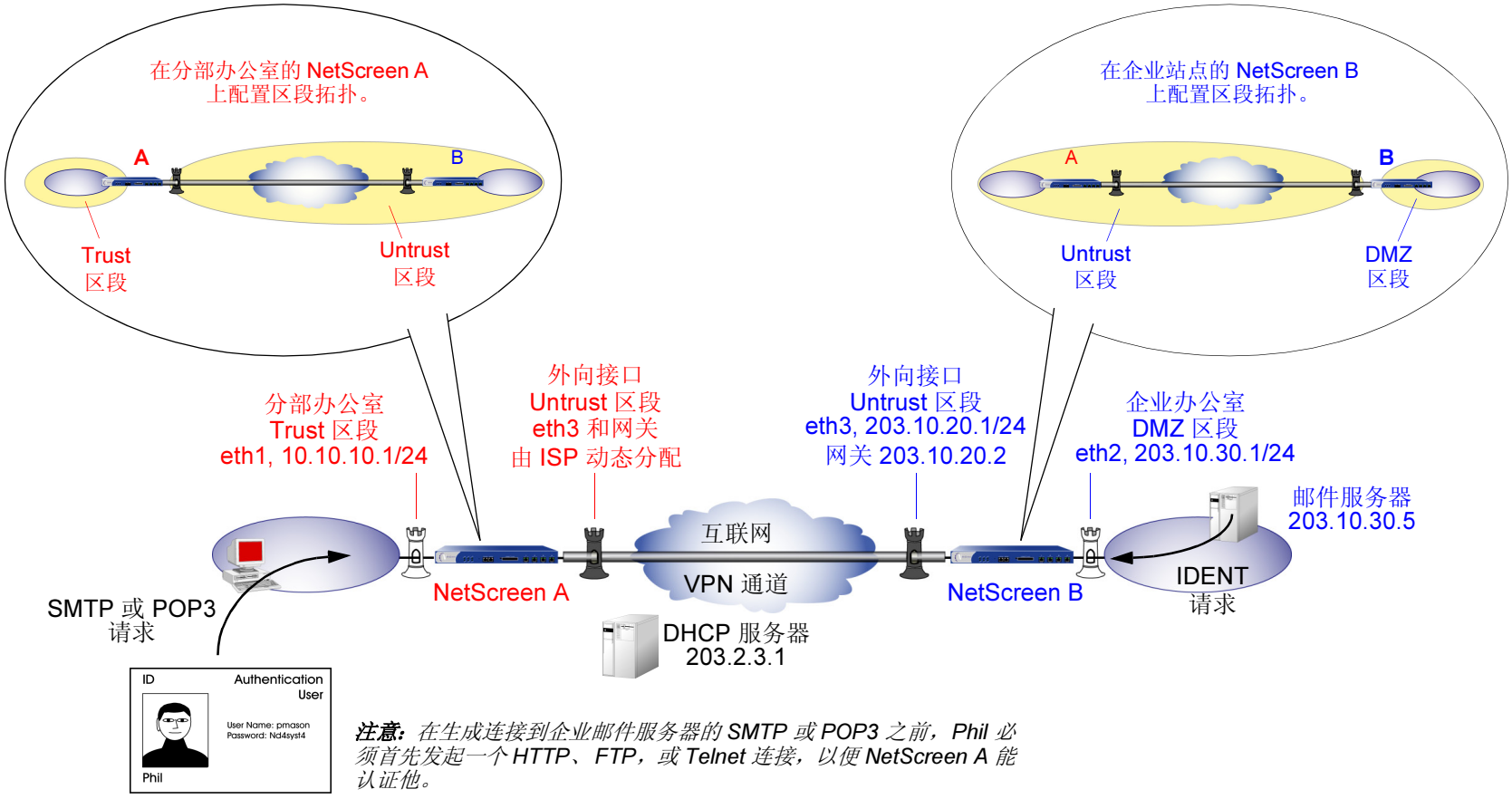
1. set ike gateway to_tokyo ip 201.22.3.14 main outgoing-interface ethernet3 preshare h1p8A24nG5 proposal pre-g2-3des-sha-1
2. set vpn paris_tokyo gateway to_tokyo sec-level compatible
3. save

证书

1. set ike gateway to_tokyo ip 201.22.3.14 main outgoing-interface ethernet3 proposal rsa-g2-3des-sha
2. set ike gateway to_tokyo cert peer-ca 1
3. set ike gateway to_tokyo cert peer-cert-type x509-sig
4. set vpn paris_tokyo gateway to_tokyo tunnel proposal nopfs-esp-3des-sha
5. save

范例：基于策略的 LAN 到 LAN 的 VPN，动态对等方

在本例中，VPN 通道安全地将 NetScreen A 后面的 Trust 区段中的用户连接到邮件服务器，该服务器在企业 DMZ 区段，并被 NetScreen B 保护。此 NetScreen B 的 Untrust 区段接口有一个静态的 IP 地址。服务 NetScreen A 的 ISP 将通过 DHCP 给它的 Untrust 区段接口动态分配 IP 地址。因为只有 NetScreen B 有其 Untrust 区段的固定地址，VPN 流量必须来自 NetScreen A 后面的主机。NetScreen A 建立通道之后，通过该通道的流量可来自任一端口。所有区域都在 trust-vr 路由域中。



***注意：**在生成连接到企业邮件服务器的 SMTP 或 POP3 之前，Phil 必须首先发起一个 HTTP、FTP，或 Telnet 连接，以便 NetScreen A 能认证他。*

在本例中，本地 auth 用户 Phil （登录名：pmason ；密码：Nd4syst4）要从企业站点的邮件服务器上获得他的电子邮件。当他试图这样做时，将被认证两次：首先，在允许流量从他那里通过通道[3]之前， NetScreen A 在本地认证他；其次，邮件服务器程序将认证他，并通过通道发送 IDENT 请求。

注意：*只有在 NetScreen A 和 NetScreen B 的管理员为邮件服务器添加了定制服务 （TCP，端口 113），并且设置了策略，允许流量通过通道到达 10.10.10.0/24 子网时，邮件服务器才能通过通道发送 IDENT 请求。*

预共享密钥为 h1p8A24nG5。此处假设两个参与者都已经拥有从证书授权机构 (CA) Verisign 获得的 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 （有关获得并下载证书的详细信息，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” 提议集。

WebUI (NetScreen A)

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.10.1/24

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**[4]：

   Zone Name: Untrust

   Obtain IP using DHCP（选择）

3. 因为 Phil 是一个认证用户，在他能提出一个 POP3 或 SMTP 请求之前，他必须首先发起一个 HTTP、FTP 或 Telnet 连接，以便 NetScreen A 能用一个防火墙用户 / 注册提示来认证他。得到 NetScreen A 认证后，将允许他通过 VPN 通道联系企业邮件服务器。

4. 不能通过 WebUI 指定 DHCP 服务器的 IP 地址，但通过 CLI 则可以。

用户

3. 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

地址

4. 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: 10.10.10.0/24

   Zone: Trust

5. 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: 203.10.30.5/32

   Zone: Untrust

服务

6. 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

7. 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

VPN

8. 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: 203.10.20.1
（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“网关”配置页：

Security Level: Custom

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

Mode (Initiator): Aggressive

（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“网关”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

9. 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

路由

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

Network Address/Netmask：0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 0.0.0.0[5]

策略

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

Source Address：

Address Book: （选择） , Trusted network

Destination Address：

Address Book: （选择） , Mail Server

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: branch_corp

Modify matching VPN policy: （选择）

Position at Top: （选择）

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

Authentication: （选择）

Auth Server: Local

User: （选择） , Local Auth User - pmason

5. ISP 通过 DHCP 动态提供网关 IP 地址。

WebUI (NetScreen B)

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet2）：输入以下内容，然后单击 **OK**：
   Zone Name: DMZ
   IP Address/Netmask：203.10.30.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 203.10.20.1/24

地址

3. 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）, 203.10.30.5/32
   Zone: DMZ
4. 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）, 10.10.10.0/24
   Zone: Untrust

服务

5. 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

6. 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

VPN

7. 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 “网关” 配置页：

Security Level: Custom

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

Mode (Initiator): Aggressive

（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): Aggressive

Preferred Certificate (optional):

Peer CA: Verisign

Peer Type: X509-SIG

8. 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

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 203.10.20.2

策略

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

Source Address:

Address Book: （选择）, Mail Server

Destination Address：

Address Book: （选择）, branch office

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: corp_branch

Modify matching VPN policy: （选择）

Position at Top: （选择）

CLI (NetScreen A)

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.10.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 dhcp
5. set dhcp client server 201.2.3.1

用户

6. set user pmason password Nd4syst4

地址

7. set address trust “trusted network” 10.10.10.0/24
8. set address untrust “mail server” 203.10.30.5/32

服务

9. set service ident protocol tcp src-port 0-65535 dst-port 113-113
10. set group service remote_mail
11. set group service remote_mail add http
12. set group service remote_mail add ftp
13. set group service remote_mail add telnet
14. set group service remote_mail add ident
15. set group service remote_mail add mail
16. set group service remote_mail add pop3

VPN

17. 预共享密钥：

    set ike gateway to_mail ip 203.10.20.1 aggressive outgoing-interface ethernet3 local-id pmason@abc.com 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 ip 203.10.20.1 aggressive outgoing-interface ethernet3 local-id pmason@abc.com proposal rsa-g2-3des-sha

    set ike gateway to_mail cert peer-ca 1[6]

    set ike gateway to_mail cert peer-cert-type x509-sig

    set vpn branch_corp gateway to_mail sec-level compatible

路由

18. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3[7]

策略

19. set policy top from trust to untrust “trusted network” “mail server” remote_mail tunnel vpn branch_corp auth server Local user pmason
20. set policy top from untrust to trust “mail server” “trusted network” remote_mail tunnel vpn branch_corp
21. save

6. 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**.
7. ISP 通过 DHCP 动态提供网关 IP 地址。

CLI (NetScreen B)

接口 – 安全区段

1. set interface ethernet2 zone dmz
2. set interface ethernet2 ip 203.10.30.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24

地址

5. set address dmz “mail server” 203.10.30.5/32
6. set address untrust “branch office” 10.10.10.0/24

服务

7. set service ident protocol tcp src-port 0-65535 dst-port 113-113
8. set group service remote_mail
9. set group service remote_mail add ident
10. set group service remote_mail add mail
11. set group service remote_mail add pop3

VPN

12. 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[8]

    set ike gateway to_branch cert peer-cert-type x509-sig

    set vpn corp_branch gateway to_branch sec-level compatible

路由

13. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2

策略

14. set policy top from dmz to untrust “mail server” “branch office” remote_mail tunnel vpn corp_branch
15. set policy top from untrust to dmz “branch office” “mail server” remote_mail tunnel vpn corp_branch
16. 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**。

拨号到 LAN 的 VPN

NetScreen 设备也支持 VPN 拨号连接。可以用静态 IP 地址配置 NetScreen 安全网关，以确保具有 NetScreen-Remote 客户端或具有动态 IP 地址的其它 NetScreen 设备的 IPSec 通道的安全。

可以为每个 VPN 拨号用户配置通道，或将用户安排到只需配置一个通道的 VPN 拨号组中。也可创建一组 IKE ID 用户，它允许定义一位用户，该用户的 IKE ID 用作拨号 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，原因是不必单独配置每个 IKE 用户。

***注意：**有关创建 IKE 用户组的详细信息，请参阅第 **2** -303 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 180 页上的 “组 IKE ID”。*

本节介绍三种类型 “拨号到 LAN 的 VPN” 的设置步骤：

- 拨号到 LAN 的 VPN，手动密钥通道
- 拨号到 LAN 的 VPN，自动密钥 IKE 通道 （具有预共享机密或证书）

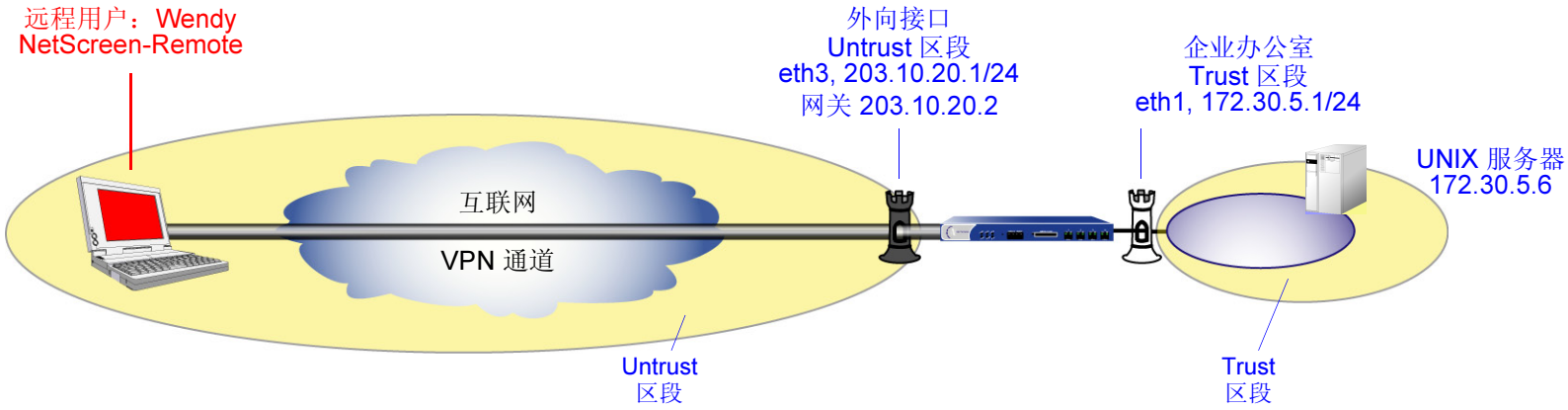
如果拨号客户端能支持 NetScreen-Remote 所支持的虚拟内部 IP 地址，则还可创建下列类型的 VPN 通道：

- 动态对等拨号到 LAN 的 VPN，自动密钥 IKE 通道 （具有预共享密钥或证书）

***注意：**除拨号客户端的内部 IP 地址为虚拟地址外，拨号到 LAN 动态对等与 “LAN 到 LAN” 动态对等几乎一样。*

范例：基于策略的拨号到 LAN 的 VPN，手动密钥

在本范例中，远程 “手动密钥” 用户 (Wendy) 需要通过拨号 VPN 通道访问企业网站 Trust 区段中的 UNIX 服务器。通道使用 3DES 进行加密，使用 SHA-1 进行认证。企业网站的所有区段都在 trust-vr 路由域中。



WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 172.30.5.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 203.10.20.1/24

地址

3. 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）, 172.30.5.6/24

Zone: Trust

手动密钥用户

4. Objects > Users > Manual Key > New：输入以下内容，然后单击 **OK**：

User Name: Wendy

Security Index: 3000 (Local), 3000 (Remote)

Outgoing Interface: ethernet3

ESP: （选择）

Encryption Algorithm: 3DES-CBC

Generate Key by Password: asdlk24234

Authentication Algorithm: SHA-1

Generate Key by Password[9] : PNas134a

9. 由于 NetScreen-Remote 将密码处理到密钥中，而与其它 NetScreen 产品不同，因此在配置通道后，应进行如下操作：(1) 在 “配置” 栏中为 “手动密钥” 用户 “Wendy” 单击 **Edit**，返回到 “Manual Key User” 配置对话框； (2) 复制生成的两个十六进制密钥；并且 (3) 在配置通道端的 NetScreen-Remote 时使用这些十六进制密钥。

路由

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3(untrust)

   Gateway IP Address: 203.10.20.2

策略

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

   Source Address:

   Address Book: （选择）, Dial-up VPN

   Destination Address:

   Address Book: （选择）, UNIX

   Service: ANY

   Action: Tunnel

   VPN Tunnel: Wendy

   Modify matching VPN policy: （不选）

   Position at Top: （选择）

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.30.5.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24

地址

5. set address trust unix 172.30.5.6/32

手动密钥用户

6. set user wendy dialup 3000 3000 outgoing-interface ethernet3 esp 3des password asdlk24234 auth sha-1 password PNas134a[10]

路由

7. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2

策略

8. set policy top from untrust to trust “Dial-Up VPN” unix any tunnel vpn-dialup wendy
9. save

10. 由于 NetScreen-Remote 将密码处理到密钥中，而与其它 NetScreen 产品不同，因此在配置通道后，应进行如下操作：(1) 输入命令 **get user wendy**；(2) 复制生成的两个十六进制密钥；并且 (3) 在配置通道端的 NetScreen-Remote 时使用这些十六进制密钥。

NetScreen-Remote Security Policy 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 ID Type: IP Address

   IP Address: 172.30.5.6

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 203.10.20.1

4. 单击位于 unix 图标左边的加号“**+**”，展开连接策略。
5. 单击 **Security Policy**，然后选择 **Use Manual Keys**。
6. 单击位于“Security Policy”图标左边的加号“**+**”，然后单击“Key Exchange”(Phase 2) 左边的加号“**+**”，进一步展开策略。
7. 单击 **Proposal 1**，然后选择下列 IPSec 策略：

   Encapsulation Protocol (ESP): （选择）

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

   Encapsulation: Tunnel

8. 单击 **Inbound Keys**，并在“Security Parameters Index”字段中键入 **3000**。
9. 单击 **Enter Key**，输入以下内容[11]，然后单击 **OK**：

   Choose key format: Binary

   ESP Encryption Key: dccbee96c7e546bc

   ESP Authentication Key: dccbe9e6c7e546bcb0b667794ab7290c
10. 单击 **Outbound Keys**，并且在“Security Parameters Index”字段中键入 **3000**。
11. 单击 **Enter Key**，输入以下内容[11]，然后单击 **OK**：

    Choose key format: Binary

    ESP Encryption Key: dccbee96c7e546bc

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

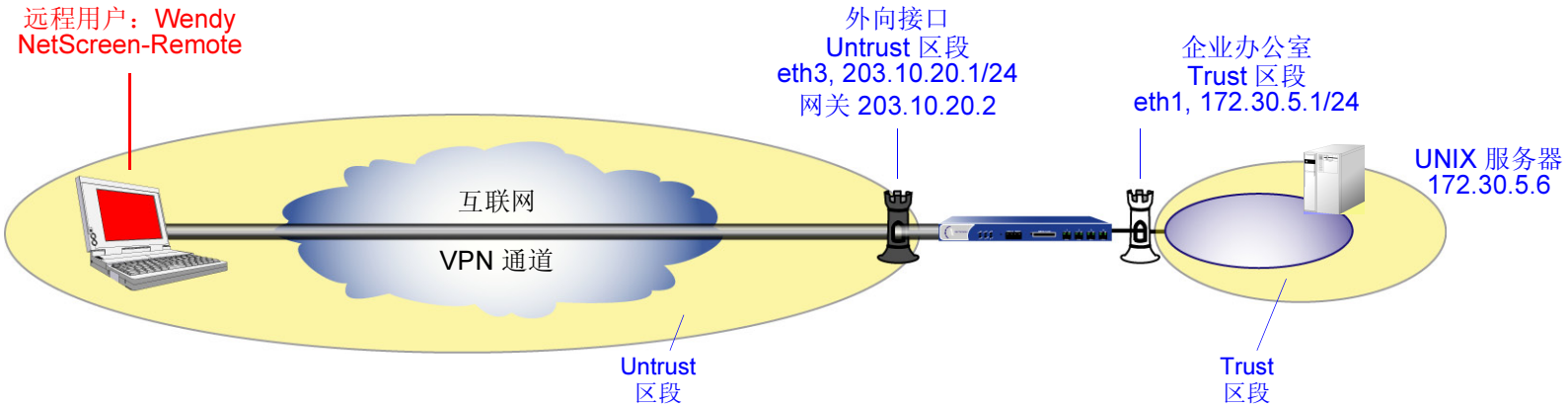
11. 它们是在配置 NetScreen 设备后所复制的两个生成的密钥。

范例：基于策略的拨号到 LAN 的 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[12] 的每端一个），提供 IKE 用户 Wendy 和 UNIX 服务器之间的安全通信通道。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，要求在企业网站执行以下操作：

1. 为 Trust 和 Untrust 区段配置接口，两个区段都在 trust-vr 路由域中。
2. 在 Trust 区段地址本中输入 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、允许从拨号用户访问 UNIX 的策略。



12. 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。（有关获得和加载证书的信息，请参阅第 29 页上的 “证书和 CRL”。）对于第 1 阶段和第 2 阶段安全级别，指定一个第 1 阶段协议（预共享密钥方法为 pre-g2-3des-sha 或证书为 rsa-g2-3des-sha）并选择第 2 阶段协议预定义的 “Compatible” 设置。

WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 172.30.5.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 203.10.20.1/24

地址

3. 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）, 172.30.5.6/32

   Zone: Trust

用户

4. 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

VPN

5. 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：输入下列高级设置，然后单击 **Return**，返回到基本 “网关” 配置页：

Security Level: Custom

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

Mode (Initiator): Aggressive

（证书）

Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，然后单击 **Return**，返回到基本 “网关” 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. 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

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 203.10.20.2

策略

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

Source Address:

Address Book: （选择） , Dial-Up VPN

Destination Address:

Address Book: （选择） , UNIX

Service: ANY

Action: Tunnel

Tunnel VPN: Wendy_UNIX

Modify matching VPN policy: （清除）

Position at Top: （选择）

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 172.30.5.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24

地址

5. set address trust unix 172.30.5.6/32

用户

6. set user wendy ike-id u-fqdn wparker@email.com

VPN

7. 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-1

   set ike gateway wendy_nsr cert peer-ca 1[13]

   set ike gateway wendy_nsr cert peer-cert-type x509-sig

   set vpn wendy_unix gateway wendy_nsr sec-level compatible

路由

8. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2

策略

9. set policy top from untrust to trust “Dial-Up VPN” unix any tunnel vpn wendy_unix
10. save

13. 数字 1 为 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。

NetScreen-Remote Security Policy 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 ID Type: IP Address

   IP Address: 172.30.5.6

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 203.10.20.1

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 类型：（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 类型：（选择 **E-mail Address**）[14]

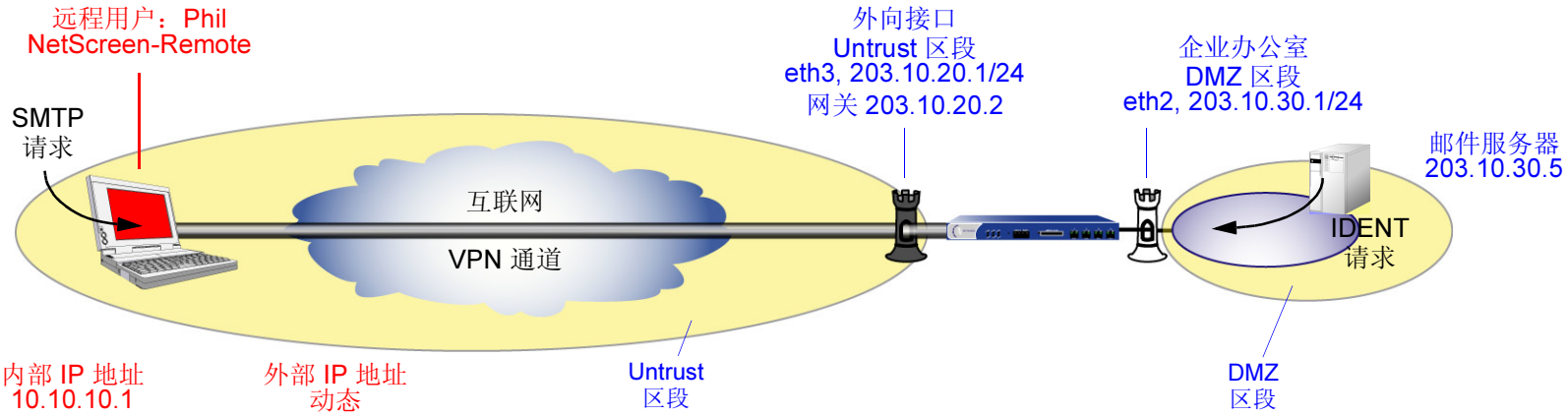
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
7. 单击位于“Security Policy”图标左边的加号“+”，然后单击“Authentication”(Phase 1) 和“Key Exchange”(Phase 2) 左边的加号“+”，进一步展开策略。

14. 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“加密”和“数据完整性算法”：
   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 **Save**。

范例：基于策略的拨号到 LAN 的 VPN，动态对等

在本范例中，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，从而保护 DMZ 区段中的邮件服务器。Untrust 区段接口拥有一个静态 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这两个地址，以便将它们添加到 Untrust 通讯薄中，用于在策略中从该源用通道传送流量。NetScreen-Remote 客户端建立通道后，通过通道的流量可来自任一端。



在本范例中， Phil 希望从公司网站的邮件服务器上获得他的电子邮件。当他尝试这样做时，邮件服务器程序对他进行认证，借助通道向他发送一条 IDENT 请求。

注意：*只有在 NetScreen 管理员为它添加了定制服务 （TCP，端口 113），并且设置了外向策略，允许流量通过通道到达 10.10.10.1 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@netscreen.com*。（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”。）对于第 1 阶段和第 2 阶段安全级别，指定一个第 1 阶段协议 （预共享密钥方法为 pre-g2-3des-sha 或证书为 rsa-g2-3des-sha）并选择第 2 阶段协议预定义的 “Compatible” 设置。

WebUI

接口 – 安全区段

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

   Zone Name: DMZ

   IP Address/Netmask: 203.10.30.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 203.10.20.1/24

地址

3. 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: 203.10.30.5/32

   Zone: DMZ

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

   Address Name: Phil

   IP Address/Domain Name:

   IP/Netmask: 10.10.10.1/32

   Zone: Untrust

服务

5. 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

6. Objects > Services > Group > New：输入以下内容，运行以下服务，然后单击 **OK**：

   Group Name: Remote_Mail

   Group Members << Available Members:

   Ident
   MAIL
   POP3

VPN

7. 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@netscreen.com

   （预共享密钥）

   Preshared Key: h1p8A24nG5

   Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，然后单击 **Return**，返回到基本“网关”配置页：

Security Level: Custom

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

Mode (Initiator): Aggressive

（证书）

Outgoing Interface: ethernet3

> Advanced：输入下列高级设置，然后单击 **Return**，返回到基本“网关”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

8. 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

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 203.10.20.2

策略

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

Source Address:

Address Book: （选择）, Phil

Destination Address:

Address Book: （选择）, Mail Server

Service: Remote_Mail

Action: Tunnel

VPN Tunnel: corp_Phil

Modify matching VPN policy: （选择）

Position at Top: （选择）

CLI

接口 – 安全区段

1. set interface ethernet2 zone dmz
2. set interface ethernet2 ip 203.10.30.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 203.10.20.1/24

地址

5. set address dmz “mail server” 203.10.30.5/32
6. set address untrust phil 10.10.10.1/32

服务

7. set service ident protocol tcp src-port 0-65535 dst-port 113-113
8. set group service remote_mail
9. set group service remote_mail add ident
10. set group service remote_mail add mail
11. set group service remote_mail add pop3

VPN

12. 预共享密钥：

    set ike gateway to_phil dynamic pm@netscreen.com 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@netscreen.com aggressive outgoing-interface ethernet3 proposal rsa-g2-3des-sha

    set ike gateway to_phil cert peer-ca 1[15]

    set ike gateway to_phil cert peer-cert-type x509-sig

    set vpn corp_phil gateway to_phil sec-level compatible

路由

13. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 203.10.20.2

策略

14. set policy top from untrust to dmz phil “mail server” remote_mail tunnel vpn corp_phil
15. set policy top from dmz to untrust “mail server” phil remote_mail tunnel vpn corp_phil
16. save

15. 数字 1 为 CA ID 号。要发现 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

   IP Address: 203.10.30.5

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 203.10.20.1

5. 单击位于 unix 图标左边的加号“**+**”，展开连接策略。
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
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**。

   内部网络 IP 地址：10.10.10.1

   ID 类型：电子邮件地址； pm@netscreen.com

   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。

   内部网络 IP 地址：10.10.10.1

   ID 类型：电子邮件地址； pm@netscreen.com

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“加密”和“数据完整性算法”：
   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 **Save**。

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，其中许多用户在断开网站时要求保证拨号到 LAN 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、拨号到 LAN 的 VPN 配置以及策略是不切实际的。

为了消除这种麻烦，“组 IKE ID”方法建立一个可用于多个用户的用户定义。组 IKE ID 用户定义适用于具有在 distinguished name（识别名称）(dn) 中有指定值的证书的所有用户，也适用于全部 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。

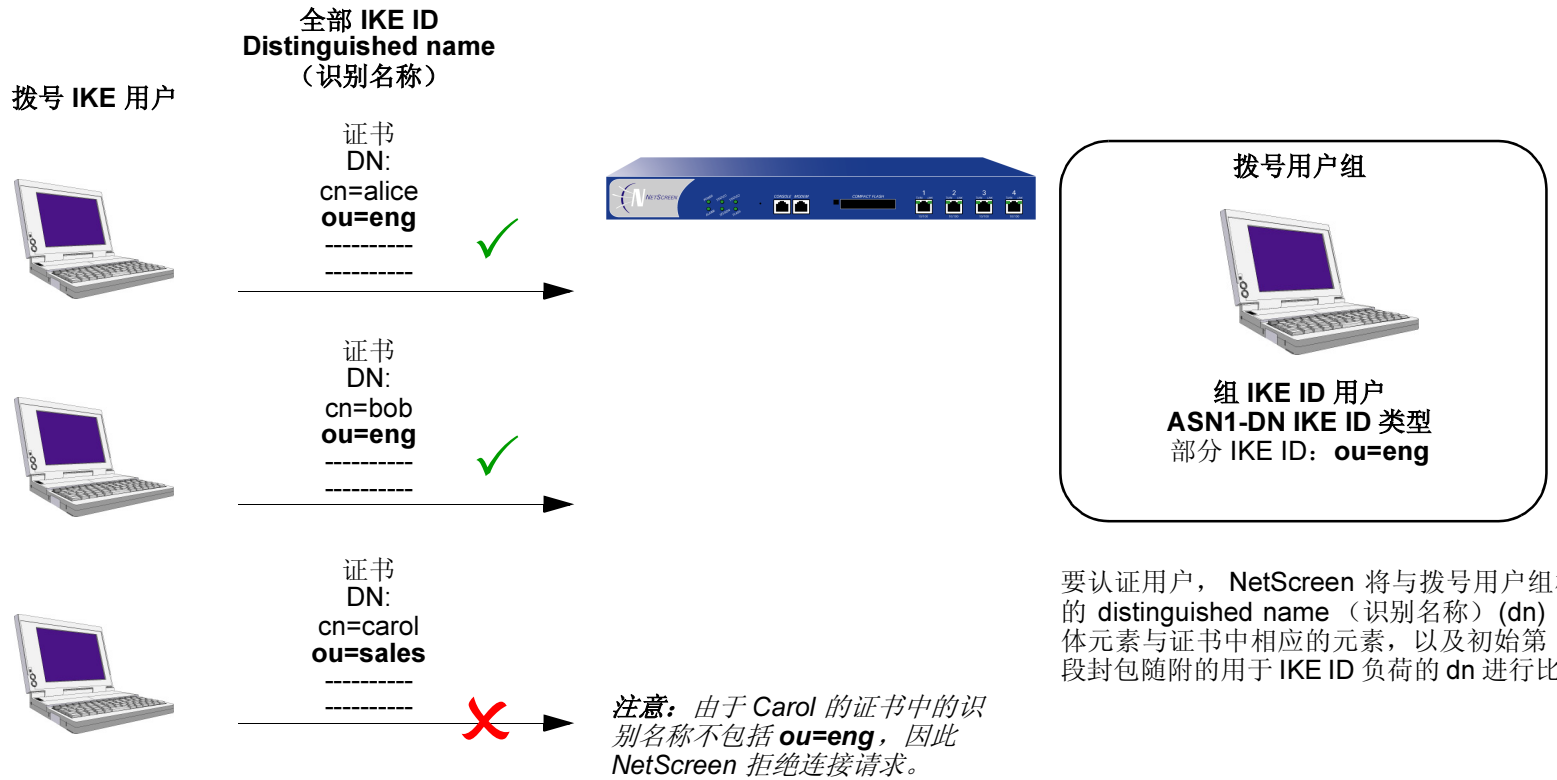
注意：*拨号 IKE 用户连接到 NetScreen 设备时， NetScreen 设备首先提取并使用全部 IKE ID，搜索其对等方网关记录以防用户不属于组 IKE ID 用户组。如果全部 IKE ID 搜索过程没有匹配条目， Netscreen 设备则检查内向嵌入的 IKE ID 和配置的组 IKE ID 用户之间的部分 IKE ID 匹配。*

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最大 “第 1 阶段 SA”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” 是一项技术，对一组没有为每个用户配置单独的用户简介的拨号 IKE 用户执行 IKE 认证。相反，NetScreen 设备使用包含部分 IKE ID 的单组 IKE ID 用户简介。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，该元素使这些配置与 NetScreen device 上的组 IKE ID 用户简介中的部分 IKE ID 定义相匹配。

具有证书的组 IKE ID



要认证用户， NetScreen 将与拨号用户组相关的 distinguished name （识别名称）(dn) 的具体元素与证书中相应的元素，以及初始第 1 阶段封包随附的用于 IKE ID 负荷的 dn 进行比较。

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 标识的组 IKE ID 用户（如 *ou=sales，o=netscreen*），并指定可使用组 IKE ID 简介进行登录的拨号用户数量。
2. 将新的组 IKE ID 用户指派到一个拨号用户组[16]，并命名该组。
3. 在拨号到LAN 自动密钥 IKE VPN 配置中，指定拨号用户组的名称，第 1 阶段协商处于Aggressive mode（主动模式），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）用于认证。
4. 创建允许入站流量通过指定的拨号 VPN 的策略。

在 VPN 客户端上：

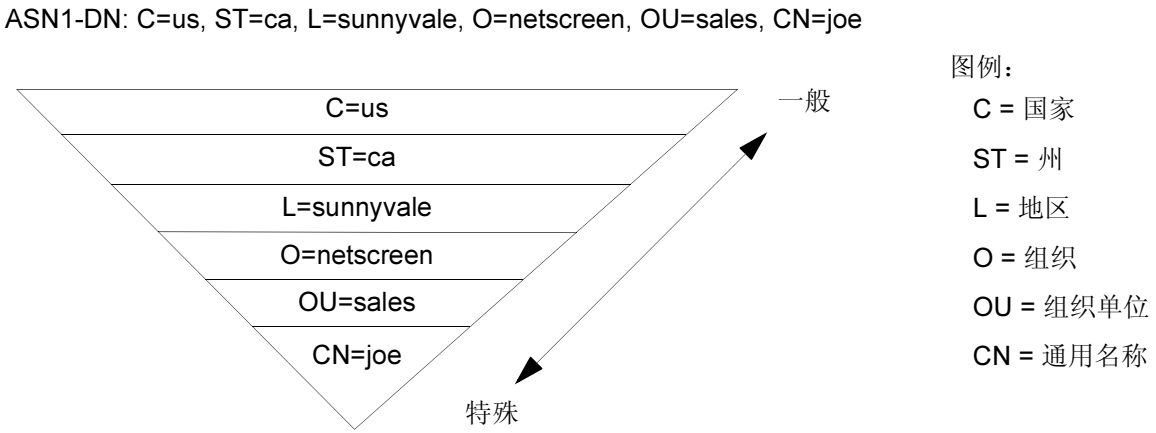
1. 获得并加载证书，该证书的识别名称包含的信息和在 NetScreen 设备上部分 IKE ID 中定义的信息相同。
2. 对于第 1 阶段协商，使用 Aggressive mode（主动模式）配置通向 NetScreen 设备的 VPN 通道，指定之前已经加载的证书，并为本地 IKE ID 类型选择 *识别名称*。

此后，每个具有证书（识别名称元素与组 IKE ID 用户简介中定义的部分 IKE ID 匹配）的单个拨号 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 设备接受来自任意用户的第 1 阶段协商，该用户拥有在其识别名称中包含这些元素的证书。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 用户简介中指定的并发会话的最大数量。

16. 可以只将一组 IKE ID 用户放置在 IKE 用户组中。

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 （但并非总是）是从一般到特殊。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：

- **Wildcard （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。对于每个标识字段， Wildcard （通配符）ID 仅支持一个值 （例如，支持 “ou=eng or 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并不重要。
- **Container （容器）**：如果拨号 IKE 用户的 ASN1-DN 标识字段中的值完全匹配组 IKE 用户的 ASN1-DN 标识字段中的值，则 NetScreen 认证拨号 IKE 用户的 ID。对于每个标识字段， Container （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。

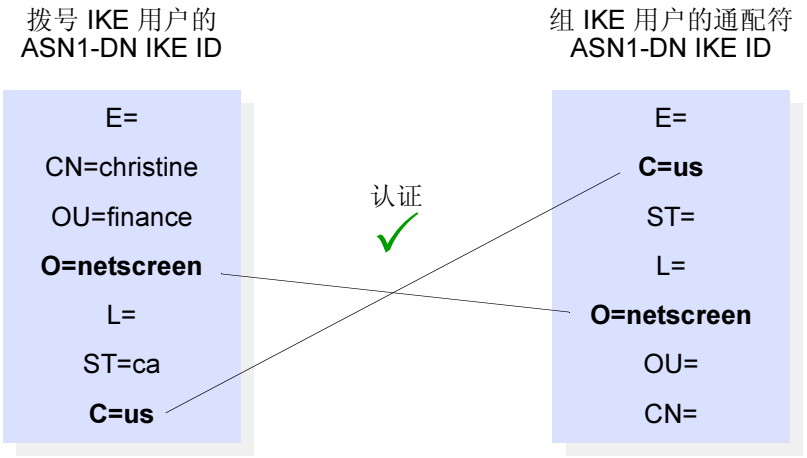
Wildcard （通配符）ASN1-DN IKE ID

通配符 ASN1-DN 要求远程对等方的 distinguished name（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并不重要。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。

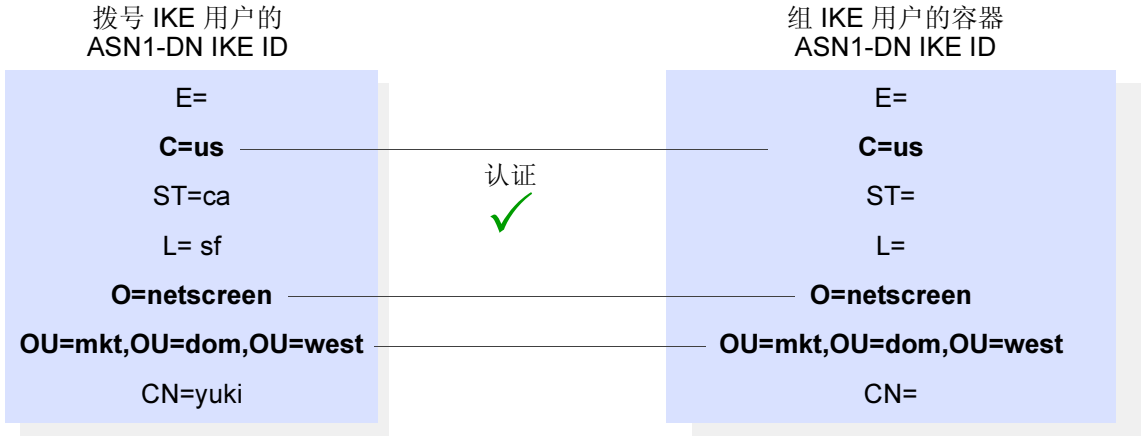
拨号 IKE 用户的 ASN1-DN 包含在组 IKE 用户的 ASN1-DN 中指定的值。值的顺序并不重要。



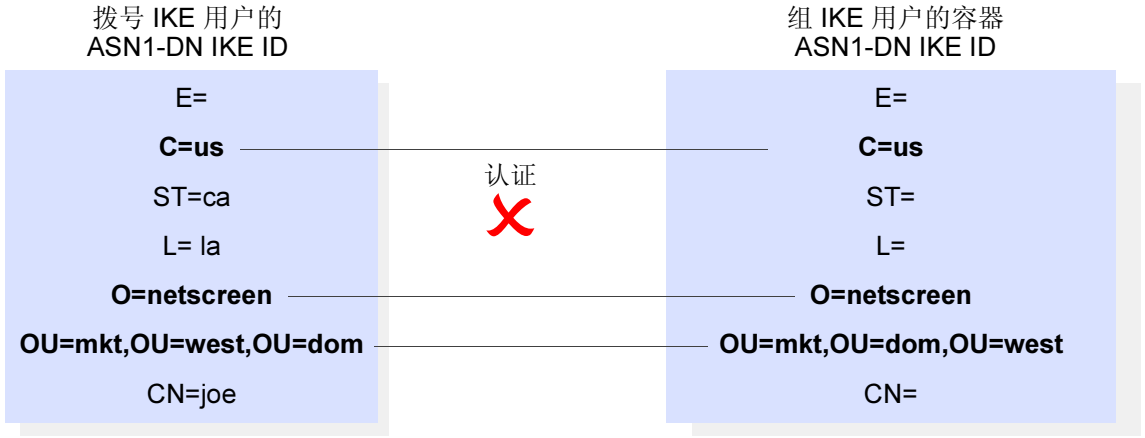
Container （容器） ASN1-DN IKE ID

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 认证组 IKE 用户。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 字段的顺序必须一样，并且这些字段中多个值的顺序也必须一样。

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一样。

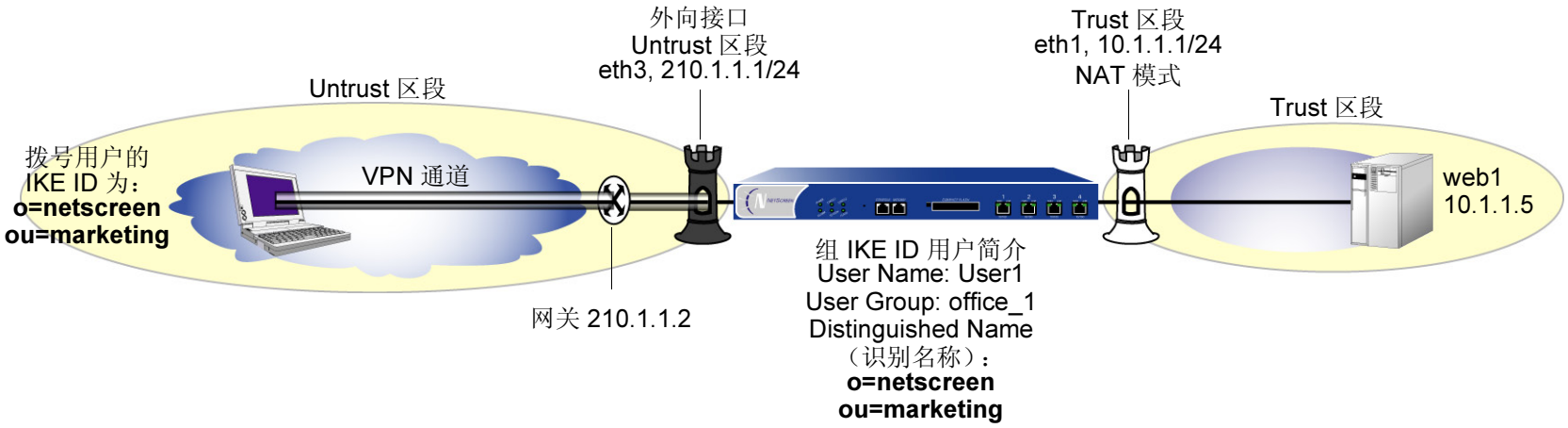


第二个拨号 IKE 用户的 ASN1-DN 包含与组 IKE 用户的 ASN1-DN 完全匹配的值。但是， OU ID 字段中多个条目的顺序不一样。



范例：组 IKE ID （证书）

在本范例中，创建命名为 *User1* 的新的组 IKE ID 用户定义。将其配置为从具有 RSA 证书的 VPN 客户端同时接受数量多达 10 个的第 1 阶段协商，该证书包含 *O=netscreen* 和 *OU=marketing*。证书授权机构 (CA) 为 Verisign。将拨号 IKE 用户组命名为 *office_1*。



拨号 IKE 用户发送识别名称作为它们的 IKE ID。此组中拨号 IKE 用户的证书中的 Distinguished Name （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，并且用户使用识别名称作为其 IKE ID 类型，因此 NetScreen 设备会认证用户。

对于第 1 阶段和第 2 阶段的安全级别，指定一个第 1 阶段协议 （证书为 rsa-g2-3des-sha），并为第 2 阶段协议选择预定义的 “Compatible” 设置。

配置拨号到 LAN 的 VPN 和一个策略，允许 HTTP 流量通过 VPN 通道到达 Web 服务器 *Web1*。其中也包括远程 VPN 客户端 （使用 NetScreen-Remote）的配置。

WebUI

接口 – 安全区段

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/24
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 210.1.1.1/24

地址

3. 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

用户

4. Objects > User Groups > Local > New：输入以下内容，然后单击 **OK**：
   Group Name: office_1
5. Objects > Users > Local > New：输入以下内容，然后单击 **OK**：
   User Name: User1
   User Group: office_1
   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: netscreen

VPN

6. 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：输入下列高级设置，然后单击 **Return**，返回到基本“网关”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

7. 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

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3(untrust)

Gateway IP Address: 210.1.1.2

策略

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

Source Address:

Address Book: （选择）, Dial-Up VPN

Destination Address:

Address Book: （选择）, web1

Service: HTTP

Action: Tunnel

Tunnel VPN: Corp_VPN

Modify matching VPN policy: （清除）

Position at Top: （选择）

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 210.1.1.1/24

地址

5. set address trust web1 10.1.1.5/32

用户

6. set user User1 ike-id asn1-dn wildcard o=netscreen,ou=marketing share-limit 10
7. set dialup-group office_1 + User1

VPN

8. set ike gateway Corp_GW dialup office_1 aggressive outgoing-interface ethernet3 proposal rsa-g2-3des-sha
9. set ike gateway Corp_GW cert peer-ca 1[17]
10. set ike gateway Corp_GW cert peer-cert-type x509-sig
11. set vpn Corp_VPN gateway Corp_GW sec-level compatible

策略

12. set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn-dialup Corp_VPN
13. save

17. 数字 1 为 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。

NetScreen-Remote Security Policy 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 ID Type: IP Address

   IP Address: 10.1.1.5

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 210.1.1.1

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[18] 中，选择在 distinguished name（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，然后选择 **Aggressive Mode**。
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: RSA Signatures

   Encrypt Alg: Triple DES

   Hash Alg: SHA-1

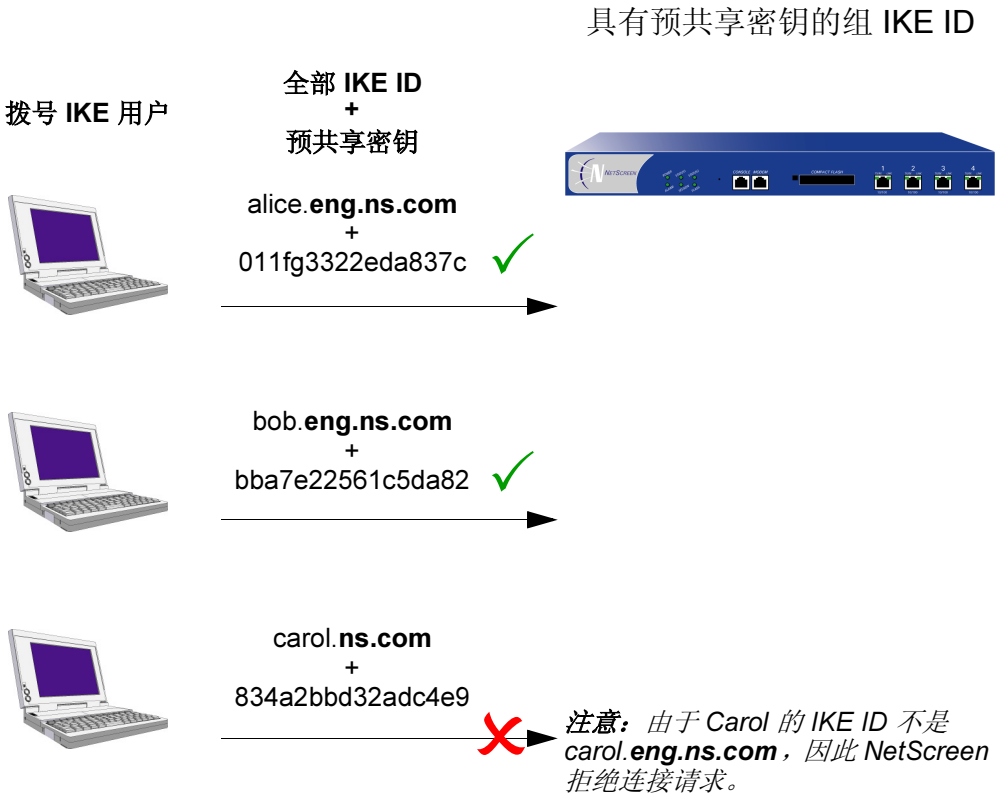
   Key Group: Diffie-Hellman Group 2

18. 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 **Save**。

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，对一组没有为每个用户配置单独的用户简介的拨号 IKE 用户执行 IKE 认证。相反， NetScreen 设备使用包含部分 IKE ID 的单组 IKE ID 用户简介。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，并且如果用户的全部 IKE ID 的最靠右侧部分与组 IKE ID 用户简介的部分 IKE ID 定义相匹配。



IKE 用户发送全部 IKE ID 时，NetScreen 在发送过程中产生预共享密钥。

（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 阶段封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 **netscreen.com**），并指定可使用组 IKE ID 简介进行登录的拨号用户数量。
2. 将新的组 IKE ID 用户指派为拨号用户组。
3. 在拨号到 LAN 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@netscreen.com**）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@netscreen.com**
5. 配置远程 VPN 客户端时，记录预共享密钥以供使用。

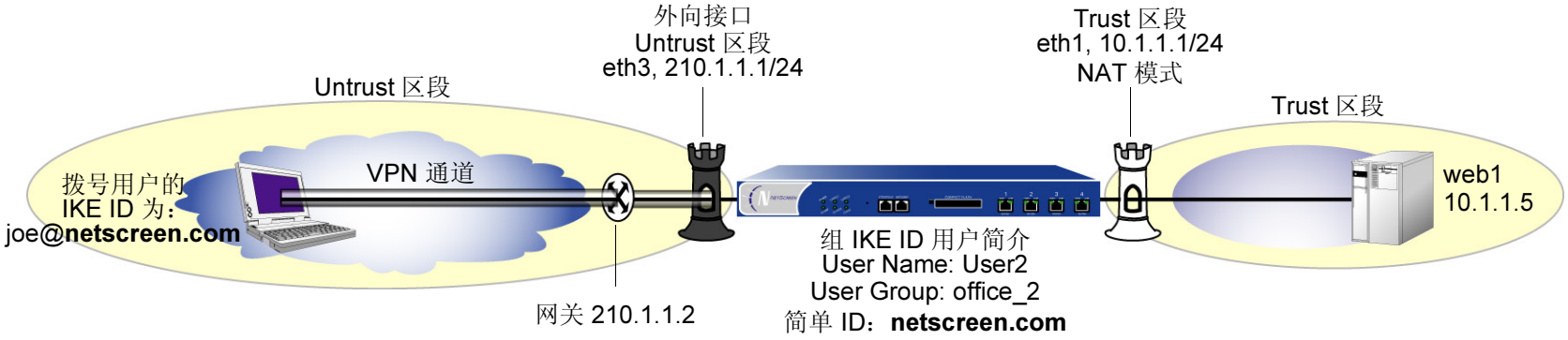
在 VPN 客户端上：

对于第 1 阶段协商，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单独的用户，该用户的全部 IKE ID 包含一部分与部分组 IKE ID 用户简介相匹配的内容。例如，如果组 IKE ID 用户具有 IKE 标识 **netscreen.com**，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 设备上发起第 1 阶段 IKE 协商。例如：**alice@netscreen.com**、**bob@netscreen.com** 和 **carol@netscreen.com**。可登录的用户数量取决于在组 IKE ID 用户简介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。将其配置为从具有预共享密钥的 VPN 客户端同时接受数量多达 10 个的第 1 阶段协商，该预共享密钥包含由字符串 *netscreen.com* 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*。



对于第 1 阶段和第 2 阶段协商，选择预定义为 “Compatible”的安全级别。所有安全区段都在 trust-vr 路由域中。

WebUI

接口 – 安全区段

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

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

地址

3. 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

用户

4. Objects > User Groups > Local > New：输入以下内容，然后单击 **OK**。

   Group Name: office_2

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

   User Name: User2

   User Group: office_2

   Status: Enable

   IKE User: （选择）

   Number of Multiple Logins with same ID: 10

   Simple Identity: （选择）

   IKE Identity: netscreen.com

VPN

> ***注意：****WebUI 仅允许输入一个预共享密钥值，不允许输入从 NetScreen 设备衍生的预共享密钥的种子值。要在配置 IKE 网关时输入预共享密钥种子值，必须使用 CLI。*

6. 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

路由

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3(untrust)

   Gateway IP Address: 210.1.1.2

策略

8. Policies > (From: Untrust, To: Trust) New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: （选择） , Dial-Up VPN
   Destination Address:
   Address Book: （选择） , web1
   Service: HTTP
   Action: Tunnel
   Tunnel VPN: Corp_VPN
   Modify matching VPN policy: （清除）
   Position at Top: （选择）

CLI

接口 – 安全区段

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 210.1.1.1/24

地址

5. set address trust web1 10.1.1.5/32

用户

6. set user User2 ike-id u-fqdn netscreen.com share-limit 10
7. set user-group office_2 user User2

VPN

8. set ike gateway Corp_GW dialup office_2 aggressive seed-preshare jk930k sec-level compatible
9. set vpn Corp_VPN gateway Corp_GW sec-level compatible

策略

10. set policy top from untrust to trust “Dial-Up VPN” web1 http tunnel vpn Corp_VPN
11. 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*（在命名为 *Corp_GW* 的远程网关的配置中指定），以及单个用户 *joe@netscreen.com* 全部标识的预共享密钥为 *11ccce1d396f8f29ffa93d11257f691af96916f2*。

NetScreen-Remote Security Policy 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 ID Type: IP Address

   IP Address: 10.1.1.5

   Connect using Secure Gateway Tunnel: （选择）

   ID Type: IP Address; 210.1.1.1
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，然后选择 **Aggressive Mode**。

6. 单击 **My Identity**：单击 **Pre-shared Key** > **Enter Key**：键入 **11ccce1d396f8f29ffa93d11257f691af96916f2**，然后单击 **OK**。

   ID 类型：（选择 **E-mail Address**），然后键入 **joe@netscreen.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
   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：

   Encapsulation Protocol (ESP): （选择）
   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：

    Encapsulation Protocol (ESP): （选择）
    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：

    Encapsulation Protocol (ESP): （选择）
    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 **Save**。

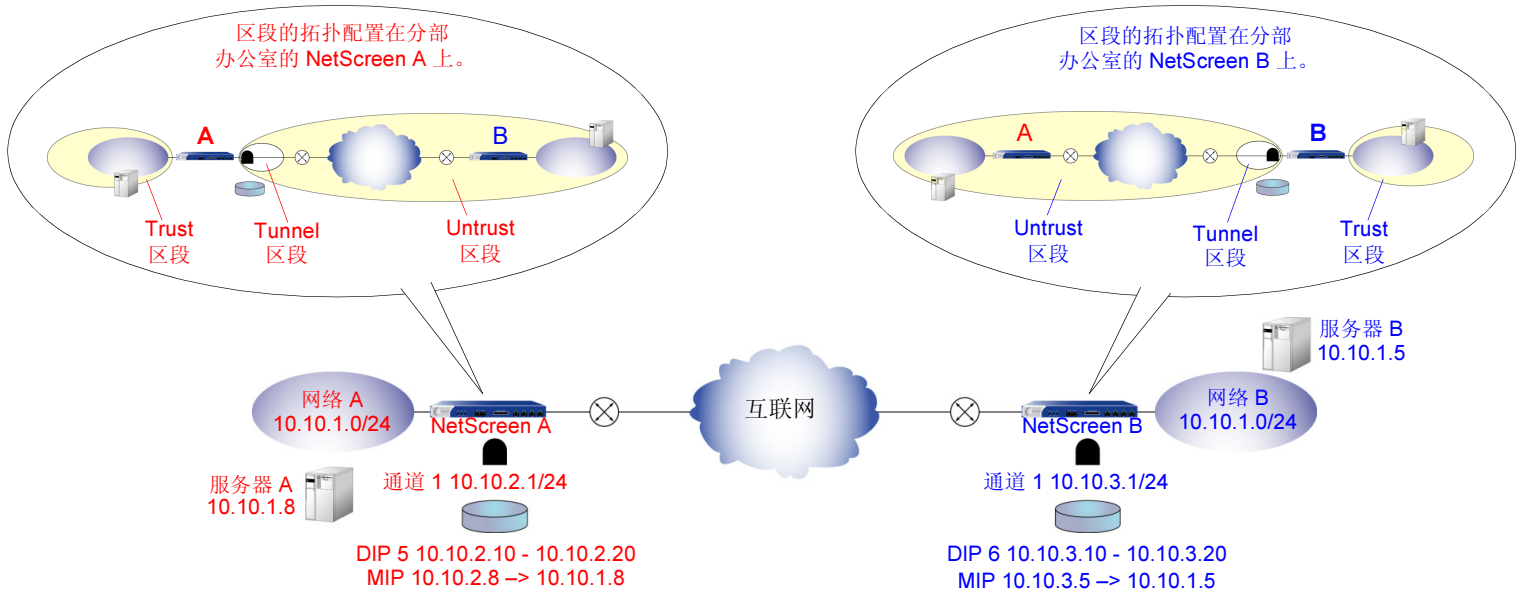
TUNNEL 区段和基于策略的 NAT

Tunnel 区段是一个允许您将一个或多个通道接口绑定到该区段的逻辑创造物。如果将通道接口绑定到安全区段，就可以将通道接口配置成无编号的 （也就是没有 IP 地址），或给它指定一个 IP 地址和网络掩码。如果将一个通道接口绑定到一个安全区段，就必须给它指定一个 IP 地址。

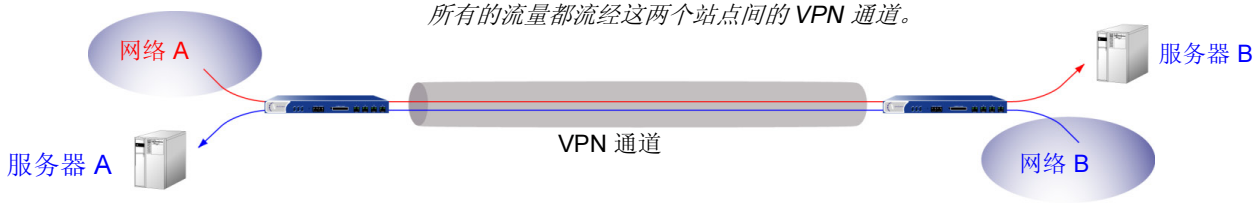
为通道接口给定一个 IP 地址和掩码将自动在该接口的路由表中制作一个条目。它还允许您在同一个子网中创建一个或多个 “动态 IP (DIP)” 池，用于申请流经此接口的流量上的基于策略的网络地址转换 (NAT)[19]。在源地址和目标地址位于重叠地址空间中的情况下[20]，可以使用基于策略的 NAT 将出站流量上的源地址更改为中立地址空间的地址。在通道的另一端，可以使用中立空间中的其它地址创建一个映射的 IP (MIP)。对于两端实体间具有重叠地址的双向 VPN 通道，通道的两端都需要基于策略的 NAT 和 MIP。

19. DIP 池中的地址范围必须在与通道接口相同的子网中，但是该池必须不包括可能也在此子网中的接口 IP 地址、任何 MIP 或 VIP 地址。对于安全区段接口，还可以在与接口 IP 地址不同的子网中定义一个扩展的 IP 地址和一个随附的 DIP 池。有关详细信息，请参阅第 **2**-129 页上的 “扩展接口和 DIP”。

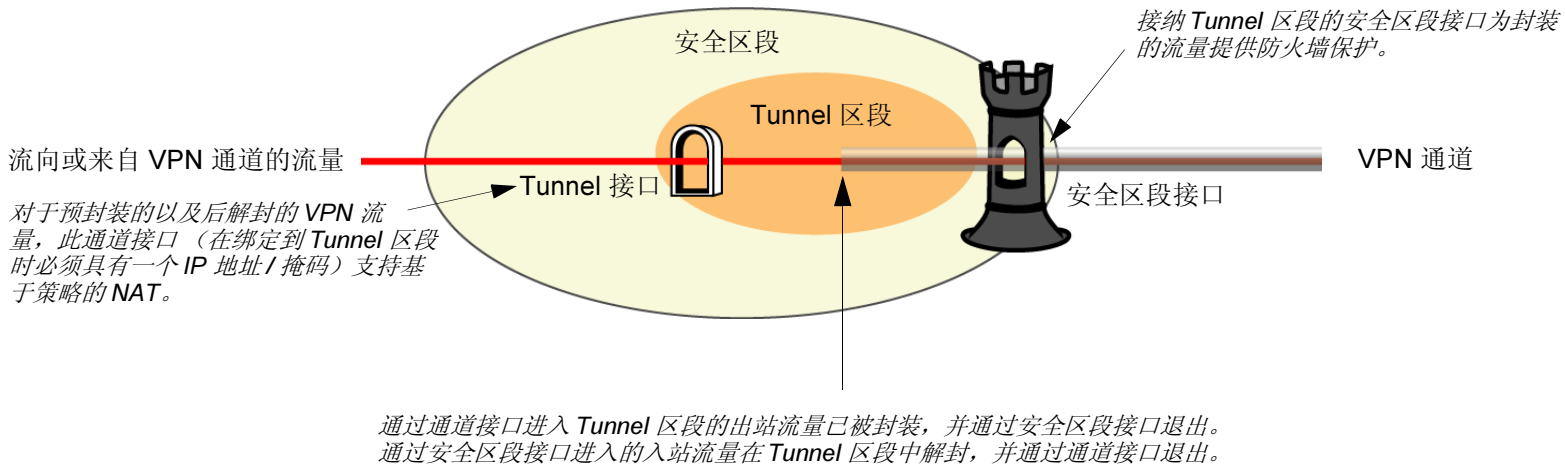
20. 重叠地址空间就是当两个网络中 IP 地址范围部分或全部相同时的空间。



网络 A 上的用户可以访问服务器 B。网络 B 上的用户可以访问服务器 A。
所有的流量都流经这两个站点间的 VPN 通道。



Tunnel 区段在概念上以一种“子父”关系附属于安全区段。安全区段充当“父”，您也可以将其想象为载体区段，该区段对封装的流量提供防火墙保护。Tunnel 区段提供封包封装 / 解封，还提供基于策略的 NAT 服务（通过支持具有可以接纳 DIP 池的 IP 地址和掩码的通道接口）。



当从 3.1.0 以下版本的 ScreenOS 升级时，缺省情况下，现有的通道接口被绑定到预配置的 Untrust-Tun 通道区段，该区段是预配置的 Untrust 安全区段的 “子” 区段。可以将多个 Tunnel 区段绑定到同一个安全区段，但是不可以将一个 Tunnel 区段绑定到另一个 Tunnel 区段。

范例：具有 MIP 和 DIP 的 Tunnel 接口

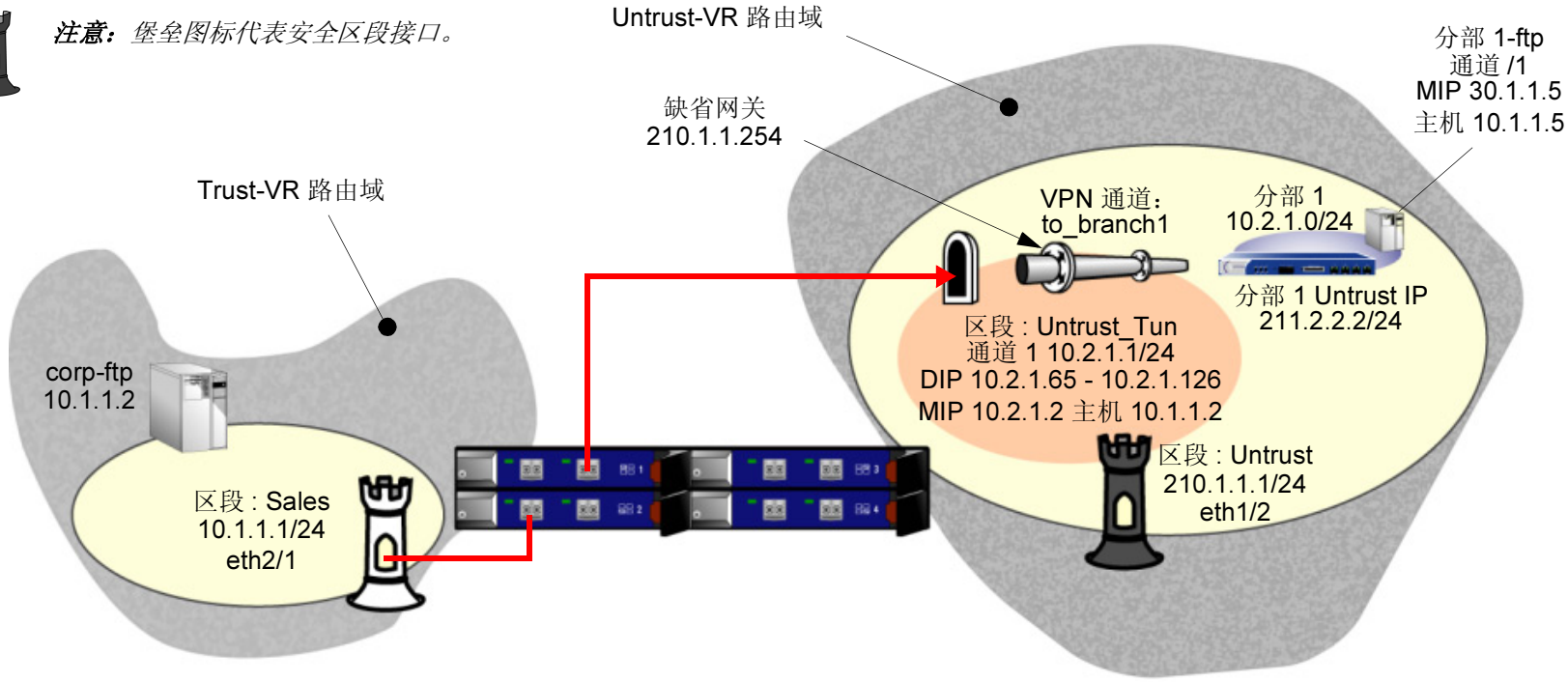
在此示例中，将在公司站点和分部办公室站点间配置一个 VPN 通道，但是， VPN 端实体的地址空间是重叠的。要解决此冲突，可以使用 NAT 修改出站 VPN 流量上的源地址以及用 MIP 修改入站 VPN 流量上的目标地址。

通道两端的 NetScreen 设备的通道参数和 ScreenOS 版本如下 :

- 第 1 阶段和第 2 阶段协议的 “自动密钥 IKE”、预共享密钥 (netscreen1)、预先定义为 “Compatible” 的安全级别 （有关这些协议的详细信息，请参阅第 11 页上的 “通道协商”。）
- 在公司站点上指定为本地网关的接口是 210.1.1.1/24。（分部办公室用此地址作为 IKE 配置中的远程网关。）
- 在分部办公室站点上指定为本地网关的接口是 211.2.2.2/24。（公司站点用此地址作为 IKE 配置中的远程网关。）
- 公司站点上的 NetScreen 设备运行 3.1.0 以上版本的 ScreenOS。
- 分部办公室的 NetScreen 设备运行 3.1.0 以下版本的 ScreenOS。

注意： *下面只给出了通道的公司端配置。有关配置运行 3.1.0 以下版本的 ScreenOS 的 NetScreen 设备的详细信息，请参阅* NetScreen 概念与范例 ScreenOS *参考指南以获取适合于您的设备的 ScreenOS 版本。*

注意： *堡垒图标代表安全区段接口。*



WebUI

安全区段和虚拟路由器

1. Network > Interfaces > Edit（对于 ethernet1/2）：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

2. Network > Interfaces > Edit（对于 ethernet1/2）：输入以下内容，然后单击 **OK**：

   Zone Name: Null

3. Network > Zones > Edit（对于 Untrust）：在 Virtual Routers Name 下拉列表中，选择 **untrust-vr**，然后单击 **OK**。
4. Network > Zones > New：输入以下内容，然后单击 **OK**：

   Name: Sales

   Virtual Router Name: trust-vr

接口 – 区段和通道

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

   Zone Name: Sales

   IP Address/Netmask: 10.1.1.1/24

6. Network > Interfaces > Edit（对于 ethernet1/2）：输入以下内容，然后单击 **OK**：

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

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

   Interface Name: tunnel.1

   Zone: Untrust-Tun

   Fixed IP:（选择）

   IP Address/Netmask: 10.2.1.1/24

MIP

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

   Mapped IP: 10.2.1.2

   Netmask: 255.255.255.255

   Host IP Address: 10.1.1.2

   Host Virtual Router Name: trust-vr

DIP

9. 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:

   Start: 10.2.1.65

   End: 10.2.1.126

   Port Translation: （选择）

地址

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

    Address Name: sales-any

    IP Address/Domain Name:

    IP/Netmask: （选择）, 10.1.1.0/24

    Zone: Sales

11. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
    Address Name: branch1-any
    IP Address/Domain Name:
    IP/Netmask: 30.1.1.0/255.255.255.192
    Zone: Untrust
12. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
    Address Name: branch1-ftp
    IP Address/Domain Name:
    IP/Netmask: 30.1.1.5/32
    Zone: Untrust

VPN

13. VPNs > AutoKey IKE > New：输入以下内容，然后单击 **OK**：
    VPN Name: to_branch1
    Security Level: Compatible
    Remote Gateway: Create a Simple Gateway: （选择）
    Gateway Name: branch1
    Type：Static IP: （选择）, IP Address: 211.2.2.2
    Preshared Key: netscreen1
    Security Level: Compatible
    Outgoing Interface: ethernet1/2[21]

21. 外向接口不必在同一区段中 （已将通道接口绑定到该区段）。

路由

14. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
    Network Address/Netmask: 0.0.0.0/0
    Next Hop Virtual Router Name: （选择）, untrust-vr
15. Network > Routing > Routing Table > untrust-vr New：输入以下内容，然后单击 **OK**：
    Network Address/Netmask: 30.1.1.0/24
    Gateway: （选择）
    Interface: tunnel.1
    Gateway IP Address: 0.0.0.0
16. Network > Routing > Routing Table > 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: ethernet1/2(untrust-vr)
    Gateway IP Address: 210.1.1.254

注意：*由于 Sales 区段 (ethernet2/1) 的接口是在“路由”模式下， NetScreen 设备将自动在 untrust-vr 路由表中为其制作一个条目。不必手动输入一个条目。*

策略

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

    Source Address:

    Address Book: （选择） , sales-any

    Destination Address：

    Address Book: （选择） , branch1-ftp

    Service: FTP

    Action: Tunnel

    Tunnel VPN: to_branch1

    Modify matching VPN policy: （清除）

    Position at Top: （选择）

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

    NAT:（选择）, DIP On:（选择）; 5 (10.2.1.65–10.2.1.126)/X-late

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

    Source Address:

    Address Book: （选择） , branch1-any

    Destination Address:

    Address Book: （选择） , MIP(10.2.1.2)

    Service: FTP

    Action: Tunnel

    Tunnel VPN: to_branch1

    Modify matching VPN policy: （清除）

    Position at Top: （选择）

CLI

安全和 Tunnel 区段

安全区段和虚拟路由器

1. unset interface ethernet1/2 ip
2. unset interface ethernet1/2 zone
3. set zone untrust vrouter untrust-vr
4. set zone name sales trust-vr

接口 – 区段和通道

5. set interface ethernet2/1 zone sales
6. set interface ethernet2/1 ip 10.1.1.1/24
7. set interface ethernet1/2 zone untrust
8. set interface ethernet1/2 ip 210.1.1.1/24
9. set interface tunnel.1 zone untrust-tun
10. set interface tunnel.1 ip 10.2.1.1/24

MIP

11. set interface tunnel.1 mip 10.2.1.2[22] host 10.1.1.2

DIP

12. set interface tunnel.1 dip 5 10.2.1.65 10.2.1.126

22. 由于缺省网络掩码是 255.255.255.255，就不必在命令中指定。

地址

13. set address sales sales-any 10.1.1.0/24
14. set address untrust branch1-any 30.1.1.0 255.255.255.192
15. set address untrust branch-ftp 30.1.1.5/32

VPN

16. set ike gateway branch1 ip 211.2.2.2 outgoing-interface ethernet1/2 preshare netscreen1 sec-level compatible
17. set vpn to_branch1 gateway branch1 sec-level compatible

路由

18. set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
19. set vrouter untrust-vr route 30.1.1.0 255.255.255.192 interface tunnel.1
20. set vrouter untrust-vr route 0.0.0.0/0 interface ethernet1/2 gateway 210.1.1.254

> ***注意：****由于 Sales 区段 (ethernet2/1) 的接口是在“路由”模式下， NetScreen 设备将自动在 untrust-vr 路由表中为其制作一个条目。不必手动输入一个条目。*

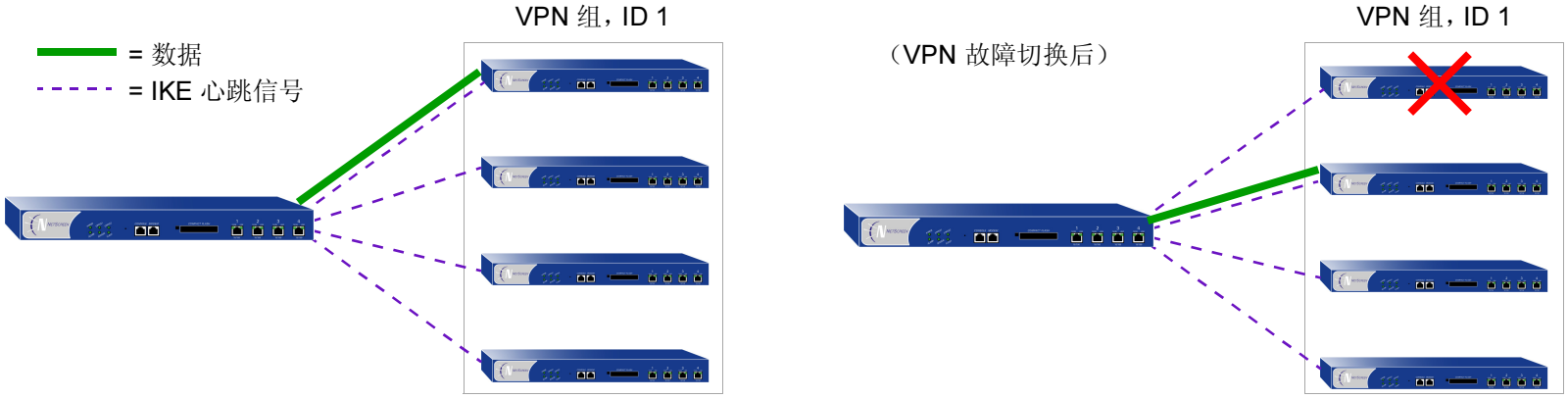
策略

21. set policy top from sales to untrust sales-any branch1-ftp ftp nat dip 5 permit
22. set policy top from untrust to global branch1-any mip(10.2.1.2) ftp permit
23. save

冗余 VPN 网关

NetScreen 冗余网关功能提供在站点到站点故障切换之中和之后 VPN 不间断连接的解决方案。可以创建一个 VPN 组以提供一组冗余网关（最多四个），LAN 到 LAN 或 LAN 到 LAN 动态对等方自动密钥 IKE IPSec[23] VPN 通道可以连接到该冗余网关上。当 NetScreen 设备首次接收到与引用 VPN 组的策略相匹配的流量时，它执行具有该组中所有成员的第 1 阶段和第 2 阶段 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 设备保持第 2 阶段的 SA 并且通过经过这些通道发送 IKE 激活封包使其保持激活状态。如果激活的 VPN 通道失败，此通道可以故障切换到组中具有第二最高优先权的通道和网关。

***注意：**此方案假设连接冗余网关后的站点，以便镜像所有站点主机中的数据。此外，每个站点（专用于高可用性 (HA)）都具有一个在 HA 模式中运行的 NetScreen 设备的冗余集群。因此，VPN 故障切换临界值必须设置高于设备故障切换临界值，否则会发生不必要的 VPN 故障切换。*

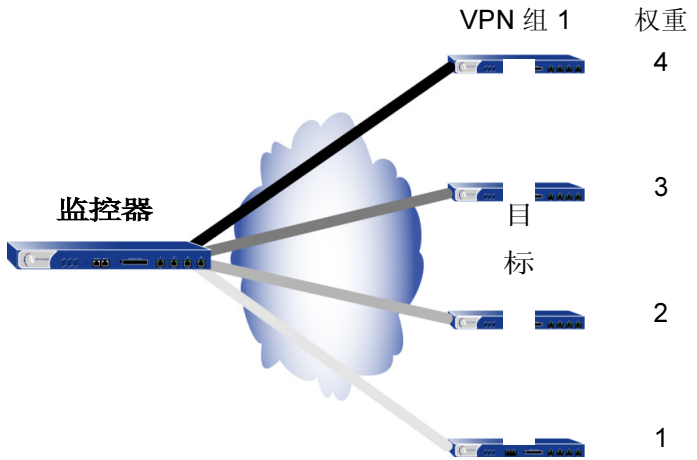


23. VPN 组不支持 L2TP、IPSec 上的 L2TP、拨号端到 LAN 或“手动密钥 VPN”通道类型。在“LAN 到 LAN 动态对等方”配置中，监视 VPN 组的 NetScreen 设备必须是动态指定 Untrust IP 地址，而 VPN 组成员的 Untrust IP 地址必须是静态地址的设备。

VPN 组

VPN 组是最多四个目标远程网关的一组 VPN 通道配置。组中各通道的第 1 阶段和第 2 阶段安全联盟 (SA) 参数可以不同或相同（除了显然必须要不同的远程网关 IP 地址）。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识别其在要作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。

注意：在此图例中，底纹是各通道权重的象征。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，各成员之间也是监控器与目标的关系。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

这两种工具在下一部分介绍第 215 页上的 “监控机制”。

***注意：**监控器到目标关系不需要是单向的。监控设备也可能是 VPN 组的一个成员，也可能是其它监控设备的目标。*

监控机制

NetScreen 使用两种机制监控 VPN 组的成员以确定各成员终止 VPN 流量的能力：

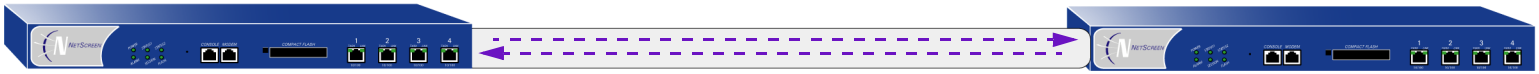
- IKE 心跳信号
- IKE 恢复尝试

使用这两种工具，加上 TCP 应用程序故障切换选项（请参阅第 219 页上的“TCP SYN 标记检查”），NetScreen 设备可以检测何时需要 VPN 故障切换，以及不必中断 VPN 设备而将流量切换到新通道。

IKE 心跳信号

IKE 心跳信号是 IKE 对等方通过 VPN 通道互相发送的 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”）没有接收到来自 device_t（“目标”）指定数量的心跳信号（缺省值是 5），device_m 就认为 device_t 已经中断。Device_m 将从 SA 高速缓存中清除相应的第 1 阶段和第 2 阶段安全联盟 (SA)，并开始 IKE 恢复过程。（请参阅第 216 页上的“IKE 恢复过程”。） Device_t 也清除自己的 SA。

注意：*在 VPN 组中 VPN 通道两端的设备上必须启用 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.（由于对等方没有发送心跳信号，已经禁用了心跳信号。）”*



“IKE 心跳信号”必须通过
VPN 通道双向流动。

要定义指定 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（用于要修改其 IKE 心跳信号临界值的网关）：在“Heartbeat Hello”和 “Heartbeat Threshold”字段中输入新值，然后单击 **OK**。

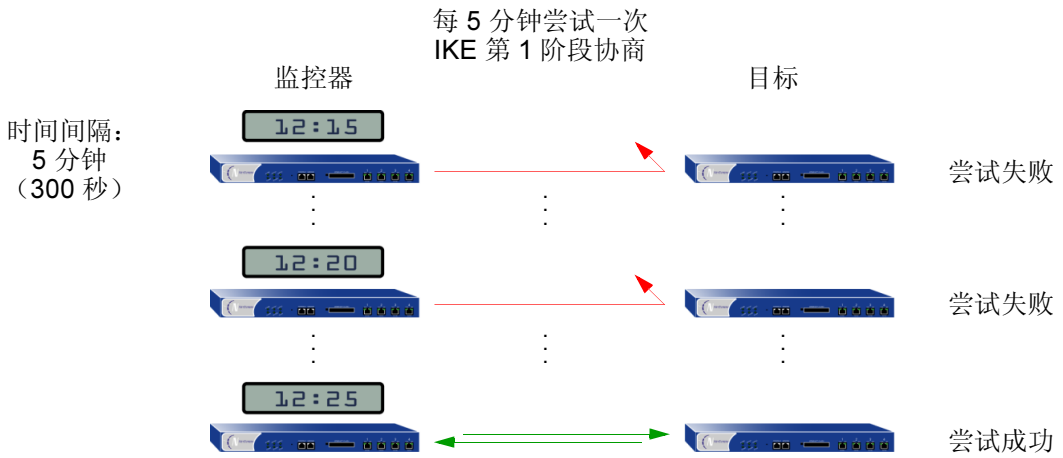
CLI

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。在定义的时间间隔后，监控器会尝试与失败的对等方开始第 1 阶段协商。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第 1 阶段协商，直到协商成功。



要定义指定 VPN 通道的 IKE 恢复时间间隔 （最小设置是 60 秒），请执行以下的任一操作：

WebUI

VPNs > AutoKey Advanced > Gateway > Edit （用于要修改其 IKE 重新连接时间间隔的网关）：在 Heartbeat Reconnect 字段中输入秒值，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，该通道将自动故障切换回第一个成员。加权系统总是使组中最好的网关处理 VPN 数据 （无论何时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

要顺利发生 VPN 故障切换，必须进行 TCP 会话的处理。故障切换后，如果新的活动网关在现有的 TCP 会话中接收到一个封包，新网关将把它作为新 TCP 会话中的第一个封包处理，并检查是否在封包包头中设置了 SYN 标记。由于此封包确实是现有会话的部分，因而它没有设置 SYN 标记。因此，新网关将拒绝此封包。启用 TCP SYN 标记检查时，在发生故障切换后，所有 TCP 应用程序必须重新连接。

要解决此问题，您可以禁用 VPN 通道中 TCP 会话的 SYN 标记检查，如下所述：

WebUI

您不可以通过 WebUI 禁用 SYN 标记检查。

CLI

unset flow tcp-syn-check-in-tunnel

注意：*缺省情况下，启用 SYN 标记检查。*

范例：冗余 VPN 网关

在此例中，公司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被镜像。数据中心是独立的，即使是在发生灾难性故障（例如，整天的电源消耗或自然灾害）时，也可以提供连续的服务。

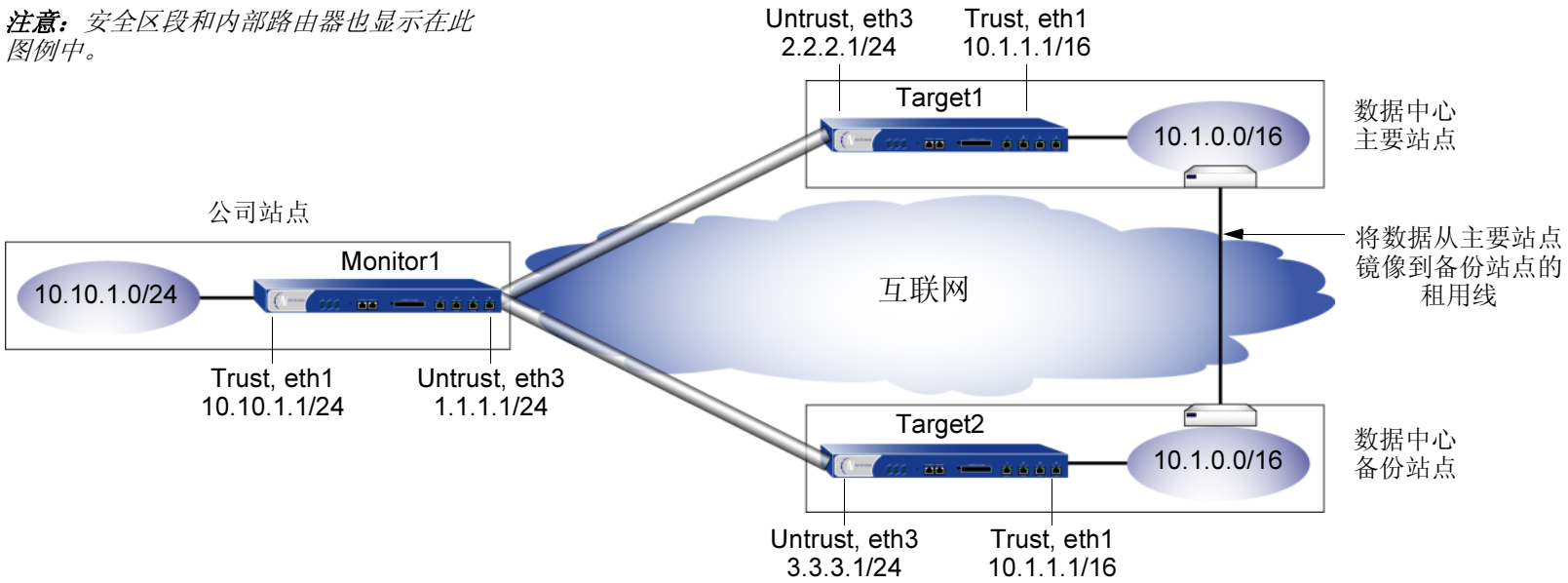
设备的位置和名称、物理接口及其 Trust 和 Untrust 区段的 IP 地址、各个 NetScreen 设备的 VPN 组 ID 和权重，如下所示：

设备位置	设备名称	物理接口和 IP 地址（Trust Zone）	物理接口 IP 地址、缺省网关 (GW)（Untrust Zone）	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（主要的）	Target1	ethernet1, 10.1.1.1/16	ethernet3, 2.2.2.1/24, (GW) 2.2.2.2	ID = 1, Weight = 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, Weight = 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 路由域中。所有“LAN 到 LAN 的自动密钥 IKE VPN”通道都使用预先定义安全级别，对第 1 阶段和第 2 阶段提议都是“Compatible”。预共享密钥认证参与者。

注意：*安全区段和内部路由器也显示在此图例中。*



WebUI (Monitor1)

安全区段接口

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

   Zone Name: Trust

   IP Address/Netmask: 10.10.1.1/24

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

   Zone Name: Untrust

   IP Address/Netmask: 1.1.1.1/24

地址

3. 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: 10.10.1.0/24

   Zone: Trust

4. 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: 10.1.0.0/16

   Zone: Untrust

VPN

5. VPNs > AutoKey Advanced > VPN Group：在“VPN Group ID”字段中输入 1，然后单击 **Add**。
6. 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：输入下列高级设置，然后单击 **Return**，返回到基本 “网关” 配置页：

   Security Level: Compatible

   Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 Seconds

Threshold: 5

7. 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 “自动密钥 IKE” 配置页：

VPN Group: VPN Group -1

Weight: 2

8. 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：输入下列高级设置，然后单击 **Return**，返回到基本 “网关” 配置页：

Security Level: Compatible

Mode (Initiator): Main (ID Protection)

Heartbeat:

Hello: 3 Seconds

Reconnect: 60 Seconds

Threshold: 5

9. 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 “自动密钥 IKE” 配置页：

VPN Group: VPN Group -1

Weight: 1

路由

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

Network Address/Netmask: 0.0.0.0/0

Gateway: （选择）

Interface: ethernet3

Gateway IP Address: 1.1.1.2(untrust)

策略

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

Source Address:

Address Book: in_trust

Destination Address:

Address Book: data_ctr

Service: ANY

Action: Tunnel

VPN: VPN Group-1

Modify matching VPN policy: （选择）

Position at Top: （选择）

WebUI (Target1)

安全区段接口

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：
   Zone Name: Trust
   IP Address/Netmask: 10.1.1.1/16
2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：
   Zone Name: Untrust
   IP Address/Netmask: 2.2.2.1/24

地址

3. 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: 10.1.0.0/16
   Zone: Trust
4. Objects > Addresses > List > New：输入以下内容，然后单击 **OK**：
   Address Name: corp
   IP Address/Domain Name:
   IP/Netmask: 10.10.1.0/24
   Zone: Untrust

VPN

5. 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: 1.1.1.1

   Preshared Key: SLi1yoo129

   Outgoing Interface: ethernet3

   > Advanced：输入下列高级设置，然后单击 **Return**，返回到基本“网关”配置页：

   Security Level: Compatible

   Mode (Initiator): Main (ID Protection)

   Heartbeat:

   Hello: 3 Seconds

   Reconnect: 0 Seconds

6. 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

路由

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

   Network Address/Netmask: 0.0.0.0/0

   Gateway: （选择）

   Interface: ethernet3

   Gateway IP Address: 2.2.2.2(untrust)

策略

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

   Source Address:

   Address Book: （选择） , in_trust

   Destination Address:

   Address Book: （选择） , corp

   Service: ANY

   Action: Tunnel

   Tunnel VPN: monitor1

   Modify matching VPN policy: （选择）

   Position at Top: （选择）

WebUI (Target2)

注意：*按照 Target1 配置步骤配置 Target2，但是需将 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)

安全区段接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.10.1.1/24
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 1.1.1.1/24

地址

5. set address trust in_trust 10.10.1.0/24
6. set address untrust data_ctr 10.1.0.0/16

VPN

7. set ike gateway target1 ip 2.2.2.1 main outgoing-interface ethernet3 preshare SLi1yoo129 sec-level compatible
8. set ike gateway target1 heartbeat hello 3
9. set ike gateway target1 heartbeat reconnect 60
10. set ike gateway target1 heartbeat threshold 5
11. set vpn to_target1 gateway target1 sec-level compatible
12. set ike gateway target2 ip 3.3.3.1 main outgoing-interface ethernet3 preshare CMFwb7oN23 sec-level compatible
13. set ike gateway target2 heartbeat hello 3
14. set ike gateway target2 heartbeat reconnect 60
15. set ike gateway target2 heartbeat threshold 5
16. set vpn to_target2 gateway target2 sec-level compatible
17. set vpn-group id 1 vpn to_target1 weight 2
18. set vpn-group id 1 vpn to_target2 weight 1
19. unset flow tcp-syn-check-in-tunnel

路由

20. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.2

策略

21. set policy top from trust to untrust in_trust data_ctr any tunnel “vpn-group 1”
22. set policy top from untrust to trust data_ctr in_trust any tunnel “vpn-group 1”
23. save

CLI (Target1)

安全区段接口

1. set interface ethernet1 zone trust
2. set interface ethernet1 ip 10.1.1.1/16
3. set interface ethernet3 zone untrust
4. set interface ethernet3 ip 2.2.2.1/24

地址

5. set address trust in_trust 10.1.0.0/16
6. set address untrust corp 10.10.1.0/24

VPN

7. set ike gateway monitor1 ip 1.1.1.1 main outgoing-interface ethernet3 preshare SLi1yoo129 sec-level compatible
8. set ike gateway monitor1 heartbeat hello 3
9. set ike gateway monitor1 heartbeat threshold 5
10. set vpn to_monitor1 gateway monitor1 sec-level compatible

路由

11. set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 2.2.2.2

策略

12. set policy top from trust to untrust in_trust corp any tunnel vpn to_monitor
13. set policy top from untrust to trust corp in_trust any tunnel vpn to_monitor
14. save

CLI (Target2)

> ***注意：****按照 Target1 配置步骤配置 Target2，但是须将 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。*

5

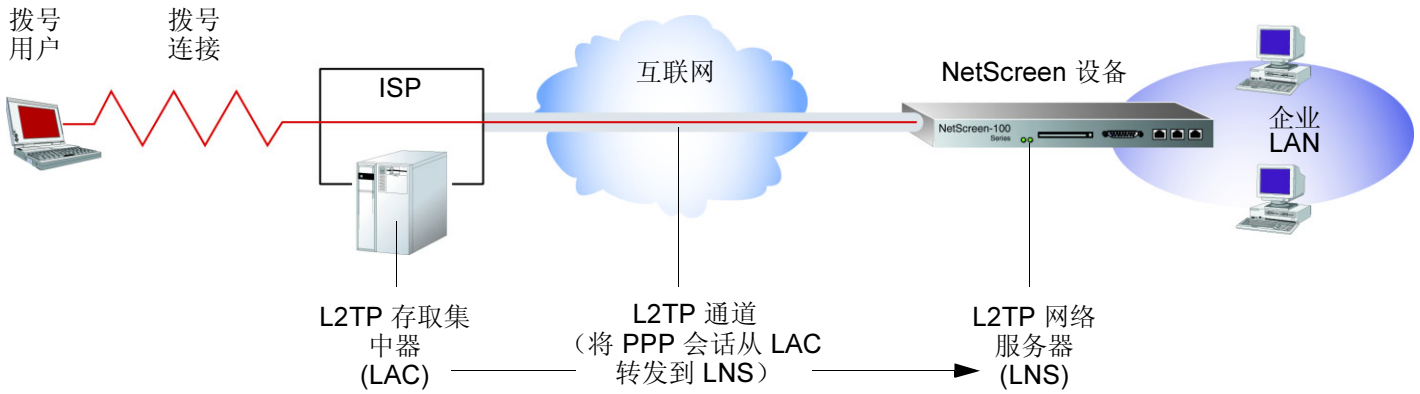
L2TP （Layer 2 Tunneling Protocol，第 2 层通道协议）

本章介绍了 “Layer 2 （第 2 层）通道协议 (L2TP)”，说明了它的单独使用和带有 IPSec （Internet Protocol Security，互联网协议安全性）支持的使用，还有 L2TP 和 IPSec 上的 L2TP 一些配置范例：

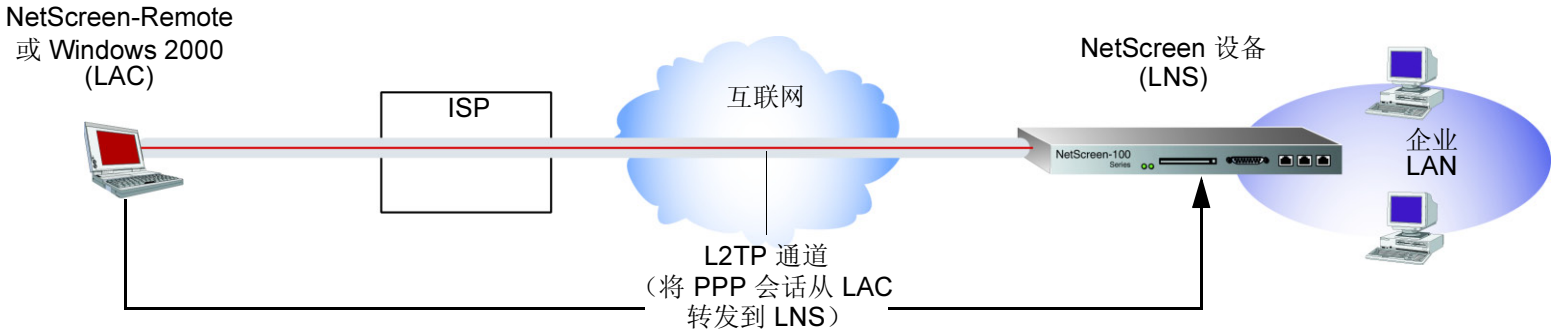
L2TP 简介

“Layer 2 （第 2 层）通道协议 (L2TP)”让拨号用户可以通过虚拟 “点对点协议 (PPP)”连接到 “L2TP 网络服务器 (LNS)”，而该服务器可以是一台 NetScreen 设备。 L2TP 通过 “L2TP 存取集中器 (LAC)”和 LNS 之间的一个通道发送 PPP 帧。

最初设计 L2TP 的目的，是在位于一个 ISP 网站上的 LAC 与另一 ISP 网站或企业网站上的 LNS 之间建立通道连接。L2TP 通道没有完全扩展到拨号用户的计算机上，而只是扩展到拨号上网用户本地 ISP 的 LAC 上。（这有时被称为强制的 L2TP 配置。）

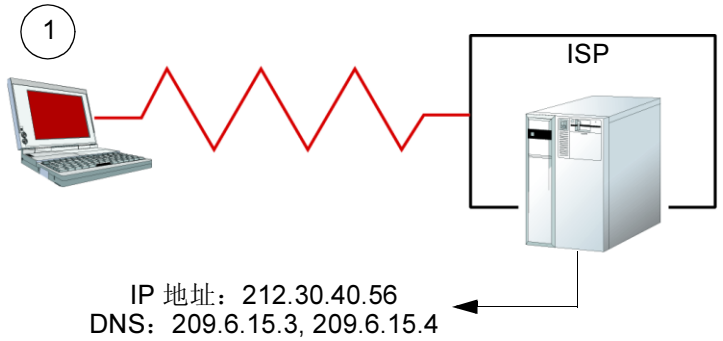


使用 Windows 2000 或 Windows NT 的 NetScreen-Remote 客户机，或 Windows 2000 客户机本身都能够充当 LAC，因此 L2TP 通道可以直接扩展到拨号用户的计算机上，从而提供端对端通道。（这种方法有时被称为自愿的 L2TP 配置。）

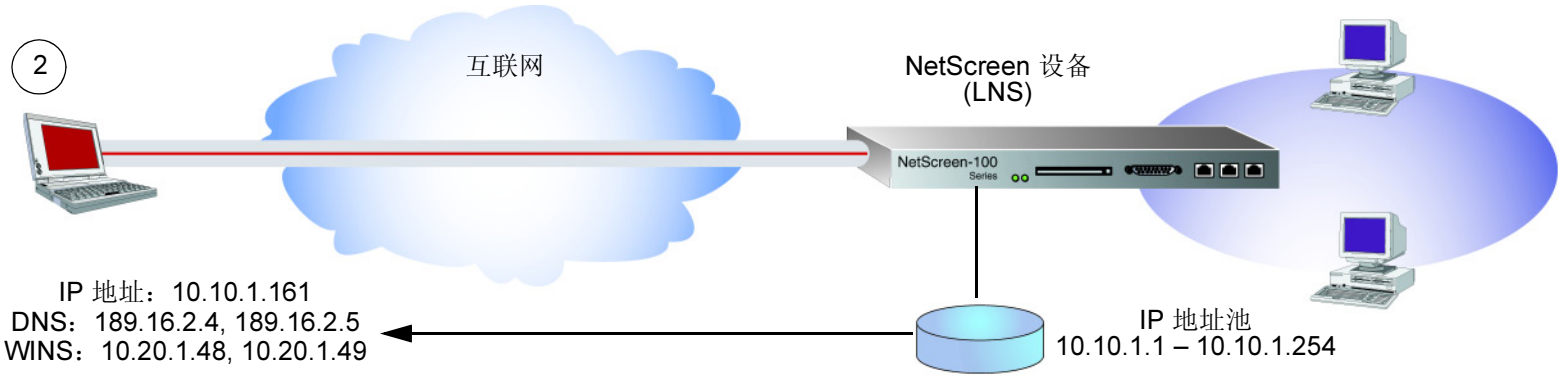


因为 PPP 链接通过互联网从拨号用户扩展到 NetScreen 设备 (LNS)，所以是由 NetScreen 设备而不是由 ISP 来分配客户机的 IP 地址、DNS 和 WINS 服务器地址，以及从本地数据库或外部认证服务器（RADIUS、SecurID 或 LDAP）认证用户。

拨号用户收到两个 IP 地址，一个用于它和 ISP 的物理连接，另一个是来自 LNS 的逻辑连接。当拨号用户（也许使用 PPP）与自己的 ISP 联系时，该 ISP 进行 IP 和 DNS 指派，并对用户进行认证。这样允许用户以可路由的 IP 地址连接到互联网，该 IP 地址成为 L2TP 通道的外部 IP 地址。



然后，当 L2TP 通道向 NetScreen 设备转发封装 PPP 帧时，该 NetScreen 设备为用户分配 IP 地址以及 DNS 和 WINS 设置。该 IP 地址可以是私有的不可路由地址，它成为 L2TP 通道的内部地址。



当前版本的 ScreenOS 提供以下 L2TP 支持：

- 来自运行 Windows 2000 的主机的 L2TP 通道[1]
- 传送模式中 （IPSec 上的 L2TP） L2TP 和 IPSec 的组合
  - 对于 NetScreen-Remote：IPSec 上的 L2TP 在 “Main” 模式协商时使用认证，在 “Aggressive” 模式时使用预共享密钥，或使用认证
  - 对于 Windows 2000：IPSec 上的 L2TP 在 “Main” 模式协商时使用认证
- 用户认证分别使用来自本地数据库或外部认证服务器 （RADIUS、 SecurID 或 LDAP） 的 “密码认证协议 (PAP)” 或 “质询握手认证协议 (CHAP)”

  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。*

- 来自本地数据库或 RADIUS 服务器的拨号用户 IP 地址、“域名系统 (DNS)” 服务器，和 “Windows 互联网命名服务 (WINS)” 服务器的分配
- 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 Layer 3 （第 3 层） 操作，并且安全区段接口处于 NAT 或 “路由” 模式。当 NetScreen 设备在 Layer 2 （第 2 层） 操作时，安全区段接口处于 “透明” 模式，在 WebUI 中不会出现与 L2TP 相关的资料，并且与 L2TP 相关的 CLI 命令会引发错误消息。*

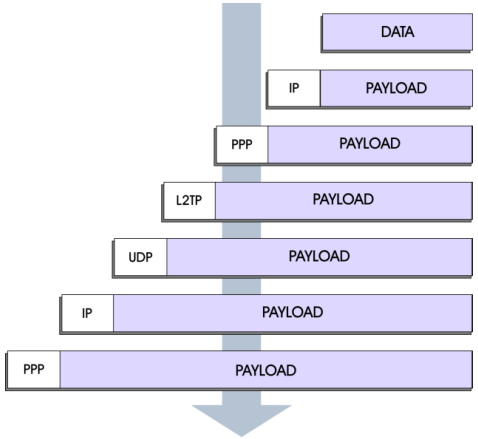
1. 缺省情况下，Windows 2000 执行 IPSec 上的 L2TP。要强制它仅使用 L2TP，必须在注册表中找到 ProhibitIPSec 密钥并将 **0**（IPSec 上的 L2TP）更改为 **1**（仅 L2TP）。（在执行此操作前，NetScreen 建议对注册表进行备份。）单击 **开始 > 运行**：键入 **regedit**。双击 **HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services > RasMan > Parameters**。双击 **ProhibitIPSec**：在 “数值” 数据字段键入 **1**，选择 **十六进制**作为基值，然后单击 **OK**。重新启动计算机。（如果在注册表中没有类似条目，请参阅 Microsoft Windows 文档以获得如何创建它的信息。）

封包的封装和解封

L2TP 使用封装封包的方法从 LAC 向 LNS 传送 PPP 帧。在查看 L2TP 和 IPSec 上的 L2TP 设置的具体范例前，首先介绍一下 L2TP 过程中涉及的封装和解封的概述。

封装

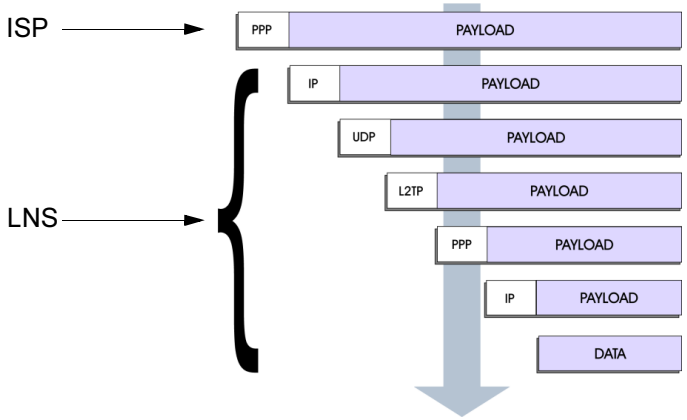
当一个 IP 网络上的拨号用户通过 L2TP 通道发送数据时，LAC 将 IP 封包封装在一系列第 2 层帧、第 3 层封包和第 4 层段中。假设该拨号用户通过 PPP 链接连接到本地 ISP，则封装过程如下：



1. 数据放置于 IP 负荷中。
2. 该 IP 封包封装在 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 片段封装在 IP 封包中。
6. 该 IP 封包封装在 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 封包。
2. ISP 移除 PPP 包头并将 IP 封包转发给 LNS。
3. LNS 移除该 IP 包头。
   在 IP 负荷中是一个指定端口 1707 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 封包。
7. LNS 将该 IP 封包路由到其最终的目的地，在那里移除 IP 包头并提取出 IP 封包中的数据。

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。这种选择在 IP 地址池中循环进行；即，在从 1.1.1.1 到 1.1.1.3 的地址池中，该地址的选择按下面的循环方式进行：1.1.1.1 – 1.1.1.2 – 1.1.1.3 – 1.1.1.1 – 1.1.1.2 ...)
- 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认证服务器 （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，或者是其它的服务器。*

另外，可以为 PPP 认证指定下列方案之一：

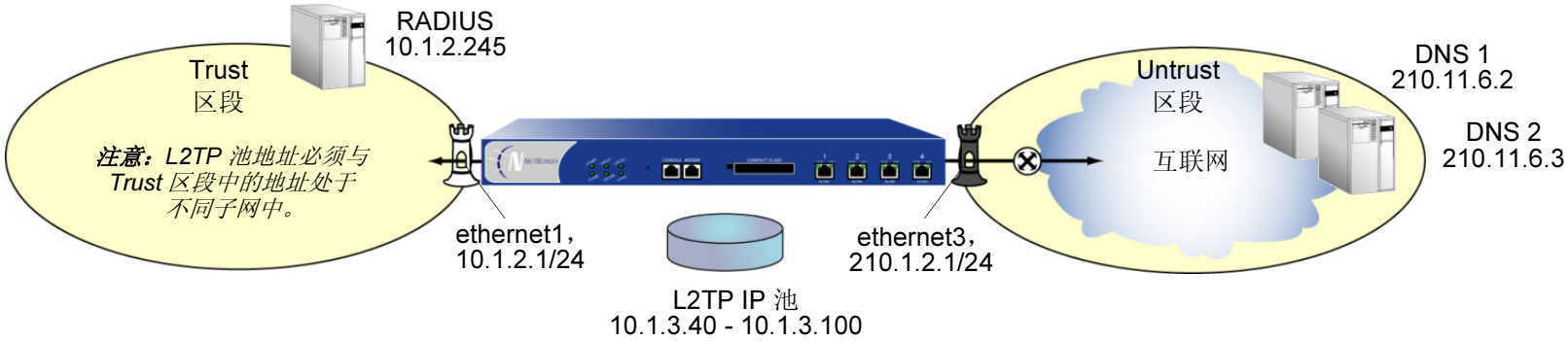
- “Challenge Handshake Authentication Protocol（质询握手认证协议 ） (CHAP)”，在拨号用户发出 PPP 链接请求后， NetScreen 设备向用户发送质询 （加密密钥），然后用户使用该密钥加密自己的登录名称和密码。本地数据库和 RADIUS 服务器支持 CHAP。
- “Password Authentication Protocol （密码认证协议）(PAP)”，它与 PPP 链接请求一起，以明文方式发送拨号用户的密码。本地数据库和 RADIUS、 SecurID 和 LDAP 服务器均支持 PAP。
- “ANY （任何）”，意思是 NetScreen 设备用 CHAP 协商，如果它出现故障，则使用 PAP。

您可以在“L2TP 缺省配置”页 (VPNs > L2TP > Default Settings) 进行配置或用 **set l2tp default** 命令来将缺省 L2TP 参数应用于拨号用户和拨号用户组。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，使用介于 10.1.3.40 到 10.1.3.100 之间的地址范围定义 IP 地址池。指定 DNS 服务器 IP 地址为 210.11.6.2 （一级）和 210.11.6.3 （二级）。 NetScreen 设备使用 CHAP 执行 PPP 认证。

注意： *以每个 L2TP 通道为基础指定认证服务器。*



WebUI

1. 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. 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: 210.11.6.2
   DNS Secondary Server IP: 210.11.40.3
   WINS Primary Server IP: 0.0.0.0
   WINS Secondary Server IP: 0.0.0.0

CLI

1. set ippool sutro 10.1.3.40 10.1.3.100
2. set l2tp default ippool sutro
3. set l2tp default ppp-auth chap
4. set l2tp default dns1 210.11.6.2
5. set l2tp default dns2 210.11.40.3
6. 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 的目的只是允许本地 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 要求用同样的端点设置一个 L2TP 通道和 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详细信息，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 237 页上的脚注。）

可以在 NetScreen 设备和下列任意一个 VPN 客户机之间创建一个 IPSec 上的 L2TP 通道：

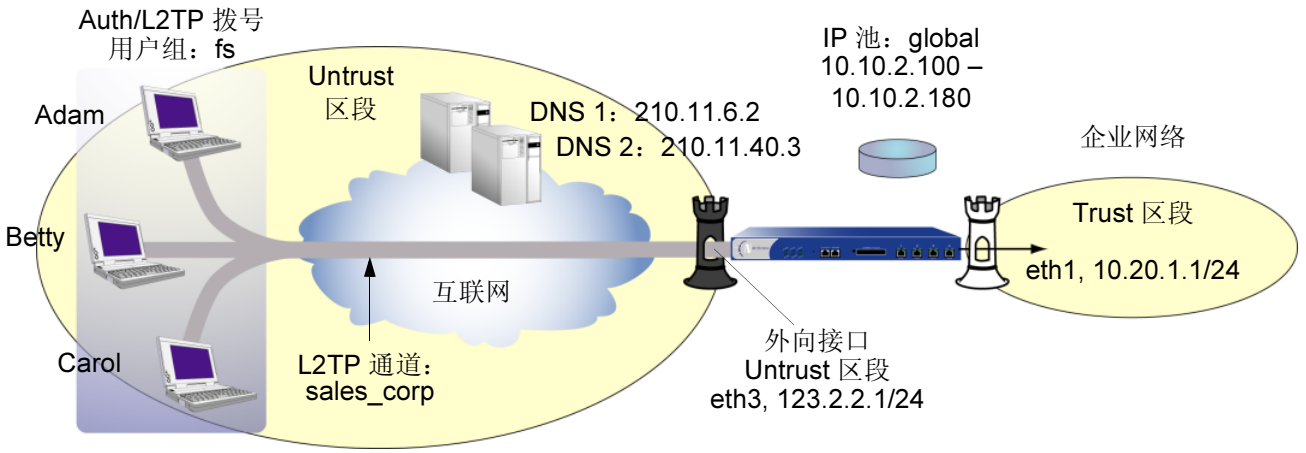
- 在 Windows 2000 或 Windows NT 操作系统上运行 NetScreen-Remote 的主机
- 运行 Windows 2000 （没有 NetScreen-Remote）的主机

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 通道的外向接口。NetScreen 设备将下列缺省 L2TP 通道设置应用于拨号用户组：

- L2TP 用户通过本地数据库认证。
- 使用 CHAP 进行 PPP 认证。
- IP 池 （命名为 “global”）中的地址范围从 10.10.2.100 到 10.10.2.180[2]。
- DNS 服务器为 210.11.6.2 （一级）和 210.11.40.3 （二级）。

***注意：** 一个只有 L2TP 的配置并不安全。仅推荐将它用于调试目的。*



远程 L2TP 客户机使用 Windows 2000 操作系统。有关如何在远程客户机上配置 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。

2. 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

L2TP 用户

1. 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
2. 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
3. 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

L2TP 用户组

4. 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**，然后使用 **<<** 按钮将它从 “Available members”列中移动到 “Group members”列中。

   选择 **Betty**，然后使用 **<<** 按钮将它从 “Available members”列中移动到 “Group members”列中。

   选择 **Carol**，然后使用 **<<** 按钮将它从 “Available members”列中移动到 “Group members”列中。

缺省 L2TP 设置

5. 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. 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: 210.11.6.2

   DNS Secondary Server IP: 210.11.40.3

   WINS Primary Server IP: 0.0.0.0

   WINS Secondary Server IP: 0.0.0.0

L2TP 通道

7. VPNs > L2TP > Tunnel > New：输入以下内容，然后单击 **OK**：

Name: sales_corp
Dialup Group: Local Dialup Group - fs
Authentication Server: Local
Outgoing Interface: ethernet3
Peer IP: 0.0.0.0[3]
Host Name (optional): 输入充当 LAC[4] 的计算机名称。
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，必须按如下说明修改 Windows 2000 注册表：

*(1) 单击**开始 > 运行**，然后键入 **regedit**。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 通道配置机密”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），不需要通道认证；所有 L2TP 消息在 IPSec 内部加密和认证。

Keep Alive: 60[5]

3. 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**。
4. 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**下的条目。
5. “Keep Alive （激活）”值是在 NetScreen 设备向 LAC 发送 L2TP hello 信号前静止的秒数。

策略

8. Policies > (From: Untrust, To: Trust) New：输入以下内容，然后单击 **OK**：
   Source Address:
   Address Book: Dial-Up VPN
   Destination Address：
   Address Book: Any
   NAT: Off
   Service: ANY
   Action: Tunnel
   Tunnel L2TP: sales_corp
   Position at Top: （选择）

CLI

拨号用户

1. set user adam type l2tp
2. set user adam password AJbioJ15
3. unset user adam type auth[6]
4. set user betty type l2tp
5. set user betty password BviPsoJ1
6. unset user betty type auth
7. set user carol type l2tp
8. set user carol password Cs10kdD3
9. unset user carol type auth

6. 为一个用户定义密码会自动将该用户分类为认证用户。所以，要严格的将用户类型定义为 L2TP，就必须撤消该认证用户类型。

L2TP 用户组

10. set user-group fs location local
11. set user-group fs user adam
12. set user-group fs user betty
13. set user-group fs user carol

缺省 L2TP 设置

14. set ippool global 10.10.2.100 10.10.2.180
15. set l2tp default ippool global
16. set l2tp default auth server Local
17. set l2tp default ppp-auth chap
18. set l2tp default dns1 210.11.6.2
19. set l2tp default dns2 210.11.40.3

L2TP 通道

20. set l2tp sales_corp outgoing-interface ethernet3
21. set l2tp sales_corp auth server Local user-group fs

策略

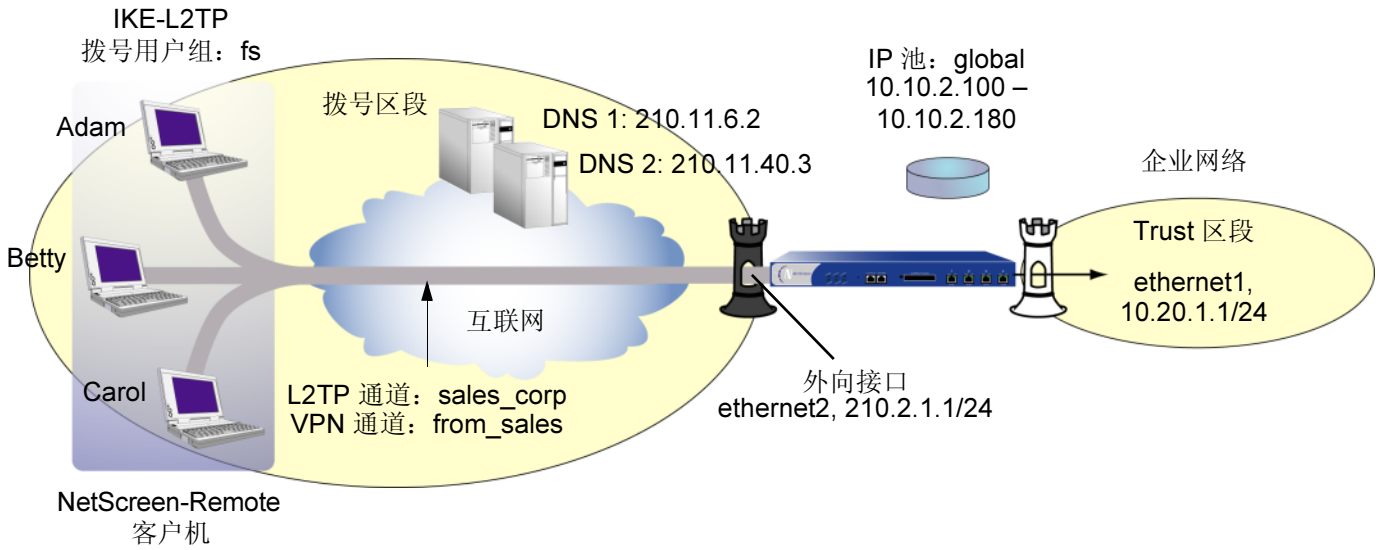
22. set policy top from untrust to trust “Dial-Up VPN” any any tunnel l2tp sales_corp
23. save

范例：配置 IPSec 上的 L2TP

本范例使用的 L2TP 通道与上例中（第 244 页上的 “范例：配置 L2TP”）创建的相同。另外，将一个 IPSec 通道覆盖到 L2TP 通道上以提供加密。IPSec 通道在 Aggressive mode（主动模式）中协商 第 1 阶段，使用之前已经加载的 RSA 证书、 3DES 加密和 SHA-1 认证。授权机构 (CA) 是 Verisign。（有关获得和加载证书的信息，请参阅第 2 章，第 23 页上的 “公开密钥密码术”。）第 2 阶段协商使用将第 2 阶段协议预定为 “Compatible” 的安全级别。 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 路由域中。用于 “拨号” 和 Trust 区段的接口分别为 ethernet2 (210.2.1.1/24) 和 ethernet1 (10.20.1.1/24)。 Trust 区段处于 NAT 模式。

拨号用户 Adam、Betty 和 Carol 使用运行 Windows 2000 操作系统[7] 的 NetScreen-Remote 客户机。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。）



7. 对于 （没有 NetScreen-Remote 的） Windows 2000，要配置 IPSec 上的 L2TP 通道，第 1 阶段协商必须处于 Main mode （主模式）而且 IKE ID 类型必须为 ASN1-DN。

WebUI

用户定义的区段

1. 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）

   Share Zone: （清除）

   Block Intra-Zone Traffic: （选择）

   注意：*Trust 区段被预先配置。不需要创建它。*

接口

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

   Zone Name: Trust

   IP Address/Netmask: 10.20.1.1/24

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

   Zone Name: Dialup

   IP Address/Netmask: 210.2.1.1/24

IKE/L2TP 用户

4. 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）[8]

   IKE Identity: ajackson@abc.com

   L2TP User: （选择）

   User Password: AJbioJ15

   Confirm Password: AJbioJ15

5. 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

8. 输入的 IKE ID 必须与 NetScreen-Remote 客户机发送的相同，它是客户机用于认证的证书中显示的电子邮件地址。

6. 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

IKE/L2TP 用户组

7. 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**，然后用 **<<** 按钮将它从“Available members”列中移动到“Group members”列中。

   选择 **Betty**，然后用 **<<** 按钮将它从“Available members”列中移动到“Group members”列中。

   选择 **Carol**，然后用 **<<** 按钮将它从“Available members”列中移动到“Group members”列中。

缺省 L2TP 设置

8. 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

9. 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: 210.11.6.2

   DNS Secondary Server IP: 210.11.40.3

   WINS Primary Server IP: 0.0.0.0

   WINS Secondary Server IP: 0.0.0.0

10. 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[9]

    Host Name (optional)：如果要将 L2TP 通道限制到一台具体主机，请输入充当 LAC[10] 的计算机名称。

    Secret (optional)：输入一个在 LAC 和 LNS[11] 之间共享的机密

    注意：*通常可以忽略主机名称和机密设置。仅建议高级用户使用这些设置。*

    Keep Alive: 60[12]

9. 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**。
10. 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**下的条目。
11. 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。
12. “Keep Alive （激活）”值是在 NetScreen 设备向 LAC 发送 L2TP hello 信号前静止的秒数。

VPN 通道

11. 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“网关”配置页：

    Security Level: User Defined: Custom

    Phase 1 Proposal: rsa-g2-3des-sha

    Mode (Initiator): Aggressive[13]

    Preferred Certificate (Optional):

    Peer CA: Verisign

    Peer Type: X509-SIG

12. 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“自动密钥 IKE”配置页：

    Security Level: Compatible

    Transport Mode: （选择）

13. Windows 2000 （没有 NetScreen-Remote）仅支持 Main mode （主模式）协商。

策略

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

Source Address:

Address Book: （选择） , Dial-Up VPN

Destination Address:

Address Book: （选择） , Any

Service: ANY

Action:Tunnel

Tunnel VPN: from_sales

Modify matching VPN policy: （清除）

L2TP: sales_corp

Position at Top: （选择）

CLI

用户定义的区段

1. set zone name dialup
2. set zone dialup vrouter trust-vr
3. set zone dialup block

接口

4. set interface ethernet1 zone trust
5. set interface ethernet1 ip 10.20.1.1/24
6. set interface ethernet2 zone dialup
7. set interface ethernet2 ip 210.2.1.1/24

L2TP/IKE 用户

1. set user adam type ike l2tp
2. set user adam password AJbioJ15
3. unset user adam type auth
4. set user adam ike-id u-fqdn ajackson@abc.com
5. set user betty type ike l2tp
6. set user betty password BviPsoJ1
7. unset user betty type auth
8. set user betty ike-id u-fqdn bdavis@abc.com
9. set user carol type ike l2tp
10. set user carol password Cs10kdD3
11. unset user carol type auth
12. set user carol ike-id u-fqdn cburnet@abc.com

IKE/L2TP 用户组

13. set user-group fs location Local
14. set user-group fs user adam
15. set user-group fs user betty
16. set user-group fs user carol

缺省 L2TP 设置

17. set ippool global 10.10.2.100 10.10.2.180
18. set l2tp default ippool global
19. set l2tp default ppp-auth chap
20. set l2tp default dns1 210.11.6.2
21. set l2tp default dns2 210.11.40.3

L2TP 通道

22. set l2tp sales_corp user fs aggressive outgoing-interface ethernet2
23. set l2tp sales_corp auth server Local user-group fs

VPN 通道

24. set ike gateway field dialup fs aggressive outgoing-interface ethernet2 proposal rsa-g2-3des-sha
25. set ike gateway field cert peer-ca1[14]
26. set ike gateway field cert peer-cert-type x509-sig
27. set vpn from_sales gateway field transport sec-level compatible

创建策略

28. set policy top from dialup to trust “Dial-Up VPN” any any tunnel vpn from_sales l2tp sales_corp
29. save

14. 数字 1 是 CA ID 号。要发现 CA 的 ID 号，请使用以下命令：**get pki x509 list ca-cert**。

NetScreen-Remote Security Policy 编辑器 (Adam[15])

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: 210.2.1.1

   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，选择包含在 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[16]

   Port: L2TP
6. 单击 **Security Policy** 图标，然后选择 **Aggressive Mode**。
7. 单击位于“Security Policy”图标左边的加号“**+**”，然后单击位于“Authentication”(Phase 1) 和“Key Exchange”(Phase 2) 左边的加号“**+**”，进一步展开策略。

15. 要为 Betty 和 Carol 的 NetScreen-Remote 客户机配置 IPSec 上的 L2TP 通道，其过程与下面为 Adam 提供的程序相同。
16. 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“加密”和“数据完整性算法”：
   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: 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 **Save**。
14. 同样需要使用“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，必须输入一个目的主机名或 IP 地址。请输入 210.2.1.1。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。*

索引

T

U

V

W

X

Y

Z