FortiGate VPN 指南

FortiGate 用户手册 第二卷

版本 2.50 MR2
2003 年 8 月 8 日

FortiGate VPN 指南
版本 2.50 MR2
2003 年 8 月 8 日

注册商标
本手册中提及的产品由他们各自的所有者拥有其商标或注册商标。

服从规范
FCC Class A Part 15 CSA/CUS

请访问 http://www.fortinet.com 以获取技术支持。

请将在本文档或任何 Fortinet 技术文档中发现的错误信息或疏漏之处发送到 techdoc@fortinet.com。

目录

简介

虚拟专用网络 （VPN）是一个拓展的私有网络，它由穿过共享或公共网络 （例如互联网）的连接组成。例如，某公司有两个办公室分别在两个不同的城市，每个都有它自己的专用网络。这两个办公室可以通过 VPN 在彼此之间创建一个安全的通道。类似地，一个电话拨号用户可以使用他的 VPN 客户端获得对他的专用办公网络的远程访问权。在这两种情况下，在用户看来安全连接如同一个专用的网络通讯，即使这个通讯是通过一个公共网络来传输的。

安全的 VPN 连接是由通道、数据加密和认证结合起来实现的。通道封装数据，以使得它可以通过公共网络传播。数据帧并不是以它原始的格式发送的，而是用一个附加的头部进行封装并在通道的两个端点之间路由。在到达目的端点之后，数据被解封并转发到它在专用网络中的目的地址。

加密将数据流从明文 （一些人类或程序能看懂的东西）转换成密文 （看不懂的东西）。这些信息根据被称为密钥的一组大量的、唯一的数字使用数学算法加密和解密。密钥有两种类型：对称密钥和非对称密钥。对称密钥标准使用相同的密钥进行加密和解密。非对称密钥使用不同的两个密钥，称做密钥对。这个密钥对中的一个，公共密钥，是公开发布的。而另一个，私有密钥，是保密的。要将一个消息加密发送给一个接收者，就需要使用这个接收者的公开密钥将这个消息加密。而接收者是唯一一个拥有私有密钥，能将这个消息解密的人。

认证能够校验数据包的来源和它内容的完整性。认证使用带有密钥的 hash 功能算法，它的工作方式类似于启用加密的校验和计算。

Fortinet VPN

Fortinet 支持许多 VPN 标准，包括互联网协议安全 （IPSec），点对点通道协议 （PPTP），和第二层通道协议 （L2TP）。

IPSec 是 IP 协议家族的一组扩展。它结合了大量的技术来提供密码安全服务，包括加密密钥管理方法和不同级别的 VPN 对等认证，从而实现一套完整的安全服务。

PPTP 和 L2TP 允许远程客户端创建一个到位于一个网关后边的私有网络的 VPN。大多数 Microsoft 操作系统提供了 PPTP 协议。L2TP 协议是从 PPTP 协议演化而来的，较新版本的 Microsoft 操作系统都提供了这个协议。

关于本文档

此文档包括了如下信息：

- *IPSec VPN 提供了关于如何创建使用互联网协议安全（IPSec）标准的 VPN 通道。*
- *预置密钥 IPSec VPN 叙述了如何配置使用自动 IKE 预置密钥认证的 IPSec VPN 通道。*
- *使用认证的 IPSec VPNs 叙述了如何配置使用数字证书认证的 IPSec VPN 通道。*
- *手工密钥的 IPSec VPN 叙述了如何配置使用手工密钥认证的 IPSec VPN 通道。*
- *IPSec VPN 集中器叙述了如何配置一个星型配置的 IPSec VPN。*
- *IPSec VPN 冗余叙述了如何配置 VPN 对等端点之间的多重冗余连接。*
- *PPTP 和 L2TP VPNs 叙述了如何配置使用点对点通道协议和第二层通道协议的 VPN。*
- *VPN 监视和故障排除提供了许多关于如何维护和监控 VPN 的一般操作方法。*

文档约定

本指南使用以下约定来描述 CLI 命令的语法。

- 尖括号 <> 所围的内容为可替换的关键词

  例如：

  要执行 `restore config <文件名_字符串>`

  您应当输入 `restore config myfile.bak`

  `<xxx_字符串>` 表示一个 ASCII 字符串关键词。

  `<xxx_整数>` 表示一个整数关键词。

  `<xxx_ip>` 表示一个 IP 地址关键词。
- 竖线和波形括号 {|} 表示从波形括号中的内容中任选其一。

  例如：

  ```
  set system opmode {nat | transparent}
  ```

  您可以输入 `set system opmode nat` 或 `set system opmode transparent`
- 方括号 [ ] 表示这个关键词是可选的

  例如：

  ```
  get firewall ipmacbinding [dhcpipmac]
  ```

  您可以输入 `get firewall ipmacbinding` 或 `get firewall ipmacbinding dhcpipmac`
- 空格用于分隔可以任意组合输入且必须用空格分隔的选项

  例如：

  ```
  set system interface internal config allowaccess
    {ping https ssh snmp http telnet}
  ```

  您可以输入以下任意一种：

  ```
  set system interface internal config allowaccess ping
  ```

  ```
  set system interface internal config allowaccess ping https
    ssh
  ```

```
set system interface internal config allowaccess https ping
  ssh
set system interface internal config allowaccess snmp
```

Fortinet 文档

从 FortiGate 用户手册的以下各卷中可以找到关于 FortiGate 产品的对应信息：

- *第一卷：FortiGate 安装和配置指南*

  描述了 FortiGate 设备的安装和基本配置方法。还描述了如何使用 FortiGate 的防火墙策略去控制通过 FortiGate 设备的网络通讯，以及如何使用防火墙策略在通过 FortiGate 设备的网络通讯中对 HTTP、FTP 和电子邮件等内容应用防病毒保护、网页内容过滤和电子邮件过滤。

- *第二卷：FortiGate 虚拟专用网络（VPN）指南*

  包含了在 FortiGate IPSec VPN 中使用认证、预置密钥和手工密钥加密的更加详细的信息。还包括了 Fortinet 远程 VPN 客户端配置的基本信息，FortiGate PPTP 和 L2TP VPN 配置的详细信息，以及 VPN 配置的例子。

- *第三卷：FortiGate 内容保护指南*

  描述了如何配置防病毒保护，网页内容过滤和电子邮件过滤，以保护通过 FortiGate 的内容。

- *第四卷：FortiGate NIDS 指南*

  描述了如何配置 FortiGate NIDS，以检测来自网络的攻击，并保护 FortiGate 不受其威胁。

- *第五卷：FortiGate 日志和消息参考指南*

  描述了如何配置 FortiGate 的日志和报警邮件。还包括了 FortiGate 日志消息的说明。

- *第六卷：FortiGate CLI 参考指南*

  描述了 FortiGate CLI，并且还包含了一个 FortiGate CLI 命令的说明。

FortiGate 在线帮助也包含了使用 FortiGate 基于 Web 的管理程序配置和管理您的 FortiGate 设备的操作步骤说明。

Fortinet 技术文档的注释

如果您在本文档或任何 Fortinet 技术文档中发现了错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com。

客户服务和技术支持

请访问我们的技术支持网站，以获取防病毒保护和网络攻击定义更新、固件更新、产品文档更新，技术支持信息，以及其他资源。网址：http://support.fortinet.com。

您也可以到 http://support.fortinet.com 注册您的 FortiGate 防病毒防火墙或在任何时间登陆到该网站更改您的注册信息。

以下电子邮件信箱用于 Fortinet 电子邮件支持：

amer_support@fortinet.com	为美国、加拿大、墨西哥、拉丁美洲和南美地区的客户提供服务。
apac_support@fortinet.com	为日本、韩国、中国、中国香港、新加坡、马来西亚、以及其他所有亚洲国家和澳大利亚地区的客户提供服务。
eu_support@fortinet.com	为英国、斯堪的纳维亚半岛、欧洲大陆、非洲和中东地区的客户提供服务。

关于 Fortinet 电话支持的信息，请访问 http://support.fortinet.com。

当您需要我们的技术支持的时候，请您提供以下信息：

- 您的姓名
- 公司名称
- 位置
- 电子邮件地址
- 电话号码
- FortiGate 设备生产序列号
- FortiGate 型号
- FortiGate FortiOS 固件版本
- 您所遇到的问题的详细说明

IPSec VPN

本章提供了一个关于如何使用互联网安全协议 （IPSec）标准创建 VPN 通道的概述。

本章包含了以下标题：

IPSec VPN 技术

IPSec 提供了使用密码的安全服务，它是建立在提高 IP 网络的加密、认证和数据完整性的标准技术的基础上的。

因为 IPSec 运行在网络层，最终系统和应用程序无须做任何改变就可以使用它。一个 IPSec VPN 通道冲传输的加密的数据包看起来就象普通的数据包，所以他们可以很容易地在任何 IP 网络之间传输和路由，例如在互联网中。唯一知道有关加密的信息的是传输的终点。

IPSec 将不同的技术组合成一个完整的加密系统。其中，主要的元素和选项包括：

- IPSec VPN 安全协议
- 密钥管理
- 安全组合
- 通道协商
- 网络拓扑

IPSec VPN 安全协议

IPSec 使用了两个安全协议，认证报头 （AH）和压缩安全有效载荷 （ESP）。认证报头协议提供了验证 IP 数据包的真实性和完整性的方法。使用 AH 时，将使用一个密钥和一个 hash 算法计算出一个校验和。HASH 算法可以是 MD5 或者 SHA-1。校验和提供了一个关于输入数据的指纹，可以用来验证数据包的来源和内容的真实性和完整性。

ESP 从 AH 扩展出来，提供了加密数据的方法和验证数据的真实性和完整性的方法。在使用 IPSec 通道模式的时候，它的工作方式是将整个 IP 数据包，包括报头和有效载荷，一起压缩成胶囊，装入一个新的数据包，并为它生成一个新的 IP 报头。这个新的 IP 报头用来将被保护的数据路由到它的目的地。

ESP 允许您同时加密和鉴别、仅加密或者仅鉴别。有效的加密选项包括 DES、3DES 和 AES。FortiGate 设备是为支持 ESP 优化的。

密钥管理

在任何加密系统中都有三个基本元素：

- 一个将信息变成编码的算法，
- 一个作为这个算法的秘密起点的密钥，
- 一个控制这个密钥的管理系统。

IPSec 提供了两种控制密钥交换和管理的方法：手工密钥和自动密钥交换 （IKE）自动密钥管理。

手工密钥

当选择了手工密钥之后，必须在通道两端的输入互相匹配的安全参数。包括加密和认证密钥在内的这些设置必须保密，可以避免未经授权的人员对数据解密，哪怕他们知道加密所使用的算法。

安全地发布的手工密钥可能有些困难。管理手工密钥所用的用户的大量的数字也将花费许多时间。

使用预置密钥或证书的自动互联网密钥交换（自动 IKE）

为了更加灵活和方便地部署多个通道，自动密钥管理系统是必须的。IPSec 支持使用互联网密钥交换协议进行自动密钥生成和协商。这种密钥管理方法通常被称做自动 IKE。Fortinet 支持预置密钥的自动 IKE 和证书自动 IKE。

预置密钥的自动 IKE

通过在会话的两端配置相同的预置密钥，可以使他们通过这一方法彼此验证对方。对等的双方不必真正把密钥发送给对方。取而代之的是，作为安全协商过程的一部分，他们可以将密钥和 Diffie-Hellman 组结合起来创建一个会话密钥。这个会话密钥可以用于加密和认证的目的，并且在通讯会话的过程中通过 IKE 自动重建。

预置密钥与手工设置密钥相似的地方在于他们都需要网络管理员去分配和管理 VPN 通道两端的匹配信息。当一个预置密钥改变时，系统管理员必须更新通道两端的设置。

使用证书的 自动 IKE

这种密钥管理方法需要一个受信任的第三方，证书发布中心 （CA）的参与。在一个 VPN 中对等的双方首先请求生成一系列密钥，通常被称做公钥 / 私钥对。CA 为每一方的公钥签名，创建一个签名的数字证书。对等的双方可以联系 CA 以找回他们自己的证书，加上 CA 自己的。一旦证书被上载到 FortiGate 设备，并配置好了适当的策略和 IPSec 通道，那么双方就可以发起通讯了。在通讯中，IKE 负责管理证书交换，从一方将签名的数字证书传送到另一方。这个签名的数字证书的有效性由每一端的 CA 证书验证。当认证完成时，IPSec 通道就建立起来了。

在某些方面，证书类似于手工密钥管理或预置密钥。因此，证书最适合部署大型网络。

安全组合

安全组合 （SA）是关于安全通讯通道所用的方法和参数的一组安全设置。VPN 会话的双方之间完全地通讯至少需要两个 SA，每个方向一个。

一个 SA 将安全算法和密钥、密钥管理方法 （手工或者自动 IKE），SA 有效期以及其他参数集合在一起。一个 SA 是由目的地址 （IPSec 终点）、安全协议 （AH 或 ESP）和安全参数索引 （SPI）唯一识别的。

通道协商

要建立一个 IPSec 通道，会话的对等的双方需要从一个协商过程开始。对于手工密钥通道，这个过程是非常简单的，因为全部安全组合 （SA）参数已经在两端都定义了。结果是，协商在会话开始之前就已经决定了。如果参数匹配，将建立通道。

对于一个自动 IKE 通道，需要两个协商阶段：

- 在第一阶段，对等的双方建立一个用于 IPSec SA 协商的安全通道。
- 在第二阶段，对等的双方协商用于加密和认证的 IPSec SA，然后交换用户数据。

第一阶段协商

自动 IKE 通道协商的第一阶段的组成包括交换关于如何认证和保证通道安全的提议的交换。对等的双方交换如下安全参数提议：

- 模式 （主模式或进取模式）
- 加密算法 (DES 和 3DES) 和认证算法 (MD5 和 SHA-1)
- 一个 Diffie-Hellman 组

一个预置密钥或 RSA/DSA 证书可选的参数包括扩展认证 （XAuth），一个用于认证除了对等的双方之外的用户的方法；双方失效检测 （DPD），一个保持激活的结构，用来检测 IKE 对等的双方失效和中断不再使用的 SA； NAT 跨越，使 IPSec 能够同使用不同 IP 报头的 NAT 和 PAT 设备协同工作。

在对等的双方都同意接受至少一组已经提出的安全参数，并交换了密钥或者证书之后，第一阶段就完成了，这个通道已经建立。

主模式和进取模式

第一阶段可以在使用主模式或者进取模式时进行。这两个模式都建立一个安全通道。主模式还提供一个附加的安全特性，称做识别保护，它可以隐藏 VPN 对等双方的身份，使得它们不被被动的窃听者发现。然而，主模式比进取模式要求交换更多的信息，并且当 VPN 的一方将它的身份用做认证过程的一部分的时候，主模式很难有效地被利用。

Diffie-Hellman 组

Diffie-Hellman 交换是通过一个不安全的媒介建立一个预置安全密钥的方法。FortiGate 设备支持 Diffie-Hellman 组 1、2 和 5。模数的大小用于根据所用的组计算密钥的变化：

- DH 组 1：768- 比特 模数
- DH 组 2：1024- 比特 模数
- DH 组 5：1536- 比特 模数

尽管 DH 组 5 使用它的更大的模数使得处理更加安全，但是它也需要更长的时间生成密钥。会话的双方必须使用相同的 DH 组。

扩展认证 (XAuth)

IKE 扩展认证 （XAuth）是现有的 IKE 协议的一个增强版本。它允许用户在第一阶段和第二阶段的交换中分别被认证 （在标准 IKE 中，只有对等的端点被认证，用户不被认证）。

XAuth 使用一个已经建立的认证机制，例如 IPSec IKE 协议的 RADIUS，PAP 和 CHAP。

当 XAuth 被应用于远程访问用户时，它是非常有价值的。因为它提供了一个比从前的应用方式更加高级的认证控制。如果远程访问用户使用一组预置密钥 （一个共享的密码），强烈建议使用 XAuth。

端点失效检测

有时候，如果路由出了问题或者有其他麻烦，对等的双方的通讯连接可能变得不可用。在这种情况下，IKE 和 IPSec 可能进入未知状态，结果是 SA 保持开通直到它们的有效期自然过期。在这种情况下，数据包可能会发进一个黑洞并丢失。

为了预防这种情况并使得通道能够被同一端或者另一端重建，发展出了端点失效检测协议 （DPD）。不同于常规的保持激活机制或者心跳计划的是，DPD 不在正常时发送探测消息。取而代之的是，DPD 只在 SA 已经空闲了很长一段时间或者 FortiGate 设备在一个最近一直空闲的 SA 上发送一个新的通讯的时候发送探测消息。

DPD 的优点是它还还提供了异步配置，允许对等的双方在一个不同的时间间隔彼此发送消息。如果，例如，一端对资源有紧急的需求，它可以被配置为每当网络变得非活动时立刻发送消息。而和它对等的一方，在另一方面，可以被配置为使用更长的时间间隔发送消息。

NAT 跨越

网络地址转换以两种方式工作。静态 NAT 将每个内部地址映射到一个可路由的公共地址。通过使用 PAT （端口地址转换），IP 地址和端口都可以被转换，可以将许多私有地址映射到同一个单独的公共 IP 地址。

因为 ESP，IPSec 安全协议，是一个端口无关的协议。它不能被 PAT 重映射。因此，当有多个用户位于一个 PAT 之后的时候，PAT 可能无法将 ESP 数据包转发到他们原定的接收者。

NAT 跨越特性通过在第一阶段协商期间沿着数据路径检测 NAT 设备和将 ESP 数据包封装进 UDP 数据包解决了这一问题。因为 NAT 设备可以操作 UDP，所以这些数据包可以按照常规的方法路由。

NAT 保持激活频率

当一个 NAT 设备为一个通讯流分配了一个 IP 地址和端口号之后，NAT 设备决定当没有通讯的时候新地址的效用持续多长时间。如果它们使用了 NAT 跨越，为了保证在 SA 过期之前 NAT 映射不被改变，IPSec 对等的双方需要定期通过 NAT 设备发送数据包。NAT 跨越激活时间间隔应当少于 NAT 设备所使用的会话有效期的值。

第二阶段协商

在建立了一个安全的通过了认证的通道之后，在第二阶段中继续协商过程。在这一阶段中，会话的双方协商用于加密和认证通道中的数据的 SA。对等的双方交换彼此的提议以决定在 SA 中使用哪些安全参数。如同已经在第一阶段见到的参数一样，这些参数包括加密和认证算法，一个 Diffie-Hellman 组，和一个密钥有效期设置。另外，还可以指定向前保密和重放检测。

向前保密

向前保密（PFS）提高了 VPN 通道的安全性。它确保在第二阶段生成的每个密钥与第一阶段或第二阶段生成的其它密钥无关。PFS 在第二阶段通道建立时强迫发起一个新的 Diffie-Hellman 密钥交换，而且在每次密钥有效期到期时都需要发起一个新的 Diffie-Hellman 密钥交换以生成新的密钥。这在付出少许处理延迟的代价的基础上，增强了系统的安全性。

如果您不启用 PFS，VPN 通道中每一个第二阶段密钥都是从第一阶段密钥中创建的。这种方法创建密钥需要更少的处理器时间，但是降低了安全性。如果一个未经授权的用户取得了在第一阶段创建的密钥，第二阶段的全部密钥都受到了威胁。

重放检测

IPSec 通道容易受到重放攻击。重放攻击发生在未被授权的一方在截获了一系列 IPSec 包后把他们重放回通道的时候。攻击者可以用这种方法制造一个拒绝服务攻击（DoS），使用这种数据包淹没通道。攻击者也可以修改并重放截获的数据包以试图取得受信网络的访问权。

启用重放攻击检测可以检查每个 IPSec 包的顺序编号确定它是否已经被接收过了。如果此数据包在给定的序列范围之外，FortiGate 将丢弃它们。

在检测到重放攻击的时候，FortiGate 可以发送一封报警邮件。

网络拓扑

您的 VPN 网络的拓扑结构决定了连接、数据流和路由通讯流的类型和数量。您可以在全网络拓扑、部分网络拓扑和星型拓扑配置方式之间作出选择。

全网状网络

在一个全网状网络拓扑结构中，全部的 VPN 端点都互相连接以形成一个网络。从一个端点到另一个端点只需要一跳的距离。通讯可以发生在哪怕是不需要通讯的两个对等的端点之间。这种拓扑结构对于失效有最大程度的容忍能力。如果一个端点失效了，只有它到网络的连接会丢失；网络的其他部分不受影响。这种拓扑的缺点是它的规模很难控制，因为它需要在所有的端点之间建立通道。

半网状网络拓扑

一个半网状网络类似于全网状网络，但不是在每两个端点之间都有通道。它只在经常需要通讯的端点之间彼此建立通道。

星型 （集线器和辐条）网络 （VPN 集中器）

在一个星型网络中，全部的 VPN 通道都连接到一个单独的端点上。它的功能就象一个通讯集中器或者集线器。而另一端的端点是网络的辐条。它们只连接到这个集线器，而不是彼此连接。全部通讯都通过这个集线器进行管理。它被称做 VPN 集中器。

星型网络的优势在于辐条配置十分简单，因为它们只需要很少的策略规则。同样，一个星型拓扑结构的网络为每个辐条提供相同的处理效率。一个星型网络的缺点是它使用单一的端点去控制和管理全部的 VPN。一旦这个端点失效，这个网络中的全部加密通讯也就都无法进行了。

与 IPSec VPN 产品的兼容性

因为 FortiGate 支持 VPN 的 IPSec 工业标准，所以可以在 FortiGate 和任何支持 IPSec VPN 的客户端或者网关 / 防火墙之间配置 VPN。

FortiGate IPSec VPN 支持以下标准：

- IPSec 互联网协议安全标准
- 基于预置密钥的自动 IKE
- 基于 X.509 认证的自动 IKE
- 可以完全定制的手工密钥
- 通道模式的 ESP 安全
- DES 、3DES （三倍 DES）和 AES 加密
- Diffie-Hellman 分组 1、2、和 5
- 杂凑信息验证代码 -MD5 （HMAC MD5 ）数据认证 / 完整性认证或杂凑信息验证代码 - 安全散列算法 1 （HMAC SHA1） 数据认证 / 完整性认证
- 进取模式和主模式
- NAT 跨越
- XAuth （扩展认证）
- 对方失效检测 (DPD)
- 重放检测
- IPSec 冗余
- 向前保密
- 星型配置的 VPN 集中器

为了能够成功地创建 IPSec VPN 通道，FortiGate IPSec VPN 配置必须兼容第三方的 IPSec VPN 配置。Fortinet 已经测试了 FortiGate VPN 同以下第三方产品的兼容性：

- NetScreen 互联网安全产品
- SonicWALL PRO 防火墙
- Cisco PIX 防火墙
- Cisco IOS 路由器
- Check Point NG 防火墙
- Check Point NG-1 防火墙
- Check Point FP-1 防火墙
- Check Point FP-2 防火墙
- Check Point FP-3 防火墙
- Linksys 防火墙路由器
- SafeNet IPSec VPN 客户端
- 安全计算 Sidewinder
- SSH 哨兵

关于 FortiGate VPN 的兼容性的详细信息，请联系 Fortinet 技术支持。

使用认证的 IPSec VPNs

本章提供了关于公共密钥密码技术和数字认证的一个概述。它还描述了如何管理 FortiGate 设备上的数字证书，以及如何使用一个 FortiGate 设备上的数字证书建立一个 IPSec VPN。本章包括了许多使用数字证书进行认证的 IPSec VPN 的例子。

注意：在配置 FortiGate VPN 时不需要数字证书。数字证书是一个用于为系统管理员提供便利的高级特征。本手册假定用户已经具有关于如何为他们自己的目的配置数字证书的有关知识。

本章叙述了如下内容：

概述

数字证书用于在 IPSec 通讯会话双方之间建立一个加密的 VPN 通道之前，保证会话双方的的可信性。

要使用数字证书，首先要成为公共密钥基础设置 （PKI）的成员。PKI 将数字证书、公共密钥密码学、和证书认证集成到一个全面的安全架构中。考虑到 IPSec VPN，PKI 至少要包括对 VPN 对等的双方 （VPN 客户和网关）发行数字证书。更多更高级的应用包括证书的管理工具、更新和撤消。

PKI 使用以下方式保护信息：

- 身份识别。证书授权中心发布的数字证书允许 VPN 对等的双方信任会话的各方的身份。
- 完整性验证。数字证书保证了证书 “签名” 的消息或文档在传输过程中没有被修改或者破坏。
- 授权访问。数字证书可以用来替代更加简单的认证方法，例如用户名和密码验证。
- 认可支持。数字证书使 VPN 对等双方的身份生效。

PKI 的规模易于控制。大型的 IPSec 网络可能难于管理。维护超过 100 个使用手工或预置密钥的 VPN 端点可能要消耗大量的时间，并且在某种程度上，总会受到错误的影响。因为在各个端点需要输入大量的彼此各不相同的配置。使用 PKI 之后，管理过程变得更加简单，可以避免出现错误。

公钥密码系统

在公钥密码系统中，每个 VPN 端点生成一对密钥。其中一个密钥是私有的，必须保密；另一个是公共的，可以自由地发布。这两个密钥的作用是互补的。任何被其中一个密钥加密的东西都可以被另一个密钥解密。例如，一个 VPN 端点使用他自己的私有密钥加密了一条信息。如果接收者可以使用发送者的公共密钥对这条信息解密，那么接收者就知道这条信息是发送者使用它自己的私有密钥加密的。这一过程需要消息的接收者拥有发送者的公开密钥的复本，并且确定这个复本属于发送者，而不是伪装成发送者的什么人。

数字证书提供了这一保证。一个数字证书包括一个公开密钥和一些识别信息。这些识别信息是由一个受信任的第三方签名的。这个第三方通常是一个证书授权中心（CA）。因为这个 CA 是可信的，所以它发行的证书也就是可信的。

要获得一个证书，VPN 会话的一方需要在一个证书申请表中将它自己的公钥发送到 CA。这个证书请求包括用来唯一识别这个 VPN 会话方的身份的信息，例如一个 IP 地址，域名或者电子邮件地址。根据所申请的数字签名，CA 创建一个数字证书，这个数字证书和 VPN 会话方自己的证书一同生效。

一旦 VPN 会话方获得了他们的数字证书和 CA 证书，他们就准备好开始通讯了。当一个会话开始时，IKE 包括一个 VPN 对等的双方交换他们的数字证书的阶段。在这期间他们是由 CA 证书验证的。在这一验证过程之后，公共密钥被从这个数字证书中提取出来，并应用到要建立的 IPSec VPN 通道中去。

RSA 和 X.509 标准

Rivest-Shamir-Adleman (RSA) 加密方法被 VPN 端点用于生成他们私有的和公开的密钥对，并由 CA 将数字签名附加到证书。

X.509 证书标准被 PKI 和 IPSec VPN 采用为证书的主要标准。一个 X.509 证书包括：

- 所有者的识别信息，
- 关于 CA 发行者的 RSA 数字签名和信息 ，
- 所有者的公共密钥，
- 有效数据，
- 分类和参考数字。

注意： VPN 会话方和 CA 必须使用 X.509 证书。

扩展认证 (XAuth)

在大多数应用中，数字证书已经足以让 VPN 会话的双方彼此认证对方。然而，为了提高安全性，您可以选择使用其他的认证方式。这在远程 VPN 端点是一个使用一组预置密钥 （一个与其他用户共享的密码）的拨号用户 （客户或者网关）的时候尤其有用。如果远程 VPN 端点使用的是静态的 IP 地址则不需要这种额外的安全保证。

要提供用户级的安全，除了由数字证书提供的设备级的安全以外，您必须实施扩展认证 （XAuth）。XAuth 依赖于一个安全机制 （例如一个外部的 RADIUS 服务器）来要求用户提供他们的用户名和密码。因为 XAuth 的这一要求是发生在第一阶段和第二阶段之间的，所以无论 VPN 会话的双方运行于主模式或者进取模式都可以实施 XAuth。

可以将 FortiGate 设备配置为 XAuth 服务器或者 XAuth 客户端。作为 XAuth 服务器时，FortiGate 与一个本地用户组或者一个远程的 RADIUS 服务器联合工作，在远程 VPN 端点试图建立通道时要求它们进行认证。作为 XAuth 客户端时，FortiGate 设备被配置为在要求认证时提供它自己的用户名和密码。

基于 ID 的认证

除了 XAuth 之外，您还有一个安全选项：您可以要求 VPN 端点提供他们的本地 IP （网关）或者主机域名 （客户端），作为认证过程的一部分。然而，这一方法需要使用进取模式 （比主模式的安全性稍微低一些），并且建议仅仅应用于将预置密钥作为他们的主要认证方法的会话方。关于详细信息请见 第 47 页 “ 预置密钥 IPSec VPN” 。

证书管理的一般配置步骤

证书管理包括两个基本过程：获取一个签名的本地证书 （FortiGate 设备用来对其他设备认证它自己的证书）和获取一个 CA 证书 （FortiGate 设备用来验证从其他设备接收到的证书的有效性的证书）。

Fortinet 使用一个手工的操作来获得证书。这包括从您的本地计算机将文本文件复制和粘贴到证书发布中心，和从证书发布中心复制和粘贴到您的本地计算机。

获得一个签名的本地证书的一般步骤

为了获得一个签名的本地证书，需要完成如下步骤：

1 生成一个证书申请。当您执行这一步的时候，生成一个本地 FortiGate 设备的私有和公共密钥对。公共密钥伴随着这个证书申请，私有密钥需要保密。
请见 第 16 页 “ 生成证书申请” 。

2 下载证书申请。在您生成完证书申请之后，需要将它从 FortiGate 设备下载到管理员电脑上。
请见下载证书申请。

3 将证书申请提交到 CA。这需要将证书申请从一个文本文件中复制出来并粘贴到一个由 CA 控制的网页页面中。
请见 第 19 页 “ 请求签名的本地证书” 。

4 从 CA 得到签名了的证书。CA 在完成了对申请的签名后会提醒您。您必须进入 CA 的网页服务器，复制这个签名了的证书并将它保存到您的本地计算机。
请见 第 19 页 “ 领取签名的本地证书” 。

5 导入签名的证书。这包括将签名的证书从您的本地电脑传输到 FortiGate 设备。
请见 第 20 页 “ 导入签名的本地证书” 。

获取一个 CA 证书的一般配置步骤

要获得一个 CA 证书，需要完成如下步骤：

1 获得这个 CA 证书。连接到 CA 控制的网页，复制这个 CA 证书，并将它保存到您的本地电脑中。这个 CA 证书包括一个认可这个 CA 发布的全部证书的合法性的证书路径。
请见 第 20 页 “ 领取一个 CA 证书” 。

2 导入这个 CA 证书。这包括将这个 CA 证书从您的本地电脑传输到 FortiGate 设备中。
请见 第 20 页 “ 导入一个 CA 证书” 。

获取一个签名的本地证书

一个签名了的本地证书为 FortiGate 设备提供了向其他设备证明它自己的身份的手段。

注意： VPN 端点必须使用服从 X.509 标准的证书。

生成证书申请

在这一过程中，您需要使用 RSA 生成一个公开密钥和私有密钥对。公开密钥是证书申请的基本元素。

证书申请的构成根据您的 PKI 的要求而各不相同。有些 PKI 可能只要求用于识别被认证的 FortiGate 设备的基本的主题信息。其他 PKI 可能要求一些附加的信息，例如这个 FortiGate 设备所在的城市、州和国家的名称等。

按如下步骤生成证书申请

1 进入 **VPN > 本地证书。**

2 单击生成。

3 输入一个证书名。典型的证书名是被认证的 FortiGate 设备的名称。

这个名称可以包含数字 (0-9)，大写或小写字母 (A-Z, a-z)，以及特殊符号 - 和 _。不能包含其他特殊符号和空格。

4 配置用于识别这个被认证的 FortiGate 设备的主题信息。

最好使用 IP 地址或者域名。如果不能用 （例如一个拨号客户端），使用一个电子邮件地址。

主机 IP	在主机 IP 栏，输入被认证的 FortiGate 设备的 IP 地址。
域名	在域名栏，输入被认证的 FortiGate 设备的完整的正式域名。不要包括协议指定 （http://）或者任何端口号和路径名。
电子邮件	在电子邮件栏，输入被认证的 FortiGate 设备的所有者的电子邮件地址。一般来说只有客户需要输入电子邮件地址。网关不需要。

注意：如果您要指定一个主机 IP 或者域名，使用 IKE 协商所在的那个接口 （例如：本地 FortiGate 设备的外部接口）所用的 IP 地址或者域名。如果证书中的 IP 地址与本地接口的 IP 地址不匹配 （或者证书中的域名与 FortiGate 设备的 IP 的 DNS 解析不匹配），某些实施方式的 IKE 将拒绝这个连接。这一规则的实施根据不同的 IPSec 产品而有所变化。

5 配置用于认证更多的需要认证的对象的可选信息。

机构部门	输入一个用于识别为这个 FortiGate 设备申请证书的机构的部门或者单位的名称。（例如制造商或者 MF）。
机构	输入为这个 FortiGate 设备申请证书的机构的合法名称 （例如 Fortinet）。
位置 （城市）	输入这个 FortiGate 设备所在的城市或者城镇的名称 （例如广州）。
州 / 省	输入这个 FortiGate 设备所在的州或者省的名称 （例如广东省）。
国家	选择这个 FortiGate 设备所在的国家。
电子邮件	为这个 FortiGate 设备输入一个联系邮件地址。一般来说只有客户需要输入电子邮件地址。网关不需要。

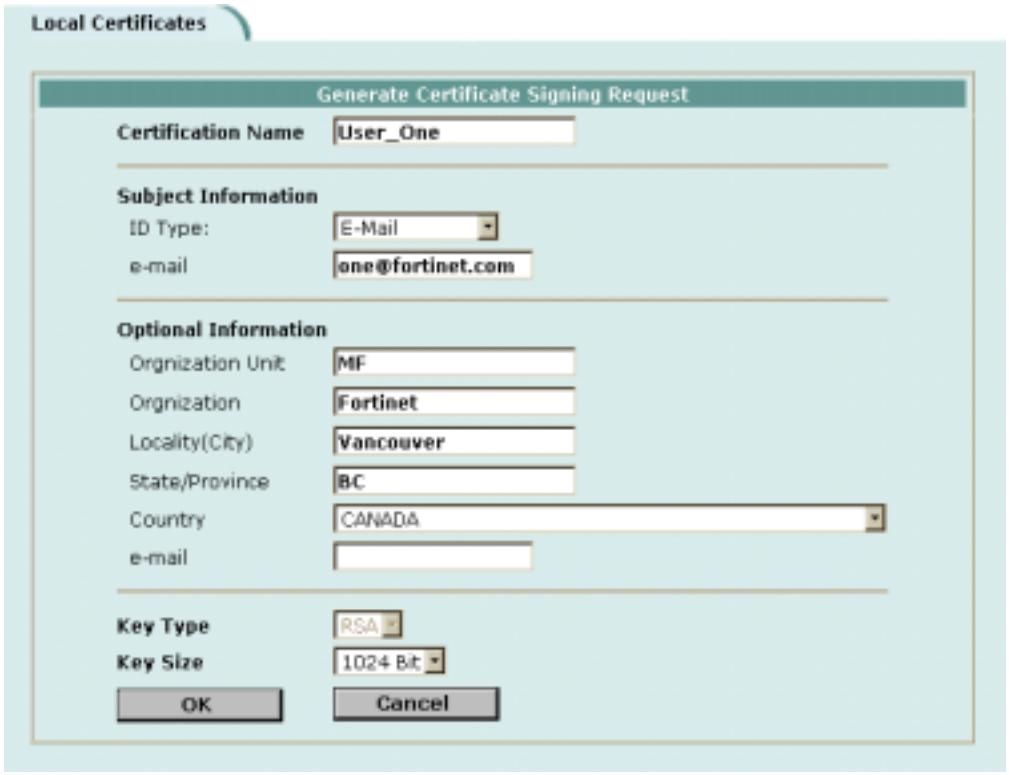
6 配置密钥。

密钥类型	选择 RSA 作为密钥加密类型。不支持其他类型的密钥。
密钥长度	选择 1024 比特、1536 比特或者 2948 比特。密钥越长，生成得越慢，但是也更安全。不是所有产品都支持这三种长度的密钥。

7 单击确定以生成私有和公共密钥对和证书申请。

将生成私有 / 公共密钥对，证书申请将显示在本地证书列表中，其状态为申请中。

图 1: 添加一个本地证书



使用 CLI：

```
execute vpn certificates local generate <名称_字符串>
subject {<主机_ip> | <域名_字符串> | 电子邮件地址_字符串>}
[unit <名称_字符串> org <组织机构名称_字符串> city <城市名称_字符串> state <省/自治区名称_字符串> country <国家代码_字符串> email <邮件地址_字符串>]]]]]
keysize {1024 | 1536 | 2048}
```

下载证书申请

这一操作从 FortiGate 设备将证书下载到您的管理员电脑中。

按如下操作下载证书申请

1 进入 **VPN > 本地证书。**

2 单击下载 以将本地证书下载到管理员电脑。

将显示文件下载对话框。

3 单击保存。

4 为文件命名，并将它保存到管理员电脑的一个目录中。

使用 CLI：

```
execute vpn certificates local download <证书名称_字符串> <文件名 _ 字符串 > <tftp_ip>
```

请求签名的本地证书

在如下操作中，您将从管理员电脑中将证书复制并粘贴到 CA 网页服务器上。

按如下步骤申请签名的本地证书

1. 启动管理员电脑，在一个文本编辑器中打开本地证书申请。
2. 复制这个证书申请。
3. 连接到 CA 网页服务器。
4. 请求签名的本地证书。

   按照 CA 网页服务器的指引完成如下步骤：

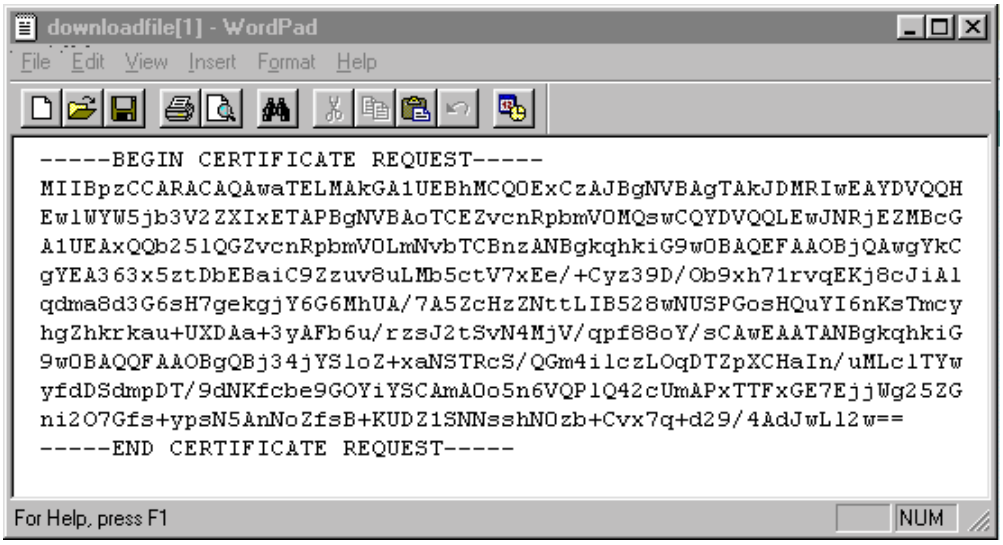
   • 在 CA 服务器上添加一个 base64 编码的 PKCS#10 证书申请，

   • 将证书申请粘贴到 CA 网页服务器，

   • 将证书申请提交给 CA 网页服务器。

   现在这个证书申请已经提交给 CA 服务器等待签名了。

图 2: 在一个文本编辑器中打开一个证书申请



领取签名的本地证书

在如下操作中，您将在受到来自 CA 的证书申请已签名的提示后，连接到 CA 网页服务器并下载签名了的本地证书，将它保存到管理员电脑。

按照如下步骤领取已经签名的本地证书

1. 连接到这个 CA 网页服务器。
2. 按照 CA 网页服务器的指引下载已经签名了的本地证书。

   将显示文件下载对话框。
3. 单击保存。

4 将文件保存到管理员电脑上的一个目录中。

导入签名的本地证书

在如下操作中，您将从管理员电脑中把签名了的本地证书导入到 FortiGate 设备中。

按照如下步骤导入签名了的本地证书

1 进入 **VPN > 本地证书。**

2 单击导入。

3 输入路径，或者单击浏览以在管理员电脑中定位签名了的本地证书。

4 单击确定。

已经签名的本地证书将显示在本地证书列表中，其状态为 OK。

使用 CLI：

```
execute vpn certificates local import < 文件名 _ 字符串 >
<tftp_ip>
```

获取一个 CA 证书

VPN 端点为了彼此向对方证明它们自己，必须都从同一个证书发布中心获得一个 CA 证书。这个 CA 证书为 VPN 端点提供了验证它们从其它设备收到的数字证书的方法。

FortiGate 设备获取 CA 证书是为了验证它从远程 VPN 端点收到的数字证书。这个远程 VPN 端点获取 CA 证书是为了验证它从 FortiGate 设备收到的数字证书。

注意：CA 证书必须服从 X.509 标准。

领取一个 CA 证书

连接到 CA 网页服务器并将 CA 证书下载到管理员电脑。

按照如下操作领取 CA 证书

1 连接到 CA 网页服务器。

2 按照 CA 网页服务器的指引下载 CA 证书。

将显示文件下载对话框。

3 单击保存。

在管理员电脑的一个目录中保存 CA 证书。

导入一个 CA 证书

将 CA 证书从管理员电脑导入 FortiGate 设备。

按照如下步骤导入 CA 证书

1 进入 **VPN > CA 证书。**

2 单击导入。

3 输入 CA 证书在管理员电脑上的路径，或者单击浏览进行定位。

4 单击确定。

这个 CA 证书将显示在 CA 证书列表中。

使用 CLI：

```
execute vpn certificates ca import <文件名_字符串> <tftp_ip>
```

使用证书的 IPSec VPN 一般配置步骤

一个使用证书的自动 IKE VPN 配置的构成包括第一阶段参数和第二阶段配置参数，通道两端的源地址和目的地址，以及用于控制对这个 VPN 通道的访问的加密策略。

按照如下步骤创建一个使用数字证书的 VPN 配置

1 添加第一阶段配置以定义认证远程 VPN 端点所用的参数。尽管远程 VPN 端点可以是一个客户端或者一个网关，这个步骤经常在 “添加一个远程网关”中提到。

请见 第 21 页 “ 添加第一阶段配置” 。

2 添加第二阶段配置以定义用于创建和维护自动密钥 VPN 通道的参数。这一步骤通常在 “添加一个通道”中提到。

请见 第 26 页 “ 添加第二阶段配置” 。

3 添加源地址。

请见 第 28 页 “ 添加一个源地址” 。

4 添加目的地址。

请见 第 28 页 “ 添加目的地址” 。

5 添加包括了这个通道、这个通道两端的源地址和目的地址的加密策略。

请见 第 29 页 “ 添加一个加密策略” 。

添加第一阶段配置

当您添加第一阶段配置的时候，您需要定义 FortiGate 设备和 VPN 远端 （网关或客户）用于彼此认证以建立 IPSec VPN 通道的有关条件。第一阶段的配置参数的构成包括远程 VPN 端点的名称，远程端点的地址类型 （静态 IP 地址或者拨号用户），建议用于认证过程的设置 （加密和认证算法），以及本地数字证书。为了能够成功地认证，远程 VPN 端点必须使用兼容的第一阶段建议设置来配置。

第一阶段配置和第二阶段配置彼此相关。在第一阶段中 VPN 的两端被认证，在第二阶段则建立起了通道。您可以选择使用相同的第一阶段参数建立多个通道。换句话说，同一个远程 VPN 端点 （网关或客户）可以有多个连接到本地 VPN 端点 （FortiGate 设备）的多个通道。

当 FortiGate 设备收到一个 IPSec VPN 连接请求时，它首先根据第一阶段参数认证 VPN 端点。然后，它根据请求的源地址和目的地址发起一个 IPSec VPN 通道和应用加密策略。

当您添加完一个第一阶段配置之后，可以修改它的某些参数。然而，无论如何您也不能更新远程 VPN 端点的 IP 地址的类型 （静态或者拨号）。如果这个 VPN 端点的地址类型从静态变成了拨号地址，您必须删除原来的第一阶段设置然后添加一个新的，反之亦然。如果您只是简单地添加了第二个第一阶段配置来说明这种变化，这个通道将失效。发生这种情况是因为这个静态第一阶段配置比拨号第一阶段配置优先，从而覆盖了它。一般的规则是对每个远程 VPN 端点只添加一个第一阶段配置。

按照如下步骤添加一个第一阶段配置

1 进入 **VPN > IPSec > 第一阶段。**

2 单击新建以添加一个新的第一阶段配置。

3 输入远程 VPN 端点的网关名称。

远端 VPN 端点可以是另一个网络的网关或者互联网上的一个独立的客户。

这个名称可以含有数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符或者空格符。

4 选择远程网关地址类型。

- 如果远程 VPN 端点有静态 IP 地址，选择静态 IP 地址。
- 如果远程 VPN 端点使用动态 IP 地址 （DHCP 或 PPPoE），或者远程 VPN 端点有一个无须端点识别处理的静态地址，选择拨号用户。

根据您所选择的远程网关地址类型，可能还要填写其他栏目。

远程网关：静态 IP 地址

IP 地址	如果您选择了静态 IP 地址，将出现地址栏。输入连接到 FortiGate 设备的远程 IPSec VPN 网关或者客户的 IP 地址。这个内容是必须输入的。

远程网关：拨号用户

端点选项	如果您选择了拨号用户，在高级选项中将出现端点选项。可以使用端点选项在第一阶段协商中认证远程 VPN 的 ID。详细信息请见步骤 13。 注意：不建议对使用数字证书的 VPN 端点使用这一认证方法。

5 选择进取模式或主模式 （ID 保护）。

两种模式都将建立一个安全通道。进取模式比主模式的步骤更少。当使用进取模式时，VPN 端点使用明文交换彼此的识别信息。当使用主模式时，识别信息是隐藏的。当一个 VPN 端点是一个拨号用户，将它的 ID 作为认证过程的一部分的时候，进取模式是标准的选择。

当使用进取模式时，有些配置参数，例如 Diffie-Hellman (DH) 组，不能协商。一般的规则是，当您使用进取模式时，您需要在 VPN 会话的双方输入匹配的配置。

VPN 双方必须使用同一模式。

6 配置 P1 提议。

最多可以为第一阶段的提议选择三个加密算法和认证算法。默认情况下选定了两个。

如果要减少选择的组合的数量，单击减号。要增加选择的组合的数量，单击加号。VPN 会话的双方必须使用相同的 P1 提议设置。

加密算法

空	仅限测试。

DES	数据加密标准。
3DES	三倍 DES。
AES	高级加密标准，128、192 和 256 比特变量。
	认证算法
空	仅限测试。
SHA1	安全 Hash 算法。
MD5	消息摘要算法。

7 选择 DH 组。

选择一个或多个 Diffie-Hellman 组用于 IPSec VPN 连接的第一阶段中的提议。您可以选择 DH 组 1、2 或 5。

- 当 VPN 端点使用静态 IP 地址并使用进取模式时，选择一个单独匹配的 DH 组。
- 当 VPN 端点在一个拨号配置中使用进取模式时，最多可以为拨号服务器选择三个 DH 组，为拨号用户（客户端或者网关）选择一个 DH 组。
- 当 VPN 端点使用主模式时，您可以选择多个 DH 组。

8 输入密钥有效期。

指定在第一阶段密钥的有效期。密钥有效期是在第一阶段加密密钥过期之前以秒为单位计算的时间。当密钥过期之后，无须中断服务就可以生成一个新的密钥。P1 提议中的密钥有效期可以从 120 秒到 172800 秒。

9 在认证方式中，选择 RSA 签名。

10 在证书名中，选择一个已经由 CA 数字签名了的本地证书。

关于在 FortiGate 设备中添加一个本地证书的方法，请见 第 16 页 “ 获取一个签名的本地证书” 。

11 不用输入本地 ID。

当 FortiGate 设备配置为使用数字证书并作为客户端运行时，它不将它的本地 ID 发送到远程的 VPN 端点。作为代替的是它发送它的公开的名称（在本地证书的主题中指定的 IP 地址、域名或者电子邮件地址）。

12 可以选择是否配置高级选项。

拨号组，端点选项， XAuth， NAT 跨越和对方失效检测都是可选的参数。

注意：如果您使用数字证书（RSA 签名的）来验证 VPN 端点，有些高级选项可能无须配置。特别是，端点选项是不推荐的。因为它们是用于预置密钥的。有关的详细信息，请见 第 47 页 “ 预置密钥 IPSec VPN” 。

13 可选的，选择一个端点选项。（在使用数字证书时不推荐）。

接受任何端点 ID	选中则可接受任何端点 ID（因此不验证远程 VPN 端点的端点 ID）。
接受这个端点 ID	这个选项使用一个共享的用户名（ID）和密码（预置密钥）认证一个特定的 VPN 端点或者一组 VPN 端点。选择这个选项还要添加端点 ID。有关的详细信息请见 第 49 页 “ 共享的用户名和密码配置细节” 。
接收拨号组中的端点 ID	选择这个选项可以使用各自的用户名（ID）和密码（预置）密钥认证每个远程 VPN 端点。选择这个选项还需要选择一个拨号组（用户组）。有关的详细信息请见 第 50 页 “ 独立用户名和密码配置细节” 。 在配置这个端点选项之前要先配置用户组。

14 （可选的）配置 XAuth。

XAuth（IKE 扩展认证）在用户级认证 VPN 端点。如果 FortiGate 设备（本地 VPN 端点）被配置为 XAuth 服务器，它将使用一个用户组对远程 VPN 端点进行认证。这个用户组中包括的用户可以是配置在 FortiGate 设备中的，或者是位于远程的 LDAP 或者 RADIUS 服务器上。如果 FortiGate 设备被配置为 XAuth 客户端，当它被要求认证的时候它将提供一个用户名和密码。

XAuth：作为客户端

名称 输入本地 VPN 端点用于对远程 VPN 端点证明它自己的用户名。

密码 输入本地 VPN 端点用于对远程 VPN 端点证明它自己的密码。

XAuth：作为服务器

加密方式 选择 XAuth 客户端、FortiGate 设备和认证服务器之间的加密方法。

PAP 密码认证协议。

CHAP 挑战－握手认证协议。

混合 选择混合可以在 XAuth 客户端和 FortiGate 设备之间使用 PAP，在 FortiGate 设备和认证服务器之间使用 CHAP。

只要可能就能使用 CHAP。如果认证服务器不支持 CHAP 则使用 PAP。（所有的 LDAP 和部分微软 RADIUS 使用 PAP）。如果认证服务器支持 CHAP 但是 XAuth 客户端不支持 CHAP，就使用混合（Fortinet 远程 VPN 客户端使用混合）。

用户组 选择 XAuth 认证的一组用户。这个用户组中的单独的一个用户可以由本地认证或者由一个或多个 LDAP 或 RADIUS 服务器认证。

在用户组被选中之前它必须被添加到 FortiGate 的配置中。

15 （可选的）配置 NAT 跨越。（NAT 跨越在默认情况下是启用的。）

启用 选择启用，如果您希望 IPSec VPN 的数据流通过一个执行 NAT 的网关。如果没有检测到 NAT 设备，启用 NAT 穿越功能不会有任何效果。在网关的两端必须使用相同的 NAT 穿越设置。

激活频率 如果启用了 NAT 穿越，则可以修改保持活动的时间间隔，以秒为单位。这个时间间隔指定了空 UDP 包发送的频率，这个 UDP 包穿过 NAT 设备，以保证 NAT 映象不会改变，直到第一阶段和第二阶段的密钥过期。保持活动的时间间隔可以从 0 一直到 900 秒。

16 （可选的）配置端点失效检测。（默认情况下 DPD 是启用的）。

使用这些设置可以监视 VPN 双方的连接状态。DPD 允许清除已经失效的连接并建立新的 VPN 通道。不是所有的销售商都支持 DPD。

启用 选择启用可以启用本地和远程端点之间的 DPD。

短时空闲 设置以秒为单位的时间。这是本地 VPN 端点需要考虑连接是否空闲之前所经历的时间。在这段时间之后，当本地端点要向远程 VPN 端点发送通讯时，它必须同时发送一个 DPD 探测，以判断连接的状态。要控制 FortiGate 设备用来使用 DPD 探测检测失效端点的时间的长度，配置重试累计和重试间隔。

重试累计 设置本地 VPN 端点认为通道已经失效并断开安全联结之前使用 DPD 探测的重复次数。根据您的网络的具体情况，将重试累计设置得足够高可以避免网络拥塞或其他传输问题带来的影响。

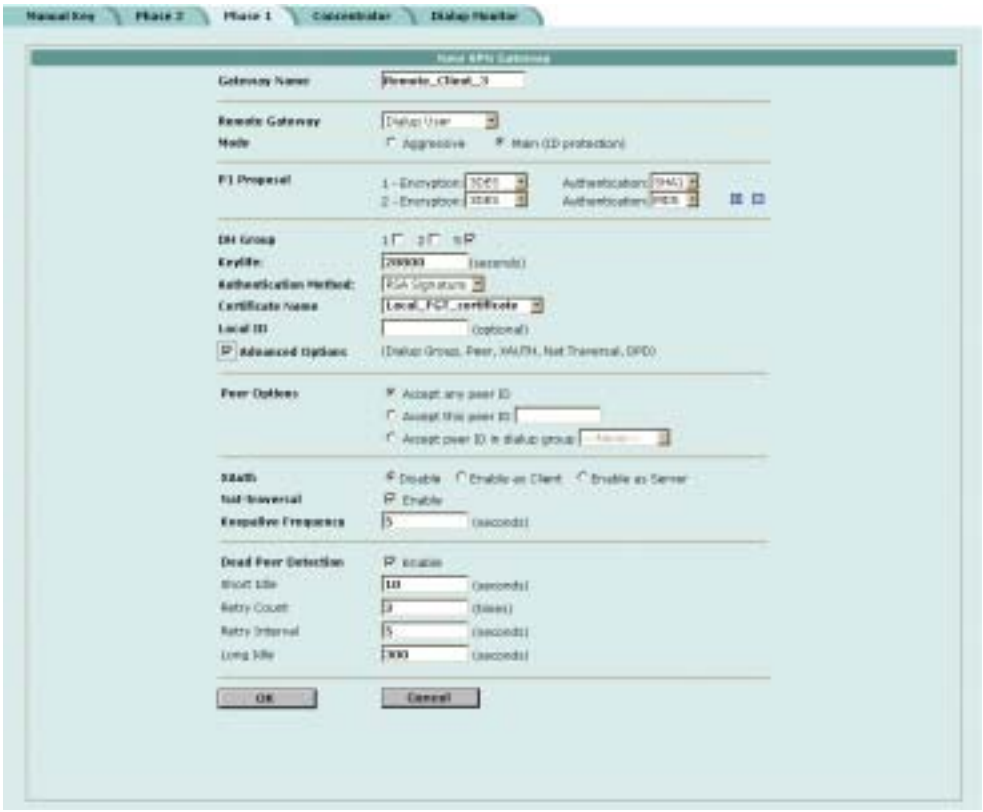
重试间隔 设置以秒为单位的时间，它是本地 VPN 端点设备在两次 DPD 探测之间等待的时间。

长时空闲 设置以秒为单位的时间。这是本地 VPN 端点在探测连接的状态之前需要等待的时间。如果在本地端点和远程端点之间没有通讯，在经历了这段时间之后本地端点将发送 DPD 探测以判断通道的状态。

注意：Fortinet 远程 VPN 客户端和 SSH 哨兵 VPN 客户端不支持 DPD。所以在使用这些客户端的时候不要配置 DPD。

17 单击确定以保存第一阶段参数。

图 3: 添加一个第一阶段配置



使用 CLI：

```
set vpn ipsec phase1 <名称_字符串>
keylife <密钥有效期_整数> type {static | dynamic} [gw <网关_ip>]
proposal {des-md5 des-sha1 3des-md5 3des-sha1 aes128-md5 aes128-sha1 aes192-md5 aes192-sha1 aes256-md5 aes256-sha1}
authmethod {psk <预置密钥_字符串> | rsasig <证书_字符串>}
mode {aggressive | main)
dhgrp {[1] [2] [5]}
nattraversal {enable | disable} keepalive <保持激活频率_整数>
dpd {enable | disable} [dpdidleworry <短期空闲_整数> dpdretrycount <重试_整数> dpdretryinterval <DPD 间隔_整数> dpdidlecleanup <长期空闲_整数>]
```

```
[localid <本地 ID_ 字符串 >]
peertype {any | one | dialup} [usrgrp <用户组名称 _ 字符串 >]
[peerid <端点 ID_ 字符串 >]
xauthtype {disable | client | server} [authusr <用户_字符串> <
密码 _ 字符串 >] [authsrvtype {pap | chap} authusrgrp <用户组名称 _
字符串 >]
```

添加第二阶段配置

添加第二阶段配置以指定在本地 VPN 端点 （Fortigate 设备）和远程 VPN 端点（VPN 网关或客户端）之间创建和维护 VPN 通道所用的参数。

按以下方法添加第二阶段配置：

1 进入 **VPN > IPSEC > 第二阶段。**

2 单击新建以添加新的第二阶段配置。

3 输入一个通道名称。

这个名称可以含有数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符或者空格符。

4 选择一个连接到这个 VPN 通道的远程网关。

远程网关可以是另一个网络中的网关或者互联网上的一个独立的客户。远程网关是作为第一阶段配置的一部分添加的。有关的详细信息请见 第 21 页 “ 添加第一阶段配置” 。

可以选择单独的拨号远程网关或者最多三个静态远程网关。如果您要配置 ISec 冗余，就需要多个静态远程网关。使用加号和减号可以增加或者减少连接到这个 VPN 通道的静态远程网关的数目。关于 IPSec 冗余的详细信息，请见 第 127 页 “ IPSec VPN 冗余” 。

5 配置 P2 提议。

可以为第二阶段的提议最多选择三个加密和认证算法组合。默认情况下选定了两个。要减少选定的组合的数量，单击减号。要增加选定的组合的数量，单击加号。加密方法可以在 DES、3DES 和 AES128、192 和 256 之间选择。认证方法可以在 SHA1 和 MD5 之间选择。“无”仅用于测试。VPN 会话的双方必须使用相同的 P2 提议设置。

6 （可选的）启用重放检测。

启用了重放检测时候，FortiGate 设备检查每个 IPSec 数据包的序列号，检查它是否已经被接收过了。如果数据包不在一个特定的序列范围内，FortiGate 设备将丢弃它们。这样提高了安全性。

FortiGate 设备还可以在检测到一个重放数据包的时候发送一个报警邮件。要接收这个报警邮件，进入**日志和报告 > 报警邮件 > 分类**，然后选择启用紧急防火墙 VPN 事件或异常的报警邮件。

注意：如果您已经为 P2 提议选择了无认证，则不用选择重放检测。请见步骤 5。

7 （可选的）启用向前保密 （PFS）。

PFS 在通道建立和每当超过密钥有效期的时候强制进行一个新的 Diffie-Hellman 交换。这保证了第二阶段的密钥于第一阶段创建的密钥或者在第二阶段创建的其他密钥无关。PFS 增加了安全性，代价是造成了少许的处理延迟。

8 选择 DH 组。

为第二阶段提议选择一个 Diffie-Hellman 组。您可以选择 DH 组 1、2 或 5。DS 组 1 的安全性最低。DH 组 5 的安全性最高。不要选择多个 DH 组。VPN 会话的双方必须使用相同的 DH 组设置。

9 输入密钥有效期。

指定在第二阶段密钥的有效期。密钥有效期限制第二阶段的密钥在一定时间内，或者给定数量的千字节的数据被 VPN 通道处理过之后过期，或者两者都有。如果您选择两者都是，则经过了指定的时间或者处理了指定量的数据这两种情况中的任何一种出现，密钥都会过期。当密钥过期之后，无须中断服务就可以生成一个新的密钥。P2 提议中的密钥有效期可以从 120 秒到 172800 秒或者从 5120 千字节到 99999 千字节。

10 （可选的）启用自动密钥保持激活。

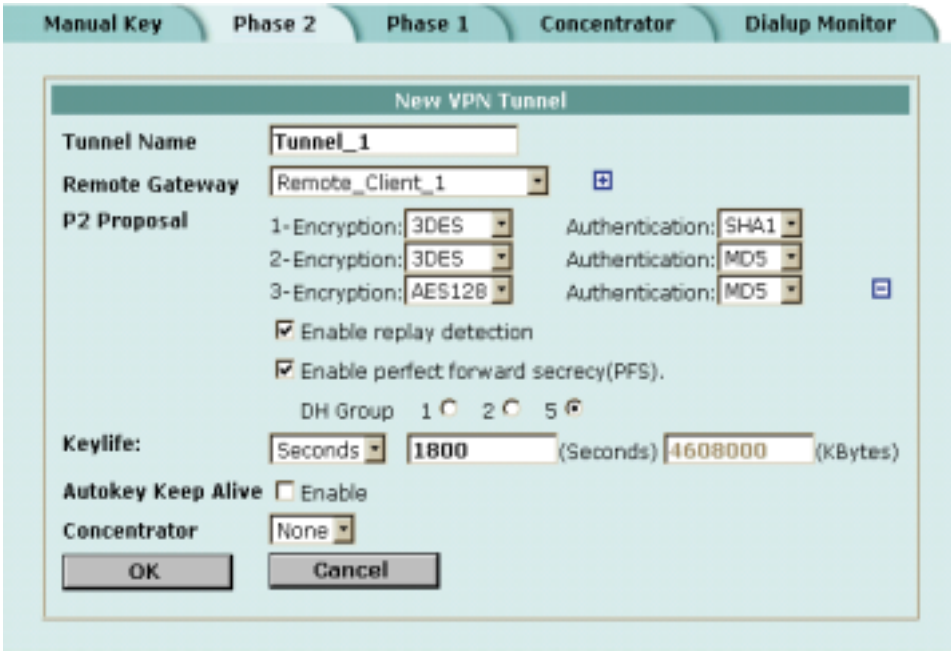
启用自动密钥保持激活可以在没有数据传输的时候也保持 VPN 通道的有效。

11 （可选的）选择一个集中器。

如果您希望通道成为星型 VPN 配置的一部分，选择集中器。如果您使用了这个操作， 在 第 116 页 “ VPN 辐条一般配置步骤” 可以为集中器添加通道。下次您打开通道，集中器栏会显示您添加到通道的集中器的名字。

12 单击 **确定** 保存自动密钥 VPN 通道。

图 4: 添加一个第二阶段配置



使用 CLI：

```
set vpn ipsec phase2 <名称_字符串>
```

```
phase1name {[<名称_字符串> [<名称_字符串> [<名称_字符串>]]] | none}
proposal {null-null | null-md5 | null-sha1 | des-null | des-md5 | des-sha1 | 3des-null | 3des-md5 | 3des-sha1 | aes128-null | aes128-md5 | aes128-sha1 | aes192-null | aes192-md5 | aes192-sha1 | aes256-null | aes256-md5 | aes256-sha1}
keylifeseconds <密钥有效期（秒）_整数> keylifekbs <密钥有效期（千字节）_整数>
dhgrp {1 | 2 | 5}
replay [enable | disable}
pfs [enable | disable} keepalive {enable | disable}
concentrator {<名称 - 字符串> | none}
```

添加一个源地址

源地址位于本地 VPN 端点的内部网络中。它可以是单独的一个计算机地址或者一个网络的地址。

1 进入**防火墙 > 地址。**
2 选择一个内部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）
3 单击新建添加一个地址。
4 输入这个地址的名称，IP 地址和网络掩码，这些参数可以是位于本地 VPN 端点的内部接口上的一个计算机或者整个子网的。
5 单击确定以保存源地址。

使用 CLI：

```
set firewall address <接口名_字符串> <名称_字符串> subnet <地址_ip> <网络掩码 _ip>
```

添加目的地址

目的地址可以是位于互联网上的一个 VPN 客户端的地址或者一个远程 VPN 网关后面的一个网络的地址。

1 进入**防火墙 > 地址。**
2 选择一个外部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）
3 单击新建添加一个地址。
4 输入地址的名称、IP 地址和网络掩码。这些参数可以是远程 VPN 端点的内部接口上的一台计算机或者整个子网的。
5 单击确定以保存目的地址。

使用 CLI：

```
set firewall address <接口_字符串> <名称_字符串> subnet <地址_ip> <网络掩码 _ip>
```

添加一个加密策略

VPN 连接本地、内部网络和远程、外部网络。加密策略的重要任务是定义（和限制）这些网络中的哪些地址可以使用这个 VPN。

一个 VPN 只需要一个加密策略来控制向内和向外的连接。根据您对它所做的配置，加密策略控制您的内部网络中的用户能否建立到远程网络的连接（向外连接），和远程网络中的用户能否建立一个到您的内部网络的通道（向内连接）。这种灵活性使得单一的加密策略就能够完成两个常规的防火墙策略的工作。

尽管加密策略同时控制进入和发出的连接，它也必须被配置成为一个向外的的策略。一个向外的策略有一个位于内部网络中的源地址和一个位于外部网络中的目的地址。这个源地址可以识别内部网络中的哪些地址属于这个 VPN。目的地址可以识别远程网络中的哪些地址属于这个 VPN。标准的向外的策略包括内部到外部和 DMZ 到外部。

注意：目的地址可以是一个位于互联网上的 VPN 客户端地址或者位于一个远程 VPN 网关后边的网络的地址。

除了通过地址定义这个 VPN 的成员之外，您还可以配置这个加密策略的服务，例如 DNS、FTP、和 POP3，以及根据一个预定义的时间表（每天中的时间，或者一周、月、年中的某一天）来允许连接。您还可以配置加密策略的以下内容：

- 向内的 NAT 以转换进入的数据包的源地址。
- 向外的 NAT 以转换发出的数据包的源地址。
- 流量控制以控制这个 VPN 可用的带宽和这个 VPN 的优先级。
- 内容配置文件可以在这个 VPN 中应用防病毒保护、网页内容过滤、电子邮件过滤、文件传输和电子邮件服务。
- 记录日志使得 FortiGate 设备记录所有使用这个 VPN 的连接。

加密策略举例

如果您的内部网络中的用户希望连接到一个远程 VPN 网关后边的网络，或者如果来自远程网络的用户希望连接到您的内部网络中的资源，那么您就需要添加一个内部到外部的加密策略。这个策略的源地址必须是您的内部网络中的一个地址。这个策略的目的地址必须是远程 VPN 网关后边的网络中的地址。

这个策略必须包含您创建的用于同远程 VPN 网关通讯的 VPN 通道。同时作为添加到 VPN 通道的一部分，您必须指定它所允许的连接的方向。在这个例子中，您将同时允许向内和向外的连接。可选地，您还可以配置流量控制、病毒防护和网页过滤，以及记录日子后。

当您的内部网络中的用户试图连接到远程 VPN 网关后边的网络的时候，这个加密策略拦截这个连接企图并发起一个添加到这个策略的 VPN 通道。这个通道使用添加到它的配置中的远程网关来连接到远程 VPN 网关。当这个远程 VPN 网关接受到这个连接企图时，它检查它自己的策略、网关和通道配置。如果配置允许，这两个 VPN 端点将协商一个 IPSec VPN 通道。

多重交叉加密策略

在大多数情况下，您需要为子网之间的每个 VPN 添加一个加密策略。为相同的 VPN 添加多重策略可能导致冲突，如果这些策略共享相同的源、目的地址和服务设置。当策略在这种情况下互相重叠时，系统可能使用错误的加密策略或者通道可能失败。

有时候，无论如何您可能都需要对单一的 VPN 添加多个加密策略。例如，在某些情况下需要加密策略以配置到一个远程网关的冗余连接。同样，要控制对同一个子网内的不同服务的访问、或者根据不同的时间表控制对一个子网的访问也需要多个加密策略。

如果您添加的多重加密策略可能重叠，记住以下规则：

- 您可以为同时包含了进取模式和主模式规则的拨号配置添加重叠的通配符策略 （组预置密钥）。
- 您可以添加重叠的策略以控制到远程网关的冗余连接 （IPSec 冗余）。
- 您可以添加重叠的策略在同一子网之间应用不同的服务，但是这些策略必须使用相同的通道。
- 您可以添加重叠的策略在同一子网中应用不同的时间表设置，但是这些策略必须使用相同的通道。

开头的两个配置包括添加相等并有相同优先级的加密策略。因为他们是相等的，所以无论系统选择哪个都没关系。后边的两个配置添加了不相等的加密策略。因为他们处理通讯的方式不同，根据这个连接请求的性质，无论系统选择哪个加密策略都没关系。为了保证系统选择正确的策略，这些加密策略必须使用相同的通道。

如果实施的内容包括不相邻的两个子网之间的连接，也需要多重加密策略。例如，如果一个外部网络中的拨号用户请求连接到 FortiGate 设备后边的内部网络和 DMZ 网络，那么 FortiGate 设备必须为每个连接配置一个单独的加密策略。在这个配置中，不要试图在两个加密策略中使用一个通道。

按以下步骤添加加密策略：

1 进入**防火墙 > 策略。**

2 选择您要添加策略的那个策略列表 （不同型号的 FortiGate 设备的选择方法略有不同）。

3 单击 新建 以添加新的策略。

4 把 源地址 设为源地址。

5 把 目的地址 设置为目的地址。

6 设置服务以控制允许通过这个 VPN 连接的服务类型。
您可以选择任意以允许全部支持的服务通过这个 VPN 连接，或者选择一个特定的服务或服务组以限制允许通过这个 VPN 连接的服务。

7 将动作设置为加密。

8 配置加密参数。

VPN 通道	为这个加密策略选择一个自动密钥通道。
允许向内	选择 **允许向内** 可以允许向内连接的用户连接到源地址上。
允许向外	选择 **允许向外** 可以允许向外连接的用户连接到目的地址上。

向内 NAT FortiGate 可以把接收到的向内的数据包的源地址转换为连接到源地址网络上的 FortiGate 内部网络接口的 IP 地址。通常这是 FORTIGate 设备的一个内部接口。

向内 NAT 使得本地主机无法看到远程主机（在远程 VPN 网关后面的网络中的主机）的 IP 地址。

向外 NAT FortiGate 可以把向外发送的数据包的源地址转换为连接到目的地址网络上的 FortiGate 的网络接口的 IP 地址。通常情况下这是 FortiGate 设备的一个外部接口。

向外 NAT 使得远程主机无法看到本地主机 （位于本地 VPN 网关后边的网络中的主机）的 IP 地址。

如果实现了向外 NAT，它受到以下限制：

只能在通道的一端配置向外 NAT。

没有实现向外 NAT 的那一端需要有一个内部 -> 外部的策略以将另一端的外部接口指定为目的地 （这将是一个公共 IP 地址）。

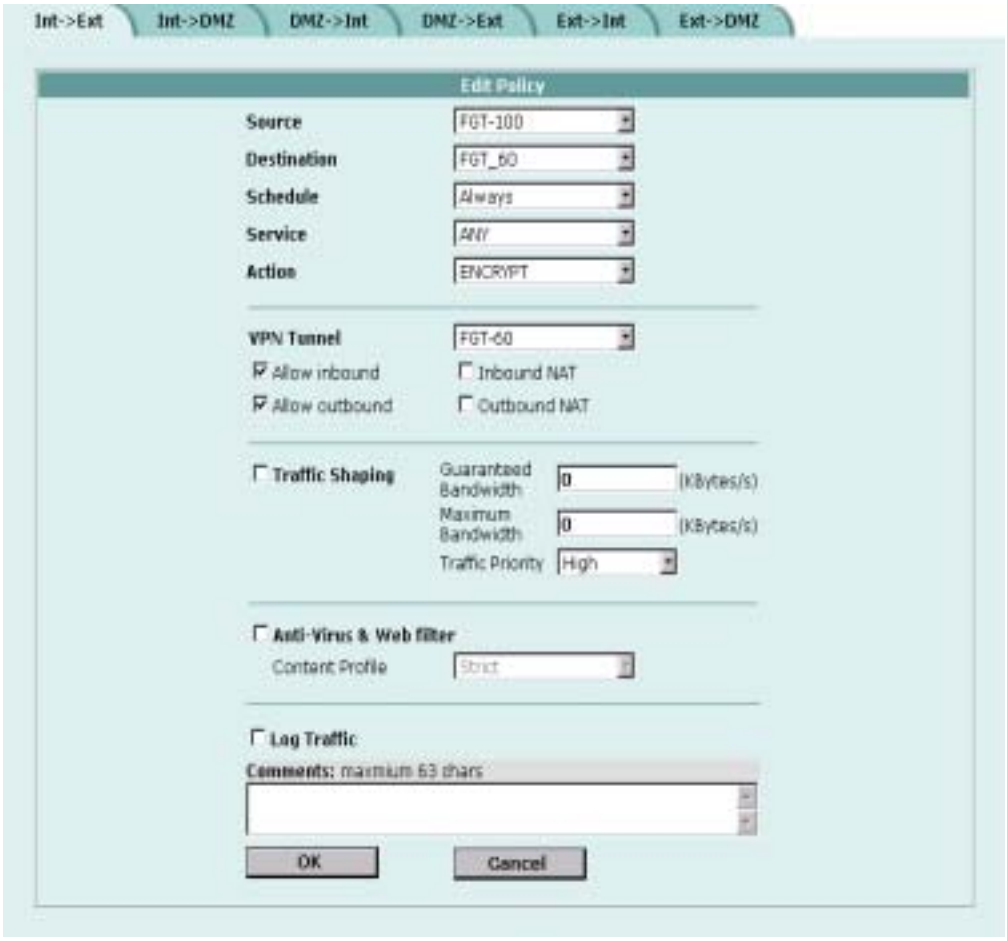
通道和通道中的通讯只能由配置了向外 NAT 的那一端初始化。

关于配置策略的其他设置的详细信息请见 *FortiGate 安装和配置指南*。

9 单击确定以保存加密策略。

10 排列加密策略在策略列表中的位置，使它在其他具有同样源和目的地址以及服务的策略之上，以确保加密策略能匹配 VPN 连接。

图 5: 添加一个加密策略



使用 CLI：

```
set firewall policy
```

```
src_intf <源接口_字符串> dstintf <目的接口_字符串> policyid <策略编号 _ 整数 > move < 从 - 策略 _ 整数 > to < 到 - 策略 _ 整数 >
```

```
status {enable | disable}
```

```
srcaddr <源地址_字符串> dstaddr <目的地址_字符串> schedule <时间表名称 _ 字符串 > service < 服务名称 _ 字符串 > action encrypt
```

```
vpntunnel <通道名称 _ 字符串 > inbound {allow | deny} natinbound {enable | disable} outbound {allow | deny} natoutbound {enable | disable}
```

```
trafficshaping {enable | disable} gbandwidth < 保证带宽 _ 整数 > maxbandwidth < 最大带宽 _ 整数 > priority {high | medium | low}
```

```
avwebfilter {enable < 配置文件名 _ 字符串 > | disable}
```

```
logtraffic {enable | disable}
```

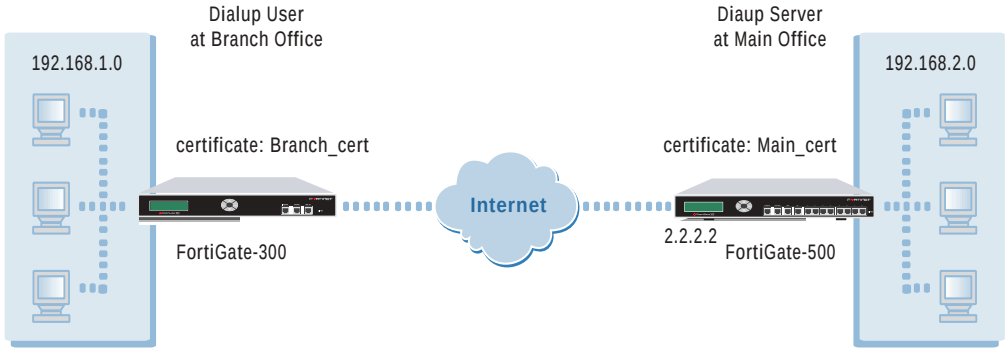
例子：单一动态 VPN 端点

在这个例子中，一个单独的 VPN 通道连接了两个 IPSec VPN 端点。它们都是网关而且都是 FortiGate 防火墙设备。它们使用数字证书来向对方证明自己的身份和保证通讯通道的安全。远程 VPN 端点使用一个动态 IP 地址，它是一个拨号用户。本地 VPN 端点使用一个静态 IP 地址，它是一个拨号服务器。

网络拓扑结构

这个在分支机构中的网关是一个 FortGate 300 防火墙。在主办公室中的网关是一台 FortiGate 500。连接私有网络的通道位于这个网关的后面。

图 6: 使用证书认证



一般配置步骤

要在使用基于证书的认证的网关之间启用自动 IKE 密钥的 IPSec VPN 通道，您必须在两个 FortiGate 设备中输入相应的设置。FortiGate500 位于主办公网络。作为拨号服务器，它被当作本地设备。FortiGate300 位于一个分之机构的网络中。作为拨号用户，它被看作远程设备。

分支机构网关配置

在位于分支机构的 FortiGate300 输入以下配置。

1. 给这个 FortiGate 设备添加一个签名的本地证书。
2. 添加第一阶段参数。第一阶段参数负责安排 VPN 对话双方在建立一个通道之前如何向对方证明自己的身份。输入主办公网关名称，选择静态 IP 地址，添加这个主办公机构 IP 地址，并且指定进取模式。然后，添加拨号用户用来向拨号服务器认证它自己的证书。
3. 添加第二阶段配置。第二阶段配置负责通道的维护。添加一个通道名称，然后选择您作为第一阶段的一部分添加的远程网关。然后指定会话双方使用的第二阶段提议的值。
4. 作为这个 VPN 的一部分，添加一个源地址以指定在分支机构的内部网络中的一个地址或者地址范围。
5. 作为这个 VPN 的一部分，添加一个目的地址以指定主办公机构的内部网络中的地址或地址范围。
6. 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到分支办公机构的内部网络的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

主办公机构配置

在位于主办公机构的 FortiGate500 中输入如下配置。

1 为这个 FortiGate 设备添加一个签名了的本地证书。

2 添加第一阶段参数。为拨号用户添加一个网关名，选择拨号拥护，指定进取模式，然后选择 P1 提议的值。另外，添加拨号服务器用于向拨号用户证明它自己的身份的证书。

3 添加第二阶段参数。添加一个通道名，然后选择您作为第一阶段参数的一部分添加的远程网关。另外还要指定会话双方所用的第二阶段提议的值。

4 作为这个 VPN 的一部分，添加一个源地址以指定在主办公机构的内部网络中的一个地址或者地址范围。

5 作为这个 VPN 的一部分，添加一个目的地址以指定分支办公机构的内部网络中的地址或地址范围。

6 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到主办公机构的内部网络的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

配置参数

在主办公机构的拨号服务器和分支办公机构的拨号用户 （远程网关）中必须输入以下配置参数。

表 1：添加到拨号服务器和拨号用户的本地证书 （远程网关）

域名	主办公机构值	分支办公机构值
证书名	Main_Cert	Branch_Cert
主题信息		
ID 类型	主机 IP	电子邮件
IP 地址 / 域名 / 电子邮件	2.2.2.2	user@branch.com
选项信息		
组织机构	空	空
机构	主办公机构	分支办公机构
位置 （城市）	空	空
州 / 县	空	空
国家	空	空
电子邮件	空	空
认证密钥		
密钥类型	RSA	RSA
密钥长度	1024 比特	1024 比特

表 2：在拨号服务器和拨号用户 （远程网关）上输入的第一阶段配置

域名	主办公机构值	分支办公机构值
网关名称	Branch_Office	Main_Office
远程网关	拨号用户	静态 IP 地址
IP 地址		2.2.2.2
模式	进取模式	进取模式
P1 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
DH 组	5	5
密钥有效期	3600	3600
认证方式	RSA 签名	RSA 签名
证书名称	Main_Cert	Branch_Cert
本地 ID	空	空
端点选项	接受任何端点 ID	接受任何端点 ID
XAuth	禁用	禁用
NAT 跨越	启用	启用
保持激活频率	6	6
端点失效检测	启用	启用
短期空闲	10	10
重试计数	3	3
重试间隔	5	5
长期空闲	300	300

表 3：在拨号服务器和拨号用户 （远程网关）上输入的第二阶段配置

域名	主办公机构值	分支办公机构值
通道名称	Branch_Office_VPN	Main_Office_VPN
远程网关	Branch_Office	Main_Office
P2 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
启用重放检测	启用	启用
启用向前保密 （PFS）	启用	启用
DH 组	5	5
密钥有效期	300 秒	300 秒
自动密钥保持激活	启用	启用
集中器	无	无

表 4：源地址和目的地址

域名	主办公机构值	分支办公机构值
源地址		
地址名	Main_Office	Branch_Office
IP 地址	192.168.2.0	192.168.1.0
网络掩码	255.255.255.0	255.255.255.0
目的地址		
地址名	Branch_Office	Main_Office
IP 地址	192.168.1.0	192.168.2.0
网络掩码	255.255.255.0	255.255.255.0

表 5：加密策略

域名	主办公机构值	分支办公机构值
源地址	Main_Office	Branch_Office
目的地址	Branch_Office	Main_Office
任务计划	总是	总是
服务	任意	任意
动作	加密	加密
VPN 通道	Branch_Office_VPN	Main_Office_VPN
允许向内	启用	启用
允许向外	启用	启用
向内 NAT	不启用	不启用
向外 NAT	不启用	不启用

配置分支机构网关

配置由 7 个步骤组成：获取一个签名的本地证书 （由 5 个子步骤组成），添加 CA 证书，添加第一阶段配置，添加第二阶段配置，添加源地址，添加目的地址，添加内部到外部的加密策略。

基于 Web 的管理程序的配置步骤

1 生成本地证书。

进入 **VPN > 本地证书。**

- 单击生成。
- 证书名：Branch_Cert
- ID 类型：电子邮件
- 电子邮件： user@branch.com
- 机构： Branch Office
- 单击确定

2 从 FortiGate 设备将这个本地证书下载到管理员电脑。

进入 **VPN > 本地证书。**

- 单击下载 将本地证书下载到管理员电脑。
- 将显示文件下载对话框。
- 单击保存。
- 命名文件并将它保存在管理员电脑的一个目录中。

3 将这个证书请求提交给 CA。

请见 第 19 页 “ 请求签名的本地证书” 。

4 从 CA 接收签名了的本地证书。

请见 第 19 页 “ 领取签名的本地证书” 。

5 导入这个签名了的本地证书。
进入 **VPN > 本地证书。**
- 单击导入。
- 输入路径或单击浏览以在管理员电脑中定位本地证书。
- 单击确定。

6 导入 CA 证书。
进入 **VPN > CA 证书。**
- 单击导入。
- 输入路径或单击浏览以在管理员电脑中定位 CA 证书。
- 单击确定。

注意：在导入 CA 证书之前，需要先将它添加到管理员电脑。请见 第 20 页 “ 获取一个 CA 证书” 。

7 添加第一阶段配置。
进入 **VPN > IPSEC > 第一阶段。**
- 单击新建。
- 网关名：Main_Office
- 远程网关：静态 IP 地址
- IP 地址 2.2.2.2
- 模式：进取
- 第一阶段提议：
  加密 1 3DES， 认证 1 SHA1
  加密 2 3DES， 认证 2 MD5
- DH 组： 5
- 密钥有效期：3600 （秒）
- 认证方式：RSA 签名
- 证书名称： Branch_Cert
- 本地 ID：空
- 端点选项：接受任意端点 ID
- XAuth：禁用
- NAT 跨越：启用
- 保持激活频率：6 （秒）
- 端点失效检测：启用
- 短期空闲：10 （秒）
- 重试计数：3 （次）
- 重试间隔：5 （秒）
- 长期空闲：300 （秒）
- 单击确定

8 添加第二阶段配置。

进入 **VPN > IPSEC > 第二阶段。**

- 单击新建。
- 通道名称：Main_Office_VPN
- 远程网关： Main_Office
- P2 提议：
  1- 加密 3DES， 认证 SHA1
  2- 加密 3DES， 认证 MD5
- 启用重放检测：启用
- 启用向前保密：启用
- DH 组：5
- 密钥有效期：300 （秒）
- 自动密钥保持激活：启用
- 集中器：无
- 单击确定

9 添加源地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部。**

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：内部。

- 单击新建。
- 地址名称：Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

10 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部。**

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：外部。

- 单击新建。
- 地址名称： Main_Office
- IP 地址：192.168.2.0
- 网络掩码：255.255.255.0
- 单击确定。

11 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部。**

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部。**

- 单击新建。
- 源地址：Branch_Office
- 目的地址：Main_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Main_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 生成本地证书。

```
execute vpn certificates local generate Branch_Cert subject
user@branch.com org Branch_Office keysize 1024
```

2 下载本地证书。

```
execute vpn certificates local download Branch_Cert Branch_Cert
192.168.1.150
```

3 导入本地证书。

```
execute vpn certificates local import Branch_Cert 192.168.1.150
```

4 导入 CA 证书。

```
execute vpn certificates ca import CA_Cert 192.168.1.150
```

5 添加第一阶段配置。

```
set vpn ipsec phase1 Main_Office keylife 28800 type static gw
2.2.2.2 proposal 3des-sha1 3des-md5 authmethod rsasig
Branch_Cert mode aggressive dhgrp 5 nattraversal enable
keepalive 6 dpd enable dpdidleworry 10 dpdretrycount 3
dpdretryinterval 5 dpdidlecleanup 300
```

6 添加第二阶段配置。

```
set vpn ipsec phase2 Main_Office_VPN phase1name Main_Office
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 5
keylifeseconds 1800 keepalive enable
```

7 添加源地址。

```
set firewall address Internal Branch_Office subnet 192.168.1.0
255.255.255.0
```

8 添加目的地址。

```
set firewall address External Main_Office subnet 192.168.2.0
255.255.255.0
```

9 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Branch_Office dstaddr Main_Office schedule Always
service ANY action encrypt vpntunnel Main_Office_VPN inbound
allow outbound allow
```

10 移动加密策略。

```
set firewall policy srcintf internal dstintf external move 2
to 1
```

配置主办公机构网关

配置由七个步骤组成：获取一个签名了的本地证书 （由 5 个子步骤组成）、添加一个 CA 证书、添加第一阶段配置、添加第二阶段配置、添加源地址、添加目的地址、添加内部到外部的加密策略。

基于 Web 的管理程序配置步骤

1 生成本地证书。

进入 **VPN > 本地证书**。

- 单击生成。
- 证书名：Main_Cert
- ID 类型：主机 IP
- IP：1.1.1.1
- 机构：Main Office
- 单击确定

2 从 FortiGate 设备将这个本地证书下载到管理员电脑。

进入 **VPN > 本地证书**。

- 单击下载  将本地证书下载到管理员电脑。
- 将显示文件下载对话框。
- 单击保存。
- 命名文件并将它保存在管理员电脑的一个目录中。

3 将这个证书请求提交给 CA。

请见 第 19 页 “ 请求签名的本地证书” 。

4 从 CA 接收签名了的本地证书。

请见 第 19 页 “ 领取签名的本地证书” 。

5 导入这个签名了的本地证书。
进入 **VPN > 本地证书**。
- 单击导入。
- 输入路径或单击浏览以在管理员电脑中定位本地证书。
- 单击确定。

6 导入 CA 证书。
进入 **VPN > CA 证书**。
- 单击导入。
- 输入路径或单击浏览以在管理员电脑中定位 CA 证书。
- 单击确定。

注意：在导入 CA 证书之前，需要先将它添加到管理员电脑。请见 第 20 页 “ 获取一个 CA 证书” 。

7 添加第一阶段配置。
进入 **VPN > IPSEC > 第一阶段**。
- 单击新建。
- 网关名：Branch_Office
- 远程网关：拨号用户
- 模式：进取
- 第一阶段提议：
  加密 1 3DES， 认证 1 SHA1
  加密 2 3DES， 认证 2 MD5
- DH 组： 5
- 密钥有效期：3600 （秒）
- 认证方式：RSA 签名
- 证书名称： Main_Cert
- 本地 ID：空
- 端点选项：接受任意端点 ID
- XAuth：禁用
- NAT 跨越：启用
- 保持激活频率：6 （秒）
- 端点失效检测：启用
- 短期空闲：10 （秒）
- 重试计数：3 （次）
- 重试间隔：5 （秒）
- 长期空闲：300 （秒）
- 单击确定

8 添加第二阶段配置。

进入 **VPN > IPSEC > 第二阶段。**

- 单击新建。
- 通道名称：Branch_Office_VPN
- 远程网关：Branch_Office
- P2 提议：
  1- 加密 3DES， 认证 SHA1
  2- 加密 3DES， 认证 MD5
- 启用重放检测：启用
- 启用向前保密：启用
- DH 组：5
- 密钥有效期：300 （秒）
- 自动密钥保持激活：启用
- 集中器：无
- 单击确定

9 添加源地址

- 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部**。
- 对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：内部。
- 单击新建。
- 地址名称：Main_Office
- IP 地址： 192.168.2.0
- 网络掩码：255.255.255.0
- 单击确定。

10 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：外部。

- 单击新建。
- 地址名称： Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

11 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部**。

- 单击新建。
- 源地址：Main_Office
- 目的地址： Branch_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Branch_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 生成本地证书。

```
execute vpn certificates local generate Main_Cert subject
user@branch.com org Branch_Office keysize 1024
```

2 下载本地证书。

```
execute vpn certificates local download Main_Cert Main_Cert
192.168.1.150
```

3 导入本地证书。 `execute vpn certificates local import Main_Cert 192.168.1.150`

4 导入 CA 证书。

```
execute vpn certificates ca import CA_Cert 192.168.1.150
```

5 添加第一阶段配置。

```
set vpn ipsec phase1 Branch_Office keylife 28800 type dynamic
proposal 3des-sha1 3des-md5 authmethod rsasig Main_Cert mode
aggressive dhgrp 5 nattraversal enable keepalive 6 dpd enable
dpdidleworry 10 dpdretrycount 3 dpdretryinterval 5
dpdidlecleanup 300
```

6 添加第二阶段配置。

```
set vpn ipsec phase2 Branch_Office_VPN phase1name Branch_Office
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 5
keylifeseconds 1800 keepalive enable
```

7 添加源地址。

```
set firewall address Internal Main_Office subnet 192.168.2.0
255.255.255.0
```

8 添加目的地址。

9 `set firewall address External Branch_Office subnet 192.168.1.0 255.255.255.0`

10 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Main_Office dstaddr Branch_Office schedule Always
service ANY action encrypt vpntunnel Branch_Office_VPN inbound
allow outbound allow
```

11 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

预置密钥 IPSec VPN

本章描述了如何使用预置密钥的自动 IKE 创建 IPSec VPN 通道。本章还包括了一些详细的例子。

本章叙述了如下内容

概述

在使用预置密钥时，VPN 会话双方都配置了一个预置的密钥。会话的双方并不真正将这个密钥传输给对方。相反，当会话的一方初始化一个 VPN 通道时，会进行一个分成两个阶段的 IKE。在第一阶段，IKE 使用预置密钥和 Diffie-Hellman 算法生成一个会话密钥。这个会话密钥可以用于会话双方彼此之间的认证和保护通讯通道的安全。一旦通讯通道建立起来了，IKE 在第二阶段协商一个 IPSec 安全组合。这个安全组合为 VPN 会话的双方建立一个公共的配置方案，用于加密它们之间传输的数据。在第二阶段，IKE 生成一个会话密钥。因为第二阶段比第一阶段持续时间长得多，IKE 定期重新生成第二阶段会话密钥。

和手工密钥相比，预置密钥的优势是网络管理员的管理更加容易一些。然而，一个预置密钥配置可能降低传输效率，特别是如果频繁生成第二阶段密钥的话。

开发一种安全的向远程客户端或者网关发布多个预置密钥已经被证明是非常困难的。这个问题的一个解决方案是使用数字证书。

主模式和进取模式的端点识别

在您实施自动 IKE 预置密钥之前，需要选择 VPN 端点在第一阶段使用主模式还是进取模式。您所选择的模式决定了会话的双方如何向对方证明自己的身份。

在主模式中，VPN 端点向对方证明自己的身份的方法是使用他们的外部 IP 地址。没有其他的识别方法。因为这个原因，主模式可以适用于所有使用静态 IP 地址的 VPN 端点的部署。Fortinet 实现了一个 IKE 的扩展，它允许在一个拨号的应用中使用主模式。请见 第 48 页 “ 主模式中的用户名和密码认证” 。

注意：一个拨号应用包括一个拨号服务器 （本地 FortiGate 设备）和一个或多个拨号用户 （远程客户端或者网关）。尽管拨号用户将它自己的 IP 发送给拨号服务器，但是拨号服务器并不将它用于识别过程。因为这个原因，一个典型的拨号用户，无论它使用的是动态分配的 IP 地址或者使用静态 IP 地址，都不被应用于识别过程 （例如一个发起一个 VPN 通道但不终止它的远程客户端 PC）。

在进取模式中，VPN 会话双方彼此交换识别信息。这就允许远程端点使用一个用户名进行识别和使用一个密码 （预置密钥）来认证。在进取模式中传输的额外的信息使得它可以适用于拨号应用中。为了减轻配置工作的负担，您可以对一组端点分配单一的一个用户名和密码。为了提高安全性，您可以为每个端点指定单独的一个用户名和密码。请见 第 49 页 “ 进取模式的用户名和密码认证” 。

主模式中的用户名和密码认证

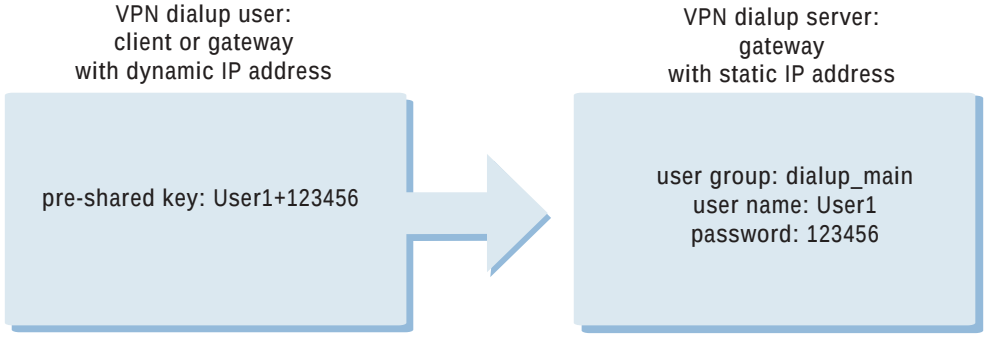
如果 VPN 会话双方都运行于主模式，识别信息仅限于 IP 地址。因此主模式在典型情况下之被拥有静态 IP 地址的 VPN 端点所使用。然而，Fortinet 已经实现了 IKE 的扩展，它允许主模式被拨号部属所使用。使用这一特性，一个拨号用户 （客户端或者网关）可以被配置一个用户名和密码来代替常规的预置密钥。（一个常规的密钥是一个可以包含任意字符的随机字符串，它的长度至少是 6 个字符）。要识别拨号用户，拨号服务器必须被配置一个匹配的用户名和密码。拨号服务器不需要预置密钥。

注意：这一特性依赖于一个 IKE 扩展，它只能被应用于 FortiGate 设备之间。在一个标准的 IKE 配置中，运行于主模式的拨号用户必须使用一个单一的，预置密钥作为他们的保密口令。

配置细节

- 在一个或者多个远程 VPN 端点 （拨号用户）上，管理员输入用户名 + 密码作为一个预置密钥，并且不输入本地 ID/ 主机域名。注意 “+” 符号是这个预置密钥的一部分，不能忽略。
- 在本地 VPN 端点 （拨号服务器）上，管理员输入一个匹配的用户名和密码并将它添加到一个用户组。管理员还为每个拨号用户添加一个单独的网关并为全部拨号用户添加一个通道。不需要预置密钥。

图 7: 主模式中的用户名和密码认证



例子：

管理员在拨号用户 （远程客户端或者网关）中添加一个预置密钥“User1+123456”。管理员在拨号服务器上创建一个新的用户，用户名是 User1，密码是 123456，然后将这个用户添加到一个用户组。管理员无须在这个拨号服务器上添加预置密钥。

当开始一个通讯会话时，拨号服务器将对这个拨号用户进行认证。如果用户名 User1 和密码 123456 能够匹配，就将建立一个加密通道。

注意：只有当远程 VPN 端点使用动态 IP 地址时才有必要使用这种方式增强安全性，当它使用静态 IP 地址的时候没必要。还要注意的是这种认证方法增加了处理时间。所以在大多数情况下，您应当在进取模式中实施用户名和密码认证，而不是主模式。

进取模式的用户名和密码认证

如果 VPN 会话的双方运行于进取模式，例如端点 ID 或者域名之类的识别信息将被提取出来作为认证过程的一部分。这就允许拨号用户使用一个用户名 （ID）和密码（预置密钥）向拨号服务器证明他们自己的身份。

在进取模式中您有两个选择：

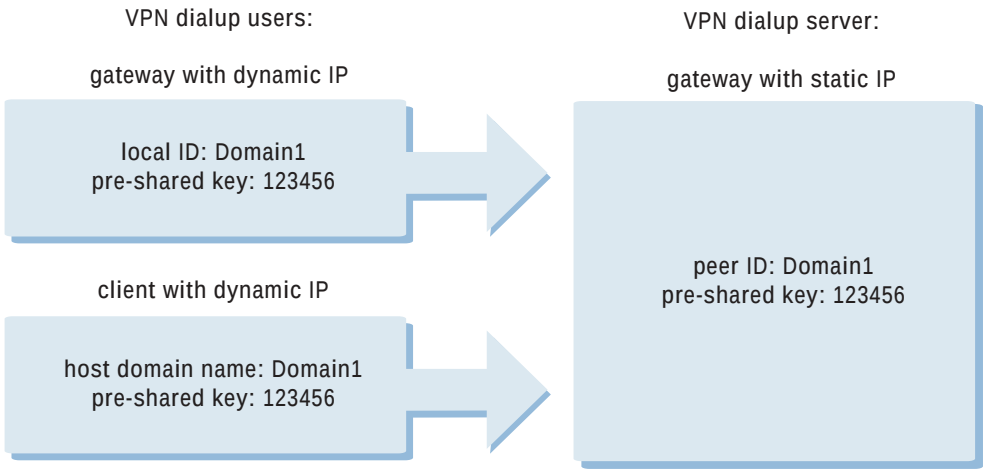
- 第一个选择是为一组 VPN 端点指定一个用户名和一个密码。
- 第二个选择是为独立的 VPN 端点分配单独的用户名和密码。

用户名的格式各不相同。在客户端 PC 中，可以输入一个电子邮件地址、主机域名或其他识别信息作为用户名 （Fortinet 远程 VPN 客户端使用主机域名）。对于 VPN 网关，通常在 ID 栏输入一个分类字符串作为用户名 （全部 FortiGate 设备都使用本地 ID）。

共享的用户名和密码配置细节

- 在一组远程 VPN 端点 （拨号用户）中，管理员添加一个共享的用户名和密码。对于客户端，典型的用户名输入在主机域名，对于网关，用户名在本地 ID 栏输入。无论是客户端还是网关，密码都是预置密钥。
- 在本地 VPN 端点 （拨号服务器），管理员为每一组远程 VPN 端点添加一个第一阶段配置。第一阶段配置有一个端点 ID 和一个预置密钥，它匹配于这个组的本地 ID 和预置密钥。

图 8: 进取模式中的共享用户名和密码



例子：

一个拨号用户组需要一个通道以连接到拨号服务器。这个组包括一个 VPN 网关和一个 VPN 客户端。在网关中，管理员指定了一个本地 ID “Domain1”和一个预置密钥“123456”。在客户端，管理员指定了一个主机名 “Domain1”和一个预置密钥“123456”。在 VPN 拨号服务器上，管理员添加了一个第一阶段配置，输入了一个端点 ID “Domain1”和一个预置密钥 “ 123456”。

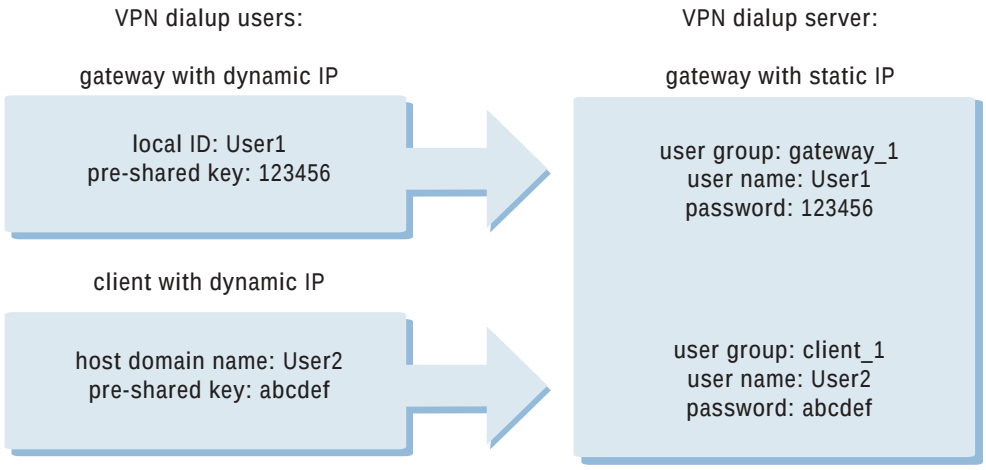
当位于这个网关后边的一台电脑试图连接到位于拨号服务器后边的一台电脑或者服务的时候，拨号服务器将认证这个网关。如果端点 ID “Domain1”和预置密钥“123456”能够匹配，将建立一个加密的 VPN 通道。

使用这种认证方法，VPN 端点共享单一的密码，或者一组预置密钥。如果密码泄露了，那么所有的端点都将受到威胁。为了增强安全性，可以为每个端点分配单独的一个用户名和密码，或者实施附加的安全机制，例如 XAuth。

独立用户名和密码配置细节

- 在每个远程 VPN 端点 （拨号用户），管理员添加一个独立的用户名和密码。对于客户端，典型的用户名输入在主机域名拦。对于网关，用户名在本地 ID 栏输入。无论是客户端还是网关，密码都是预置密钥。
- 在本地 VPN 端点 （拨号服务器），管理员为每个拨号用户输入一个用户名和密码，并将它添加到一个用户组。管理员还可以为每个拨号用户添加一个第一阶段配置。在拨号服务器上的第一阶段配置中不需要添加预置密钥。

图 9: 进取模式的独立用户名和密码认证



例子：

两个拨号用户需要通道来连接 VPN 拨号服务器。第一个用户是一个网关。第二个用户是一个客户端。在网关上，管理员添加一个本地 ID “User1”和一个预置密钥“123456”。在客户端，管理员添加了一个主机域名 “User2”和一个预置密钥“abcdef”。在拨号服务器上，管理员创建了两个新的用户分别匹配于两个拨号用户，并将他们添加到用户组。管理员不添加预置密钥。

当远程客户端试图连接到位于拨号服务器后边的一台计算机或者服务时，拨号服务器将认证这个客户端。如果用户名 “User2”和密码 abcdef 能够匹配，将建立一个加密的 VPN 通道。

扩展认证 (XAuth)

XAuth 是远程 VPN 端点向对方证明自己身份的另一种方法。XAuth 依赖于一种安全机制 （例如一个位于外部的 LDAP 或者 RADIUS 服务器）来提示 VPN 端点提供他们的用户名和密码。因为这个挑战发生在第一阶段和第二阶段之间，XAuth 既可以在主模式中使用，也可以在进取模式中使用。

一个 FortiGate 设备可以配置为一个 XAuth 服务器或者一个 XAuth 客户端。作为一个 XAuth 服务器，在一个远程 VPN 端点试图建立通道时 FortiGate 设备和一个安全机制联合起来对它发出挑战。作为一个 XAuth 客户端，FortiGate 设备被配置为使用它自己的用户名和密码在挑战时提供给远程 VPN 端点。

XAuth 在进取模式和主模式的工作方式是相等的。然而，比较典型的应用方式是将 XAuth 应用在 FortiGate 设备以认证使用一组预置密钥 （共享的密码）的拨号用户（客户端或者网关）。使用独立的预置密钥或者拥有静态 IP 地址的远程 VPN 端点不需要这种额外的安全性。

一般配置步骤

一个使用预置密钥的自动 IKE VPN 配置包括第一阶段的参数和第二阶段配置参数，通道两端的源地址和目的地址，以及一个用于控制对这个 VPN 通道的访问的加密策略。

按照如下步骤创建一个预置密钥 VPN 配置

1 添加第一阶段配置以定义认证远程 VPN 端点所用的参数。尽管远程 VPN 端点可以是一个客户端或者一个网关，这个步骤经常在“添加一个远程网关”中提到。
请见 第 52 页 “添加第一阶段配置”。

2 添加第二阶段配置以定义用于创建和维护自动密钥 VPN 通道的参数。这一步骤经常在“添加一个通道”中提到。
请见 第 57 页 “添加第二阶段配置”。

3 添加源地址。
请见 第 59 页 “添加一个源地址”。

4 添加目的地址。
请见 第 59 页 “添加目的地址”。

5 添加包括了这个通道、这个通道两端的源地址和目的地址的加密策略。
第 60 页 “添加一个加密策略”请见。

添加第一阶段配置

当您添加第一阶段配置的时候，您需要定义 FortiGate 设备和 VPN 远端 （网关或客户）用于彼此认证以建立 IPSec VPN 通道的有关条件。第一阶段的配置参数的构成包括远程 VPN 端点的名称，远程端点的地址类型 （静态 IP 地址或者拨号用户），建议用于认证过程的设置 （加密和认证算法），以及本地数字证书。为了能够成功地认证，远程 VPN 端点必须使用兼容的第一阶段建议设置来配置。

第一阶段配置和第二阶段配置彼此相关。在第一阶段中 VPN 的两端是经过认证的，在第二阶段则建立起了通道。您可以选择使用相同的第一阶段参数建立多个通道。换句话说，同一个远程 VPN 端点 （网关或客户）可以有多个连接到本地 VPN 端点 （FortiGate 设备）的多个通道。

当 FortiGate 设备收到一个 IPSec VPN 连接请求时，它首先根据第一阶段参数认证 VPN 端点。然后，它根据请求的源地址和目的地址发起一个 IPSec VPN 通道和应用加密策略。

当您添加完一个第一阶段配置之后，可以修改它的某些参数。然而，无论如何您也不能更新远程 VPN 端点的 IP 地址的类型 （静态或者拨号）。如果这个 VPN 端点的地址类型从静态变成了拨号地址，您必须删除原来的第一阶段设置然后添加一个新的，反之亦然。如果您只是简单地添加了第二个第一阶段配置来说明这种变化，这个通道将失效。发生这种情况是因为这个静态第一阶段配置比拨号第一阶段配置优先，从而覆盖了它。一般的规则是对每个远程 VPN 端点只添加一个第一阶段配置。

按照如下步骤添加一个第一阶段配置

1 进入 **VPN > IPSec > 第一阶段。**

2 单击新建以添加一个新的第一阶段配置。

3 输入远程 VPN 端点的网关名称。
远端 VPN 端点可以是另一个网络的网关或者互联网上的一个独立的客户。
这个名称可以含有数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符或者空格符。

4 选择远程网关地址类型。

- 如果远程 VPN 端点有静态 IP 地址，选择静态 IP 地址。
- 如果远程 VPN 端点使用动态 IP 地址 （DHCP 或 PPPoE），或者远程 VPN 端点有一个无须端点识别处理的静态地址，选择拨号用户。

根据您所选择的远程网关地址类型，可能还要填写其他栏目。

远程网关：静态 IP 地址

IP 地址	如果您选择了静态 IP 地址，将出现地址栏。输入连接到 FortiGate 设备的远程 IPSec VPN 网关或者客户的 IP 地址。这个内容是必须输入的。

远程网关：拨号用户

端点选项	如果您选择了拨号用户，在高级选项中将出现端点选项。可以使用端点选项在第一阶段协商中认证远程 VPN 的 ID。详细信息请见步骤 13。

5 选择进取模式或主模式 （ID 保护）。

两种模式都将建立一个安全通道。进取模式比主模式的步骤更少。当使用进取模式时，VPN 端点使用明文交换彼此的识别信息。当使用主模式时，识别信息是隐藏的。当一个 VPN 端点是一个拨号用户，将它的 ID 作为认证过程的一部分的时候，进取模式是标准的选择。

当使用进取模式时，有些配置参数，例如 Diffie-Hellman (DH) 组，不能协商。一般的规则是，当您使用进取模式时，您需要在 VPN 会话的双方输入匹配的配置。

VPN 双方必须使用同一模式。

6 配置 P1 提议。

最多可以为第一阶段的提议选择三个加密算法和认证算法。默认情况下选定了两个。如果要减少选择的组合的数量，单击减号。要增加选择的组合的数量，单击加号。VPN 会话的双方必须使用相同的 P1 提议设置。

加密算法

空	仅限测试。
DES	数据加密标准。
3DES	三倍 DES。
AES	高级加密标准，128、192 和 256 比特变量。

认证算法

空	仅限测试。
SHA1	安全 Hash 算法。
MD5	消息摘要算法。

7 选择 DH 组。

选择一个或多个 Diffie-Hellman 组用于 IPSec VPN 连接的第一阶段中的提议。您可以选择 DH 组 1、2 或 5。

遵守如下规则：

- 当 VPN 端点使用静态 IP 地址并使用进取模式时，选择一个单独匹配的 DH 组。
- 当 VPN 端点在一个拨号配置中使用进取模式时，最多可以为拨号服务器选择三个 DH 组，为拨号用户 （客户端或者网关）选择一个 DH 组。
- 当 VPN 端点使用主模式时，您可以选择多个 DH 组。

8 输入密钥有效期。

指定在第一阶段密钥的有效期。密钥有效期是在第一阶段加密密钥过期之前以秒为单位计算的时间。当密钥过期之后，无须中断服务就可以生成一个新的密钥。P1 提议中的密钥有效期可以从 120 秒到 172800 秒。

9 在认证方式中，选择预置密钥。

10 输入一个预置密钥。

这个密钥至少要包含 6 个可印刷字符，并且只能有网络管理员知道这个密钥。为了抵御字典攻击，一个好的预置密钥最少应当由 16 个从字母表中随机选择的字符组成。

VPN 会话双方必须使用相同的预置密钥。

11 （可选的）输入 FortiGate 设备的本地 ID。

只有当 FortiGate 设备作为客户端并使用它的本地 ID 对远程 VPN 端点认证它自己的时候才需要这个条目。如果 FortiGate 作为客户端但是不发送它的本地 ID，它将发送它的 IP 地址。

为了交换 ID，两个 VPN 端点必须都使用进取模式。

12 （可选的）选择高级选项。

端点选项， XAuth， NAT 跨越和对方失效检测都是可选的参数。

13 （可选的）选择一个端点选项。

使用端点选项可以根据远程 VPN 端点在第一阶段传输的 ID 进行认证。

接受任何端点 ID	选中则可接受任何端点 ID （因此不验证远程 VPN 端点的端点 ID）。
接受这个端点 ID	这个选项使用一个共享的用户名 （ID）和密码 （预置密钥）认证一个特定的 VPN 端点或者一组 VPN 端点。选择这个选项还要添加端点 ID。有关的详细信息请见 第 49 页 “ 共享的用户名和密码配置细节” 。
接收拨号组中的端点 ID	选择这个选项可以使用各自的用户名 （ID）和密码 （预置）密钥认证每个远程 VPN 端点。选择这个选项还需要选择一个拨号组 （用户组）。有关的详细信息请见 第 50 页 “ 独立用户名和密码配置细节” 。 在配置这个端点选项之前要先配置用户组。

14 （可选的）配置 XAuth。

XAuth （IKE 扩展认证）在用户级认证 VPN 端点。如果 FortiGate 设备 （本地 VPN 端点）被配置为 XAuth 服务器，它将使用一个用户组对远程 VPN 端点进行认证。这个用户组中包括的用户可以是配置在 FortiGate 设备中的，或者是位于远程的 LDAP 或者 RADIUS 服务器上。如果 FortiGate 设备被配置为 XAuth 客户端，当它被要求认证的时候它将提供一个用户名和密码。

XAuth: 作为客户端

名称	输入本地 VPN 端点用于对远程 VPN 端点证明它自己的用户名。
密码	输入本地 VPN 端点用于对远程 VPN 端点证明它自己的密码。

XAuth: 作为服务器

加密方式 选择 XAuth 客户端、FortiGate 设备和认证服务器之间的加密方法。

PAP 密码认证协议。

CHAP 挑战 - 握手认证协议。

混合 选择混合可以在 XAuth 客户端和 FortiGate 设备之间使用 PAP，在 FortiGate 设备和认证服务器之间使用 CHAP。

只要可能就能使用 CHAP。如果认证服务器不支持 CHAP 则使用 PAP。（所有的 LDAP 和部分微软 RADIUS 使用 PAP）。如果认证服务器支持 CHAP 但是 XAuth 客户端不支持 CHAP，就使用混合 （Fortinet 远程 VPN 客户端使用混合）。

用户组 选择 XAuth 认证的一组用户。这个用户组中的单独的一个用户可以由本地认证或者由一个或多个 LDAP 或 RADIUS 服务器认证。

在用户组被选中之前它必须被添加到 FortiGate 的配置中。

15 （可选的）配置 NAT 跨越。（NAT 跨越在默认情况下是启用的。）

启用 选择启用，如果您希望 IPSec VPN 的数据流通过一个执行 NAT 的网关。如果没有检测到 NAT 设备，启用 NAT 穿越功能不会有任何效果。在网关的两端必须使用相同的 NAT 穿越设置。

激活频率 如果启用了 NAT 穿越，则可以修改保持活动的时间间隔，以秒为单位。这个时间间隔指定了空 UDP 包发送的频率，这个 UDP 包穿过 NAT 设备，以保证 NAT 映象不会改变，直到第一阶段和第二阶段的密钥过期。保持活动的时间间隔可以从 0 一直到 900 秒。

16 （可选的）配置端点失效检测。（默认情况下 DPD 是启用的）。

使用这些设置可以监视 VPN 双方的连接状态。DPD 允许清除已经失效的连接并建立新的 VPN 通道。不是所有的销售商都支持 DPD。

启用 选择启用可以启用本地和远程端点之间的 DPD。

短时空闲 设置以秒为单位的时间。这是本地 VPN 端点需要考虑连接是否空闲之前所经历的时间。在这段时间之后，当本地端点要向远程 VPN 端点发送通讯时，它必须同时发送一个 DPD 探测，以判断连接的状态。要控制 FortiGate 设备用来使用 DPD 探测检测失效端点的时间的长度，配置重试累计和重试间隔。

重试累计 设置本地 VPN 端点认为通道已经失效并断开安全联结之前使用 DPD 探测的重复次数。根据您的网络的具体情况，将重试累计设置得足够高可以避免网络拥塞或其他传输问题带来的影响。

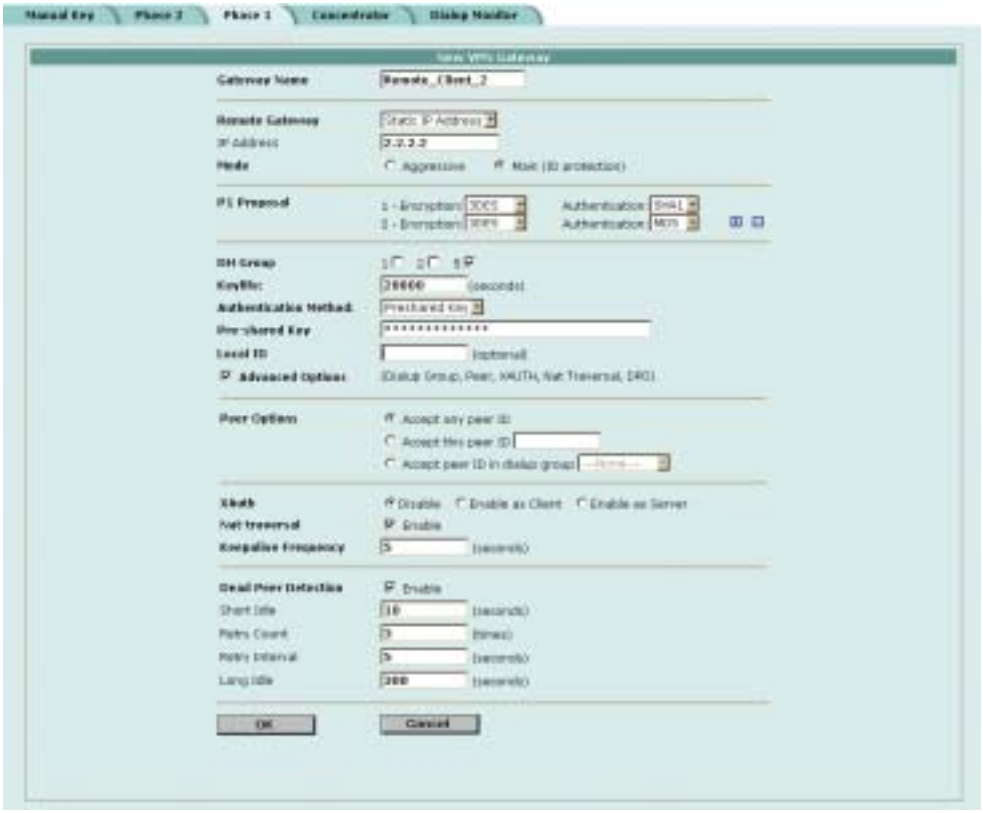
重试间隔 设置以秒为单位的时间，它是本地 VPN 端点设备在两次 DPD 探测之间等待的时间。

长时空闲 设置以秒为单位的时间。这是本地 VPN 端点在探测连接的状态之前需要等待的时间。如果在本地端点和远程端点之间没有通讯，在经历了这段时间之后本地端点将发送 DPD 探测以判断通道的状态。

注意： Fortinet 远程 VPN 客户端和 SSH 哨兵 VPN 客户端不支持 DPD。所以在使用这些客户端的时候不要配置 DPD。

17 单击确定以保存第一阶段参数。

图 10: 添加一个第一阶段配置



使用 CLI：

```
set vpn ipsec phase1 <名称_字符串>

keylife <密钥有效期_整数> type {static | dynamic} [gw <网关_ip>]

proposal {des-md5 des-sha1 3des-md5 3des-sha1 aes128-md5 aes128-sha1 aes192-md5 aes192-sha1 aes256-md5 aes256-sha1}

authmethod {psk <预置密钥_字符串> | rsasig <证书_字符串>}

mode {aggressive | main)

dhgrp {[1] [2] [5]}

nattraversal {enable | disable} keepalive <保持激活频率_整数>

dpd {enable | disable} [dpdidleworry <短期空闲_整数> dpdretrycount <重试_整数> dpdretryinterval <DPD 间隔_整数> dpdidlecleanup <长期空闲_整数>]

[localid <本地 ID_字符串>]

peertype {any | one | dialup} [usrgrp <用户组名_字符串>] [peerid <端点 ID_字符串>]
```

```
xauthtype {disable | client | server} [authusr <用户名_字符串>
<密码_字符串>] [authsrvtype {pap | chap} authusrgrp <用户组名称_字
符串 >]
```

添加第二阶段配置

添加第二阶段配置以指定在本地 VPN 端点 （FortiGate 设备）和远程 VPN 端点（VPN 网关或客户端）之间创建和维护 VPN 通道所用的参数。

按以下方法添加第二阶段配置：

1 进入 **VPN > IPSEC > 第二阶段。**

2 单击新建以添加新的第二阶段配置。

3 输入一个通道名称。

这个名称可以含有数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符或者空格符。

4 选择一个连接到这个 VPN 通道的远程网关。

远程网关可以是另一个网络中的网关或者互联网上的一个独立的客户。远程网关是作为第一阶段配置的一部分添加的。有关的详细信息请见 第 52 页 “ 添加第一阶段配置” 。

可以选择单独的拨号远程网关或者最多三个静态远程网关。如果您要配置 ISec 冗余，就需要多个静态远程网关。使用加号和减号可以增加或者减少连接到这个 VPN 通道的静态远程网关的数目。关于 IPSec 冗余的详细信息，请见 第 127 页 “ IPSec VPN 冗余” 。

5 配置 P2 提议。

可以为第二阶段的提议最多选择三个加密和认证算法组合。默认情况下选定了两个。要减少选定的组合的数量，单击减号。要增加选定的组合的数量，单击加号。加密方法可以在 DES、3DES 和 AES128、192 和 256 之间选择。认证方法可以在 SHA1 和 MD5 之间选择。“无”仅用于测试。VPN 会话的双方必须使用相同的 P2 提议设置。

6 （可选的）启用重放检测。

启用了重放检测时候，FortiGate 设备检查每个 IPSec 数据包的序列号，检查它是否已经被接收过了。如果数据包不在一个特定的序列范围内，FortiGate 设备将丢弃它们。这样提高了安全性。

FortiGate 设备还可以在检测到一个重放数据包的时候发送一个报警邮件。要接收这个报警邮件，进入**日志和报告 > 报警邮件 > 分类**，然后选择启用紧急防火墙 VPN 事件或异常的报警邮件。

注意：如果您已经为 P2 提议选择了无认证，则不用选择重放检测。请见步骤 5.

7 （可选的）启用向前保密 （PFS）。

PFS 在通道建立和每当超过密钥有效期的时候强制进行一个新的 Diffie-Hellman 交换。这保证了第二阶段的密钥于第一阶段创建的密钥或者在第二阶段创建的其他密钥无关。PFS 增加了安全性，代价是造成了少许的处理延迟。

8 选择 DH 组。

为第二阶段提议选择一个 Diffie-Hellman 组。您可以选择 DH 组 1、2 或 5。DS 组 1 的安全性最低。DH 组 5 的安全性最高。不要选择多个 DH 组。VPN 会话的双方必须使用相同的 DH 组设置。

9 输入密钥有效期。

指定在第二阶段密钥的有效期。密钥有效期限制第二阶段的密钥在一定时间内，或者给定数量的千字节的数据被 VPN 通道处理过之后过期，或者两者都有。如果您选择两者都是，则经过了指定的时间或者处理了指定量的数据这两种情况中的任何一种出现，密钥都会过期。当密钥过期之后，无须中断服务就可以生成一个新的密钥。P2 提议中的密钥有效期可以从 120 秒到 172800 秒或者从 5120 千字节到 99999 千字节。

10 （可选的）启用自动密钥保持激活。

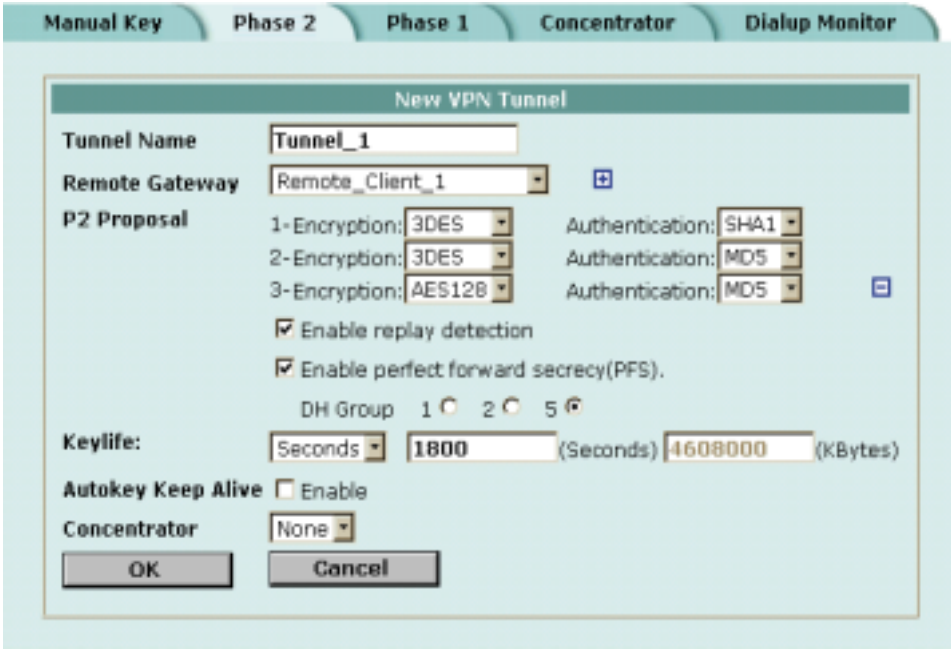
启用自动密钥保持激活可以在没有数据传输的时候也保持 VPN 通道的有效。

11 （可选的）选择一个集中器。

如果您希望通道成为星型 VPN 配置的一部分，选择集中器。如果您使用了这个操作，第 116 页 “ VPN 辐条一般配置步骤” 可以为集中器添加通道。下次您打开通道，集中器栏会显示您添加到通道的集中器的名字。

12 单击 **确定** 保存自动密钥 VPN 通道。

图 11: 添加一个第二阶段配置



使用 CLI：

```
set vpn ipsec phase2 <名称_字符串>
phase1name {[<名称_字符串> [<名称_字符串> [<名称_字符串>]]] | none}
```

```
proposal {null-null | null-md5 | null-sha1 | des-null | des-md5 | des-sha1 | 3des-null | 3des-md5 | 3des-sha1 | aes128-null | aes128-md5 | aes128-sha1 | aes192-null | aes192-md5 | aes192-sha1 | aes256-null | aes256-md5 | aes256-sha1}
keylifeseconds <密钥有效期（秒）_整数> keylifekbs <密钥有效期（千字节）_整数>
dhgrp {1 | 2 | 5}
replay [enable | disable}
pfs [enable | disable} keepalive {enable | disable}
concentrator {<名称_字符串> | none}
```

添加一个源地址

源地址位于本地 VPN 端点的内部网络中。它可以是单独的一个计算机地址或者一个网络的地址。

1. 进入**防火墙 > 地址**。
2. 选择一个内部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）
3. 单击新建添加一个地址。
4. 输入这个地址的名称，IP 地址和网络掩码，这些参数可以是位于本地 VPN 端点的内部接口上的一个计算机或者整个子网的。
5. 单击确定以保存源地址。

使用 CLI：

```
set firewall address <源接口_字符串> <名称_字符串> subnet <地址_ip> <网络掩码 _ip>
```

添加目的地址

目的地址可以是位于互联网上的一个 VPN 客户端的地址或者一个远程 VPN 网关后面的一个网络的地址。

1. 进入**防火墙 > 地址**。
2. 选择一个外部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）
3. 单击新建添加一个地址。
4. 输入地址的名称、IP 地址和网络掩码。这些参数可以是远程 VPN 端点的内部接口上的一台计算机或者整个子网的。
5. 单击确定一保存目的地址。

使用 CLI：

```
set firewall address <目的接口_字符串> <名称_字符串> subnet <地址_ip> <网络掩码 _ip>
```

添加一个加密策略

VPN 连接本地、内部网络和远程、外部网络。加密策略的重要任务是定义（和限制）这些网络中的哪些地址可以使用这个 VPN。

一个 VPN 只需要一个加密策略来控制向内和向外的连接。根据您对它所做的配置，加密策略控制您的内部网络中的用户能否建立到远程网络的连接（向外连接），和远程网络中的用户能否建立一个到您的内部网络的通道（向内连接）。这种灵活性使得单一的加密策略就能够完成两个常规的防火墙策略的工作。

尽管加密策略同时控制进入和发出的连接，它也必须被配置成为一个向外的的策略。一个向外的策略有一个位于内部网络中的源地址和一个位于外部网络中的目的地址。这个源地址可以识别内部网络中的哪些地址属于这个 VPN。目的地址可以识别远程网络中的哪些地址属于这个 VPN。标准的向外的策略包括内部到外部和 DMZ 到外部。

注意：目的地址可以是一个位于互联网上的 VPN 客户端地址或者位于一个远程 VPN 网关后边的网络的地址。

除了通过地址定义这个 VPN 的成员之外，您还可以配置这个加密策略的服务，例如 DNS、FTP、和 POP3，以及根据一个预定义的时间表（每天中的时间，或者一周、月、年中的某一天）来允许连接。您还可以配置加密策略的以下内容：

- 向内的 NAT 以转换进入的数据包的源地址。
- 向外的 NAT 以转换发出的数据包的源地址。
- 流量控制以控制这个 VPN 可用的带宽和这个 VPN 的优先级。
- 内容配置文件可以在这个 VPN 中应用防病毒保护、网页内容过滤、电子邮件过滤、文件传输和电子邮件服务。
- 记录日志使得 FortiGate 设备记录所有使用这个 VPN 的连接。

加密策略举例

如果您的内部网络中的用户希望连接到一个远程 VPN 网关后边的网络，或者如果来自远程网络的用户希望连接到您的内部网络中的资源，那么您就需要添加一个内部到外部的加密策略。这个策略的源地址必须是您的内部网络中的一个地址。这个策略的目的地址必须是远程 VPN 网关后边的网络中的地址。

这个策略必须包含您创建的用于同远程 VPN 网关通讯的 VPN 通道。同时作为添加到 VPN 通道的一部分，您必须指定它所允许的连接的方向。在这个例子中，您将同时允许向内和向外的连接。可选地，您还可以配置流量控制、病毒防护和网页过滤，以及记录日子后。

当您的内部网络中的用户试图连接到远程 VPN 网关后边的网络的时候，这个加密策略拦截这个连接企图并发起一个添加到这个策略的 VPN 通道。这个通道使用添加到它的配置中的远程网关来连接到远程 VPN 网关。当这个远程 VPN 网关接受到这个连接企图时，它检查它自己的策略、网关和通道配置。如果配置允许，这两个 VPN 端点将协商一个 IPSec VPN 通道。

多重交叉加密策略

在大多数情况下，您需要为子网之间的每个 VPN 添加一个加密策略。为相同的 VPN 添加多重策略可能导致冲突，如果这些策略共享相同的源、目的地址和服务设置。当策略在这种情况下互相重叠时，系统可能使用错误的加密策略或者通道可能失败。

有时候，无论如何您可能都需要对单一的 VPN 添加多个加密策略。例如，在某些情况下需要加密策略以配置到一个远程网关的冗余连接。同样，要控制对同一个子网内的不同服务的访问、或者根据不同的时间表控制对一个子网的访问也需要多个加密策略。

如果您添加的多重加密策略可能重叠，记住以下规则：

- 您可以为同时包含了进取模式和主模式规则的拨号配置添加重叠的通配符策略 （组预置密钥）。
- 您可以添加重叠的策略以控制到远程网关的冗余连接 （IPSec 冗余）。
- 您可以添加重叠的策略在同一子网之间应用不同的服务，但是这些策略必须使用相同的通道。
- 您可以添加重叠的策略在同一子网中应用不同的时间表设置，但是这些策略必须使用相同的通道。

开头的两个配置包括添加相等并有相同优先级的加密策略。因为他们是相等的，所以无论系统选择哪个都没关系。后边的两个配置添加了不相等的加密策略。因为他们处理通讯的方式不同，根据这个连接请求的性质，无论系统选择哪个加密策略都没关系。为了保证系统选择正确的策略，这些加密策略必须使用相同的通道。

如果实施的内容包括不相邻的两个子网之间的连接，也需要多重加密策略。例如，如果一个外部网络中的拨号用户请求连接到 FortiGate 设备后边的内部网络和 DMZ 网络，那么 FortiGate 设备必须为每个连接配置一个单独的加密策略。在这个配置中，不要试图在两个加密策略中使用一个通道。

按以下步骤添加加密策略：

1 进入**防火墙 > 策略。**

2 选择您要添加策略的那个策略列表 （不同型号的 FortiGate 设备的选择方法略有不同）。

3 单击 新建 以添加新的策略。

4 把 源地址 设为源地址。

5 把 目的地址 设置为目的地址。

6 设置服务以控制允许通过这个 VPN 连接的服务类型。
您可以选择任意以允许全部支持的服务通过这个 VPN 连接，或者选择一个特定的服务或服务组以限制允许通过这个 VPN 连接的服务。

7 将动作设置为加密。

8 配置加密参数。

VPN 通道	为这个加密策略选择一个自动密钥通道。
允许向内	选择 **允许向内** 可以允许向内连接的用户连接到源地址上。
允许向外	选择 **允许向外** 可以允许向外连接的用户连接到目的地址上。

向内 NAT FortiGate 可以把接收到的向内的数据包的源地址转换为连接到源地址网络上的 FortiGate 内部网络接口的 IP 地址。通常这是 FORTIGate 设备的一个内部接口。

向内 NAT 使得本地主机无法看到远程主机（在远程 VPN 网关后面的网络中的主机）的 IP 地址。

向外 NAT FortiGate 可以把向外发送的数据包的源地址转换为连接到目的地址网络上的 FortiGate 的网络接口的 IP 地址。通常情况下这是 FortiGate 设备的一个外部接口。

向外 NAT 使得远程主机无法看到本地主机 （位于本地 VPN 网关后边的网络中的主机）的 IP 地址。

如果实现了向外 NAT，它受到以下限制：

只能在通道的一端配置向外 NAT。

没有实现向外 NAT 的那一端需要有一个内部 -> 外部的策略以将另一端的外部接口指定为目的地 （这将是一个公共 IP 地址）。

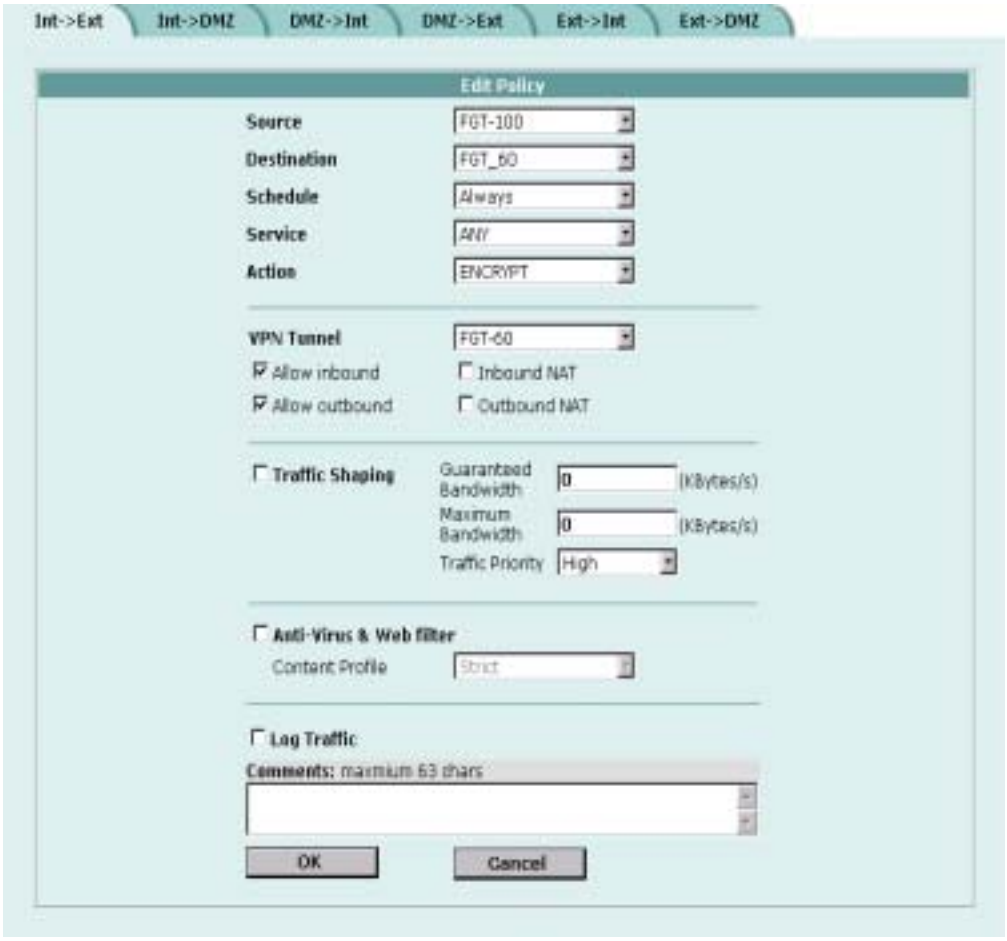
通道和通道中的通讯只能由配置了向外 NAT 的那一端初始化。

关于配置策略的其他设置的详细信息请见 *FortiGate 安装和配置指南*。

9 单击确定以保存加密策略。

10 排列加密策略在策略列表中的位置，使它在其他具有同样源和目的地址以及服务的策略之上，以确保加密策略能匹配 VPN 连接。

图 12: 添加一个加密策略



使用 CLI：

```
set firewall policy
```

```
src_intf <源接口_字符串> dstintf <目的接口_字符串> policyid <策略编号 _ 整数 > move < 从 - 策略 _ 整数 > to < 移动到 - 策略 _ 整数 >
```

```
status {enable | disable}
```

```
srcaddr <源地址名_字符串> dstaddr <目的地址名_字符串> schedule <时间表名称 _ 字符串 > service < 服务名称 _ 字符串 > action encrypt
```

```
vpntunnel < 通道名称 _ 字符串 > inbound {allow | deny} natinbound {enable | disable} outbound {allow | deny} natoutbound {enable | disable}
```

```
trafficshaping {enable | disable} gbandwidth < 保证带宽 _ 整数 > maxbandwidth < 最大带宽 _ 整数 > priority {high | medium | low}
```

```
avwebfilter {enable < 配置文件名 _ 字符串 > | disable}
```

```
logtraffic {enable | disable}
```

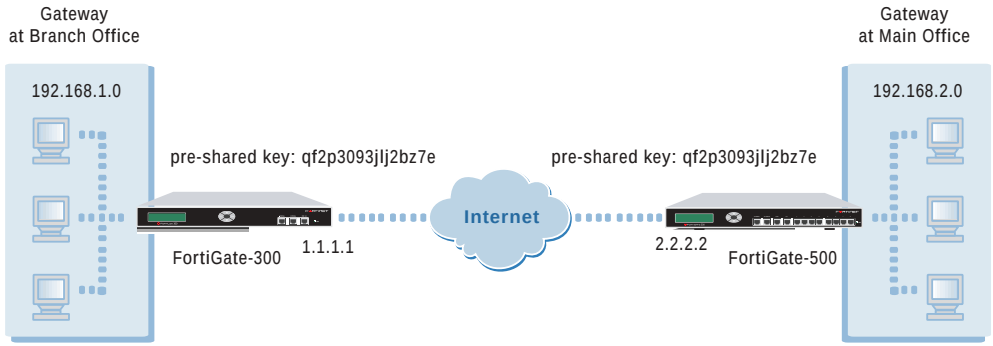
例子：使用预置密钥的静态 VPN 端点认证

在这个例子中，一个单独的 VPN 通道连接了两个 IPSec VPN 端点。它们都是网关而且都使用静态 IP 地址。他们使用预置密钥来向对方证明自己的身份并使用 DPD 监视通道的状态。会话的双方都运行与主模式。

网络拓扑结构

这个在分支机构中的网关是一个 FortGate 300 防火墙。在主办公室中的网关是一台 FortiGate 500。连接私有网络的通道位于这个网关的后面。

图 13: 使用预置密钥静态 IP 地址认证的 FortiGate 设备



一般配置步骤

要启用自动 IKE IPSec VPN 通道，您必须在两个 FortiGate 设备中输入相应的设置。远程网关（FortiGate300）位于一个分之机构的网络中。本地网关（FortiGate500）位于主办公网络。

分支机构网关配置

在位于分支机构的 FortiGate300 输入以下配置。

1. 添加第一阶段参数。第一阶段参数负责安排 VPN 对话双方在建立一个通道之前如何向对方证明自己的身份。输入主办公网关名称，选择静态 IP 地址，添加这个主办公机构 IP 地址，并且指定主模式。然后，选择 P1 提议的值。还要输入预置密钥和配置 DPD。
2. 添加第二阶段配置。第二阶段配置负责通道的维护。添加一个通道名称，然后选择您作为第一阶段的一部分添加的远程网关。然后指定会话双方使用的第二阶段提议的值。
3. 作为这个 VPN 的一部分，添加一个源地址以指定在分支机构的内部网络中的一个地址或者地址范围。
4. 作为这个 VPN 的一部分，添加一个目的地址以指定主办公机构的内部网络中的地址或地址范围。
5. 添加一个内部到外部的加密策略。这个策略为连接到分支办公机构的内部网络的通讯和从分支机构内部网络发出的通讯激活这个 VPN 通道。指定在步骤 3 和 4 中添加的源地址和目的地址。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

主办公机构配置

在位于主办公机构的 FortiGate500 中输入如下配置。

1 添加第一阶段参数。添加分支机构网关名称，选择静态 IP 地址，然后添加分支办公机构 IP 地址，指定主模式，然后选择 P1 提议的值。另外，输入预置密钥和配置 DPD。

2 添加第二阶段参数。添加一个通道名，然后选择您作为第一阶段参数的一部分添加的远程网关。另外还要指定会话双方所用的第二阶段提议的值。

3 作为这个 VPN 的一部分，添加一个源地址以指定在主办公机构的内部网络中的一个地址或者地址范围。

4 作为这个 VPN 的一部分，添加一个目的地址以指定分支办公机构的内部网络中的地址或地址范围。

5 添加一个内部到外部的加密策略。这个策略为连接到主办公机构的内部网络的通讯和从主机构内部网络发出的通讯激活这个 VPN 通道。指定在步骤 3 和 4 中添加的源地址和目的地址。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

配置参数

在主办公机构的拨号服务器和分支办公机构的拨号用户 （远程网关）中必须输入以下配置参数。

表 6：在主办公机构和分支办公机构网关上输入的第一阶段配置

域名	主办公机构值	分支办公机构值
网关名称	Branch_Office_gw	Main_Office_gw
远程网关	静态 IP 地址	静态 IP 地址
IP 地址	1.1.1.1	2.2.2.2

表 6：在主办公机构和分支办公机构网关上输入的第一阶段配置（续）

模式	主模式（ID 保护）	主模式（ID 保护）
P1 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
DH 组	5	5
密钥有效期	28800 秒	28800 秒
认证方式	预置密钥	预置密钥
预置密钥	qf2p3093jlj2bz7e	qf2p3093jlj2bz7e
本地 ID	空	空
端点选项	接受任意 ID	接受任意 ID
XAuth	禁用	禁用
NAT 跨越	启用	启用
保持激活频率	6	6
端点失效检测	启用	启用
短期空闲	10	10
重试计数	3	3
重试间隔	5	5
长期空闲	300	300

表 7：在主办公机构和分支办公机构网关上输入的第二阶段配置

域名	主办公机构值	分支办公机构值
通道名称	Branch_Office_VPN	Main_Office_VPN
远程网关	Branch_Office_gw	Main_Office_gw
P2 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
启用重放检测	启用	启用
启用向前保密（PFS）	启用	启用
DH 组	5	5
密钥有效期	1800 秒	1800 秒
自动密钥保持激活	启用	启用
集中器	不选中	不选中

表 8：在主办公机构和分支办公机构网关上输入的源地址和目的地址

域名	主办公机构值	分支办公机构值
源地址		
地址名	Main_Office	Branch_Office
IP 地址	192.168.2.0	192.168.1.0
网络掩码	255.255.255.0	255.255.255.0
目的地址		
地址名	Branch_Office	Main_Office
IP 地址	192.168.1.0	192.168.2.0
网络掩码	255.255.255.0	255.255.255.0

表 9：在主办公机构和分支办公机构网关上输入的加密策略

域名	主办公机构值	分支办公机构值
源地址	Main_Office	Branch_Office
目的地址	Branch_Office	Main_Office
任务计划	总是	总是
服务	任意	任意
动作	加密	加密
VPN 通道	Branch_VPN	Main_Office_VPN
允许向内	启用	启用
允许向外	启用	启用
向内 NAT	不启用	不启用
向外 NAT	不启用	不启用

配置分支机构网关

配置由五个步骤组成：

- 添加第一阶段配置
- 添加第二阶段配置
- 添加源地址
- 添加目的地址
- 添加内部到外部的加密策略

基于 Web 的管理程序的配置步骤

按照如下步骤添加第一阶段配置

1 进入 **VPN > IPSEC > 第一阶段**。

2 单击**新建**。

3 输入以下信息然后单击**确定**：

网关名称	Main_Office_gw
远程网关	静态 IP 地址
IP 地址	2.2.2.2
模式	主模式 （ID 保护）
P1 提议	1- 加密 3DES， 认证 SHA1 2- 加密 3DES， 认证 MD5
DH 组	5
密钥有效期	28800 （秒）
认证方式	预置密钥
预置密钥	qf2p3093jlj2bz7e
本地 ID	
端点选项	接受任意 ID
XAuth	禁用
NAT 跨越	启用
保持激活频率	6 （秒）
端点失效检测	启用
短期空闲	10 （秒）
重试计数	3 （次）
重试间隔	5 （秒）
长期空闲	300 （秒）

添加第二阶段配置

1 进入 **VPN > IPSEC > 第二阶段**。

2 单击新建。

3 输入以下信息然后单击确定：

通道名称：	Main_Office_VPN
远程网关：	Main_Office_gw
P2 提议	1- 加密 3DES， 认证 SHA1 2- 加密 3DES， 认证 MD5
启用重放检测	启用
启用向前保密	启用
H 组	5
密钥有效期	1800 （秒）
自动密钥保持激活	启用
集中器	无

添加源地址

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：内部。

2 单击新建。

3 输入以下信息然后单击确定：

地址名称	Branch_Office
IP 地址	192.168.1.0
网络掩码	255.255.255.0

添加目的地址

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：外部。

2 单击新建。

3 输入以下信息然后单击确定：

地址名称	Main_Office
IP 地址	192.168.2.0
网络掩码	255.255.255.0

添加加密策略

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部**。

2 单击新建。

3 输入以下信息然后单击确定：

源地址	Branch_Office
目的地址	Main_Office
任务计划	总是
服务	任意
动作	加密
VPN 通道	Main_Office_VPN
允许向内	启用
允许向外	启用
向内 NAT	不启用
向外 NAT	不启用
流量控制	根据需要配置这个策略的设置。
流量日志	如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
病毒防护和网页过滤	根据需要配置这个策略的设置。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加第一阶段配置。

```
set vpn ipsec phase1 Main_Office_gw keylife 28800 type static
gw 2.2.2.2 proposal 3des-sha1 3des-md5 authmethod psk
qf2p3093jlj2bz7e mode main dhgrp 5 nattraversal enable
keepalive 6 dpd enable dpdidleworry 10 dpdretrycount 3
dpdretryinterval 5 dpdidlecleanup 300
```

2 添加第二阶段配置。

```
set vpn ipsec phase2 Main_Office_VPN phase1name Main_Office_gw
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 5
keylifeseconds 1800 keepalive enable
```

3 添加源地址。

```
set firewall address Internal Branch_Office subnet 192.168.1.0
255.255.255.0
```

4 添加目的地址。

```
set firewall address External Main_Office subnet 192.168.2.0
255.255.255.0
```

5 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Branch_Office dstaddr Main_Office schedule Always
service ANY action encrypt vpntunnel Main_Office_VPN inbound
allow outbound allow
```

6 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

配置主办公机构网关

配置由五个步骤组成：

- 添加第一阶段配置
- 添加第二阶段配置
- 添加源地址
- 添加目的地址
- 添加内部到外部的加密策略

基于 Web 的管理程序配置步骤

添加第一阶段配置

1 进入 **VPN > IPSEC > 第一阶段**。

2 单击**新建**。

3 输入如下信息然后单击**确定**。

网关名称	Branch_Office_gw
远程网关	静态 IP 地址
IP 地址	1.1.1.1
模式	主模式 （ID 保护）
P1 提议	1- 加密 3DES， 认证 SHA1 2- 加密 3DES， 认证 MD5
DH 组	5
密钥有效期	28800 （秒）
认证方式	预置密钥
预置密钥	qf2p3093jlj2bz7e
本地 ID	
端点选项	接受任意 ID
XAuth	禁用
NAT 跨越	启用
保持激活频率	6 （秒）
端点失效检测	启用
短期空闲	10 （秒）
重试计数	3 （次）
重试间隔	5 （秒）
长期空闲	300 （秒）

添加第二阶段配置

1 进入 **VPN > IPSEC > 第二阶段**。

2 单击新建。

3 输入如下信息然后单击确定。

通道名称：	Branch_Office_VPN
远程网关：	Branch_Office_gw
P2 提议	1- 加密 3DES， 认证 SHA1 2- 加密 3DES， 认证 MD5
启用重放检测	启用
启用向前保密	启用
H 组	5
密钥有效期	1800 （秒）
自动密钥保持激活	启用
集中器	无

添加源地址

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：内部。

2 单击新建。

3 输入以下信息然后单击确定：

地址名称	Main_Office
IP 地址	192.168.2.0
网络掩码	255.255.255.0

添加目的地址

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：外部。

2 单击新建。

3 输入以下信息然后单击确定：

地址名称	Branch_Office
IP 地址	192.168.1.0
网络掩码	255.255.255.0

添加加密策略

1 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部**。
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部**。

2 单击新建。

3 输入以下信息然后单击确定：

源地址	Main_Office
目的地址	Branch_Office
任务计划	总是
服务	任意
动作	加密
VPN 通道	Branch_Office_VPN
允许向内	启用
允许向外	启用
向内 NAT	不启用
向外 NAT	不启用
流量控制	根据需要配置这个策略的设置。
流量日志	如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
病毒防护和网页过滤	根据需要配置这个策略的设置。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加第一阶段配置。

```
set vpn ipsec phase1 Branch_Office_gw keylife 28800 type static
gw 1.1.1.1 proposal 3des-sha1 3des-md5 authmethod psk
qf2p3093jlj2bz7e mode main dhgrp 5 nattraversal enable
keepalive 6 dpd enable dpdidleworry 10 dpdretrycount 3
dpdretryinterval 5 dpdidlecleanup 300
```

2 添加第二阶段配置。

```
set vpn ipsec phase2 Branch_Office_VPN phase1name
Branch_Office_gw proposal 3des-sha1 3des-md5 replay enable pfs
enable dhgrp 5 keylifeseconds 1800 keepalive enable
```

3 添加源地址。

```
set firewall address Internal Main_Office subnet 192.168.2.0
255.255.255.0
```

4 添加目的地址。

```
set firewall address External Branch_Office subnet 192.168.1.0
255.255.255.0
```

5 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Main_Office dstaddr Branch_Office schedule Always
service ANY action encrypt vpntunnel Branch_Office_VPN inbound
allow outbound allow
```

6 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

例子：使用单独密码的 VPN 端点 （客户端）认证

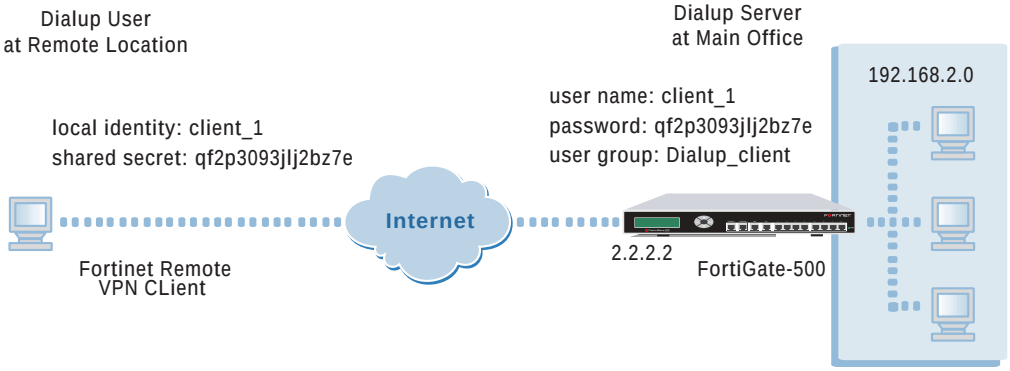
在这个例子中，一个单独的 VPN 通道连接了两个 IPSec VPN 端点。远程端点是一个客户端电脑，它使用一个公共的 IP 地址，是一个拨号用户。本地端点是一个使用静态 IP 地址的网关，它是一个拨号服务器。

除了标准的第一阶段和第二阶段设置 （加密和认证算法、密钥有效期等等），VPN 会话双方还可以配置为使用可选的设备级认证。在这一配置中，拨号用户使用单独的用户名和密码 （它的共享密钥）向拨号服务器证明它自己的身份。关于这种认证方案的概述，请见 第 50 页 “ 独立用户名和密码配置细节” 。端点运行在进取模式。

网络拓扑结构

位于远端的电脑运行 Fortinet 远程 VPN 客户端软件。在主办公机构的网关是一台 FortiGate500 设备。通道将远程电脑连接到位于主办公机构网络后边的私有网络中。

图 14: 使用单独密码的拨号 FortinetVPN 客户端认证



一般配置步骤

要启用自动 IKE IPSec VPN 通道，您必须在两个 FortiGate 设备中输入相应的设置。拨号用户 （一台运行 Fortinet 远程 VPN 客户端的电脑）位于远端。拨号服务器（一台 FortiGate500VPN 网关）位于主办公网络。

远程配置

在远端的 Fortinet 远程 VPN 客户端上输入如下配置。

1 添加一个拨号用户用于向拨号服务器证明它自己的身份的预置密钥 （共享保密）。

2 添加一个本地识别符 （用户名）。

3 在拨号用户和拨号服务器 （主办公机构网关）之间添加一个 VPN 连接。这包括添加一个拨号服务器的 IP 地址、以及添加拨号服务器后边的远程网络的名称和地址。

4 对这个 VPN 连接应用这个预置密钥 （共享保密）。

5 配置 IKE 和 IPSec 提议设置并选择进取模式。配置安全组合有效期。

主办公机构配置

在位于主办公机构的 FortiGate500 中输入如下配置。

1 添加一个用户。这个用户由用户名和密码组成，它们应当匹配于拨号用户的用户名和预置密钥。添加完用户之后，将它添加到一个用户组。当拨号用户试图建立一个通道时将使用这些信息认证。

2 添加第一阶段参数。为拨号用户添加一个网关名，选择拨号用户，指定进取模式。然后选择 P1 提议的值。还要在端点选项中选择一个拨号组。

3 添加第二阶段配置。添加一个通道名称，然后选择您作为第一阶段的一部分添加的远程网关。然后指定会话双方使用的第二阶段提议的值。

4 作为这个 VPN 的一部分，添加一个源地址以指定在主办公机构的内部网络中的一个地址或者地址范围。

5 添加一个内部到外部的加密策略，它包括了源地址，目的地址为外部 _ 全部，以及 VPN 通道。这个策略为目的地为主办公机构的内部网络的通讯启动这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

为 Fortinet VPN 客户端 （拨号用户）配置参数

以下配置参数必须输入到 Fortinet 远程 VPN 客户端 （拨号用户）。

表 10：在远程客户端输入的 VPN 连接

字段名	值
网关 IP 地址	2.2.2.2
远程网络	
网络名称	Main_Dialup_Server
IP 地址	192.168.2.0
子网掩码	255.255.255.0

表 11：在远程客户端输入的预置密钥

字段名	值
本地识别符	client_1
共享密码	qf2p3093jlj2bz7e

表 12：添加到远程客户端的 VPN 连接的预置密钥

字段名	值
远程终点	
远程网络	Main_Dialup_Server
IPSec / IKE 提议	
认证密钥	client_1
IKE 提议设置	
加密算法	3DES
完整性验证	SHA-1
IKE 模式	进取模式
IKE 组	MODP 1024 （组 2）
IPSec 提议设置	
加密算法	3DES
完整性验证	HMAC-SHA-1
PFS 组	MODP 1024 （组 2）
只将选定的值附加到提议	启用

表 13：在远程客户端输入的安全组合有效期

字段名	值
IKE 安全组合	
以分钟为单位的有效期	480
以兆字节为单位的有效期	0
IPSec 安全组合	
以分钟为单位的有效期	60
以兆字节为单位的有效期	400

配置 FortiGate500 的参数 （拨号服务器）

在位于主办公机构的 FortiGate500 中输入如下配置。

表 14：在主办公机构网关上输入的用户

字段名	参数值
用户名	client_1
密码	qf2p3093jlj2bz7e

表 15：在主办公机构网关上输入的用户组

字段名	参数值
组名	Dialup_Client
有效用户	client_1

表 16：在主办公机构网关上输入的第一阶段配置

字段名	参数值
网关名称	Remote_Client
远程网关	拨号用户
模式	进取
P1 提议	
1- 加密	3DES
2- 加密	3DES
1- 认证	SHA1
2- 认证	MD5
密钥有效期	28800 秒
DH 组	2
认证方式	预置密钥
预置密钥	空
本地 ID	空
端点选项	接受拨号组中的 ID: Dialup_Client
XAuth	禁用
NAT 跨越	启用
保持激活频率	6
端点失效检测	启用
短期空闲	10
重试计数	3
重试间隔	5
长期空闲	300

表 17：在主办公机构网关上输入的第二阶段配置

字段名	参数值
通道名称	Remote_Client_VPN
远程网关	Remote_Client
P2 提议	
加密 1	3DES
加密 2	3DES
认证 1	SHA1
认证 2	MD5
启用重放检测	启用
启用向前保密 （PFS）	启用
DH 组	2
密钥有效期	1800 秒
自动密钥保持激活	启用
集中器	不选中

表 18：在主办公机构网关上输入的源地址

字段名	参数值
源地址	
地址名	Main_Office
IP 地址	192.168.2.0
网络掩码	255.255.255.0

表 19：在主办公机构网关上输入的加密策略

字段名	参数值
源地址	Main_Office
目的地址	外部 _ 全部
任务计划	总是
服务	任意
动作	加密
VPN 通道	Remote_Client_VPN
允许向内	启用
允许向外	启用
向内 NAT	不启用
向外 NAT	不启用

配置分支机构客户端

配置由六个步骤组成：启动策略编辑器，添加一个预置密钥，添加 ID，创建一个新的 VPN 连接，将密钥应用到这个 VPN 策略，配置提议设置。完成了配置工作之后，您可以测试这个 VPN 连接并启动 VPN 连接。

注意：不要将 Fortinet 远程 VPN 客户端配置为请求一个虚拟 IP 地址，或者连接到远程私有网络中的 WINS 和 DNS 服务器。目前 FortiGate 设备不支持这些功能。

Fortinet 远程 VPN 客户端配置步骤

1 启动策略编辑器。

- 右键单击 SSH 图标并单击运行策略编辑器。

2 添加预置密钥。

- 进入 **密钥管理 > 我的密钥。**
- 单击添加。
- 在新认证密钥向导中，单击创建一个预置密钥。
- 单击下一步。

  名称： client_1

  共享密码： qf2p3093jlj2bz7e

  确认共享密码： qf2p3093jlj2bz7e
- 单击完成。
- 单击应用以保存预置密钥信息。

3 为本地主机添加一个识别符。

- 进入 **密钥管理 > 我的密钥。**
- 选择 client_1。
- 选择 属性。
- 进入**预置密钥 > 识别。**

  本地主识别符：主机域名

  主机域名： client_1
- 单击确定。
- 单击应用以保存本地主机的这个 ID。

4 创建一个新的 VPN 连接。

- 进入 **安全策略。**
- 选择 VPN 连接并单击添加。
- 配置这个 VPN 连接。

  网关名称：选择 IP。

  网关 IP 地址：2.2.2.2。
- 单击...以添加一个新的远程网络。
- 在网络编辑器中，选择新建并输入 Fortinet 远程 VPN 客户端要使用 VPN 连接到的 FortiGate-500 内部网络的信息。

  网络名称： Main_Dialup_Server

  IP 地址：192.168.2.0

  子网掩码： 255.255.255.0
- 单击确定两次。
- 单击应用以保存这个 VPN 连接的信息。

5 将预置密钥应用到这个 VPN 策略。

- 进入**安全策略。**
- 选择这个 VPN 连接： 2.2.2.2
- 单击属性。

  远程网络：Main_Dialup_Server

  认证密钥：client_1
- 单击确定。

6 配置提议设置。

- 进入**安全策略。**
- 选择这个 VPN 连接： 2.2.2.2
- 单击属性。
- 在 IPSec/IKE 提议中，单击设置。
- 选择 IKE 提议的参数。

  加密算法：3DES

  完整性验证：SHA-1

  IKE 模式：进取模式

  IKE 组：MODP 1024（组 2）
- 选择 IPSec 提议参数。

  加密算法：3DES

  完整性验证： HMAC-SHA-1

  PFS 组： MODP 1024（组 2）
- 单击只将选定的值附加到这个提议。
- 单击确定。
- 进入 **规则属性 > 高级。**
- 对于安全组合的有效期，单击设置。

  IKE 安全组合：以分钟为单位的有效期： 480， 以兆字节为单位的有效期： 0

  IPSec 安全组合： 以分钟为单位的有效期： 60， 以兆字节为单位的有效期：400
- 单击确定。
- （可选） 高级选项：单击在启动时打开。
- 单击确定两次。
- 单击应用以保存提议设置。

7 测试这个 VPN 连接。（在配置完 VPN 端点后进行这一步）

- 进入 **安全策略。**
- 选择 VPN 连接：2.2.2.2
- 单击协商。

  如果这个 VPN 连接是活动的，将显示一个协商窗口和一个确认信息。

8 启动拨号 VPN 连接。（在完成 VPN 端点配置后进行这一步）

- 右键单击 SSH 图标。
- 进入**选择 VPN** ，选择拨号 VPN 连接以启动：2.2.2.2（主 _ 拨号 _ 服务器）

配置主办公机构网关

配置由六个步骤组成：添加一个用户、添加一个用户组、添加第一阶段配置、添加第二阶段配置、添加源地址、添加内部到外部的加密策略。

基于 Web 的管理程序的配置步骤

1 添加用户。

进入 **用户 > 本地**。

- 单击新建。
- 用户名： client_1
- 密码： qf2p3093jlj2bz7e
- 单击确定。

2 添加用户组。

进入 **用户 > 用户组。**

- 单击新建。
- 组名称：Dialup_Client
- 可用用户： client_1
- 单击确定。

3 添加第一阶段配置。

进入 **VPN > IPSEC > 第一阶段。**

- 单击新建。
- 网关名： Remote_Client
- 远程网关：拨号用户
- 模式：进取
- 第一阶段提议：

  加密 1 3DES， 认证 1 SHA1

  加密 2 3DES， 认证 2 MD5
- DH 组： 2
- 密钥有效期： 28800 （秒）
- 认证方式：预置密钥
- 预置密钥：空
- 本地 ID：空
- 端点选项：接受拨号组中的端点 ID：Dialup_Client
- XAuth：禁用
- NAT 跨越：启用
- 保持激活频率：6 （秒）
- 端点失效检测：启用
- 短期空闲：10 （秒）
- 重试计数：3 （次）
- 重试间隔：5 （秒）
- 长期空闲：300 （秒）
- 单击确定

4 添加第二阶段配置。

进入 **VPN > IPSEC > 第二阶段。**

- 单击新建。
- 通道名称： Remote_Client_VPN
- 远程网关： Remote_Client
- P2 提议：
  1- 加密 3DES， 认证 SHA1
  2- 加密 3DES， 认证 MD5
- 启用重放检测：启用
- 启用向前保密：启用
- DH 组： 2
- 密钥有效期：1800 （秒）
- 自动密钥保持激活：启用
- 集中器：无
- 单击确定

5 添加源地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部。**

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：内部。

- 单击新建。
- 地址名称： Main_Office
- IP 地址： 192.168.2.0
- 网络掩码： 255.255.255.0
- 单击确定。

6 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部。**

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部。**

- 单击新建。
- 源地址： Main_Office
- 目的地址： External_All
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Remote_Client_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加用户。

```
set user local client_1 status enable type password
qf2p3093jlj2b27e
```

2 添加用户组。

```
set user group Dialup_Client member client_1
```

3 添加第一阶段配置。

```
set vpn ipsec phase1 Remote_Client keylife 28800 type dynamic
proposal 3des-sha1 3des-md5 authmethod psk qf2p3093jlj2b27e
mode aggressive dhgrp 2 nattraversal enable keepalive 6 dpd
enable dpdidleworry 10 dpdretrycount 3 dpdretryinterval 5
dpdidlecleanup 300 peertype dialup usrgrp Dialup_Client
```

4 添加第二阶段配置。

```
set vpn ipsec phase2 Remote_Client_VPN phase1name Remote_Client
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 2
keylifeseconds 1800 keepalive enable
```

5 添加源地址。

```
set firewall address Internal Main_Office subnet 192.168.2.0
255.255.255.0
```

6 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Main_Office dstaddr External_All schedule Always
service ANY action encrypt vpntunnel Remote_Client_VPN inbound
allow outbound allow
```

7 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

例子：使用单独密码的动态 VPN 端点 （网关）认证

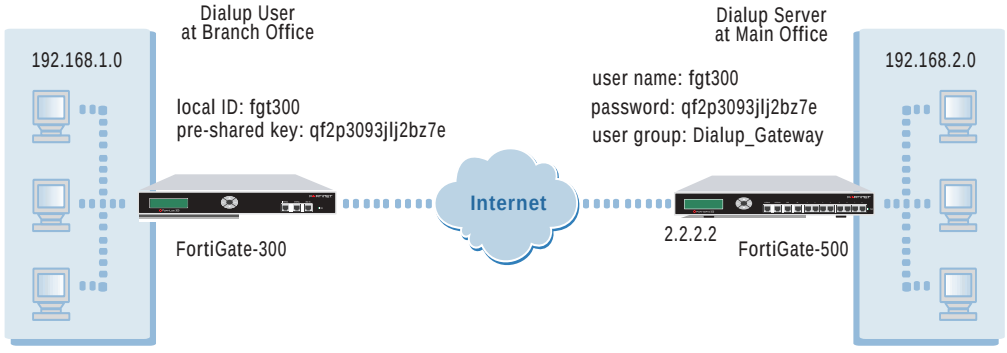
在这个例子中，一个单独的 VPN 通道连接了两个 IPSec VPN 端点。它们都是网关而且都是 FortiGate 防火墙设备。远程 VPN 端点使用一个动态 IP 地址，它是一个拨号用户。本地 VPN 端点使用一个静态 IP 地址，它是一个拨号服务器。

除了标准的第一阶段和第二阶段设置 （加密和认证算法、密钥有效期等等），VPN 会话双方还可以配置为使用可选的设备级认证。在这一配置中，拨号用户使用单独的用户名和密码 （它的共享密钥）向拨号服务器证明它自己的身份。关于这种认证方案的概述，请见 第 50 页 “ 独立用户名和密码配置细节” 。端点运行在进取模式。

网络拓扑结构

这个在分支机构中的网关是一个 FortGate 300 防火墙。在主办公室中的网关是一台 FortiGate 500。连接私有网络的通道位于这个网关的后面。

图 15: 使用独立用户名和密码的拨号 FortiGate300 认证



一般配置步骤

要启用两个使用预置密钥和设备级认证的网关之间的自动 IKE IPSec VPN 通道，您必须在两个 FortiGate 设备上输入相应的设置。FortiGate500 位于主办公网络。作为拨号服务器，它被当作本地设备。FortiGate300 位于一个分之机构的网络中。作为拨号用户，它被看作远程设备。

分支机构网关配置

在位于分支机构的 FortiGate300 输入以下配置。

1 添加第一阶段参数。第一阶段参数负责安排 VPN 对话双方在建立一个通道之前如何向对方证明自己的身份。为拨号服务器输入网关名称，选择静态 IP 地址，添加这个主办公机构 IP 地址，并且指定进取模式并选择 P1 提议的值。然后，输入拨号用户用于向拨号服务器证明它自己的身份的的本地 ID 和预置密钥。

2 添加第二阶段配置。第二阶段配置负责通道的维护。添加一个通道名称，然后选择您作为第一阶段的一部分添加的远程网关。然后指定会话双方使用的第二阶段提议的值。

3 作为这个 VPN 的一部分，添加一个源地址以指定在分支机构的内部网络中的一个地址或者地址范围。

4 作为这个 VPN 的一部分，添加一个目的地址以指定主办公机构的内部网络中的地址或地址范围。

5 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到主办公机构的内部网络的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

主办公机构配置

在位于主办公机构的 FortiGate500 中输入如下配置。

1 添加一个用户。这个用户由用户名和密码组成，它们应当匹配于拨号用户的本地 ID 和预置密钥。添加完用户之后，将它添加到一个用户组。当拨号用户试图建立一个通道时将使用这些信息认证。

2 添加第一阶段参数。为拨号用户添加一个网关名，选择拨号用户，指定进取模式。然后选择 P1 提议的值。还要在端点选项中选择一个拨号组。

3 添加第二阶段配置。添加一个通道名称，然后选择您作为第一阶段的一部分添加的远程网关。然后指定会话双方使用的第二阶段提议的值。

4 作为这个 VPN 的一部分，添加一个源地址以指定在主办公机构的内部网络中的一个地址或者地址范围。

5 作为这个 VPN 的一部分，添加一个目的地址以指定分支办公机构的内部网络中的地址或地址范围。

6 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到主办公机构的内部网络的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

配置参数

在主办公机构的拨号服务器和分支办公机构的拨号用户 （远程网关）中必须输入以下配置参数。

表 20：在主办公机构网关上输入的用户

字段名	参数值
用户名	fgt300
密码	qf2p3093jlj2b27e

表 21：在主办公网关上输入的用户组

字段名	参数值
组名	Dialup_Gateway
有效用户	fgt300

表 22：在拨号服务器和拨号用户 （远程网关）上输入的第一阶段配置

域名	主办公机构值	分支办公机构值
网关名称	Branch_Office	Main_Office
远程网关	拨号用户	静态 IP 地址
IP 地址		2.2.2.2
模式	进取模式	进取模式
P1 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
DH 组	5	5
密钥有效期	28800 秒	28800 秒
认证方式	预置密钥	预置密钥
预置密钥	空	qf2p3093jlj2b27e
本地 ID	空	fgt300
端点选项	接受拨号组中的端点 ID：Dialup_Gateway	接受任意端点 ID。
XAuth	禁用	禁用
NAT 跨越	启用	启用
保持激活频率	6	6
端点失效检测	启用	启用
短期空闲	10	10
重试计数	3	3
重试间隔	5	5
长期空闲	300	300

表 23：在拨号服务器和拨号用户 （远程网关）上输入的第二阶段配置

域名	主办公机构值	分支办公机构值
通道名称	Branch_Office_VPN	Main_Office_VPN
远程网关	Branch_Office	Main_Office
P2 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
启用重放检测	启用	启用
启用向前保密 （PFS）	启用	启用
DH 组	5	5
密钥有效期	1800 秒	1800 秒
自动密钥保持激活	启用	启用
集中器	无	无

表 24：主办公机构和分支办公机构网关的源地址和目的地址

域名	主办公机构值	分支办公机构值
源地址		
地址名	Main_Office	Branch_Office
IP 地址	192.168.2.0	192.168.1.0
网络掩码	255.255.255.0	255.255.255.0
目的地址		
地址名	Branch_Office	Main_Office
IP 地址	192.168.1.0	192.168.2.0
网络掩码	255.255.255.0	255.255.255.0

表 25：主办公机构和分支办公机构网关的加密策略

域名	主办公机构值	分支办公机构值
源地址	Main_Office	Branch_Office
目的地址	Branch_Office	Main_Office
任务计划	总是	总是
服务	任意	任意
动作	加密	加密
VPN 通道	Branch_VPN	Main_Office_VPN
允许向内	启用	启用
允许向外	启用	启用
向内 NAT	不启用	不启用
向外 NAT	不启用	不启用

配置分支机构网关

配置由五个步骤组成：添加第一阶段配置，添加第二阶段配置，添加源地址，添加目的地址，添加内部到外部的加密策略。

基于 Web 的管理程序的配置步骤

1 添加第一阶段配置。

进入 **VPN > IPSEC > 第一阶段。**

- 单击新建。
- 网关名：Main_Office
- 远程网关：静态 IP 地址
- IP 地址 2.2.2.2
- 模式：进取
- 第一阶段提议：

  加密 1 3DES， 认证 1 SHA1

  加密 2 3DES， 认证 2 MD5
- DH 组： 5
- 密钥有效期：28800 （秒）
- 认证方式：预置密钥
- 预置密钥： qf2p3093jlj2b27e
- 本地 ID： fgt300
- 端点选项：接受任意端点 ID
- XAuth：禁用
- NAT 跨越：启用
- 保持激活频率：6 （秒）
- 端点失效检测：启用
- 短期空闲：10 （秒）
- 重试计数：3 （次）
- 重试间隔：5 （秒）
- 长期空闲：300 （秒）
- 单击确定

2 添加第二阶段配置。

进入 **VPN > IPSEC > 第二阶段。**

- 单击新建。
- 通道名称：Main_Office_VPN
- 远程网关： Main_Office
- P2 提议：

  1- 加密 3DES， 认证 SHA1

  2- 加密 3DES， 认证 MD5
- 启用重放检测：启用
- 启用向前保密：启用
- DH 组：5
- 密钥有效期：1800 （秒）
- 自动密钥保持激活：启用
- 集中器：无
- 单击确定

3 添加源地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：内部。

- 单击新建。
- 地址名称：Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

4 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：外部。

- 单击新建。
- 地址名称： Main_Office
- IP 地址：192.168.2.0
- 网络掩码：255.255.255.0
- 单击确定。

5 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部。**

- 单击新建。
- 源地址：Branch_Office
- 目的地址：Main_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Main_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加第一阶段配置。

```
set vpn ipsec phase1 Main_Office keylife 28800 type static gw
2.2.2.2 proposal 3des-sha1 3des-md5 authmethod psk
qf2p3093jlj2b27e mode aggressive dhgrp 5 nattraversal enable
keepalive 6 dpd enable dpdidleworry 10 dpdretrycount 3
dpdretryinterval 5 dpdidlecleanup 300 localid fgt300
```

2 添加第二阶段配置。

```
set vpn ipsec phase2 Main_Office_VPN phase1name Main_Office
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 5
keylifeseconds 1800 keepalive enable
```

3 添加源地址。

```
set firewall address Internal Branch_Office subnet 192.168.1.0
255.255.255.0
```

4 添加目的地址。

```
set firewall address External Main_Office subnet 192.168.2.0
255.255.255.0
```

5 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Branch_Office dstaddr Main_Office schedule Always
service ANY action encrypt vpntunnel Main_Office_VPN inbound
allow outbound allow
```

6 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

配置主办公机构网关

配置由七个步骤组成：添加一个用户、添加一个用户组、添加第一阶段配置、添加第二阶段配置、添加源地址、添加目的地址、添加内部到外部的加密策略。

基于 Web 的管理程序的配置步骤

1 添加用户。

进入 **用户 > 本地**。

- 单击新建。
- 用户名： fgt300
- 密码：qf2p3093jlj2b27e
- 单击确定。

2 添加用户组。

进入 **用户 > 用户组。**

- 单击新建。
- 组名称：Dialup_Gateway
- 可用用户： fgt300
- 单击确定。

3 添加第一阶段配置。

进入 **VPN > IPSEC > 第一阶段。**

- 单击新建。
- 网关名：Branch_Office
- 远程网关：拨号用户
- 模式：进取
- 第一阶段提议：

  加密 1 3DES， 认证 1 SHA1

  加密 2 3DES， 认证 2 MD5
- DH 组： 5
- 密钥有效期： 28800 （秒）
- 认证方式：预置密钥
- 预置密钥：空
- 本地 ID：空
- 端点选项：接受拨号组中的端点 ID： Dialup_Gateway
- XAuth：禁用
- NAT 跨越：启用
- 保持激活频率：6 （秒）
- 端点失效检测：启用
- 短期空闲：10 （秒）
- 重试计数：3 （次）
- 重试间隔：5 （秒）
- 长期空闲：300 （秒）
- 单击确定

4 添加第二阶段配置。

进入 **VPN > IPSEC > 第二阶段。**

- 单击新建。
- 通道名称： Branch_Office_VPN
- 远程网关：Branch_Office
- P2 提议：

  1- 加密 3DES， 认证 SHA1

  2- 加密 3DES， 认证 MD5
- 启用重放检测：启用
- 启用向前保密：启用
- DH 组： 5
- 密钥有效期：1800 （秒）
- 自动密钥保持激活：启用
- 集中器：无
- 单击确定

5 添加源地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：内部。

- 单击新建。
- 地址名称： Main_Office
- IP 地址： 192.168.2.0
- 网络掩码： 255.255.255.0
- 单击确定。

6 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址，**然后选择接口：外部。

- 单击新建。
- 地址名称： Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

7 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部。**
对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部。**

- 单击新建。
- 源地址：Main_Office
- 目的地址： Branch_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Branch_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加用户。

```
set user local fgt300 status enable type password
qf2p3093jlj2b27e
```

2 添加用户组。

```
set user group Dialup_Gateway member fgt300
```

3 添加第一阶段配置。

```
set vpn ipsec phase1 Branch_Office keylife 28800 type dynamic
proposal 3des-sha1 3des-md5 authmethod psk qf2p3093jlj2b27e
mode aggressive dhgrp 5 nattraversal enable keepalive 6 dpd
enable dpdidleworry 10 dpdretrycount 3 dpdretryinterval 5
dpdidlecleanup 300 peertype dialup usrgrp Dialup_Gateway
```

4 添加第二阶段配置。

```
set vpn ipsec phase2 Branch_Office_VPN phase1name Branch_Office
proposal 3des-sha1 3des-md5 replay enable pfs enable dhgrp 5
keylifeseconds 1800 keepalive enable
```

5 添加源地址。

```
set firewall address Internal Main_Office subnet 192.168.2.0
255.255.255.0
```

6 添加目的地址。

```
set firewall address External Branch_Office subnet 192.168.1.0
255.255.255.0
```

7 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Main_Office dstaddr Branch_Office schedule Always
service ANY action encrypt vpntunnel Branch_Office_VPN inbound
allow outbound allow
```

8 移动加密策略。

```
   set firewall policy srcintf internal dstintf external move 2
to 1
```

手工密钥的 IPSec VPN

本章提供了一个关于手工密钥加密系统的概述。它还描述了如何在 FortiGate 设备上设置使用手工密钥的 IPSec VPN。本章包括了一个关于手工密钥 VPN 通道的详细的例子。

本章叙述了如下内容：

概述

使用手工密钥时，必须在通道的两端输入补充的安全参数。除了加密和认证用的算法和密钥之外，还需要输入安全参数索引（SPI）。SPI 是一个任意值，它定义了双方之间的通讯的结构。在其他的方式中 SPI 是自动生成的，但是在手工密钥配置中它必须作为 VPN 设置的一部分事先输入。

本地和远端的加密和认证密钥必须匹配；并且彼此的 SPI 值也必须互为镜像。当您输入了这些值之后，无须再协商认证和加密算法即可发起 VPN 通道。只要您正确、完整地输入了所有的值，双方之间即可建立通道。实质上通道一直存在于双方之间。结果是当被一个策略所匹配的通讯请求通道时，它可以立刻被认证和加密。

手工密钥配置方式受到一些特定的限制。因为它使用的是手工交换的安全信息，所以它的规模和劳动强度紧密相连，而且具有潜在的不安全性，比较容易受到重放攻击。除此之外，它只能应用于本地和远程的两个端点都使用静态 IP 地址（使用静态 IP 地址的 IPSec VPN）的 IPSec VPN 中。由于这些原因，手工密钥方式的部署仅限于小规模的应用和测试目的的应用中。

一般配置步骤

一个手工密钥 VPN 配置包括一个手工密钥 VPN 通道、通道两端的源地址和目的地址、以及一个用于控制对这个 VPN 通道的访问的加密策略。

按照如下步骤创建一个手工密钥 VPN 配置

1 添加一个手工密钥 VPN 通道。
请见 第 98 页 “ 添加一个手工密钥 VPN 通道” 。

2 添加一个源地址。
请见 第 100 页 “ 添加一个源地址” 。

3 添加一个目的地址。
请见 第 100 页 “ 添加目的地址” 。

4 添加一个包含了这个通道、通道两端的源地址和目的地址的加密策略。
请见 第 101 页 “ 添加一个加密策略” 。

添加一个手工密钥 VPN 通道

配置一个手工密钥的通道可以在 FortiGate 设备和远程 IPSev VPN 客户端或者网关之间创建使用手工密钥的 IPSec VPN 通道。一个手工密钥 VPN 通道的组成包括这个通道本身、通道另一端的 VPN 网关或者客户端的 IP 地址、加密和认证算法的选择、以及十六进制格式的密钥。因为密钥是在您配置这个通道的时候创建的，所以发起这个 VPN 通道时无须协商。然而，连接到这个 VPN 通道的 VPN 网关或者客户端必须使用相同的加密算法和认证算法并拥有相同的加密和认证密钥。

按照如下步骤添加一个手工密钥 VPN 通道

1 进入 **VPN > IPSec > 手工密钥。**

2 单击新建以添加一个新的手工密钥 VPN 通道。

3 输入一个 VPN 通道名。
这个名称可以含有数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符或者空格符。

4 输入本地 SPI。
本地安全参数索引是一个不多于八位的十六进制数 （数字 （0-9）和 / 或 字母 （a-f））。这个十六进制数必须添加到通道另一端的远程 SPI 中。本地 SPI 的取值范围是 bb8 到 FFFFFFF。

5 输入远程安全参数索引。
远程安全不多于八位的一个十六进制数。这个十六进制数必须添加到通道另一端的本地 SPI 中。远程 SPI 的取值范围是 bb8 到 FFFFFFF。

6 输入远程网关。
这是通道另一端的 FortiGate 或者 IPSec 网关的外部 IP 地址。

7 从列表中选择一个算法。
确定在通道的两端选择了相同的算法。

8 输入加密密钥。
每两个字符的组合表示十六进制格式中的一个字节。根据您所指定的加密算法，您可能需要输入十六进制的加密密钥的多个部分。在通道的两端需要使用相同的加密密钥。

DES	输入一个由 16 个字符 (8 字节) 的十六进制数 (0-9， A-F)。
3DES	输入一个 48 个字符 (24 字节) 的十六进制数 (0-9， A-F)。将这个数分成三个 16 个字符的部分。

AES128	输入一个 32 个字符（16 字节）的十六进制数（0-9，A-F）。将这个数分成两个 16 个字符的部分。
AES192	输入一个 48 个字符（24 字节）的十六进制数（0-9，A-F）。将这个数分成三个 16 个字符的部分。
AES256	输入一个 64 个字符（32 字节）的十六进制数（0-9，A-F）。将这个数分成四个 16 个字符的部分。

9 从列表中选择一个认证算法。

在通道的两端需要使用相同的认证算法。

10 输入认证密钥。

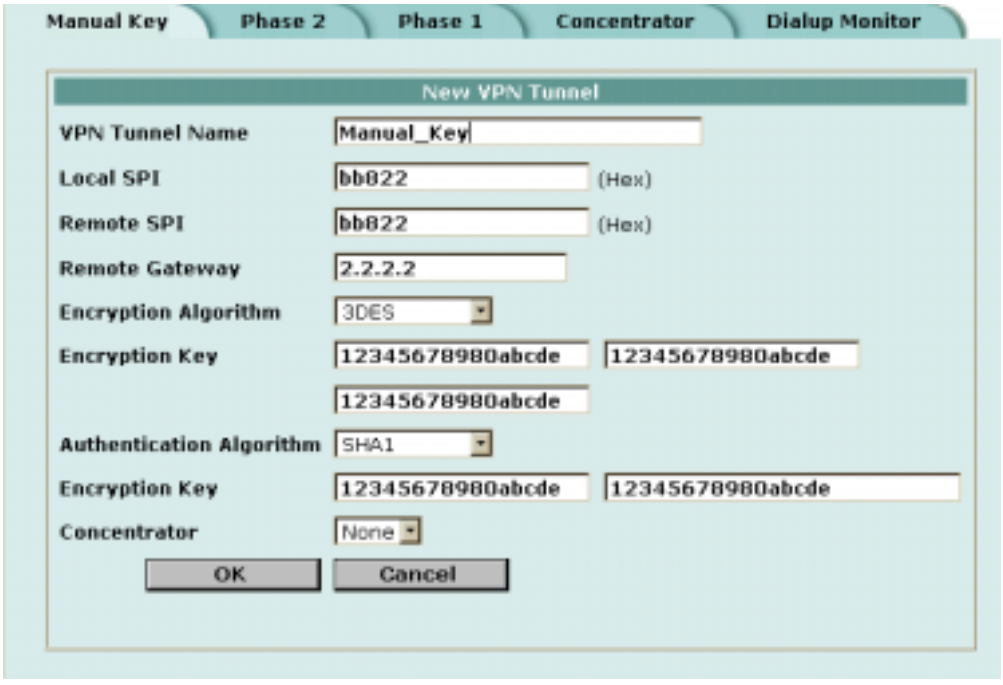
每两个字符的组合表示十六进制格式中的一个字节。在通道的两端需要使用相同的认证密钥。

MD5	输入一个 32 个字符（16 字节）的十六进制数（0-9，A-F）。将这个数分成两个 16 个字符的部分。
SHA1	输入一个 40 个字符（20 字节）的十六进制数（0-9，A-F）。将这个数分成一个 16 个字符的部分和一个 24 个字符的部分。

11 如果您希望通道成为星型 VPN 配置的一部分，就选择集中器选项。见 第 113 页 “IPSec VPN 集中器” 。

12 单击 **确定** 保存手工密钥 VPN 通道。

图 16: 添加一个手工密钥 VPN 通道



使用 CLI：

```
set vpn ipsec manualkey <通道名_字符串>
localspi <本地-spi_十六进制>
remotespi <远程-spi_十六进制>
```

```
gateway <网关_ip>
encalg {null | des | 3des | aes128 | aes192 | aes256}
enckey <加密密钥_十六进制 hex>
authalg {null | md5 | sha1}
authkey <认证密钥_十六进制>
concentrator {<名称_字符串> | none}
```

添加一个源地址

源地址位于本地 VPN 端点所在的内部网络中。它可以是单独一台计算机的地址或者一个网络的地址。

1 进入 **防火墙 > 地址。**

2 选择一个内部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）

3 单击新建添加一个地址。

4 输入这个地址的名称，IP 地址和网络掩码，这些参数可以是位于本地 VPN 端点的内部接口上的一个计算机或者整个子网的。

5 单击确定以保存源地址。

使用 CLI：

```
set firewall address <源接口_字符串> <名称_字符串> subnet <地址_ip> <网络掩码_ip>
```

添加目的地址

目的地址可以是位于互联网上的一个 VPN 客户端的地址或者一个远程 VPN 网关后面的一个网络的地址。

1 进入**防火墙 > 地址。**

2 选择一个外部接口。（根据 FortiGate 设备型号的不同，方法略有差别。）

3 单击新建添加一个地址。

4 输入地址的名称、IP 地址和网络掩码。这些参数可以是远程 VPN 端点的内部接口上的一台计算机或者整个子网的。

5 单击确定一保存目的地址。

使用 CLI：

```
set firewall address <目的接口_字符串> <名称_字符串> subnet <地址_ip> <网络掩码_ip>
```

添加一个加密策略

VPN 连接本地、内部网络和远程、外部网络。加密策略的重要任务是定义（和限制）这些网络中的哪些地址可以使用这个 VPN。

一个 VPN 只需要一个加密策略来控制向内和向外的连接。根据您对它所做的配置，加密策略控制您的内部网络中的用户能否建立到远程网络的连接（向外连接），和远程网络中的用户能否建立一个到您的内部网络的通道（向内连接）。这种灵活性使得单一的加密策略就能够完成两个常规的防火墙策略的工作。

尽管加密策略同时控制进入和发出的连接，它也必须被配置成为一个向外的的策略。一个向外的策略有一个位于内部网络中的源地址和一个位于外部网络中的目的地址。这个源地址可以识别内部网络中的哪些地址属于这个 VPN。目的地址可以识别远程网络中的哪些地址属于这个 VPN。标准的向外的策略包括内部到外部和 DMZ 到外部。

注意：目的地址可以是一个位于互联网上的 VPN 客户端地址或者位于一个远程 VPN 网关后边的网络的地址。

除了通过地址定义这个 VPN 的成员之外，您还可以配置这个加密策略的服务，例如 DNS、FTP、和 POP3，以及根据一个预定义的时间表（每天中的时间，或者一周、月、年中的某一天）来允许连接。您还可以配置加密策略的以下内容：

- 向内 NAT 以转换进入的数据包的源地址。
- 向外的 NAT 以转换发出的数据包的源地址。
- 流量控制以控制这个 VPN 可用的带宽和这个 VPN 的优先级。
- 内容配置文件可以在这个 VPN 中应用防病毒保护、网页内容过滤、电子邮件过滤、文件传输和电子邮件服务。
- 记录日志使得 FortiGate 设备记录所有使用这个 VPN 的连接。

按以下步骤添加加密策略：

1 进入**防火墙 > 策略。**

2 选择您要添加策略的那个策略列表（不同型号的 FortiGate 设备的选择方法略有不同）。

3 单击 新建 以添加新的策略。

4 把 源地址 设为源地址。

5 把 目的地址 设置为目的地址。

6 设置服务以控制允许通过这个 VPN 连接的服务类型。
您可以选择任意以允许全部支持的服务通过这个 VPN 连接，或者选择一个特定的服务或服务组以限制允许通过这个 VPN 连接的服务。

7 将动作设置为加密。

8 配置加密参数。

VPN 通道	为这个加密策略选择一个自动密钥通道。
允许向内	选择 **允许向内** 可以允许向内连接的用户连接到源地址上。
允许向外	选择 **允许向外** 可以允许向外连接的用户连接到目的地址上。

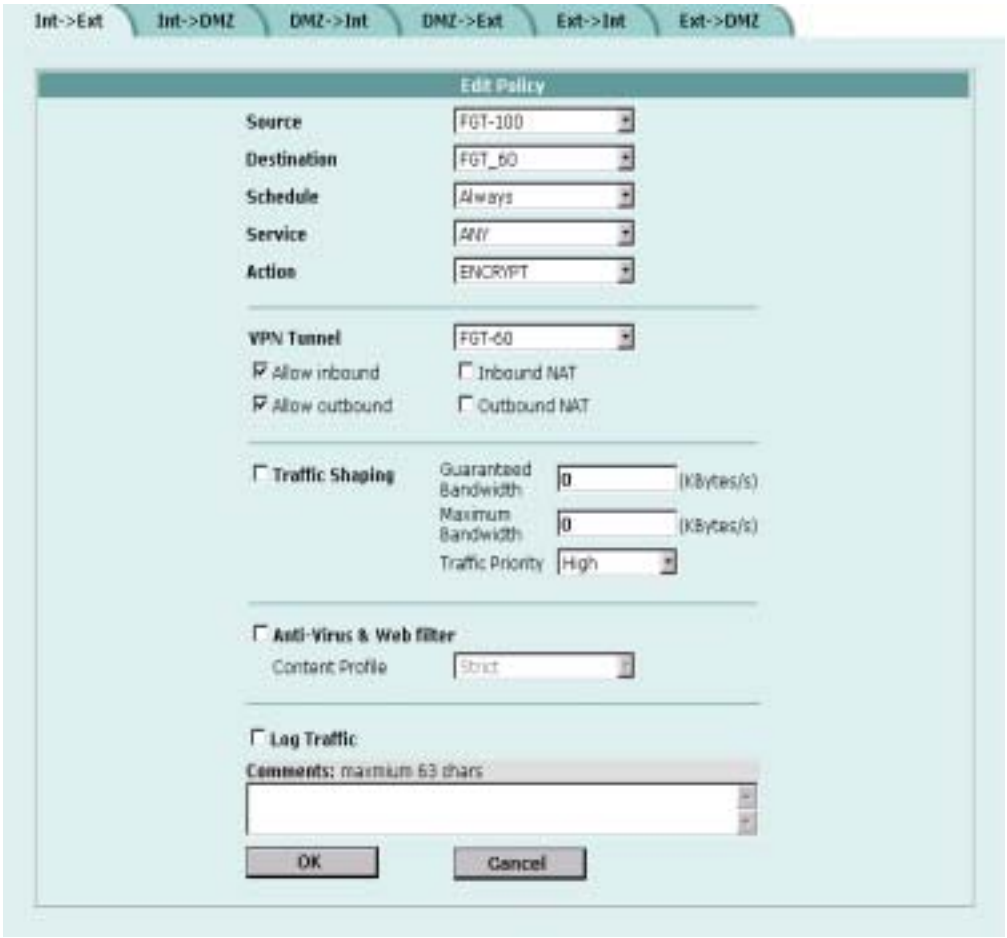
向内 NAT	FortiGate 可以把接收到的向内的数据包的源地址转换为连接到源地址网络上的 FortiGate 内部网络接口的 IP 地址。通常这是 FORTIGate 设备的一个内部接口。 向内 NAT 使得本地主机无法看到远程主机（在远程 VPN 网关后面的网络中的主机）的 IP 地址。
向外 NAT	FortiGate 可以把向外发送的数据包的源地址转换为连接到目的地址网络上的 FortiGate 的网络接口的 IP 地址。通常情况下这是 FortiGate 设备的一个外部接口。 向外 NAT 使得远程主机无法看到本地主机 （位于本地 VPN 网关后边的网络中的主机）的 IP 地址。 如果实现了向外 NAT，它受到以下限制： 只能在通道的一端配置向外 NAT。 没有实现向外 NAT 的那一端需要有一个内部 -> 外部的策略以将另一端的外部接口指定为目的地 （这将是一个公共 IP 地址）。 通道和通道中的通讯只能由配置了向外 NAT 的那一端初始化。

关于配置策略的其他设置的详细信息请见 *FortiGate 安装和配置指南*。

9 单击确定以保存加密策略。

10 排列加密策略在策略列表中的位置，使它在其他具有同样源和目的地址以及服务的策略之上，以确保加密策略能匹配 VPN 连接。

图 17: 添加一个加密策略



使用 CLI：

```
set firewall policy
```

```
src_intf <源接口_字符串> dstintf <目的接口_字符串> policyid <策略编号 _ 整数 > move < 从 - 策略 _ 整数 > to < 到 - 策略 _ 整数 >
```

```
status {enable | disable}
```

```
srcaddr <源地址名称_字符串> dstaddr <目的地址名称_字符串> schedule < 时间表名称 _ 字符串 > service < 服务名称 _ 字符串 > action encrypt
```

```
vpntunnel < 通道名称 _ 字符串 > inbound {allow | deny} natinbound {enable | disable} outbound {allow | deny} natoutbound {enable | disable}
```

```
trafficshaping {enable | disable} gbandwidth < 保证带宽 _ 整数 > maxbandwidth < 最大带宽 _ 整数 〉 priority {high | medium | low}
```

```
avwebfilter {enable < 配置文件名 _ 字符串 > | disable}
```

```
logtraffic {enable | disable}
```

例子：单一手工密钥端点

在本例中，一个单独的 VPN 通道连接了两个 IPSec 网关。这两个网关都是 FortiGate 设备并且都使用静态 IP 地址。

这两个网关使用一个手工密钥来向对方彼此认证，以及用来加密 VPN 通道中他们之间的信息流。这个密钥由多种信息组成，包括加密的认证算法、实际密钥条目和一个安全参数索引 （SPI），一个用于定义端点之间的通讯结构的任意值。

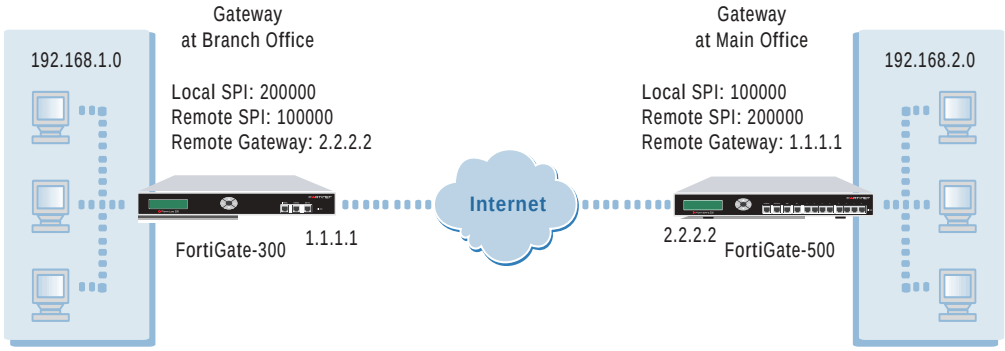
在两个网关之间的加密和认证算法以及密钥必须匹配。本地网关的向内 SPI 值必须匹配远程网关的向外 SPI 值。

网络拓扑结构

网络拓扑结构包括一个标准的手工密钥配置、使用了两个网关，他们彼此使用外部接口通过一个 VPN 通道连接。这些设备使用的手工密钥包括全部的参数：认证和加密算法，密钥和 SPI。

在本例中，两个网关都是 FortiGate 防火墙。这个例子可以到一个非 FortiGate 设备中，只要这个设备服从 IPSec 标准并使用了兼容的的手工密钥加密和认证参数配置。

图 18: 手工密钥认证



一般配置步骤

要启用在两个网关之间的手工密钥 IPSec VPN 通道，您必须在两个 FortiGate 设备中输入相应的设置。其中一个位于主办公机构，而另洋位于分支办公机构。

主办公机构网关配置

1. 配置将主办公机构网关连接到分支办公机构网关的手工密钥通道。这项工作包括指定这个通道的名称、选择加密和认证算法、输入密钥并指定本地 （主办公机构）和远程（分支办公机构）的 SPI。
2. 作为这个 VPN 的一部分，添加一个源地址以指定主办公机构的内部网络中的地址或地址范围。
3. 作为这个 VPN 的一部分，添加一个目的地址以指定在分支机构的内部网络中的一个地址或者地址范围。
4. 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到主办公机构的内部网络和从主办公机构内部网络发出的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

分支机构网关配置

1 配置将分支办公机构网关连接到主办公机构网关的手工密钥通道。这项工作包括指定这个通道的名称、选择加密和认证算法、输入密钥并指定本地 （分支办公机构）和远程 （主办公机构）的 SPI。

2 作为这个 VPN 的一部分，添加一个源地址以指定在分支机构的内部网络中的一个地址或者地址范围。

3 作为这个 VPN 的一部分，添加一个目的地址以指定主办公机构的内部网络中的地址或地址范围。

4 添加一个包含了源地址和目的地址的内部到外部的加密策略。这个策略为连接到分支办公机构的内部网络和从分支机构内部网络发出的通讯激活这个 VPN 通道。排列加密策略在策略列表中的位置，使它位于具有相同源地址和目的地址的其他策略之上。

注意：两个网关的加密算法、加密密钥和认证密钥必须互相匹配。SPI 值的设置必须互补 （换句话说，主办公机构的本地 SPI 是分支办公机构的远程 SPI）。全部参数都要使用十六进制（HEX）字符。SPI 值必须大于 BB8。

配置参数

在两个网关中必须输入如下配置。

表 26：手工密钥通道参数

域名	主办公机构值	分支办公机构值
通道名	Branch_Office_VPN	Main_Office_VPN
本地 SPI	100000	200000
远程 SPI	200000	100000
远程网关	1.1.1.1	2.2.2.2
加密算法	3DES	3DES
加密密钥	003f2b01a9002f3b 004f4b0209003f01 3b00f23bff003eff	003f2b01a9002f3b 004f4b0209003f01 3b00f23bff003eff
认证算法	SHA1	SHA1
认证密钥	ff003f012ba90bbb 00f402303f0100ff3b00f23b	ff003f012ba90bbb 00f402303f0100ff3b00f23b
集中器	无	无

表 27：源地址和目的地址

域名	主办公机构值	分支办公机构值
源地址		
地址名	Main_Office	Branch_Office
IP 地址	192.168.2.0	192.168.1.0
网络掩码	255.255.255.0	255.255.255.0
目的地址		
地址名	Branch_Office	Main_Office
IP 地址	192.168.1.0	192.168.2.0
网络掩码	255.255.255.0	255.255.255.0

表 28：加密策略

域名	主办公机构值	分支办公机构值
源地址	Main_Office	Branch_Office
目的地址	Branch_Office	Main_Office
任务计划	总是	总是
服务	任意	任意
动作	加密	加密
VPN 通道	Branch_Office_VPN	Main_Office_VPN
允许向内	启用	启用
允许向外	启用	启用
向内 NAT	不启用	不启用
向外 NAT	不启用	不启用

配置主办公机构网关

配置由四个步骤组成：添加手工密钥通道、添加源地址、添加目的地址、添加内部到外部的加密策略。其结果是建立一个 IPSec VPN 通道从主办公机构的网络连接到分支办公机构的网络，并允许从主办公机构的内部网络流出和流入的通讯。

基于 Web 的管理程序配置步骤

1 添加一个手工密钥通道。

进入 **VPN > IPSec > 手工密钥。**

- 单击新建。
- VPN 通道名称： Branch_Office_VPN
- 本地 SPI: 100000
- 远程 SPI: 200000
- 远程网关： 1.1.1.1
- 加密算法： 3DES
- 加密密钥：

  003f2b01a9002f3b

  004f4b0209003f01

  3b00f23bff003eff
- 认证算法：SHA1
- 认证密钥：

  ff003f012ba90bbb

  00f402303f0100ff3b00f23b
- 集中器：无

2 添加源地址。

- 对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：内部。

- 单击新建
- 地址名称： Main_Office
- IP 地址： 192.168.2.0
- 网络掩码：255.255.255.0
- 单击确定。

3 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：外部。

- 单击新建
- 地址名称：Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

4 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部**。

- 单击新建。
- 源地址：Main_Office
- 目的地址： Branch_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Branch_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加手工密钥通道。

```
set vpn ipsec manualkey Branch_Office_VPN localspi 100000
remotespi 200000 gateway 1.1.1.1 encalg 3des enckey
003f2b01a9002f3b-004f4b0209003f01-3b00f23bff003eff authalg sha1
authkey ff003f012ba90bbb-00f402303f0100ff3b00f23b concentrator
none
```

2 添加源地址。

```
set firewall address Internal Main_Office subnet 192.168.2.0
255.255.255.0
```

3 添加目的地址。

```
set firewall address External Branch_Office subnet 192.168.1.0
255.255.255.0
```

4 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Main_Office dstaddr Branch_Office schedule Always
service ANY action encrypt vpntunnel Branch_Office_VPN inbound
allow outbound allow
```

5 移动加密策略。

```
set firewall policy srcintf internal dstintf external move 2 to
1
```

配置分支机构网关

配置由四个步骤组成：添加手工密钥通道、添加源地址、添加目的地址、添加内部到外部的加密策略。其结果是建立一个 IPSec VPN 通道从主办公机构的网络连接到分支办公机构的网络，并允许从分支办公机构的内部网络流出和流入的通讯。

基于 Web 的管理程序的配置步骤

1 添加手工密钥通道。

进入 **VPN > IPSec > 手工密钥。**

- 单击新建。
- VPN 通道名称：Main_Office_VPN
- 本地 SPI：200000
- 远程 SPI：100000
- 远程网关： 2.2.2.2
- 加密算法： 3DES
- 加密密钥：

  003f2b01a9002f3b

  004f4b0209003f01

  3b00f23bff003eff
- 认证算法： SHA1
- 认证密钥：

  ff003f012ba90bbb

  00f402303f0100ff3b00f23b
- 集中器：无

2 添加源地址。

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 内部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：内部。

- 单击新建
- 地址名称： Branch_Office
- IP 地址： 192.168.1.0
- 网络掩码： 255.255.255.0
- 单击确定。

3 添加目的地址

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 地址 > 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 地址**，然后选择接口：外部。

- 单击新建
- 地址名称：Main_Office
- IP 地址： 192.168.2.0
- 网络掩码： 255.255.255.0
- 单击确定。

4 添加加密策略

对于 FortiGate-300 或者更低型号的设备，进入 **防火墙 > 策略 > 内部 -> 外部**。

对于 FortiGate-400 或更高型号的设备，进入**防火墙 > 策略 > 内部 -> 外部**。

- 单击新建。
- 源地址：Branch_Office
- 目的地址： Main_Office
- 任务计划：总是
- 服务：任意
- 动作：加密
- VPN 通道：Main_Office_VPN
- 允许向内：启用
- 允许向外：启用
- 向内 NAT：不启用
- 向外 NAT：不启用
- 流量控制：根据需要配置这个策略的设置。
- 流量日志：如果您希望无论何时，当这个策略处理一个连接时都将消息写入日志，则选中此项。
- 病毒防护和网页过滤：根据需要配置这个策略的设置。
- 单击确定。

为了保证加密策略能够匹配 VPN 连接，将它放在策略列表中指定源地址和目的地址的策略的下方，放在比它的源地址和目的地址范围更大的常规 （非加密）策略的上方。

CLI 配置步骤

1 添加手工密钥通道。

```
set vpn ipsec manualkey Main_Office_VPN localspi 200000
remotespi 100000 gateway 2.2.2.2 encalg 3des enckey
003f2b01a9002f3b-004f4b0209003f01-3b00f23bff003eff authalg sha1
authkey ff003f012ba90bbb-00f402303f0100ff3b00f23b concentrator
none
```

2 添加源地址。

```
set firewall address Internal Branch_Office subnet 192.168.1.0
255.255.255.0
```

3 添加目的地址。

```
set firewall address External Branch_Office subnet 192.168.2.0
255.255.255.0
```

4 添加加密策略。

```
set firewall policy srcintf internal dstintf external policyid
2 srcaddr Branch_Office dstaddr Main_Office schedule Always
service ANY action encrypt vpntunnel Main_Office_VPN inbound
allow outbound allow
```

5 移动加密策略。

```
set firewall policy srcintf internal dstintf external move 2 to
1
```

IPSec VPN 集中器

本章描述了星型配置 （集线器和辐条）的 IPSec VPNs。除此之外还提供了一个技术方面的概述。本章也提供了一个例子。

本章叙述了如下内容：

概述

在一个星型配置的网络中，所有的 VPN 通道都终结在一个起集线器作用的端点上。其他的端点就象辐条一样连接到这个集线器上。这个集线器的功能如同网络中的一个集中器，管理着辐条之间的 VPN 连接。

星型配置的网络的优势在于辐条的配置更加简单，因为它们只需较少的策略。一个星型配置的网络能够为每个辐条提供同样的处理效率。星型配置的网络的劣势是它依赖于一个端点去管理所有的 VPN。如果这个端点发生故障或关闭，这个网络中将无法进行任何加密通讯。

一个星型配置的 VPN 网络需要一个特定的配置。配置的不同取决于 VPN 端点所扮演的角色的不同。如果 VPN 端点是一个作为集线器或集中器的的 FortiGate 设备，它需要对它所连接到每个辐条 （自动 IKE 第一阶段和第二阶段设置或手工密钥设置，加上加密策略）设置一个 VPN 配置。还需要一个集中器配置以将星型配置的通道彼此分组。这个集中器配置将 FortiGate 设备定义为星型配置网络中的集线器。

如果 VPN 端点是一个辐条，它需要一个通道以将它连接到集线器 （但是不连接到其他辐条）。它还需要控制它到其他辐条的加密连接策略和到其他网络，例如互联网的非加密连接的策略。

总之，一个星型配置的 IPSec VPN 配置与常规的 IPSec VPN 配置有两点重要的不同。首先，集线器需要一个额外的配置步骤，使集中器将星型的通道彼此组织起来。其次，辐条需要至少一个配置步骤，因为他们彼此之间不需要通道，只需要加密策略。

VPN 集中器 （集线器）一般配置步骤

作为集线器的中央 FortiGate 需要以下配置：

- 每个辐条一个通道 （自动 IKE 第一阶段和第二阶段配置或者手工密钥配置）
- 每个辐条的目的地址
- 一个集中器配置
- 每个辐条一个加密策略

按照如下步骤创建一个 VPN 集中器配置

1 为每个辐条配置一个通道。可以选择手工密钥通道或者自动 IKE 通道。

- 一个手工密钥通道的构成包括这个通道的名称，在通道对应的另一端的辐条 （客户端或者网关）的 IP 地址，以及这个通道所用的加密和认证算法。

  请见 第 97 页 “ 手工密钥的 IPSec VPN” 。
- 一个自动 IKE 通道的构成包括第一阶段和第二阶段参数。第一阶段参数包括辐条（客户端或者网关）的名称，指定辐条如何接收它的 IP 地址 （静态或者拨号），加密和认证算法，以及认证方法，可以是预置密钥或者 PKI 证书。第二阶段参数包括通道的名称，加密和认证算法，以及一些安全参数。

  请见 第 47 页 “ 预置密钥 IPSec VPN” 或者 第 13 页 “ 使用认证的 IPSec VPNs” 。

2 为每个辐条添加目的地址。目的地址是辐条 （可以是在互联网上的一个客户端或者位于一个网关后边的一个网络）的地址。

请见 第 59 页 “ 添加目的地址” 。

3 添加一个集中器配置，这个步骤将 FortiGate 设备上的通道彼此分组。这些通道将集中器连接到辐条。这个通道是作为自动 IKE 第二阶段配置或者手工密钥配置的一部分添加的。

请见 第 115 页 “ 添加一个 VPN 集中器” 。

注意：在为全部辐条添加完通道之后再为中央 FortiGate （集线器）设备添加集中器配置。

4 为每个辐条添加一个加密策略。加密策略控制着通过集线器的通讯的方向，允许集线器和辐条之间的向内和向外的 VPN 连接。每个辐条的加密策略必须包含这个辐条的通道名。源地址必须是内部 _ 全部。在加密策略中使用如下配置：

源	内部 _ 全部
目的	VPN 辐条的地址
动作	加密
VPN 通道	VPN 辐条通道名。
允许向内	选择允许向内。
允许向外	选择允许向外。
向内 NAT	如果需要选择向内 NAT。
向外 NAT	如果需要选择向外的 NAT。

请见 第 60 页 “ 添加一个加密策略” 。

5 按照如下顺序排列策略的位置：
- 加密策略
- 默认非加密策略（内部_全部 -> 外部_全部）

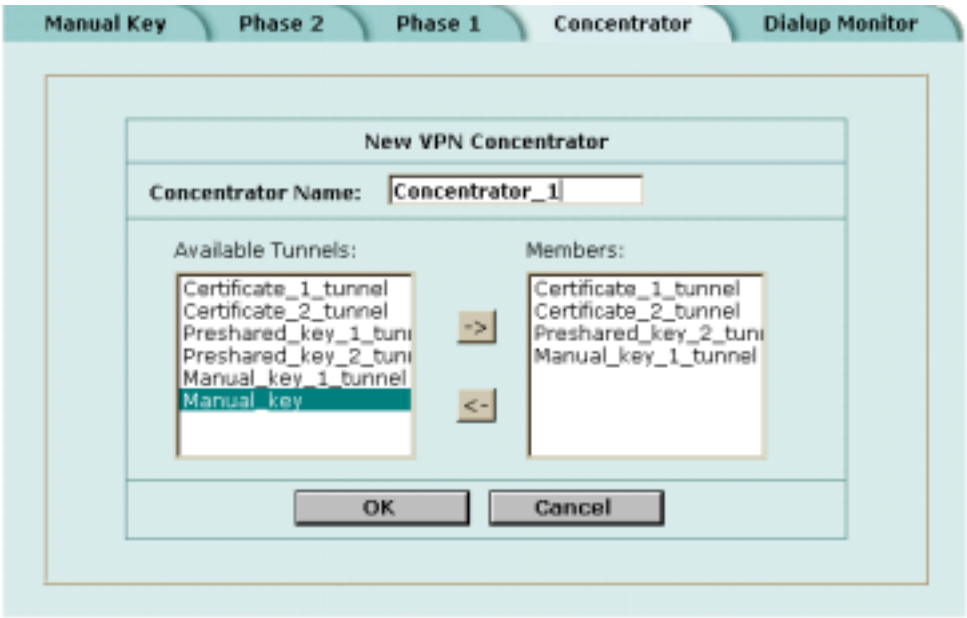
添加一个 VPN 集中器

VPN 集中器将集线器和辐条的通道汇总到一个组中。这使得 VPN 通讯可以通过 FortiGate 设备从一个通道到另一个。使用这种配置，FortiGate 设备的功能如同一个星型配置的网络中的集中器，或者集线器。

按照如下步骤添加一个 VPN 集中器配置

1 进入 **VPN > IPSec > 集中器**。
2 单击 **新建** 以添加新的 VPN 集中器。
3 在 集中器名称 一栏输入新集中器的名称。
4 把通道添加到 VPN 集中器，从 **可用通道列表** 中选择 VPN 通道然后单击右箭头。
5 要从集中器中删除通道，从 **成员列表** 中选定要删除的通道然后单击左箭头。
6 单击 **确定** 添加 VPN 集中器。

图 19: 添加一个 VPN 集中器



使用 CLI（集中器）：

```
set vpn ipsec concentrator <名称_字符串> member {none | <通道_字符串> <通道_字符串> ...}
```

VPN 辐条一般配置步骤

一个实现辐条功能的远程 VPN 端点需要以下配置：

- 一个到集线器的通道 （自动 IKE 第一阶段和第二阶段配置或手工密钥配置）。
- 本地 VPN 辐条的源地址。
- 每个远程 VPN 辐条的目的地址。
- 每个远程 VPN 辐条一个独立的向外加密策略。这些策略允许本地 VPN 辐条初始化加密连接。
- 一个单独的向内加密策略。这个策略允许本地 VPN 辐条接受加密连接。

按以下步骤创建 VPN 辐条配置：

1 在辐条和集线器之间配置通道。

选择手工密钥通道或者自动 IKE 通道。

- 要添加手工密钥通道，请见 第 97 页 “ 手工密钥的 IPSec VPN” 。
- 要添加手工密钥通道，请见 第 47 页 “ 预置密钥 IPSec VPN” 。
- 要添加一个自动 IKE 通道，请见 第 13 页 “ 使用认证的 IPSec VPNs” 。

2 添加源地址。需要一个本地 VPN 辐条的源地址。

请见 第 28 页 “ 添加一个源地址” 。

3 为每个远程 VPN 辐条输入一个目的地址。目的地址是辐条 （互联网上的客户端或者网关后边的网络）的地址。

请见 第 28 页 “ 添加目的地址” 。

4 为每个远程 VPN 辐条设置一个独立的向外加密策略。这个策略控制这本地 VPN 辐条初始化的加连接。

加密策略必须包括在步骤 1 中添加的适当的源地址和目的地址和通道。使用如下配置：

源	本地 VPN 辐条的地址。
目的	远程 VPN 辐条的地址。
动作	加密
VPN 通道	在步骤 1 中添加的 VPN 通道名。（对所有加密策略使用相同的通道名）
允许向内	不启用。
允许向外	选择允许向外。
向内 NAT	如果需要选择向内 NAT。
向外 NAT	如果需要选择向外的 NAT。

请见 第 60 页 “ 添加一个加密策略” 。

5 添加一个向内加密策略。这个策略控制这由远程 VPN 辐条初始化的加密连接。

集线器的加密策略必须包含在步骤 1 中添加的通道的源地址和目的地质。使用如下配置：

源	本地 VPN 辐条的地址。
目的	外部 _ 全部
动作	加密
VPN 通道	在步骤 1 中添加的 VPN 通道名。（对所有加密策略使用相同的通道名）
允许向内	选择允许向内。

允许向外 不启用。

向内 NAT 如果需要选择向内 NAT。

向外 NAT 如果需要选择向外的 NAT。

请见 第 60 页 “ 添加一个加密策略” 。

6 按照如下顺序排列策略：

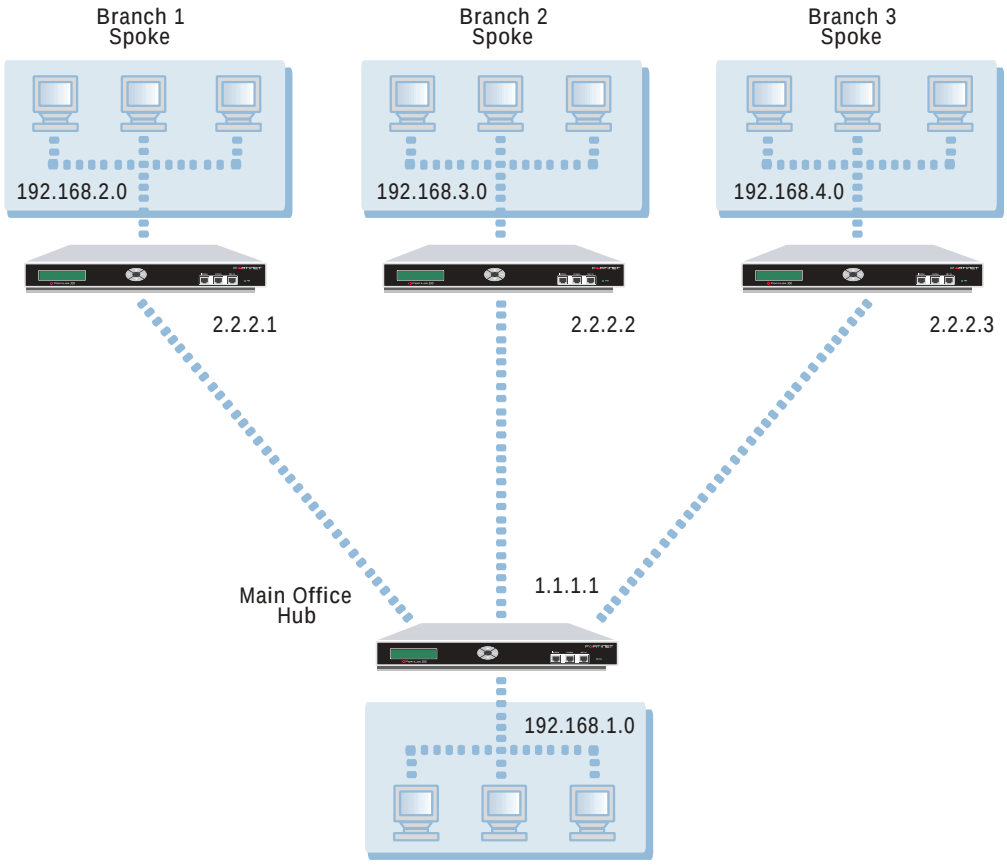
- 向外加密策略
- 向内加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

注意：为了允许 VPN 辐条访问其他网络，例如互联网，默认的非加密策略是必须的。

例子：带有三个辐条的一个 VPN 集中器

在这个例子中，中心的 FortiGate 设备的作用如同一个集中器，或者集线器，使用 IPSedc 通道连接三个辐条。

图 20： 集线器和辐条配置



网络拓扑结构

这个网络的拓扑结构包括一个主办公网络，它负责引导三个分支办公机构之间的通讯。主办公机构是一个作为集中器或集线器的 FortiGate 设备。三个分支机构的 FortiGate 设备的功能如同辐条。

一般配置步骤

要启用一个星型配置的网络的配置，您必须在四个 FortiGate 设备上输入相应的设置，其中一个位于主办公机构，其他三个位于分支办公机构。

主办公机构网关 （集线器）配置

1 为主办公机构到每个辐条配置一个通道。

- 对于分支 1，配置一个手工密钥通道。
- 对于分支 2，配置一个使用预置密钥的自动 IKE 通道。
- 对于分支 3，配置一个使用证书的自动 IKE 通道。

2 为每个辐条添加一个目的地址。

3 添加一个集中器配置。

4 为每个辐条添加一个加密策略。

5 按照如下顺序排列策略的位置：
- 分支 1、2、3 的加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

分支 1 网关 （辐条）配置

1 添加一个手工密钥通道连接分支 1 和集线器。
2 为本地辐条添加源地址。
3 为远程辐条 （分支 2 和 3）添加目的地址。
4 添加向外的加密策略以控制本地辐条初始化的到远程辐条 （分支 2 和 3）的 VPN 连接。
5 添加一个向内的加密策略以控制远程辐条 （分支 2 和 3）初始化的到本地辐条的 VPN 连接。
6 按照如下顺序排列策略的位置：
- 分支 2 和 3 的向外加密策略
- 向内加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

分支 2 网关 （辐条）配置

1 添加一个预置密钥的自动 IKE 密钥通道连接分支 2 和集线器。
2 添加源地址。
3 为远程辐条 （分支 1 和 3）添加目的地址。
4 添加向外的加密策略以控制本地辐条初始化的到远程辐条 （分支 1 和 3）的 VPN 连接。
5 添加一个向内的加密策略以控制远程辐条 （分支 1 和 3）初始化的到本地辐条的 VPN 连接。
6 按照如下顺序排列策略的位置：
- 分支 1 和 3 的向外加密策略
- 向内加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

分支 3 网关 （辐条）配置

1 添加一个使用证书的自动 IKE 密钥通道连接分支 3 和集线器。
2 添加源地址。
3 为远程辐条 （分支 1 和 2）添加目的地址。
4 添加向外的加密策略以控制本地辐条初始化的到远程辐条 （分支 1 和 2）的 VPN 连接。
5 添加一个向内的加密策略以控制远程辐条 （分支 1 和 2）初始化的到本地辐条的 VPN 连接。
6 按照如下顺序排列策略的位置：
- 分支 1 和 2 的向外加密策略
- 向内加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

配置参数

必须在 FortiGate 设备上输入以下配置参数。

主办公机构和分支 1 之间的通道

表 29：主办公机构和分支 1 之间的手工密钥配置

字段名	主办公机构信息	分支 1 信息
VPN 通道名称	Branch1_VPN	Main_Office_VPN
本地 SPI	10000	20000
远程 SPI	20000	10000
远程网关	2.2.2.1	1.1.1.1
加密算法	3DES	3DES
加密密钥	1234567890abcdef 1234567890abcdef 1234567890abcdef	1234567890abcdef 1234567890abcdef 1234567890abcdef
认证算法	MD5	MD5
认证密钥	1234567890abcdef 0987654321abcdef	1234567890abcdef 0987654321abcdef

主办公机构和分支 2 之间的通道

表 30：主办公机构和分支 2 之间的第一阶段配置

字段名	主办公机构信息	分支 2 信息
网关名称	Branch2_GW	Main_Office_GW
远程网关	静态 IP 地址	静态 IP 地址
IP 地址	2.2.2.2	1.1.1.1
模式	主模式（ID 保护）	主模式（ID 保护）
P1 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
DH 组	5	5
认证方式	预置密钥	预置密钥
预置密钥	ddcHH01887d	ddcHH01887d
本地 ID	空	空
高级选项	无	无

表 31：在主办公机构和分支办公机构 2 上输入的第二阶段配置

字段名	主办公机构信息	分支 2 信息
通道名称	Branch2_VPN	Main_Office_VPN
远程网关	Branch2_GW	Main_Office_GW
P2 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
启用重放检测	启用	启用
启用向前保密 （PFS）	启用	启用
DH 组	5	5
密钥有效期	300 秒	300 秒
自动密钥保持激活	启用	启用
集中器	不选中	不选中

主办公机构和分支 3 之间的通道

表 32：主办公机构和分支 3 的第一阶段配置

字段名	主办公机构信息	分支 3 信息
网关名称	Branch3_GW	Main_Office_GW
远程网关	静态 IP 地址	静态 IP 地址
IP 地址	2.2.2.3	1.1.1.1
模式	主模式（ID 保护）	主模式（ID 保护）
P1 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
DH 组	5	5
认证方式	RSA 签名	RSA 签名
预置密钥	Main_Office_certificate	Branch_3_certificate
本地 ID	空	空
高级选项	无	无

表 33：在主办公机构和分支办公机构 3 上输入的第二阶段配置

字段名	主办公机构信息	分支 3 信息
通道名称	Branch3_VPN	Main_Office_VPN
远程网关	Branch3_GW	Main_Office_GW
P2 提议		
加密 1	3DES	3DES
加密 2	3DES	3DES
认证 1	SHA1	SHA1
认证 2	MD5	MD5
启用重放检测	启用	启用
启用向前保密 （PFS）	启用	启用
DH 组	5	5
密钥有效期	300 秒	300 秒
自动密钥保持激活	启用	启用
集中器	不选中	不选中

主办公机构集中器

表 34：VPN 集中器配置

字段名	VPN 集中器信息
集中器名称	Main_Office_Concentrator
成员	Branch1_VPN Branch2_VPN Branch3_VPN

主办公机构的目的地址

表 35：目的地址信息

字段名	主办公机构信息		
目的地址			
地址名称	Branch1	Branch2	Branch3
IP 地址	192.168.2.0	192.168.3.0	192.168.4.0
网络掩码	255.255.255.0	255.255.255.0	255.255.255.0

分支 1、2、3 的源地址和目的地址

表 36：源地址和目的地址信息

字段名	分支 1 信息	分支 2 信息	分支 3 信息
源地址			
地址名称	Branch1	Branch2	Branch3
IP 地址	192.168.2.0	192.168.3.0	192.168.4.0
网络掩码	255.255.255.0	255.255.255.0	255.255.255.0
目的地址			
地址名称	Branch2	Branch1	Branch1
IP 地址	192.168.3.0	192.168.2.0	192.168.2.0
网络掩码	255.255.255.0	255.255.255.0	255.255.255.0
地址名称	Branch3	Branch3	Branch2
IP 地址	192.168.4.0	192.168.4.0	192.168.3.0
网络掩码	255.255.255.0	255.255.255.0	255.255.255.0

主办公机构加密策略

表 37：主办公机构加密策略

字段名称	策略信息
主办公机构到分支 1	
源地址	内部 _ 全部
目的地址	Branch1
动作	加密
VPN 通道名称	Branch1_VPN
允许向内	启用
允许向外	启用
主办公机构到分支 2	
源地址	内部 _ 全部
目的地址	Branch2
动作	Encrypt
VPN 通道名称	Branch2_VPN
允许向内	启用
允许向外	启用
主办公机构到分支 3	
源地址	内部 _ 全部
目的地址	Branch3
动作	Encrypt
VPN 通道名称	Branch3_VPN
允许向内	启用
允许向外	启用

分支机构 1 加密策略

表 38：分支机构 1 加密策略

字段名称	策略信息
向外加密策略 （分支 1 到分支 2）	
源地址	Branch1
目的地址	Branch2
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向外加密策略 （分支 1 到分支 3）	
源地址	Branch1
目的地址	Branch3
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向内加密策略 （分支 2 和分支 3 到分支 1）	
源地址	Branch1
目的地址	外部 _ 全部
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	启用
允许向外	不启用

分支机构 2 加密策略

表 39：分支机构 2 加密策略

字段名称	策略信息
向外加密策略（分支 2 到分支 1）	
源地址	Branch2
目的地址	Branch1
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向外加密策略（分支 2 到分支 3）	
源地址	Branch2
目的地址	Branch3
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向内加密策略（分支 1 和分支 3 到分支 2）	
源地址	Branch1
目的地址	外部 _ 全部
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	启用
允许向外	不启用

分支机构 3 加密策略

表 40：分支机构 3 加密策略

字段名称	策略信息
向外加密策略 （分支 3 到分支 1）	
源地址	Branch3
目的地址	Branch1
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向外加密策略 （分支 3 到分支 2）	
源地址	Branch3
目的地址	Branch2
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	不启用
允许向外	启用
向内加密策略 （分支 1 和分支 2 到分支 3）	
源地址	Branch1
目的地址	外部 _ 全部
动作	加密
VPN 通道名称	Main_Office_VPN
允许向内	启用
允许向外	不启用

IPSec VPN 冗余

本章提供了一个关于 IPSec VPN 冗余的简要介绍。它还描述了如何设置 FortiGate 设备的 IPSec VPN 冗余。

本章叙述了如下内容

概述

为了保证一个 IPSec VPN 通道的连续有效，您可以配置本地 FortiGate 设备和远程 VPN 端点（远程网关）之间的多重连接。使用了冗余配置后，如果一个连接失败了，FortiGate 设备将使用其他连接建立通道。

配置由每个 VPN 端点拥有的到互联网的连接数量决定。例如，如果本地 VPN 端点有两个到互联网的连接，那么它可以提供两个到远程 VPN 端点的冗余连接。

单独一个 VPN 端点最多可以配置三个冗余连接。

VPN 连接双方不需要具有相同的互联网连接数。例如，在两个 VPN 端点之间，一个可以有多个到互联网的连接，而另一个可以只有一个到互联网的连接。当然，使用不对称的配置的情况下，VPN 的一端的冗余级别和另一端不同。

注意： IPSec 冗余只能应用于有静态 IP 地址和使用预置密钥或数字证书彼此认证的 VPN 端点。它不能应用于使用动态分配 IP 地址（拨号用户）的 VPN 端点。它也不能应用于使用手工密钥的 VPN 端点。

一般配置步骤

在配置 IPSec 冗余之前，先配置这些 VPN 端点到互联网的连接。最低限度地，这两个端点中的一个需要有两个到互联网的连接。最低限度地，这两个端点一共要有三个到互联网的连接。

IPSec 冗余的配置的构成包括 VPN 的远程端点的每一个到互联网的第一阶段配置、一个或多个第二阶段配置、以及一个或多个加密策略。第二阶段配置和加密策略的数量取决于本地的互联网连接是如何配置的。如果本地的互联网连接配置被分组到一个区域中，那么全部的冗余连接只需要一个第二阶段配置和一个加密策略。如果本地的互联网连接被分组到了不同的区域或者被指定到单独的接口，那么对每个冗余的连接都需要一个单独的第二阶段配置和一个加密策略。

IPSec 冗余配置举例：

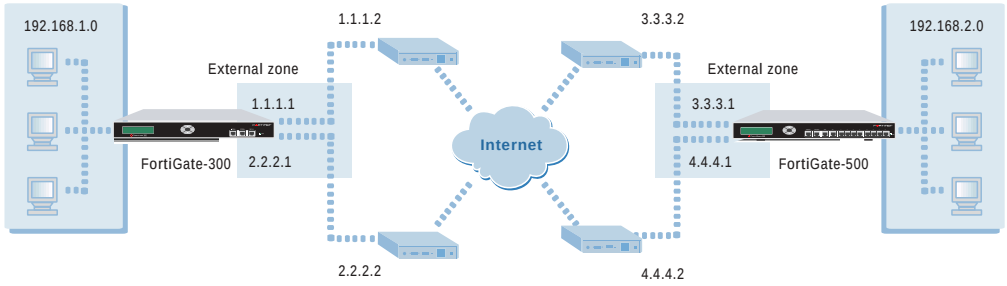
- 外部接口在同一区域中
- 外部接口在不同的区域中

外部接口在同一区域中

如果外部接口被分组到了单一的一个区域中，那么 IPSec 冗余的配置非常简单。例如，如果两个 VPN 端点都有两个到互联网的连接并且他们都被分组到了每个设备中的单一的一个区域中，IPSec 冗余可以按照如下方式配置：

- 2 个第一阶段配置 （远程端点的每个到互联网的连接使用一个配置）
- 1 个第二阶段配置 （指定添加到第一阶段的两个远程网关）
- 1 个加密策略 （指定添加到第二阶段的 VPN 通道）

图 21： 两个外部接口在同一区域中的 VPN 端点

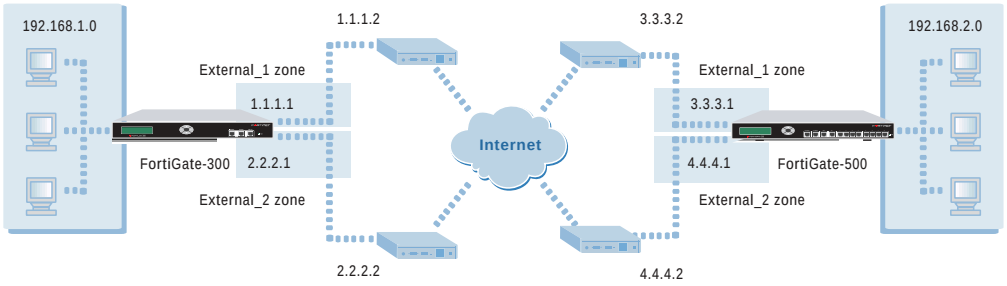


外部接口在不同的区域中

如果外部接口被分组到了不同的区域中或者指定了单独的接口，那么 IPSec 冗余的配置稍微复杂一些。例如，如果两个 VPN 端点都有两个到互联网的连接并且他们被分组到了每个设备中的不同的区域中，IPSec 冗余可以按照如下方式配置：

- 2 个第一阶段配置 （远程端点的每个到互联网的连接使用一个配置）
- 2 个第二阶段配置 （每个添加到第一阶段的远程网关使用一个）
- 2 个加密策略 （每个添加到第二阶段的 VPN 通道使用一个）

图 22： 两个外部接口在不同区域的 VPN 端点



按照如下方式配置 IPSec 冗余

1 最多为三个远程 VPN 连接添加第一阶段参数 （远程网关）。

除了网关名称和 IP 地址之外，为每个 VPN 连接输入相同的值。确保远程 VPN 端点 （远程网关）具有静态 IP 地址。

请见 第 52 页 “ 添加第一阶段配置” 。（使用预置密钥的自动 IKE）

请见 第 21 页 “ 添加第一阶段配置” 。（使用证书的自动 IKE）。

2 最多为三个远程 VPN 连接添加第二阶段参数。

- 如果这些到互联网的连接在同一区域内，添加一个 VPN 通道并为它添加远程网关。您最多可以添加三个远程网关。
- 如果这些到互联网的连接在不同的区域内，或者指定了单独的接口，为输入的每个远程网关添加一个 VPN 通道。

请见 第 57 页 “ 添加第二阶段配置” 。 （使用预置密钥的自动 IKE）

请见 第 26 页 “ 添加第二阶段配置” 。（使用证书的自动 IKE）。

3 添加源地址和目的地址。

请见 第 59 页 “ 添加一个源地址” 。

请见 第 59 页 “ 添加目的地址” 。

4 最多为三个远程 VPN 连接添加加密策略。

- 如果这些 VPN 连接在同一区域内，添加一个向外的加密策略；例如一个内部 -> 外部策略。为这个策略添加自动 IKE 密钥通道。
- 如果这些 VPN 连接在不同的区域中，为每个连接添加一个单独的向外的策略；例如，一个内部 -> 外部策略和一个内部 ->DMZ 策略。每个策略的源地址和目的地址必须相同。为每个策略添加一个不同的自动 IKE 密钥通道。

请见 第 60 页 “ 添加一个加密策略” 。

PPTP 和 L2TP VPNs

本章提供了一个 PPTP 和 L2TP VPN 的概述。它还包括了一些 PPTP 和 L2TP VPN 的详细的例子。

本章叙述了如下内容：

点对点隧道协议 （PPTP）概述

PPTP 允许您在一个远程客户端和您的内部网络之间创建一个虚拟私有网络（VPN）。因为它是一种 Windows 标准，所以 PPTP 无须在客户端电脑上安装第三方软件。只要互联网服务供应商在他的服务器上支持 PPTP，您就可以通过在客户端电脑和 FortiGate 设备上做一些简单的相关配置来创建一个安全连接。

顾名思义，PPTP 是包含了点对点的协议。PPTP 将数据打包放入 PPP 数据包中然后将 PPP 数据包封装为 IP 数据包以通过一个 VPN 通道来传送。

本指南致力于 PPTP 的主要应用，包括一个使用 PPP 拨号网络的远程客户端通过互联网创建一个到服务器的 VPN 连接。本指南不考虑应用在 LAN 上的 PPTP 连接。

注意：只有 NAT/ 路由模式支持 PPTP VPN。

PPTP 一般配置步骤

一个 PPTP VPN 的构成包括一个包含了要被认证的 PPTP 客户端的用户组、一个当 PPTP 连接到内部网络时分配给它们的地址范围、以及一个指定外部源地址的防火墙策略。作为添加这个策略的一部分，您需要将源地址和目的地址添加到 FortiGate 设备。

按照如下步骤创建一个 PPTP VPN 配置

1 添加一个用户组。

在 PPTP 客户端被允许启动一个 VPN 通道之前，它必须通过认证。要启用认证，您必须在 FortiGate 设备上添加一个用户组。在这个用户组中，为每个 PPTP 客户端添加一个用户。您可以将用户添加到 FortiGate 用户数据库，或者认证服务器 （RADIUS 或者 LDAP），或者在两个地方都添加。

请见 第 133 页 “ 添加一个用户” 和 第 134 页 “ 添加一个用户组” 。

2 启用 PPTP 和指定一个 PPTP 地址范围。

PPTP 地址范围是为远程 PPTP 客户端保留的一个地址范围。当一个远程 PPTP 客户端使用 PPTP 连接到内部网络时，这个客户端电脑被从这个范围内分配一个地址。PPTP 地址范围可以在任何子网内。

请见 第 134 页 “ 启用 PPTP 并指定一个地址范围” 。

3 添加一个防火墙策略。

要创建一个防火墙策略，您必须添加如下内容：源地址；目的地址；指定了源地址和目的地址的防火墙策略。

- 源地址由 PPTP 地址范围构成。将它们添加到外部区域。在添加完单独的 PPTP 地址之后，将它们汇总到一个地址组中。这使得您可以对整个 PPTP 地址范围使用单一的防火墙策略，胜过每个地址一个策略。（或者，如果 PPTP 地址范围由整个一个子网组成，添加这个子网的地址。不要添加一个地址组。）

  请见 第 135 页 “ 添加一个源地址” 和 第 135 页 “ 添加一个地址组” 。

- 目的地址是 PPTP 客户端可以连接到的地址。将它们添加到除了外部区域以外的任何区域。例如，如果目的地址位于内部网络中，您可以创建一个外部 -> 内部的策略以控制 PPTP 通过 FortiGate 设备的访问。典型情况下您可以为整个内部子网络只添加一个目的地址。

- 请见 第 136 页 “ 添加一个目的地址” 。

- 防火墙策略指定了源地址和目的地址，并设置了策略的服务选项以指定 PPTP VPN 通道内部的通讯的类型。例如，如果您希望 PPTP 客户端可以访问一个网页服务器，就将服务设置为 HTTP。

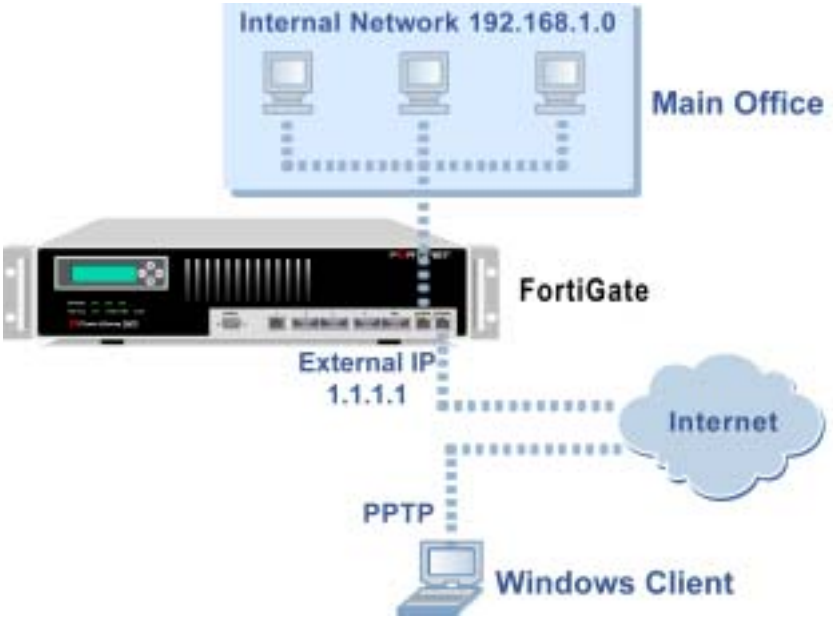
  请见 第 136 页 “ 添加一个防火墙策略” 。

4 配置一个 Windows 客户端。请见：

- 配置 PPTP 的 Windows98 客户端
- 配置 Windows2000 的 PPTP 客户端
- 配置 WindowsXP 的 PPTP 客户端

注意：确保您的 ISP 支持 PPTP 连接。

图 23: Windows 客户端和 FortiGate 设备之间的 PPTP VPN



将 FortiGate 设备配置为 PPTP 网关

添加一个用户

按照如下步骤为每个 PPTP 客户端添加一个用户

1 进入**用户 > 本地。**

2 单击新建以添加一个新的用户名。

3 输入这个用户名。

4 选择以下认证配置之一：

密码	输入用户用于认证的密码。这个密码的长度不得少于 6 个字符。这个密码可以包含数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符和空格符。
Radius	用于要求用户取得 LDAP 服务器的认证。选择用于用户认证的 LDAP 服务器的名字。您只能选择一个已经添加到 FortiGate LDAP 配置中的 LDAP 服务器。有关的详细信息请参阅您的 FortiGate 设备随机附带的 《FortiGate 安装和配置指南》。
LDAP	用于要求用户取得 RADIUS 服务器的认证。选择用于用户认证的 RADIUS 服务器的名字。您只能选择一个已经添加到 FortiGate RADIUS 配置中的 RADIUS 服务器。有关的详细信息请参阅您的 FortiGate 设备随机附带的 《FortiGate 安装和配置指南》。

注意：如果实现了 LDAP，那么必须在客户端、网关和 LDAP 服务器之间使用 PAP 来加密消息。不支持其他的加密方法，例如 CHAP 或者 MS-CHAP。

5 如果您希望 FortiGate 在连接 RADIUS 服务器失败时尝试连接 FortiGate RADIUS 配置中的其它 RADIUS 服务器，可以选择 如果选用的服务器连接失败则尝试连接其它服务器。

6 单击确定。

使用 CLI：

```
set user local <名称_字符串> [status {enable | disable}]
[tryother {enable | disable}] type {password | radius | ldap} {<
密码_字符串> | <radius 服务器名_字符串> | <ldap 服务器名_字符串>}
```

添加一个用户组

按照如下步骤为 PPTP 客户端添加一个用户组

1 进入 **用户 > 用户组**。

2 单击 **新建** 以添加新的用户组。

3 输入一个用于识别此用户组的 **组名** 。
这个组名可以是数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符和空格符。

4 要向这个用户组中添加 **用户** ，需从 **有效用户列表** 中选择用户，然后单击右箭头将用户名添加到成员列表中。

5 要向用户组中添加 RADIUS 服务器或者 LDAP 服务器，从 **有效用户列表** 中选择服务器名然后单击右箭头将 RADIUS 服务器添加到成员列表中。

6 单击 **确定** 。

使用 CLI：

```
set user group <组名_字符串> member <名称_字符串> [<名称_字符串
>,<名称_字符串>,...]
```

启用 PPTP 并指定一个地址范围

1 进入 **VPN > PPTP > PPTP 范围。**

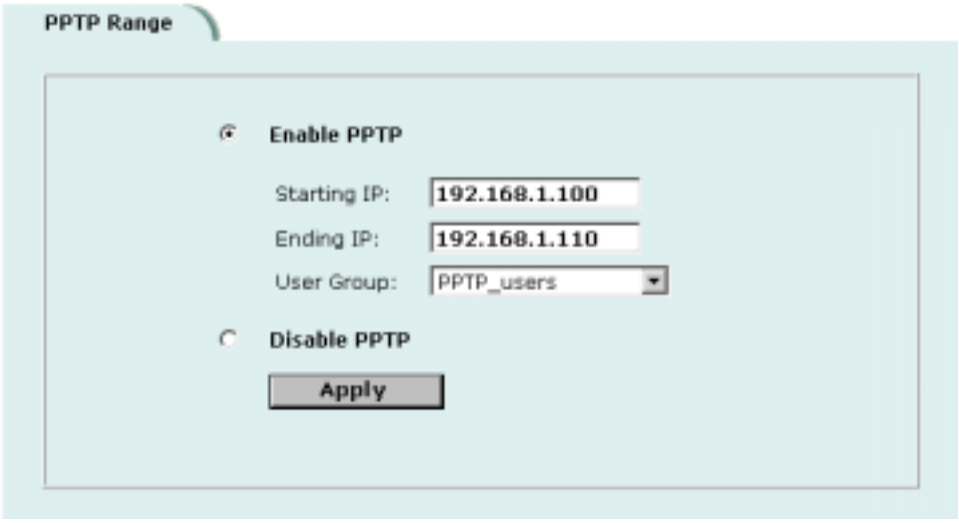
2 单击启用 PPTP。

3 输入 PPTP 地址范围的**起点 IP 地址**和**终点 IP 地址**。

4 选择您在 第 134 页 “ 添加一个用户组” 中添加的用户组。

5 单击 **应用** 以启用通过 FortiGate 的 PPTP。

图 24: PPTP 地址范围配置的例子



使用 CLI：

```
set vpn pptp [status {enable | disable}] sip <启始 _ip> eip <终止 _ip> usrgrp <名称 _ 字符串 >
```

添加一个源地址

对 PPTP 地址范围中的每个地址添加一个源地址。

1 进入 **防火墙 > 地址。**

2 选择 PPTP 客户要连接到的接口。

对于 FortiGate-400 或者更高型号的设备，这可以是一个接口、VLAN 子接口或者区域。

3 单击新建以添加一个地址。

4 为 PPTP 地址范围内的一个地址输入地址名，IP 地址和网络掩码。

5 单击确定以保存源地址。

6 对 PPTP 地址范围内的所有地址重复上述步骤。

注意：如果 PPTP 地址范围包含某个子网的全部地址，您可以添加这个子网的地址。不要添加地址组。

使用 CLI：

```
set firewall address <接口_字符串> <名称_字符串> subnet <子网地址 _ip> <网络掩码 _ip>
```

添加一个地址组

将源地址编进地址组。

1 进入 **防火墙 > 地址 > 组。**

2 在 PPTP 客户连接到的网络接口添加一个新的地址组。
对于 FortiGate-400 或者更高型号的设备，这可以是一个接口、VLAN 子接口或者区域。

3 输入一个用于识别地址组的组名称。
这个名称可以包含数字 (0-9)， 大写或小写字母 (A-Z， a-z)， 以及特殊字符 - 和 _。不能包含其他字符和空格。

4 要添加地址组，在可用地址列表中选择一个地址，单击右箭头将它添加到成员列表。

5 要从地址组中删除地址，从成员列表中选择一个地址，然后单击左箭头以将它从组中删除。

6 单击确定以添加这个地址组。

使用 CLI：

```
set firewall addrgrp <接口_字符串> <地址_组_字符串> member <成员_字符串>,[< 成员 _ 字符串 >,< 成员 _ 字符串 >,...]
```

添加一个目的地址

添加一个 PPTP 用户可以连接到的地址。

1 进入 **防火墙 > 地址。**

2 选择一个内部接口或者 DMZ 接口。（对于不同型号的的 FortiGate，方法一些差别。）

3 单击新建以添加新的地址。

4 为本地 VPN 的内部接口上的单个电脑或一个子网输入地址名，IP 地址和网络掩码。

5 单击确定以保存目的地址。

使用 CLI：

```
set firewall address <接口_字符串> <名称_字符串> subnet <子网地址 _ip> < 网络掩码 _ip>
```

添加一个防火墙策略

添加一个指定了源地址和目的地址的策略，并将策略的服务类型设置为 PPTP VPN 通道内的通讯类型。

1 进入 **防火墙 > 策略。**

2 选择您要添加策略的策略列表。（对于不同型号的的 FortiGate，方法一些差别。）

3 单击新建以添加新的策略。

4 将源地址设置为与 PPTP 地址范围匹配的组。

5 将目的地址设置为 PPTP 用户可以连接到的地址。

6 将服务设置为与 PPTP VPN 通道内的通讯匹配的类型。
例如，如果 PPTP 用户可以访问网页，选择 HTTP。

7 将动作设置为 接受。

8 如果需要地址转换则选择 NAT。
您还可以配置 PPTP 策略的流量控制、记录日志以及病毒防护和网页内容过滤。

9 单击确定以保存防火墙策略。

使用 CLI：

```
set firewall policy status {enable | disable}
srcaddr <源地址名称_字符串> dstaddr <目的地址名称_字符串> schedule <时间表名称_字符串> service <服务名称_字符串> action encrypt
trafficshaping {enable | disable} gbandwidth <保证带宽_整数> maxbandwidth<最大带宽_整数> priority {high | medium | low}
logtraffic {enable | disable}
avwebfilter {enable <配置文件名_字符串> | disable}
vpntunnel <通道名_字符串>
inbound {allow | deny} natinbound {enable | disable} outbound {allow | deny} natoutbound {enable | disable}
```

配置 PPTP 的 Windows98 客户端

按照以下步骤配置运行Windows98 操作系统的电脑以使得它可以连接到FortiGate PPTP VPN。为了配置 Windows98 的客户端，您必须安装和配置 Windows 拨号网络和虚拟专用网络支持。

安装 PPTP 支持

1. 进入**开始** > **设置** > **控制面板** > **网络**。
2. 选择**添加**。
3. 选择**网络适配器**。
4. 选择**添加**。
5. 选择**微软公司**作为供应商。
6. 选择**微软虚拟专用网络适配器**。
7. 单击两次**确定**。
8. 如果需要的话插入软盘或者 CD。
9. 重新启动电脑。

配置 PPTP 拨号连接

1. 进入**我的电脑** > **拨号 网络** > **配置**。
2. 双击**新建拨号连接**。
3. 为连接起一个**名字**，然后单击**下一步**。
4. 输入要连接到的 FortiGate 的主机名或者 IP 地址，然后单击**下一步**。
5. 单击**完成**。

   在拨号网络文件夹将出现新的连接的 **图标**。
6. 鼠标右键单击新图标，选择 **属性**。
7. 转到**服务器类型**。
8. 取消对 **IPX/SPX 兼容** 的选中。
9. 选择 **TCP/IP 设置**。

10 取消对 **IP 头压缩** 的选中。
11 取消对 **使用远程网络的默认网关** 的选中。
12 单击两次 **确定**。

连接到 PPTP VPN

1 启动您在上面步骤中刚刚建立的拨号连接。
2 输入您的 PPTP VPN 用户名和密码。
3 单击 **连接**。

配置 Windows2000 的 PPTP 客户端

按照以下步骤配置运行 Windows2000 操作系统的电脑以使它可以连接到 FortiGate PPTP VPN 上。

配置 PPTP 拨号网络连接

1 进入**开始 > 设置 > 网络 与拨号连接**。
2 双击 **建立新连接** 以启动网络连接向导，单击 **下一步**。
3 在 **网络连接类型** 选项，选择 **通过互联网连接到专用网络**，单击 **下一步**。
4 在 **目的地址**一项，输入要连接的 FortiGate 的主机名或者 IP 地址，单击 **下一步**。
5 设置 **只有我能使用此连接**，单击 **下一步**。
6 单击 **完成**。
7 在连接窗口，选择 **属性**。
8 选择 安全 **属性页**。
9 取消对 **需要数据加密** 的选中。
10 单击 确定。

连接到 PPTP VPN

1 启动您在上面步骤中刚刚建立的拨号连接。
2 输入您的 PPTP VPN 用户名和密码。
3 单击 **连接**。
4 在连接窗口，输入您用来连接到您的拨号网络连接的用户名 和密码。
这个用户名和密码不同于您的 VPN 用户名和密码。

配置 WindowsXP 的 PPTP 客户端

按照以下步骤配置运行 WindowsXP 操作系统的电脑，即可连接到 FortiGate PPTP VPN。

配置一个 PPTP 拨号网络连接

1 进入**开始 > 控制面板**。
2 选择 **网络和互联网连接**。

3 选择 **建立一个您的工作间的网络连接**，单击 **下一步**。
4 选择 **虚拟专用网络连接**， 单击 **下一步**。
5 为连接输入一个名字，单击 **下一步**。
6 如果弹出公共网络对话框，选择 **自动初始化连接**， 单击 **下一步**。
7 在 VPN 服务器选择 **对话框**，输入您要连接到的 FortiGate 的主机名或者 IP 地址，单击 **下一步**。
8 单击 **完成**。

配置 VPN 连接

1 鼠标右键单击您在上面操作中创建的连接图标。
2 选择 **属性** > **安全**。
3 选择 **常规** 以进行常规设置。
4 选择 **需要数据加密**。

注意：如果是用 RADIUS 服务器进行认证，不要选择 需要数据加密。RADIUS 服务器认证不支持 PPTP 加密。

5 单击 **高级** 以配置高级设置。
6 单击 **设置**。
7 选择 **挑战握手认证协议** (CHAP)。
8 确定没有选中其它设置。
9 选择 **网络** 属性页。
10 确定以下选项已经被选中了：
- TCP/IP
- QoS 数据包调度程序

11 确定以下选项没有没选中：
- 微软网络的文件和打印共享
- 微软网络客户

12 单击 **确定**。

连接到 PPTP VPN

1 连接到您的 ISP。
2 启动您在上面步骤中刚刚配置的 VPN 连接。
3 输入您的 PPTP VPN 用户名和密码。
4 单击 **连接**。
5 在 **连接** 窗口，输入您用来连接到您的 拨号网络连接 的用户名和密码。
这个用户名和密码不同于 VPN 连接的用户名和密码。

第二层隧道协议（L2TP）概述

使用 L2TP 虚拟专用网络 (VPN)，您可以在运行微软 Windows 操作系统的客户端计算机和您的内部网络之间创建一个安全的连接。

数年前 CISCO 创建了一套与 PPTP 竞争的协议，称做 L2F。L2F 现在已经被取代了。它的替代者是 L2TP，L2TP 从 L2F 和 PPTP 中借用了相应的元素来创建一个更高级的 VPN 通道协议。大多数较新版本的 Windows 操作系统都支持 L2TP。

VPN 通过将通过安全通道的数据加密来保证它的机密性。此外，认证可以保证数据是来自于原始的发送者，并且在传送过程中没有被破坏或者篡改。当一台客户端计算机连接到一个 VPN 通道时，它看起来就象直接连接到内部网络的一台客户端计算机。

有些 L2TP 的实现方式支持了 IPSec 的一些基本元素。当与 FortiGate 设备协同使用 L2TP 时必须禁用这些元素。

注意：只有在 NAT/ 路由模式下才支持 L2TP VPN。

L2TP 一般配置步骤

一个 L2TP VPN 配置的构成包括一个包含了要被认证的 L2TP 客户端的用户组，一个当 L2TP 连接到内部网络时分配给它们的地址范围，以及一个指定外部源地址的防火墙策略。作为添加的策略的一部分，您需要在 FortiGate 设备上添加源地址和目的地址。

按照如下步骤创建一个 L2TP VPN 配置

1 添加一个用户组。

T 在 L2TP 客户端被允许启动一个 VPN 通道之前，它必须通过认证。要启用认证，您必须在 FortiGate 设备上添加一个用户组。在这个用户组中，为每个 L2TP 客户端添加一个用户。您可以将用户添加到 FortiGate 用户数据库，或者认证服务器 （RADIUS 或者 LDAP），或者在两个地方都添加。

请见 第 142 页 “添加一个用户”和 第 142 页 “添加一个用户组”。

2 启用 L2TP 并指定一个 L2TP 地址范围。

L2TP 地址范围是为远程 L2TP 客户端保留的一个地址范围。当一个远程 L2TP 客户端使用 L2TP 连接到内部网络时，这个客户端电脑被从这个范围内分配一个地址。L2TP 地址范围可以在任何子网内。

请见 第 143 页 “启用 L2TP 并指定一个地址范围”。

3 添加一个防火墙策略。

要创建一个防火墙策略，您必须添加如下内容：源地址；目的地址；指定了源地址和目的地址的防火墙策略。

- 源地址由 L2TP 地址范围构成。将它们添加到外部区域。在添加完单独的 L2TP 地址之后，将它们汇总到一个地址组中。这使得您可以对整个 L2TP 地址范围使用单一的防火墙策略，胜过每个地址一个策略。（或者，如果 L2TP 地址范围由整个一个子网组成，添加这个子网的地址。不要添加一个地址组。）

  请见 第 143 页 “ 添加源地址” 和 第 144 页 “ 添加一个地址组” 。
- 目的地址是 PPTP 客户端可以连接到的地址。将它们添加到除了外部区域以外的任何区域。例如，如果目的地址位于内部网络中，您可以创建一个外部 -> 内部的策略以控制 L2TP 通过 FortiGate 设备的访问。典型情况下您可以为整个内部子网络只添加一个目的地址。

  请见 第 144 页 “ 添加一个目的地址” 。
- 防火墙策略指定了源地址和目的地址，并设置了策略的服务选项以指定 L2TP VPN 通道内部的通讯的类型。例如，如果您希望 PPTP 客户端可以访问一个网页服务器，就将服务设置为 HTTP。

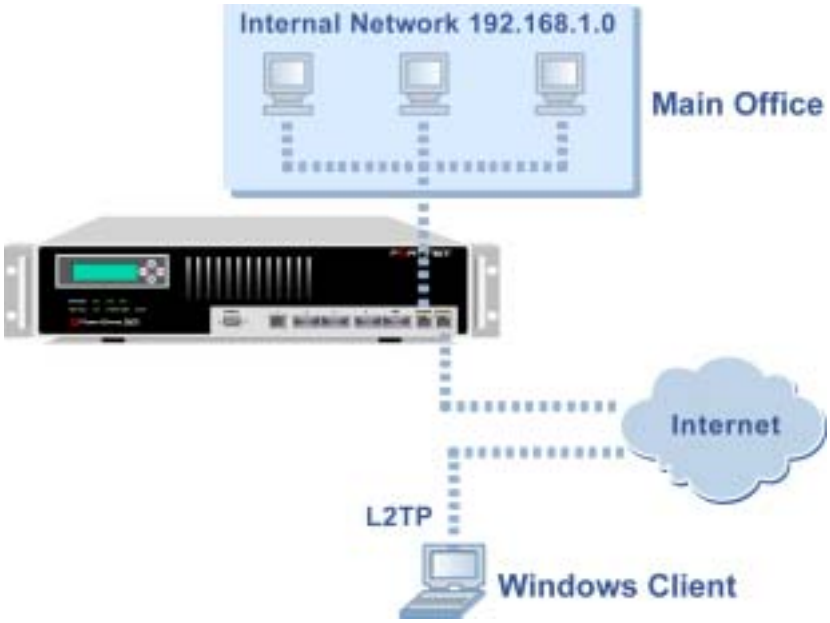
  请见 第 144 页 “ 添加一个防火墙策略” 。

4 配置一个 Windows 客户端。在以下两种配置中选择：

- 配置 Windows2000 客户的 L2TP
- 配置 WindowsXP 客户的 L2TP

注意：确保您的 ISP 支持 L2TP 连接。

图 25: Windows 客户端和 FortiGate 设备之间的 L2TP VPN



把 FortiGate 配置为 L2TP 网关

添加一个用户

按照如下步骤为每个 L2TP 客户端添加一个用户

1 进入**用户 > 本地。**

2 单击新建以添加一个新的用户名。

3 输入这个用户名。

4 选择以下认证配置之一：

密码	输入用户用于认证的密码。这个密码的长度不得少于 6 个字符。这个密码可以包含数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符和空格符。
Radius	用于要求用户取得 LDAP 服务器的认证。选择用于用户认证的 LDAP 服务器的名字。您只能选择一个已经添加到 FortiGate LDAP 配置中的 LDAP 服务器。有关的详细信息请参阅您的 FortiGate 设备随机附带的 《FortiGate 安装和配置指南》。
LDAP	用于要求用户取得 RADIUS 服务器的认证。选择用于用户认证的 RADIUS 服务器的名字。您只能选择一个已经添加到 FortiGate RADIUS 配置中的 RADIUS 服务器。有关的详细信息请参阅您的 FortiGate 设备随机附带的 《FortiGate 安装和配置指南》。

注意：如果实现了 LDAP，那么必须在客户端、网关和 LDAP 服务器之间使用 PAP 来加密消息。不支持其他的加密方法，例如 CHAP 或者 MS-CHAP。

5 如果您希望 FortiGate 在连接 RADIUS 服务器失败时尝试连接 FortiGate RADIUS 配置中的其它 RADIUS 服务器，可以选择 如果选用的服务器连接失败则尝试连接其它服务器。

6 单击确定。

使用 CLI：

```
set user local <名称_字符串> [status {enable | disable}]
[tryother {enable | disable}] type {password | radius | ldap} {<
密码_字符串> | <radius 服务器名_字符串> | <ldap 服务器名_字符串>}
```

添加一个用户组

按照如下步骤为 L2TP 客户端添加一个用户组

1 进入 **用户 > 用户组**。

2 单击 **新建** 以添加新的用户组。

3 输入一个用于识别此用户组的 **组名** 。

这个组名可以是数字 （0-9），大写和小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不能使用其它特殊字符和空格符。

4 要向这个用户组中添加 **用户** ，需从 **有效用户列表** 中选择用户，然后单击右箭头将用户名添加到成员列表中。

5 要向用户组中添加 RADIUS 服务器或者 LDAP 服务器，从 **有效用户列表** 中选择服务器名然后单击右箭头将 RADIUS 服务器添加到成员列表中。

6 单击 **确定** 。

使用 CLI：

```
set user group <组名_字符串> member <名称_字符串> [<名称_字符串>,<名称_字符串>,...]
```

启用 L2TP 并指定一个地址范围

1 进入 **VPN > L2TP > L2TP 范围。**

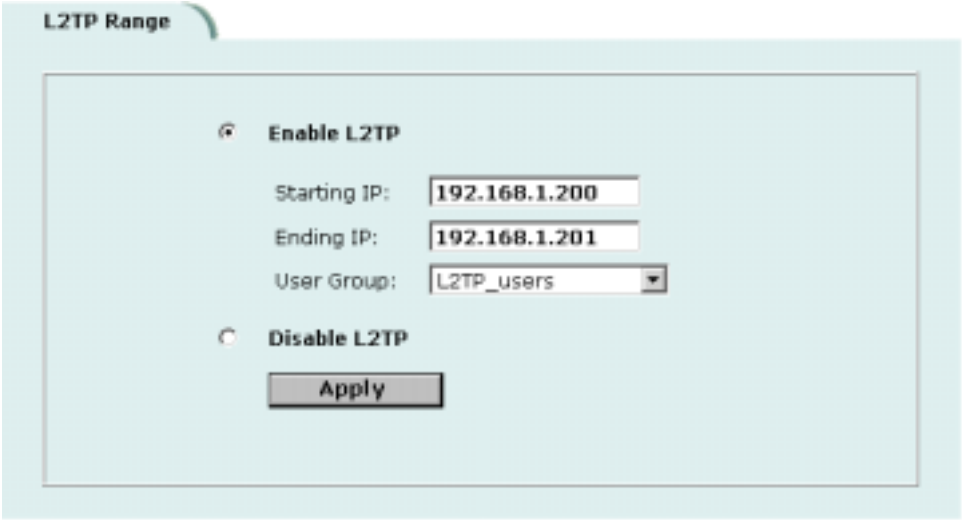
2 单击启用 L2TP。

3 输入 L2TP 地址范围的 **起点 IP 地址** 和 **终点 IP 地址**。

4 选择您在 第 134 页 “ 添加一个用户组” 添加的用户组。

5 单击**应用** 以启动通过 FortiGate 的 L2TP。

图 26: L2TP 地址范围配置的例子



使用 CLI：

```
set vpn l2tp [status {enable | disable}] sip <启始_ip> eip <终止_ip> usrgrp <名称_字符串>
```

添加源地址

对 L2TP 地址范围中的每个地址添加一个源地址。

1 进入 **防火墙 > 地址**。

2 选择 L2TP 客户要连接到的接口。
对于 FortiGate-400 或者更高型号的设备，这可以是接口、VLAN 子接口或区域。

3 单击新建以添加一个地址。

4 为 L2TP 地址范围内的一个地址输入地址名，IP 地址和网络掩码。

5 单击确定以保存源地址。

6 对 PPTP 地址范围内的所有地址重复上述步骤。

注意：如果 L2TP 地址范围包含某个子网的全部地址，您可以添加这个子网的地址。不要添加地址组。

使用 CLI：

```
set firewall address <接口_字符串> <名称_字符串> subnet <子网地址_ip> < 网络掩码 _ip>
```

添加一个地址组

将源地址编进地址组。

1 进入 **防火墙 > 地址 > 组**。

2 在 L2TP 客户连接到的网络接口添加一个新的地址组。
对于 FortiGate-400 或者更高型号的设备，这可以是接口、VLAN 子接口或区域。

3 输入一个用于识别地址组的组名称。
这个名称可以包含数字 (0-9)， 大写或小写字母 (A-Z， a-z)， 以及特殊字符 - 和 _。不能包含其他字符和空格。

4 要添加地址组，在可用地址列表中选择一个地址，单击右箭头将它添加到成员列表。

5 要从地址组中删除地址，从成员列表中选择一个地址，然后单击左箭头以将它从组中删除。

6 单击确定以添加这个地址组。

使用 CLI：

```
set firewall addrgrp <接口_字符串> <地址组_字符串> member <成员_字符串>,[< 成员 _ 字符串 >,< 成员 _ 字符串 >,...]
```

添加一个目的地址

添加一个 L2TP 用户可以连接到的地址。

1 进入 **防火墙 > 地址**。

2 选择一个内部接口或者 DMZ 接口。（对于不同型号的的 FortiGate，方法一些差别。）

3 单击新建以添加新的地址。

4 为本地 VPN 的内部接口上的单个电脑或一个子网输入地址名，IP 地址和网络掩码。

5 单击确定以保存目的地址。

使用 CLI：

```
set firewall address <接口_字符串> <名称_字符串> subnet <子网地址_ip> < 网络掩码 _ip>
```

添加一个防火墙策略

添加一个指定了源地址和目的地址的策略，并将策略的服务类型设置为 L2TP VPN 通道内的通讯类型。

1 进入 **防火墙 > 策略**。

2 选择您要添加策略的策略列表。（对于不同型号的的 FortiGate，方法一些差别。）

3 单击新建以添加新的策略。

4 将源地址设置为与 L2TP 地址范围匹配的组。

5 将目的地址设置为 L2TP 用户可以连接到的地址。

6 将服务设置为与 L2TP VPN 通道内的通讯匹配的类型。

例如，如果 PPTP 用户可以访问网页，选择 HTTP。

7 将动作设置为 接受。

8 如果需要地址转换则选择 NAT。

您还可以配置 PPTP 策略的流量控制、记录日志以及病毒防护和网页内容过滤。

9 单击确定以保存防火墙策略。

使用 CLI：

```
set firewall policy status {enable | disable}
srcaddr <源地址名_字符串> dstaddr <目的地址名_字符串> schedule <时间表 _ 字符串 > service < 服务名 _ 字符串 > action encrypt
trafficshaping {enable | disable} gbandwidth < 保证带宽 _ 整数 > maxbandwidth< 最大带宽 _ 整数 > priority {high | medium | low}
logtraffic {enable | disable}
avwebfilter {enable < 配置文件名 _ 字符串 > | disable}
vpntunnel < 通道名 _ 字符串 >
inbound {allow | deny} natinbound {enable | disable} outbound {allow | deny} natoutbound {enable | disable}
```

配置 Windows2000 客户的 L2TP

按照以下步骤配置运行 Windows2000 的电脑，使得它能够连接到 FortiGate L2TP VPN。

配置 L2TP 拨号连接

1 进入**开始 > 设置 > 网络 与拨号连接**。

2 双击 **新建连接** 以启动网络连接向导，单击 **下一步**。

3 在 **网络连接类型** 中，选择 通过互联网连接到专用网络 ，单击 **下一步**。

4 在 **目的地址** 一栏，输入您要连接的 FortiGate 的地址，单击 **下一步**。

5 将连接设置为 **只有我自己可以使用此连接**，单击 **下一步**。

6 单击 **完成**。

7 在连接窗口，单击 **属性**。

8 选择 **安全** 属性页。

9 确定 **需要数据加密** 已经被选中了。

10 选择 **网络** 属性页。

注意： 如果使用 RADIUS 服务器做认证，不要选择 需要数据加密。 RADIUS 服务器认证不支持 L2TP 加密。

11 将 VPN 服务器类型设置为第二层隧道协议 (L2TP)。

12 保存您所做的修改，继续以下操作。

禁用 IPSec

1 选择 **网络** 属性页。

2 选择互联网协议 (TCP/IP) 属性。

3 双击 **高级** 属性页。

4 进入**选项** 页，选择 **IP 安全** 属性。

5 确认 **不使用 IPSec** 被选中了。

6 单击 **确定** 关闭连接属性窗口。

注意：缺省的 Windows2000L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密。您可以通过修改 Windows2000 注册表来禁用缺省的行为。具体方法在下面步骤中讨论。在修改 Windows 注册表之前请详细查阅 Windows 文档。

7 使用注册表编辑器 (regedit) 在注册表中定位以下主键：
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\
Parameters
```

8 为这个键添加以下键值：
```
Value Name: ProhibitIPSec
Data Type: REG_DWORD
Value: 1
```

9 保存您所做的修改，重新启动电脑以使改动生效。
您必须添加 ProhibitIpSec 注册表键值到每个要使用 L2TP 和 IPSec 的运行 Windows2000 操作系统的电脑。以防止 L2TP 或 IPSec 连接在启动时起用自动过滤功能。当 ProhibitIpSec 注册键值被设置为 1 的时候，您的 Windows2000 电脑不生成使用 CA 认证的自动过滤器，取而代之的是，它检查本地或者活动目录上的 IPSec 策略。

连接到 L2TP VPN

1 启动您在前面步骤中创建的拨号连接。

2 输入您的 L2TP 用户名和密码。

3 单击 **连接**。

4 在连接窗口，输入您的拨号网络连接的用户名和密码。
这个用户名和密码不同于您的 L2TP VPN 用户名和密码。

配置 WindowsXP 客户的 L2TP

按照以下步骤配置运行 WindowsXP 系统的电脑使得它能够连接到 FortiGate L2TP VPN。

配置 L2TP VPN 拨号网络连接

1 进入**开始 > 设置**。

2 选择 **网络和互联网连接**。

3 选择 **建立一个您的工作间的网络连接**，单击 **下一步**。

4 一选择 **虚拟专用网络连接**， 单击 **下一步**。
5 为连接输入一个名字，单击 **下一步**。
6 如果弹出公共网络对话框，选择 **自动初始化连接**， 单击 **下一步**。
7 在 VPN 服务器选择 对话框，输入您要连接到的 FortiGate 的主机名或者 IP 地址，单击 **下一步**。
8 单击 **完成**。

配置 VPN 连接

1 鼠标右键单击您在上面操作中创建的连接图标。
2 选择 **属性** > **安全**。
3 选择 **常规** 以进行常规设置。
4 选择 **需要数据加密**。

注意： 如果是用 RADIUS 服务器进行认证，不要选择 需要数据加密。RADIUS 服务器认证不支持 PPTP 加密

5 单击 **高级** 以配置高级设置。
6 选择 **设置**。
7 选择 **挑战握手认证协议** (CHAP)。
8 确认没有选中其它设置。
9 选择 **网络** 属性页。
10 确认以下选项被选中了：
- TCP/IP
- QoS 数据包调度

11 确认以下选项没有被选中：
- 微软网络文件和打印共享
- 微软网络客户

禁用 IPSec

1 选择 **网络** 标签。
2 选择互联网 （TCP/IP）协议属性。
3 双击 **高级** 标签。
4 进入 **选项标签**，选择 IP 安全 属性。
5 确认 **不使用 IPSec** 被选中了。
6 单击 **确定** 关闭连接属性对话框。

注意： 缺省的 WindowsXP L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密。您可以通过修改 WindowsXP 注册表来禁用缺省的行为。具体方法在下面步骤中讨论。在修改 Windows 注册表之前请详细查阅 Windows 文档。

7 使用注册表编辑器 （regedit）定位注册表中的以下主键：
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`

8 添加以下键值：
`Value Name: ProhibitIPSec`
`Data Type: REG_DWORD`
`Value: 1`

9 保存您所做的改动并重新启动电脑以使修改生效。

您必须添加 ProhibitIpSec 注册表键值到每个要使用 L2TP 和 IPSec 的运行 WindowsXP 操作系统的电脑。以防止 L2TP 或 IPSec 连接在启动时起用自动过滤功能。当 ProhibitIpSec 注册键值被设置为 1 的时候，您的 WindowsXP 电脑不生成使用 CA 认证的自动过滤器，取而代之的是，它检查本地或者活动目录上的 IPSec 策略。

连接到 L2TP VPN

1 连接到您的 ISP。

2 启动您在前面步骤中创建的拨号连接。

3 输入您的 L2TP VPN 用户名和密码。

4 单击 **连接**。

5 在连接窗口，输入您的拨号网络连接的用户名和密码。
这个用户名和密码不同于您的 VPN 用户名和密码。

VPN 监视和故障排除

本章提供了一些常用的 VPN 维护和监视方法。

本章叙述了如下内容：

查看 VPN 通道状态

您可以使用 IPSec VPN 通道列表查看所有 IPSec 自动密钥 VPN 通道的状态。对于每个通道，列表中都显示了通道的状态以及通道超时。

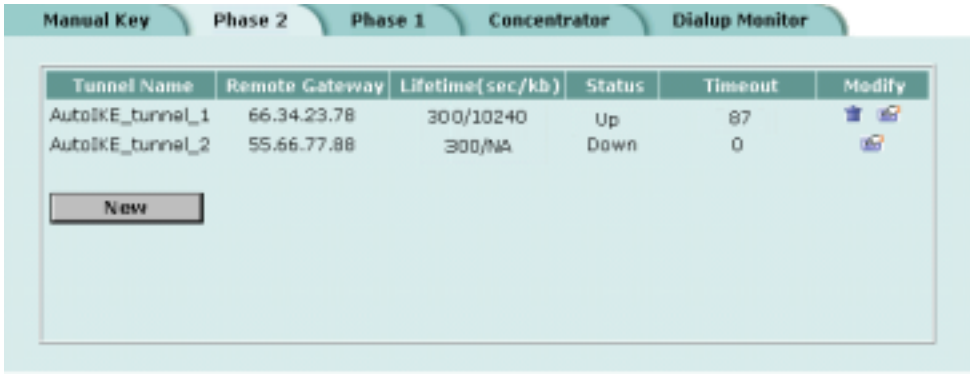
以下操作用于查看通道状态

1 进入 **VPN > IPSEC > 第二阶段**。

在 状态 列显示了每个通道的状态。如果状态是 **向上**，则通道是激活的，如果状态是**向下**，则通道是非激活的。

在 超时 列显示了下次密钥交换时间的剩余时间。这个时间的计算方法是从密钥有效期中减去自上次密钥交换以来经历过的时间。

图 27: 自动 IKE 密钥通道状态



查看拨号 VPN 连接的状态

您可以使用拨号监视器查看拨号 VPN 的连接状态。拨号监视器列出了远程网关和每个网关上处于活动状态的 VPN 通道。监视器上还列出了每个通道的通道有效期、超时、源代理 ID 和目的代理 ID。

按以下步骤查看拨号连接状态

1 进入 **VPN > IPSec > 拨号。**

有效期 列显示了这个连接建立以来经历的时间。

超时 列显示了下次密钥交换之前剩下的时间。这个时间等于密钥有效期减去上次密钥交换以来经历的时间。

源代理 ID 列 显示了远端的实际的 IP 地址或者子网地址。

目的代理 ID 列 显示了本地院的实际 IP 地址或者子网地址。

图 28: 拨号监视器

测试 VPN

为了确认位于两个网络之间的 VPN 是否配置正确，可以使用 PING 命令从一个内部网络连接另一个内部网络中的一台计算机。当 FortiGate 收到第一个发往 VPN 的数据包时，就会发起 VPN 连接。

为了确认一个在网络和一个或多个远程用户之间的 VPN 是否配置正确，可以发起一个 VPN 客户端连接然后使用 PING 命令连接到内部网络中的一台电脑上。当客户试图连接时，VPN 通道会自动初始化。您只需从客户端 PING 内部网络中的一台电脑就可以同时发起这个通道并测试它。

将 VPN 事件记录日志

您可以将 FortiGate 设备配置为将 IPSec 和 PPTP/L2TP VPN 事件记录日志。IPSec VPN 事件的日志记录包括：第一阶段和第二阶段协商 （例如，加密和认证算法）。PPTP/L2TP 事件的日志记录包括：连接、通道状态 （启动 / 关闭）。

按照如下操作记录 VPN 事件日志

1 进入 **日志和报告 > 日志设置。**

2 选择日志的一个目的地。

在以下选项中选择：

- 记录到远程主机
- 以 WebTrends 增强格式日志记录
- 记录到内存

3 根据您选择的目的地，单击配置策略。

4 选择事件日志和 IPSec 协商事件。

5 单击确定以保存您所做的修改。

术语表

连接： 两台电脑之间、应用程序之间、进程之间或者其他诸如此类的对象之间的物理上或逻辑上的联系，或者两者都有的联系。

DMZ，非军事区： 用来提供互联网服务而无须允许对内部（私有）网络的未经授权的访问。典型情况下，DMZ 包含了可以访问互联网的服务器，例如网页服务器（HTTP），文件传输服务器（FTP），邮件服务器（SMTP）和域名解析服务器（DNS）。

DMZ 接口： FortiGate 上连接到 DMZ 网络的接口。

DNS，域名解析服务： 把用字母表示的节点名转换为 IP 地址的服务。

以太网： 一个局域网（LAN），使用总线型或星型拓扑结构，支持 10Mbps 的传输速率。以太网是被广泛应用的局域网标准之一。新版本的以太网被称做 100 Base-T（或快速以太网），支持 100 Mbps 的数据传输速率。而最新的标准，千兆以太网，支持每秒 1 吉（1,000 兆比特）的数据传输速率。

外部接口： FortiGate 连接到互联网的网络接口。

FTP，文件传输协议： 一个 TCP/IP 协议和应用程序，用于上载或下载文件。

网关： 它包括相应的软件和硬件，用来连接不同的网络。例如，TCP/IP 网络之间的网关可以连接不同的子网。

HTTP，超文本传输协议： 被万维网（WWW）所使用的协议。HTTP 定义了消息的格式和传输方式，以及服务器和浏览器应当如何对不同的命令作出响应。

HTTPS：使用网页浏览器跨过互联网传输私人文件的 SSL 协议。

内部接口： FortiGate 用于连接到内部（私有）网络的网络接口。

互联网： 以 NFSNET 为骨干网，覆盖全球的彼此连接的网络总称。在一般的术语中，也可以表示一些互相连接的网络。

IICMP，互联网控制信息协议： 互联网协议（IP）的一部分。它一般被用来发送错误信息、测试数据包以及一些与 IP 有关的信息。当 PING 功能发送 ICMP 响应请求到网络中的一台主机时会用到这一协议。

IKE，互联网密钥交换： 一种在两台安全服务器之间自动交换认证密钥和加密密钥的方法。

IMAP，互联网消息访问协议： 一种互联网电子邮件协议，用来通过任何兼容 IMAP 的浏览器访问您的电子邮件。使用 IMAP 时，您的电子邮件保存在服务器上。

IP，互联网协议：TCP/IP 协议的一部分，处理数据包路由。

IP 地址： 在 TCP/IP 网络中的一台电脑或者设备的识别标志。IP 地址是一个 32 比特的数字地址，通常写成用小数点分隔的四个数字。每个数字都可以是从 0 到 255 中的任何一个。

L2TP，第二层通道协议： 点对点传输协议（PPTP）的扩展，允许互联网服务供应商通过它操作虚拟专用网络（VPN）。L2TP 融合了微软公司的 PPTP 和思科公司的 L2F 系统。要建立一个 L2TP VPN，您的互联网服务供应商的路由器必须支持 L2TP。

IPSec，互联网协议安全： 支持 IP 层上的数据包安全交换的一组协议。IPSec 通常用来支持 VPN。

LAN，局域网：在一个较小范围内建立的网络。大多数局域网连接工作站和个人电脑。局域网上的每个电脑都可以访问位于局域网上任何位置的任何数据和设备。这意味着大多数用户可以把他们的数据象打印机那样的物理资源一样共享。

MAC 地址，介质访问控制地址： 用来唯一识别网络上的每个节点的硬件地址。

MIB，管理信息数据库：可以被简单网络管理协议（SNMP）网络管理程序监控的对象的数据库。

调制解调器： 可以把数字信号转换成模拟信号和把模拟信号转换成数字信号并通过电话线路传输的设备。

MTU，最大传输单元： 一个网络可以传输的数据包的最大物理尺寸，以字节为单位。任何大于 MTU 的数据包在发送之前都会被分成较小的数据包。理想情况下，网络中的 MTU 应当等于从您的电脑到目的地之间所经过的所有网络中的最小 MTU。如果您的消息大于其中的任何一个 MTU，它们会把它分割 （破碎），这将会减慢传输速度。

网络掩码： 也称做子网掩码。忽略了一个完整的 IP 地址中的一部分的一组规则，从而可以无须广播就可以达到目的地址。它表示一个大的 TCP/IP 网络中的子网部分。有时用来表示一个地址掩码。

NTP，网络时间协议： 用来把一台电脑的时间同步为 NTP 服务器的时间。NTP 互联网提供精确到十毫秒以内的互联网时间 （UTC）。

包： 通过包交换网络传送的消息的一部分。包的一个关键特征是它除了数据之外还包含了目的地的地址。在 IP 网络中包通常被称做数据包。

Ping，数据包互联网分组： 一个用来判定特定 IP 地址是否可以访问的工具。它的工作原理是向指定的地址发送一个数据包并等待回复。

POP3，邮局协议： 用于从邮件服务器通过互联网向邮件客户端传输电子邮件的协议。多数电子邮件客户端使用 POP 协议。

PPP，点对点传输协议： 提供了主机到网络和路由器到路由器的连接的 TCP/IP 协议。

PPTP，点对点通道协议： 基于 Windows 的建立虚拟专用网络的技术。Windows98，Windows2000 和 WindowsXP 都支持 PPTP 协议。要建立 PPTP 虚拟专用网络，您的 ISP 的路由器必须支持 PPTP。

端口： 在 TCP/IP 和 UDP 网络中，端口是逻辑连接的终点。端口号标识了端口的类型。例如，80 端口用于 HTTP 协议的数据传输。

协议：两个设备之间商定的传输数据的格式。协议决定了要使用的错误检测的类型，数据压缩的方法 （如果有的话），发送设备如何指示它完成了一个消息的发送，接收设备如何指示它已经完成了一个消息的接收。

RADIUS，远程拨号访问用户认证服务： 很多 INTERNET 服务供应商 （ISP）使用的认证和计帐系统。当用户拨入一个 ISP 时，他们输入一个用户名和密码。这些信息被传送到 RADIUS 服务器，RADIUS 检验这些信息的正确性，然后授予访问 ISP 系统的权限。

路由器： 把局域往连接到互联网并为他们之间的数据提供路由的设备。

路由： 决定发送数据到目的地时要经过的路径的过程。

路由表：含有一系列有效的数据传送路径的列表。

服务： 应答其他设备 （客户）的请求的应用程序。通常用来描述任何在网络上提供类似打印、海量存储、网络访问等服务的设备。

SMTP，简单邮件传输协议：在 TCP/IP 网络中提供邮件发送服务的程序。

SNMP，简单网络管理协议： 一组网络管理协议。SNMP 对网络的不同部分发送消息。支持 SNMP 的设备，称做代理，把他们自己的数据存储在管理信息库 （MIB）中，并且把这些信息返回给 SNMP 请求的发送者。

SSH，安全命令解释器： 远程登录程序安全的替代品。您可以用它跨过网络登录到其他电脑上并执行命令。SSH 通过安全通道提供了强大的安全认证和安全通信。

子网： 网络具有相同子网地址的部分。在 TCP/IP 网络中，子网定义为所有 IP 地址前缀相同的设备。例如，所有 IP 地址从 100.100.100 开始的设备属于同一子网。从安全和性能角度考虑，把网络分割成子网是必要的。IP 网络使用子网掩码分割子网。

子网地址： IP 地址中标识子网的部分。

TCP，传输控制协议： TCP/IP 网络的主要部分之一。TCP 保证了数据的提交，也保证了数据包能够按照它们被发送时的顺序提交。

UDP，用户数据报协议：一种无连接协议。类似于 TCP，运行于 IP 网络的顶端。与 TCP 协议不同的是，UDP 提供很少的纠错服务，取而代之的是提供了通过 IP 网络发送和接收数据报的直接传输途径。它主要用于在网络上广播消息。

VPN，虚拟专用网： 一个跨越在 INTERNET 上类似于私有网络的网络。VPN 使用加密和其它安全机制来保证只有经过认证的用户可以访问网络，并且数据不会被篡改。

病毒：一种把自己附加到别的程序上的电脑程序，并通过这种机制在电脑中或网络上传播，通常具有有害的企图。

蠕虫：通过电脑网络复制自己的程序或算法，通常使用电子邮件，并且会进行一些恶意的活动，例如耗尽电脑系统的资源并且可能导致系统关闭。

索引

J

K

L

M

N

P

Q

R

S

T

V

W

X

Y

Z