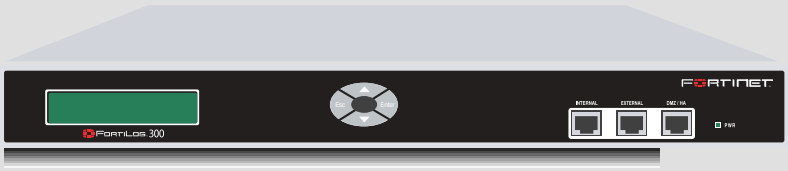
FORTINET™

FortiGate 300

安装和配置指南



FortiGate 用户手册 第一卷

2.50 版
2003 年 7 月 21 日

FortiGate-300 安装和配置指南

2.50 版

2003 年 7 月 21 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

注意：如果更换的电池型号错误，有可能会导致爆炸。请根据使用说明中的规定处理用过的电池。

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

FortiGate 防病毒防火墙支持应用层服务的基于网络的部署，包括防病毒保护和全内容扫描过滤。FortiGate 防病毒防火墙增强了网络的安全性，避免了网络资源的误用和滥用，可以帮助您更好地使用通讯资源而不会降低网络的性能。FortiGate 防病毒防火墙获得了 ICSA 防火墙认证，IP 安全认证和防病毒服务认证。

FortiGate 防病毒防火墙是一个易于管理的安全设备，它提供了一套完整的功能，包括：

- 应用层服务，例如病毒防护和内容过滤，
- 网络曾服务，例如防火墙、入侵检测、VPN，以及流量控制等。

FortiGate 采用了先进的行为加速 （Accelerated Behavior）和内容分析系统技术（ABACAS™），突破了芯片设计、网络通信、安全防御及内容分析等诸多难点。公司所独有的，基于 ASIC 上的网络安全构架能实时进行网络内容和状态分析，并及时启动在网络边界布署的防护关键应用程序，对您的网络进行最有效的安全保护。FortiGate 系列对现有的一些解决方案，如以主机为基础的防病毒保护进行补充，并在大力降低设备，管理和维修成本的同时，为您提供一些新的应用和服务。

FortiGate-300 型在性能、可用性及可靠性上满足了企业级应用的需要。拥有高可用性包括无会话 (Session) 损失的失效自动恢功能，FortiGate-300 是您企业中运行重大关键性任务所需的最佳选择。

防病毒保护

ICSA 认证的 FortiGate 防病毒保护，可将通过 FortiGate 传输的 WEB （HTTP），文件传输 （FTP）和 EMAIL(SMTP, POP3, 和 IMAP ）内容中被病毒感染的文件删除。当 FortiGate 从内容流中检测出病毒时，自动病毒防护功能可以删除那些感染了病毒的文件，用一条病毒感染信息替换掉原来的文件，然后转发到内容流的接收方。Web 和电子邮件内容可以是存在于常规网络通讯中的或者是被封装在 IPSec VPN 通讯流中的。

您还可以提高安全防护的级别，将防病毒保护功能设置为阻塞通过 FortiGate 设备的特定类型的文件。使用这一功能可以阻塞可能含有新型病毒的文件。

如果 FortiGate 设备内配有硬盘，可以将被感染或被阻塞的文件隔离。FortiGate 管理员可以下载被隔离的文件，然后对它们进行病毒扫描，杀毒，再将它们发送给原来的接收者。您也可以将 FortiGate 设备配置为每过一段时间就自动删除被隔离的文件。

当 FortiGate 设备从内容流中检测到病毒并将它删除的时候，它可以向系统管理员发送一封报警邮件。

ICSA LABS 认证了 FortiGates 的以下功能：

- 100% 检测到 The Wild List(www.wildlist.org) 中列举的所有病毒。
- 检测 PKZip 格式压缩文件中的病毒。
- 检测以 UUENCODE 格式编码的 EMAIL 中的病毒。
- 检测以 MIME 格式编码的 EMAIL 中的病毒。
- 在扫描同时对所有动作进行日志记录。

Web 内容过滤

FortiGate Web 内容过滤可设置为扫描 URL 和 WEB 网页内容中的全部 HTTP 内容协议数据流。如果在 URL 阻塞列表中找到与 URL 匹配的条目，或在网页中发现了内容阻塞列表中的词或短语，FortiGate 将阻塞此页。被阻塞的网页会被一条内容阻塞消息所替代，您可以使用基于 Web 的管理程序编辑这个消息。

通过设置 URL 阻塞可以阻挡来自某一网站上的所有或部分网页。利用这一特点，可拒绝某个站点中的部分而不是阻塞整个网站。

为防止无意封锁到一些合法的网页，可将 URLs 添加到一则例外列表中，从而覆盖 URL 封锁及内容封锁列表中的设置。

Web 网页内容过滤也包括脚本过滤，它可以配置为阻塞如下一些非安全 web 内容如 Java 小程序、Cookies、ActiveX。

您还可以使用 Cerberian URL 阻塞去阻塞不受欢迎的 URL。

电子邮件过滤

通过配置 FortiGate 的电子邮件过滤功能，可以扫描所有的 IMAP 和 POP3 邮件内容，找出不受欢迎的发件人或不受欢迎的内容。如果发现某个邮件的发件人地址与电子邮件阻塞列表中的某一项相匹配，或者在邮件的内容中含有和禁忌词汇列表中的词汇相匹配的内容，FortiGate 会在这个邮件的标题栏中添加一个电子邮件标签。接收者可以用他们的电子邮件客户端软件根据这个电子邮件标签过滤不想要的邮件。

对于所有的或部分已知的广告邮件发送组织，您可以通过配置电子邮件阻塞功能在属于这些组织的发件人所发送的电子邮件上添加电子邮件标签。为了避免无意中在正常发件人发送的邮件上加上电子邮件标签，您可以将发件人的地址模板添加到一个排除列表中，以使该发件人发送的邮件不收邮件阻塞功能和禁忌词汇列表的限制。

防火墙

ICSA 认证的 FortiGate 防火墙可以在互联网这个充满敌意的环境中保护您的电脑网络。ISCA 已对 FortiGate 防火墙 4.0 版本授予了证书，确保了 FortiGates 可以成功保护企业网络不受来自公共或其它非信任网络的各种威胁。

在完成 FortiGate 的基本安装后，防火墙可设置为允许用户从受保护内部网络访问 Internet，并同时封锁从 Internet 到内部网的访问。您可对防火墙进行设置，使其对从内部网到 Internet 的访问，和从 Internet 到内部往的访问加以控制。

您可以使用以下选项灵活地配置 FortiGate 安全策略：

- 控制所有进入和输出的网络流通，
- 控制加密的 VPN 流通，
- 应用防病毒保护和 WEB 内容过滤，
- 阻塞或允许对全部策略选项的访问，
- 根据单个策略进行控制，
- 接受或拒绝出入单个地址的流通，
- 单独或成组地控制标准的和用户定义的网络服务，
- 要求用户在获取访问之 前进行用户认证，
- 包含了流通控制用以设置每条策略的访问优先权和带宽保证或带宽限制，
- 包含日志用以逐个追记某策略下的网络连接，
- 包含网络地址转换 / 路由 （NAT/ 路由）模式策略，
- 包含混合 NAT 和路由模式策略。

FortiGate 防火墙支持网络地址转换 / 路由模式或透明模式。

NAT/ 路由模式

在 NAT/ 路由模式下， 您可创建 NAT 模式和路由模式策略。

- NAT 模式策略通过网络地址转换对较不安全网络中的用户隐藏较安全网络中的地址。
- 路由模式策略在不执行地址转换下接受或拒绝网络间的连接。

透明模式

透明模式提供了与 NAT 模式相同的基本防火墙保护。从 FortiGate 中接收到的数据包根据防火墙策略可被智能地转发或阻塞掉。FortiGate 可插入到网络的任何一点而不需要对此网络或其它相关组件做任何的改变。然而，VPN 及一些高级防火墙功能只能在 NAT/ 路由模式下使用。

网络入侵检测系统 （NIDS）

FortiGate 网络入侵侦测系统 (NIDS) 是一种实时网络入侵探测器，它能对外界各种可疑的网络活动进行识别及采取行动。NIDS 通过攻击特征来识别超过 1000 种的攻击。您可以启用或禁止 NIDS 对某一类型的攻击进行检测。还可以自行编写攻击特征从而生成用户自定义的攻击类型检测。

NIDS 可以防止探测、大部分常见的拒绝服务攻击和基于数据包的攻击。您可以启用或禁用预防攻击的特征，和定制攻击检测的灵敏度和其他参数。

为通知系统管理员有攻击，NIDS 将此攻击及一切可疑流通记录到攻击日志中，并根据设置发送报警 EMAIL。

Fortinet 可定期更新攻击数据库。您可下载并手动安装攻击数据库。也可设置 FortiGate 自动查询和下载更新的 IDS 数据库。

虚拟专用网络 （VPN）

使用 FortiGate 虚拟专用网 （VPN），可为您在办公网络和分散的办公室网络、从远程安全通讯系统登陆到公司网的用户或旅行者 之间提供一个安全的网络连接。

FortiGate VPN 包括以下特性：

- 执行行业标准及 ICSA 认证的 IPSec VPN 包括：
  - 在通道模式下的 IPSec，ESP 安全，
  - DES 和 3DES （triple-DES） 加密的硬件加速，
  - HMAC MD5 和 HMAC SHA1 认证和数据整体化，
  - 基于预置密钥隧道的自动密钥交换，
  - 使用本地验证或 CA 验证的 IPSec VPN ，
  - 手工密钥通道，
  - Diffie-Hellman 组 1、2、和 5，
  - 积极模式和主模式，
  - 重放检测，
  - 向前保密，
  - XAuth 认证，
  - 失效对等检测，
- 易于连接的 PPTP，支持为大多数常用的操作系统所支持的 VPN 标准。
- 易于连接的 L2TP，支持为大多数常用的操作系统所支持的更加安全的 VPN 标准。
- 基于 IPSec VPN 流通控制的防火墙策略。
- IPSec NAT 跨越技术使得位于 NAT 后边的远程 IPSec VPN 网关或客户端可以连接到 IPSec VPN 通道。
- 用 VPN 集中器的 VPN 星形连接，可以使 VPN 流通从一个通道经 FortiGate 连接到另一个通道。
- IPSec 冗余可以创建到远程网络的自动密钥交换 IPSec VPN 连接。

高可用性

高可用性 （HA） 提供两个或多个 FortiGate 之间的 失效恢复机制。Fortinet 通过冗余硬件实现 HA 功能，匹配在 NAT/ 路由模式运行下的 FortiGate。您可以将 FortiGates 配置为主动 - 被动 (A-P) 模式或主动 - 主动 (A-A)HA 模式。

A-P 模式和 A-A 模式的 HA 均使用类似的高可用性冗余硬件配置。高可用性软件保证了当 HA 组中一个 FortiGate 失效，所有功能及已建的防火墙连接仍能维持现状。

安全安装、配置、管理

安装过程即快捷又简单。 初次启动 FortiGates 时，它已经配置为使用默认的 IP 地址及安全策略配置。为了使 FortiGate 开始保护您的网络，只需连接到基于 Web 的管理程序，设置操作模式并使用安装向导来配置您网络的 FortiGate IP 地址。在此基础上，可用基于 Web 的管理程序来进行更进一步的配置以满足您更多的需要。

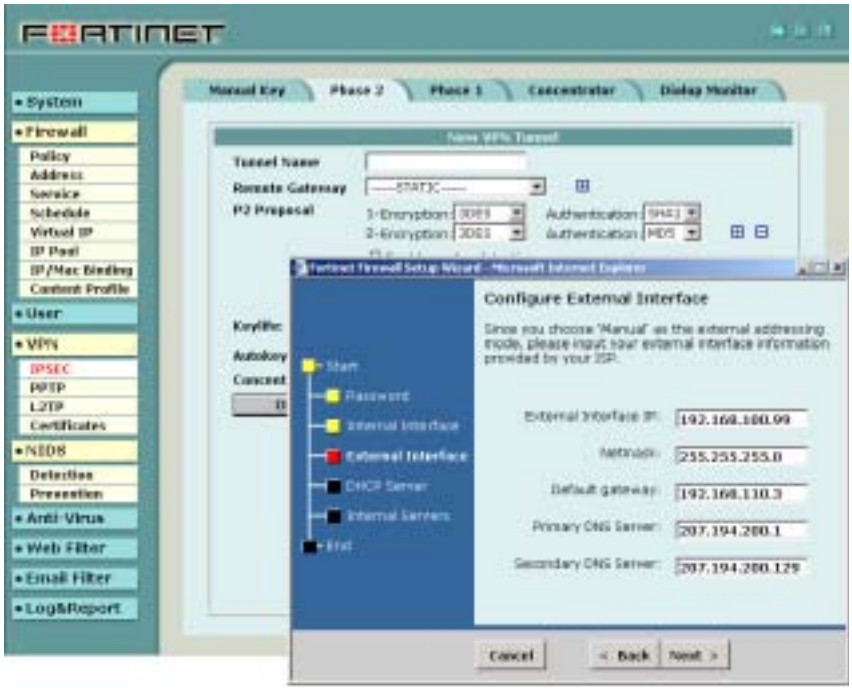
您也可使用 FortiGate 面板上的控制按钮和 LCD 对其进行基本配置。

基于 Web 的管理程序

从任何一个装有 IE 流览器的电脑上以 HTTP 或安全 HTTPS 方式连接到基于 Web 的管理程序，即可对 FortiGates 设备进行配置和管理。基于 Web 的管理程序支持多种语言。您可以从任何 FortiGate 接口将 FortiGate 设备配置为使用 HTTP 或 HTTPs 进行管理维护。

您可以使用基于 Web 的管理程序完成大部分 FortiGate 配置工作。也可以使用基于 Web 的管理程序监视 FortiGate 设备的状态。使用 基于 Web 的管理程序对配置所做的修改会立即生效，而无须重新启动防火墙或中断服务。您可以将已经完成的配置下载并保存。您所保存的设置可以在任何时间恢复到系统中。

图 1: FortiGate 基于 Web 的管理程序 和设置向导



命令行接口 （CLI）

您可以将管理员计算机的串行通讯接口连接到 FortiGate 的 RS-232 串行控制台接口上，从而访问 FortiGate 命令行控制界面 （CLI）。或者也可以使用 Telnet 或者安全的 SSH 连接方式从任何与 FortiGate 连接的网络，包括互联网，中访问 CLI 界面。

CLI 具有和 基于 Web 的管理程序相同的管理和监视功能。另外，您可以使用 CLI 进行一些高级配置工作，这是 基于 Web 的管理程序无法实现的。*安装和配置指南* 中包含了有关基本 CLI 命令和高级 CLI 命令的信息。您可以在 *FortiGate CLI 参考指南* 中找到关于如何连接到 CLI 和如何使用 FortiGate CLI 的更加完整和详细的说明。

日志和报告

FortiGate 支持记录各种类别的流通和配置修改。您可将日志设置如下：

- 报告连接到防火墙接口的通讯，
- 报告被使用的网络服务，
- 报告被防火墙策略允许的通讯，
- 报告被防火墙策略拒绝的通讯，
- 报告配置改变和其它一些管理事件，如 IPSec 通道协商、 病毒检测、攻击、web 网页阻塞，
- 报告被 NIDS 检测到的攻击，
- 向系统管理员发送报警 EMAIL 以报告病毒事件、入侵及防火墙或 VPN 事件及异常违法情况。

日志可被传送到远程系统日志服务器或以 WebTrends 增强日志格式传输到远程 WebTrends NetIQ 安全报告中心和防火墙服务器上。某些型号的防火墙可将日志存储在可选择的内置硬盘上。如果没有安装硬盘，您可配置 FortiGate 日志和报告，把最近的事件记录到共享系统内存中去。

2.50 版本的新特点

本节主要描述了 FortiOS v2.50 中的一些新的特征：

系统管理

- 改善了 FortiGate 系统健康状态监视图象功能，包括 CPU 及内存的使用率，会话数量，网络带宽使用率，以及检测到的病毒和入侵的数量，详细内容请见 第 86 页 “ 系统状态” 。
- 修订了防病毒和攻击定义更新功能，使其连接到新版本的 Fortinet 响应发布网络。现在可以以小时为单位进行定期更新，并且，**系统 > 更新**页面显示关于更新状态的更多的详细信息。详情请见 第 91 页 “ 病毒防护定义和攻击定义更新” 。
- 可以从基于 Web 的管理程序直接连接到 Fortinet 技术支持网页的页面。您可以注册您的 FortiGate 设备并获得访问其他技术支持资源的权利。详情请见 第 100 页 “ 注册 FortiGate 设备” 。

网络配置

- 新的网络接口配置选项，详情请见 第 107 页 “ 配置网络接口” 。
  - 在所有网络接口上的 Ping 服务器和失效网关检测，
  - 从任何接口进行 HTTP 和 Telnet 管理访问，
  - 所有 FortiGate 网络接口的第二个 IP 地址。

路由

- 简单的基于方向的路由配置。
- 高级策略路由配置 （仅限于 CLI）。

DHCP 服务器

- 在 DHCP 配置中添加了 WINS 服务器。

路由信息协议 （RIP）

• 新的 RIP v1 和 v2 功能。详情请见 第 119 页 “ RIP 配置” 。

简单网络管理协议 （SNMP）

• 支持 SNMP v1 和 v2。
• 支持 RFC 1213 和 RFC 2665。
• 监视全部的 FortiGate 配置和功能。
• 详情请见 第 131 页 “ 配置 SNMP” 。

HA

• 主动 - 主动模式的 HA 使用了交换机，并且具有选择时间表的能力
• 透明模式的 HA
• HA 簇的 A/V 更新
• HA 功能的配置同步

详情请见 第 55 页 “ 高可用性” 。

替换信息

您可以定制 FortiGate 设备发送的以下替换信息：

• 当检测到病毒时，
• 当有文件被阻塞时，
• 当一个碎片文件被阻塞时，
• 发送警报邮件时。

详情请见 第 133 页 “ 定制替换信息” 。

防火墙 Firewall

• 防火墙的默认配置有一些改动，详情请见 第 138 页 “ 默认防火墙配置” 。
• 在所有接口上添加了虚拟 IP。详情请见 第 155 页 “ 虚拟 IP” 。
• 为防火墙策略添加了内容配置文件，可以组合有关阻塞、扫描、隔离、网页内容阻塞和电子邮件过滤的有关配置信息。详情请见 第 163 页 “ 内容配置文件” 。

用户和认证

• LDAP 认证。详情请见 第 170 页 “ 配置 LDAP 支持” 。

VPN

关于 FortiGateVPN 功能的详细说明请见 *FortiGate VPN 指南*。新的特性包括：

- 第一阶段
  - AES 加密
  - 证书
  - 高级选项，包括拨号组、对等、Peer, XAUTH, NAT 跨越，DPD
- 第二阶段
  - AES 加密
- 加密策略选择服务
- 生成和导入本地证书
- 导入 CA 证书

NIDS

关于 FortiGate NIDS 功能的完整说明，请见 *FortiGate NIDS 指南* 。新特性包括：

- 攻击检测特征分组
- 用户定义的攻击预防方式
- 在多个接口监视攻击
- 用户定义的攻击检测特征

防病毒

关于 FortiGate 防病毒功能的完整说明请见 *FortiGate 内容保护指南* 。新特性包括：

- 内容配置文件
- 隔离含有病毒的文件或被阻塞的文件
- 阻塞大小超过限制的文件

网页过滤

关于 FortiGate 网页过滤功能的完整说明，请见 *FortiGate 内容保护指南*。新特性包括：

- Cerberian URL 过滤

电子邮件过滤

关于 FortiGate 电子邮件过滤功能的完整说明请见 *FortiGate 内容保护指南*

日志和报告

关于 FortiGate 日志记录的详细说明请见 *FortiGate 日志和消息参考指南*。

- 使用 CSV 格式将日志记录到远程主机
- 日志消息级别：紧急、警报、危急、错误、警告、注意、信息
- 日志级别策略
- 通讯日志过滤
- 新病毒、网页过滤和电子邮件过滤日志
- 支持认证的报警邮件
- 抑制邮件泛滥
- 扩展的 WebTrends 活动图表支持

关于本手册

安装和配置向导描述了如何安装和配置 FortiGate-300。本手册包含以下内容：

- 开始 描述了拆包，安置，和启动 FortiGate。
- NAT/ 路由 模式安装 描述了如果您希望 FortiGate 运行于 NAT/ 路由模式，应当如何安装。
- 透明模式安装 描述了如果您希望 FortiGate 运行于透明模式，应当如何安装。
- 高可用性 描述了如何安装和配置以高可用性方式配置和运行的 FortiGate 设备。
- 系统状态 描述了如何查看您的 FortiGate 设备的当前状态，以及相关的系统进度，包括安装更新的 FortiGate 固件，备份和恢复系统设置，在透明模式和 NAT/ 路由模式间切换等等。
- 病毒和攻击定义升级及注册 描述了病毒和攻击定义自动更新的配置方法。本章还包括了连接到 FortiGate 技术支持网站和注册您的 FortiGate 设备所需的步骤。
- 网络配置 描述了如何配置接口、配置路由以及如何在 FortiGate 上为您的内部网络配置 DHCP 服务器。
- RIP 配置 描述了 FortiGate RIP2 如何实现以及如何配置 RIP 的相关设置。
- 系统配置 描述了在**系统 > 配置** 基于 Web 的管理程序页可以进行的系统管理操作。本章描述了如何设置系统时间、添加和更改有管理权限的用户，配置 SNMP，以及编辑可自定义的消息。
- 防火墙配置 描述了如何配置防火墙策略以控制通过 FortiGate 设备的数据通讯，和对数据通讯应用内容过滤。
- 用户与认证 描述了如何在 FrotiGate 用户数据库中添加用户名，如何将 FortiGate 配置为连接到一个 RADIUS 服务器进行用户认证。
- IPSec VPN 描述如何配置 FortiGate IPSec VPN 。
- PPTP 和 L2TP VPN 描述了如何在 FortiGate 和 windows 客户端之间配置 PPTP 和 L2TP VPN。
- 网络入侵检测系统 (NIDS) 描述了如何配置 FortiGate NIDS 以检测和阻止网络攻击。
- 防病毒保护 描述了如何使用 FortiGate 保护您的网络不受病毒和蠕虫的侵袭。
- 网页内容过滤 描述了如何配置网页内容过滤以阻止不受欢迎的网页内容通过 FortiGate。
- 电子邮件过滤描述了如何配置电子邮件过滤以阻止不受欢迎的电子邮件内容。
- 日志和报告 描述了如何配置日志和报警邮件以记录和响应 FortiGate 的活动。
- 术语表 定义了在本手册中使用的一些术语。

文档中的约定

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`

Fortinet 的文档

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

开始

本章描述了有关拆包、安装及如何启动 FortiGate 防病毒防火墙的内容。一旦完成此章内容，您可按如下章节进行配置：

- 如果要在 NAT/ 路由 模式下运行 FortiGate，请参阅 第 29 页 “ NAT/ 路由 模式安装”。
- 如果要在 透明 模式下运行 FortiGate，请参阅 第 43 页 “ 透明模式安装”。
- 如果要在 HA 模式下运行两个或多个 FortiGate，请参阅 第 55 页 “ 高可用性”。

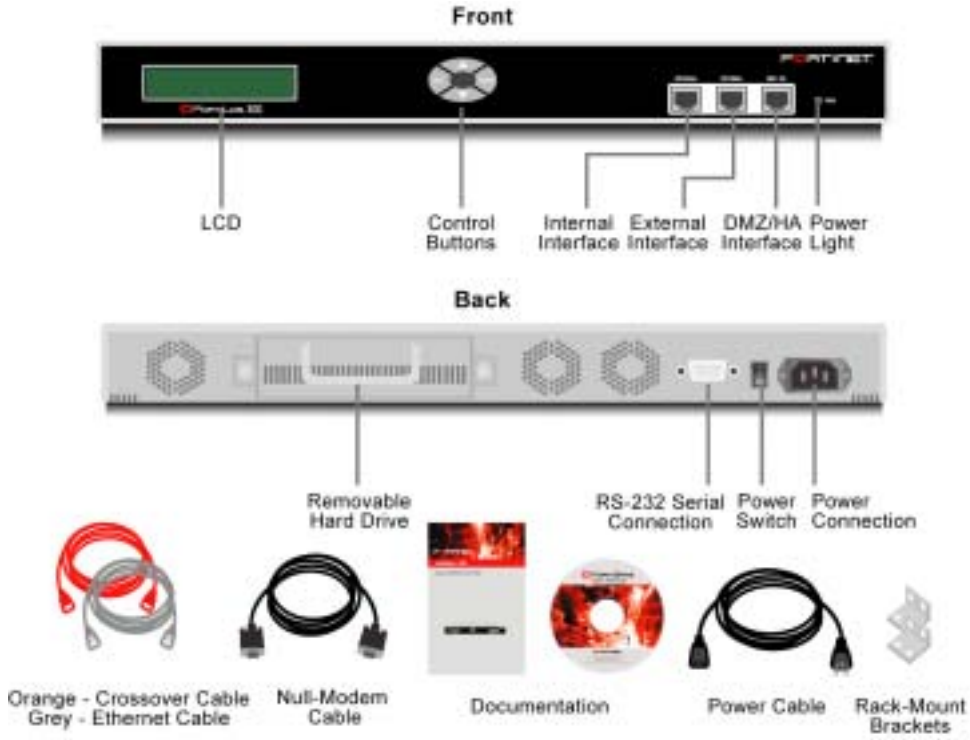
本章叙述了以下内容：

包装中的物品

FortiGate-300 包装中含有以下物品：

- FortiGate-300 防病毒防火墙
- 一根黄色交叉连接以太网电缆
- 一根灰色普通以太网电缆
- 一根串行通信电缆
- FortiGate-300 快速入门手册
- 一根电源线
- 包含了用户手册内容的光盘
- 两个 19 英寸机架安装支架

图 2: FortiGate-300 包装中的物品



安置

FortiGate-300 可安置在 19 英寸标准机架上。它需占据机架中 1 U 的空间。

FortiGate-300 也可被独立安装在任何稳定平台上。独立安装需确保在其周围每侧留有 1.5 英寸（3.75 厘米）的空间以保证空气流通和风冷。

尺寸

- 16.75 x 11 x 1.75 英寸 42.7 x 27.8 x 4.5 厘米

重量

• 7.3 磅 (3.3 公斤)

电源要求

• 功率需求：100 W (最大)
• 交流输入电压： 100 至 250 VAC
• 交流输入电流：1.5 A
• 频率：47 至 63 Hz

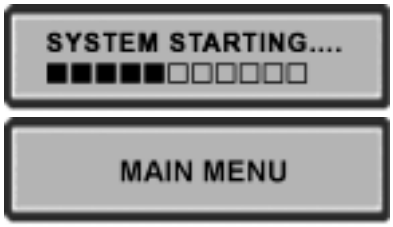
运行环境

• 工作温度： 32 至 104 华氏度 (0 至 40 摄氏度)
• 保存温度： -13 至 158 华氏度 (-25 至 70 摄氏度)
• 湿度： 5 至 95% 非冷凝

启动

按以下步骤启动 FortiGate-300：

1 确认 FortiGate-300 后面的电源开关处在关闭状态。
2 将电源线连接到 FortiGate-300 背面的电源接口处。
3 将电源线接到电源插座。
4 接通电源开关。
数秒后， LCD 显示 SYSTEM STARTING（系统启动）。



当系统启动完毕并正常运行后，LCD 将显示主菜单 (MAIN MENU)。

表 1: FortiGate-300 LED 指示灯

LED	状态	说明
Power	绿色	FortiGate 设备已经加电。
	熄灭	FortiGate 设备已经断电。
Internal External DMZ/HA	橙色	当前电缆使用中，并且所连接的设备已经加电。
	橙色闪烁	此接口有网络活动。
	绿色	此接口已建立速率为 100Mbps 的连接。
	熄灭	未建立连接。

连接到基于 Web 的管理程序

当初始启动 FortiGate 时，可按如下步骤连接到基于 Web 的管理程序。在基于 Web 的管理程序中所做的配置修改，无需重启动防火墙或中断服务即可生效。

欲连接到基于 Web 的管理程序，您需要：

- 一台能连接以太网的控制电脑，
- IE 4.0 及以上版本，
- 一根交叉电缆或以太网集线器，和两根以太网电缆。

注意：您可以使用大多数常见的老版本的网页浏览器访问 基于 Web 的管理程序。微软互联网浏览器 4.0 及以上版本能够完全支持 基于 Web 的管理程序 。

连接到 基于 Web 的管理程序

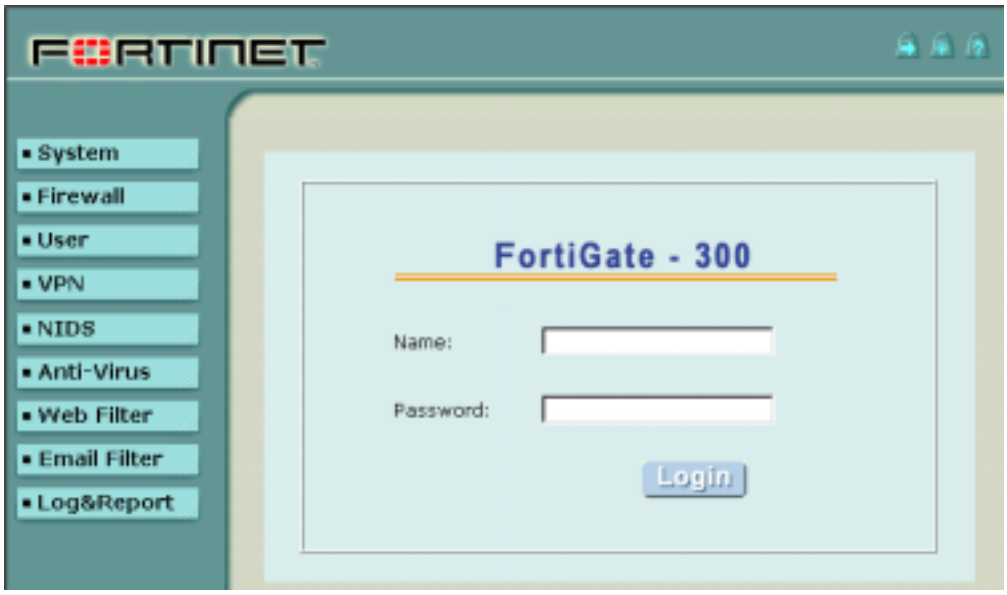
1 将与以太网相连的控制电脑的静态 IP 地址设定为 :192.168.1.2，网络掩码 255.255.255.0。

2 用交叉电缆或以太网集线器及电缆，控制电脑与 FortiGate 设备的内部接口相连。

3 启动 Internet 浏览器并访问 https://192.168.1.99。（需要输入 https://）将显示 FortiGate 登录界面。

4 在登录页面的姓名域中输入 admin 后按登录按钮。
“现在注册” 页面将显示。根据此页所给信息来注册 FortiGate。这样，以便 Fortinet 在需要固件升级时与您联系。同时，也为了您可及时收到更新的防病毒和入侵侦测数据库。

图 3: FortiGate 登录



连接到命令行接口（CLI）

除了基于 Web 的管理程序，您可使用 CLI 来安装和设置 FortiGate。在 CLI 中所做的配置修改，无需重启动防火墙或中断服务即可生效。

欲连接到 CLI 上，您需具备如下器材：

- 一台拥有可用的通信端口的电脑，
- 一个 FortiGate 套装包中带有的零调制解调器连接线，
- 终端端模拟软件，如 Windows 中的超级终端程序 （HyperTerminal）。

注意：以下步骤描述了如何用 Windows HyperTerminal 软件与 CLI 连接。您可以使用任何一种终端模拟软件。

连接到 CLI：

1 用串行通讯线将电脑的通信端口和 FortiGate 控制台端口相连。

2 确认 FortiGate 的电源已打开。

3 运行超级终端，为连接输入一个名称，然后单击 “确定”。

4 将超级终端的连接方式配置为直接连接到计算机的串行通讯接口，这个接口即串行通讯线所连接的接口，单击 “确定”。

5 选择以下端口设置并单击确定。

每秒比特数	115200
数据位	8
奇偶校验	无
停止位	1
流控制	无

6 按回车键，连接到 CLI。
将出现以下提示：

```
FortiGate-300 login:
```

7 输入 “admin” 后按两次回车键。
将出现以下提示：

```
Type ? for a list of commands.
```

关于如何使用 CLI，请参阅 *FortiGate CLI 参考手册*。

FortiGate 出厂默认设置

FortiGate 设备出厂时已经根据默认的配置方式进行了设置。这一默认设置允许您连接到 FortiGate 并根据您的网络配置 FortiGate 设备。要将 FortiGate 设备配置为在您的网络中工作，您需要添加管理员密码、修改网络接口的 IP 地址、DNS 服务器地址、如果需要的话还可以配置路由。

如果您准备让 FortiGate 设备运行于透明模式，您可以将 FortiGate 设备从出厂默认配置切换到透明模式，并根据您的网络配置透明模式下的 FortiGate 设备。

完成网络配置之后，您还可以做一些其他的配置工作，例如设置系统时间，配置防病毒和攻击定义更新，注册 FortiGate 设备等。

出厂时默认的防火墙配置包括了单一网络地址转换策略，允许您的内部网络中的用户连接到外部网络，而禁止外部网络中的用户连接到内部网络。您可以添加更多的策略，从而对通过 FortiGate 设备的通讯进行更多的控制。

出厂时默认的内容配置文件可以用来快速地在防火墙策略中设置不同级别的防病毒保护、网页内容过滤、电子邮件过滤，以控制网络通讯。

出厂默认的 NAT/ 路由模式的网络配置

FortiGate 设备首次加电时，它运行于 NAT/ 由模式，并具有表 2 中列出的基本网络配置。这一配置允许您连接到 FortiGate 设备的基于 Web 的管理程序，并根据您网络连接的要求配置 FortiGate 设备。在 表 2 中 HTTPS 管理访问意味着您可以使用这一接口连接到 基于 Web 的管理程序 。Ping 管理访问意味着这一接口可以响应 ping 请求。

表 2：出厂默认的 NAT/ 路由模式网络配置

管理员帐号		用户名： 密码：	admin （无）
内部接口		IP: 网络掩码： 管理访问：	192.168.1.99 255.255.255.0 HTTPS, Ping
外部接口	手工设置：	IP: 网络掩码： 默认网关： 主 DNS 服务器： 辅助 DNS 服务器： 管理访问：	192.168.100.99 255.255.255.0 192.168.100.1[a] 207.194.200.1 207.194.200.129 Ping
DMZ/HA 接口		IP: 网络掩码： 管理访问：	10.10.10.1 255.255.255.0 HTTPS, Ping

a. 当您修改外部接口的 IP 地址时，FortiGate 设备将删除默认路由。

出厂默认的透明模式的网络设置

如果您将 FortiGate 设备切换到透明模式，它具有表 3 中所列出的设置内容。

表 3：出厂默认的透明模式网络设置

管理员帐号	用户名： 密码	admin （无）
管理 IP	IP： 网络掩码：	10.10.10.1 255.255.255.0
DNS	主 DNS 服务器： 辅助 DNS 服务器：	207.194.200.1 207.194.200.129
管理访问	Internal External DMZ/HA	HTTPS, Ping Ping HTTPS, Ping

出厂时默认的防火墙配置

NAT/ 路由模式和透明模式具有相同的出厂默认的防火墙配置。

表 4：出厂默认防火墙设置

内部地址	内部 _ 全部	IP：0.0.0.0 掩码：0.0.0.0	表示内部网络中的全部 IP 地址
外部地址	外部 _ 全部	IP：0.0.0.0 掩码：0.0.0.0	表示外部网络中的全部 IP 地址
DMZ 地址	DMZ_ 全部	IP：0.0.0.0 掩码：0.0.0.0	表示 DMZ 网络中的全部 IP 地址。
循环任务计划	总是		任务计划始终有效。这意味着防火墙策略始终有效。
防火墙策略	**内部 -> 外部**		从内部网络到外部网络的防火墙策略
	源	内部 _ 全部	策略的源地址。内部 _ 全部意味着策略接受来自任何内部 IP 地址的连接请求。
	目的	外部 _ 全部	策略的目的地址。外部 _ 全部意味着策略接受到外部网络中的任何 IP 地址的连接请求。
	任务计划	总是	策略的任务计划。 总是 意味着这个策略始终有效。
	服务	任意	策略的服务。任意 意味着这个策略可以处理所有服务类型的连接。
	动作	接受	策略的动作。接受 意味着策略允许建立连接。

表 4：出厂默认防火墙设置（续）

☑ NAT		NAT 在 NAT/ 路由模式的默认策略中被选中，以使得策略对其处理的通讯进行网络地址转换。NAT 在透明模式下不可用。
☐ 流量控制		流量控制未被选中。策略不会对其所控制的通讯应用流量控制。您可以选中这一选项，以控制这一策略所处理的通讯的最大或最小带宽。
☐ 认证		认证没有被选中。用户在建立到目的地址的连接之前，无须通过防火墙的认证。您可以在防火墙上配置用户组，并启用认证功能，要求用户在通过防火墙建立连接之前先取得防火墙的认证。
☐ 防病毒和网页内容过滤		防病毒和网页内容过滤功能没有被选中。此策略不包含关于在此策略所处理的通讯中应用防病毒保护、网页内容过滤、或电子邮件过滤的内容配置文件。您可以选中此选项，并选择一个内容配置文件。根据配置文件，可以对此策略所处理的通讯进行不同级别的保护。
☐ 通讯日志		通讯日志没有被选中。此策略不会将策略所处理的通讯记录到通讯日志中。您可以配置 FortiGate 日志功能，启用通讯日志以记录此策略所接受的全部通过防火墙的通讯。

出厂时默认的内容配置文件

您可以使用内容配置文件对防火墙策略所控制的通讯内容应用不同级别的保护设置方式。您可以使用内容配置文件设置以下项目：

- HTTP, FTP, IMAP, POP3, 和 SMTP 网络通讯的防病毒保护
- HTTP 网络通讯的网页内容过滤
- IMAP 和 POP3 网络通讯的电子邮件过滤
- HTTP, FTP, POP3, SMTP, 和 IMAP 网络通讯的超大型文件和邮件阻塞
- IMAP, POP3, 和 SMTP 电子邮件通讯的邮件片段传输

您可以使用内容配置文件建立各种保护设置，并且可以很容易地应用到不同类型的防火墙策略上。这就使得您可以对不同的防火墙策略选择不同类型和不同级别的保护。

例如，内部地址和外部地址之间的通讯可能需要严谨的保护，受信任的内部地址之间的通讯仅需要中等的保护。您可以为不同的通讯服务配置不同的防火墙策略，然后使用相同或不同的内容配置文件。

内容配置文件可以添加到 NAT/ 路由模式或透明模式策略中。

严谨型内容配置文件

使用严谨的内容配置文件可以对 UHTTP, FTP, IMAP, POP3, 和 SMTP 等通讯的内容应用最大限度的防护。通常情况下您不需要使用严谨型内容配置文件，但是如果您受到病毒的严重威胁，需要最大限度地屏蔽病毒，可以选择严谨型内容配置文件。

表 5：严谨型内容配置文件

选项	HTTP	FTP	IMAP	POP3	SMTP
防病毒保护	☑	☑	☑	☑	☑
文件阻塞	☑	☑	☑	☑	☑
隔离	☑	☑	☑	☑	☑
Web URL 阻塞	☑				
Web 内容阻塞	☑				
Web 脚本过滤	☑				
Web 排除列表	☑				
Email 阻塞列表			☑	☑	
Email 排除列表			☑	☑	
Email 内容阻塞			☑	☑	
超大型文件 / 邮件阻塞	阻塞	阻塞	阻塞	阻塞	阻塞
传输邮件片段			☐	☐	☐

扫描型内容配置文件

使用扫描型内容配置文件可以对 HTTP、FTP、IMAP、POP3 和 SMTP 通讯的内容应用防病毒扫描。同时，隔离功能也被启用了，并适用于所有类型的服务。在 FortiGate 设备中装备了一个硬盘，如果防病毒扫描功能发现了在某个文件中有病毒，这个文件可以被隔离到 FortiGate 的硬盘上。系统管理员可以根据需要决定是否恢复被隔离的文件。

表 6：扫描型内容配置文件

选项	HTTP	FTP	IMAP	POP3	SMTP
防病毒保护	☑	☑	☑	☑	☑
文件阻塞	☐	☐	☐	☐	☐
隔离	☑	☑	☑	☑	☑
Web URL 阻塞	☐				
Web 内容阻塞	☐				
Web 脚本过滤	☐				
Web 排除列表	☐				
Email 阻塞列表			☐	☐	
Email 排除列表			☐	☐	
Email 内容阻塞			☐	☐	
超大型文件 / 邮件阻塞	传输	传输	传输	传输	传输
传输邮件片段			☐	☐	☐

网页型内容配置文件

使用网页型内容配置文件可以对 HTTP 通讯的内容应用防病毒扫描和网页内容阻塞。您可以在控制 HTTP 通讯的防火墙策略中添加这一内容配置文件。

表 7：网页型内容配置文件

选项	HTTP	FTP	IMAP	POP3	SMTP
防病毒保护	☑	☐	☐	☐	☐
文件阻塞	☐	☐	☐	☐	☐
隔离	☑	☐	☐	☐	☐
Web URL 阻塞	☑				
Web 内容阻塞	☑				
Web 脚本过滤	☐				
Web 排除列表	☐				
Email 阻塞列表	☐		☐	☐	
Email 排除列表			☐	☐	
Email 内容阻塞			☐	☐	
超大型文件 / 邮件阻塞	传输	传输	传输	传输	传输
传输邮件片段			☐	☐	☐

非过滤型内容配置文件

如果您不希望对通讯内容施加任何内容保护，可以选择非过滤型内容配置文件。您可以在控制无须保护的通讯类型的防火墙策略上添加这一内容配置文件，例如两个高度可信或高度安全的网络之间的通讯。

表 8：非过滤型内容配置文件

选项	HTTP	FTP	IMAP	POP3	SMTP
防病毒保护	☐	☐	☐	☐	☐
文件阻塞	☐	☐	☐	☐	☐
隔离	☐	☐	☐	☐	☐
Web URL 阻塞	☐				
Web 内容阻塞	☐				
Web 脚本过滤	☐				
Web 排除列表	☑				
Email 阻塞列表	☐		☐	☐	
Email 排除列表			☑	☑	
Email 内容阻塞			☐	☐	
超大型文件 / 邮件阻塞	传输	传输	传输	传输	传输
传输邮件片段			☑	☑	☑

规划您的 FortiGate 设备的配置

在开始配置 FortiGate 之前，您需要计划一下如何将它集成到您的网络中去。首先，您需要决定这个设备在网络中是否可见，要提供哪些防火墙功能，以及如何控制网络接口之间的数据流。

您所选择的操作模式决定了 FortiGate 的配置方式。FortiGate 有两种配置方式：NAT/ 路由模式 （默认），或者透明模式。

NAT/ 路由模式

在 NAT/ 模式，FortiGate 在网络中是可见的。此时它类似于路由器，所有的网络接口连接到不同的子网中。在 NAT/ 路由模式下有以下接口可用：

- 外部 是默认的连接到外部网络 （通常是互联网）的接口，
- 内部 是连接到内部网络的接口，
- DMZ/HA 是连接到 DMZ 网络的接口。 如果您建立了 HA 簇，DMZ/HA 接口也可以连接到其他 FortiGate-300 上面。

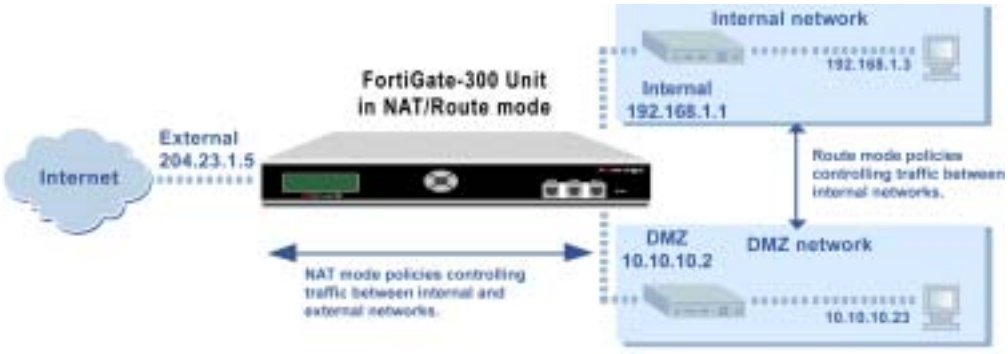
无论 FortiGate-300 工作在 NAT 模式或是路由模式，您都可以添加安全策略以控制通过 FortiGate-300 的通讯连接。安全策略根据每个数据包的源地址、目的地址和服务控制数据流。在 NAT 模式下，FortiGate 在将数据包发送到目的网络之前进行网络地址转换。在路由模式下，不进行转换。

默认情况下，FortiGate 只有一个 NAT 模式的策略，它使内部网络中的用户可以安全地从外部网络下载内容。如果您没有配置其他安全策略，其他的数据流都将被阻塞。

FortiGate-300 的 NAT/ 路由模式的一个比较典型的应用是作为私有网络和公共网络之间的网关。在这种配置中，您可以创建 NAT 模式的策略以控制内部的私有网络和外部的公共网络 （通常是互联网）之间的数据流通。

如果您安装了多个内部网络，例如除了内部私有网络之外还有 DMZ 网络，您也可以添加从 DMZ 网络到内部或外部网络之间的路由模式策略。

图 4: NAT/ 路由模式网络配置的例子



具有多个外部网络连接的 NAT/ 路由模式

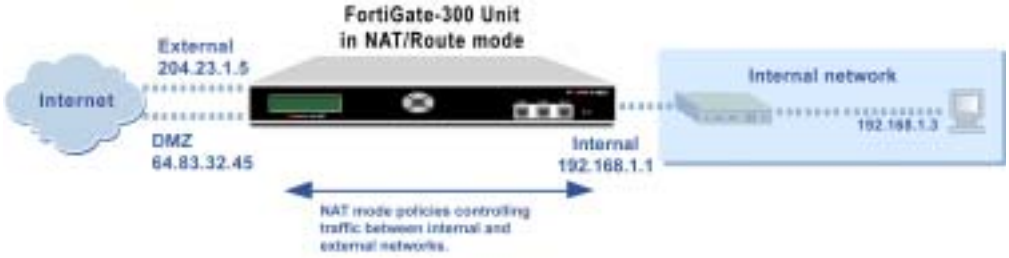
在 NAT/ 路由模式下，您可以为 FortiGate 设备配置到外部网络 （通常是互联网）的多重冗余连接。例如，您可以创建以下配置：

- 外部接口作为到外部网络 （通常是互联网）的默认接口。
- DMZ 接口是到外部网络的冗余接口。
- 内部接口作为到内部网络的接口。

您必须将路由配置为支持到互联网的冗余连接。当到外部网络的某个连接失效时，路由可以自动地将所有连接重定向到其他可用的外部网络连接上。

除此之外，安全策略的配置基本上等同于 NAT/ 路由模式下的单互联网连接的配置方式。您需要创建控制从内部的私有网络到外部的公共网络 （通常是互联网）的通讯的 NAT 模式策略。

图 5: NAT/ 路由模式下多重互联网连接配置的例子



透明模式

在透明模式下，FortiGate 设备在网络中是不可见的。此时它如同一个网桥，所有的 FortiGate 设备接口必须在同一子网内。您必须配置一个管理 IP 地址以便修改 FortiGate 的配置。这个管理 IP 地址还将用于获得防病毒保护和攻击定义的更新。

透明模式下的 FortiGate 设备一个比较典型的应用是安装在一个位于防火墙或路由器后面的私有网络中。FortiGate 提供一些基本的防护，例如防病毒和内容扫描，但是不支持 VPN。

图 6: 透明模式网络配置的例子

您可以将 3 个网段连接到 FortiGate 设备上，以控制这些网段之间的数据流通。

- 外部 可以连接到外部的防火墙或路由器。
- 内部 可以连接到内部网络。
- DMZ/HA 可以连接到其他网段。 如果您创建了 HA 簇，DMZ/HA 接口也可以连接到其他 FortiGate-300 上。

配置选项

选择了透明模式或 NAT/ 路由模式操作之后，您可以继续完成您的配置计划，并开始配置 FortiGate 设备。

您可以使用基于 Web 的管理程序上的设置向导，控制按钮和 LCD 或命令行界面 (CLI) 对 FortiGate 进行基本配置。

配置向导

如果您将 FortiGate 设备设置为以 NAT/ 路由模式 （默认）运行，设置向导会提醒您添加管理员密码，内部网络的接口地址。设置向导还会提醒您为外部网络接口选择静态 （手工设置）或动态 （DHCP 或 PPPoE）地址。也可以使用设置向导为外部接口添加 DNS 服务器 IP 地址和默认路由。

在 NAT/ 路由模式下，您还可以配置 FortiGate 的 DHCP 服务器为您的内部网络中的计算机分配 IP 地址。以及将 FortiGate 设备配置为允许从互联网访问您的内部网络中的网页、FTP 或电子邮件服务器。

如果您计划将 FortiGate 设备设置为透明模式，您可以使用基于 Web 的管理程序切换到透明模式，设置向导会提醒您添加管理员密码，管理 IP 地址和网关，以及 DNS 服务器地址。

CLI

如果您将 FortiGate 设备设置为以 NAT/ 路由模式 （默认）运行，您可以添加管理员密码，内部网络的全部接口地址。您也可以使用 CLI 配置外部网络接口的静态 （手工设置）或动态 （DHCP 或 PPPoE）地址。使用 CLI，您也可以为外部接口添加 DNS 服务器 IP 地址和默认路由。

在 NAT/ 路由模式下，您还可以配置 FortiGate 的 DHCP 服务器为您的内部网络中的计算机分配 IP 地址。

如果您计划将 FortiGate 设备设置为透明模式，您可以使用 CLI 切换到透明模式，添加管理员密码，管理 IP 地址和网关，以及 DNS 服务器地址。

前面板和 LCD

如果您计划将 FortiGate 设备设置为以 NAT/ 路由模式运行，您可以使用控制按钮和 LCD 添加 FortiGate 接口的 IP 地址和外部默认网关。

如果您计划将 FortiGate 设备培植为以透明模式运行，您可以使用控制按钮和 LCD 切换到透明模式，然后添加管理 IP 地址和默认网关。

FortiGate 系列产品参数最大值列表

表 9: FortiGate 参数最大值列表

	FortiGate 产品型号										
	50	60	100	200	300	400	500	1000	2000	3000	3600
策略	200	500	1000	2000	5000	5000	20000	50000	50000	50000	50000
地址	500	500	500	500	3000	3000	6000	10000	10000	10000	10000
地址组	500	500	500	500	500	500	500	500	500	500	500
服务	500	500	500	500	500	500	500	500	500	500	500
服务组	500	500	500	500	500	500	500	500	500	500	500
循环任务计划	256	256	256	256	256	256	256	256	256	256	256
一次性任务计划	256	256	256	256	256	256	256	256	256	256	256
用户	20	500	1000	1000	1000	1000	1000	1000	1000	1000	1000

表 9: FortiGate 参数最大值列表

	FortiGate 产品型号										
	50	60	100	200	300	400	500	1000	2000	3000	3600
用户组	100	100	100	100	100	100	100	100	100	100	100
组成员	300	300	300	300	300	300	300	300	300	300	300
虚拟 IP	500	500	500	500	500	500	500	500	500	500	500
IP/MAC 绑定	500	500	500	500	500	500	500	500	500	500	500
路由	500	500	500	500	500	500	500	500	500	500	500
策略路由网关	500	500	500	500	500	500	500	500	500	500	500
管理员权限用户	500	500	500	500	500	500	500	500	500	500	500
IPsec 第一阶段	20	50	80	200	1500	1500	3000	5000	5000	5000	5000
VPN 集中器	500	500	500	500	500	500	500	500	500	500	500
VLAN 子接口	N/A	N/A	N/A	N/A	N/A	1024*	1024*	2048*	2048*	8192*	8192*
区域	N/A	N/A	N/A	N/A	N/A	100	100	200	200	300	500
IP 池	50	50	50	50	50	50	50	50	50	50	50
RADIUS 服务器	6	6	6	6	6	6	6	6	6	6	6
文件模板	56	56	56	56	56	56	56	56	56	56	56
PPTP 用户	500	500	500	500	500	500	500	500	500	500	500
L2TP 用户	500	500	500	500	500	500	500	500	500	500	500
URL 阻塞	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制
内容阻塞	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制
排除的 URL	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制	无限制

下一步

至此，FortiGate 已启动并正常运行，您可继续配置如下设置：

- 如果要在 NAT/ 路由模式下运行 FortiGate，请参阅 第 29 页 “NAT/ 路由 模式安装”。
- 如果要在 透明 模式下运行 FortiGate ，请参阅 第 43 页 “透明模式安装”。
- 如果要在 HA 模式下运行 FortiGate，请参阅 第 55 页 “高可用性”。

NAT/ 路由 模式安装

本章说明了如何进行 FortiGate NAT/Route（路由）模式的安装。如果要在透明模式下安装 FortiGate，请参阅 第 43 页 “透明模式安装”。如果您要在 HA 模式下安装两个或多个 FortiGate，请参阅 第 55 页 “高可用性”。

本章叙述了以下内容：

准备配置 NAT/ 路由模式

使用 表 10 收集您设置 NAT/ 路由 模式配置所需的信息。

表 10：NAT/ 路由 模式配置

管理员密码：		
内部接口	IP： 网络掩码：	_____.____.____.____ _____.____.____.____

表 10：NAT/ 路由 模式配置 （续）

外部接口 （手工设置。您也可以使用 DHCP 或 PPPoE，详情请见 第 30 页 表 11 。）	IP: 网络掩码： 默认网关： 主 DNS 服务器： 辅助 DNS 服务器：	_____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____
内部服务器	Web 服务器： SMTP 服务器： POP3 服务器： IMAP 服务器： FTP 服务器：	_____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____
	如果要从 Internet 访问内部网中的 WEB 服务器、邮件服务器、IMAP 服务器，或 FTP 服务器，请在此添加服务器的 IP 地址。	

NAT/ 路由模式高级设置

使用 表 11 收集您设置 NAT/ 路由 模式配置所需的信息。

表 11：NAT/ 路由模式高级设置

外部接口	DHCP:	如果您的互联网服务供应商（ISP）为您提供了使用 DHCP 的 IP 地址，则无须更多的信息。	
	PPPoE:	用户名： 密码：	
	如果您的互联网服务供应商使用 PPPoE 为您分配 IP 地址，记录您的 PPPoE 用户名和口令。		
DHCP 服务器		启始 IP: 终止 IP: 网络掩码： 默认路由： DNS IP:	_____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____ _____.____.____.____
	FortiGate 设备包含了一个 DHCP 服务器，您可以将它配置为为您的内部网络中的计算机自动分配 IP 地址。		

DMZ 接口

如在安装时进行配置，可使用 表 12 记录 FortiGate DMZ 接口的 IP 地址和子网掩码。

表 12：DMZ 接口 （可选）

DMZ:	IP:	_____.____.____.____	网络掩码：	_____.____.____.____

使用安装向导

您可以从基于 Web 的管理程序中使用安装向导来建立 FortiGate 初始配置。欲连接到基于 Web 的管理程序，请参阅 第 18 页 “ 连接到基于 Web 的管理程序” 。

启动安装向导

为启动安装向导：

1 选择简易安装向导（基于 Web 的管理程序页面右上方中间的按钮）。

2 根据 第 29 页 表 10 中所获得的信息进行设置，选“下一步”按顺序逐步完成安装向导的若干页面。
您也可以使用 第 30 页 表 11 中的信息。

3 确保您的输入无误后按完成按钮结束。

注意：如果您使用安装向导来配置内部服务器设置，FortiGate 会向每个配置的服务器分配端口转送 IPs 和防火墙策略。对位于内部网的每个服务器，FortiGate 添加一个外部 --> 内部策略。对位于 DMZ 里的每个服务器，FortiGate 则添加一个外部 ->DMZ 策略。

重连接到 基于 Web 的管理程序

如果您使用安装向导修改了内部接口的 IP 地址，必须使用新 IP 地址重新连接基于 Web 的管理程序。浏览 https:// 后跟着 内部接口的新 IP 地址。或者，您也可通过 https://192.168.1.99. 重连接到基于 Web 的管理程序。

至此，您已完成 FortiGate 的初始 配置。现在 可以进入 第 34 页 “ 完成配置” 。

使用前面板控制按钮和 LCD

除安装向导外，也可使用 第 29 页 表 10 和 第 30 页 表 12 中记录的信息来完成如下步骤。从 LCD 上显示的主菜单开始，用前面板控制按钮和 LCD:

注意：您不能使用控制按钮和 LCD 为外部接口配置 DHCP 或 PPPoE。您可以使用设置向导或者基于 Web 的管理程序。

1 按回车键三次来配置内部接口 的 IP 地址。

2 设置内部接口 的 IP 地址。

使用上箭头和下箭头增加或减少 IP 地址中每位的值。按回车到下一位。按退出 （Esc） 回到前一位。

注意：当输入 IP 地址时，每部分地址将成 三位数字显示在 LCD 上。例如，IP 地址 192.168.100.1 在 LCD 上显为 192.168.100.001。 IP 地址 192.168.23.45 显为 192.168.023.045。

3 在输入完最后一位 IP 地址后按回车。

4 用向下箭头选择子网掩码。

5 按回车并设置内部子网掩码。

6 在输入完最后一位子网掩码地址后按回车。

7 按 退出 （Esc）返回主菜单。

8 如需要，重复如上步骤来设置外部接口，外部缺省网关，以及 DMZ/HA 接口。

您已完成 FortiGate 初始 配置。可进入 第 34 页 “ 完成配置” 。

使用命令行界面

除了使用设置向导，您还可以使用命令行界面 （CLI）配置 FortiGate。要连接到 CLI，请参阅 第 19 页 “ 连接到命令行接口 (CLI)” 。

将 FortiGate 配置为在 NAT/ 路由模式操作

使用您在 第 29 页 表 10 中收集的信息完成以下操作。

配置 NAT/ 路由模式 IP 地址

1 如果您还没有登录，首先登录到 CLI。

2 将内部网络接口的 IP 地址和网络掩码设置为您在 第 29 页 表 10 中记录的 IP 地址和网络掩码。输入：

```
set system interface internal mode static ip <IP_地址> <网络掩码>
```

例如

```
set system interface internal mode static ip 192.168.1.1
255.255.255.0
```

3 将外部网络接口的 IP 地址和网络掩码设置为您在 第 29 页 表 10 中记录的外部 IP 地址和网络掩码。输入：

```
set system interface external mode static ip <IP_地址> <网络掩码>
```

例如

```
set system interface external mode static ip 204.23.1.5
255.255.255.0
```

要将外部网络接口设置为使用 DHCP，输入：

```
set system interface external mode dhcp connection enable
```

要将外部网络接口设置为使用 PPPoE，输入：

```
set system interface external mode pppoe username <用户名_字符串>
password <密码_字符串> connection enable
```

例如

```
set system interface external mode pppoe username
user@domain.com password mypass connection enable
```

4 可以选择设置 DMZ 接口，将 DMZ 接口的 IP 地址和网络掩码设置为您在 第 29 页 表 10 中记录的 DMZ IP 地址和网络掩码。输入：

```
set system interface dmz mode static ip <IP 地址> <网络掩码>
```

例如

```
set system interface dmz mode static ip 10.10.10.2
255.255.255.0
```

5 确认地址是正确的。输入：

```
get system interface
```

CLI 列出每个 FortiGate 网络接口的 IP 地址，网络掩码和其它设置信息。

6 设置主 DNS 服务器的 IP 地址。输入

```
set system dns primary <IP 地址 >
```

例如

```
set system dns primary 293.44.75.21
```

7 还可以选择是否输入辅助 DNS 服务器 IP 地址，输入

```
set system dns secondary <IP 地址 >
```

例如

```
set system dns secondary 293.44.75.22
```

8 设置到默认路由的默认网关的 IP 地址（如果使用 DHCP 或 PPPoE 则不需要）。

```
set system route number < 路由编号 _ 整数 > dst 0.0.0.0 0.0.0.0 gw1
< 网关 IP 地址 >
```

例如

```
set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 204.23.1.2
```

将 FortiGate 连接到网络中

在完成了初始配置之后，您可以在内部网络和互联网之间连接 FortiGate 了。

FortiGate-300 有以下 10/100 BaseTX 接口：

- 内部接口，用于连接到内部网络，
- 外部接口，用于连接到互联网，
- DMZ/HA 用于连接到 DMZ 网络或其他 FortiGate-300 组成高可用性应用（请见 第 55 页 “ 高可用性”）。

注意： 您也可以把外部接口 和 DMZ /HA 接口连接到不同的互联网连接，以提供一个到互联网的冗余连接。请参阅 第 36 页 “ 配置举例：到互联网的多重连接” 。

按以下方式连接运行于 NAT/ 路由模式的 FortiGate:

1 将内部接口连接到您的内部网络的交换机或集线器上，

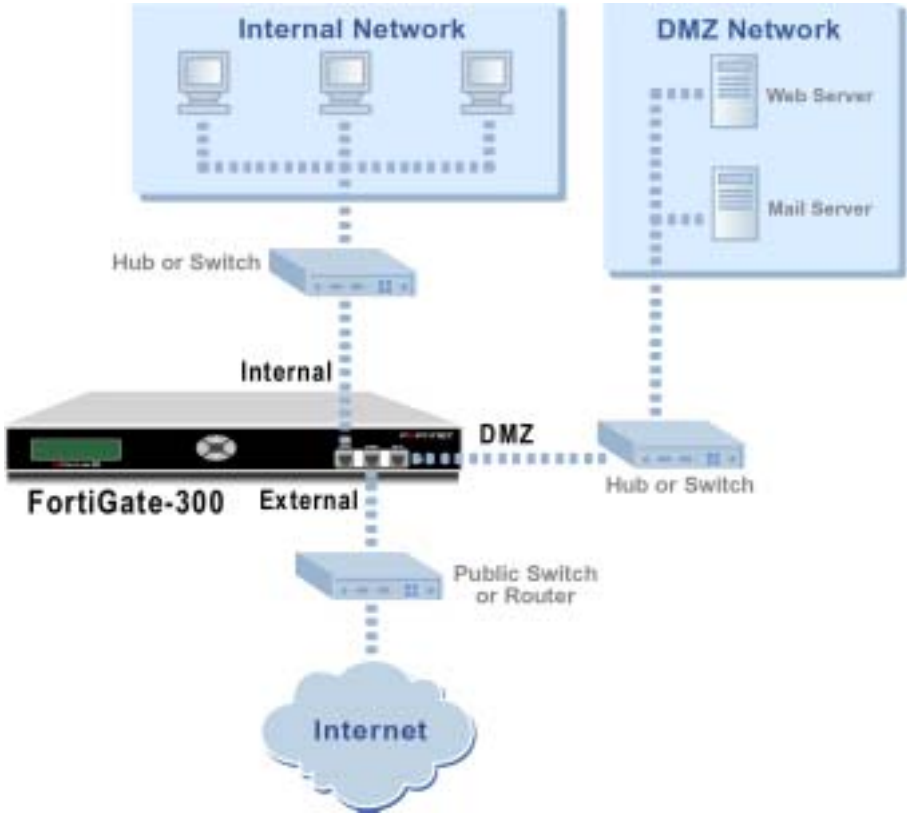
2 将外部接口连接到互联网上。

连接到 ISP 服务商提供的公共交换机和路由器上。如果使用 DSL 或带宽上网，需将外部接口连接到与您 DSL 或电缆调制解调器相连的内部网或 LAN 网上。

3 可以选择是否将 DMZ/HA 接口连接到 DMZ 网络。

您可通过 DMZ 网提供从 Internet 到 Web 或其它服务器的访问，而无需在内部网安装其它服务器。

图 7: FortiGate-300 NAT/路由模式连接



配置网络

如果在 NAT/路由模式下运行 FortiGate，您需要将网络设置为将所有 Internet 流通路由到它们所连接到的 FortiGate 接口的 IP 地址上。对于内部网，需将所有连接到内部网上的电脑和路由器的缺省网关地址改为 FortiGate 内部接口的 IP 地址。对于 DMZ 网，需将所有连接到 DMZ 网上的电脑和路由器的缺省网关地址改为 FortiGate DMZ 接口的 IP 地址。对于外部网，则路由所有的数据包到 FortiGate 的外部接口上。

如果使用 FortiGate 作为您内部网的 DHCP 服务器，需对内部网的电脑进行配置。

一旦 FortiGate 连接好，可通过从内部网的电脑连接到 Internet 来确保其运行是否正常。您应该能连接到任何的 Internet 地址。

完成配置

根据用本节内容来完成 FortiGate 的初始配置。

配置 DMZ/HA 接口

如果您要设置 DMZ 网络，就需要改变 DMZ/HA 接口的 IP 地址。按如下步骤用基于 Web 的管理程序配置 DMZ/HA 接口 ：

1 登录到 基于 Web 的管理程序。
2 进入 **系统 > 网络 > 接口**。
3 选择 DMZ/HA 接口 并单击 修改  。
4 确认接口被设置为 DMZ 模式。
5 根据需要改变 IP 地址和子网掩码。
6 单击 应用 。

设置日期和时间

为了有效的安排日程和记录日志， FortiGate 的日期和时间必须精确。 您可手动设置时间，或通过配置 FortiGate 来自动与网络时间协议服务器 (NTP) 同步从而更正时间。

设置 FortiGate 日期和时间，请参阅 第 127 页 “ 设置系统日期和时间”.

启用防病毒保护

按以下步骤启用防病毒保护，可以防止您的内部网络中的用户从互联网上下载病毒：

1 进入 **防火墙 > 策略 > 内部 -> 外部**。
2 单击编辑  以编辑这个策略。
3 单击 防病毒和网络过滤，以启用这个策略的防病毒防火墙功能。
4 选择扫描型内容配置文件。
5 单击确定以保存您所做的修改。

注册 FortiGate 设备

在购买和安装了一个新的 FortiGate 设备之后，您可以进入 系统 > 更新 > 支持来注册您的设备，或者使用网页浏览器连接到 http://support.fortinet.com 然后选择产品注册。

注册内容包括您的联系方式、您或者您所在的机构购买的 FortiGate 设备的产品序列号。注册过程非常方便快捷。您可以一次就注册多个 FortiGate 设备，而无须重复输入您的联系方式。

关于注册的更多信息，请见 第 100 页 “ 注册 FortiGate 设备” 。

配置防病毒和攻击定义更新

您可以进入系统 > 更新以配置 FortiGate 设备的自动检查新版本的防病毒定义和攻击定义。如果它发现了新的版本，FortiGate 设备会自动下载和安装更新的定义。

FortiGate 设备使用 8890 端口的 HTTPS 方式连接去检查更新。FortiGate 外部接口必须能够使用 8890 端口访问更新中心。

要配置自动防病毒和攻击定义更新，请访问 第 91 页 “ 病毒防护定义和攻击定义更新” 。

配置举例：到互联网的多重连接

本节描述了 FortiGate 设备使用多重连接到互联网的 （见图 8）一些基本的路由和防火墙策略配置的例子。在这种拓扑结构中，该组织使用的 FortiGate 设备分别通过两个互联网服务供应商连接到互联网。FortiGate 设备使用外部接口和 DMZ/HA 接口连接到互联网。外部接口连接到 ISP1 提供的网关 1，DMZ/HA 连接到 ISP2 提供的网关 2。

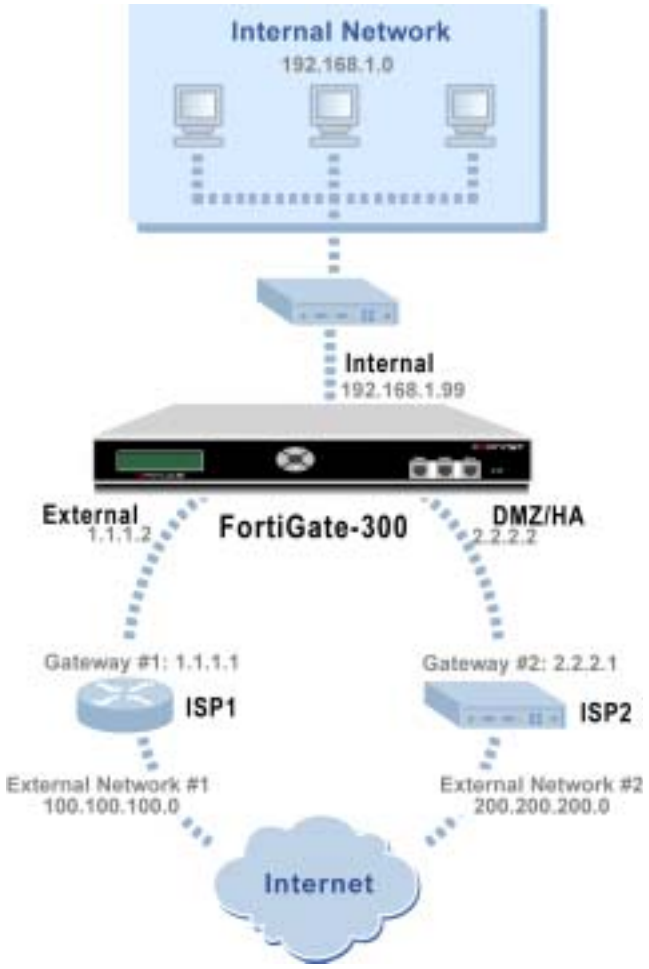
在接口上添加了 ping 服务器，并配置了路由之后，您可以控制通讯如何使用每个到互联网的连接。在这种路由配置方式下您可以继续创建支持到互联网的多重连接的防火墙策略。

本节提供了一些具有到互联网的多重连接的 FortiGate 设备中配置路由和防火墙的例子。要使用本节中的所提供的信息，我们建议您先熟悉一下关于 FortiGate 路由（请见 第 113 页 “ 配置路由” ）和 FortiGate 防火墙配置（见 第 137 页 “ 防火墙配置” ）。

下面的例子显示了如何配置基于目的地的路由和策略路由以控制不同类型的通讯。

- 配置 Ping 服务器
- 基于目的地的路由配置举例
- 策略路由的例子
- 防火墙策略举例

图 8: 到互联网的多重连接的配置的例子



配置 Ping 服务器

按照以下步骤将网关 1 设置为外部接口的 Ping 服务器，将网关 2 设置为 DMZ/HA 接口的 Ping 服务器。

1 进入**系统 > 网络 > 接口**。

2 在外部接口上选择修改 。

- Ping 服务器： 1.1.1.1
- 选择启用 Ping 服务器
- 单击确定

3 在 DMZ/HA 接口上选择修改 。

- Ping 服务器： 2.2.2.1
- 选择启用 Ping 服务器
- 单击确定

使用 CLI

1 将 ping 服务器添加到外部接口。

```
set system interface external config detectserver 1.1.1.1
gwdetect enable
```

2 将 ping 服务器添加到 DMZ/HA 接口。

```
set system interface dmz/ha config detectserver 2.2.2.1
gwdetect enable
```

基于目的地的路由配置举例

本节描述了以下基于目的地的路由的例子：

- 到互联网的主连接和备份连接
- 负载分配
- 负载分配与主连接、备份连接

到互联网的主连接和备份连接

按照以下步骤添加默认的基于目的地的路由，以将所有向外的通讯定向到网关 1。如果网关 1 失效了，所有连接会被重定向到网关 2。网关 1 是到互联网的主连接，网关 2 是备份连接。

1 进入 **系统 > 网络 > 路由表**。

2 选择 新建。

- 目的 IP：0.0.0.0
- 掩码：0.0.0.0
- 网关 #1：1.1.1.1
- 网关 #2：2.2.2.1
- 设备 #1：外部
- 设备 #2：dmz/ha
- 单击确定。

使用 CLI

1 在路由表中添加路由

```
set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 1.1.1.1
dev1 external gw2 2.2.2.1 dev2 dmz/ha
```

表 13：主连接和备份连接的路由

目的 IP 口	掩码	网关 #1	设备 #1	网关 #2	设备 #2
0.0.0.0	0.0.0.0	1.1.1.1	external	2.2.2.1	dmz/ha

负载分配

您也可以将基于目的的路由配置为同时将通讯定向到两个网关。如果您的内部网络中的用户连接到 IPS1 和 IPS2 的网络中，您可以为每个目的地添加路由。每个路由可以包括一个到另一个 ISP 的网络的备份目的地址。

表 14：负载分配路由

目的 IP 口	掩码	网关 #1	设备 #1	网关 #2	设备 #2
100.100.100.0	255.255.255.0	1.1.1.1	external	2.2.2.1	dmz/ha
200.200.200.0	255.255.255.0	2.2.2.1	dmz/ha	1.1.1.1	external

第一条路由将所有的到 100.100.100.0 的通讯定向到外部接口上 IP 为 1.1.1.1 的网关 1。如果这条路由不通，到 100.100.100.0 的网络的通讯将被重定向到 DMZ/HA 接口上 IP 地址为 2.2.2.1 的网关 2。

负载分配与主连接、备份连接

您可以将这些路由组合到一个更加复杂的到互联网多重连接的配置中。在 第 37 页 图 8 中所显示的拓扑结构中，内部网络中的用户需要连接到互联网上访问网页，或者其他互联网资源。然而，他们也可能要访问由他们的 ISP 所提供的其他服务，例如电子邮件。您可以将上述例子中的路由方法组合起来，为用户提供一个到互联网的主连接和一个备份连接，并根据需要将通讯分配到每个 ISP 的网络上。

下面所描述的路由允许内部网络中的用户通过网关 1 和 ISP1 访问互联网。同时，这个用户还可以通过 ISP2 的网关 2 去访问他的电子邮件服务器。

使用 基于 Web 的管理程序添加路由

1 进入 **系统 > 网络 > 路由表**。

2 单击新建以添加到互联网的主连接和备份连接的默认路由。

- 目的 IP：0.0.0.0
- 掩码：0.0.0.0
- 网关 #1：1.1.1.1
- 网关 #2：2.2.2.1
- 设备 #1：外部
- 设备 #2：dmz/ha
- 单击确定。

3 单击新建以添加到 ISP1 的网络的路由。

- 目的 IP：0.0.0.0
- 掩码：0.0.0.0
- 网关 #1：1.1.1.1
- 网关 #2：2.2.2.1
- 设备 #1：外部
- 设备 #2：dmz/ha

4 单击新建以添加到 ISP2 的网络的路由。

- 目的 IP：0.0.0.0
- 掩码：0.0.0.0
- 网关 #1：1.1.1.1
- 网关 #2：2.2.2.1
- 设备 #1：dmz/ha
- 设备 #2：外部
- 单击确定。

5 将路由表中的路由排序，将默认路由移动到路由表的最下方。

- 在默认路由上单击移动  。
- 在移动栏输入输入数字将这条路由移动到路由表的底部。
  如果只有 3 个路由，就输入 3。
- 单击确定。

使用 CLI 添加路由

1 添加到 ISP1 的网络的路由。

```
set system route number 1 dst 100.100.100.0 255.255.255.0 gw1
1.1.1.1 dev1 external gw2 2.2.2.1 dev2 dmz/ha
```

1 添加到 ISP2 的网络的路由。

```
set system route number 2 dst 200.200.200.0 255.255.255.0 gw1
2.2.2.1 dev1 dmz/ha gw2 1.1.1.1 dev2 external
```

2 添加到互联网的主连接和备份连接的默认路由。

```
set system route number 3 dst 0.0.0.0 0.0.0.0 gw1 1.1.1.1
dev1 external gw2 2.2.2.1 dev2 dmz/ha
```

路由表中的路由应当按照 表 15 中的顺序排序。

表 15：组合路由表的例子

目的 IP 口	掩码	网关 #1	设备 #1	网关 #2	设备 #2
100.100.100.0	255.255.255.0	1.1.1.1	external	2.2.2.1	dmz/ha
200.200.200.0	255.255.255.0	2.2.2.1	dmz/ha	1.1.1.1	external
0.0.0.0	0.0.0.0	1.1.1.1	external	2.2.2.1	dmz/ha

策略路由的例子

添加策略路由可以增强您对数据包被路由的方式的控制能力。策略路由工作在基于目的的路由的顶部。这意味着您应当先配置基于目的的路由并在顶部建立策略路由以增强由基于目的的路由提供的控制能力。

例如，如果您为一个到互联网的双重连接配置了基于目的的路由，您可以使用策略路由对通讯被发送到哪条目的路由进行控制。本节描述了以下策略路由的例子，它们基于类似于 第 37 页 图 8 的拓扑结构。在每个例子中标出了不同点。

只有您已经定义了类似于在前面章节中描述的目的路由之后，在这些例子中描述的策略路由才能正常工作。

- 将通讯从内部子网路由到不同的外部网络
- 路由到外部网络的服务

关于策略路由的详细信息，请见 第 115 页 “ 策略路由” 。

将通讯从内部子网路由到不同的外部网络

如果 FortiGate 提供了从多个内部子网到互联网的访问，您可以使用策略路由控制从各个内部子网到互联网的通讯的路由。例如，如果内部网络包含了 192.168.10.0 子网和 192.168.20.0 子网，您可以输入如下策略路由：

1 输入以下命令路由从 192.168.10.0 子网到外部网络 100.100.100.0 的通讯：

```
set system route policy 1 src 192.168.10.0 255.255.255.0 dst
100.100.100.0 255.255.255.0 gw 1.1.1.1
```

2 输入以下命令路由从 192.168.20.0 子网到外部网络 200.200.200.0 的通讯：

```
set system route policy 2 src 192.168.20.0 255.255.255.0 dst
200.200.200.0 255.255.255.0 gw 2.2.2.1
```

路由到外部网络的服务

您可以使用以下策略路由将所有 HTTP 通讯 （使用 80 端口）定向到一个外部网络，而将其他的全部通讯定向到另一个外部网络。

1 输入以下命令将使用 80 端口的全部 HTTP 通讯路由到 IP 地址为 1.1.1.1 的网关。

```
set system route policy 1 src 0.0.0.0 0.0.0.0 dst 0.0.0.0
0.0.0.0 protocol 6 port 1 1000 gw 1.1.1.1
```

2 输入以下命令将其他的全部通讯路由到 IP 地址为 2.2.2.1 的网关。

```
Set system route policy 2 src 0.0.0.0 0.0.0.0 dst 0.0.0.0
0.0.0.0 gw 2.2.2.1
```

防火墙策略举例

防火墙策略控制着通过 FortiGate 设备的通讯流。一旦配置了到互联网的多重连接的路由，您需要创建对应的防火墙策略，控制允许通过 FortiGate 设备的通讯，以及允许通讯使用的接口。

为了使从内部网络发出的通讯能够通过两个互联网连接线路连接到互联网，您必须添加从内部接口到每个带有互联网连接的接口的冗余策略。添加完策略之后，路由配置可以控制使用哪个到互联网的连接。

添加冗余的默认策略

第 37 页 图 8 显示了 FortiGate 设备使用外部和 DMZ 接口连接到互联网的例子。默认的策略允许全部的通讯从内部网络通过外部接口连接到互联网。如果您添加了一个类似的从内部网络到 DMZ 的策略列表，这一策略将允许所有通讯从内部网络通过 DMZ 接口连接到互联网。在防火墙配置中添加了这两个策略之后，路由配置可以决定从内部网络到互联网的连接实际使用哪条到互联网的线路。关于默认策略的详细信息，请见 第 138 页 “ 默认防火墙配置” 。

按以下步骤添加冗余的默认策略：

1 进入 **防火墙 > 策略 > 内部 -> 外部**。

2 单击新建。

3 根据默认策略配置相应的策略。

源	内部 _ 全部
目的	DMZ_ 全部
任务计划	总是
服务	任意
动作	接受
NAT	选种 NAT。

4 单击确定以保存您所做的修改。

添加更多的防火墙策略

大多数情况下您的防火墙配置中不只包含了默认的策略。然而，创建冗余策略将使得防火墙的配置变得更加复杂。为了将 FortiGate 设备配置为使用到互联网的多重连接，您必须为从内部网络到每个连接到互联网的接口的连接方式创建双重的策略。而且，您添加了冗余策略后，还需要在两个策略列表中将他们按照相同的顺序排列。

限制到单一互联网连接的访问

在某些情况下，您可能希望将一些通讯限制为仅能通过一个到互联网的线路进行连接。例如，在 第 37 页 图 8 所示的拓扑结构中，该机构可能希望只有通过 ISP1 的到 SMTP 服务器可以连接到他们的邮件服务器。为此，您需要为 SMTP 连接添加一个内部 -> 外部防火墙策略。因为没有添加冗余策略，来自内部网络的 SMTP 通讯总是连接到 ISP1。如果到 ISP1 的连接失败，SMTP 连接就无法建立。

透明模式安装

本章说明了如何进行透明模式的安装。如果要在 FortiGate NAT/ 路由模式下安装 FortiGate ，请参阅 第 29 页 “ NAT/ 路由 模式安装” 如果您要在 HA 模式下安装两个或多个 FortiGate ，请参阅 第 55 页 “ 高可用性” 。

本章叙述了以下内容：

准备配置透明模式

使用 表 16 收集您设置 NAT/ 路由 模式配置所需的信息。

表 16：透明模式设置

管理员密码：		
管理用 IP 地址	IP: 子网掩码： 默认网关：	_____.____.____.____ _____.____.____.____ _____.____.____.____
	管理 FortiGate 的网络中的管理 IP 地址和子网掩码必须有效。如 FortiGate 须连接到路由器来到达控制电脑，则需填入缺省网关地址。	
DNS 设置：	主 DNS 服务器： 辅助 DNS 服务器：	_____.____.____.____ _____.____.____.____

使用安装向导

从 基于 Web 的管理程序 ，使用安装向导来建立您 FortiGate 的初始配置。欲连接到基于 Web 的管理程序，请参阅 第 18 页 “ 连接到基于 Web 的管理程序” 。

切换到透明模式

当首次连接到 FortiGate 时，它被预设在 NAT/ 路由模式下运行。欲切换为透明模式需使用基于 Web 的管理程序：

1 进入**系统 > 状态**。

2 单击 **更改** 以切换到透明模式。

3 在操作模式列表中选择 **透明模式** 。

4 单击 **确定** 。

至此，FortiGate 已切换为透明模式。

要重新连接到基于 Web 的管理程序，需要将您的管理员电脑的 IP 地址改为 10.10.10.2。然后连接到内部接口或 DMZ/HA 接口，用浏览器访问 https:// 后边跟上透明模式的管理 IP 地址。默认的 FortiGate 透明模式管理 IP 地址是 10.10.10.1。

启动安装向导

按以下步骤启动安装向导：

1 选择简易安装向导（基于 Web 的管理程序右上方中间的按钮）。

2 根据 第 43 页 表 16 中所获得的信息进行设置，单击下一步按顺序逐步完成安装向导的若干页面。

3 保您的输入无误后按完成按钮结束。

重连接到 基于 Web 的管理程序

如果使用安装向导更换内部接口的 IP 地址，必须使用新 IP 地址重连接到基于 Web 的管理程序上。流览 https:// 跟着管理接口的新 IP 地址。或者，您也可通过 https://10.10.10.1。 重连到基于 Web 的管理程序。如果要通过一路由器连接到管理接口，请确保在管理 IP 缺省网关域里填入此路由器的缺省网关值。

使用前面板控制按钮和 LCD

以下步骤描述了如何使用控制按钮和 LCD 配置透明模式下的 IP 地址。使用您在 第 43 页 表 16 中记录的信息完成如下步骤。从 LCD 上显示的主菜单开始，使用前面板的控制按钮和 LCD：

1 按回车键三次来配置管理 的 IP 地址。

2 设置管理接口的 IP 地址。

使用上箭头和下箭头增加或减少 IP 地址中每位的值。按回车到下一位。按退出 （Esc） 回到前一位。

注意：当输入 IP 地址时，每部分地址将成 三位数字显示在 LCD 上。例如，IP 地址 192.168.100.1 在 LCD 上显为 192.168.100.001。 IP 地址 192.168.23.45 显为 192.168.023.045。

3 在输入完最后一位 IP 地址后按回车。

4 用向下箭头选择子网掩码。

5 按回车并设置内部子网掩码。

6 在输入完最后一位子网掩码地址后按回车。

7 按 退出 （Esc）返回主菜单。

8 如需要，重复如上步骤来设置缺省网关。

使用命令行接口

除了使用连接向导以外，您还可以使用命令行接口 （CLI）配置 FortiGate。要连接到 CLI 接口，请参阅 第 19 页 “ 连接到命令行接口 (CLI)” 。使用您在 第 43 页 表 16 中收集的信息完成以下步骤。

切换到透明模式

1 如果您还没有登录，首先登录到 CLI。

2 切换到透明模式。输入：
```
set system opmode transparent
```
几秒种后，会出现登录提示。

3 输入 admin 然后回车。
将出现以下提示：
```
Type ? for a list of commands.
```

4 确认 FortiGate 已经切换到了透明模式。输入：
```
get system status
```
CLI 显示 FortiGate 的状态。最后一行显示了当前的操作模式。
```
Operation mode: Transparent
```

配置透明模式的管理 IP 地址

1 如果您还没有登录，首先登录到 CLI。

2 将管理用 IP 地址和网络掩码设置为您在 第 43 页 表 16 。输入：
```
set system management ip <IP 地址 > < 网络掩码 >
```
例如
```
set system management ip 10.10.10.2 255.255.255.0
```

3 确认地址是正确的。输入：
```
get system management
```
CLI 列出管理 IP 地址和网络掩码。

配置透明模式的默认网关

1 如果您还没有登录，首先登录到 CLI。

2 将默认路由设置为您在 第 43 页 表 16 中记录的 IP 地址和网络掩码。输入：
```
set system route number < 编号 > gw1 <IP 地址 >
```
例如
```
set system route number 0 gw1 204.23.1.2
```

现在您已经完成了 FortiGate 的初始设置。

完成配置

根据用本节内容来完成 FortiGate 的初始配置。

设置日期和时间

为了有效的安排日程和记录日志， FortiGate 的日期和时间必须精确。 您可手动设置时间，或通过配置 FortiGate 来自动与网络时间协议服务器 (NTP) 同步从而更正时间。

设置 FortiGate 日期和时间，请参阅 第 127 页 “ 设置系统日期和时间” 。

启用防病毒保护

按以下步骤启用防病毒保护，可以防止您的内部网络中的用户从互联网上下载病毒：

1 进入 **防火墙 > 策略 > 内部 -> 外部**。

2 单击编辑  以编辑这个策略。

3 单击 防病毒和网络过滤，以启用这个策略的防病毒防火墙功能。

4 选择扫描型内容配置文件。

5 单击确定以保存您所做的修改。

注册 FortiGate 设备

在购买和安装了一个新的 FortiGate 设备之后，您可以进入 系统 > 更新 > 支持来注册您的设备，或者使用网页浏览器连接到 http://support.fortinet.com 然后选择产品注册。

注册内容包括您的联系方式、您或者您所在的机构购买的 FortiGate 设备的产品序列号。注册过程非常方便快捷。您可以一次就注册多个 FortiGate 设备，而无须重复输入您的联系方式。

关于注册的更多信息，请见 第 100 页 “ 注册 FortiGate 设备” 。

配置防病毒和攻击定义更新

您可以进入 系统 > 更新 以配置 FortiGate 设备的自动检查新版本的防病毒定义和攻击定义。如果它发现了新的版本，FortiGate 设备会自动下载和安装更新的定义。

FortiGate 设备使用 8890 端口的 HTTPS 方式连接去检查更新。FortiGate 外部接口必须能够使用 8890 端口访问 Forti 响应发布网络 （FDN）。

要配置自动防病毒和攻击定义更新，请访问 第 91 页 “ 病毒防护定义和攻击定义更新” 。

将 FortiGate 连接到网络中

在完成了初始配置之后，您可以在内部网络和互联网之间连接 FortiGate-300 了。

FortiGate-300 有三个 10/100 BaseTX 接口：

- 内部接口，用于连接到您的内部网络，
- 外部接口，用于连接到互联网，
- DMZ/HA 接口，用于连接到其他网络。

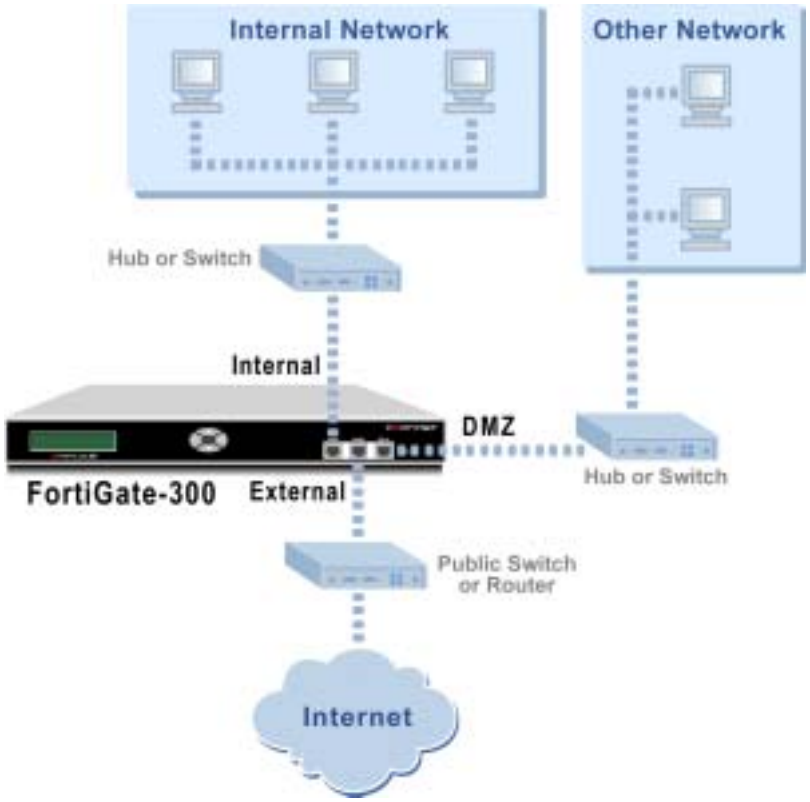
按以下方式连接运行于透明模式的 FortiGate-300:

1 将内部接口连接到您的内部网络的交换机或集线器上，

2 将外部接口连接到互联网上。
连接到 ISP 服务商提供的公共交换机和路由器上。

3 将 DMZ/HA 接口连接到其他网络的集线器或交换机上。

图 9: FortiGate-300 透明模式连接



在透明模式下，FortiGate 不改变网络的第三层拓扑结构。这意味着它的所有接口在相同的子网中，并且对于其他设备来说它相当于一个网桥。FortiGate 透明模式的一个典型的应用是在一个已有的防火墙配置后面提供防病毒和内容扫描。

透明模式的 FortiGate 也可以提供防火墙功能，尽管它不是第三层拓扑结构中的一部分，但是它可以检验第三层头信息以决定是否阻塞或允许流通。

透明模式配置的例子

运行于透明模式的 FortiGate 也需要一个基本配置，以成为 IP 网络中的一个结点。至少，FortiGate 必须配置一个 IP 地址和子网掩码。它们可以用来对 FortiGate 进行管理访问，并允许 FortiGate 进行防病毒和攻击定义的更新。另外，FortiGate 必须有足够的信息达到：

- 管理员电脑，
- Forti 响应发布网络 (FDN)，
- DNS 服务器。

无论何时，FortiGate 都需要一个路由配置以连接到路由器，从而连接到目的地址。如果所有的目的地址都在外部网络中，您可能只需要输入一个默认路由。然而，如果网络拓扑比较复杂，您可能需要再输入一个或多个路由。

本节描述了：

默认路由和静态路由

要创建到一个目的地的路由，您需要根据 IP 网络地址和相应的网络掩码定义一个 IP 前缀。一个默认的路由匹配任何前缀，可以将数据流转发到下一个路由器 （或默认网关）。一个静态的路由匹配特定的前缀，并将数据流转发到下一个路由器。

默认路由的例子：

IP 前缀 0.0.0.0（IP 地址）
0.0.0.0（网络掩码）
下一个跳跃 192.168.1.2

静态路由的例子：

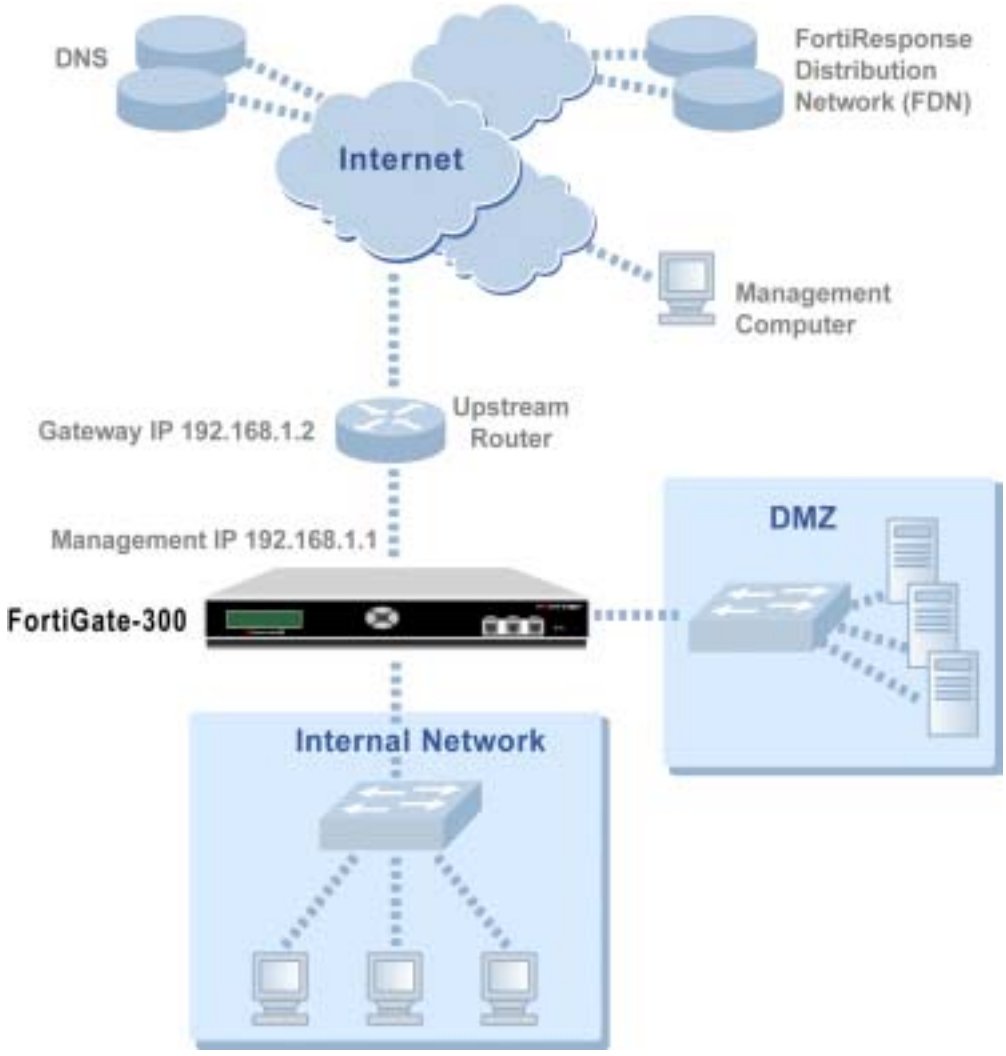
IP 前缀 172.100.100.0（IP 地址）
255.255.255.0（网络掩码）
下一个跳跃 192.168.1.2

注意：在 FortiGate 中添加路由时，最后添加默认路由，使它出现在路由表的底部。这可以保证 FortiGate 先匹配特定的路由，最后再选择默认路由。

到外部网络的默认路由的例子

图 10 展示了 FortiGate 中包括管理站点在内的所有目的地址都位于外部网络的例子。要达到这些地址，FortiGate 必须连接到通向外部网络的上游路由器。为了便于连接，您需要输入单一的默认路由指向上游路由器，使之成为下一个跳跃 / 默认网关。

图 10: 到外部网络的默认路由



通用配置步骤

1 将 FortiGate 设置为透明模式。

2 配置 FortiGate 的管理 IP 地址和网络掩码。

3 配置到外部网络的默认路由。

基于 Web 的管理程序配置步骤的例子

使用基于 Web 的管理程序配置基本的透明模式设置和默认路由：

1 进入 **系统 > 状态**。
- 选择切换到透明模式。
- 在操作模式列表中选择 透明。
- 单击 确定。

FortiGate 已切换到透明模式。

2 进入 **系统 > 网络 > 管理**。
- 修改管理 IP 地址和网络掩码：

IP：192.168.1.1

掩码： 255.255.255.0
- 单击 应用。

3 进入**系统 > 网络 > 路由**。
- 单击 新建 添加到外部网络的默认路由。

IP：0.0.0.0

掩码： 0.0.0.0

网关： 192.168.1.2
- 单击 确定。

CLI 配置步骤

要使用 CLI 配置 FortiGate 基本设置和路由：

1 将系统操作模式修改为透明模式。ode.

```
set system opmode transparent
```

2 添加管理 IP 地址和掩码。

```
set system management ip 192.168.1.1 255.255.255.0
```

3 添加到外部网络的默认路由。

```
set system route number 1 gw1 192.168.1.2
```

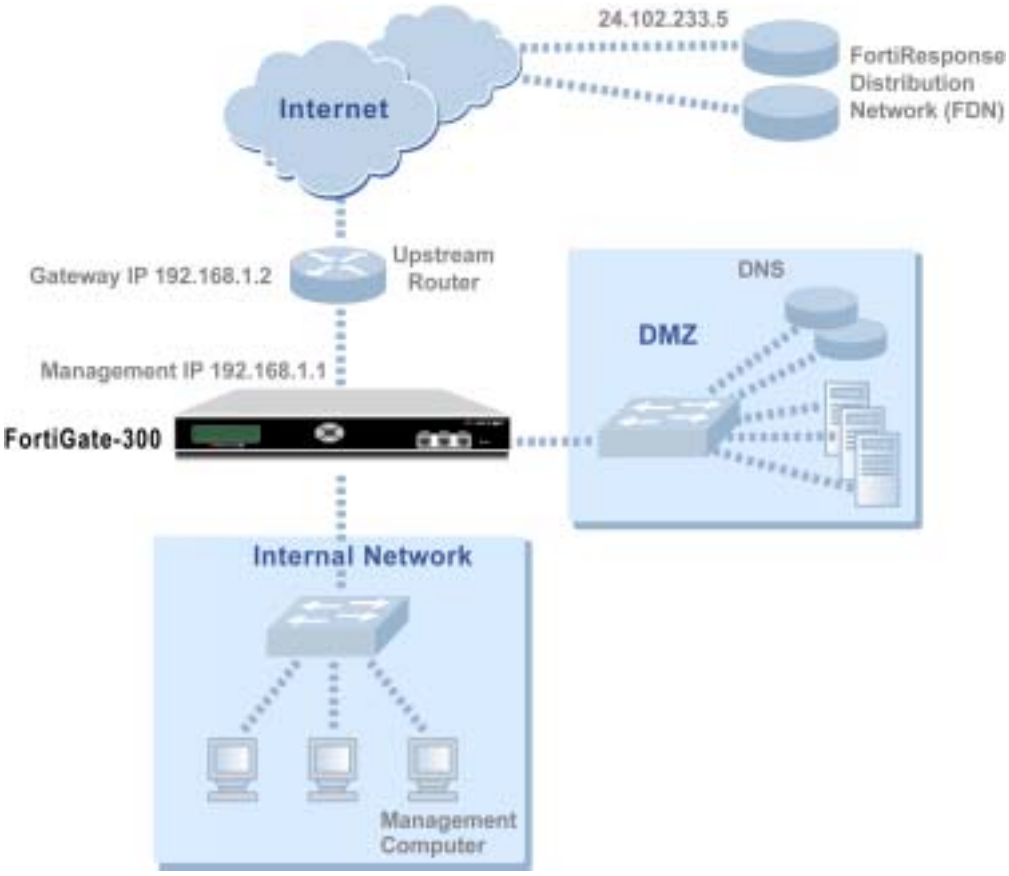
到外部目的地址的静态路由的例子

图 11 展示了需要到 FDN 的路由的 FortiGate 配置的例子。FortiGate 不需要到 DNS 服务器或管理工作站的路由，因为它们位于内部网络中。

要连接到 FDN，您只需要输入一个到外部网络的默认路由。然而如果您希望使用更加安全的方法，除了到外部网络的默认路由外，还可以输入到一个特定 FortiResponse 服务器的静态路由。如果静态路由不可用 （可能是因为 Fortiresponse 服务器的 IP 地址发生了变化），FortiGate 仍可以使用默认路由接收防病毒和 NIDS 更新。

注意：这只是一个配置举例。要配置静态路由，您需要一个 IP 地址。

图 11: 到外部地址的静态路由



通用配置步骤

1 将 FortiGate 设置为透明模式。

2 配置 FortiGate 的管理 IP 地址和网络掩码。

3 配置到 FortiResponse 服务器的静态路由。

4 配置到外部网络的默认路由。

基于 Web 的管理程序配置步骤

要使用基于 Web 的管理程序配置基本的 FortiGate 设置和静态路由：

1 进入 **系统 > 状态**。

- 选择 切换到透明模式。
- 在操作模式列表中选择透明。
- 单击 确定。

FortiGate 现在已经切换到透明模式。

2 进入 **系统 > 网络 > 管理**。

- 修改管理 IP 地址和网络掩码：

  IP： 192.168.1.1

  掩码： 255.255.255.0

- 单击 应用。

3 进入 **系统 > 网络 > 路由**。

- 选择新建 添加到 FortiResponse 服务器的静态路由。

  IP： 24.102.233.5

  掩码： 255.255.255.0

  网关： 192.168.1.2

- 单击 确定。
- 选择新建 添加到外部网络的默认路由。

  IP： 0.0.0.0

  掩码： 0.0.0.0

  网关： 192.168.1.2

- 单击 确定。

CLI 配置步骤

要使用 CLI 配置 FortiGate 基本设置和静态路由：

1 将系统操作模式设置为透明模式。

```
set system opmode transparent
```

2 添加管理 IP 地址和网络掩码。

```
set system management ip 192.168.1.1 255.255.255.0
```

3 添加到主 FortiResponse 服务器的静态路由。

```
set system route number 1 dst 24.102.233.5 255.255.255.0 gw1
  192.168.1.2
```

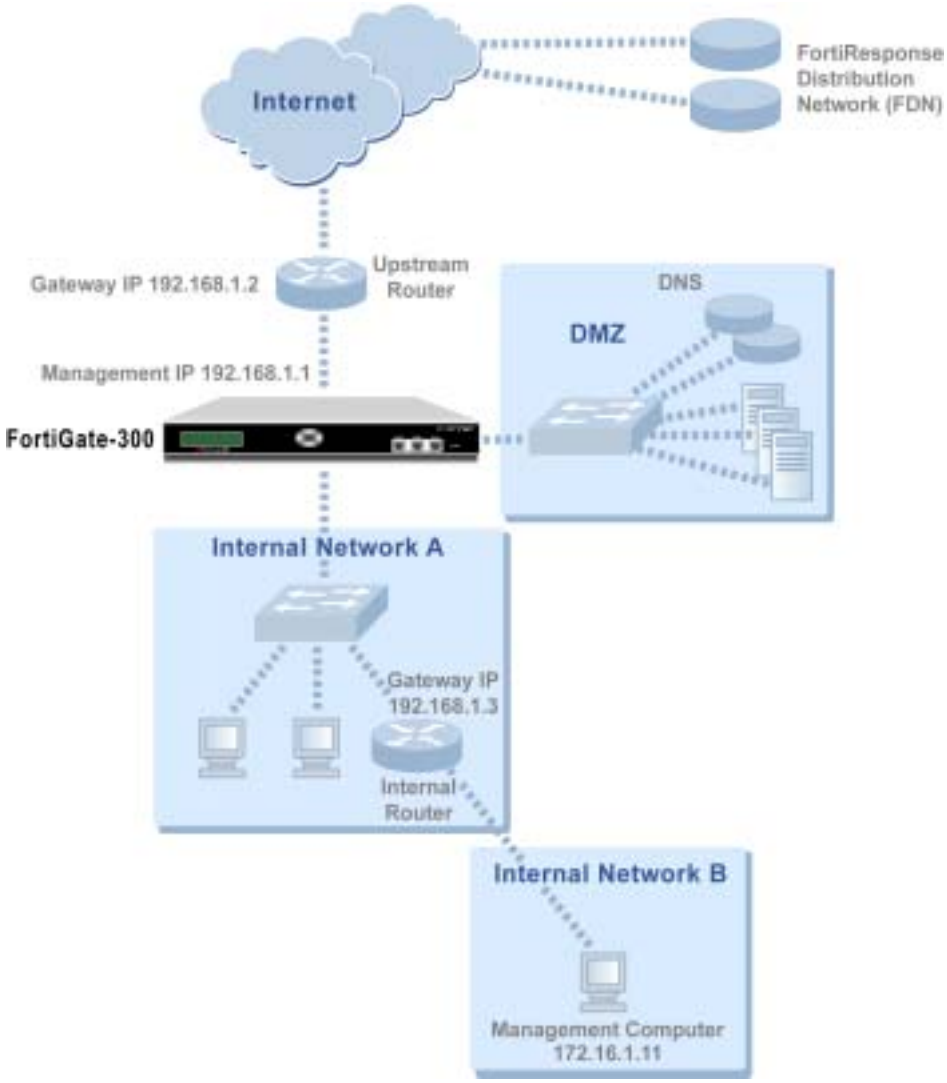
4 添加到外部网络的默认路由。

```
set system route number 2 gw1 192.168.1.2
```

到内部目的地址的静态路由的例子

图 12 展示了 FDN 位于一个外部子网而管理工作站位于一个远程的内部子网的 FortiGate 连接的例子。要达到 FDN，您需要输入一个默认路由指向作为下一个跳跃 / 默认网关的上游路由器。要达到管理工作站，您需要输入一个静态路由定向到它。这个路由指向内部路由器，并将其作为路由的下一个跳跃。（因为 DNS 服务器和 FortiGate 位于相同的第三层子网中，所以不需要为它们设置路由）。

图 12: 到内部目的地址的静态路由



通用配置步骤

1 将 FortiGate 切换到透明模式。
2 配置 FortiGate 的管理 IP 地址和网络掩码。
3 配置到内部网络中的管理工作站的静态路由。
4 配置到外部网络的默认路由。

基于 Web 的管理程序的配置步骤举例

要使用基于 Web 的管理程序配置 FortiGate 基本设置、静态路由和默认路由：

1 进入 **系统 > 状态**。

- 选择切换到透明模式。
- 在操作模式列表中选择透明模式。
- 单击 **确定**。

FortiGate 已经切换到透明模式。

2 进入 **系统 > 网络 > 管理**。

- 修改管理 IP 和网络掩码：

IP： 192.168.1.1
掩码： 255.255.255.0

- 单击 **应用**。

3 进入 **系统 > 网络 > 路由**。

- 选择新建 添加到管理工作站的静态路由。

IP： 172.16.1.11
掩码： 255.255.255.0
网关： 192.168.1.3

- 单击 **确定**。
- 选择新建添加到外部网络的默认路由。

IP： 0.0.0.0
掩码： 0.0.0.0
网关： 192.168.1.2

- 单击 **确定**。

CLI 配置步骤

使用 CLI 配置 FortiGate 基本设置和静态路由、默认路由：

1 将系统操作模式设置为透明模式。

```
set system opmode transparent
```

2 添加管理 IP 地址和掩码。

```
set system management ip 192.168.1.1 255.255.255.0
```

3 添加到管理工作站的静态路由。

```
set system route number 1 dst 172.16.1.11 255.255.255.0 gw1
  192.168.1.3
```

4 添加到外部网络的默认路由。

```
set system route number 2 gw1 192.168.1.2
```

高可用性

Fortinet 通过使用冗余的硬件设备和 FortiGate 聚合协议 （FGCP）实现高可用性（HA）的目标。HA 簇中的 FortiGate 设备全部使用完全相同的安全策略，并共享同样的设置内容。您可以在一个 HA 簇中最多加入 32 个 FortiGate 设备。HA 簇中的每个 FortiGate 设备必须是同一型号的，并且运行同一版本的 FortiOS 固件映像。

FortiGate HA 是一种设备冗余。如果 HA 簇中的某个 FortiGate 设备出现故障而失效，这个设备的全部功能、所有已经建立的防火墙连接和所有 IPSec VPN 会话[1] 将由这个 HA 簇中的其他 FortiGate 设备维持。

在这个 HA 簇中的 FortiGate 设备使用专用的 HA 以太网接口进行簇会话信息通讯和报告各自的系统状态。这个 HA 簇中的设备会一直进行 HA 状态信息通讯以保证 HA 簇工作正常。因此，在这个 HA 簇中全部 FortiGate 设备的 HA 接口之间的连接必须妥善地维护。这些通讯的任何中断都将导致不可预知的后果。

您可以连接到主 FortiGate 的任何接口去管理 HA 簇。

FortiGate 设备可以设置为以主动 - 被动 （A-P）模式或主动 - 主动 （A-A）模式运行。NAT/ 路由模式和透明模式下的 FortiGate 设备都支持主动 - 主动模式和主动 - 被动模式的 HA。

本章提供了一个关于 HA 功能的概述，并描述了在 NAT/ 路由模式和透明模式下如何创建一个 HA 簇。

主动 - 被动 HA

主动 - 被动 （A-P）式的 HA，也可以称作热备份型的 HA，它包含了一个负责处理通讯的主 FortiGate 设备，和一个或多个不处理通讯的附属 FortiGate 设备。附属 FortiGate 设备通过网络与主 FortiGate 设备连接。

在启动过程中，同一个 HA 簇中的成员会彼此协商，以选出一个主设备。主设备可以允许其他 FortiGate 设备作为附属设备加入这个 HA 簇，并为每个附属设备分配优先权。

1.HA 不能为 PPPoE, DHCP, PPTP, 和 L2TP 服务提供会话失效恢复。

主 FortiGate 设备通过 FortiGate HA 接口向附属设备发送会话信息。在同一个 HA 簇中的所有设备共同维护所有的会话信息。如果主 FortiGate 设备失效了，附属设备会互相协商选出一个新的主设备。新的主设备负责恢复所有已经建立的连接。

在失效恢复期间，HA 组会通知附近的网络设备，以使得整个网络可以迅速地转换到新的数据路径中。新的主设备还会将 HA 簇中发生的变动通知管理员。它会在它自己的事件日志中写入一条消息，发送一个 SNMP 陷阱 （如果启用了 SNMP），并且发送一个报警邮件。

如果一个附属的 FortiGate 设备失效了，主 FortiGate 设备会在它自己的事件日志中写入一条消息，发送一个 SNMP 陷阱和一个报警邮件。主 FortiGate 设备还将调整 HA 簇中剩下的设备的优先级。

主动 - 主动 HA

主动 - 主动 （A-A）HA 为同一个 HA 簇中的所有 FortiGate 设备提供负载均衡。一个主动 - 主动 HA 簇包括一个主动 FortiGate 设备和一个或多个附属 FortiGate 设备，所有设备全都参与通讯的处理。主 FortiGate 设备使用一个负载均衡算法将会话分配到 HA 簇中的每个 FortiGate 设备中去。

在主动 - 主动 HA 模式下，主设备使用下面所列出的算法之一在 HA 簇的成员设备中分配网络会话。

表 17：主动 - 主动 HA 负载均衡算法

算法	说明
无	无负载均衡。当 HA 簇接口连接到负载均衡交换机上时使用此选项。
集线器	当 HA 簇接口连接到集线器上时使用此选项。根据包的源 IP 和目的 IP 地址将通讯分配到同一簇的不同设备上。
最小连接	将通讯分配到同一簇的不同设备中，使得每个设备上所承担的连接最少。
循环	依次将每个通讯分配到 HA 簇中的一个设备上。
加权循环	类似于循环算法，但是为 HA 簇中的每个设备根据他们的容量计权。例如，主设备应该具有最低的权重，因为它要负责处理和分配通讯连接。
随机	将通讯随机分配到 HA 簇中的设备上。
IP	根据包的源 IP 地址和目的 IP 地址将通讯分配到 HA 簇的设备上。
IP 端口	根据包的源 IP 地址、目的 IP 地址、源端口、目的端口将通讯分配到 HA 簇的设备上。

HA 簇的成员在启动过程中协商推选出主设备。主设备可以允许其他 FortiGate 设备作为附属设备加入这个 HA 簇，并为每个附属设备分配优先权。

FortiGate 设备通过 FortiGate HA 接口传输状态和会话信息。在同一个 HA 簇中的所有设备共同维护所有的会话信息。在使用负载均衡的工作模式下，主 FortiGate 设备将数据包转发到附属设备，它将数据包从收到数据包的那个接口发送到附属 FortiGate 设备的对应的接口上。

如果主设备失效，在已经失效的主设备上注册的第一个附属设备将成为新的主设备。新的主设备会通知其他的 FortiGate 设备它已经成为主设备，并重新设置剩下的附属设备的优先级。新的主设备还将重新分配 HA 簇中的每个设备所负担的通讯会话。

在失效恢复期间，HA 组会通知附近的网络设备，以使得整个网络可以迅速地转换到新的数据路径中。新的主设备还会将 HA 簇中发生的变动通知管理员。它会在它自己的事件日志中写入一条消息，发送一个 SNMP 陷阱 （如果启用了 SNMP），并且发送一个报警邮件。

如果一个附属的 FortiGate 设备失效了，主 FortiGate 设备会在它自己的事件日志中写入一条消息，发送一个 SNMP 陷阱和一个报警邮件。主 FortiGate 设备还将调整 HA 簇中剩下的设备的优先级。

NAT/ 路由模式下的 HA

按照以下步骤将 NAT/ 路由模式下的一组 FortiGate 设备配置以 HA 方式工作。

- 安装和配置 FortiGate 设备
- 配置 HA 接口
- 配置 HA 簇
- 将 HA 簇连接到您的网络
- 启动 HA 簇

安装和配置 FortiGate 设备

按照 第 29 页 “ NAT/ 路由 模式安装” 的指示安装和配置 FortiGate 设备。HA 组中的所有 FortiGates 应具有相同的配置。在完成 “配置 HA 接口” 之前，先不要将 FortiGate 设备接入网络。

配置 HA 接口

将 HA 簇中的全部 FortiGate-300 的 DMZ/HA 接口配置为 HA 模式。当您将 DMZ/HA 接口配置为 HA 模式的时候，系统 > 配置 >HA 选项变成活动状态。在 HA 模式下运行时，DMZ/HA 接口不能连接到 DMZ 网络，因为它们是 HA 通讯专用的。

每个 FortiGate-300 的 DMZ/HA 接口必须配置不同的 IP 地址。DMZ/HA 接口的 IP 地址必须在同一子网内，并且他们必须配置为可以进行管理访问。

对 HA 组中的所有 FortiGate 重复以下操作：

1. 连接 FortiGate 设备，并登录基于 Web 的管理程序。
2. 进入 **系统 > 网络 > 接口**。
3. 对于 DMZ/HA 接口，单击修改  。
4. 选择 工作于 HA ，把 DMZ/HA 接口配置为 HA 模式。
5. 根据需要修改 IP 地址和子网掩码。
6. 选择这个 HA 接口的管理访问模式：

HTTPS	允许通过这个接口建立到基于 Web 的管理程序的安全的 HTTPS 连接。
PING	如果您希望这个接口响应 PING 请求，则选中此选项。这一设置可以用来验证您的安装和进行网络测试。
HTTP	允许通过此接口建立到基于 Web 的管理程序的 HTTP 连接。HTTP 连接并不安全，有可能被第三方截获。

SSH	允许通过此接口建立到 CLI 的 SSH 连接。
SNMP	允许一个远程 SNMP 管理者连接到此接口并请求 SNMP 管理信息。
TELNET	允许通过此接口建立到 CLI 的 Telnet 连接。Telnet 连接并不安全，有可能被第三方截获。

7 单击应用。

现在您已经完成了对 HA 接口的配置，可以进入下一步 “配置 HA 簇”。

配置 HA 簇

按照以下步骤配置 HA 簇中的 FortiGate。对于 HA 簇中的每一台 FortiGate 都需重复这些步骤。

注意：以下操作叙述了在将 HA 簇连接到您的网络之前如何配置 HA 簇中的每个 FortiGate 设备。您还可以使用 第 59 页 “将 HA 簇连接到您的网络” 中的步骤先将 HA 簇连接到您的网络。

1 连接到 FortiGate 设备并登录基于 Web 的管理程序。

2 进入 **系统 > 配置 > HA**。

3 单击 **HA**。

只有在 DMZ/HA 接口已经配置为 HA 操作模式之后您才能选择 HA。见 第 57 页 “配置 HA 接口”。

4 选择 HA 模式。

选择 **主动 - 被动模式** 可以创建一个主动 - 被动的 HA 组。HA 组中的一台 FortiGate 处于主动模式，处理所有的连接，其它的 FortiGate 处于被动模式，监视主动 FortiGate 的状态并保持与主动设备同步。

选择**主动 - 主动模式**可以创建一个主动 - 主动的 HA 组。在这个 HA 组中，每一台 FortiGate 都主动地处理连接并监视其它的 FortiGate 的状态。

在 HA 簇中的全部 FortiGate 设备的 HA 模式必须相同。

5 为这个 HA 簇设置一个密码。

在这个 HA 簇中，所有的密码必须相同。

6 为这个 HA 簇选择一个**组 ID**。

在这个 HA 中的所有 FortiGate 必须使用相同的组 ID。

7 如果您将设备配置为以主动 - 主动 HA 模式工作，选择一个负载均衡算法。

算法控制主动 - 主动 HA 簇中的 FortiGate 设备之间的负载均衡。在这个 HA 簇中的所有 FortiGate 设备的负载均衡算法必须相同。

无	无负载均衡。当 HA 簇接口连接到负载均衡交换机上时使用此选项。
集线器	用于集线器的负载均衡。当 HA 簇接口连接到集线器上时使用此选项。根据包的源 IP 和目的 IP 地址将通讯分配到同一簇的不同设备上。
最小连接	最小连接负载均衡。如果 FortiGate 设备使用交换机连接，选择最小连接负载均衡可以将通讯分配到同一簇的不同设备中，使得每个设备上所承担的连接最少。
循环	循环负载均衡。如果 FortiGate 设备使用交换机连接，选择循环负载均衡可以依次将每个通讯分配到 HA 簇中的一个设备上。

加权循环	加权循环负载均衡。类似于循环算法，但它是为 HA 簇中的每个设备根据他们的容量和其当前处理的连接数计权。例如，主设备应该具有最低的权重，因为它要负责处理和分配通讯连接。加权循环负载均衡能够将通讯分配得更加均匀，因为处理较少通讯的设备将比处理较多通讯的设备更容易被分配到通讯连接。
随机	随机负载均衡。如果 FortiGate 设备使用交换机连接，选择随机负载均衡可以将通讯随机分配到 HA 簇中的设备上。
IP	根据 IP 地址的负载均衡。如果 FortiGate 设备使用交换机连接，选择 IP 负载均衡可以根据包的源 IP 地址和目的 IP 地址将通讯分配到 HA 簇的设备上。
IP 端口	根据 IP 地址和端口的负载均衡。如果 FortiGate 设备使用交换机连接，选择 IP 和端口负载均衡可以根据包的源 IP 地址、目的 IP 地址、源端口、目的端口将通讯分配到 HA 簇的设备上。

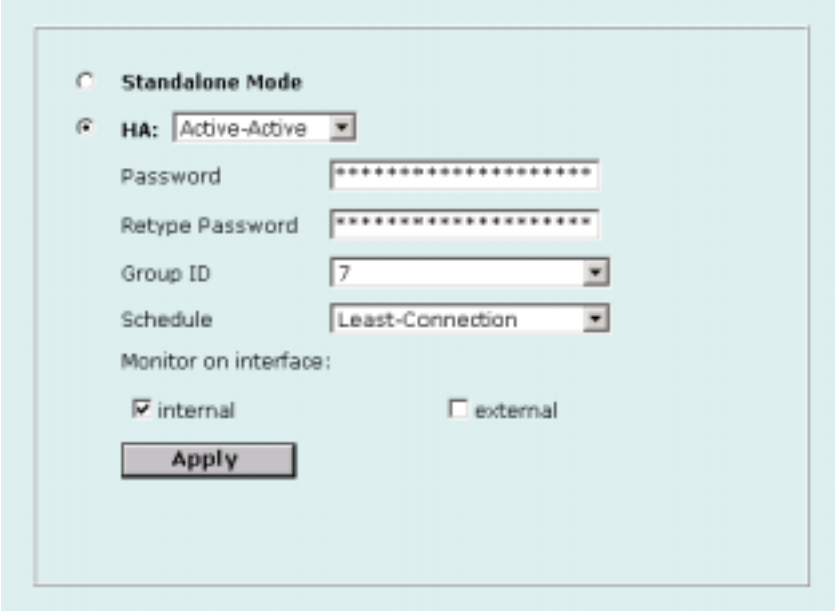
8 在 **端口监视器** 的选项中，选择要监视的的 FortiGate 网络接口的名称。

监视 FortiGate 接口可以确认它们是否已经连接到他们的网络上并且工作正常。如果一个被监视的接口失效或者从它的网络断开，FortiGate 设备将停止处理通讯并从这个 HA 簇中删除。如果您重建通过这个接口的通讯流 （例如，如果您重新连接了一个断开的线缆），FortiGate 设备将重新加入 HA 簇。您只能监视连接到网络的接口。

9 单击应用。

FortiGate 设备相互协商以建立一个 HA 簇。当您选择了应用之后，在 HA 簇协商期间您可能会暂时丢失到 FortiGate 设备的连接。

图 13: 主动 – 主动 HA 配置举例



10 对于 HA 簇中的每个 FortiGate 重复以上操作。

当您配置完全部的 FortiGate 设备之后，可以进行 “将 HA 簇连接到您的网络”操作。

将 HA 簇连接到您的网络

要将 HA 簇接入您的网络，您必须将 HA 簇内所有对应的接口连接到同一个集线器或交换机上。然后您必须将这些接口通过相同的交换机或集线器分别连接到对应的网络上。

还有，您必须将这一 HA 簇中所有的 HA 接口连接到同一交换机或集线器上。您还需要将一台管理员电脑连接到这个交换机或集线器上。这个簇中的设备将一直进行 HA 状态通讯以确保簇工作正常。因此，这个簇中全部 FortiGate 设备的 HA 接口之间的连接必须妥善地维护。这个通讯的任何中断都将导致不可预料的后果。

建议您使用交换机以提高网络的性能。

无论您将 FortiGate 设备配置为主动 - 主动 HA 模式或主动 - 被动 HA 模式，所需的网络设备和配置的步骤都十分相似。

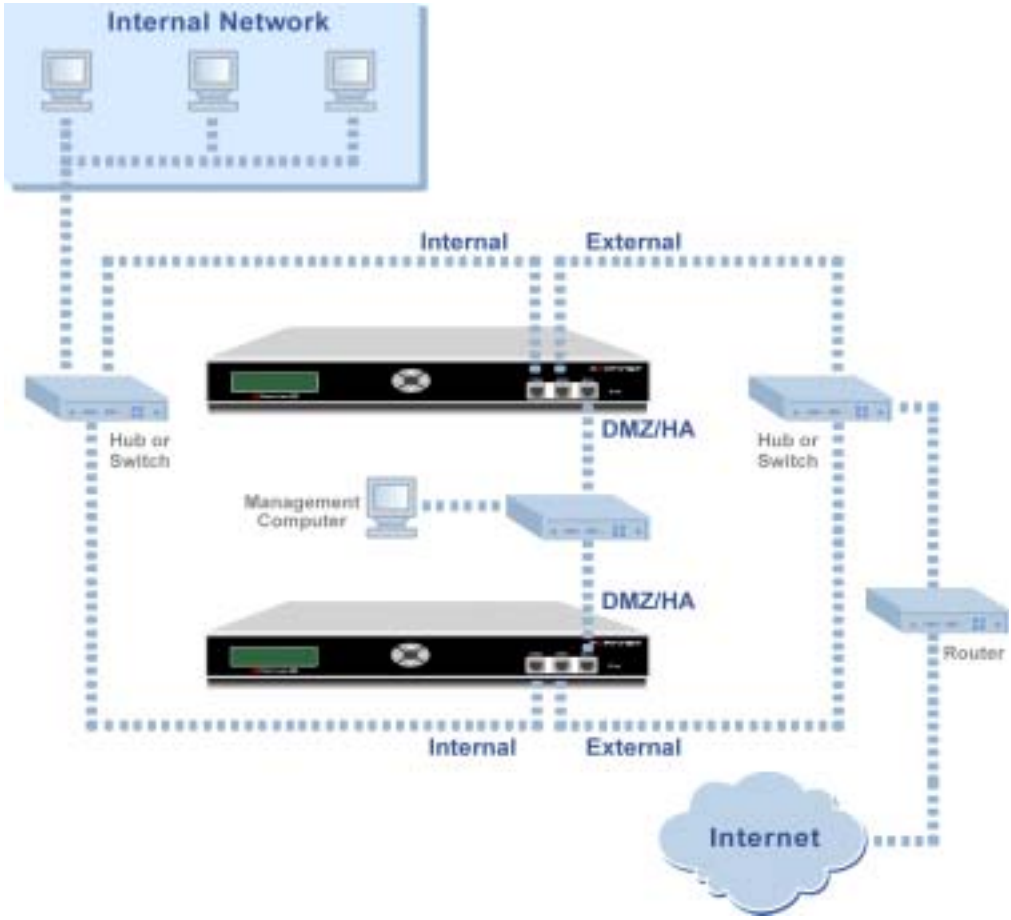
以下操作用于把 FortiGate 连接到您的网络上：

1 将每一台 FortiGate 的内部网络接口都连接到一个与您的部网络相连的交换机或者集线器上。

2 将每一台 FortiGate 的外部网络接口都连接到一个与您外部网络相连的交换机或者集线器上。

3 把 FortiGates 的 DMZ/HA 接口连接到一台单独的交换机或者集线器上。

图 14: HA 网络配置



当您连接完 HA 簇之后，可以进行 “启动 HA 簇”操作。

启动 HA 簇

将 HA 簇中的全部 FortiGate 设备都配置为 HA 并且将这个簇连接起来之后，可以使用以下操作启动 HA 簇。

1 为簇中的所有 HA 设备加电。

在设备启动过程中，它们将协商以选出主簇设备和附属设备。这个协商过程是自动进行的，无须用户干预。

当协商完成后，这个簇已经准备好处理网络通讯了，您可以使用 第 64 页 “管理 HA 组” 中的信息在这个簇登录和进行管理。

透明模式下的 HA

按照如下步骤将运行于透明模式的 FortiGate 设备配置成 HA 簇。

- 安装和配置 FortiGate 设备
- 配置 HA 接口和 IP 地址
- 配置 HA 簇
- 将 HA 簇连接到您的网络中
- 启动 HA 簇

安装和配置 FortiGate 设备

按照 第 29 页 “NAT/路由 模式安装” 的指示安装和配置 FortiGate 设备。HA 组中的所有 FortiGates 应具有相同的配置。在完成 “配置 HA 接口”之前，先不要将 FortiGate 设备接入网络。

配置 HA 接口和 IP 地址

将 HA 簇中的全部 FortiGate-300 的 DMZ/HA 接口配置为 HA 模式。当您将 DMZ/HA 接口配置为 HA 模式的时候，系统 > 配置 >HA 选项必须设置为活动。在 HA 模式下运行时，DMZ/HA 接口不能连接到 DMZ 网络，因为它们是 HA 通讯专用的。

每个 FortiGate-300 的 DMZ/HA 接口必须配置不同的 IP 地址。DMZ/HA 接口的 IP 地址必须在同一子网内，并且他们必须配置为可以进行管理访问。

对 HA 组中的所有 FortiGate 重复以下操作：

1 连接 FortiGate 设备，并登录 基于 Web 的管理程序。

2 进入 **系统 > 网络 > 接口**。

3 对于 DMZ/HA 接口，选择 工作于 HA ，把 DMZ/HA 接口配置为 HA 模式。

4 设置 DMZ/HA 接口的管理访问模式。

HTTPS	允许通过这个接口建立到基于 Web 的管理程序的安全的 HTTPS 连接。
PING	如果您希望这个接口响应 PING 请求，则选中此选项。这一设置可以用来验证您的安装和进行网络测试。
HTTP	允许通过此接口建立到基于 Web 的管理程序的 HTTP 连接。HTTP 连接并不安全，有可能被第三方截获。
SSH	允许通过此接口建立到 CLI 的 SSH 连接。

SNMP 允许一个远程 SNMP 管理者连接到此接口并请求 SNMP 管理信息。

TELNET 允许通过此接口建立到 CLI 的 Telnet 连接。Telnet 连接并不安全，有可能被第三方截获。

5 根据需要修改 IP 地址和子网掩码。

6 可以选择配置其他接口的管理访问方式。

7 单击应用。

现在您已经完成了对 HA 接口的配置，可以进入下一步 “配置 HA 簇”。

配置 HA 簇

在将 HA 簇连接到您的网络之前，按照如下步骤为每个 FortiGate 设备配置 HA。

注意：以下操作叙述了在将 HA 簇连接到您的网络之前如何配置 HA 簇中的每个 FortiGate 设备。您还可以使用 第 63 页 “ 将 HA 簇连接到您的网络中” 中的步骤先将 HA 簇连接到您的网络。

1 连接到 FortiGate 设备并登录进基于 Web 的管理程序。

2 进入 **系统 > 配置 > HA**。

3 单击 **HA**。

只有在 DMZ/HA 接口已经配置为 HA 操作模式之后您才能选择 HA。见 第 61 页 “配置 HA 接口和 IP 地址” 。

4 选择 HA 模式。

选择 主动 - 被动模式 可以创建一个主动 - 被动的 HA 组。HA 组中的一台 FortiGate 处于主动模式，处理所有的连接，其它的 FortiGate 处于被动模式，监视主动 FortiGate 的状态并保持与主动设备同步。

选择主动 - 主动模式可以创建一个主动 - 主动的 HA 组。在这个 HA 组中，每一台 FortiGate 都主动地处理连接并监视其它的 FortiGate 的状态。

在这个 HA 簇中的全部 FortiGate 设备的 HA 模式必须相同。

5 为这个 HA 簇设置一个密码。

在这个 HA 簇中，所有的密码必须相同。

6 为这个 HA 簇选择一个组 ID。

在这个 HA 中的所有 FortiGate 必须使用相同的组 ID。

7 如果您将设备配置为以主动 - 主动 HA 模式工作，选择一个负载均衡算法。

算法控制主动 - 主动 HA 簇中的 FortiGate 设备之间的负载均衡。在这个 HA 簇中的所有 FortiGate 设备的负载均衡算法必须相同。

无 无负载均衡。当 HA 簇接口连接到负载均衡交换机上时使用此选项。

集线器 用于集线器的负载均衡。当 HA 簇接口连接到集线器上时使用此选项。根据包的源 IP 和目的 IP 地址将通讯分配到同一簇的不同设备上。

最小连接 最小连接负载均衡。如果 FortiGate 设备使用交换机连接，选择最小连接负载均衡可以将通讯分配到同一簇的不同设备中，使得每个设备上所承担的连接最少。

循环 循环负载均衡。如果 FortiGate 设备使用交换机连接，选择循环负载均衡可以依次将每个通讯分配到 HA 簇中的一个设备上。

加权循环	加权循环负载均衡。类似于循环算法，但是为 HA 簇中的每个设备根据他们的容量和他们当前处理的连接数计权。例如，主设备应该具有最低的权重，因为它要负责处理和分配通讯连接。加权循环负载均衡能够将通讯分配得更加均匀，因为处理的通讯少的设备将比任务重的设备更容易被分配到通讯连接。
随机	随机负载均衡。如果 FortiGate 设备使用交换机连接，选择随机负载均衡可以将通讯随机分配到 HA 簇中的设备上。
IP	根据 IP 地址的负载均衡。如果 FortiGate 设备使用交换机连接，选择 IP 负载均衡可以根据包的源 IP 地址和目的 IP 地址将通讯分配到 HA 簇的设备上。
IP 端口	根据 IP 地址和端口的负载均衡。如果 FortiGate 设备使用交换机连接，选择 IP 和端口负载均衡可以根据包的源 IP 地址、目的 IP 地址、源端口、目的端口将通讯分配到 HA 簇的设备上。

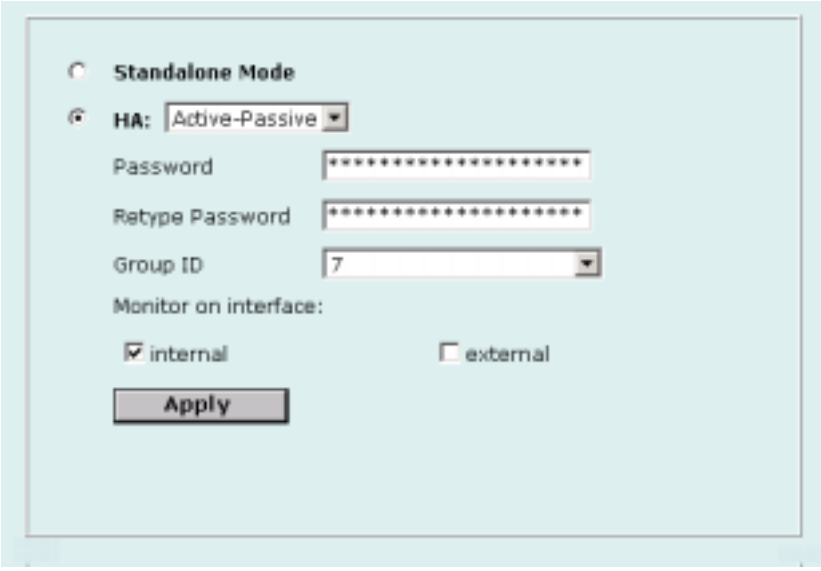
8 在 **端口监视器** 的选项中，选择要监视的的 FortiGate 网络端口。

监视 FortiGate 接口可以确认它们是否已经连接到他们的网络上并且工作正常。如果一个被监视的接口失效或者从它的网络断开，FortiGate 设备将停止处理通讯并从这个 HA 簇中删除。如果您重建通过这个接口的通讯流 （例如，如果您重新连接了一个断开的线缆），FortiGate 设备将重新加入 HA 簇。您只能监视连接到网络的接口。

9 单击应用。

FortiGate 设备相互协商以建立一个 HA 簇。当您选择了应用之后，在 HA 簇协商期间您可能会暂时丢失到 FortiGate 设备的连接。

图 15: 主动 - 被动 HA 配置举例



10 对 HA 簇中的每个 FortiGate 设备重复以上操作。

当您完成了对每个 FortiGate 设备的配置工作之后，可以进入下一步 “将 HA 簇连接到您的网络中”。

将 HA 簇连接到您的网络中

要将 HA 簇接入您的网络，必须将 HA 簇内所有对应的接口连接到同一个集线器或交换机上。然后您必须将这些接口通过相同的交换机或集线器分别连接到对应的网络上。

还有，您必须将这一 HA 簇中所有的 HA 接口连接到同一交换机或集线器上。此外还需要将一台管理员电脑连接到这个交换机或集线器上。

建议使用交换机以提高网络的性能。

无论将 FortiGate 设备配置为主动 - 主动模式 HA 或者主动 - 被动模式 HA，网络设备连接和下面的操作步骤都完全相同。

以下操作用于把 FortiGate 连接到您的网络上：

1 将每一台 FortiGate 的内部网络接口都连接到一个与您的内部网络相连的交换机或者集线器上。

2 将每一台 FortiGate 的外部网络接口都连接到一个与您的外部网络相连的交换机或者集线器上。

3 把 FortiGates 的 DMZ/HA 接口连接到一台单独的交换机或者集线器上。

当您连接了 HA 簇之后，可以进行 “启动 HA 簇”操作。

启动 HA 簇

将 HA 簇中的全部 FortiGate 设备都配置为 HA 并且将这个簇连接起来之后，可以使用以下操作启动 HA 簇。

1 为簇中的所有 HA 设备加电。

在设备启动过程中，它们将协商以选出主簇设备和附属设备。这个协商过程是自动进行的，无须用户干预。

当协商完成后，这个簇已经准备好处理网络通讯了，您可以使用 第 64 页 “管理 HA 组” 中的信息在这个簇登录和进行管理。

管理 HA 组

当 FortiGate 设备启动并运行时，您可以把它作为一个簇进行管理，而不是管理一组独立的 FortiGate 设备。对 HA 簇的管理，可以通过将基于 Web 的管理程序或者 CLI 连接到为管理访问配置好的任何接口来实现。因为这个簇中的全部设备都配置了相同的接口 IP 地址（除了 HA 接口），连接到 IP 地址配置为管理访问连接的任意接口都将自动将连接转到主 FortiGate 设备。

您还可以通过连接到簇中的单独设备的 HA 接口（每个接口配置了不同的 IP 地址）来对它们进行管理。

您也可以通过连接到主设备的 CLI 来管理单独的设备。从这里可以使用命令 **execute ha manage** 连接到簇中的每个设备的 CLI。

本节描述了以下内容：

- 查看 HA 簇成员状态
- 监视簇成员
- 监视簇会话
- 查看和管理簇日志消息
- 单独管理簇中的设备
- 同步簇配置
- 返回到独立模式配置
- 在失效恢复后替换 FortiGate

查看 HA 簇成员状态

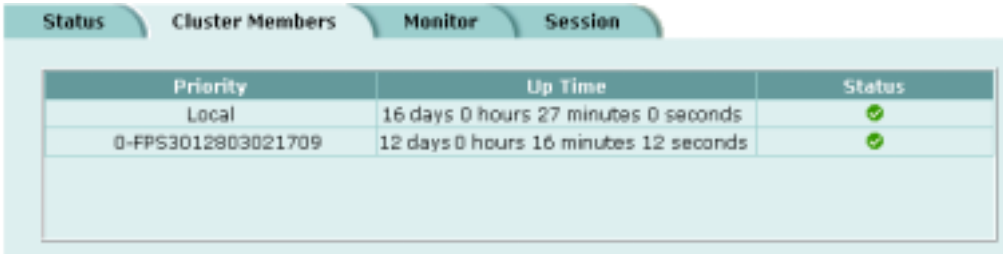
按以下步骤查看 HA 簇成员的状态：

1 连接到 HA 簇中，登录基于 Web 的管理程序。

2 进入 **系统 > 状态 > 簇成员。**

基于 Web 的管理程序显示了这个 HA 簇中的 FortiGate 设备的序列号。主设备的识别符是本地，列表中还包括了簇成员的运行时间和状态。

图 16: 簇成员列表的例子



监视簇成员

按如下步骤操作可以监视每一个簇成员的状态信息。

1 连接到簇并登录基于 Web 的管理程序。

2 进入**系统 > 状态 > 监视器。**

显示每个簇成员的 CPU、内存状态和硬盘状态。主设备的标识符是本地，其他设备则按照序列号列出。

显示内容还包括了当前 CPU 和内存使用率的柱状图示，以及过去数分钟的 CPU 和内存使用率的曲线图。

关于详细信息请见 第 87 页 “ 查看 CPU 和内存状态” 。

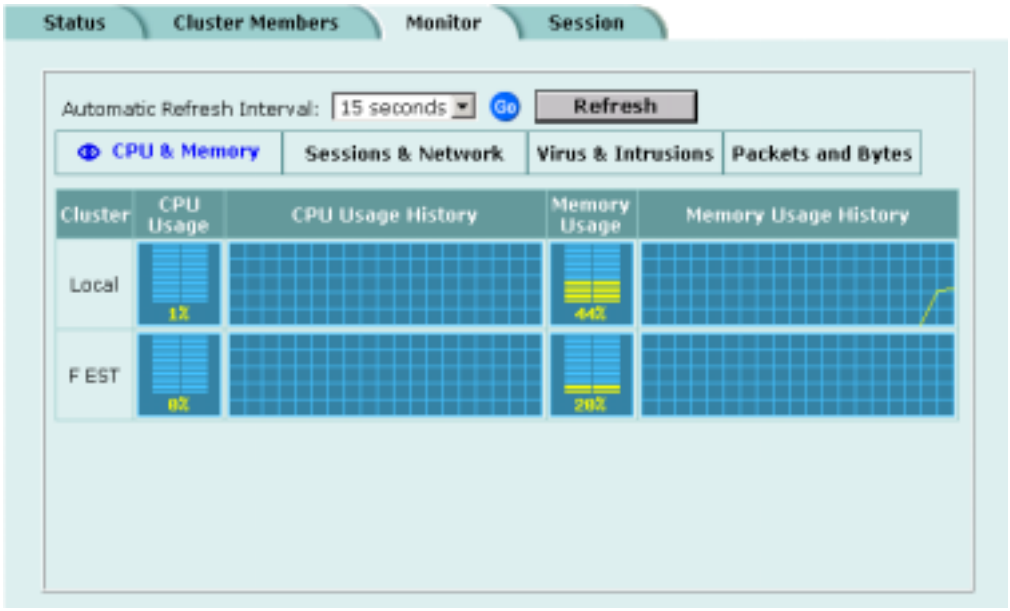
3 选择会话和网络。

显示出每个簇成员的会话和网络状态。主设备的识别标志是本地，其他设备根据他们的序列号列出。

显示的内容还包括当前会话数和当前网络利用率的柱状显示，以及过去数分钟内的会话数和网络利用率的曲线图。曲线图的比例尺在图的左上角显示。

有关详细信息，请见 第 88 页 “ 查看会话和网络状态” 。

图 17: 簇会话数和网络显示的例子



4 选择病毒和入侵。

显示出每个簇成员的病毒和入侵状态。主设备的识别标志是本地，其他设备根据他们的序列号列出。

显示的内容还包括当前每小时检测到的病毒数和当前入侵次数的柱状显示，以及过去 20 小时内的病毒数和入侵次数的曲线图。曲线图的比例尺在图的左上角显示。

有关详细信息，请见 第 88 页 “ 查看病毒和入侵状态” 。

5 选择数据包和字节。

显示每个簇成员处理的数据包数和字节数。

6 您可以设置上述显示内容的刷新次数，然后单击执行以控制基于 Web 的管理程序更新显示的次数。

刷新得越频繁，消耗的系统资源和网络通讯就越多。然而，只有在您使用基于 Web 的管理程序查看显示的时候才会出现这种情况。曲线图比例尺显示在图的右上角。

监视簇会话

如下操作可以查看当前主设备上的会话。

1 连接到簇并登录进基于 Web 的管理程序。

2 进入 **系统 > 状态 > 会话。**

会话表显示了簇中的主设备处理的会话。会话包括主设备和附属设备之间的 HA 通讯。

查看和管理簇日志消息

按如下步骤查看每个簇成员的日志消息：

1 连接到簇并登录基于 Web 的管理程序。

2 进入**日志和报告 > 记录日志。**

显示主设备通讯日志、事件日志、攻击日志、病毒防护日志、网页过滤日志和电子邮件日志。

右上角的下拉列表控制着要显示的日志类别。主设备的识别标志是本地，其他设备根据他们的序列号列出。

3 选择簇中的一个设备的序列号可以显示这个簇成员的日志。

您可以查看保存在内存中的日志或者保存在硬盘中的日志，这取决于这个簇成员的配置。

4 对于簇中的每个设备：

- 您可以查看和搜索日志消息（请见 第 252 页 “ 查看记录到内存的日志” 和 第 253 页 “ 查看和管理保存在硬盘上的日志”）。
- 如果簇中的设备装备了硬盘您可以管理日志消息（请见 第 254 页 “ 将日志文件下载到管理员电脑”，第 254 页 “ 删除当前日志中的全部消息”，和 第 255 页 “ 删除一个保存了的日志文件”）。

注意：您可以查看和管理全部簇成员的日志消息。然而，从主设备上您只能配置主设备的日志记录。要配置簇中其他设备的日志记录，您必须单独对簇中的设备进行管理。

单独管理簇中的设备

您可以通过使用基于 Web 的管理程序或者 CLI 连接到簇中设备的 HA 接口单独管理这个设备。首先，每个设备的 HA 接口必须配置为允许 HTTPS 和 SSH 管理访问。

您还可以按照如下操作连接到簇中的每个设备的 CLI：

从基于 Web 的管理程序单独管理设备：

1 使用 SSH 连接到簇并登录基于 Web 的管理程序。

连接到簇的任何配置了 SSH 管理访问的接口可以自动地登录到主设备。

您还可以使用直接电缆连接登录到主设备的 CLI（首先您要知道哪个设备是主设备，请见 第 69 页 “ 从 FortiGate 设备中选择一个主设备” 以控制哪个 FortiGate 设备成为主设备）。

2 输入以下命令，后边加上一个空格和一个问号（？）：

```
execute ha manage
```

将显示簇中的全部附属设备的列表。这个列表中的每个簇设备从 1 开始编号。显示的每个簇设备的信息包括设备序列号和主机名。

3 在命令后加上附属设备的编号即可登录。例如，要登录到一号附属设备，输入如下命令：

```
execute ha manage 1
```

您可以连接和登录到选定附属设备的 CLI。如果这个附属设备有一个不同的主机名，CLI 的提示符将变成这个主机名。您可以使用 CLI 命令管理这个附属设备。

4 输入以下命令可以返回到主设备的 CLI：

```
exit
```

您可以使用 `execute manage ha` 命令登录到这个簇中的任何其他附属设备的 CLI。

同步簇配置

当运行于簇模式的时候，为了达到较好的效果，必须确保簇中的全部设备的配置始终同步。您可以在主设备上对配置做修改，然后在 HA 簇中的每个附属设备上使用 **execute ha synchronize** 命令手工将它的配置和主设备的配置同步。您可以使用这个命令同步如下内容：

表 18：execute ha synchronize 关键字

关键字	说明
config	同步 FortiGate 配置。包括常规系统配置、防火墙配置、VPN 配置以及其他保存在 FortiGate 配置文件中的内容。
avupd	同步主设备从 Forti 响应发布网络 （FDN）接收的防病毒引擎和防病毒定义。
attackdef	同步主设备从 FDN 接收的 NIDS 攻击定义更新。
weblists	同步主设备上添加或更改的网页过滤列表。
emaillists	同步主设备上添加或更改的电子邮件过滤列表。
resmsg	同步主设备上修改的替换信息。
ca	同步添加到主设备的 CA 证书。
localcert	同步主设备上的本地证书。
all	同步以上全部内容。

使用如下步骤在主设备上修改配置，然后同步附属设备的配置。

1 连接到簇并登录到基于 Web 的管理程序或 CLI。

2 根据需要修改配置。

3 连接到簇中的每个设备的 CLI。

要连接到附属设备，请见 第 67 页 “ 单独管理簇中的设备” 。

4 使用 execute ha synchronize 命令同步附属设备的配置。

对于 HA 簇中的每个设备重复步骤 3 和 4。

返回到独立模式配置

在 HA 簇中的每个 FortiGate 上都重复以下操作，即可返回到独立配置：

1 连接到基于 Web 的管理程序。

2 进入 **系统** > **配置** > **HA**。

3 选择 **独立模式** ，然后单击 **应用**。

现在 FortiGate 设备退出了 **HA 模式** 并返回到了 独立模式。

在失效恢复后替换 FortiGate

失效 - 恢复 出现在软件或者硬件有问题的情况下。当 失效 - 恢复出现时，您可以尝试关闭失效的 FortiGate 的电源再打开它，重新启动这台 FortiGate。如果这个 FortiGate 能够正常地启动，它将重新加入到 HA 组中并正常工作。如果 FortiGate 没能正常启动或者无法重新加入 HA 组中，您必须把它从网络中取出，更换它或者重新配置它。

一旦重新配置或者更换了新的 FortiGate 设备，需要改变它的 HA 配置以与原来失效的 FortiGate 的配置相匹配。然后把它重新连接到网络中。这个 FortiGate 将自动地加入 HA 组中。

高级 HA 选项

可以从 FortiGate CLI 使用以下 HA 高级选项：

从 FortiGate 设备中选择一个主设备

在一个典型的 FortiGate 簇配置中，主设备的选择过程是自动的。HA 簇每次启动之后选定的主设备都可能不同。此外作为主设备运行的 FortiGate 设备也可能会改变（例如，如果当前的主设备重新启动，另一个设备可能会代替它成为主设备）。

在某些情况下，您可能希望控制哪一个设备最终成为主设备。您可以将一个 FortiGate 设备配置为主设备，只需要修改这个设备的优先级使它能控制其他设备。

当簇中的 FortiGate 设备协商主设备的时候，总是拥有最低优先权的设备成为主设备。如果两个设备有同样的优先权，则使用标准的协商过程选择主设备：

以下操作将一个 FortiGate 设备配置为 HA 簇中的永久性的主设备：

1 连接到永久性主 FortiGate 设备的 CLI。

2 设置永久主设备的优先级。输入：

```
set system ha priority <优先级_整数>
```

<优先级_整数> 是永久主设备要设置的优先级。优先级最低的设备将成为主设备。默认的优先级 128。将永久性主设备的优先级设置为一个小于 128 的数。

例如，将永久性主设备的优先级设置为 10，使用如下命令：

```
set system ha priority 10
```

3 确保这个簇中的其他所有设备的优先级高于这个永久性主设备的优先级。

`get system ha mode` 命令显示您当前连接到的 FortiGate 设备的优先级。

4 当永久性主设备加入簇时覆盖一个现有的主设备的设置，使用如下命令：

```
set system ha override enable
```

启用覆盖可以使永久性主设备总是能够覆盖其他主设备的设置。例如，如果永久性主设备关机，簇中的其他另一个设备将代替它成为主设备。当永久性主设备重新启动后，如果它启用了覆盖，它将再次成为主设备。

配置加权轮询的权重

默认情况下，主动 - 主动 HA 模式的加权轮询调度为这个簇中的每个 FortiGate 设备分配相同的权重。一旦这个簇被配置为加权轮询调度，您可以使用 `set system ha weight` 命令为簇中的每个设备配置权重。权重的值设置了在连接被发送到下一个设备之前，发送到这个设备的最大连接数。您可以通过设置权重值来控制每个簇设备能处理的连接数。这项技术的一个用处就是减少主簇设备处理的连接数，只需增加分配给其他附属簇设备的权重。

权重值根据簇中的设备优先级的次序设置。例如，如果您有一个包含了 3 个 FortiGate 设备的 HA 簇，您可以输入以下命令配置每个设备的权重：

```
set system ha weight 1 3 3
```

这个命令有以下结果：

- 第一个连接由主设备处理
- 下面的三个连接由第一个附属设备处理
- 在下面的三个连接由第二个附属设备处理

附属设备将比主设备处理更多的连接，而两个附属设备处理的连接数一样多。

系统状态

您可以连接到基于 Web 的管理程序进入系统 > 状态 以查看您的 FortiGate 设备的当前状态。显示的状态信息包括当前的固件版本，当前的病毒防护定义和攻击定义以及 FortiGate 设备的序列号。

如果您使用管理员帐号 admin 登录到基于 Web 的管理程序，您可以使用系统状态对 FortiGate 系统设置做以下修改：

- 修改 FortiGate 主机名
- 修改 FortiGate 固件
- 手动更新病毒防护定义库
- 手动更新攻击定义库
- 备份系统设备
- 恢复系统设置
- 将系统设置恢复到出厂设置
- 转换到透明模式
- 转换到 NAT/ 路由模式
- 重新启动 FortiGate 设备
- 关闭 FortiGate 设备

如果您使用任何其他管理员帐号登录到基于 Web 的管理程序，您可以进入系统 > 状态 以查看包括如下系统设置：

- 显示 FortiGate 的序列号
- 显示 FortiGate 运行时间
- 显示日志硬盘状态

所有的管理员用户还可以进入系统 > 状态 > 监视器 查看 FortiGate 系统的状态。系统状态显示了 FortiGate 的健康状态监视信息，包括 CPU 和内存状态、会话和网络状态。

- 系统状态

所有的管理员用户也可以进入系统 > 状态 > 会话查看连接到 FortiGate 设备和通过该设备的活动的通讯会话。

- 会话列表

修改 FortiGate 主机名

FortiGate 设备的主机名显示在系统 > 状态页和 FortiGate CLI 提示符中。主机名也被用做 SNMP 系统名 （见 第 131 页 “ 配置 SNMP” ）。

默认的主机名是 FortiGate-300。

按如下步骤修改 FortiGate 主机名：

1 进入 **系统 > 状态。**

2 单击编辑主机名  。

3 输入一个新的主机名。

4 单击确定。

新的主机名将显示在系统状态页并添加到 SNMP 系统名中。

修改 FortiGate 固件

您从 Fortinet 中下载了一个 FortiGate 固件映像之后，您可以按照表 1 中所列的步骤在您的 FortiGate 设备中安装固件映像。

表 1：固件升级步骤

步骤	说明
升级到新版本的固件	通常使用基于 Web 的管理程序和 CLI 操作将 FortiOS 升级到一个新的 FortiOS 固件版本或者同一固件版本的较新的子版本。
恢复到一个旧的固件版本	使用基于 Web 的管理程序 或 CLI 恢复到一个从前版本的固件。这一操作可以将您的 FortiGate 设备恢复到它的出厂默认设置。
使用 CLI 重新启动系统安装固件	使用这一操作可以安装新版本的固件或者恢复一个老版本的固件。您只能使用 FortiGate 串行通讯接口和串行通讯线缆通过 CLI 执行这一操作。这一操作将您的 FortiGate 设备恢复到它的出厂默认设置。
在安装新版本的固件之前进行测试	使用这一操作可以在安装新版本的固件映像之前对它进行测试。您只能使用 FortiGate 串行通讯接口和串行通讯线缆通过 CLI 执行这一操作。这一操作临时安装新版本的固件映像并使用您当前的系统配置。您可以在永久性地安装它之前测试固件映像。如果固件映像能够正常工作，您可以使用本表中列出的其他方法永久性地安装固件映像。
安装和使用一个备份了的固件映像	如果您的 FortiGate 设备运行的是 v3.x 版本的 BIOS，您可以安装一个备份固件映像。安装完固件映像备份之后，您根据需要切换到这个备份映像。

升级到新版本的固件

使用以下操作可以将您的 FortiGate 设备的固件升级到的版本。

使用基于 Web 的管理程序升级固件

注意：安装固件将使用您所安装的固件中包含的病毒防护定义和攻击定义替换您当前的病毒防护定义和攻击定义。当您安装一个新的固件时，使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中的步骤确保病毒防护定义和攻击定义是最新的。

1 将固件映像文件拷贝到您的管理员电脑。

2 使用 admin 管理员帐号登录到基于 Web 的管理程序。

3 进入 **系统** > **状态**。

4 单击 **固件升级**  。

5 输入固件升级文件的文件名，或者单击 **浏览** 然后定位那个文件。

6 单击确定。

FortiGate 设备将上载固件映像文件，升级到新的固件版本，重新启动，然后显示 FortiGate 登录界面。这一步骤需要数分钟时间。

7 登录到基于 Web 的管理程序。

8 进入 **系统** > **状态**检查固件的版本，确认固件的升级版本已经成功地安装了。

9 使用 第 95 页 “手工更新病毒防护定义和攻击定义” 中的操作更新病毒防护定义和攻击定义。

使用 CLI 升级固件

必须有一个可以从 FortiGate 连接到的 TFTP 服务器才能按照下述步骤升级。

注意：安装固件将使用您所安装的固件中包含的病毒防护定义和攻击定义替换您当前的病毒防护定义和攻击定义。当您安装一个新的固件时，使用 第 95 页 “手工更新病毒防护定义和攻击定义” 中的步骤确保病毒防护定义和攻击定义是最新的。您也可以使用 CLI 命令 `execute updatecenter updatenow` 更新病毒防护定义和攻击定义。

1 确保 TFTP 正在运行。

2 将新的固件映像文件拷贝到 TFPT 服务器的根目录下。

3 用 admin 帐号登录到 FortiGate。

4 确保 FortiGate 可以连接到 TFTP 服务器。

确认您可以从 FortiGate 连接到 TFTP 服务器上。具体方法是使用以下命令 ping 运行 TFPT 服务的电脑。例如，如果 TFTP 服务器的 IP 地址是 192.168.1.168：

```
execute ping 192.168.1.168
```

5 输入下述命令将固件映像文件从 TFPT 服务器拷贝到 FortiGate 上：

```
execute restore image <名称_字符串> <tftp_ip>
```

<名称_字符串> 是 TFTP 服务器上的固件映像文件的文件名，**<tftp_ip>** 是 TFTP 服务器的 IP 地址。例如，如果固件映像文件的文件名是 FGT-60-v236-build068-FORTINET.out ，TFTP 服务器的 IP 地址为 192.168.1.168，输入：

```
execute restore image FGT-60-v236-build068-FORTINET.out
192.168.1.168
```

FortiGate 上载固件映像文件，升级到新版本的固件，重新启动。这一过程需要一些时间。

6 重新连接到 CLI。

7 要确认新版本的固件已经加载了，输入：

```
get system status
```

8 使用 第 95 页 “手工更新病毒防护定义和攻击定义” 中的操作更新病毒防护定义和攻击定义，或者使用 CLI，输入

```
execute updatecenter updatenow
```

9 要确认病毒防护定义和攻击定义是否已经被更新，输入以下命令显示病毒防护引擎、病毒和攻击定义的版本，合同有效期和最新更新信息。

```
get system objver
```

恢复到一个旧的固件版本

按照如下操作可以将您的 FortiGate 设备恢复到一个旧的固件版本。

使用基于 Web 的管理程序恢复到一个旧版本的固件

以下操作将您的 FortiGate 设备恢复到它的出厂时的默认配置状态，并删除 NIDS 用户定义的特征，网页内容列表，电子邮件过滤列表和您对替换信息所做的修改。

您可以在进行这一操作之前先进行：

- 备份 FortiGate 设备的配置，使用 第 84 页 “ 备份系统设备” 中的步骤。
- 备份 NIDS 用户定义的特征，请见 *FortiGate NIDS 指南*。
- 备份网页内容和电子邮件过滤列表，请见 *FortiGate 内容保护指南*。

如果您要恢复到一个旧版本的 FortiOS （例如，从 FortiOS v2.50 恢复到 v2.36），您可能无法恢复您的配置备份文件中保存的从前的配置。

注意：安装固件将使用您所安装的固件中包含的病毒防护定义和攻击定义替换您当前的病毒防护定义和攻击定义。当您安装一个新的固件时，使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中的步骤确保病毒防护定义和攻击定义是最新的。

1 将固件映像文件拷贝到您的管理员电脑。

2 使用 admin 管理员帐号登录到基于 Web 的管理程序。

3 进入 **系统 > 状态**。

4 单击 **固件升级**  。

5 输入固件升级文件的文件名和路径，或者单击 **浏览** 然后定位那个文件。

6 单击 **确定**。

FortiGate 将上载升级文件，回复到旧版本的固件并重新启动，复位系统配置，重新启动，显示 FortiGate 登录提示。这一过程需要几分钟的时间。

7 登录到基于 Web 的管理程序。

当 FortiGate 设备设置为出厂默认设置时，关于登录到基于 Web 的管理程序的详细信息请见 第 18 页 “ 连接到基于 Web 的管理程序” 。

8 进入 **系统 > 状态** 检查固件的版本，确认固件已经被成功地安装上了。

9 恢复您的配置。

请见 第 84 页 “ 恢复系统设置” 如何恢复您从前的配置。

10 使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中的步骤更新病毒防护定义和攻击定义。

使用 CLI 恢复到一个旧版本的固件

以下操作将您的 FortiGate 设备恢复到它的出厂时的默认配置状态，并删除 NIDS 用户定义的特征，网页内容列表，电子邮件过滤列表和您对替换信息所做的修改。

您可以在进行这一操作之前先进行：

- 使用命令 `execute backup config` 备份 FortiGate 设备的配置。
- 使用命令 `execute backup nidsuserdefsig` 备份 NIDS 用户定义的特征。
- 备份网页内容和电子邮件过滤列表，请见 *FortiGate 内容保护指南*。

如果您要恢复到一个旧版本的 FortiOS （例如，从 FortiOS v2.50 恢复到 v2.36），您可能无法恢复您的配置备份文件中保存的从前的配置。

注意：安装固件将使用您所安装的固件中包含的病毒防护定义和攻击定义替换您当前的病毒防护定义和攻击定义。当您安装一个新的固件时，使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中的步骤确保病毒防护定义和攻击定义是最新的。您也可以使用 CLI 命令 `execute updatecenter updatenow` 更新病毒防护定义和攻击定义。

您必须有一个可以从 FortiGate 连接到的 TFTP 服务器才能按照下述步骤升级。

1 确保 TFTP 正在运行。

2 将您要恢复的固件映像文件拷贝到 TFPT 服务器的根目录下。

3 用 admin 帐号登录到 FortiGate。

4 确保 FortiGate 可以连接到 TFTP 服务器。

确认您可以从 FortiGate 连接到 TFTP 服务器上。具体方法是使用以下命令 ping 运行 TFPT 服务的电脑。例如，如果 TFTP 服务器的 IP 地址是 192.168.1.168：

```
execute ping 192.168.1.168
```

5 输入下述命令将固件映像文件从 TFPT 服务器拷贝到 FortiGate 上：

```
execute restore image < 名称 _ 字符串 > <tftp_ip>
```

〈名称 _ 字符串〉是 TFTP 服务器上的固件映像文件的文件名，〈tftp_ip〉是 TFTP 服务器的 IP 地址。例如，如果固件映像文件的文件名是 FGT-60-v236-build068-FORTINET.out ，TFTP 服务器的 IP 地址为 192.168.1.168，输入：

```
execute restore image FGT_300-v250-build045-FORTINET.out
192.168.1.168
```

FortiGate 将上载升级文件。一旦文件上载完成，将显示如下信息：

```
Get image from tftp server OK.
This operation will downgarde the current firmware version!
Do you want to continue? (y/n)
```

6 输入 Y。

FortiGate 设备回复到旧版本的固件，将配置恢复到出厂默认设置，并重新启动。这一过程将需要几分钟时间。

7 重新连接到 CLI。

关于在 FortiGate 设备的出厂默认状态下连接到 CLI 的详细信息，请见 第 19 页 “ 连接到命令行接口 (CLI)” 。

8 要确认回复的版本的固件已经加载了，输入：

```
get system status
```

9 要恢复到您从前的配置，使用如下命令：

```
execute restore config
```

10 使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中描述的步骤更新病毒防护定义和攻击定义，或从 CLI 输入

```
execute updatecenter updatenow
```

11 要确认病毒防护定义和攻击定义是否已经被更新，输入以下命令显示病毒防护引擎、病毒和攻击定义的版本，合同有效期和最新更新信息。

```
get system objver
```

使用 CLI 重新启动系统安装固件

这一方法可以安装给定的固件映像并把 FortiGate 恢复到默认设置。您可以使用这一方法把固件升级到一个新版本，或者恢复一个固件的旧版本，或者重新安装当前版本的固件。

注意：在不同的版本的 FortiGate BIOS 中这一操作有一些细微的不同。这些不同在受到影响的操作步骤中有相应的说明。您使用串行通讯线缆连接到 FortiGate 串行通讯接口访问 CLI 的时候，您的 FortiGate 设备会在重新启动过程中显示所运行的 BIOS 版本。

要执行这一操作您需要：

- 使用一条串行通讯线缆连接到 FortiGate 串行通讯接口访问 CLI。
- 安装一个 TFTP 服务器，并使内部网络接口可以连接到此服务器上。TFTP 服务器必须和 FortiGate 的内部网络接口在同一子网内。

在执行这一操作之前您可以：

- 备份 FortiGate 设备的配置，使用 第 84 页 “ 备份系统设备” 中的步骤。
- 备份 NIDS 用户定义的特征，请见 *FortiGate NIDS 指南*。
- 备份网页内容和电子邮件过滤列表，请见 *FortiGate 内容保护指南*。

如果您要恢复到一个旧版本的 FortiOS （例如，从 FortiOS v2.50 恢复到 v2.36），您可能无法恢复您的配置备份文件中保存的从前的配置。

注意：安装固件将使用您所安装的固件中包含的病毒防护定义和攻击定义替换您当前的病毒防护定义和攻击定义。当您安装一个新的固件时，使用 第 95 页 “ 手工更新病毒防护定义和攻击定义” 中的步骤确保病毒防护定义和攻击定义是最新的。

从系统重新启动中安装固件

1 使用一根零调制解调器电缆和 FortiGate 控制端口连接到 CLI。

2 确认 TFTP 服务器工作正常。

3 将新版本的固件映像文件拷贝到您的 TFTP 服务器的根目录下。

4 确认 FortiGate 的内部接口和 TFTP 服务器连接到同一网络上。

5 确认您可以从 FortiGate 连接到 TFTP 服务器上。具体方法是使用以下命令 ping 运行 TFPT 服务的电脑。例如，如果 TFTP 服务器的 IP 地址是 192.168.1.168：

```
execute ping 192.168.1.168
```

6 输入以下命令重新启动 FortiGate：

```
execute reboot
```

在 FortiGate 设备启动过程中，将显示一系列的系统启动信息。

当下面信息之一显示的时候：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

```
Press Any Key To Download Boot Image.
...
```

- 运行 v3.x 版 BIOS 的 FortiGate 设备

```
Press any key to enter configuration menu.....
......
```

7 立刻按任意键中断系统启动过程。

注意：您只有三秒钟时间按动任意键。如果您没有尽快地按任何一个键，FortiGate 将完成重新启动的步骤，而您就必须登录进去然后重新执行 `execute reboot` 命令。

如果您成功地中断了启动过程，将显示下面的消息之一：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

```
Enter TFTP Server Address [192.168.1.168]:
```

转到步骤 9。

- 运行 v3.x 版 BIOS 的 FortiGate 设备

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:
```

8 按 G 从 TFTP 服务器获得新版本的固件。

9 输入 TFTP 服务器的地址并按回车。

将显示以下信息：

```
Enter Local Address [192.168.1.188]:
```

10 输入 FortiGate 设备的内部网络接口的地址然后回车。

注意：本地 IP 地址只能用来下载固件映像。固件安装完之后，内部网络接口的 IP 地址将被网络接口的默认 IP 地址。

将会出现以下消息：

```
Enter File Name [image.out]:
```

11 输入固件文件的名称然后回车。

TFPT 服务器会把固件的映像文件上载到 FortiGate 上，并会出现类似以下消息：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

  ```
  Do You Want To Save The Image? [Y/n]
  ```

  输入 Y。

- 运行 v3.x 版 BIOS 的 FortiGate 设备

  ```
  Save as Default firmware/Run image without saving:[D/R]
  Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
  ```

  输入 D。

FortiGate 设备安装新版本的固件映像并重新启动。整个安装过程可能需要几分钟时间才能完成。

恢复您从前的配置

您现在可以恢复您从前的配置。首先要根据需要修改接口的地址。您可以从 CLI 执行如下命令：

```
set system interface
```

修改完接口地址后，您可以从基于 Web 的管理程序访问 FortiGate 设备并恢复您的配置。

要恢复您的 FortiGate 设备的配置，请见 第 84 页 “恢复系统设置”。要恢复 NIDS 用户定义特征，请见 *FortiGate NIDS 指南*。要恢复网页内容和邮件过滤列表，请见 *FortiGate 内容保护指南*。

如果您是回复到一个从前版本的固件（例如，从 FortiOS2.50 回复到 FortiOS v2.36），您可能无法恢复您保存过的配置文件。

12 将病毒防护和攻击定义更新到最新版本，请见 第 95 页 “手工更新病毒防护定义和攻击定义”。

在安装新版本的固件之前进行测试

您可以在从系统重新启动安装新版本固件之前先测试这个版本的固件映像并将它保存到系统内存。这一操作完成之后，FortiGate 设备将使用新的固件映像运行，但是仍旧使用当前的配置。这一新版本的固件映像并没有永久性地安装。下一次 FortiGate 重新启动的时候将重新使用原来的固件映像和当前的配置。如果新的固件映像能够正常运行，你可以按照 第 72 页 “升级到新版本的固件” 中的步骤永久性地安装它。

要执行这一操作您需要：

- 使用一根零调制解调器电缆连接到 FortiGate 的控制端口，以访问 CLI。
- 安装一个 TFTP 服务器，并使内部网络接口可以连接到此服务器上。TFTP 服务器必须和 FortiGate 的内部网络接口在同一子网内。

用以下方法测试固件：

1 使用一根零调制解调器电缆和 FortiGate 控制端口连接到 CLI。

2 确认 TFTP 服务器工作正常。

3 将新版本的固件映像文件拷贝到您的 TFTP 服务器的根目录下。

4 确认 FortiGate 的内部接口和 TFTP 服务器连接到内部网络上。

确认您可以从 FortiGate 连接到 TFTP 服务器上。具体方法是使用以下命令 ping 运行 TFPT 服务的电脑。例如，如果 TFTP 服务器的 IP 地址是 192.168.1.168：

```
execute ping 192.168.1.168
```

5 输入以下命令重新启动 FortiGate：

```
execute reboot
```

6 在 FortiGate 重新启动过程中，按任意键中断系统启动过程。

在 FortiGate 设备启动过程中，将显示一系列的系统启动信息。

当下面信息之一显示的时候：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

```
Press Any Key To Download Boot Image.
...
```

- 运行 v3.x 版 BIOS 的 FortiGate 设备

```
Press any key to enter configuration menu.....
......
```

7 立刻按任意键中断系统启动过程。

注意：您只有三秒钟时间按动任意键。如果您没有尽快地按任何一个键，FortiGate 将完成重新启动的步骤，而您就必须登录进去然后重新执行 execute reboot 命令。

如果您成功地中断了启动过程，将显示下面的消息之一：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

```
Enter TFTP Server Address [192.168.1.168]:
```

转到步骤 9。

- 运行 v3.x 版 BIOS 的 FortiGate 设备

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,Q,or H:
```

8 按 G 从 TFTP 服务器获得新版本的固件。

9 输入 TFTP 服务器的地址并按回车。

将显示以下信息：

```
Enter Local Address [192.168.1.188]:
```

10 输入 FortiGate 设备的内部网络接口的地址然后回车。

注意：本地 IP 地址只能用来下载固件映像。固件安装完之后，内部网络接口的 IP 地址将被网络接口的默认 IP 地址。

将会出现以下消息：

```
Enter File Name [image.out]:
```

11 输入固件文件的名称然后回车。

输入固件文件的名称然后回车。

TFPT 服务器会把固件的映像文件上载到 FortiGate 上，并会出现类似以下消息：

- 运行 v2.x 版 BIOS 的 FortiGate 设备

  ```
  Do You Want To Save The Image? [Y/n]
  ```

  输入 N。

- 运行 v3.x 版 BIOS 的 FortiGate 设备

  ```
  Save as Default firmware/Run image without saving:[D/R]
  ```

  输入 R。

FortiGate 固件映像将被安装到系统内存，然后 FortiGate 开始使用新的固件映像并保持当前的配置。

12 您可以使用任何管理员帐号登录到 CLI 或者基于 Web 的管理程序。

13 要确认新版本的固件已经加载了，可以从 CLI 输入：

```
get system status
```

您可以根据需要测试新版本的固件。

安装和使用一个备份了的固件映像

如果您的 FortiGate 设备运行的 BIOS 是 v3.x 版，您可以安装一个备份固件映像。在备份固件映像安装成功之后您可以在需要时切换到备份映像上。

本节叙述了如下内容：

安装备份固件映像

要进行这一操作您需要：

- 使用一根零调制解调器电缆连接到 FortiGate 的控制端口，以访问 CLI。
- 安装一个您可以从 FortiGate 连接到的 TFTP 服务器，如同 第 76 页 “使用 CLI 重新启动系统安装固件” 中的步骤所描述的那样。

要安装备份固件映像：

1 使用一根零调制解调器电缆和 FortiGate 控制端口连接到 CLI。

2 确认 TFTP 服务器工作正常。

3 将新版本的固件映像文件拷贝到您的 TFTP 服务器的根目录下。

4 确认您可以从 FortiGate 连接到 TFTP 服务器上。具体方法是使用以下命令 ping 运行 TFPT 服务的电脑。例如，如果 TFTP 服务器的 IP 地址是 192.168.1.168：

```
execute ping 192.168.1.168
```

5 输入以下命令重新启动 FortiGate：

```
execute reboot
```

在 FortiGate 设备启动过程中，将显示一系列的系统启动信息。

当下面信息之一显示的时候：

```
Press any key to enter configuration menu.....
......
```

6 立刻按任意键中断系统启动过程。

注意：您只有三秒钟时间按动任意键。如果您没有尽快地按任何一个键，FortiGate 将完成重新启动的步骤，而您就必须登录进去然后重新执行 execute reboot 命令。

如果您成功地中断了启动过程，将显示下面的消息之一：

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:
```

7 按 G 从 TFTP 服务器获得新版本的固件。

8 输入 TFTP 服务器的地址并按回车。

将显示以下信息：

```
Enter Local Address [192.168.1.188]:
```

9 输入 FortiGate 设备可以连接到 TFTP 服务器的接口地址然后按回车。

将显示以下信息：

```
Enter File Name [image.out]:
```

10 输入固件文件的名称然后回车。

TFPT 服务器会把固件的映像文件上载到 FortiGate 上，并会出现类似以下消息：

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]
```

11 输入 B。

FortiGate 设备将保存备份固件映像并重新启动。当 FortiGate 设备重新启动时它将运行原先安装的版本的固件。

切换到备份固件影象

使用如下步骤将您的 FortiGate 设备切换到以您安装过的备份固件影响运行。当您将 FortiGate 设备切换到备份固件映像时，FortiGate 设备将使用与固件映像一同保存的配置运行。

如果您从重启动方式安装了一个备份映像，跟固件映像一同保存的是出厂默认的配置。如果使用 第 82 页 “ 切换回默认的固件映像” 中所描述的步骤切换到曾经作为默认固件映像运行过的备份固件映像，随同这个固件映像一同保存的配置将被恢复。

1 使用一根零调制解调器电缆和 FortiGate 控制端口连接到 CLI。

2 输入以下命令重新启动 FortiGate：
```
execute reboot
```
在 FortiGate 设备启动过程中，将显示一系列的系统启动信息。
当下面信息之一显示的时候：
```
Press any key to enter configuration menu.....
......
```

3 立刻按任意键中断系统启动过程。

注意：您只有三秒钟时间按动任意键。如果您没有尽快地按任何一个键，FortiGate 将完成重新启动的步骤，而您就必须登录进去然后重新执行 execute reboot 命令。

如果您成功地中断了启动过程，将显示下面的消息之一：
```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:
```

4 输入 B 加载备份固件映像。

FortiGate 设备将加载固件映像并重新启动。当 FortiGate 重新启动时它将运行备份固件并将配置设置为出厂默认状态。

切换回默认的固件映像

使用下面的操作可以将您的 FortiGate 设备切换到以曾经作为默认固件映像运行过的备份固件运行。当您切换到备份固件映像的时候，同这个固件一起被保存的配置将被恢复。

1 使用一根零调制解调器电缆和 FortiGate 控制端口连接到 CLI。

2 输入以下命令重新启动 FortiGate：
```
execute reboot
```
在 FortiGate 设备启动过程中，将显示一系列的系统启动信息。
当下面信息之一显示的时候：
```
Press any key to enter configuration menu.....
......
```

3 立刻按任意键中断系统启动过程。

注意：您只有三秒钟时间按动任意键。如果您没有尽快地按任何一个键，FortiGate 将完成重新启动的步骤，而您就必须登录进去然后重新执行 execute reboot 命令。

如果您成功地中断了启动过程，将显示下面的消息之一：

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:
```

4 输入 B 以加载备份固件映像。

FortiGate 设备将加载备份固件映像并重新启动。当 FortiGate 设备再次启动的时候它回使用恢复的配置和备份固件映像运行。

手动更新病毒防护定义库

按照以下步骤手动更新病毒防护定义库。

注意：如果想把 FortiGate 配置为自动更新病毒防护定义库，请参阅 第 91 页 “ 病毒和攻击定义升级及注册” 。您也可以进入 **系统 > 更新** 然后选择现在更新，从而手动更新您的病毒防护定义库。

1 从 FortiNet 下载最新的病毒防护定义库更新文件，然后把它拷贝到用来连接基于 Web 的管理程序的电脑上。

2 启动基于 Web 的管理程序，进入 **系统 > 状态**。

3 在 病毒防护定义库的右边，单击 更新定义 。

4 输入病毒防护定义库更新文件的路径和文件名，或者单击 浏览 然后在浏览器中定位该文件。

5 单击 确定 ，将病毒防护定义库文件上载到 FortiGate 设备上。

FortiGate 将上载病毒防护定义库更新文件，整个过程将持续约 1 分钟。

6 进入 **系统 > 状态** 检查病毒防护定义库的版本信息，确定它已经被更新了。

手动更新攻击定义库

按照以下步骤手动更新的攻击定义库。

注意：要将 FortiGate 配置为自动更新攻击定义库，请参阅 第 91 页 “ 病毒和攻击定义升级及注册” 。也可以进入 **系统 > 更新** 选择现在更新以手动更新攻击定义库。

1 从 Fortinet 下载最新版本的攻击定义库更新文件，并将文件拷贝到您用来连接基于 WEB 的管理程序的电脑上。

2 启动基于 WEB 的管理程序并进入**系统 > 状态**。

3 在 **攻击定义库版本** 的右边，单击 **更新定义** 。

4 输入攻击定义库更新文件的路径和文件名，或者单击 **浏览** 然后在浏览器中定位攻击定义库文件。

5 单击 **确定** 将攻击定义库文件上载到 FortiGate。
FortiGate 将更新新的攻击定义库，整个过程将持续约 1 分钟。

6 进入 **系统 > 状态** 查看攻击定义库的信息，确认它已经被更新了。

显示 FortiGate 的序列号

1 进入 **系统 > 状态**。.
序列号 显示在基于 Web 的管理程序的系统状态页面。序列号是分配给您的 FortiGate 的唯一标识，即使固件更新了也不会改变。

显示 FortiGate 运行时间

1 进入 **系统 > 状态**。
FortiGate 运行时间以天、小时、分钟显示了 FortiGate 设备从启动到现在所经历的时间。

显示日志硬盘状态

1 进入 **系统 > 状态。**

如果 FortiGate 设备包含了一个硬盘则可显示日志硬盘状态。如果没有安装硬盘，则此功能不可用。FortiGate 设备使用硬盘保存日志消息和隔离的被病毒感染的文件或被防病毒保护功能阻塞的文件。

备份系统设备

可以将系统设置下载到管理员电脑上并保存成一个文本文件，从而以这种方式备份它们：

1 进入 **系统 > 状态**。
2 选择 **系统设置备份**。
3 选择 **备份系统设置**。
4 输入 **文件名** 和 **路径** 。
系统设置文件将被保存到管理员电脑上。
5 单击 **返回** 即可回到状态页面。

恢复系统设置

可以通过上载一个以前下载过的系统设置文件的方式来恢复系统设置：

1 进入 **系统 > 状态**。

2 选择 **系统设置恢复** 。

3 输入系统设置文件的名称和路径，或者单击 **浏览** 然后在浏览器中定位文件。

4 单击 **确定** 将系统设置文件恢复到 FortiGate 上。
FortiGate 将上载系统设置文件并重新启动，调入新的系统设置。

5 重新连接到基于 Web 的管理程序并查看您的系统设置，确认上载的系统设置已经生效了。

将系统设置恢复到出厂设置

按照以下步骤可以将系统设置恢复到出厂时的设置值。这一操作不会改变固件版本、病毒防护定义库或是攻击定义库。

警告： 这一操作将删除您在 FortiGate 配置中所做的任何改动，并将系统恢复到原始状态，包括复位网络接口的地址。

1 进入 **系统 > 状态**。

2 选择 **恢复出厂设置** 。

3 单击 **确定** 以确认操作。
FortiGate 将使用第一次加电时的配置重新启动。

4 重新连接到基于 Web 的管理程序并查看系统配置，确认它已经恢复到了默认设置。

要恢复您的系统设置，请参阅 第 84 页 “ 恢复系统设置” 。

转换到透明模式

使用如下操作可以将 FortiGate 设备从 NAT/ 路由模式转换到透明模式。当 FortiGate 设备改到透明模式之后，它的配置将被设置为透明模式的默认配置。

1 进入 **系统 > 状态**。

2 选择 **转换到透明模式**。

3 选择 **操作模式列表** 中的 **透明模式** 选项。

4 单击 **确定** 。
FortiGate 现在已经转换到了透明模式。

5 用以下方法重新连接到基于 Web 的管理程序：将浏览器连接到为透明模式管理访问设置的网络接口上，在地址栏输入 https:// 后边是透明模式管理所用的接口的 IP 地址。在透明模式的默认情况下，您可以连接到内部接口或者 DMZ 接口。默认的透明模式管理所用的 IP 地址是 10.10.10.1。

转换到 NAT/ 路由模式

使用如下操作可以将 FortiGate 设备从透明模式转换到 NAT/ 路由模式。当 FortiGate 设备改到 NAT/ 路由模式式之后，它的配置将被设置为 NAT/ 路由模式的默认配置。

1 进入 **系统 > 状态**。

2 选择 **转换到 NAT/ 路由模式** 。

3 在 **操作模式列表** 中选择 **NAT/ 路由** 选项。

4 单击 **确定** 。

FortiGate 现在已经转换到了 NAT/ 路由模式。

5 用以下方法重新连接到基于 Web 的管理程序：将浏览器连接到为管理访问配置的网络接口，使用 https:// 后边跟上该接口的 IP 地址。

在 NAT/ 路由模式的默认情况下，您可以连接到内部接口或者 DMZ 接口。默认的 NAT/ 路由模式管理所用的 IP 地址是 192.168.1.99。

请见 第 18 页 “ 连接到基于 Web 的管理程序” 或 第 19 页 “ 连接到命令行接口 (CLI)” 。

重新启动 FortiGate 设备

1 进入 **系统 > 状态**。

2 单击 **重新启动** 。

FortiGate 将重新启动。

关闭 FortiGate 设备

1 进入 **系统 > 状态**。

2 单击 **关机** 。

FortiGate 将会关闭，所有的连接都被断开。

FortiGate 关闭后，只有切断电源然后再次接通，才能重新启动。

系统状态

您可以使用系统状态监视器显示 FortiGate 系统当前的健康状态信息。系统的健康状态信息包括 CPU 和内存使用率、活动的通讯会话数、当前使用的网络带宽统计等。基于 Web 的管理程序同时显示当前的统计信息和过去数分钟内的统计信息。

如果 FortiGate 设备配备了硬盘，系统状态监视器可以显示硬盘的容量、硬盘当前已使用的和空闲的空间统计。

您还可以查看当前的病毒和攻击状态。基于 Web 的管理程序显示当前的病毒和攻击数量，以及用图形方式显示过去 20 小时内的病毒和攻击等级。

您可以设置一个自动更新时间间隔每过一段时间就更新当前的显示。这个时间间隔可以从 5 秒到 30 秒。您还可以手工刷新显示的内容。

- 查看 CPU 和内存状态
- 查看会话和网络状态
- 查看病毒和入侵状态

查看 CPU 和内存状态

当前 CPU 和内存状态指示了 FortiGate 设备接近于满负荷运行的程度。 基于 Web 的管理程序只显示核心进程对 CPU 和内存的使用率。 被管理进程所使用的 CPU 和内存（例如，用于到基于 Web 的管理程序的 HTTPS 的连接）没有被统计进去。

如果 CPU 和内存使用率很低，这个 FortiGate 设备还有能力处理比它现在所运行的更多的网络通讯。如果 CPU 和内存使用率很高，FortiGate 设备已经接近于满负荷工作。此时再增加更多的任务可能会导致系统对通讯的处理出现延迟。

对 CPU 和内存要求较多的进程，例如 IPSec VPN 通讯的加密和解密、病毒扫描以及包含了小数据包的网络通讯的高级处理将增加 CPU 和内存的使用率。

1 进入 **系统 > 状态 > 监视器。**

将显示 CPU 和内存的状态。显示的内容包括图形显示的当前 CPU 和内存的使用率、过去数分钟内的 CPU 和内存的使用率曲线。

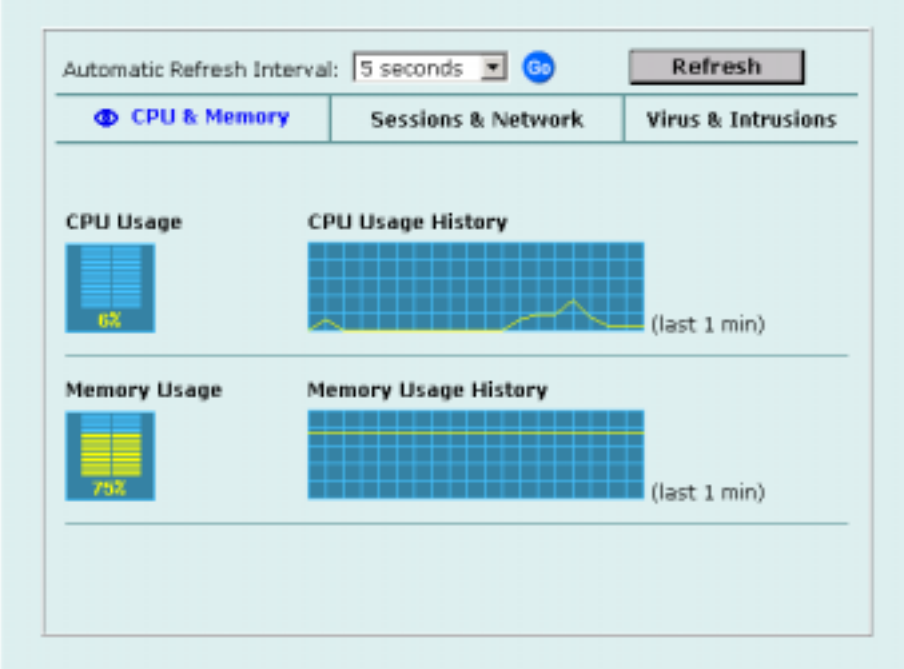
如果您的 FortiGate 设备配备了硬盘，将显示 CPU、内存和硬盘状态。

2 设置自动刷新的时间间隔并单击执行以设置基于 Web 的管理程序更新当前显示的频率。

频繁地刷新将消耗系统资源并增加网络通讯。然而，这只发生在您使用 基于 Web 的管理程序查看显示的时候。

3 单击刷新可以手工更新当前显示的信息。

图 1: CPU 和内存状态监视器



查看会话和网络状态

使用会话和网络状态显示可以跟踪 FortiGate 设备正在处理的网络会话并查看可用网络带宽上的会话数量。另外通过对比 CPU、内存使用率和网络、会话状态，您可以知道系统资源可以承担多少网络通讯。

会话显示了当前 FortiGate 设备的全部接口所处理的会话总数。会话还显示了 FortiGate 设备当前处理的会话数占它设计的处理能力的百分比。

网络使用显示了通过 FortiGate 全部网络接口的网络带宽的总量。网络使用还显示了当前所使用的网络带宽占 FortiGate 设备能处理的最大网络带宽的百分比。

1 进入 **系统 > 状态 > 监视器。**

2 单击会话和网络。

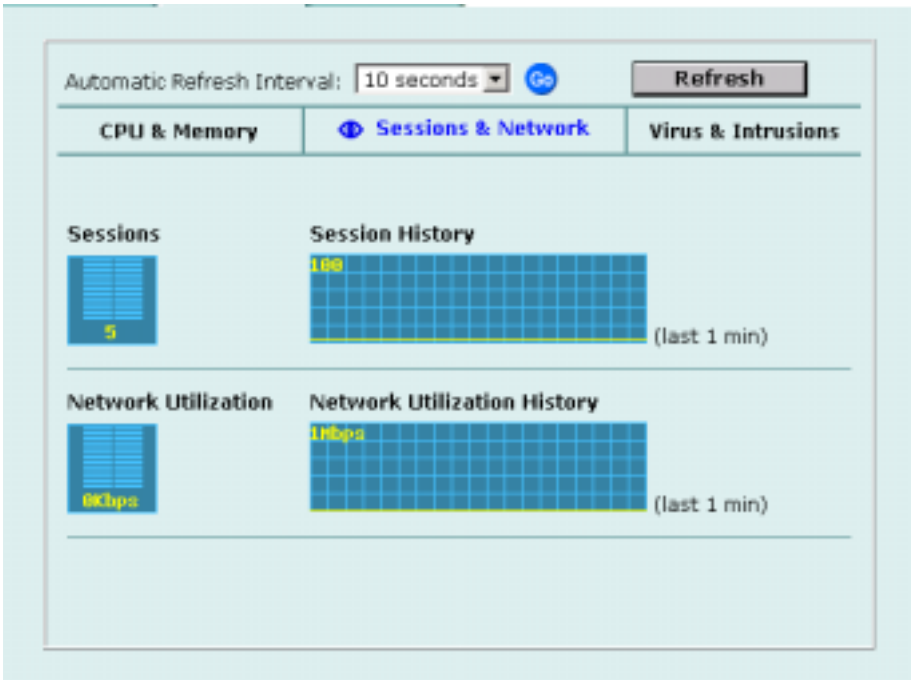
显示会话和网络状态。显示的内容包括图形化显示的当前会话数和当前网络使用量，以及过去数分钟内的会话数曲线和网络使用量曲线。曲线图的比例显示在图的左上角。

3 设置自动刷新的时间间隔并单击执行以设置基于 Web 的管理程序更新当前显示的频率。

频繁地刷新将消耗系统资源并增加网络通讯。然而，这只发生在您使用 基于 Web 的管理程序查看显示的时候。

4 单击刷新可以手工更新当前显示的信息。

图 2: 会话和网络监视器



查看病毒和入侵状态

使用病毒和入侵状态显示可以跟踪 FortiGate 病毒防护系统发现的病毒和 NIDS 检测到的网络攻击。

1 进入 **系统 > 状态 > 监视器。**

2 单击病毒和入侵。

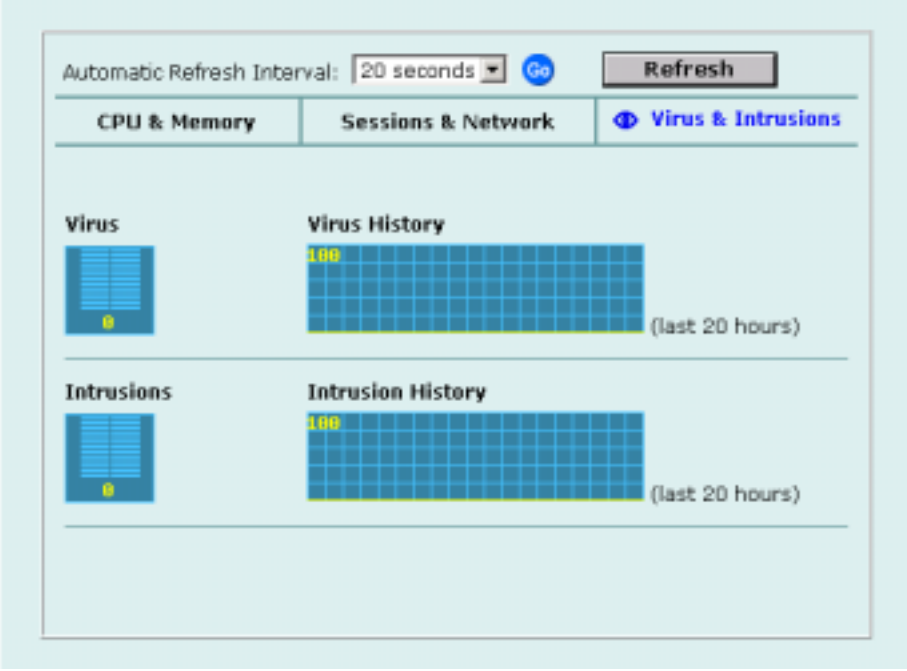
显示病毒和入侵状态。显示的内容包括以条形图方式显示的每小时检测到的病毒和入侵数量，以及过去 20 小时内的病毒和入侵数量统计曲线。

3 设置自动刷新的时间间隔并单击执行以设置基于 Web 的管理程序更新当前显示的频率。

频繁地刷新将消耗系统资源并增加网络通讯。然而，这只发生在您使用 基于 Web 的管理程序查看显示的时候。

4 单击刷新可以手工更新当前显示的信息。

图 3: 病毒和入侵状态监视器



会话列表

会话列表显示了关于 FortiGate 设备当前处理的通讯会话的信息。您可以使用会话列表查看当前会话。FortiGate 有读写权限的管理员以及 FortiGate 的 admin 管理员可以终止活动的通讯会话。

查看会话列表

1 进入**系统 > 状态 > 会话。**

基于 Web 的管理程序在 FortiGate 设备会话列表中显示了会话的总数并列出前 16 个会话。

2 要在列表中翻页浏览会话，单击上一页 或下一页 。

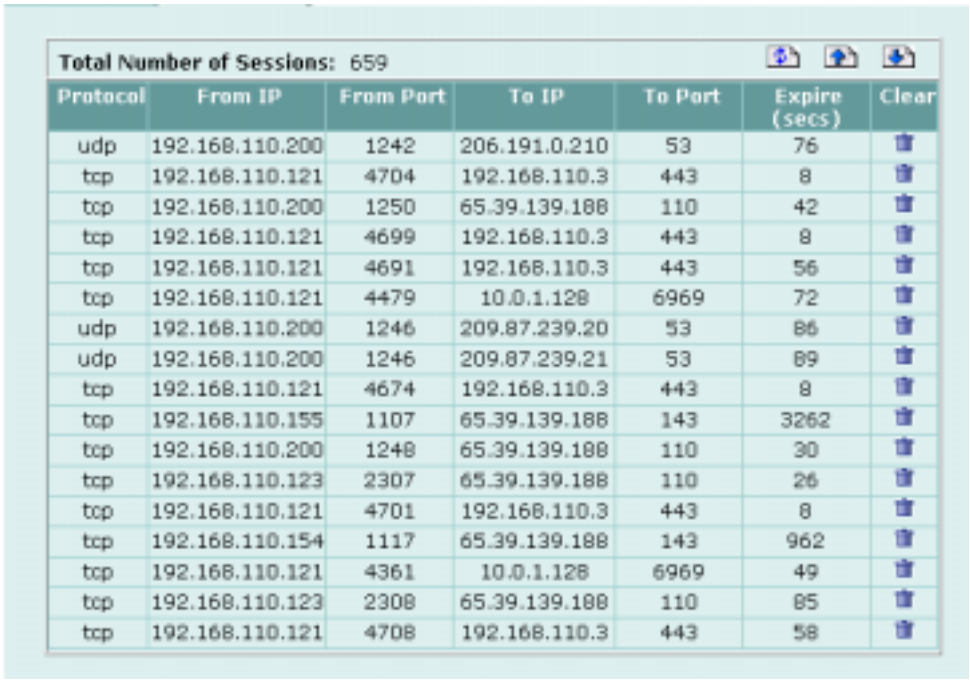
3 单击更新 可以更新会话列表。

4 如果您使用具有读写权限的管理员用户或者 admin 用户登录，您可以单击清除 以停止任何活动的会话。

会话列表中的每一行显示了以下信息：

协议 连接的服务类型或者协议类型。例如 TCP、UDP、ICMP
源 IP 连接的源 IP 地址。
源端口 连接的源端口。
目的 IP 连接的目的 IP 地址。
目的端口 连接的目的端口。
到期时间 在连接到期前剩余的时间，以秒为单位。
清除 中断一个处于活动状态的通讯会话。

图 4: 会话列表举例



Total Number of Sessions: 659

Protocol	From IP	From Port	To IP	To Port	Expire (secs)	Clear
udp	192.168.110.200	1242	206.191.0.210	53	76	
tcp	192.168.110.121	4704	192.168.110.3	443	8	
tcp	192.168.110.200	1250	65.39.139.188	110	42	
tcp	192.168.110.121	4699	192.168.110.3	443	8	
tcp	192.168.110.121	4691	192.168.110.3	443	56	
tcp	192.168.110.121	4479	10.0.1.128	6969	72	
udp	192.168.110.200	1246	209.87.239.20	53	86	
udp	192.168.110.200	1246	209.87.239.21	53	89	
tcp	192.168.110.121	4674	192.168.110.3	443	8	
tcp	192.168.110.155	1107	65.39.139.188	143	3262	
tcp	192.168.110.200	1248	65.39.139.188	110	30	
tcp	192.168.110.123	2307	65.39.139.188	110	26	
tcp	192.168.110.121	4701	192.168.110.3	443	8	
tcp	192.168.110.154	1117	65.39.139.188	143	962	
tcp	192.168.110.121	4361	10.0.1.128	6969	49	
tcp	192.168.110.123	2308	65.39.139.188	110	85	
tcp	192.168.110.121	4708	192.168.110.3	443	58	

病毒和攻击定义升级及注册

您可以将 FortiGate 设备配置为连接到 Forti 响应发布网络 (FDN) 并自动更新病毒防护定义和攻击定义，以及病毒防护引擎。您可以使用以下更新选项：

- 从 FDN 手工请求更新，
- 每小时、每天或每周定期启动请求最新版本的更新，
- 使用推送更新使得 FDN 可以在发布新的更新时连接到您的 FortiGate 设备。

您必须先在 Fortinet 支持网页注册您的 FortiGate 设备，才能将 FortiGate 设备配置为接受自动更新和推送更新。

本章描述了以下内容：

病毒防护定义和攻击定义更新

您可以将 FortiGate 设备配置为连接到 Forti 响应发布网络 (FDN) 并自动更新病毒防护定义和攻击定义，以及病毒防护引擎。FortiGte 设备支持以下病毒防护和攻击定义更新功能：

- 用户定义的从 FDN 手工更新，
- 每小时、每天或每周定期从 FDN 更新病毒防护定义、攻击定义和病毒防护引擎，
- 来自 FDN 的推送更新，
- 查看更新状态，包括版本号、有效期、更新日期和时间，
- 通过 NAT 设备的推送更新。

基于 Web 的管理程序的系统 > 更新页面显示了以下病毒防护定义和攻击定义更新信息。

版本	显示当前的防病毒引擎、病毒定义和攻击定义的版本号。
有效期	显示您的病毒防护引擎、病毒定义和攻击定义更新许可证的有效期。
最后更新企图	显示 FortiGate 设备最后一次试图下载病毒防护引擎、病毒定义和攻击定义更新的日期和时间。
最后更新状态	显示最后一次试图更新是成功还是失败。没有更新意味着最后一次企图更新成功，但是没有可用的更新内容。更新成功或者类似的信息意味着最后一次更新企图成功，并且新的更新内容已经被安装。其他信息指示了 FortiGate 设备无法连接到 FDN 或者其他情况的错误。

本节描述了以下内容：

连接到 Forti 响应发布网络

FortiGate 设备必须能够连接到 Forti 响应发布网络 （FDN）才能接受病毒防护和攻击定义更新。FortiGate 设备使用 HTTPS 协议和 8890 端口连接 FDN。ForitGate 外部接口必须能够使用 8890 端口连接到更新中心。要配置定期更新，请见 第 93 页 “配置周期性更新”

也可以将 FortiGate 配置为允许推送更新。推送更新由 FDN 使用 UDP 端口 9443 和 HTTPS 协议提供给 FortiGate 设备。要接收推送更新，FDN 必须有一条使用 UDP 端口 9443 连接到 ForitGate 外部接口的路径。要配置推送更新，请见 第 95 页 “配置推送更新”

FDN 是 Forti 响应分布服务器 （FDS）组成的一个世界范围的网络。当您的 FortiGate 设备连接到 FDN 时，它实际上连接的是最近的 FDS。这是因为所有的 FortiGate 设备内部都保存了一个 FDS 地址列表。这个地址列表根据 FortiGate 设备的时区设置，按照距离这个时区的远近排序。要确保 FortiGate 设备从最近的 FDS 接收更新，进入系统 > 配置 > 时间并确认您根据您所在的区域正确选择了时区设置。

以下方法可以确认 FortiGate 设备能否连接到 FDN：

1 进入 **系统 > 配置 > 时间** 并确保时区已经根据您所在的区域正确地设置了。

2 进入 **系统 > 更新**。

3 单击更新。

FortiGate 设备将测试它到 FDN 的连接。测试结果显示在系统更新页的顶部：

表 1：连接到 FDN

连接	状态	说明
Forti 响应发布网络	可用	FortiGate 设备可以连接到 FDN。您可以将 FortiGate 设备配置为定期更新。请见 第 93 页 “配置周期性更新” 。
	不可用	FortiGate 设备无法连接到 FDN。您 需要配置您的 FortiGate 设备和您的网络使使得 FortiGate 设备可以连接到互联网和 FDN。例如，您可能需要在 FortiGate 设备的路由表中添加路由或配置您的网络以允许 FortiGate 设备使用 HTTPS 协议通过端口 8443 连接到互联网。 您可能还需要连接到一个 Forti 响应服务器代理以接受推送更新。请见 第 94 页 “添加后备服务器” 。

表 1：连接到 FDN

连接	状态	说明
推送更新	可用	FDN 可以连接到 FortiGate 设备以发送推送更新。您可以将 FortiGate 设备配置为接收推送更新。请见 第 95 页 “ 配置推送更新” 。
	不可用	FDN 不能连接到 FortiGate 设备发送推送更新。如果您没有注册您的 FortiGate 设备（请见 第 101 页 “ 注册 FortiGate 设备” ），推送更新可能无法使用。如果在 FortiGate 设备和 FDN 之间有一个 NAT 设备（请见 第 96 页 “ 通过 NAT 设备的推送更新” ），或者您的 FortiGate 设备使用代理服务器（请见 第 100 页 “ 通过代理服务器定期更新” ）连接到互联网，推送更新也可能无法使用。

配置周期性更新

您可以将 FortiGate 设备配置为根据您指定的时间表，每小时、每天、每周检查并下载病毒防护定义和攻击定义的更新。

1 进入 **系统 > 更新。**

2 单击周期性更新。

3 选择检查和下载更新的时间表：

每小时 每 1 小时到每 23 小时检查一次。选择两次更新请求之间的时间间隔，可以精确到小时和分钟。

每天 每天检查一次。您可以指定一天当中检查更新的具体时间。

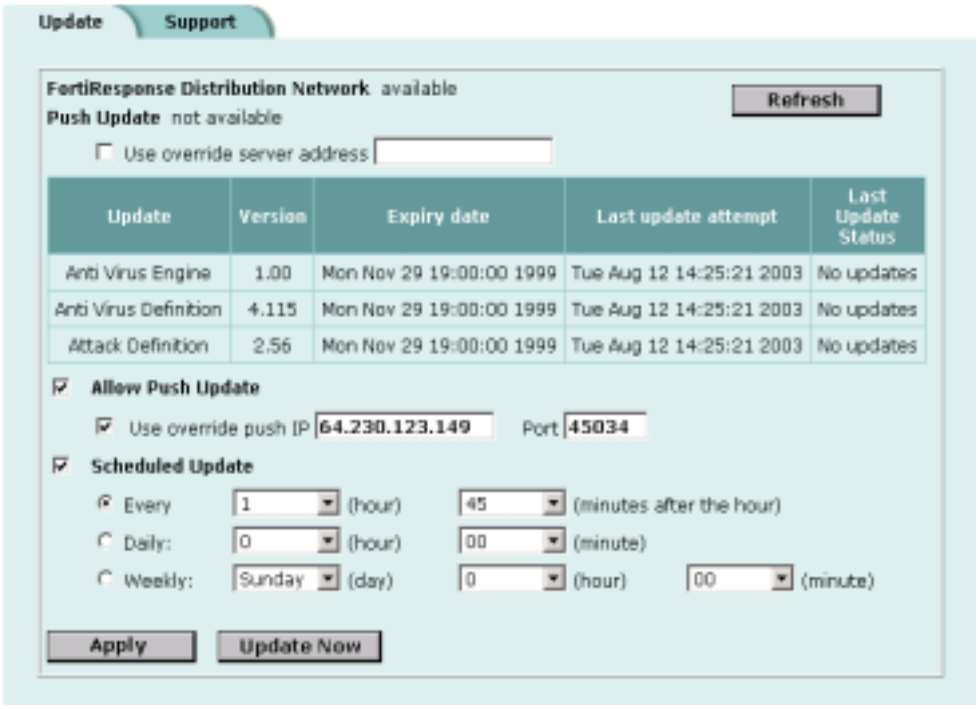
每周 每周检查一次。您可以指定一周当中进行更新检查的日子和在那一天当中进行检查的具体时间。

4 单击应用。

FortiGate 设备将根据新的更新时间表启动下一次定期更新。

无论何时当一个周期性更新开始运行时，它都会在 FortiGate 事件日志中写入一条记录。

图 1: 配置病毒防护和攻击定义自动更新



配置更新日志

使用如下步骤配置 FortiGate 日记记录可以在 FortiGate 设备更新病毒防护和攻击定义的时候记录日志消息。更新日志消息记录在 FortiGate 事件日志中。

1 进入 **日志和报告 > 日志设置**。

2 在 FortiGate 设备要记录的日志类型上单击配置策略。

请见 第 245 页 “ 记录日志” 。

3 单击更新，FortiGate 设备将在更新病毒防护和攻击定义时记录日志消息。

4 选择以下更新日志选项：

更新失败	FortiGate 设备在试图更新失败的时候记录一条日志消息。
更新成功	FortiGate 设备在成功地更新之后记录一条日志消息。
FDN 错误	FortiGate 设备在无法连接到 FDN 或者它从 FDN 接收到一条错误信息时记录一条日志消息。

5 单击确定。

添加后备服务器

如果您不能连接到 FDN 或者您所在的机构使用他们自己的 Forti 响应服务器提供病毒防护和攻击定义的更新，您可以按照如下步骤添加一个 Forti 响应后备服务器。

1 进入 **系统 > 更新。**

2 单击使用后备服务器地址并添加一个 Forti 响应服务器的 IP 地址。

3 单击应用。

FortiGate 设备将测试到这个后备服务器的连接。

如果 Forti 响应发布网络的修改是正确的，FortiGate 设备应当可以连接到后备服务器。

如果 Forti 响应发布网络的设置仍旧不可用，FortiGate 设备就无法连接到后备服务器。检查 FortiGate 的配置和网络配置，确保您可以从 FortiGate 设备连接到后备服务器。

手工更新病毒防护定义和攻击定义

您可以在任何时候按照如下步骤更新病毒定义和攻击定义。要进行如下操作，您的 FortiGate 设备必须可以连接到 FDN 或者一个 Forti 响应代理服务器。

1 进入 **系统 > 更新。**

2 单击现在更新以更新病毒防护和攻击定义。

如果到 FDN 或者后备服务器的连接成功，基于 Web 的管理程序将显示类似下面的消息：

您的更新请求已经发出。您的数据库将在几分钟内被更新。请检查您的更新页面以获取当前的更新工作的状态。

数分钟后，如果有更新可用，系统更新页面将显示出病毒防护定义、病毒防护引擎、或攻击定义的新版本的信息。系统状态页还将显示病毒防护定义和攻击定义的新的日期和版本信息。无论更新工作成功与否，都将在事件日志中记录一条消息。

配置推送更新

FDN 可以将更新主动发送到 FortiGate 设备上，以最快的速度对紧急的事态作出响应。您必须先注册您的 FortiGate 设备才能接收推送更新。请见 第 101 页 “注册 FortiGate 设备”。

如果 FDN 必须通过一个 NAT 设备才能连接到 FortiGate 设备上，请见 “通过 NAT 设备的推送更新”。

如果 FortiGate 设备必须使用一个代理服务器才能连接到 FDN，则无法支持推送更新。有关的详细信息请见 第 100 页 “通过代理服务器定期更新”。

按照如下步骤启用推送更新

1 进入 **系统 > 更新。**

2 单击允许推送更新。

3 单击应用。

关于推送更新

当您将 FortiGate 设备配置为允许推送更新时，FortiGate 设备将向 FDN 发送一个 SETUP 消息。下一次当发布新的病毒防护引擎、新病毒定义或者新攻击定义的时候，FDN 将通报所有配置为推送更新的 FortiGate 设备，有一个新的更新可用。在收到一个推送更新之后的 60 秒之内，FortiGate 设备将试图从 FDN 请求更新。

如果您的网络配置允许，除了配置定义更新之外，建议您配置推送更新。推送更新意味着平均起来 FortiGate 设备收到新的更新的速度比只定期更新的 FortiGate 设备要快。然而，定义更新可以确保 FortiGate 设备最后能够收到最新的更新。

不建议将启用推送更新作为唯一的获取更新的方式。FortiGate 设备可能无法收到推送更新。同样，当 FortiGate 设备接收到一个更新通报的的时候，它只尝试一次连接到 FDN 和下载更新。

推送更新和外部动态 IP 地址

如果 FortiGate 设备的外部接口是使用动态 IP 地址配置的 （使用 PPPoE 或者 DHCP），当外部接口的 IP 地址发生变化时，FortiGate 设备将向 FDN 发送一条 SETUP 消息通报这个变化。这个 SETUP 消息发送之后，FDN 将记录这个新的 IP 地址，下次的推送更新将发送到这个 IP 地址。

通过 NAT 设备的推送更新

如果 FDN 必须通过一个 NAT 设备才能连接到 FortiGate 设备，您必须在 NAT 设备上配置端口转发并在推送更新配置中添加端口转发信息。使用端口转发，FDN 使用 9443 或者您指定的备份端口连接到 FortiGate 设备。

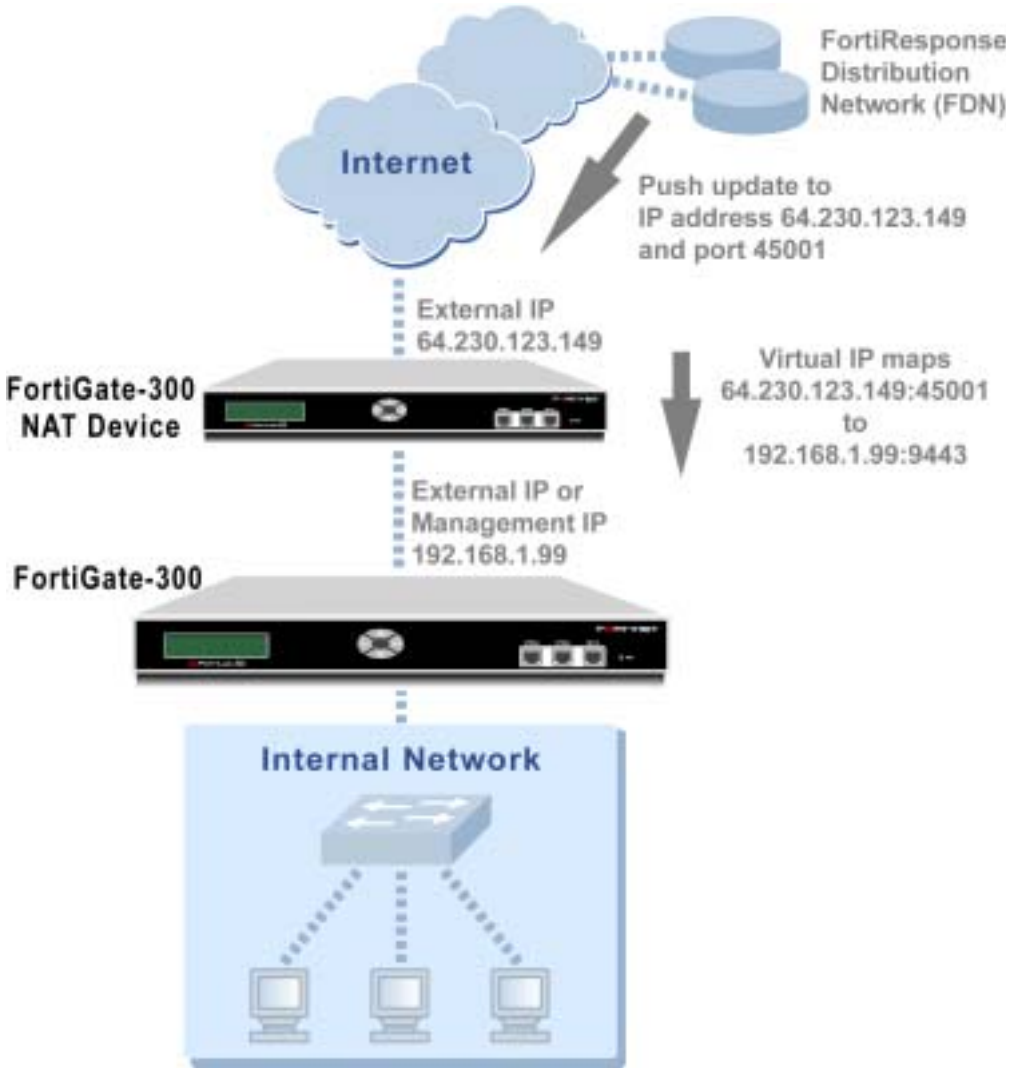
注意：如果 NAT 设备的外部接口 IP 地址的动态的 （例如，使用 PPPoE 或 DHCP 设置的接口），您将无法通过 NAT 设备接收推送更新。

例子：通过一个 NAT 设备的推送更新

这个例子描述了如何配置一个 FortiGate NAT 设备以向安装在它的内部网络中的一个 FortiGate 设备转发推送更新。为了让内部网络中的 FortiGate 设备能够接收推送更新，这个 FortiGate NAT 设备必须配置一个端口转发虚拟 IP。这个虚拟 IP 将这个 FortiGate NAT 设备的外部接口的 IP 地址和一个指定的端口影射到内部网络中的那个 FortiGate 设备的 IP 地址上去。如果这个 FortiGate 设备运行于 NAT/ 路由模式，这个 IP 地址可以是它的外部接口 IP 地址，如果这个 FortiGate 设备运行于透明模式，那么这个 IP 地址可以是它的管理 IP 地址。

注意：本例描述了一个关于 FortiGate NAT 设备配置的例子。然而，您也可以使用任何具有配置了端口转发的静态外部 IP 地址的 NAT 设备。

图 2: 网络拓扑结构举例：通过一个 NAT 设备的推送更新



一般配置步骤

使用以下步骤配置 FortiGate NAT 设备和内部网络中的 FortiGate 设备，使得内部网络中的 FortiGate 设备可以接收推送更新：

1 向 FortiGate NAT 设备添加一个端口转发虚拟 IP。

2 向包含了端口转发虚拟 IP 的 FortiGate NAT 设备添加一个防火墙策略。

3 为内部网络中的 FortiGate 设备配置一个代理推送 IP 地址和端口。

注意：在完成如下操作之前，您需要注册您的内部网络中的 FortiGate 设备，这样它才能接收推送更新。

在 FortiGate NAT 设备上添加端口转发虚拟 IP

使用以下步骤配置 FortiGate NAT 设备，使用端口转发将来自 FDN 的推送更新连接转发到内部网络的一个 FortiGate 设备上。

按照如下步骤配置 FortiGate NAT 设备：

1 进入 **防火墙 > 虚拟 IP**。

2 单击新建。

3 为虚拟 IP 地址添加一个名称。

4 选择 FDN 连接到的外部接口。
对于例子中的拓扑结构，选择外部接口。

5 选择端口转发。

6 输入 FDN 连接到的外部 IP 地址。
对于例子中的拓扑结构，输入 64.230.123.149。

7 输入 FDN 连接到的外部服务端口。
对于例子中的拓扑结构，输入 45001。

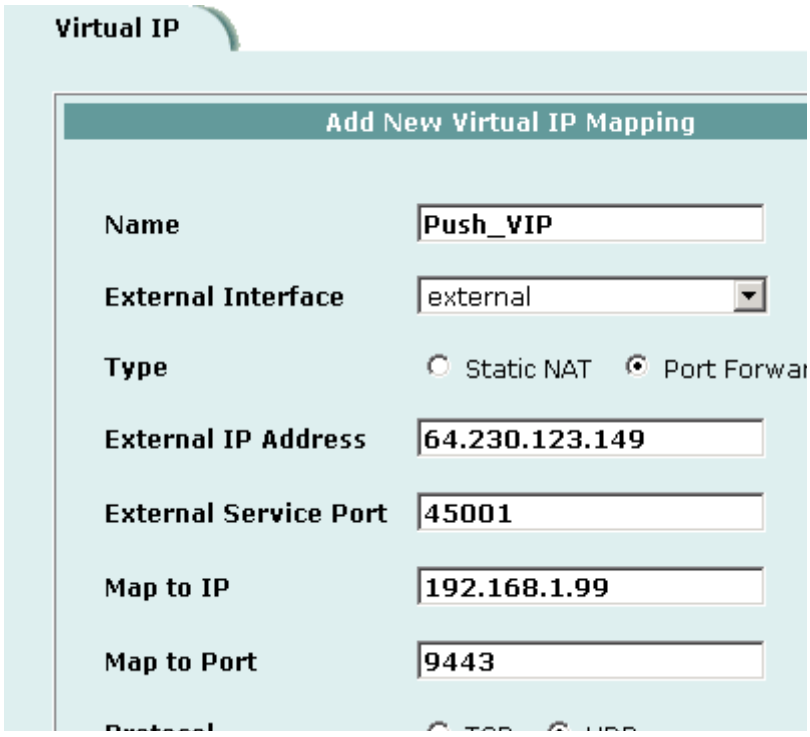
8 将映射到的 IP 地址设置为内部网络中的 FortiGate 设备的 IP 地址。
如果这个 FortiGate 设备运行于 NAT/ 路由模式，输入外部接口的 IP 地址。
如果这个 FortiGate 设备运行于透明模式，输入管理 IP 地址。
对于例子中的拓扑结构，输入 192.168.1.99。

9 将影射到的端口设置为 9443。

10 将协议设置为 UDP。

11 单击确定。

图 3: 推送更新端口转发虚拟 IP



为端口转发虚拟 IP 添加一个防火墙策略

按照如下步骤配置 FortiGate NAT 设备：

1 添加一个新的外部到内部的防火墙策略。

2 使用如下设置配置策略：

源地址	外部 _ 全部
目的地址	前面步骤中添加的虚拟 IP 地址。
任务计划	总是。
服务	任意。
动作	接受。
NAT	选中。

3 单击确定。

使用一个代理 IP 地址和端口配置 FortiGate 设备

按照如下步骤配置内部网络中的 FortiGate 设备 ：

1 进入 **系统 > 更新**。

2 选择允许推送更新。

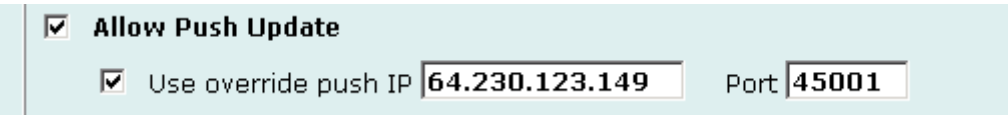
3 选择使用代理推送更新。

4 将 IP 地址设置为添加到虚拟 IP 的外部 IP 地址。
对于例子中的拓扑结构，输入 64.230.123.149。

5 将端口号设置为添加到虚拟 IP 的外部服务端口。
对于这个例子中的拓扑结构，输入 45001。

6 单击应用。
FortiGate 设备将代理推送更新 IP 地址和端口发送给 FDN。现在 FDN 使用这个 IP 地址和端口向内部网络中的 FortiGate 设备发送推送更新。
如果外部 IP 地址或者外部服务端口有所改变，将所做的改变添加到使用代理推送更新的配置中并单击应用，即可更新 FDN 的推送更新信息。

图 4: 推送更新配置举例



7 单击应用。

8 您可以单击刷新以确定推送更新是否正常工作。
推送更新的状态应当变为可用。

通过代理服务器定期更新

如果您的 FortiGate 设备必须通过一个代理服务器才能连接到互联网，您可以使用 **set system autoupdate tunneling** 命令使得FortiGate设备 可以使用这个代理服务器连接到 （或者通过通道）FDN。您可以使用这个命令来指定代理服务器的 IP 地址和端口号。如果代理服务器要求认证的话，您最好为自动更新配置添加代理服务器所须的用户名和密码。启用通过代理服务器的更新的完整的语法是：

```
set system autouopdate tunneling enable [address <代理服务器 _IP> [port <代理服务器端口> [username <用户名_字符串> [password <密码_字符串 >]]]]
```

例如，如果代理服务器的 IP 地址是 64.23.6.89，端口是 8080，您需要输入如下命令：

```
set system autouopdate tunneling enable address 64.23.6.89 port 8080
```

关于 **set system autoupdate** 命令的详细信息，请见第六卷，*FortiGate CLI 参考指南*。

FortiGate 设备使用 HTTP CONNECT 方法连接到代理服务器，这一方法在 RFC2616 中有详细描述。FortiGate 设备将一个 HTTP CONNECT 连接请求发送到代理服务器 （可选是否附加认证信息），指定请求连接到 FDN 的 IP 地址和端口。代理服务器建立到 FDN 的连接并在 FortiGate 设备和 FDN 之间传输信息。

CONNECT 方法通常被用于 SSL 通讯通道。有些代理服务器不允许 CONNECT 连接到任意端口；他们将允许连接的端口范围限制在使用 HTTPS 连接众所周知的端口和类似的服务。因为 FortiGate 自动更新使用 HTTPS 协议和 8890 端口来连接 FDN，所以您所使用的代理服务器必须被配置为允许连接到这一端口。

如果您已经配置了一个连接到 FDN 的代理服务地址，就无须指定通道。

如果 FortiGate 设备必须通过一个代理服务器连接到互联网，则无法支持推送更新。

注册 FortiGate 设备

您购买和安装了一个新的 FortiGate 设备之后，可以使用基于 Web 的管理程序进入系统 > 更新 > 支持注册您的设备，或者使用一个网页浏览器连接到 http://support.fortinet.com 并选择产品注册。

注册内容包括输入您的联系方式和您或者您所在的机构购买的 FortiGate 设备的产品序列号。注册过程方便快捷。您可以一次注册多个 FortiGate 设备，无须重复输入您的联系方式。

完成注册之后，Fortinet 会将技术支持用户名和密码发送到您的电子邮箱。您可以使用这个用户名和密码登录到 Fortinet 技术支持网站以获得如下服务：

- 查看您注册的 FortiGate 设备列表
- 注册更多的 FortiGate 设备
- 添加或修改每个 FortiGate 设备的支持合同号
- 查看和修改注册信息
- 下载病毒和攻击定义更新

很快您将可以获得如下服务：

- 访问 Fortinet 用户文档
- 访问 Fortinet 知识库
- 下载固件升级

所有注册信息存储在 Fortinet 客户支持数据库中。这些信息用来确保您所注册的 FortiGate 设备能够被更新。所有信息都是严格保密的。Fortinet 不会以任何理由同第三方分享这些信息。

本节描述了如下内容：

FortiCare 服务合同

新的 FortiGate 设备的所有者有资格享受 90 天的技术支持服务。当 90 天的技术支持服务到期后，如果您要继续享受技术支持服务，，您必须从 Fortinet 授权的分销商处购买 FortiCare 支持合同。您可以根据您所需要的支持购买不同级别的服务。为了最大限度地保护您的网络，Fortinet 强烈建议所有的客户购买包含病毒防护和攻击定义更新再内的服务合同。请联系您的 Fortinet 分销商以获得关于包装和价格的详细信息。

您必须注册您的 FortiGate 设备并在注册信息中添加 FortiCare 支持合同号以激活您的 FortiCare 支持合同。您也可以不购买 FortiCare 支持合同，仅仅注册 FortiGate 设备。在这种情况下，当您购买一个 FortiGate 支持合同的时候，您可以更新您的注册信息，添加这个支持合同号。

一个 FortiGate 支持合同可以覆盖多个 FortiGate 设备。您必须为这个服务合同涵盖的每一个 FortiGate 设备输入相同的合同号。

注册 FortiGate 设备

在您注册 FortiGate 设备之前，您需要以下信息：

- 您的联系方式，包括：
  - 姓名（全名）
  - 公司名
  - 电子邮件地址（您的 Fortinet 支持登录用户名和密码将被发送到这个地址。）
  - 地址
  - 联系电话
- 安全提示问题和答案

  这一信息用于密码恢复。安全提示问题应当是一个只有您知道答案的简单问题。答案不要简单的别人能够猜到。
- 您要注册的每个 FortiGate 设备的产品型号和序列号。

  序列号在每个 FortiGate 设备的底部的标签上。

  您可以使用 基于 Web 的管理程序进入系统 > 状态 查看序列号。

  也可以通过 CLI 使用命令 `get system status` 查看序列号。
- FortiCare 支持合同号，如果您为您要注册的 FortiGate 设备购买了 FortiCare 支持合同。

按以下步骤注册一个或多个 FortiGate 设备

1 进入 **系统 > 更新 > 支持。**

2 在产品注册单中输入您的联系信息。

图 5: 注册 FortiGate 设备 （联系信息和安全提示问题）

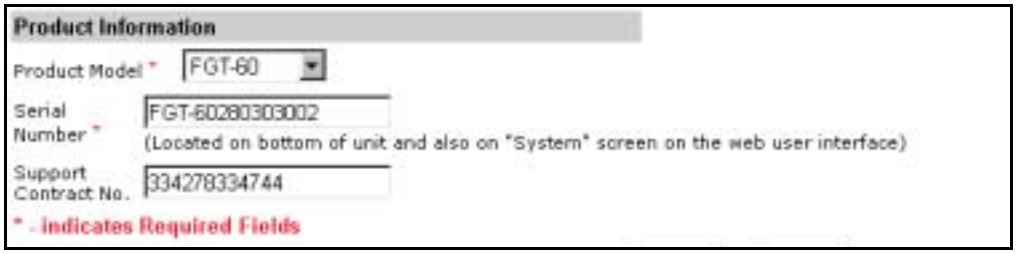
3 提供一个安全提示问题和这个问题的答案。

4 选择要注册的产品的型号。

5 输入 FortiGate 设备的序列号。

6 如果您为这个 FortiGate 设备购买了 FortiCare 支持合同，请输入支持合同号。

图 6: 注册 FortiGate 设备 （产品信息）



7 单击完成。

如果您还没有输入 FortiCare 支持合同号 （SCN），您可以回到上一个页面并输入这个号码。如果您没有购买 FortiCare 支持合同您可以选择继续以完成注册过程。

如果您输入了一个支持合同号，将出现一个实时确认提示以验证 SCN 信息是否与 FortiGate 设备匹配。如果信息不匹配您可以尝试再次输入信息。

包含了可用于您注册的 FortiGate 设备的 Fortinet 技术支持服务的详细信息将显示在一个网页中。

您的 Fortinet 支持用户名和密码将被发送到您在联系信息中提供的电子邮件地址。

更新注册信息

您可以在任何时间使用您的 Fortinet 支持用户名和密码登录到 Fortinet 支持网站以查看和更新您的 Fortinet 支持信息。

本节描述了以下内容：

找回丢失的 Fortinet 支持密码

如果您在注册到 Fortinet 支持网站时提供了一个安全提示问题和答案，您可以按照如下步骤接收一个临时密码。如果您没有提供安全提示问题和答案，请联系 Fortinet 技术支持。

1 进入 **系统 > 更新 > 支持。**

2 选择支持登录。

3 输入您的 Fortinet 支持用户名。

4 单击 忘记了您的密码?

5 输入您的电子邮件地址并单击提交。

您在注册时输入的安全提示问题将会显示。

6 输入您的安全提示问题的答案并单击获取密码。

如果您输入的答案是正确的，一个含有新密码的电子邮件将被发送到您的电子邮件信箱中。您可以使用您的当前用户名和这个密码登录到 Fortinet 支持网站。

7 单击支持登录。

8 当您收到新的密码后，输入您的用户名和新密码以登录到 Fortinet 支持网站。

查看注册的 FortiGate 设备列表

1 进入 **系统 > 更新 > 支持** 并单击支持登录。

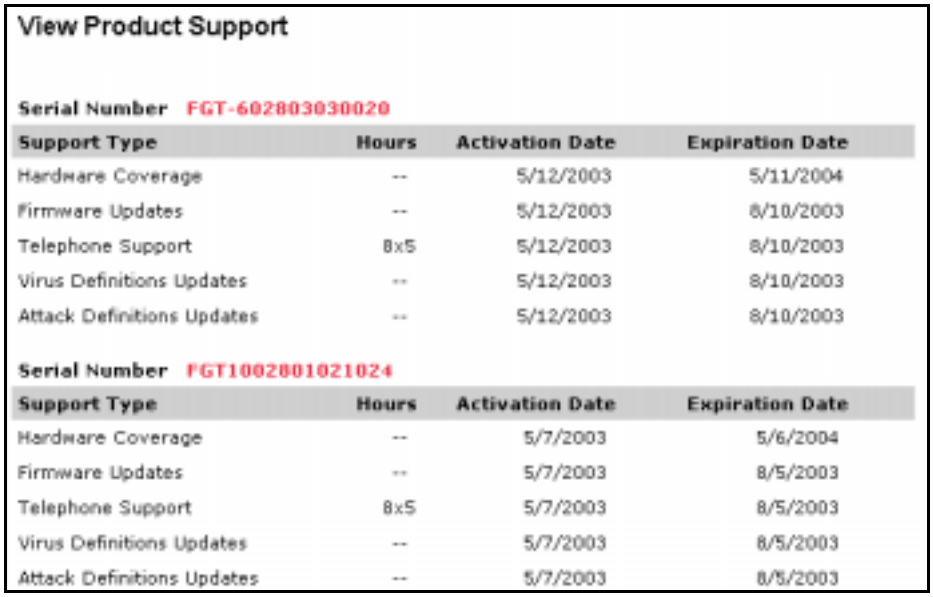
2 输入您的 Fortinet 支持用户名和密码。

3 单击登录。

4 单击查看产品。

将显示出您已注册过的 FortiGate 产品列表。对于每个 FortiGate 设备，列表包括了产品序列号和当前的支持选项。

图 7: 注册的 FortiGate 设备列表举例



View Product Support

Serial Number FGT-602803030020

Support Type	Hours	Activation Date	Expiration Date
Hardware Coverage	--	5/12/2003	5/11/2004
Firmware Updates	--	5/12/2003	8/10/2003
Telephone Support	8x5	5/12/2003	8/10/2003
Virus Definitions Updates	--	5/12/2003	8/10/2003
Attack Definitions Updates	--	5/12/2003	8/10/2003

Serial Number FGT1002801021024

Support Type	Hours	Activation Date	Expiration Date
Hardware Coverage	--	5/7/2003	5/6/2004
Firmware Updates	--	5/7/2003	8/5/2003
Telephone Support	8x5	5/7/2003	8/5/2003
Virus Definitions Updates	--	5/7/2003	8/5/2003
Attack Definitions Updates	--	5/7/2003	8/5/2003

注册一个新的 FortiGate 设备

1 进入 **系统 > 更新 > 支持**单击支持登录。
2 输入您的 Fortinet 支持用户名和密码。
3 单击登录。
4 单击添加注册。
5 选择您要注册的产品的型号。
6 输入您要注册的 FortiGate 设备的序列号。
7 如果您为这个 FortiGate 设备购买了 FortiCare 支持，请输入支持合同号。
8 单击完成。
将显示您已经注册了的 FortiGate 产品列表。这个列表现在包括您刚注册的 FortiGate 设备。

添加或修改 FortiCare 支持合同号

1 进入 **系统 > 更新 > 支持** 单击支持登录。
2 输入您的 Fortinet 支持用户名和密码。
3 单击登录。
4 单击添加 / 修改合同号。
5 选择您要添加或修改 FortiCare 合同号的 FortiGate 设备的序列号。
6 添加一个新的支持合同号。
7 单击完成。
将显示您已经注册的 FortiGate 产品列表。这个列表现在包括新的支持合同信息。

修改您的 Fortinet 支持密码

1 进入 **系统 > 更新 > 支持** 并单击支持登录。
2 输入您的 Fortinet 支持用户名和密码。
3 单击登录。
4 单击我的配置文件。
5 单击修改密码。
6 输入您当前的密码。
7 输入并确认一个新的密码。
一个确认您的密码已修改的电子邮件将被发送到您的电子邮件信箱中。下次您登录到 Fortinet 技术支持网站时需要使用您当前的用户名和新的密码。

修改您的联系信息或安全提示问题

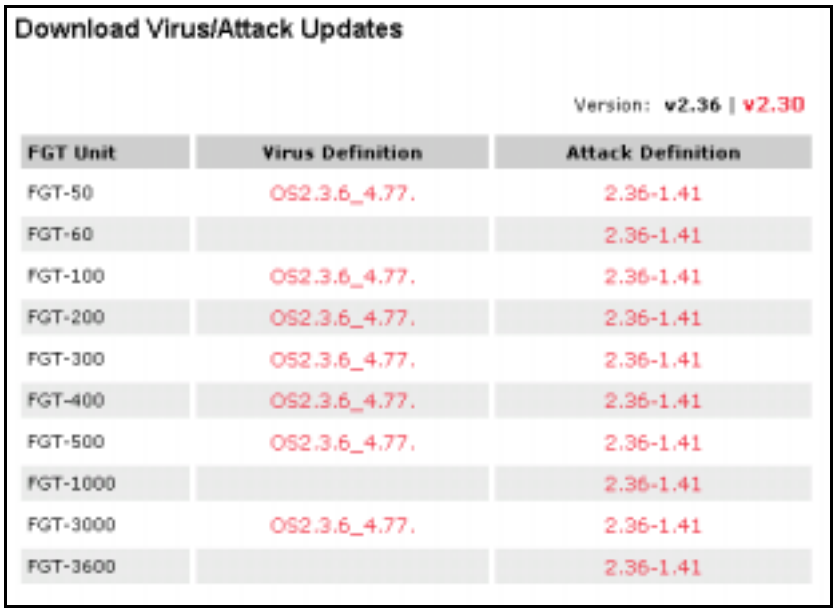
1 进入 **系统 > 更新 > 支持** 并单击支持登录。
2 输入您的 Fortinet 支持用户名和密码。
3 单击登录。
4 单击我的配置文件。
5 单击修改配置文件。
6 根据需要修改您的联系信息。
7 根据需要修改您的安全提示问题。
8 单击更新配置文件。
您所做的修改将被保存到 Fortinet 技术支持数据库中。如果您修改了您的联系信息，您所做的改动将被显示。

下载病毒防护和攻击定义更新

按照如下步骤手工下载病毒防护和攻击定义更新。下述步骤还包括了如何在您的 FortiGate 设备上安装定义的更新。

1 进入 **系统 > 更新 > 支持** 并单击支持登录。
2 输入您的 Fortinet 支持用户名和密码。
3 单击登录。
4 单击下载病毒 / 攻击更新。
5 如果需要，选择 FortiOS 的版本。
6 单击病毒和攻击定义以下载。

图 8: 下载病毒和攻击定义更新



关于如何安装下载的文件的详细信息，请见 第 83 页 “ 手动更新病毒防护定义库” 和 第 83 页 “ 手动更新攻击定义库” 。

RMA 之后注册 FortiGate 设备

返修设备授权 （RMA）过程发生在用户注册的 FortiGate 设备出现硬件故障无法正常工作的时候。如果这一情况发生在 FortiGate 设备的硬件维修期内，您可以将出现故障的 FortiGate 设备送回到您的分销商处。

RMA 是有记录的，而您将收到一个代替的设备。Fortinet 会将 RMA 信息添加到 Fortinet 支持数据库中。当您受到代替的设备之后，您可以按照如下步骤更新您的产品注册信息。

1 进入 **系统 > 更新 > 支持** 并单击支持登录。

2 输入您的 Fortinet 支持用户名和密码以登录到 Fortinet 支持。

3 单击添加注册。

4 单击 从 RMA 用新设备替换现有设备的链接。

5 如果 RMA 已经被输入了 Fortinet 的支持数据库，您可以选择替换现有设备并输入那个替代设备的序列号。

6 单击完成。

将显示您已注册的 FortiGate 产品列表。这个列表现在包括了那个替换的 FortiGate 设备。所有您原有的支持服务都将被转到这个替换的设备上。

网络配置

进入 **系统 > 网络** 可以对 FortiGate 网络设置做以下修改：

- 配置网络接口
- 添加 DNS 服务器 IP 地址
- 配置路由
- 在您的内部网络中提供 DHCP 服务

配置网络接口

按照以下步骤可以配置网络接口：

- 查看接口列表
- 启动一个接口
- 修改一个接口的静态 IP 地址
- 为接口添加第二个 IP 地址
- 为接口添加 ping 服务器
- 控制到接口的管理访问
- 为接口的连接配置通讯日志
- 使用静态 IP 地址配置外部网络接口
- 使用 DHCP 配置外部网络接口
- 为以太网点对点传输协议 （PPPoE）配置外部网络接口
- 修改外部网络接口的 MTU 大小以提高网络性能
- 将 DMZ/HA 接口配置为 DMZ 模式
- 将 DMZ/HA 网络接口配置为以 HA 方式工作
- 配置管理接口 （透明模式）

查看接口列表

按照如下步骤查看接口列表。

1 进入 **系统 > 接口。**

将显示接口列表。接口列表显示了 FortiGate 所有接口的以下状态信息：

- 接口的 IP 地址
- 接口的网络掩码
- 接口的管理访问配置
- 接口的连接状态

如果连接状态是绿色箭头，则此接口在工作中并可以接受网络通讯。如果连接状态是红色箭头，则此接口关闭并且不能接受网络通讯。要启动一个接口，请见 “启动一个接口”中所描述的步骤。

启动一个接口

如果一个接口的接口连接状态是关闭，您可以使用以下步骤启动这个接口。

1 进入 **系统 > 接口。**

显示接口列表。

2 单击您要启动的接口的启动按钮。

修改一个接口的静态 IP 地址

使用以下步骤可以修改任何 FortiGate 接口的 IP 地址。您还可以使用以下步骤为一个接口添加 IP 地址。

1 进入 **系统 > 网络 > 接口。**

2 对你要修改的接口单击修改  。

3 根据需要修改 IP 地址和网络掩码。

接口的 IP 地址必须和接口所连接的网络在同一子网内。

任何两个接口不能有相同的 IP 地址或在同一子网内的 IP 地址。

4 单击确定以保存您所做的修改。

如果您修改了你用来连接到 FortiGate 设备进行管理操作的接口的 IP 地址，您必须使用新的 IP 地址重新连接到基于 Web 的管理程序。

为接口添加第二个 IP 地址

您可以使用 CLI 为任何 FortiGate 接口添加第二个 IP 地址。第二个 IP 地址不能和主 IP 地址相同，但是它们可以在同一子网内。

用以下 CLI 命令添加第二个 IP 地址：

```
set system interface internal config secip <第二 ip> <网络掩码_ip>
```

您还可以为第二个 IP 地址配置管理访问和添加 PING 服务器。

```
set system interface <接口名_字符串> config secallowaccess ping
https ssh snmp http telnet
```

```
set system interface <接口名_字符串> config secgwdetect enable
```

为接口添加 ping 服务器

如果您希望 FortiGate 设备确认连接到一个网络接口的网络中的下一个路由器到这个接口的连接是否有效，可以为这个接口添加一个 ping 服务器。路由失效功能需要添加 ping 服务器。请见 第 114 页 “ 向路由表添加基于目的的路由” 。

1 进入 **系统 > 网络 > 接口。**

2 在您要添加 ping 服务器的接口上单击修改  。

3 将 PING 服务器设置为到连接到这个接口的网络中的下一个路由器的 IP 地址。

4 单击启用。

FortiGate 设备使用失效网关检测功能 ping 您所设置的 ping 服务器的 IP 地址，以确定 FortiGate 设备可以连接到这个 IP 地址。要配置失效网关检测功能，请见 第 129 页 “ 修改失效网关检测设置” 。

5 单击确定以保存您所做的修改。

控制到接口的管理访问

1 进入 **系统 > 网络 > 接口。**

2 对您要配置管理访问的接口，单击修改  。

3 选择这个接口的管理访问权限。

HTTPS	允许安全 HTTPS 连接通过此接口连接到 基于 Web 的管理程序。
PING	如果您希望网络接口对 PING 作出响应，选中此项。用于验证您的安装和测试。
HTTP	允许 HTTP 连接通过此接口连接到 基于 Web 的管理程序。 HTTP 连接是不安全的，可能被第三方所截获。
SSH	允许安全 SSH 连接通过此接口连接到 CLI。
SNMP	允许远程 SNMP 管理者连接到这个接口请求 SNMP 信息。见 第 131 页 “ 配置 SNMP” 。
TELNET	允许通过这个接口使用 CLI 的 Telnet 连接。Telnet 连接是不安全的，可能被第三方所截获。

配置对一个连接到互联网的接口的管理访问方式将允许从互联网中的任何地方对这个 FortiGate 设备进行远程管理。允许来自互联网的对您的 FortiGate 设备的远程管理可能会危及您的设备的安全性。您应当禁止对连接到互联网的网络接口的管理访问的许可，除非这是必须的。要提高允许从互联网访问的 FortiGate 设备的安全性，需要为有管理权限的用户设置安全的密码，定期更换这些密码，并且只启用 HTTPS 或 SSH 的安全管理访问。

4 单击确定以保存您所做的修改。

为接口的连接配置通讯日志

1 进入 **系统 > 网络 > 通讯。**

2 在要配置日志的接口上单击修改  。

3 单击日志以将这个接口设置为某个防火墙策略接收连接时记录日志消息。

4 单击确定以保存您所做的修改。

图 1: 配置内部接口

使用静态 IP 地址配置外部网络接口

1 进入**系统 > 网络 > 接口**。

2 选择对应的 外部网络接口，单击 修改 。

3 将 地址模式 改为 指定 。

4 根据需要修改 IP 地址 和 子网掩码 。

5 单击 确定 以保存修改。

使用 DHCP 配置外部网络接口

按照以下步骤将外部网络接口配置为使用 DHCP。只有当您的 ISP 使用 DHCP 来分配您的外部网络接口的 IP 地址时，才需要使用这种配置。

1 进入 **系统 > 网络 > 接口**。

2 对外部网络接口，单击 修改 。

3 将地址模式设置为 DHCP，单击 确定 以切换到 DHCP 模式。
此时 IP 地址和子网掩码都将变成 0.0.0.0。

4 选择 启用到 DHCP 服务器的连接，使 FortiGate 在启动时自动连接到 DHCP 服务器上。
如果您没有选择连接到 DHCP 服务器，FortiGate 设备将不连接到 DHCP 服务器。如果您要将 FortiGate 设备配置为离线状态，可以取消对这一选项的选中。

5 单击 确定 。
FortiGate 将试图从外部网络接口连接到一个 DHCP 服务器，以获取外部网络接口的 IP 地址，子网掩码和网关的配置信息。当 FortiGate 从 DHCP 服务器取得了这些信息之后，新的 IP 地址和子网掩码将显示在 IP 地址和子网掩码区域里。

为以太网点对点传输协议 （PPPoE）配置外部网络接口

以下步骤可以将外部网络接口配置为使用以太网点对点传输协议 （PPPoE）。如果您的 ISP 使用 PPPoE 为外部网络接口分配 IP 地址，就需要使用这种配置。

1 进入 **系统 > 网络 > 接口**。

2 对外部网络接口，单击 修改  。

3 将 地址模式 改为 PPPoE ，单击 确定 以转换到 PPPoE 模式。

4 输入您的 PPPoE 帐号的 用户名 和 密码 。

5 单击 确定 。

FortiGate 将试图连接到 PPPoE 服务器以获取外部网络接口的 IP 地址、子网掩码和网关的配置信息。当 FortiGate 从 PPPoE 服务器上获得了这些信息之后，新的 IP 地址和子网掩码将显示在外部 IP 地址和子网掩码区域里。如果到您的 ISP 的 PPPoE 连接已经中断了，FortiGate 将自动重新建立连接。

6 如果您希望 FortiGate 在每次启动时自动连接到 PPPoE 服务器，选择 启用 PPPoE 连接。

如果您没有选择连接到 PPPoE 服务器，FortiGate 设备将不连接到 PPPoE 服务器。如果您要将 FortiGate 设备配置为离线状态，可以取消对这一选项的选中。

7 单击 确定 。

修改外部网络接口的 MTU 大小以提高网络性能

为了提高互联网连接的性能，可以调整 FortiGate 在外部网络接口上传输数据时数据包的最大传输 （MTU）的尺寸。理想情况下，FortiGate 的外部网络接口上的 MTU 的尺寸应该等于从 FortiGate 到互联网所经过的所有网络中最小的 MTU 的尺寸。如果 FortiGate 发送的 MTU 大于这一尺寸，数据包在传输过程中将被分割成碎片，这将减慢传输速度。

只有一种方法能够找出最优的 MTU 尺寸，那就是反复实验。但是也有一些信息能对我们调整 MTU 的尺寸提供帮助。例如，多数点对点协议 （PPP）连接的 MTU 是 576，所以如果您是通过 PPP 或者 PPPoE 连接到互联网的，您可以试试将 MTU 的尺寸设为 576。DSL 调制解调器使用很小的 MTU 尺寸。大多数以太网使用的 MTU 是 1500。

注意：如果您的 ISP 使用 DHCP 为外部网络接口分配 IP 地址，则不能把 MTU 设置得小于 576。因为这是 DHCP 通信的最小值。

注意：如果外部网络接口使用的是 PPPoE，MTU 可能是使用 PPPoE 协议的两端协商的结果。在这种情况下，系统将覆盖您对 MTU 尺寸的设定。

以下操作将改变从外部网络接口发出的数据包的 MTU 尺寸：

1 进入 **系统 > 网络 > 接口**。

2 对外部网络接口，单击 修改  。

3 选择 大于 MTU 的发出数据包 。

4 选择 MTU 尺寸 。

可以将最大的数据包尺寸设定在 68 字节到 1500 字节之间。默认的 MTU 尺寸是 1500 字节。您可以试着减小 MTU 的尺寸以找到网络性能最高的时对应的 MTU 尺寸。

将 DMZ/HA 接口配置为 DMZ 模式

按照如下步骤可以将 DMZ/HA 接口配置为连接到 DMZ 网络。当您将 DMZ/HA 接口配置为 DMZ 模式的时候，您可以创建用于连接 DMZ 网络和内部网络、DMZ 网络和外部网络的防火墙策略。DMZ 模式是这个接口的默认操作模式。

以下步骤将 DMZ/HA 接口配置为 DMZ 模式

1 进入 **系统 > 网络 > 接口**。

2 选择 **DMZ/HA 接口** ，单击 **修改**  。

3 选择 **DMZ**。

4 单击 **确定** 以保存您所做的修改。

将 DMZ/HA 网络接口配置为以 HA 方式工作

如果您将两台 FortiGate 连接起来以高可用性方式运行，则必须把他们的 DMZ/HA 网络接口切换到 HA 模式。在这种模式下，不能再将 DMZ/HA 接口连接到 DMZ 网络上。它只能用来连接 HA 组中的另一台 FortiGate 的 DMZ/HA 接口。在 HA 组中的 FortiGate-300 使用这个接口交流 HA 模式的状态和配置信息。

以下步骤将 DMZ/HA 接口配置为以 HA 模式工作：

1 进入 **系统 > 网络 > 接口**。

2 选择 **DMZ/HA 接口**，单击 **修改**  .

3 选择 **HA** 。

4 单击 **确定** 以保存您所做的修改。

配置管理接口（透明模式）

在透明模式下，您可以配置 FortiGate 用于管理访问的管理接口。

1 进入 **系统 > 网络 > 管理**。

2 根据需要修改管理用的 **IP 地址** 和 **子网掩码** 。
设置的 IP 地址和子网掩码必须是您用来管理 FortiGate 的网络中的有效地址和掩码。

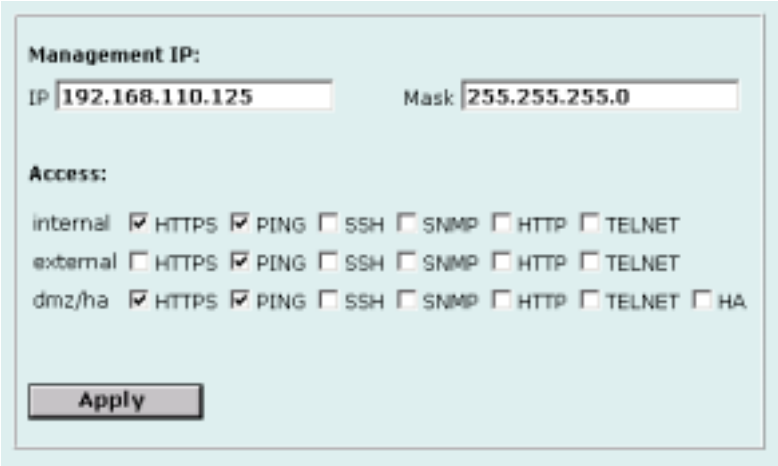
3 如果 FortiGate 设备需要通过默认网关才能访问管理员电脑，则为接口添加默认网关 IP 地址。

4 选择每个网络接口的 **管理访问方式** 。
在透明模式的默认情况下，您可以连接到内部网络接口或 DMZ 网络接口对 FortiGate 进行管理。但是您可以配置用于管理的网络接口，所以您可以连接到任何一个网络接口进行管理。

HTTPS	允许安全 HTTPS 连接通过此接口连接到 基于 Web 的管理程序。
PING	如果您希望网络接口对 PING 作出响应，选中此项。用于验证您的安装和测试。
HTTP	允许 HTTP 连接通过此接口连接到 基于 Web 的管理程序。 HTTP 连接是不安全的，可能被第三方所截获。
SSH	允许安全 SSH 连接通过此接口连接到 CLI。
SNMP	允许远程 SNMP 管理者连接到这个接口请求 SNMP 信息。见 第 131 页 “ 配置 SNMP” 。
TELNET	允许通过这个接口使用 CLI 的 Telnet 连接。Telnet 连接是不安全的，可能被第三方所截获。

5 单击 **应用** 以保存您所做的修改。

图 2: 配置管理接口



添加 DNS 服务器 IP 地址

包括发送报警邮件和 URL 阻塞在内的多数 FortiGate 功能都需要使用 DNS 服务。

以下操作用来设置 DNS 服务器地址：

1 进入 **系统** > **网络** > **DNS**。

2 根据需要修改 **主 DNS 服务器** 和 **辅助 DNS 服务器** 的设定。

3 单击 **应用** 以保存修改。

配置路由

本节描述了如何配置 FortiGate 的路由。您可以将路由配置为从 FortiGate 到本地路由器的静态路由。您还可以使用策略路由提高 FortiGate 路由的灵活性，以提供更高级的路由功能。

您也可以使用多重路由网关和建立广域网的多重配置以提供对两个互联网连接的冗余和负载均衡的支持。

本节叙述了以下内容：

- 添加默认路由
- 向路由表添加基于目的的路由
- 添加路由 （透明模式）
- 配置路由表
- 策略路由

添加默认路由

以下操作将为外部网络接口向外发出的数据设定一个默认的路由。

1 进入 **系统 > 网络 > 路由 表**。
2 单击 **新建** 。
3 将 **源 IP 地址** 和 **子网掩码** 设置为 0.0.0.0。
4 将 **目的 IP 地址** 和 **子网掩码** 设置为 0.0.0.0。
5 将 **网关 1** 的 **IP 地址** 设置为发送到互联网的数据要使用的路由网关的 IP 地址。
6 单击 **确定** 以保存这个路由。

注意：在同一时间只有一条路由是活动的。如果在一个路由表中添加了两条默认路由，只有接近路由表顶部的那条默认路由是活动的。

向路由表添加基于目的的路由

按照如下步骤可将基于目的的路由添加到路由表。添加基于目的的路由可以控制从 FortiGate 设备发出的通讯的目的地。您可以通过添加目的 IP 地址和网络掩码、添加这些目的地址的网关来配置路由。这个网关是与路由中的目的地址匹配的路由通讯中的下一个跳跃的路由器。

您可以为一个路由添加一个或两个网关。如果您添加了一个网关，FortiGate 设备将通讯路由到这个网关。您可以添加第二个网关，这样当第一个网关失效时通讯将被路由到第二个网关。

要支持路由失效恢复，必须将每个网关的 IP 地址添加到同一网络内的对应的 FortiGate 设备的网络接口的 ping 服务器设置中。请见 第 109 页 “ 为接口添加 ping 服务器” 。

为路由表添加基于目的的路由

1 进入 **系统 > 网络 > 路由表**。
2 单击 **新建** 以添加一个新的路由。
3 输入这个路由的 **目的 IP 地址** 和 **子网掩码** 。
4 输入一号网关的 IP 地址。

一号网关是这个路由的主目的地址的 IP 地址。

一号网关必须和 FortiGate 网络接口在同一子网内。

如果您是从 ForitGate 设备添加一个到单一目的路由器的静态路由，您只须指定一个网关。

5 （可选的）如果您希望为路由通讯提供多重网关，可以添加二号网关的 IP 地址。
6 （可选的）一号设备以指定 FortiGate 用来将路由通讯连接到一号网关的接口。
7 （可选的）二号设备以指定 FortiGate 用来将路由通讯连接到二号网关的接口。
8 单击确定以保存路由设置。

注意：路由表中的任意两条路由除了网关之外必须有一些不同点，才能在同一时间生效。如果在路由表中添加了两条除了网关 IP 地址以外完全一致的路由，只有接近路由表顶部的路由能够生效。

注意：将路由表中的路由按照从特殊到一般的顺序排列。有关路由表中的路由的排列顺序，请参阅 “配置路由表”。

添加路由 （透明模式）

以下操作用于 FortiGate 在透明模式运行时添加路由：

1 进入 **系统** > **网络** > **路由**。
2 单击 **新建** 以添加新的路由。
3 输入这个路由的 **目的 IP 地址** 和 **子网掩码** 。
4 输入这个路由的 **网关的 IP 地址**。
5 单击 **确定** 以保存新的路由。
6 如果需要的话重复以上操作添加更多路由。

配置路由表

路由表显示了每个路由的目的地址、网络掩码和添加到路由的网关和设备。路由表还显示了网关的连接状态。 一个绿色的对勾表示 FortiGate 使用 ping 服务器和网关失效检测判断可以连接到这个网关，一个红色的叉子意味着 FortiGate 无法建立到这个网关的连接。兰色问号的意思是这个连接的状态未知。关于更进一步的信息，请见 第 109 页 “ 为接口添加 ping 服务器” 。

FortiGate 选用路由的方式是从上到下地扫描路由表寻找匹配的路由，直到它找到第一个匹配的路由为止。您必须把路由在路由表中按照专用的路由到通用路由的顺序排列。默认的路由是通用路由中的最后一个。所以如果添加了默认路由，它应该位于路由表的最底端的位置。

1 进入 **系统** > **网络** > **路由表** 。
2 选择要移动的路由，然后单击 **移动** 以改变它在路由表中的位置。
3 在 **移动到的位置** 一栏输入序号，这个序号是您想要这个路由移动到路由表中的位置序号。然后单击 **确定** 。
4 单击 **删除** 可以从路由表中删除一个路由。

图 3: 路由表

策略路由

策略路由拓展了目的路由的功能。您可以使用策略路由根据以下内容路由通讯：

- 源地址
- 协议、服务类型或端口范围
- 进入的或源接口

您可以使用策略路由创建一个路由策略数据库 (RPDB)，从一组路由规则中为通讯找出适当的路由。要为通讯选择一个路由，FortiGate 从头搜索 RPDB 寻找与通讯匹配的路由策略。搜索到的第一个匹配的策略将被用于设置通讯的路由。路由支持网络跳跃网关和用于此通讯的 FortiGate 接口。

数据包在匹配目的路由之前，先于策略路由进行匹配。如果不能使用一条策略路由来匹配这个数据包，将使用目的路由来路由这个数据包。

添加到策略路由的网关必须也被添加到一条目的路由。当 FortiGate 设备使用 RPDB 中的路由匹配数据包时，它在目的路由表中搜索添加到这个策略路由的网关。如果发现了匹配的结果，FortiGate 设备将使用匹配的目的路由来路由这个数据包。如果没有找到匹配的结果，FortiGate 设备将使用常规路由来路由这个数据包。

为了找到带有匹配的网关的路由，FortiGate 设备从目的路由表的顶部开始向下搜索，直到它找到第一条匹配的目的路由为止。这条匹配的路由将被用来路由这个数据包。

策略路由命令语法

使用以下 CLI 命令配置策略路由。

```
set system route policy <路由编号_整数> src <源_ip> <源_掩码> iifname <源接口_名称> dst <目的_ip> <目的_掩码> oifname <目的接口_名称> protocol <协议编号_整数> port <低端口_整数> <高端口_整数> gw <网关_ip>
```

在第六卷：*FortiGateCLI 参考指南*中有关于策略路由语法的完整叙述。

在您的内部网络中提供 DHCP 服务

如果 FortiGate 运行在 NAT/ 路由模式下，可以把它配置成内部网络的 DHCP 服务器。

1 进入 **系统 > 网络 > DHCP** 。

2 选择 **启用 DHCP** 。

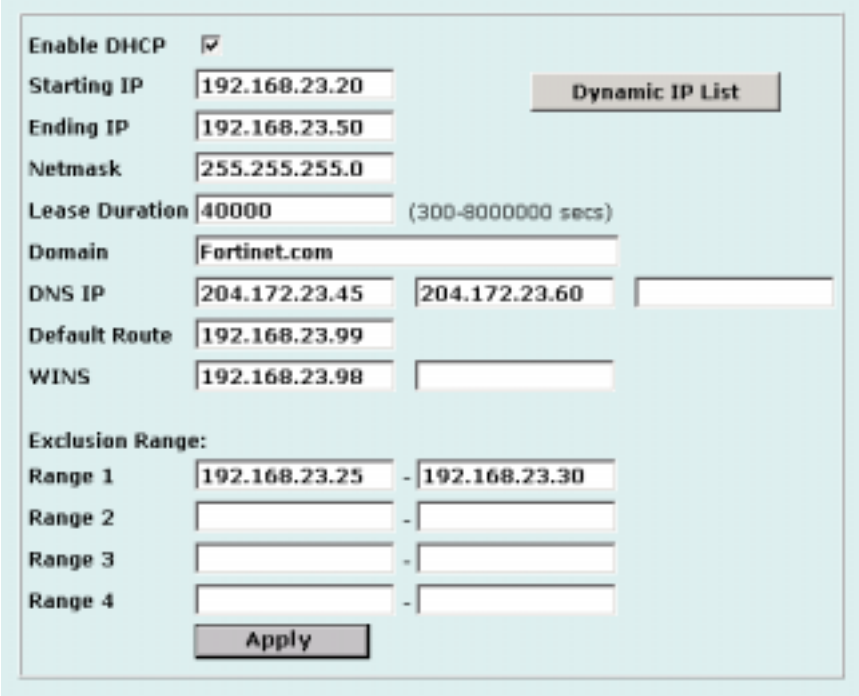
3 配置 **DHCP 设置** 。

起点 IP **终点 IP**	FortiGate 根据您输入的起点 IP 和终点 IP 确定能够分配给 DHCP 客户的 IP 地址范围。这些 IP 地址必须是您内部子网上的 IP 地址。
子网掩码	输入 FortiGate 分配给 DHCP 客户的子网掩码。
有效期	输入以秒为单位的时间间隔。这个时间间隔是 DHCP 客户需要向 DHCP 服务器申请新的 IP 之前所经历的时间。可以输入的有效期的范围是 300 到 604800 秒。
域	可选的项目。域中输入的是 DHCP 服务器分配给 DHCP 客户的域名。
DNS IP	输入最多 3 个 DNS 服务器的 IP 地址。DHCP 客户 可以用这些 DNS 服务器做域名解析。
默认路由	输入分配给 DHCP 客户的默认网关。默认网关必须和起点地址、终点地址在同一子网内。
WINS	添加一个或两个要为 DHCP 客户指定的 WINS 服务器 IP 地址。
排除范围	可选的输入项。最多可以输入 4 个排除范围。这些由起点 IP 地址和终点 IP 地址限定的排除范围内的 IP 将不会被分配给 DHCP 客户。

4 单击 **应用** 。

5 把网络上的电脑的 IP 地址设置配置为 **通过 DHCP 自动获取 IP 地址** 。

图 4: DHCP 设置的例子



查看动态 IP 列表

如果您已经配置了 FortiGate 上的 DHCP 服务器，您可以查看 DHCP 服务器已经分配的动态 IP 列表。 列表中除了 IP 地址外，还包括相应的 MAC 地址以及这些 IP 地址的有效期。FortiGate 把这些地址添加到动态 IP/MAC 地址列表中。并且如果启用了 IP/MAC 绑定功能，动态 IP/MAC 地址列表中的地址将被加入信任的 IP/MAC 地址对中去。要获取关于 IP/MAC 地址绑定的更多信息，请查阅 第 160 页 “ IP/MAC 绑定” 。

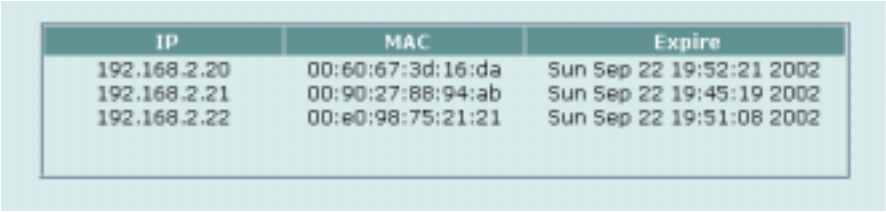
以下操作用于查看动态 IP 地址列表：

1 进入 **系统** > **网络** > **DHCP** 。

2 选择 **动态 IP 地址列表** 。

将显示动态 IP 地址列表。

图 5: 动态 IP 地址列表的例子



RIP 配置

FortiGate 路由信息协议 （RIP）实现支持 RIP 版本 1 （RFC1058 所定义）和 RIP 版本 2 （也称做 RIP2，RFC2453 所定义）。RIP2 启用了 RIP 消息从而能够承载更多信息和支持简单的认证。RIP2 也支持 RIP 不支持的子网掩码功能。

RIP 每过一个固定的时间间隔或网络拓扑结构改变时就发送路由更新消息。 当 FortiGate 设备接收到一个包含了改动了的条目的路由表时，它将在自己的路由表上做相应的改动。FortiGateRIP 表保存着到目的地的最佳路由。在更新完自己的路由表之后，FortiGate 设备开始发送路由更新以提醒其他网络路由器路由已经改变。您可以配置 FortiGat RIP 以控制更新的时机。

RIP 使用跳跃统计作为路由度量以衡量一个路由的源网络和目的网络之间的距离。在路由的路径中的每个跳跃都将被添加到这个路由的度量中。RIP 将一个路径中允许的最大跳跃数限制为 15 以防止路由循环。这一特性也将 RIP 网络的最大半径限制为 15 个跳跃。

RIP 使用水平分割来防止网络拓扑改变引起的临时路由循环。水平分割可以保证永远不会将关于路由器的信息发送回它发出的地方。例如，路由器 1 可以告诉路由器 2 它有一个关于网络 A 的路由。路由器 2 通过从路由器 1 获取信息知道了这一事实，所以当路由器 2 将它自己的更新发送给路由器 1 时，它不会把关于网络 A 的路由更新信息包括进去。在本例中，如果路由器 1 收到了路由器 2 发送的关于网络 A 的路由信息，路由器 1 可能会试图使用这一路由去连接网络 A，而不是使用它自己的路由。

RIP 使用计时器来调节性能。一个路由更新计时器控制了两次路由更新之间的时间间隔。通常这一计时器被设置为 30 秒。每个路由表中的条目都有一个路由超时设置。当发生路由超时的时候此路由将被标记为无效。无效的路由在路由刷新超时到期之前将一直保存在路由表中。

RIP 是一个基于 UDP 的协议，它使用 UDP 端口 520 发送和接收数据包。主动的路由更新消息包含源端口和目的端口，且此两端口都等于 RIP 端口。根据更新请求发出的更新消息将发送到请求所来自的那个端口。特定的查询可以从除了 RIP 端口外的端口发出，但是它们必须发送到目的主机的 RIP 端口上。

本章描述了如何配置 FortiGate RIP：

RIP 设置

配置 RIP 设置以启用基本的 RIP 功能和度量，以及配置 RIP 计时器。

1 进入 **系统 >RIP> 设置。**

2 单击启用 RIP 服务器以将 FortiGate 设备配置为一个 RIP 服务器。

3 单击启用广告默认值以使得 FortiGate 设备在 RIP 路由表更新中包含它的默认路由。

4 单击启用自动归纳以自动将子网路由归纳进网络级路由中。

如果自动归纳功能没有启用，FortiGate 将穿过常规网络的边界传输子网络后缀路由。

5 修改以下 RIP 默认设置以调整并优化 RIP 性能。

RIP 默认设置在大多数配置中是有效的。只有当您的 RIP 配置出现问题的时候您才有必要修改这些设置。

默认度量 对默认度量的修改将应用到带有不兼容的度量的路由上。默认的度量帮助解决如何分配带有不兼容的度量的路由问题。任何时候当度量无法被转换时，RIP 使用默认的度量提供一个合理的替代度量以使得重新分配工作可以继续进行。默认度量的默认设置是 2。

输入队列 修改 RIP 输入队列的长度。设置的数值越大，则队列越长。如果您的 FortiGate 设备使用很高的速度向一个可能无法以此速度接收的低速的路由器发送数据，则您可以修改队列长度以适应这一情况。修改这一配置可以防止路由表丢失信息。可以设置的值的范围是从 0 到 1024。默认的输入队列的长度是 50。长度为 0 的输入队列意味着没有输入队列。

输出延迟 修改输出延迟可以在多数据包 RIP 更新的数据包时间添加毫秒级的延迟。标准的输出延迟是 8 到 50 毫秒。如果您配置 RIP 的 FortiGate 设备要将更新数据包发送到一个路由器，而这个路由器又无法以 FortiGate 设备发送的速率接收更新数据包，那么您可以为 FortiGate RIP 设定一个输出延迟。默认的输出延迟是 0 毫秒。

6 修改以下 RIP 计时器设置以调整和优化 RIP 的性能。

RIP 计时器的默认设置在大多数配置中都能正常工作。只有当您的 RIP 配置出现问题的时候您才有必要修改计时器设置。

更新 两次发送路由表更新之间的以秒为单位的时间间隔。默认的间隔是 30 秒。

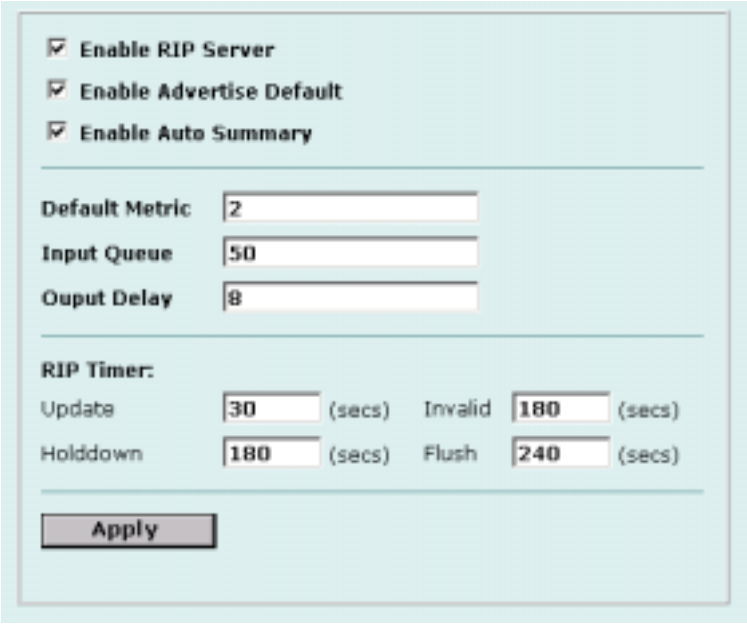
失效 路由被宣布为失效的以秒为单位的时间间隔。失效时间间隔应当至少是更新时间间隔的三倍。当没有更新信息刷新一条路由时，这个路由即被宣布为失效。于是这条路由进入阻挡状态。这条路由将被标记为不可访问，并对外宣布路由不可到达。然而，这个路由仍旧可以用于转发数据包。默认的值是 180 秒。

阻挡 路由信息表明路径被禁止的以秒为单位的时间间隔。阻挡应当至少是更新时间间隔的三倍。当收到一个更新数据包指示路由不可到达时，该路由进入阻挡状态。此路由将被标记为不可访问和对外宣布为不可到达，且不再用于转发数据包。当阻挡过期时，路由可以被从路由表中清除。默认的设置是 180 秒。

清除 一条路由被从路由表中删除之前必须经历的以秒为单位的时间。清除的值必须大于失效的时间设置。如果清除的值小于失效时间设置，系统将不会等待正常的阻挡时间间隔完成，结果就是将在阻挡时间间隔完成之前就接受了一条新的路由。默认的值是 240 秒。

7 单击应用以保存您所做的设置。

图 1: 配置 RIP 设置



为 FortiGate 接口配置 RIP

您可以为每个 FortiGate 接口创建一个单独的配置。这样一来您就可以为您的 FortiGate 设备的每个接口上所连接的网络定制专用的 RIP。例如：

- 如果您有一个复杂的内部网络，其中包含了使用 RIP2 协议的设备。您可能希望在内部接口上配置 RIP2 发送和接收功能。
- 如果外部接口是连接到互联网的，您可能不希望在这个接口上启用 RIP 发送功能，使得内部路由不被暴露到互联网上。然而，您可能希望配置 RIP 接收功能使得 FortiGate 设备可以从您的 ISP 接收路由信息。
- 如果 DMZ 接口连接到一个小型的 DMZ 网络，您可能无须为这个接口配置 RIP。

按如下步骤配置 FortiGate 接口的 RIP

1 进入 **系统 >RIP> 接口**。
在本页您可以看到每个 FortiGate 接口的 RIP 设置的摘要。

2 对要配置 RIP 设置的接口单击修改。

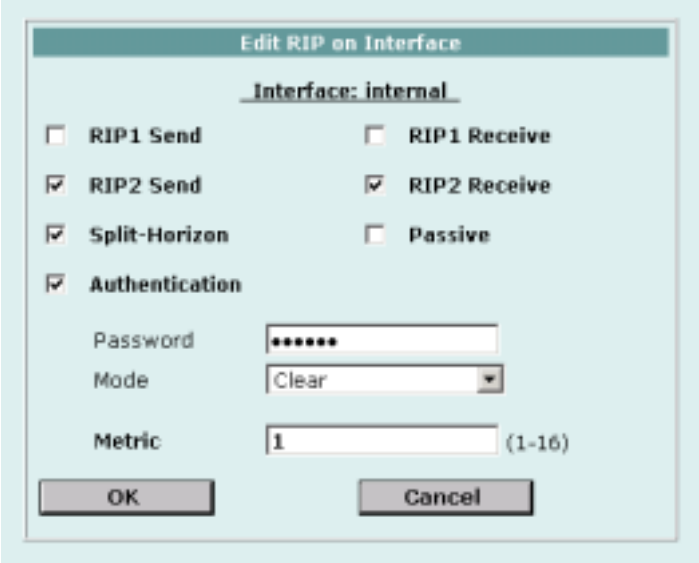
3 配置以下 RIP 设置：

RIP1 发送	本接口可以将 RIP1 路由广播发送到此网络上的其他路由器。路由信息是目的端口为 520 的 UDP 数据包。
RIP1 接收	这个接口可以接收 RIP1 广播。这个接口将在 520 端口监听 RIP1 路由消息。
RIP2 发送	此接口可以向它所连接的网络中的路由器广播 RIP2 路由消息。路由消息是目的端口为 520 的 UDP 数据包。
RIP2 接收	这个接口可以接收 RIP2 广播。这个接口将在 520 端口监听 RIP2 路由消息。
水平分割	配置水平分割可以防止路由循环。默认情况下，水平分割已经被启用。只有您确定这一接口所连的网络中不会产生路由循环时才能禁用此选项。
被动	此版本不支持被动模式。
认证	启用这个接口发送的 RIP2 数据包的认证。只有 RIP2 支持认证。如果您将接口配置为使用 RIP1，不要选择认证功能。
密码	在 RIP2 请求中输入密码。密码最多可以有 16 个字符。
模式	定义 FortiGate RIP2 数据包的认证方式。可以选择明文或 MD5。 无 意味着不发送密码。 明文 意味着不加密。密码为明文。 MD5 意味着使用 MD5 加密算法加密密码。
度量	修改由这个接口发送的路由的度量。从这个接口发送的全部路由将把这个度量值添加到他们的当前度量值中。您可以设置接口的度量值以提高一些接口的优先级。例如，如果您有两个接口可以为同一个目的地提供路由，如果您将其中一个接口的度量值设置得比另一个接口高，这个接口上的度量值较低的路由看起来代价较低，所以大多数通讯将使用这个接口上的度量值较低的路由。度量的值范围是从 1 到 16。

注意： MD5 认证用于 FortiGate 设备发送的路由信息的完整性。使用 MD5 认证时，路由信息中附加了密码并且使用 MD5 为这条路由信息创建 MD5 摘要。这条路由信息中的密码将被 MD5 摘要替换并进行广播。当一个路由器收到这条路由信息时，它将 MD5 摘要信息替换为密码，计算这条新信息的 MD5 摘要，然后将这个 MD5 摘要和原始信息中的 MD5 摘要做对比。如果两个 MD5 摘要是一致的，接收者将接受这条消息。如果它们不同，接收者将拒绝这条消息。

4 单击确定一保存选定接口上的 RIP 配置。

图 2: 一个内部接口上的 RIP 配置的例子



添加 RIP 邻居

添加 RIP 邻居可以定义用于交换路由信息的邻近的路由器。将邻居添加到非广播网络中。

当您添加邻居的时候，FortiGate 设备与邻居直接交换信息，而不是依赖于广播路由。这种 FortiGate 和添加到邻居列表的路由器之间的点对点的路由信息交换更加安全，并且可以减少网络通讯。在非广播网络中必须添加邻居以交换路由。

当使用组合的 RIP 过滤器时，FortiGate 设备可以配置为与路由器的子网交换路由和访问一个局域网中的服务器。

添加 RIP 邻居

1 进入 **系统 >RIP> 邻居。**

2 单击新建以添加 RIP 邻居。

3 添加您希望 FortiGate 与之交换路由信息的邻居路由器的 IP 地址。

4 单击发送 RIP1 以将 RIP1 消息发送到邻居。

5 单击启用发送 RIP2 以将 RIP2 消息发送到邻居。

6 单击确定以将 RIP 邻居添加到列表。

添加 RIP 过滤器

使用 RIP 过滤器可以控制 FortiGate 设备接收的路由信息和 FortiGate 设备发送的路由信息。您可以创建两种过滤器：

邻居过滤器 用于过滤从邻近路由器接收的路由。当 FortiGate 设备从一个邻近的路由器接收路由时，邻居过滤器定义了哪些从邻居接收的路由可以保存到 FortiGate 路由列表，那些路由将被丢弃。

路由过滤器 用于在路由表被发送到邻近路由器之前对路由进行过滤。在 FortiGate 设备将路由发送到邻近的路由器之前，路由过滤器决定了哪些路由可以发送、哪些路由不能被发送。

RIP 过滤器包括路由的 IP 地址和网络掩码、对这个路由执行的操作 （接受或拒绝）、以及这个过滤器应用到的接口。在 RIP 过滤器中找不到匹配的路由将被允许接受。

单一 RIP 过滤器包含对单一路由的接受或拒绝的指令。您可以在同一个 RIP 过滤器名下添加多个 RIP 路由入口，以创建一个 RIP 过滤器列表。您可以使用一个 RIP 过滤列表过滤多个路由。

创建完 RIP 过滤器和过滤器列表之后，您可以通过为每种类型的过滤器选择一个过滤器或者过滤列表来配置邻居过滤器或路由过滤器。如果您没有为邻居或路由选择 RIP 过滤器，则不会对它们应用过滤。您最多可以添加 4 个 RIP 过滤器或过滤列表，但是您只能设置一个活动的邻居过滤器和一个活动的路由过滤器。

本节叙述了如下内容：

添加单一 RIP 过滤器

添加单一 RIP 过滤器可以过滤单一过滤。您可以对邻居过滤器或路由过滤器应用单一 RIP 过滤器。您最多可以添加 4 个 RIP 过滤器或 RIP 过滤列表。

如果您希望过滤多条路由，可以使用 RIP 过滤器列表。请见 第 124 页 “ 添加一个 RIP 过滤列表” 。

1 进入 **系统 >RIP> 过滤器。**

2 单击新建以添加一个 RIP 过滤器。

3 配置这个 RIP 过滤器。

过滤器名	为这个 RIP 过滤器输入一个名称。每个 RIP 过滤器和 RIP 过滤器列表必须有一个单独的名称。这个名称的长度为 15 个字符，可以包含大写和小写字母、数字和特定字符。名称不能包含空格。
空白过滤器	使用过滤器列表。请见 第 124 页 “ 添加一个 RIP 过滤列表” 。
IP	添加路由的 IP 地址。
掩码	添加路由的网络掩码。
动作	选择允许可以使过滤器允许这个路由的通讯。选择拒绝可以阻止这个路由被交换。
接口	选择这个 RIP 过滤器要应用到的接口。

4 单击确定以保存这个过滤器。

添加一个 RIP 过滤列表

添加一个 RIP 过滤器列表可以过滤多条路由。一个 RIP 过滤器列表包括一个 RIP 过滤器名和一系列的路由前缀。您最多可以添加 4 个 RIP 过滤器或者 RIP 过滤器列表。

当一个 RIP 过滤器列表被添加到邻居过滤器或者路由过滤器时，RIP 过滤器列表中的所有路由都将被过滤。

1 进入 **系统 >RIP> 过滤器。**

2 单击新建以添加一个 RIP 过滤器。

3 配置这个 RIP 过滤器列表。

过滤器名	输入 RIP 过滤器列表的名称。每个 RIP 过滤器和 RIP 过滤器列表必须有一个单独的名称。这个名称的长度为 15 个字符，可以包含大写和小写字母、数字和特定字符。名称不能包含空格。
空白过滤器	可以选择空白过滤器将 RIP 过滤器列表开头设置为一个空白。添加空白过滤器后您可以将路由添加到 RIP 过滤器列表。

4 单击确定以保存 RIP 过滤器列表。

5 对 RIP 过滤器列表名，单击 添加前缀可以将路由前缀添加到这个过滤器列表。

6 配置路由前缀。

IP	添加这个路由的 IP 地址。
掩码	添加这个路由的掩码。
动作	选择允许可以使过滤器允许这个路由的通讯。选择拒绝可以阻止这个路由被交换。
接口	选择这个 RIP 过滤器要应用到的接口。

7 单击确定以将路由前缀添加到这个过滤器。

8 重复步骤 5 到 7 将路由前缀添加到这个过滤器。

添加一个邻居过滤器

您可以将一个 RIP 过滤器或者 RIP 过滤器列表设置为邻居过滤器。

1 进入 **系统 >RIP> 过滤器。**

2 根据需要添加 RIP 过滤器和 RIP 过滤器列表。

3 对于邻居过滤器，选择一个 RIP 过滤器或 RIP 过滤器列表的名称，使之成为邻居过滤器。

4 单击应用。

从邻居接收到的路由将被选定的 RIP 过滤器或 RIP 过滤器列表过滤。

添加一个路由过滤器

您可以将一个 RIP 过滤器或者 RIP 过滤器列表设置为路由过滤器。

1 进入 **系统 >RIP> 过滤器。**

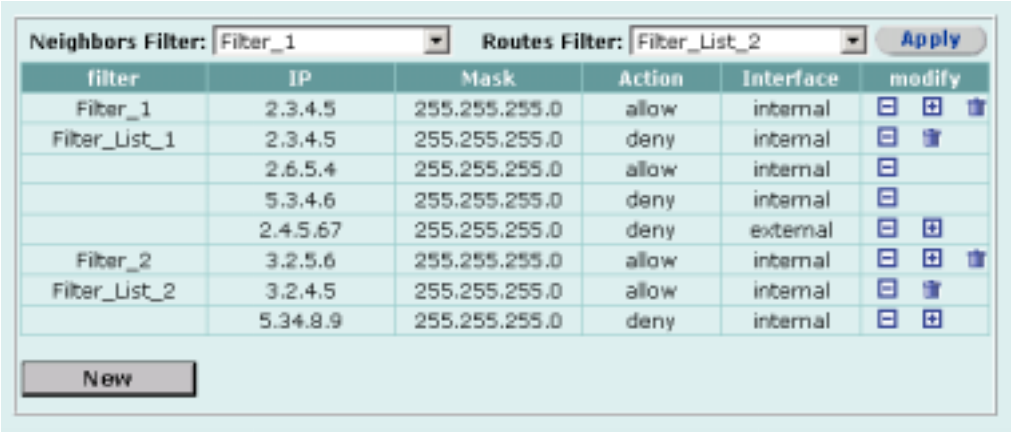
2 根据需要添加 RIP 过滤器和 RIP 过滤器列表。

3 对于路由过滤器，选择一个 RIP 过滤器或 RIP 过滤器列表的名称，使之成为路由过滤器。

4 单击应用。

FortiGate 设备发送的路由将被选定的 RIP 过滤器或 RIP 过滤器列表过滤。

图 3: RIP 过滤器配置举例



系统配置

进入 系统 > 配置 可以对 FortiGate 系统配置做以下改动：

设置系统日期和时间

为了有效地设定任务计划和记录日志，需要精确地设定 FortiGate 的时钟。您可以手工设置时间，也可以将 FortiGate 配置为自动地和一个网络时间协议 （NTP）服务器的时钟保持同步。

如欲得到关于 NTP 的更多信息或需要查找可用的 NTP 服务器，请访问 http://www.ntp.org。

按以下步骤设置日期和时钟：

1 进入 **系统 > 配置 > 时间** 。

2 单击 **刷新** 以显示 FortiGate 中的当前日期和时间。

3 从列表中选择您所在的 **时区** 。

4 如果您希望 FortiGate 系统时钟当您所在的时区调整为夏令时的时候自动调整，请单击自动调整时钟。

5 可以选择 **设置时间**，然后将 FortiGate 的日期和时间设定为当前的日期和时间。

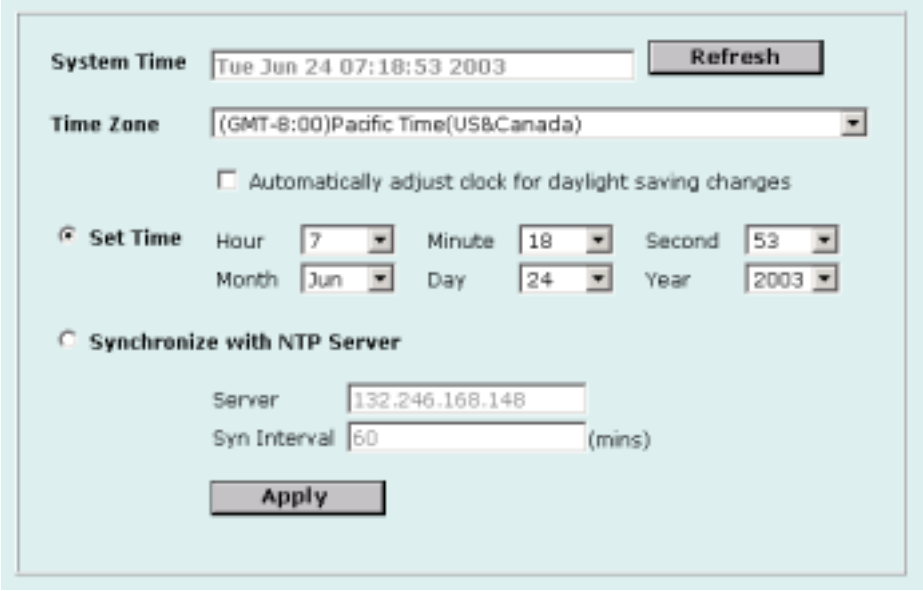
6 如果要将 FortiGate 配置为使用 NTP，选择 **与 NTP 服务器同步** 。
您可以从 www.ntp.org 站点中流览关于网络时间协议 (NTP) 的信息并选择您地区的 NTP 服务器。

7 输入 FortiGate 设备用于设置日期和时间的 **NTP 服务器的 IP 地址 或域名**。

8 指定 FortiGate 把自己的时钟同步到 NTP 服务器的 **时间间隔** 。FortiGate 每天同步它的时钟的一般的时间间隔是 1440 分钟。

9 单击 **应用** 。

图 1: 日期和时间设置的例子



更改基于基于 Web 的管理程序的选项

在 系统 > 配置 > 选项页，您可以：

- 设置系统空闲超时。
- 设置认证超时。
- 选择基于 Web 的管理程序所用的语言。
- 修改网关失效检测的设置。

您还可以要求使用控制按钮和 LCD 时先输入一个 PIN（个人识别码）。

设置系统空闲超时

1 在空闲超时栏输入以分钟为单位的数字。

2 单击应用。

设定的空闲超时时间控制着基于 Web 的管理程序在要求管理员重新登录前所经历的非活动状态的等待时间。

默认的空闲超时时间是 5 分钟。可以设置的最大空闲超时时间是 480 分钟 （8 小时）。

设置认证超时

1 在认证超时栏输入一个以分钟为单位的数字。

2 单击应用。

认证超时时间控制了防火墙在要求用户再认证前所等待的非活动时间的时间间隔。查看 第 167 页 “ 用户与认证” 以获取更多信息。

默认的认证超时时间是 15 分钟。您可以设置的最大认证超时时间是 480 分钟 （8 小时）。

选择基于 Web 的管理程序所用的语言

1 在语言列表中选择基于 Web 的管理程序使用的语言。

2 单击应用。

您可以选择英文、简体中文、日文、韩文或繁体中文。

注意：如果基于 Web 的管理程序的语言被设定为使用简体中文、日文、韩文或者繁体中文，您可以使用基于 Web 的管理程序右上角的 Englsih 按钮切换回英文。

为 LCD 控制面板设置 PIN 保护

1 单击 LCD 面板的 PIN 保护。

2 输入 6 位数的 PIN。

管理员必须输入 PIN 才能使用控制按钮和 LCD。

3 单击应用。

修改失效网关检测设置

修改失效网关检测可以控制 FortiGate 设备如何使用添加到网络接口的 ping 服务器确认连接是否有效。要在接口添加 ping 服务器，请见 。

1 在时间间隔栏，输入以秒为单位的数字以指定 FortiGate 设备测试到 ping 目标的时间间隔。

2 在失效检测栏，输入 FortiGate 设备在确认连接已经中断之前检测到的失败次数。

3 单击应用。

添加和编辑管理员帐号

在最初安装 FortiGate 时，只为它配置了一个管理员帐号。这个帐号的用户名是 admin。您可以使用这个管理员帐号再添加和编辑其它的管理员帐号。也可以控制您所添加的每个管理员帐号的访问级别。另外还可以选择限制管理员用来连接到 FortiGate 的 IP 地址。

管理员帐号可以有三种访问级别：

admin	拥有所有权限。可以查看、添加、编辑和删除管理员帐号。可以查看和修改配置。只有拥有管理级别访问权限的管理员可以进行以下操作：进入 **系统 > 状态**、手工升级固件、更新病毒防护定义库、更新攻击定义库、下载或者上载系统设置、将 FortiGate 恢复到出厂设置，重新启动 FortiGate 和关闭 FortiGate。只能有一个 **admin** 级别的用户。
读 / 写	可以查看和修改配置。可以查看但是不能添加、编辑、或者删除管理员帐号。可以修改它自己的管理员帐号密码。不能修改**系统 > 状态** 页面中的系统设置。
只读	可以查看系统配置。

添加新的管理员帐号

使用 admin 帐号按照以下步骤可以在 FortiGate 中添加新的管理员帐号和设定他们的权限：

1 进入 **系统 > 配置 > Admin**。

2 单击 **新建** 以添加新的管理员帐号。

3 输入管理员帐号登录时所用的 **用户名** 。
用户名的长度不能少于 6 个字符。用户名可以包括数字 （0-9），大写或者小写字母（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 输入并确认一次这个管理员帐号的 **密码** 。
为了提高安全性，密码的长度应当不少于 6 个字符。密码可以包括除了空格以外的任何字符。

5 可以选择是否输入受信任主机的 **IP 地址** 和 **子网掩码** 。这将限制这个管理员帐号只能从指定的位置登录到基于 Web 的管理程序上。
如果希望管理员可以从任何地方访问 FortiGate，就需把受信任主机的 IP 地址设置为 0.0.0.0，掩码设置为 0.0.0.0。
如果要限制管理员只能从指定的网络访问 FortiGate，只需要把受信任主机的地址设置为那个网络的地址，并把掩码设置为那个网络的网络掩码。例如，如果要限制管理员只能从您的内部网络访问 FortiGate，需把受信任主机的地址设置为内部网络地址（例如，192.168.1.0），把掩码设置为 255.255.255.0。

6 设置这个管理员帐号的 **访问级别**。

7 单击确定以添加这个**管理员帐号** 。

编辑管理员帐号

拥有管理权限的帐号的用户可以更改其它管理员帐号的密码，配置允许管理员帐号访问 FortiGate 基于 Web 的管理程序的 IP 地址和更改管理员帐号的权利级别。

拥有读 / 写访问权限的管理员帐号用户可以更改他们自己的帐号的密码。

按以下步骤编辑管理员帐号：

1 进入 **系统** > **配置** > **Admin**。

2 如果要改变管理员帐号的密码，单击 **修改密码**  。

3 输入 **旧的密码** 。

4 输入 **新的密码** ，然后再次 **确认新密码** 。
为了提高安全性，密码的长度应当不少于 6 个字符。密码可以包括除了空格以外的任何字符。如果您输入的密码长度少于 6 个字符，系统将显示一个警告信息，但仍会接受这个密码。

5 单击 **确定** 。

6 要编辑一个管理员帐号的设置，单击 **编辑**  。

7 （可选的）输入受信任主机的的 **IP 地址** 和 **网络掩码** ，从而允许这个管理员用来访问基于 Web 的管理程序。
如果您希望管理员可以从任何地方访问 FortiGate，就把受信任主机的 IP 地址设置为 0.0.0.0，把掩码设置为 255.255.255.255。
如果要限制管理员只能从指定的网络访问 FortiGate，只需要把受信任主机的地址设置为该网络的地址，并把掩码设置为该网络的网络掩码。例如，如果要限制管理员只能从内部网络访问 FortiGate，需把受信任主机的地址设置为您的内部网络地址 （例如，192.168.1.0），把掩码设置为 255.255.255.0。

8 如果需要的话，可以更改这个管理员帐号的 **权限级别** 。

9 单击 **确定** 。

10 如果要删除某个管理员帐号，选中要删除的帐号然后单击 **删除**  。

配置 SNMP

为 FortiGate 配置的 SNMP 可以允许运行在 FortiGate 上的 SNMP 代理报告系统信息和发送陷阱。FortiGate 中的 SNMP 代理支持 SNMP 版本 1 和 SNMP 版本 2c。RFC 支持包括 RFC1213 和 RFC2665。FortiGateSNMP 实现是只读的。服从 SNMP v1 和 v2c 的 SNMP 管理者可以只读访问 FortiGate 系统信息和接收 FortiGate 陷阱。要监视 FortiGate 系统信息和接收 FortiGate 陷阱，您必须将 Fortinet 特征 MIB 和标准 MIB 编译进 SNMP 管理器。

本节描述了以下内容：

为 SNMP 监视配置 FortiGate 设备

只有将一个或几个网络接口配置为接受 SNMP 连接之后，远程的 SNMP 管理程序才能连接到您的 FortiGate SNMP 代理。要获得这方面的更多信息，请参阅 第 109 页 “ 控制到接口的管理访问” 以及相关的网络接口配置章节。

配置 FortiGate 的 SNMP 支持

1 进入 **系统 > 配置 > SNMP v1/v2c**。

2 单击启用 SNMP。

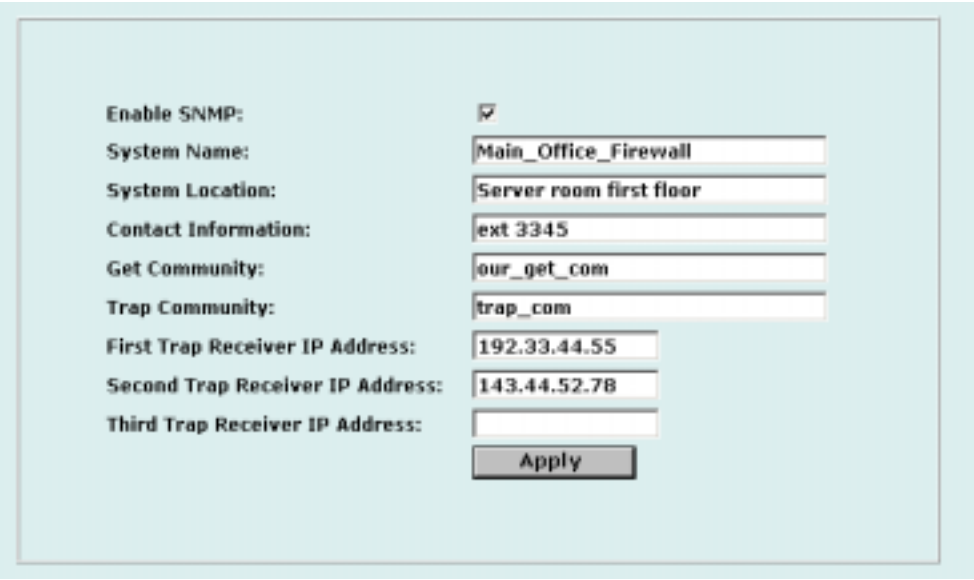
3 配置 SNMP 设置：

系统名称	自动设置 FortiGate 主机名称。要修改系统名称，请见 第 72 页 “ 修改 FortiGate 主机名” 。
系统位置	描述了 FortiGate 的物理位置。系统位置描述的长度最长为 31 个字符。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 _。空格符和 \<>[]` $ % & 等符号都不能使用。
联系信息	添加这个 FortiGate 的负责人的联系信息。联系信息的长度最长为 31 个字符。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 _。空格符和 \<>[]` $ % & 等符号都不能使用。
接受团体	也可以称做读团体。接受团体是一个用来识别发送到 FortiGate 上的 SNMP 访问请求的密码。当一个 SNMP 管理程序发送访问请求到 FortiGate 的时候，它必须包括正确的访问团体的字符串。 默认的接受团体字符串是 “public”。修改这个默认的接受团体字符串可以防止入侵者通过 SNMP 的访问请求获取您的网络配置信息。而您的 SNMP 管理程序必须使用这个接受团体字符串才能取得 FortiGate SNMP 信息。 访问团体字符串的长度最长为 31 个字符。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 _。空格符和 \<>[]` $ % & 等符号都不能使用。

陷阱团体	陷阱团体字符串类似于密码，在发送 SNMP 陷阱时被一起发送出去。 默认的陷阱团体名称字符串是 “public”。如果需要可把这个字符串改为接收您发送的陷阱消息的管理程序的名称。 陷阱团体字符串的长度最长为 31 个字符。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 _。空格符和 \<>[]` $ % & 等符号都不能使用。
陷阱接收器 IP 地址	最多可以输入三个陷阱接收器的 IP 地址，这些 IP 地址必须都在您的网络上。这些陷阱接收器被配置为接收从 FortiGate 中发出的陷阱消息。而您的 FortiGate 只向这些地址发送陷阱消息。

4 单击应用。

图 2: SNMP 配置的例子



FortiGate 管理信息库 （MIB）

FortiGate SNMP 代理支持 FortiGate 私有 MIB 也支持标准的 RFC 1213 和 RFC 2665 MIB。 表 1 中列出了 FortiGate MIB。您可以从 Fortinet 技术支持获得这些 MIB 文件。要使用 SNMP 代理通讯，必须将这些 MIB 全部编译进您的 SNMP 管理者。

您的 SNMP 管理者可能已经在一个已编译的数据库中包含了标准的和私有的 MIB，并且已经可以使用了。您必须将 Fortinet 私有 MIB 添加到这个数据库。如果 FortinetSNMP 代理使用的标准 MIB 已经被编译进了您的 SNMP 管理者，您无须再次重新编译它们。

表 1: FortiGate MIBs

MIB 文件名	描述
EtherLike.mib	以太网连接 MIB 是基于 RFC2665 的标准 MIB。这个 MIB 包含了用来管理以太网接口的信息。
FN-TRAP.mib	Fortinet 陷阱 MIB 是一个私有 MIB。您的 SNMP 管理者需要用它来接收来自 FortiGateSNMP 代理的陷阱消息。关于 FortiGate 陷阱的详细信息，请见 第 133 页 “ FortiGate 陷阱” 。
FORTINET.mib	Fortinet MIB 是一个私有 MIB，它包含了 FortiGate 系统配置的详细信息。您需要将这个 MIB 添加到您的 SNMP 管理者以监视所有的 FortiGate 配置设置。
RFC1213.mib	RFC 1213 MIB 是服从 MIB-II 标准的 MIB，它描述了用于 TCP/IP 网络的网络管理协议。

FortiGate 陷阱

FortiGate SNMP 代理最多可以向三个 SNMP 陷阱接收器发送陷阱消息。这些陷阱接收器必须是在您的网络中的并且已经配置为可接收从 FortiGate 发出的陷阱消息。为了使这些 SNMP 管理者能接收陷阱，您必须在 SNMP 管理者中加载并编译 Fortinet 陷阱 MIB。表 2 列出了 FortiGate SNMP 代理发送的陷阱。

表 2: FortiGate 陷阱

陷阱消息	描述
< 接口名称 > 接口的 IP 地址更改为 < 新 _IP> (Fortigate 序列号 : <FortiGate_ 序列号 >)	FortiGate 设备的一个网络接口的 IP 地址已经改变。陷阱消息包括改变了 IP 地址的网络接口的名称，该接口的新 IP 地址和 FortiGate 设备的序列号。当接口被配置为使用 DHCP 或 PPPoE 设置动态 IP 地址时，这个陷阱可以用于跟踪接口 IP 地址的改变。
系统关闭	FortiGate 设备关闭。
代理关闭	一个管理者已经禁用了 SNMP 代理。当代理在系统关闭前停止服务时也会发送这个陷阱。
冷启动	FortiGate 设备启动或重新启动。一个管理者启用了 SNMP 代理或者修改了 FortiGateSNMP 设置。当代理在系统启动过程中启动的时候会发送这个陷阱。
认证失败	一个 SNMP 管理者团体字符串与 FortiGate 接受团体字符串不匹配。

定制替换信息

FortiGate 设备在通过它的内容流中用替换信息替换以下内容：

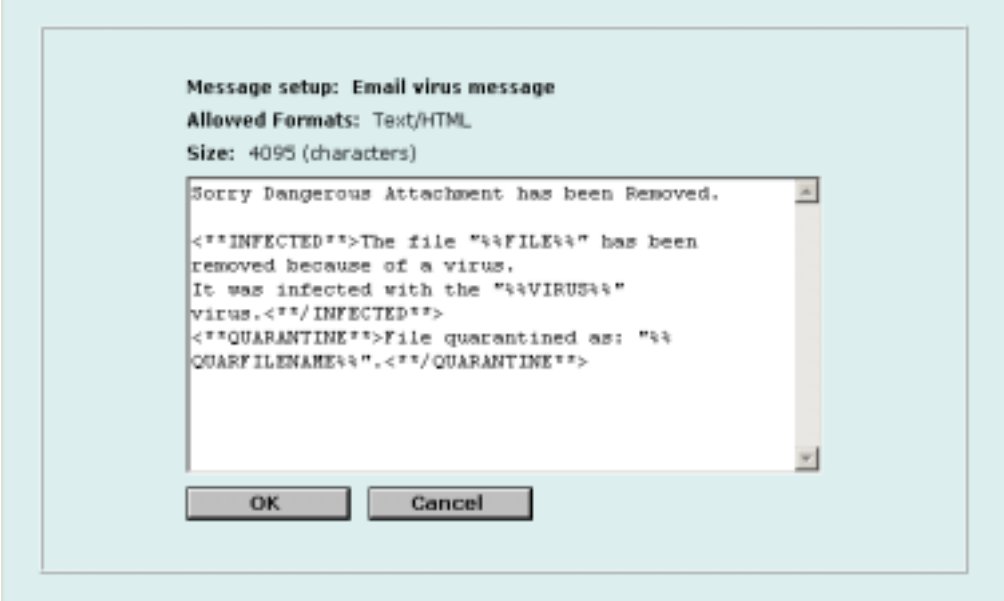
- 被病毒防护系统从电子邮件中删除的文件或其他内容
- 被病毒防护系统或网页过滤器从 HTTP 下载数据中删除的文件或其他内容
- 被病毒防护系统从 FTP 下载数据中删除的文件

您可以编辑替换信息以控制最终用户看到的替换信息的内容。

您还可以编辑添加到报警邮件信息的内容，以控制在报告病毒入侵、NIDS 事件、紧急系统事件和硬盘满事件的报警邮件中的信息。

本节描述了以下内容：

图 3: 替换信息的例子



定制替换信息

替换信息列表中的每个替换信息由不同的几个部分组成。您可以利用这些部分的组合创建您自己的替换信息。

您可以编辑替换信息列表中的任何替换信息，并且可以根据需要添加替换信息片段。

1 进入 **系统 > 配置 > 替换信息。**

2 对于您要定制的替换信息单击修改 。

3 在消息设置对话框，编辑这个消息的内容。

表 3 列出了可以添加到替换信息的替换信息片段和每个片段的标签书写格式。对于每个合法的标签您可以添加任何文字。对于电子邮件和 HTTP 消息您还可以添加 HTML 编码。

4 单击确定以保存您所做的修改。

表 3: 替换信息片段

文件阻塞	用于阻塞文件 （所有服务）。	
片段开始	<**BLOCKED**>	
允许的标签	%%FILE%%	这个名字的文件被阻塞。
	%%URL%%	被阻塞的网页页面的 URL。
片段结束	<**/BLOCKED**>	

表 3：替换信息片段

扫描	用于病毒扫描 （所有服务）。	
片段开始	<**INFECTED**>	
允许的标签	%%FILE%%	被感染的文件的文件名。
	%%VIRUS%%	感染文件的病毒名称。
	%%URL%%	被阻塞的网页页面或文件的 URL。
片段结束	<**/BLOCKED**>	

隔离	当隔离功能被启用时使用。（可以被电子邮件的阻塞服务和所有的扫描服务使用。）	
片段开始	<**QUARANTINE**>	
允许的标签	%%QUARFILENAME%%	被隔离的文件的文件名。
片段结束	<**/QUARANTINE**>	

定制报警邮件

定制报警邮件可以控制发送给系统管理员的报警邮件的内容。

1 进入 **系统 > 配置 > 替换信息。**

2 对于您要定制的报警邮件信息，单击修改  。

3 在消息设置对话框，编辑消息的文本。

表 4 列出了可以添加到报警邮件的替换信息片段和每个片段的标签的书写方法。对于合法的标签您还可以添加任何文字和 HTML 编码。

4 单击确定以保存您所做的任何修改。

表 4：报警邮件消息的片段

NIDS 事件	用于 NIDS 事件报警邮件。	
片段开始	<**NIDS_EVENT**>	
允许的标签	%%NIDS_EVENT%%	NIDS 攻击消息。
片段结束	<**/NIDS_EVENT**>	

病毒警报	用于病毒警报邮件消息	
片段开始	<**VIRUS_ALERT**>	
允许的标签	%%VIRUS%%	病毒名称。
	%%PROTOCOL%%	检测到病毒的服务。
	%%SOURCE_IP%%	接收到病毒所来自的 IP 地址。对于电子邮件，这个 IP 地址是发送包含病毒的电子邮件的邮件服务器的地址。对于 HTTP 协议数据流这是发送病毒的网页的 IP 地址。
	%%DEST_IP%%	会接收到病毒的计算机的 IP 地址。对于 POP3 协议这是试图下载含有病毒的电子邮件的用户的计算机的 IP 地址。
	%%EMAIL_FROM%%	发现带有病毒的消息的发件人的邮件地址。
	%%EMAIL_TO%%	发现被病毒感染的消息的收件人的邮件地址。

表 4：报警邮件消息的片段（续）

阻塞事件	用于文件阻塞报警邮件消息	
片段开始	<**BLOCK_ALERT**>	
允许的标签	%%FILE%%	
	%%PROTOCOL%%	被阻塞的文件所用的服务。
	%%SOURCE_IP%%	接收被阻塞的文件时的源 IP 地址。对于电子邮件，这个 IP 地址是发送包含了被阻塞的文件的电子邮件的邮件服务器的地址。对于 HTTP，它是发送被阻塞的文件的网页页面的 IP 地址。
	%%DEST_IP%%	要接收被阻塞的文件的计算机的 IP 地址。对于电子邮件这个 IP 地址是试图下载含有被感染了的病毒的消息的用户计算机的 IP 地址。
	%%EMAIL_FROM%%	含有被阻塞的文件的消息的发件人的邮件地址。
	%%EMAIL_TO%%	含有被阻塞的文件的消息的收件人的邮件地址。

紧急事件	用于紧急防火墙报警邮件。	
片段开始	<**CRITICAL_EVENT**>	
允许的标签	%%CRITICAL_EVENT%%	防火墙紧急事件消息。
片段结束	<**/CRITICAL_EVENT**>	

防火墙配置

防火墙策略控制着所有通过 FortiGate 设备的通讯。防火墙策略是 FortiGate 设备用来决定如何处理一个连接请求的一系列指令。当防火墙收到一个数据包内的连接请求时，它提取出这个数据包的源地址、目的地址和服务 （端口号）进行分析。

对于要通过 FortiGate 设备传输的数据包，必须在 FortiGate 设备上添加一个与该数据包源地址、目的地址和服务相匹配的防火墙策略。这个策略指导防火墙如何处理这个数据包。处理方式可以是允许连接、拒绝连接、在连接前要求认证，或将数据包作为 IPSec VPN 包处理。您还可以在策略中添加任务计划使得防火墙可以在每天不同时间、一周、月或年中的不同日子用不同的方式处理连接。

每个策略都可以单独地配置为路由连接或应用网络地址转换 （NAT）以转换源地址、目的地址和端口。您可以添加 IP 池使防火墙转换源地址的时候使用动态 NAT。您可以使用策略配置通过 FortiGate 的端口地址转换 （PAT）。

您可以在策略中添加内容配置文件，从而获得对网页、文件传输和电子邮件服务的防病毒保护、网页过滤和电子邮件过滤。您可以创建由下面动作之一或任意组合的功能的内容配置文件：

- 在 HTTP, FTP, SMTP, IMAP, 或 POP3 服务中应用防病毒保护。
- 隔离已经被病毒感染或可能被病毒感染了的文件。
- 对 HTTP 服务应用网页过滤。
- 对 IMAP 和 POP3 服务应用电子邮件过滤。

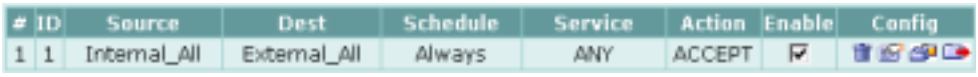
您也可以对防火墙策略添加日志记录，从而使 FortiGate 设备记录所有使用此策略的连接。

本章描述了以下内容：

默认防火墙配置

防火墙策略控制接口之间的连接。默认情况下，您内部网络中的用户可以通过 FortiGate 设备连接到互联网。防火墙阻塞其他所有的连接。防火墙被配置为用一条默认策略匹配从内部网络上收到的所有的连接请求。这条策略指示防火墙将这些连接转发到互联网上。

图 4: 默认防火墙策略



- 地址
- 服务
- 任务计划
- 内容配置文件

地址

添加策略可以控制 FortiGate 接口之间的连接和到这些接口的网络之间的连接。要添加接口之间的策略，这个接口必须包含地址。默认情况下 FortiGate 设备配置了以下防火墙地址：

- 内部 _ 全部，添加到内部接口，这个地址匹配于内部网络上的全部地址。
- 外部 _ 全部，添加到外部接口，这个地址与外部网络中的全部地址匹配。
- DMZ_ 全部，添加到 DMZ 接口。这个地址匹配于 DMZ 网络中的全部地址。

防火墙使用这些地址匹配防火墙接收到的数据包的源地址和目的地址。默认的策略匹配从内部网络来的全部连接，因为它包含了内部 _ 全部 地址。默认策略也匹配到外部网络的全部连接，因为它包含了 外部 _ 全部 地址。

您可以在每个接口上添加更多的地址以增强对通过防火墙的连接的控制能力。关于防火墙地址的详细信息，请见 第 145 页 “ 地址” 。

如果 DMZ/HA 接口配置为 HA 模式，您不能为 DMZ/HA 接口添加地址或为这个接口配置防火墙策略。

您也可以添加提供网络地址转换 （NAT）功能的防火墙策略。要使用 NAT 转换目的地址，必须添加虚拟 IP。虚拟 IP 将一个网络中的地址映射到另一个网络中的被转换的地址上。关于虚拟 IP 的详细信息请见 第 155 页 “ 虚拟 IP” 。

服务

防火墙策略也可以根据数据包的服务或目的端口来控制连接。默认的策略接受使用任何服务或目的端口的连接。防火墙配置中包含了 40 多个预定义的服务。您可以将这些服务添加到策略中以提高对使用这些服务通过防火墙的连接的控制能力。您也可以添加用户自定义的服务。关于服务的详细信息，请见 第 148 页 “ 服务” 。

任务计划

策略也可以根据防火墙收到的连接在一天当中的时间或一周中的日子来控制连接。默认的策略可以在任何时间接受连接。防火墙配置中包括了一个在任何时间接受连接的任务计划。您可以添加更多的任务计划以控制策略生效的时间。关于任务计划的详细信息，请见 第 152 页 “ 任务计划” 。

内容配置文件

内容配置文件可以添加到策略中以应用对网页、文件传输和电子邮件服务的防病毒保护、网页内容过滤和电子邮件过滤。FortiGate 设备包括了以下默认的内容配置文件：

- 严谨： 对 HTTP, FTP, IMAP, POP3, 和 SMTP 内容通讯应用最大程度的内容保护。
- 扫描： 对 HTTP, FTP, IMAP, POP3, 和 SMTP 内容通讯应用防病毒扫描。
- 网页： 对 HTTP 内容通讯应用防病毒扫描和网页内容阻塞。
- 不过滤： 允许超大型的文件不经过防病毒扫描直接通过 FortiGate 设备。

关于内容配置文件的详细信息，请见 第 163 页 “ 内容配置文件” 。

添加防火墙策略

添加防火墙策略可以控制 FortiGate 接口之间的连接和通讯。

1 进入 **防火墙 > 策略。**

2 选择您要添加策略的策略 列表。

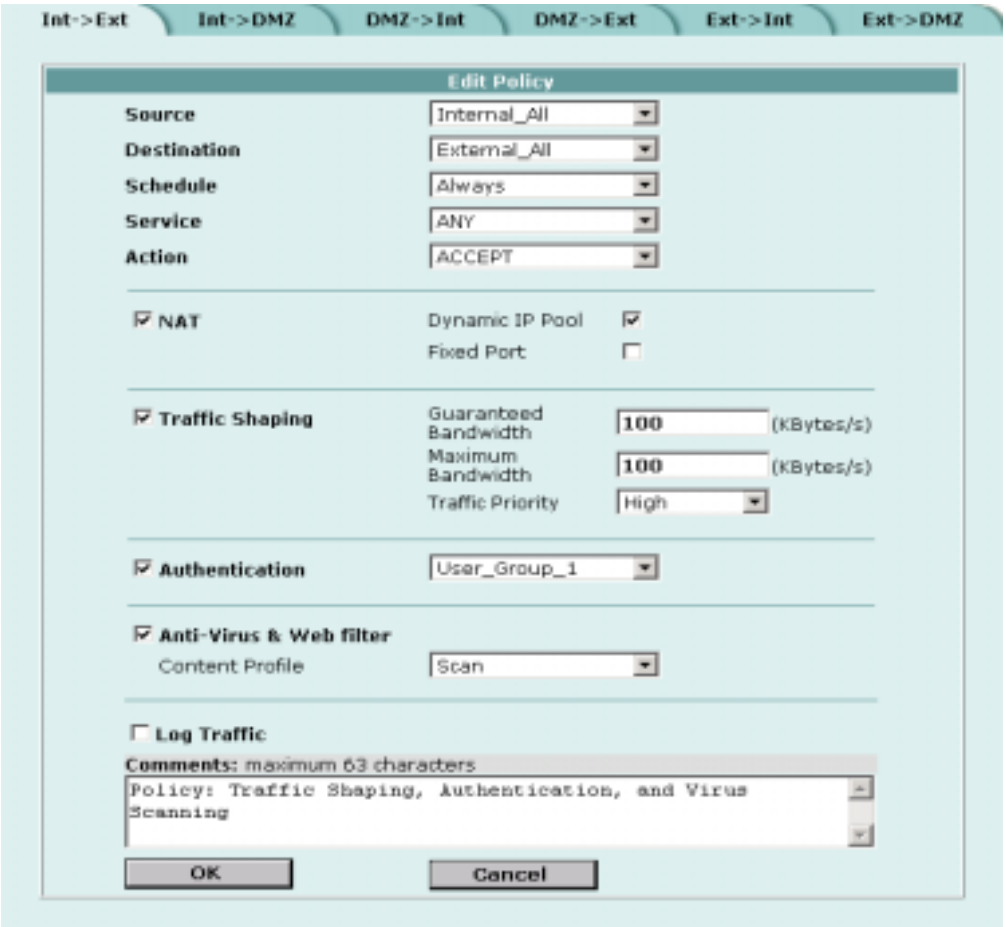
3 单击新建以添加一个新的策略。
也可以在策略列表中的一条策略前面单击在策略前面插入  ，在这个策略的上面添加一条新策略。

4 配置这个策略：
关于策略选项的详细信息请见 第 140 页 “ 防火墙策略选项” 。

5 单击 **确定** 以添加这条策略。

6 重新安排策略在策略列表中的位置以达到您所期望的效果。
关于策略在策略列表中的排列在 第 143 页 “ 配置策略列表” 有详细描述。

图 5: 添加 NAT/ 路由策略



防火墙策略选项

本节叙述了您可以在防火墙策略中设置的选项。

源地址

选择与数据包源地址匹配的地址或地址组。在您把这个地址添加到策略之前，必须先把它添加到源网络接口上。关于添加地址，见 第 145 页 “ 地址” 。

目的地址

选择与数据包目的地址匹配的地址或者地址组。在您把这个地址添加到策略之前，必须先把它添加到目的网络接口上。关于添加地址，请参阅 第 145 页 “ 地址” 。

NAT 模式下的策略，目的网络上的地址是源网络中使用 NAT 隐藏的地址。目的地址还可以是一个虚拟 IP 地址，它将数据包的目的地址映射到一个隐藏的目的地址。请见 第 155 页 “ 虚拟 IP” 。

任务计划

选择任务计划可以控制策略生效和用于匹配连接的时间，见 第 152 页 “ 任务计划” 。

服务

选择一个服务与数据包的服务 （端口）相对应。您可以从大量的预定义服务中选择，或者添加自己定制的服务类型和服务组。 见 第 148 页 “ 服务” 。

动作

选择当策略与连接尝试相匹配时防火墙的响应方式。

接受	接受连接。如果您选择接受，可以配置这个策略的 NAT 和认证选项。
拒绝	拒绝连接。在这种情况下您唯一能配置的其他选项就是记录日志。记录日志选项 将此策略拒绝的连接记录到日志中。
加密	把这个策略设置为 IPSec VPN 策略。如果选择了 加密，可以为这个策略选择一个自动密钥交换的 VPN 通道或者一个手工密钥的 VPN 通道，并配置其它 IPSec 设置。您不能为加密策略设置认证。并且加密在透明模式下不可用。请见 第 188 页 “ 配置加密策略” 。

NAT

配置策略的 NAT 选项。NAT 把策略接收到的数据包的源地址和源端口进行转换。如果您选择了 NAT，您还可以选择一个动态 IP 池和一个固定的端口。NAT 在透明模式下不可用。

动态 IP 池	如果外部接口被配置为使用 DHCP 或 PPPoE，您不能为内部 -> 外部或 DMZ-> 外部型的策略选择动态 IP 池。 选择动态 IP 池可以将源地址转换为从此策略添加到目的接口的 IP 池中随机选择的一个地址。要添加 IP 池，请见 第 158 页 “ IP 池” 。
固定端口	选择固定端口可以防止 NAT 转换源端口。如果源端口改变了，有些应用程序将无法工作。如果选择了固定端口，必须也选择动态 IP 池并为策略的目的网络接口上添加一个动态 IP 池的地址范围。如果没有选择动态 IP 池，使用固定端口的策略一次只允许一个连接使用某个端口的服务。

VPN 通道

为加密策略选择 VPN 通道。可以选择一个自动密钥交换的 VPN 通道或者手工密钥交换的 VPN 通道。VPN 通道在透明模式下不可用。

允许向内	选择**允许向内** 可以使远程 VPN 网关后面的用户能够连接到策略的源地址上。
允许向外	选择**允许向外** 可以使用户能够连接到远程 VPN 网关后面的目的地址上。
向内 NAT	选择**向内 NAT** 可以把向内传输的数据包的源地址转换为 FortiGate 的内部 IP 地址。
向外 NAT	选择**向外 NAT** 可以把向外发送的数据包的源地址转换为 FortiGate 的外部 IP 地址。

流量控制

流量控制功能控制可以使用的带宽并设置被策略处理的数据流的优先权。在大量的数据通过 FortiGate 时，流量控制可以控制哪个策略具有更高的优先权。例如，为网页服务器设定的策略可能被分配比大多数为雇员电脑设定的策略更高的优先级。当一个雇员需要非同寻常的对互联网的高速访问的时候，可以为他设置一个具有较高带宽的特定的向外连接策略。

如果设置保证带宽和最大带宽均为 0，策略将拒绝所有流通流量。

保证带宽 使用 **流量控制**可以保证策略允许经过防火墙的通讯享有一定的带宽。 保证带宽（以 kbps 为单位）确保对优先级高的服务有足够的带宽可用。

最大带宽 您还可以使用 **流量控制** 限制某个策略经过防火墙的带宽的限度。限制带宽可以限制重要程度较低的服务使用更为重要的服务所需要带宽。

数据流优先级 可以选择高、中、低。选择**数据流优先级**可以使 FortiGate 管理不同类型的数据流的优先权关系。例如，连接到一个安全的网页服务器的策略用于支持电子商务通讯，应当被分配给一个较高的优先权。而对于重要程度较低的服务应当标上较低的优先权。只有当高优先级的连接不再需要带宽时，防火墙才会将带宽分配给低优先级的连接。

认证

选择认证并选择一个用户组可以要求用户在防火墙接受连接请求之前输入用户名和密码。选择用户组可以控制哪些用户可以通过认证使用这个策略。要添加和配置一个用户组，见 第 172 页 “ 配置用户组” 。您必须在选择认证之前添加用户组。

您可以选择对任何服务的认证。用户可以在防火墙上使用 HTTP、Telnet 或者 FTP 认证。为了让用户能够认证，必须添加为认证配置的 HTTP、Telnet 或者 FTP 策略。当用户试图通过防火墙使用这个策略连接时，他们将会被提示输入防火墙用户的用户名和密码。

如果您希望用户在使用其它服务时认证 （例如，POP3 或者 IMAP），可以创建一个包含了您想要进行认证的服务和 HTTP、Telnet 或 FTP 服务的服务组。用户可以在使用这个策略的其它服务之前先使用 HTTP、Telnet 或 FPT 认证。

在大多数情况下，您必须确定用户无须认证就可以通过防火墙使用 DNS。如果 DNS 不可用，用户将无法使用域名访问网页服务、FTP 或者 Telnet 服务。

病毒防护与 Web 过滤器

启用防病毒保护和网页内容过滤功能可以过滤由这个策略控制的通讯。如果服务类型是 任意、HTTP、SMTP、POP3 或者 IMAP，或者是一个包含了 HTTP、SMTP、POP3 或 IMAP 的服务组，您可以选择病毒防护和网页过滤。

选择一个内容配置文件以配置应用到这个策略的防病毒保护和内容过滤功能。请见 第 163 页 “ 内容配置文件” 。

图 6: 添加透明模式策略

记录流通日志

选择记录流通日志可以在策略处理一个连接的时候向日志写入一条消息。关于记录日志的详细信息请见 第 245 页 “ 日志和报告” 。

注释

可以选择添加一个关于这个策略的描述或者其他信息。注释的长度最多可以到 63 个字符，包括空格。

配置策略列表

防火墙从策略列表的顶端向下搜索匹配的策略，直到找到第一个匹配的策略为止。您必须把策略列表中的策略按照从特殊到一般的顺序排列。

例如，默认策略是非常一般的策略，因为它匹配所有的连接尝试。当创建这个策略的一个例外策略时，必须把这些例外的策略添加到默认策略的上方。任何在默认策略下面的策略都永远不会被匹配到。

本节讨论了以下内容：

- 策略匹配的细节
- 更改策略列表中策略的顺序
- 启用和禁用策略

策略匹配的细节

当 FortiGate 从网络接口上收到一个连接请求时，它首先要选择一个策略列表，在这个策略列表中查找与这个连接请求匹配的策略。FortiGate 根据连接请求的源地址和目的地址决定使用哪个策略列表。

随后 FortiGate 从选定的策略列表的顶端开始向下搜索策略列表，查找第一个与连接请求的源地址、目的地址、服务端口以及接收到连接请求的日期和时间相匹配的策略。匹配的第一个策略将被应用于连接。如果没有找到匹配的策略，连接将被丢弃。

默认的策略接受所有的从内部网络到互联网的连接请求。用户可以从内部网络浏览网页、使用 POP3 接收邮件、使用 FTP 通过 FortiGate 下载文件等等。如果 默认的策略在内部 -> 外部策略列表的顶端，防火墙将允许全部从内部网络到互联网的连接，因为所有的连接都和默认策略匹配。如果有其他特殊策略被添加到了策略列表并处在默认策略的下方，他们永远也不会被匹配。

对于默认策略的例外策略，例如，一个阻塞 FTP 连接的策略，必须在内部 -> 外部策略列表中位于默认策略的上方。在这个例子中，所有来自内部网络的 FTP 连接尝试都与这个 FTP 策略匹配，于是被阻塞。而其它类型服务的连接请求将不会被这个 FTP 策略所匹配，但是它们能够匹配默认策略。于是，防火墙仍然接受来自内部网络的所有其它连接。

注意：需要认证的策略必须添加到策略列表中不需认证的策略的前面。否则，不需要认证的策略将先被匹配。

更改策略列表中策略的顺序

1 进入 **防火墙 > 策略**。

2 选择所要重新排序的策略列表的标签。

3 选择要移动的策略然后单击 **移动**  以改变这个策略在策略列表中的位置。

4 在 **移动到** 一栏输入一个数字以指定这个策略要移动到策略列表中的位置，单击 **确定**。

启用和禁用策略

您可以启用和禁用策略列表中的策略以控制这个策略是否生效。FortiGate 匹配已被启用了的策略，而不匹配被禁用的策略。

禁用一个策略

禁用一个策略可以暂时防止防火墙试图匹配这个策略。禁用一个策略不会中断当前由这个策略建立的通讯会话。要中断活动的会话，请见 第 86 页 “ 系统状态” 。

1 进入 **防火墙 > 策略**。

2 选择含有要禁用的策略的策略列表的标签。

3 清除要禁用的策略的选中标志。

启用一个策略

启用一个被禁用了的策略可以使防火墙继续用这个策略匹配连接：

1 进入 **防火墙 > 策略**。

2 选择含有要启用的策略的策略列表的标签。

3 选中要启用的策略的选中标志。

地址

所有的策略都需要配置源地址和目的地址。要为两个接口之间的策略添加地址，您必须先把这些地址添加到每个接口的地址列表中去。

您可以根据需要添加、编辑和删除全部的防火墙地址。您也可以将相关的地址编入地址组以简化创建的策略。

- 一个防火墙地址由一个 IP 地址和一个网络掩码构成。这一信息可以描述为：
- 子网的地址 （例如，对于一个 C 类子网，IP 地址：192.168.20.0 和网络掩码：255.255.255.0）。
- 一个单独的 IP 地址 （例如，IP 地址：192.168.20.1 和网络掩码：255.255.255.255）
- 全部可能的 IP 地址 （表示方式为 IP 地址：0.0.0.0 和网络掩码：0.0.0.0）。

注意：IP 地址：0.0.0.0 和网络掩码： 255.255.255.255 不是有效的防火墙地址。

本节叙述了如下内容：

添加地址

按如下步骤添加一个地址

1 进入 **防火墙 > 地址**。

2 选择要添加地址的接口。

3 单击新建以添加新的地址。

4 输入一个 地址名 以识别这个地址。
这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

5 输入这个 IP 地址。

这个 IP 地址可以是：

- 单个电脑的 IP 地址 （例如，192.45.46.45）。
- 一个子网的地址 （例如，一个 C 类子网 192.168.1.0）。
- 0.0.0.0 来表示全部可能的 IP 地址。

6 输入子网掩码。

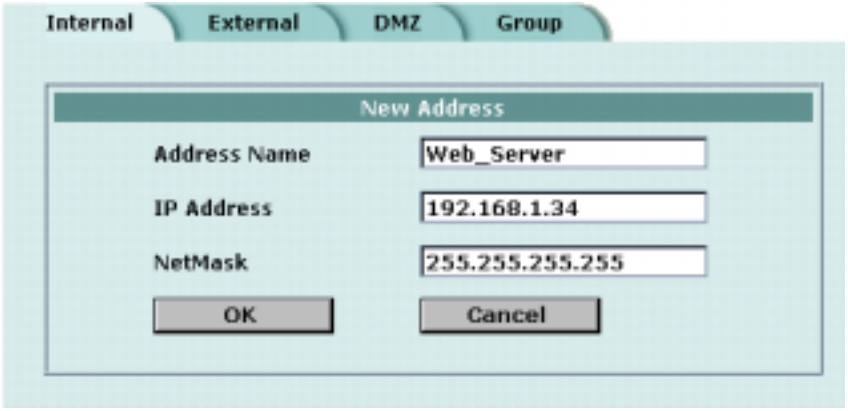
子网掩码应当对应于所添加的 IP 地址的类型。例如：

- 对于单个主机的 IP 地址的子网掩码应当是 255.255.255.255。
- A 类子网的子网掩码应该是 255.0.0.0。
- B 类子网的子网掩码应该是 255.255.0.0。
- C 类子网的子网掩码应该是 255.255.255.0。
- 全部地址的网络掩码应当是 0.0.0.0。

注意：要添加一个地址以表示在一个网络中的任意地址，可以将 IP 地址设置为 0.0.0.0，并将网络掩码设置为 0.0.0.0。

7 单击确定以保存地址。

图 7: 添加内部地址



编辑地址

可以编辑一个地址，修改它的 IP 地址和子网掩码。您不能修改一个地址的名称。如果需要修改一个地址的名字，您必须删除这个地址然后用一个新的名字来添加它。

1 进入 **防火墙 > 地址**。

2 选择包含了您所要编辑的那个地址的列表。

3 选择要编辑的地址，单击编辑地址 。

4 完成所需的改动，单击 **确定** 以保存您所做的修改。

删除地址

删除一个地址可以把此地址移出地址列表。一旦地址被删除了，这个地址就不能再添加到策略中。要删除一个已经添加到策略的地址，必须先把它从那个策略中删除。

1 进入 **防火墙 > 地址**。

2 选择含有您要删除的地址的列表。
您可以删除被列出的地址中带有 **删除标志**  的任何地址。

3 选择要删除的地址，单击 **删除**  。

4 单击 **确定** 以删除地址。

将地址编入地址组

您可以把相关的地址编入一个地址组，这样便于以后添加到策略。例如，如果添加三个地址并将其添加到一个地址组，您只需要为这个地址组创建一个策略，而不用去为三个地址创建三个单独的策略。

您可以把地址组添加到任何网络接口中。地址组只能包含已经添加到这个网络接口的地址。地址组可以用于网络接口的源地址或者目的地址列表。

地址组的名字不能和独立地址相同。如果一个地址组已经被加到一个策略中了，就不能删除它，除非先从这个策略中删除这个地址组。

1 进入 **防火墙 > 地址 > 组**。

2 选择要添加地址组的接口。

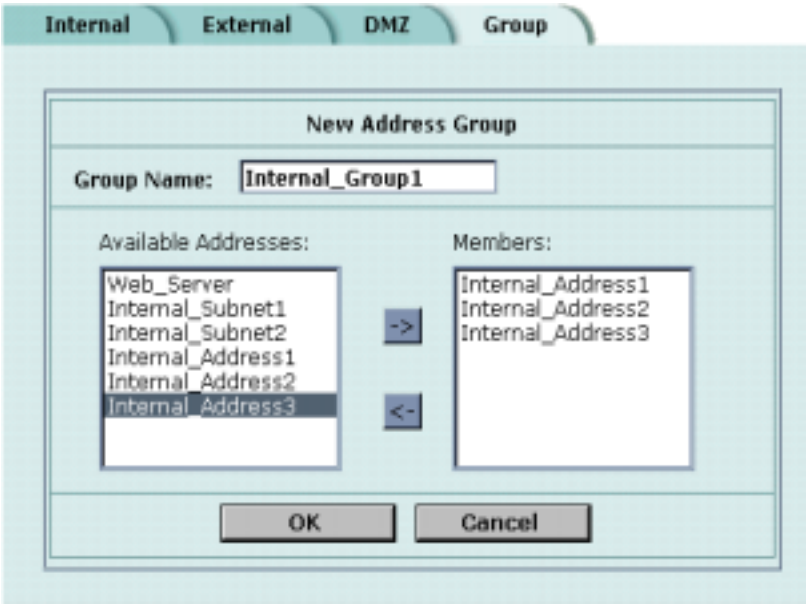
3 输入一个**地址组名** 以标识这个地址组。
这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 要把 **地址** 添加到这个地址组，从有效地址列表中选择一个地址，然后单击向右箭头把它添加到成员列表中。

5 要从地址组中删除地址，从成员列表中选择要删除的地址，然后单击向左箭头把它从这个组中删除。

6 单击 **确定** 以添加这个地址组。

图 8: 添加一个内部地址组。



服务

使用服务可以控制防火墙接受或者拒绝的流通类型。可以为一个策略添加任何预定义的服务。也可以创建您自己定制的服务然后把服务添加到服务组中去

本节叙述了以下内容：

- 预定义的服务
- 访问定制服务
- 服务分组

预定义的服务

FortiGate 预定义服务在表 5 中列出。您可以将这些服务添加到任何策略中。

表 5: FortiGate 预定义的服务

服务名称	内容	协议	端口
任意	可以在任何端口匹配连接。使用任何预定义服务的连接都可以通过防火墙。	全部	全部
GRE	通用路由封装。通过把协议的数据包封装为 GRE 数据包的方式，允许任意一个网络协议通过任意一个另外的网络协议传输的协议。		47
AH	认证头。AH 提供安全主机认证和数据验证，但是不加密。这个协议用于设置为积极模式的 IPSec 远程网关的认证。		51

表 5: FortiGate 预定义的服务（续）

服务名称	内容	协议	端口
ESP	封装安全有效载荷。这个服务用于自动密钥交换的 VPN 通道和手工密钥 VPN 通道，以传输加密的数据。自动密钥交换 VPN 通道在使用 IKE 建立连接之后使用 ESP 传输数据。		50
AOL	AOL 即时消息协议。	tcp	5190-5194
BGP	边界网关协议路由协议。BGP 是一个内部 / 外部路由协议。	tcp	179
DHCP- 中继	DHCP 中继协议。	udp	67
DNS	域名解析服务，用于查找域名对应的 IP 地址。	tcp	53
		udp	53
FINGER	Finger 服务。	tcp	79
FTP	FTP 文件传输协议。	tcp	21
GOPHER	Gopher 通讯服务。	tcp	70
H323	H.323 多媒体协议。H.323 是由国际电信联盟（ITU）核准的标准，它定义了通过网络进行视频会议数据传输的标准。	tcp	1720, 1503
HTTP	HTTP 是用于万维网的网页数据传输的协议。	tcp	80
HTTPS	使用安全数据包层面的 HTTP 服务，用于 WEB 服务器的安全通讯。	tcp	443
IKE	IKE 是用来使用 IPSEC 的 ISAKMP 获得原始认证密钥的协议。	udp	500
IMAP	互联网消息访问协议 （IMAP）是用于接收邮件消息的协议。	tcp	143
互联网定位服务	互联网定位协议包括 LDAP、用户定位服务和 TLS/SSL 上的 LDAP。	tcp	389
IRC	互联网聊天中继允许人们连接到互联网并加入聊天组。	tcp	6660-6669
L2TP	L2TP 是一个用于远程访问的基于 PPP 的通道协议。	tcp	1701
LDAP	轻型目录访问协议是用于访问信息目录的一组协议。	tcp	389
NetMeeting	网络会议允许用户将互联网作为传输介质进行远程电信会议。	tcp	1720
NFS	网络文件系统允许网络用户访问存贮在不同类型的计算机上的共享文件。	tcp	111, 2049
NNTP	网络新闻传输协议是一个用于张贴、发布和接收 USENET 消息的协议。	tcp	119
NTP	网络时间协议用于将计算机的时钟与时间服务器同步。	tcp	123
OSPF	开放最短路径优先路由协议。OSPF 是一个公共连接状态路由协议。		89
PC-Anywhere	PC-Anywhere 是一个远程控制和文件传输协议。	udp	5632
PING	数据包互联网探索是一个用来判断是否可以通过特定主机的 IP 地址进行访问的工具。	icmp	8
POP3	POP3 邮件协议用于从 POP3 服务器上下载邮件。	tcp	110

表 5: FortiGate 预定义的服务（续）

服务名称	内容	协议	端口
PPTP	点对点通道协议是一个允许组织结构通过公共网络上的私有通道拓展他们自己的网络的协议。	tcp	1723
QUAKE	流行的多人电脑游戏 Quake 的连接协议。	udp	26000, 27000, 27910, 27960
RAUDIO	用于实时多媒体音频流传输。	udp	7070
RLOGIN	用于远程登录到服务器的 Rlogin 服务。	tcp	513
RIP	路由信息协议是一个公共距离向量路由协议。	udp	520
SMTP	用于在互联网上的电子邮件服务器之间发送邮件。	tcp	25
SNMP	简单网络管理协议是用于管理复杂网络的一组协议。	tcp	161-162
		udp	161-162
SSH	用于安全连接到一台电脑进行远程管理的 SSH 服务。	tcp	22
		udp	22
SYSLOG	用于远程记录日志的系统日志服务。	udp	514
TALK	一种支持两个或多个用户之间交谈的协议。	udp	517-518
TCP	全部 TCP 端口。	tcp	0-65535
TELNET	连接到远程电脑运行命令的 Telnet 服务。	tcp	23
TFTP	微型文件传输协议，一个比 FTP 更简单的文件传输协议，没有安全功能。	udp	69
UDP	全部的 UPD 端口。	udp	0-65535
UUCP	UNIX 到 UNIX 文件拷贝协议。一个简单的文件复制协议。	udp	540
VDOLIVE	用于 VDO Live 多媒体数据流通讯。	tcp	7000-7010
WAIS	广域信息服务器。一种互联网搜索协议。	tcp	210
WINFRAME	两台运行 Windows NT 的电脑之间 WinFrame 通讯的协议。	tcp	1494
X-WINDOWS	在 X-Windows 服务器和 X-Windows 客户之间远程通讯的协议。	tcp	6000-6063

访问定制服务

如果需要创建一个含有不包括在预定义服务列表中的服务的策略，可以添加一个定制的服务。

1 进入 **防火墙 > 服务 > 定制**。

2 单击 **新建** 。

3 输入服务的**名字** 。当您添加一个新的策略时，这个名字将出现在服务列表中。

这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 选择服务使用的 **协议** （可以是 TCP 或者 UDP）。

5 通过输入 **最高端口号** 和 **最低端口号** ，为这个协议指定一个源端口和一个目的端口号的范围。如果服务仅使用一个端口，就在最高和最低端口号上输入相同的数字。

6 如果这个服务有多于一个的 **端口地址范围** ，选择 **添加** 以指定附加的协议和端口范围。

如果错误地添加了太多的端口地址范围，可以单击 **删除** 删除多余的行。

7 单击 **确定** 以添加这个定制服务。

现在您可以把这个服务添加到策略中了。

服务分组

为了便于添加策略，可以创建服务组，然后添加一个接受或者阻塞此组中的全部服务的策略。一个服务组可以包括预定义服务和定制服务并以任何方式将其组合。您不能把一个服务添加到其它服务组里。

1 进入 **防火墙 > 服务 > 组**。

2 单击 **新建** 。

3 输入一个用于识别这个组的 **组名**。

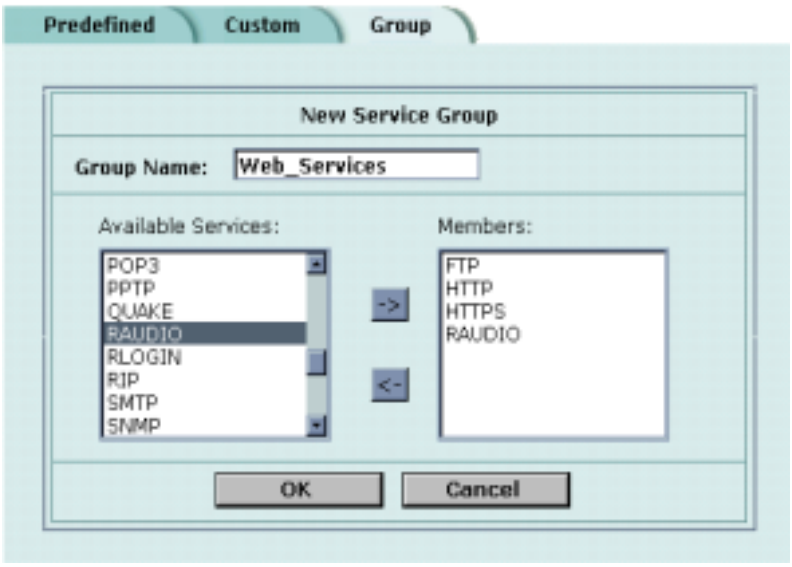
当添加策略的时候，这个名字将出现在服务列表中。这个名字不能和预定义服务相同。这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 要向服务组中 **添加服务**，从可用服务列表中选择服务，然后单击向右箭头把服务复制到成员列表中。

5 要从服务组中 **删除服务**，从成员列表中选择要删除的服务，单击向左箭头把它从这个组中删除。

6 单击 **确定** 以保存这个服务组。

图 9: 添加服务组



任务计划

任务计划用来控制策略生效和无效的时间。可以创建一次性的任务计划和周期性的任务计划。您可以使用一次性的任务计划创建策略，这个策略只在任务计划指定的时间段内有效。周期性的任务计划不断地重复生效；可以使用周期性任务计划创建策略，这个策略只在每天的特定时间或者每周的特定日期生效。

本节叙述了以下内容：

创建一个一次性任务计划

可以创建一个一次性任务计划用于在特定的时间内激活策略或者解除对策略的激活。例如，您的防火墙可能被配置为默认的 内部到外部 策略，它允许在任何时间从内部网络访问互联网上的任何服务。您可以添加一个一次性任务计划以阻止在节日期间对互联网的访问。

1 进入 **防火墙 > 任务计划 > 一次性**。

2 单击 **新建** 。

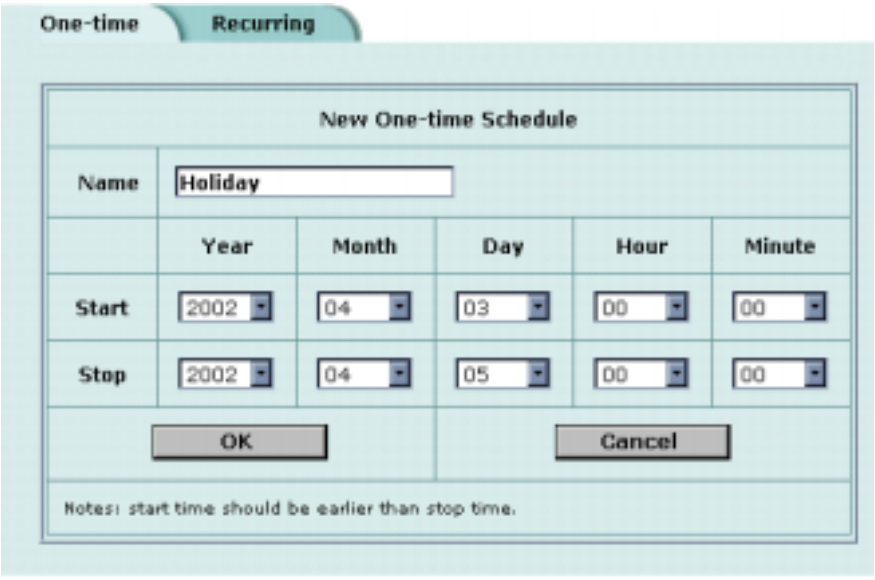
3 输入一个任务计划任务计划的 **名称**。
这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 输入任务计划的 **开始日期** 和 **时间** 。
如果需要任务计划在一整天中都有效，就把开始和结束时间都设置为 00。

5 设置任务计划的 **结束日期** 和 **时间** 。
一次性任务计划使用 24 小时制。

6 单击 **确定** 以保存任务计划。

图 10: 添加一次性任务计划任务计划



创建周期性任务计划

可以创建一个周期性的任务计划在每天的特定时间或者每周的特定天数里激活策略或者取消对策略的激活。例如，您可能需要创建一个任务计划阻止在工作时间以外的时间里访问互联网。

如果创建了一个结束时间在开始时间之前的周期性任务计划，这个任务计划将于您所设置的开始时间开始，并于第二天的结束时间终止。您可以使用这种方法创建一个周期性任务计划让它从第一天运行到第二天。也可以创建一个 24 小时运行的周期性任务计划，只需要把它的开始时间和结束时间设置成相同的时间既可。

1 进入 **防火墙 > 任务计划 > 周期性**。

2 单击 **新建** 以添加新的任务计划。

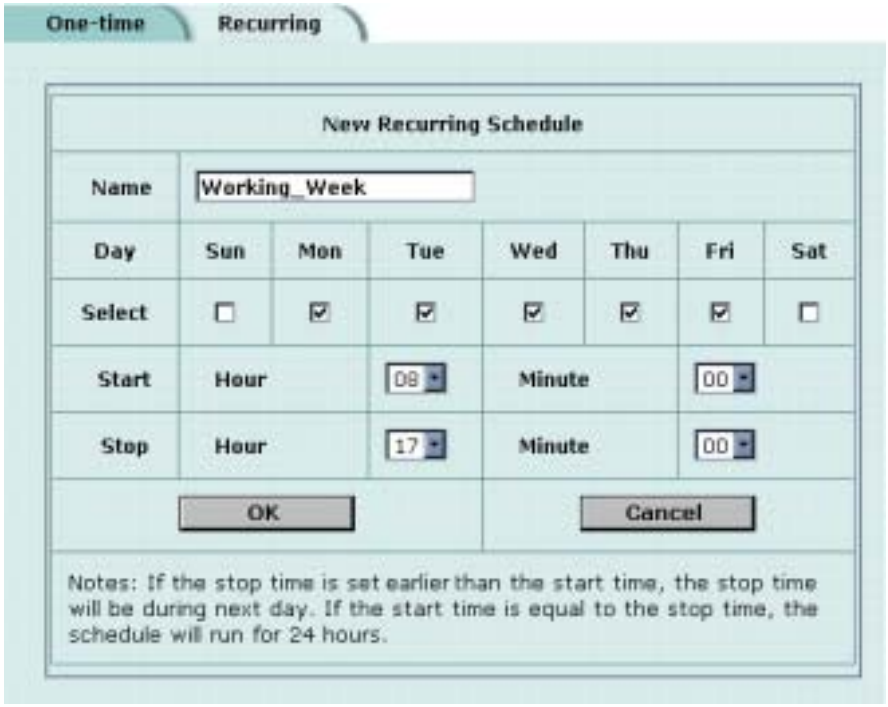
3 输入任务计划的 **名称** 。
这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 选择在一周里任务计划生效的 **日期** 。

5 设置 **开始时间** 和 **结束时间** ，在这段时间里任务计划是激活的。
周期性任务计划使用 24 小时制的时间表示法。

6 单击 **确定** 以保存周期性任务计划。

图 11: 添加周期性任务计划



在策略中添加一个任务计划

在创建一个任务计划之后，您可以把它添加到策略中，以控制策略生效的时间。在创建策略的时候，可以在策略中添加新的任务计划，或者可以编辑现有的策略，向其添加一个新的任务计划。

1 进入 **防火墙 > 策略**。

2 选择要添加的策略类型对应的标签。

3 单击 **新建** 以添加新的策略，或者单击 **编辑** 以编辑一个策略，改变它的运行时间。

4 根据需要配置策略。

5 从任务计划列表中选择要添加的 **任务计划** 。

6 单击 **确定** 以保存策略。

7 安排这个策略在策略列表中的顺序，以达到预期的效果。

例如，使用一个一次性任务计划来拒绝对一个策略的访问，可以添加一个与这个策略相匹配的新策略来拒绝任何访问，并选择您所添加的一次性任务计划，把动作方式设置为拒绝。然后把这个包含一次性任务计划的策略放到策略列表中要被拒绝的策略的上方。

虚拟 IP

NAT 模式的安全策略可以对较不安全的网络隐藏较安全的网络中的地址。要允许从一个较不安全的网络连接到一个较安全的网络中的某个地址上，您必须创建一个从较不安全的网络中的地址到较安全的网络中的地址的映射。这个映射称为虚拟 IP。

例如，如果在您的 DMZ 网络中有一台提供 Web 服务的电脑，它可以使用一个诸如 10.10.10.3 的私有 IP。为了让互联网内的数据包能够达到网页服务器，您必须为网页服务器提供一个互联网上的外部地址。然后需要添加一个虚拟 IP 地址把 Web 服务器的外部地址映射到位于 DMZ 网络中的 Web 服务器的真实地址上。为了允许从互联网到网页服务器的连接，必须添加一个外部 ->DMZ 的防火墙策略并把目的地址设置为这个虚拟 IP。

您可以创建两种类型的虚拟 IP：

静态 NAT	用于把源网络中的地址转换成目的网络中的隐藏的地址。静态 NAT 把返回的数据包的源地址转换为源网络中的地址。
端口转发	把一个源网络中的地址和端口号转换成一个目的网络中的隐藏的地址，并且可以选择是否使用不同的端口号。使用端口转发功能，您还可以路由发往特定端口和目的地址上的，与接收数据包的网络接口相匹配的数据包。这个技术叫做端口转发或者端口地址转换 （PAT）。也可以使用端口转发功能改变被转发的数据包的目的端口。

本节讨论了以下内容：

添加静态 NAT 虚拟 IP

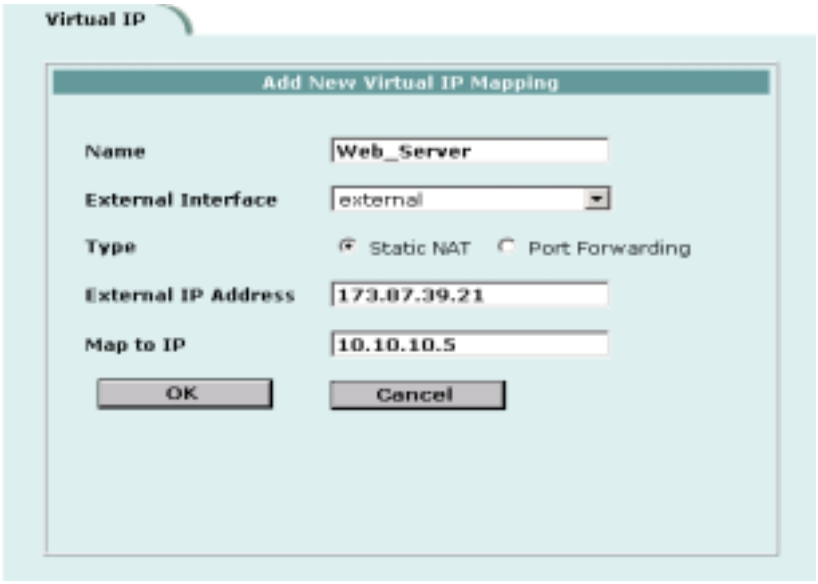
1. 进入 **防火墙 > 虚拟 IP**。
2. 单击 **新建** 以添加一个虚拟 IP。
3. 输入虚拟 IP 的**名称**。
   这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。
4. 选择这个虚拟 IP 的外部网络接口。
   外部接口是安全程度较低的区域中的网络接口。它接收数据包，并转发到安全程度较高的区域中。
5. 确保类型被设置为 **静态 NAT**。
6. 在 **外部 IP 地址** 一栏，输入影射到网络中的地址的那个外部 IP 地址。
   例如，如果虚拟 IP 提供了从互联网到 DMZ 网络或者内部网络上的一台 Web 服务器的访问，那么外部 IP 地址应当是从您的 ISP 那里获得的一个为 Web 服务器准备的静态 IP 地址。这个地址必须是唯一的，不能被其它主机使用，也不能跟步骤 4 中选择的外部网络接口的地址相同。而且，这个地址必须是可以在这个网络接口中路由的。
   如果在步骤 4 中选择的外部接口的 IP 地址被设置为使用 PPPoE 或 DHCP，您可以在外部 IP 地址中输入 0.0.0.0。FortiGate 设备使用 PPPoE 或 DHCP 替换这个接口的 IP 地址设置。
7. 在 **映射到 IP** 栏，输入在目的网络中的真实 IP。例如，您的内部网络中的 Web 服务器的 IP 地址。

注意：防火墙把从主机向外发出的数据包的源地址从被映射的 IP 地址转换为外部的虚拟 IP 地址，而不是防火墙的地址。

8 单击 **确定** 以保存虚拟 IP 地址。

您现在可以把这个虚拟 IP 地址添加到防火墙的策略中了。

图 12: 添加静态 NAT 虚拟 IP



添加端口转发虚拟 IP

1 进入 **防火墙 > 虚拟 IP**。

2 单击 **新建** 以添加新的虚拟 IP。

3 输入虚拟 IP 的 **名称** 。

这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

4 选择虚拟 IP 外部接口。 外部接口是接收转发到目的网络的数据包的源网络的接口。

5 修改端口转发的类型。

6 在外部 IP 地址一栏，输入被影射到目的区域的地址上的外部地址。

您可以将外部地址设置为在步骤 4 中选择的外部接口的地址或者其他任何地址。

如果在步骤 4 中选择的外部接口的 IP 地址被设置为使用 PPPoE 或 DHCP，您可以在外部 IP 地址中输入 0.0.0.0。FortiGate 设备使用 PPPoE 或 DHCP 替换这个接口的 IP 地址设置。

例如，如果虚拟 IP 提供了从互联网到您内部网络上的一台服务器的访问，那么此外部地址必须是由您的 ISP 分配给这个服务器的一个静态的 IP 地址。这个地址必须是唯一的一个地址，不能用于网络上的其它主机，而且这个地址必须是可以被步骤 4 中选定的外部网络接口路由的。

7 输入为端口转发配置的 **外部的服务端口号**。

外部设备端口号必须与数据包要转发到的目的地址的端口号相匹配。例如，如果虚拟 IP 地址提供了一个从互联网到您内部网络或者 DMZ 网络上的网页服务器的访问，那么外部的服务端口拷应当是 80 （即 HTTP 端口）。

8 在 **映射 IP 地址** 一栏中，需要输入在目的网络上的 **真实 IP 地址** 。

例如，真实 IP 地址可以是位于您的内部网络中的 Web 服务器的地址。

如果您输入的是和内部接口在同一子网内的一个 IP 地址，虚拟 IP 可以被添加到外部 -> 内部 >，或 DMZ-> 内部类型的策略中去。

如果您输入的是和 DMZ 接口在同一子网内的 IP 地址，虚拟 IP 可以被添加到外部 ->DMZ 类型的策略中去。

9 把 **映射到端口** 设置为转发数据包时要给它们添加的端口号。

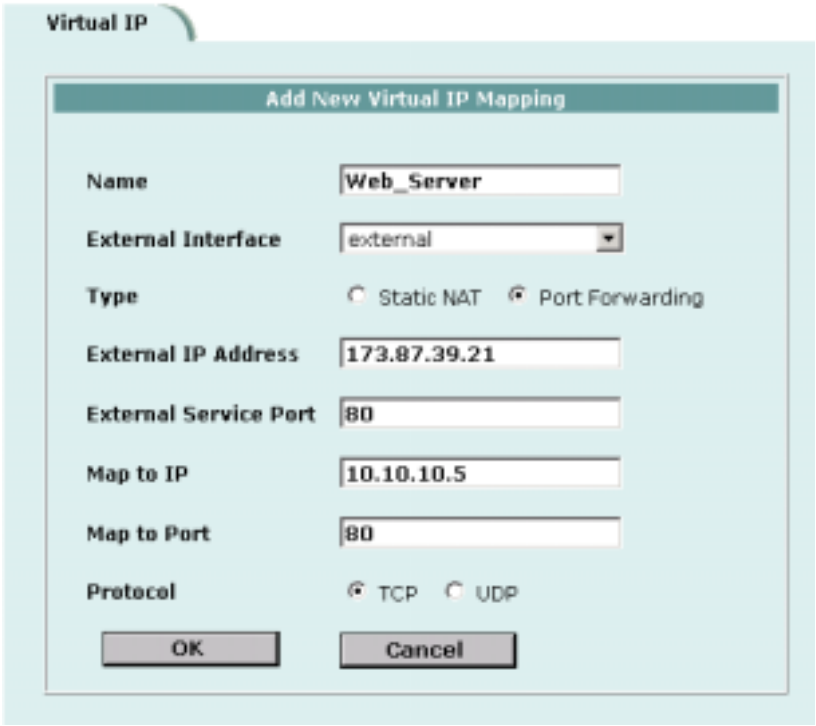
如果您不希望转换端口，可以输入和外部服务端口相同的端口号。

如果您希望转换端口，输入要转换到的目的端口的端口号，当数据包被防火墙转发时，它们的目的端口将被按照这个号码被修改。

10 选择被转发的端口所要使用的 **协议**。

11 单击 **确定** 以保存端口转发虚拟 IP。

图 13: 添加端口转发虚拟 IP



添加使用虚拟 IP 的策略

按照如下步骤添加使用虚拟 IP 转发数据包的策略。

1 进入 **防火墙 > 策略**。

2 选择要添加的策略的 **类型** ：

- 源接口必须匹配于外部接口列表中选中的接口。
- 目的区域必须匹配于映射到的 IP 地址所在网络相连接的接口。

3 使用以下信息配置策略。

源地址	选择用户可以用来访问服务器的**源地址**。
目的地址	选择虚拟 IP。
任务计划	根据需要选择**任务计划**。
服务	选择的服务应当对应于您选择的端口转发虚拟 IP 所映射到的**服务**。
动作	将 **动作** 设置为 **接受**以接受到内部网络服务器的连接。也可以选择**拒绝**以拒绝对服务器的访问。
NAT	如果防火墙对于源地址网络隐藏了目的网络上的私有地址，则选择 NAT。
认证	可选项。选择**认证**并选择一个用户组可以要求用户在使用端口转发访问服务器的时候先取得防火墙的认证。
记录流通日志 **病毒防护与 Web 过滤器**	可以选中此项启用对端口转发的数据流记录日志，并启用对数据流应用防病毒保护、Web 内容过滤功能。

4 单击 **确定** 以保存这个策略。

IP 池

一个 IP 池 （也称做动态 IP 池）是一个添加到防火墙网络接口的 IP 地址范围。如果您为一个接口添加了 IP 池，当配置一个其目的地址设为此接口的策略时可以选择动态 IP 池。如果您希望添加一个 NAT 模式的策略，以将源地址转换为从 IP 池中随机选择的地址，而不仅仅是使用目的接口的地址，您也可以添加一个 IP 池。

例如，如果您将一个 IP 池添加到了内部接口，您可以为外部 -> 内部和 DMZ-> 内部策略选择动态 IP 池。

IP 池中的地址必须和此网络接口的 IP 地址在同一子网内。例如，如果一个 FortiGate 网络接口是 192.168.1.99，那么一个有效的 IP 池可以是从 192.168.1.10 到 192.168.1.20 的 IP 地址。这个 IP 池可以为防火墙提供 11 个可选的 IP 地址，供防火墙在转换源地址时候使用。

IP 池地址范围中的地址不能和所添加到的那个网络接口位于同一网络中的其它地址冲突。

您可以在任何接口上添加多个 IP 池，但是只有 IP 池被防火墙使用。

本节描述了以下内容：

添加 IP 池

以下操作用于添加 IP 池：

1 进入 **防火墙 > IP 池**。

2 选择要添加 IP 池的 **网络接口** 。

3 单击 **新建** 以将新的 IP 池添加到选中的网络接口。

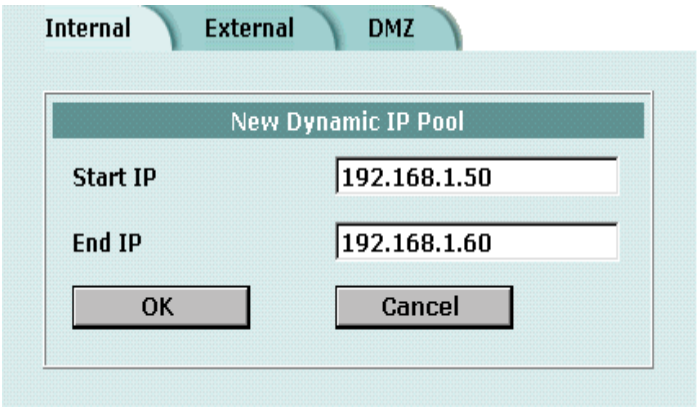
4 输入这个 IP 池的地址范围的 **起点 IP 地址** 和 **终点 IP 地址** 。

这个起点 IP 和终点 IP 须用来定义 IP 池的 IP 地址范围的起止点地址。其中，起点 IP 地址必须小于终点 IP 地址。起点 IP 地址和终点 IP 地址必须有相同的子网地址，并且都 IP 地址池添加到的那个网络接口所在的子网内。

如果您已经将外部接口配置为使用 PPPoE 或者 DHCP，您只能将起点 IP 地址和终点 IP 地址设置为外部接口当前的 IP 地址。

5 单击 **确定** 以保存这个 IP 池。

图 14: 添加一个 IP 池



使用固定端口的防火墙策略的 IP 池

如果一个 NAT 防火墙策略转换连接所使用的数据报的源端口，有些网络配置就无法正常工作。NAT 通过转换源端口来跟踪特定服务的连接。您可以为 NAT 策略选择固定的端口以防止源端口转换。然而，选择固定端口意味着这个服务只有一个连接可以通过防火墙。为了支持多个连接，您可以为目的接口添加一个 IP 池，然后在这个策略中选择动态 IP 池。防火墙将从 IP 池中随机选择 IP 地址并将它们分配给每个连接。在这种情况下防火墙能够支持的连接的数量仅仅受这个 IP 池中 IP 地址数量的限制。

IP 池和动态 NAT

您可以在动态 NAT 中使用 IP 池。例如，您所在的机构可能购买了某个地址范围内的 IP 地址，但是您可能只有一个到互联网的连接：您的 FortiGate 设备的外部接口。

您可以为您的 FortiGate 设备的外部接口指定一个您所在的机构购买的互联网 IP 地址。如果您的 FortiGate 设备运行在 NAT/ 路由模式，所有从您的网络到互联网的连接看起来都来自于这个地址。

如果您希望这些连接来自于您所有的互联网 IP 地址，可以将这个 IP 地址范围设置成一个 IP 地址池添加到外部接口。然后可以为所有以外部接口作为目的接口的策略设置动态 IP 池。防火墙对于每个连接动态地从 IP 池中选择一个 IP 地址作为连接的源地址。结果是到互联网的那些连接看起来似乎来源于这个 IP 池中的全部地址。

IP/MAC 绑定

IP/MAC 绑定可以保护 FortiGate 和您的网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到 FortiGate 或者通过 FortiGate。这个电脑的 IP 地址可以轻易地改变为受信任的地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

您可以在静态 IP/MAC 地址表中输入可信的电脑的静态 IP 地址和对应的 MAC 地址。

如果您有一台受信任的主机，它使用的是 FortiGate DHCP 服务器设置的动态 IP 地址，FortiGate 设备会将这些 IP 地址和它们对应的 MAC 地址添加到动态 IP/MAC 表。请见 第 116 页 “ 在您的内部网络中提供 DHCP 服务” 。动态 IP/MAC 绑定列表在透明模式下不可用。

IP/MAC 绑定可以应用于连接到防火墙的数据包或者穿过防火墙的数据包。

注意：在您启用了 IP/MAC 绑定后，如果您修改了一台电脑的 IP 地址或者 MAC 地址，且此 IP 地址和 MAC 地址已经在 IP/MAC 绑定列表中，则您必须同时修改 IP/MAC 列表中的相应的条目。否则这台电脑将无法访问 FortiGate 或者通过 FortiGate。您必须为网络中的新增的电脑在 IP/MAC 地址列表中添加 IP/MAC 地址对，否则这台新添加到您的网络中的电脑也无法访问 FortiGate 或者通过 FortiGate。

本节讨论了以下内容：

为穿过防火墙的数据包配置 IP/MAC 绑定

对匹配于防火墙策略，可以使用防火墙策略穿越防火墙的数据包，使用以下操作可以对它进行 IP/MAC 绑定过滤。

1 进入 **防火墙 > IP/MAC 绑定 > 设置** 。

2 选择 **启用经过防火墙的 IP/MAC 地址绑定** 。

3 进入 **防火墙 > IP/MAC 绑定 > 静态 IP/MAC**。

4 单击 **新建** 在 IP/MAC 地址绑定列表中添加新的 IP/MAC 地址绑定对。

所有能够正常地匹配策略并通过防火墙的数据包将首先和 IP/MAC 地址绑定列表中的条目比较，如果能够发现匹配的条目，防火墙将试图把这个数据包同策略相匹配。

例如，如果 IP 地址为 1.1.1.1 和 MAC 地址为 12:34:56:78:90:ab:cd 的 IP/MAC 地址对已经添加到 IP/MAC 地址绑定列表了：

- 一个 IP 地址为 1.1.1.1 ，MAC 地址为 12:34:56:78:90:ab:cd 的数据包将被允许到策略列表中搜索匹配的策略。
- 一个 IP 地址为 1.1.1.1， 但是使用了不同 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击。
- 一个使用了不同 IP 地址但是 MAC 地址是 12:34:56:78:90:ab:cd 的数据包也将被丢弃以防止 IP 欺骗。
- 如果这个数据包的 IP 地址和 MAC 地址在 IP/MAC 地址绑定列表都没有定义：
  - 如果 IP/MAC 绑定被设置为 **允许流通**，则允许它继续去匹配防火墙的策略。
  - 如果 IP/AMC 绑定被设置为 **阻塞流通**，那么数据包将被阻塞。

为连接到防火墙的数据包配置 IP/MAC 绑定

对于可以正常连接到防火墙的数据包 （例如，管理员连接到 FortiGate 以进行管理的时候），通过以下操作可以使用 IP/MAC 地址绑定对数据包进行过滤。

1 进入**防火墙 > IP/MAC 绑定 > 设置**。

2 选择**启用到防火墙的 IP/MAC 绑**定。

3 进入**防火墙 > IP/MAC 绑定 > 静态 IP/MAC**。

4 单击新建在 IP/MAC 地址列表中添加新的 IP/MAC 地址绑定对。

所有能正常连接到防火墙的数据包都将首先在 IP/MAC 绑定列表中查找匹配的 IP/MAC 地址对。

例如，如果 IP 地址为 1.1.1.1 和 MAC 地址为 12:34:56:78:90:ab:cd 的 IP/MAC 地址对已经添加到 IP/MAC 地址绑定列表了：

- 一个 IP 地址为 1.1.1.1 ，MAC 地址为 12:34:56:78:90:ab:cd 的数据包将被允许连接到防火墙
- 一个 IP 地址为 1.1.1.1， 但是使用了不同 MAC 地址的数据包将立即被丢弃，以防止 IP 欺骗攻击。
- 一个使用了不同 IP 地址但是 MAC 地址是 12:34:56:78:90:ab:cd 的数据包也将被丢弃以防止 IP 欺骗。
- 如果这个数据包的 IP 地址和 MAC 地址在 IP/MAC 地址绑定列表都没有定义：
  - 如果 IP/MAC 绑定被设置为允许流通，则允许它连接到防火墙。
  - 如果 IP/AMC 绑定被设置为阻塞流通，那么数据包将被阻塞。

添加 IP/MAC 地址

1 进入**防火墙 > IP/MAC 绑定 > 静态 IP/MAC**。

2 单击**新建**以添加 IP 地址 /MAC 地址对。

3 输入 IP 地址和对应的 MAC 地址。

可以在同一个 MAC 地址上绑定多个 IP 地址。但是不能把多个 MAC 地址绑定到同一个 IP 地址上。

然而，您可以为多个 MAC 地址设置 IP 地址为 0.0.0.0 的绑定。这意味着来自这些地址的所有数据包都可以匹配 IP/MAC 地址绑定列表。

类似地，您也可以为多个 IP 地址设置 MAC 地址为 00:00:00:00:00:00 的 IP 地址绑定。这意味着所有来自这些 IP 地址的数据包都可以匹配 IP/MAC 地址绑定列表。

4 为新的 IP/MAC 地址绑定对输入一个名字。
这个名字可以包含数字 （0-9），大写或者小写字母 （A-Z，a-z），以及特殊字符 - 和 _。不允许使用其它特殊字符和空格符。

5 选择启用以启用这个 IP/MAC 地址对的 IP/MAC 地址绑定。

6 单击确定以保存这个 IP/MAC 地址对。

查看动态 IP/MAC 列表

1 进入 **防火墙 > IP/MAC 绑定 > 动态 IP/MAC**。

启用 IP/MAC 地址绑定

警告：确保您在启用 IP/MAC 绑定之前已经添加了您的管理员电脑的 IP/MAC 地址对。

1 进入**防火墙 > IP/MAC 绑定 > 设置**。

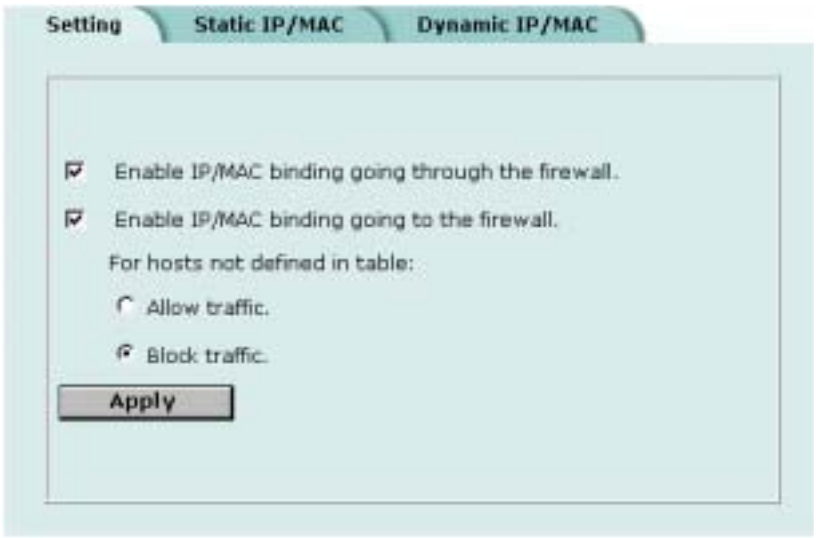
2 选择启用通过防火墙的 IP/MAC 绑定可以启用对匹配防火墙策略的数据包的 IP/MAC 地址绑定。

3 选择启用到防火墙的 IP/MAC 绑定可以启用对连接到 FortiGate 的数据包的 IP/MAC 地址绑定。

4 配置 IP/MAC 地址绑定如何处理在 IP/MAC 地址列表中没有定义 IP 和 MAC 地址的数据包：
选择允许流通可以允许所有具有不在 IP/MAC 地址列表中的 IP/MAC 地址对的数据包通过。
选择阻塞流通可以阻塞所有具有不在 IP/MAC 地址列表中的 IP/MAC 地址对的数据包通过。

5 单击应用以保存您所做的修改。

图 15: IP/MAC 设置



内容配置文件

使用内容配置文件可以对防火墙策略控制的内容通讯应用不同的保护设置。您可以使用内容配置文件完成以下任务：

- 为 HTTP, FTP, POP3, SMTP, 和 IMAP 策略配置防病毒保护
- 为 HTTP 策略配置网页过滤
- 为 IMAP 和 POP3 策略配置电子邮件过滤
- 为 HTTP, FTP, POP3, SMTP, 和 IMAP 策略配置超大型邮件过滤
- 为 POP3, SMTP, 和 IMAP 策略配置邮件片段传输

您可以使用内容配置文件建立对不同类型的防火墙策略都易于配置的保护配置方式。这就使得您可以为不同的防火墙策略定制不同类型和不同级别的保护。

例如，内部和外部地址之间的通讯可能需要严格的保护，内部地址之间的通讯可能仅仅需要中等的保护。您可以使用相同或不同的内容配置文件为不同的通讯服务的策略进行配置。

内容配置文件可以添加到 NAT/ 路由模式或透明模式策略。

默认的内容配置文件

FortiGate 设备具有以下四种默认的内容配置文件，它们位于防火墙 > 内容配置文件。 您可以使用现有的内容配置文件或者创建您自己的：

严谨	使用严谨的内容配置文件可以对 UHTTP, FTP, IMAP, POP3, 和 SMTP 等通讯的内容应用最大限度的防护。通常情况下您不需要使用严谨型内容配置文件，但是如果您受到病毒的严重威胁，需要最大限度地屏蔽病毒，可以选择严谨型内容配置文件。
扫描	使用扫描型内容配置文件可以对 HTTP、FTP、IMAP、POP3 和 SMTP 通讯的内容应用防病毒扫描。同时，隔离功能也被启用了，并适用于所有类型的服务。在 FortiGate 设备中装备了一个硬盘，如果防病毒扫描功能发现了在某个文件中有病毒，这个文件可以被隔离到 FortiGate 的硬盘上。系统管理员可以根据需要决定是否恢复被隔离的文件。
网页	使用网页型内容配置文件可以对 HTTP 通讯的内容应用防病毒扫描和网页内容阻塞。您可以在控制 HTTP 通讯的防火墙策略中添加这一内容配置文件。
非过滤	如果您不希望对通讯内容施加任何内容保护，可以选择非过滤型内容配置文件。您可以在控制无须保护的通讯类型的防火墙策略上添加这一内容配置文件，例如两个高度可信或高度安全的网络之间的通讯。

添加一个内容配置文件

如果默认的内容配置文件不能提供您所要求的保护，您可以创建新的内容配置文件并根据您的需要定制它的内容。

1 进入 **防火墙 > 内容配置文件。**

2 单击新建。

3 输入一个配置文件名。

4 启用防病毒保护选项。

防病毒扫描 扫描网页，FTP 和邮件通讯中的病毒和蠕虫。请见 第 224 页 “ 防病毒扫描” 。

文件阻塞 删除与文件阻塞样板匹配的文件，即使它们不包含病毒。只有发现了新的，防病毒扫描功能无法检测的病毒时，您才有必要启用这一功能。请见 第 225 页 “ 文件阻塞” 。

隔离 隔离被阻塞和被感染的文件。

注意：如果防病毒扫描和文件阻塞功能都启用了，FortiGate 设备将在文件被扫描病毒之前阻塞与文件模板匹配的文件。

5 启用网页过滤选项。

网页 URL 阻塞 阻塞不受欢迎的网页和网站。这个选项将 Fortinet URL 阻塞（请见 第 233 页 “ 阻塞对 URL 的访问”）和 Cerberian URL 过滤（请见 第 235 页 “ 使用 Cerberian 网页过滤器”）添加到策略接受的 HTTP 通讯中。

网页内容阻塞 阻塞包含不受欢迎的词汇或短语的网页。请见 第 232 页 “ 内容阻塞” 。

网页脚本过滤 从网页中删除脚本。请见 第 238 页 “ 脚本过滤” 。

网页排除列表 从网页过滤和病毒扫描中排除 URL。请见 第 239 页 “ URL 排除列表” 。

6 启用电子邮件过滤保护选项。

电子邮件阻塞列表 对来自不受欢迎的地址的邮件添加主题标签。请见 第 242 页 “ 电子邮件阻塞列表” 。

电子邮件排除列表 从电子邮件过滤中排除某些发件人地址模板。请见 第 243 页 “ 邮件排除列表” 。

电子邮件内容阻塞 对包含不受欢迎的词汇活短语的电子邮件 添加主题标签。请见 第 241 页 “ 电子邮件禁忌词汇列表” 。

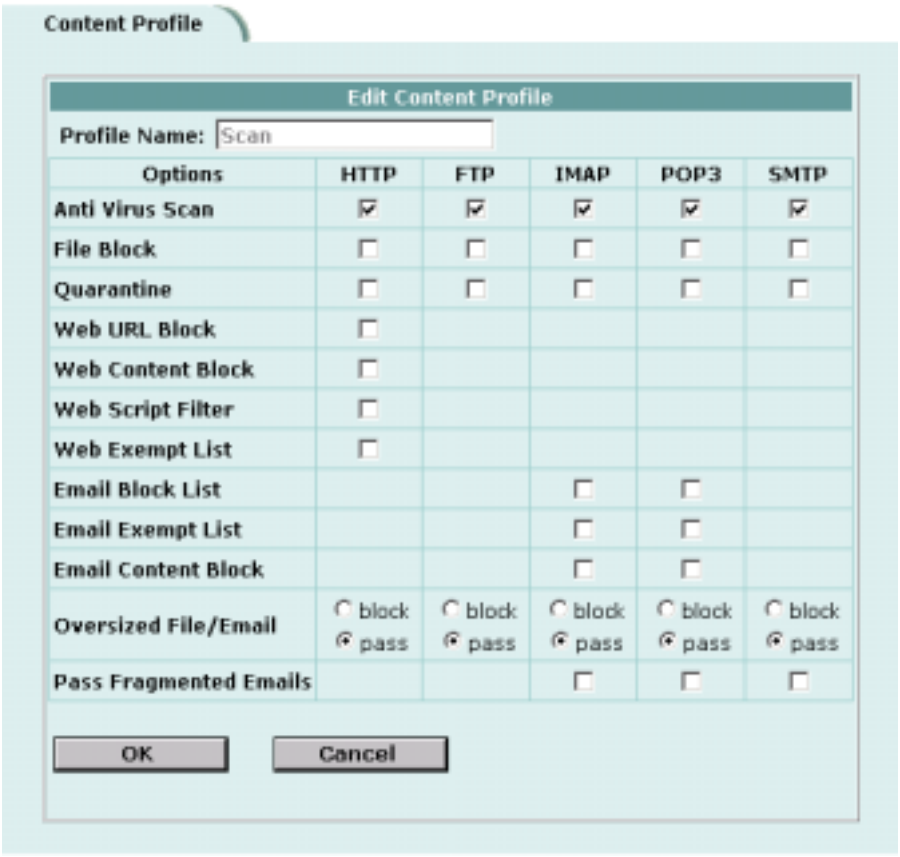
7 启用邮件片段和超大型文件 / 邮件选项。

超大型文件 / 邮件阻塞 阻塞或传输超过了配置中指定的系统内存的百分比的文件或邮件。请见 第 229 页 “ 阻塞过大的文件和电子邮件” 。

传输邮件片段 允许被分割成片段的邮件不经防病毒扫描直接传输。请见 第 229 页 “ 对邮件片段免除阻塞” 。

8 单击确定。

图 16: 内容配置文件举例



将内容配置文件添加到策略

您可以将内容配置文件添加到一个策略，这个策略的动作可以是接受或拒绝、服务类型可以是任意、HTTP、FTP、IMAP、POP3、SMTP 或一个包含以上服务的服务组。

1 进入 **防火墙 > 策略。**

2 单击包含了您要添加内容配置文件的那个策略的策略列表。

例如，要内部网络用户从网站上下载的文件启用网络保护，选择一个内部到外部的策略。

3 单击新建以添加一个新的策略，或选择一个策略并单击编辑。

4 选择病毒防护和网页过滤。

5 选择内容配置文件。

6 如果需要的话配置其余的策略选项。

7 单击确定。

8 对您要启用网络保护的任何策略重复以上步骤。

用户与认证

FortiGate 支持使用 FortiGate 用户数据库、RADIUS 服务器和 LDAP 服务器的用户认证。您可以把用户名添加到 FortiGate 用户数据库中，然后为用户设置一个密码以允许用户使用这个内部数据库进行认证。也可以添加一个 RADIUS 服务器并且选择 RADIUS，以允许用户使用选定的 RADIUS 服务器进行认证或添加一个 LDAP 服务器并且选择 LDAP，以允许用户使用选定的 LDAP 服务器进行认证。您还可以禁用某些用户使他们无法通过 FortiGate 进行认证。

要启用认证，您必须在一个或者多个用户组中添加用户名，也可以把 RADIUS 服务器和 LDAP 服务器添加到用户组中。然后当您需要认证的时候，可以选择相应的用户组。

可以在以下操作中要求认证：

- 任何 动作 被设置为 接受 的防火墙策略
- IPSec 拨号用户第一阶段配置
- 第一阶段 IPSec VPN 配置的 XAuth 功能
- PPTP
- L2TP

当一个用户输入用户名和密码时，FortiGate 在内部用户数据库上搜索匹配的用户名。如果这个用户名被设置成了禁用，那么这个用户就无法取得认证，连接将被放弃。如果这个用户设置了密码并且密码匹配，那么就允许连接。如果密码不匹配，连接同样会被放弃。

如果选择的是 RADIUS，而且配置了 RADIUS 支持，用户名和密码与 RADIUS 服务器中的用户名和密码相匹配，则允许连接。如果用户名和密码不同于 RADIUS 服务器中的用户名和密码，连接将被放弃。

如果选择的是 LDAP，而且配置了 LDAP 支持，用户名和密码与 LDAP 服务器中的用户名和密码相匹配，则允许连接。如果用户名和密码不同于 LDAP 服务器中的用户名和密码，连接将被放弃。

如果在用户组中包含了用户名、RADIUS 服务器和 LDAP 服务器，FortiGate 设备按照它们被添加到用户组的顺序在其中检索用户名。

本章描述了以下内容：

设置认证超时

按以下步骤设置认证超时：

1 进入 **系统 > 配置 > 选项**。

2 设置 **认证超时** 以控制在用户再次认证以取得对防火墙的访问权之前，防火墙能够保持空闲的时间。
默认的认证超时是 15 分钟。

添加用户名并配置认证

使用以下操作添加用户名并配置认证。

本节讨论了以下内容：

添加用户名和配置认证

1 进入 **用户 > 本地**。

2 单击 **新建** 以添加新的用户名。

3 输入用户名。
用户名可以包括数字 （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。

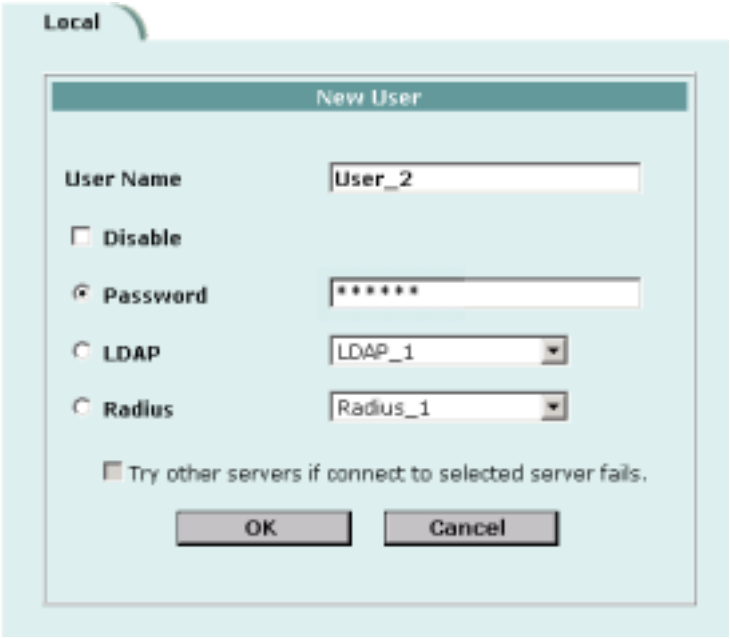
4 从以下内容中选择一项认证配置认证：

禁用	阻止这个用户认证。
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。
LDAP	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。请参阅 第 170 页 “ 配置 LDAP 支持” 。
Radius	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。请参阅 第 169 页 “ 配置 RADIUS 支持” 。

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。

图 17: 添加用户名



从内部数据库中删除用户名

您不能删除已经添加到用户组的用户名。在删除用户之前必须将它们从所添加到的用户组中删除。

1 进入**用户 > 本地**。

2 对于要删除的用户的用户名，单击 **删除用户** 。

3 单击 **确定**。

注意：删除用户名将删除这个用户的认证配置。

配置 RADIUS 支持

如果您配置了 RADIUS 支持，当某个用户被配置为要求使用 RADIUS 服务器认证的时候，FortiGate 将连接 RADIUS 服务器以获得认证。

本节描述了以下内容：

- 添加 RADIUS 服务器
- 删除 RADIUS 服务器

添加 RADIUS 服务器

按照以下步骤为 FortiGate 配置 RADIUS 认证：

1 进入 **用户 > RADIUS**。

2 单击 **新建** 以添加新的 RADIUS 服务器。

3 输入 RADIUS 服务器的名称。
您可以输入任何名称。此用户名可以包括数字 （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 输入 **RADIUS 服务器的域名** 或者 **IP 地址**。

5 输入 RADIUS 服务器 **密码**。

6 单击 **确定** 。

图 18: RADIUS 配置举例

删除 RADIUS 服务器

您不能删除已经添加到用户组的 RADIUS 服务器。

1 进入**用户 > RADIUS**。

2 对您要删除的 RADIUS 服务器，单击服务器名旁边的 **删除** 。

3 单击 **确定**。

配置 LDAP 支持

如果您配置了 LDAP 支持，当某个用户被配置为要求使用 LDAP 服务器认证的时候，FortiGate 将连接 LDAP 服务器以获得认证。要通过 FortiGate 设备进行认证，这个用户需要输入一个用户名和对应的密码。FortiGate 将拥护名和密码发送到 LDAP 服务器。如果 LDAP 服务器认证了这个用户，那么用户即可成功地通过 FortiGate 设备的认证。如果 LDAP 服务器不能认证这个用户，FortiGate 设备将拒绝这个连接。

FortiGate 设备支持 RFC2251 定义的 LDAP 协议功能，用于搜索有效的用户名和密码。ForitGate LDAP 支持所有兼容于 LDAP v3 的 LDAP 服务器。

FortiGate LDAP 支持不包括 LDAP 的扩展功能，例如某些 LDAP 服务器的密码到期通知功能。FortiGate LDAP 支持不为用户提供有关认证失败的原因等信息。

PPTP, L2TP, IPSec VPN 和防火墙认证都支持 LDAP 用户认证。PPTP, L2TP, 和 IPSec VPN 支持 PAP （包认证协议），但不支持 CHAP （挑战 - 握手协议）。

本节描述了以下内容：

添加 LDAP 服务器

按以下步骤配置 FortiGate 设备的 LDAP 认证：

1 进入**用户 > LDAP**。

2 单击新建以添加新的 LDAP 服务器。

3 输入 LDAP 服务器的名称。
您可以输入任何名称。此用户名可以包括数字 （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 输入 LDAP 服务器的域名 或者 IP 地址。

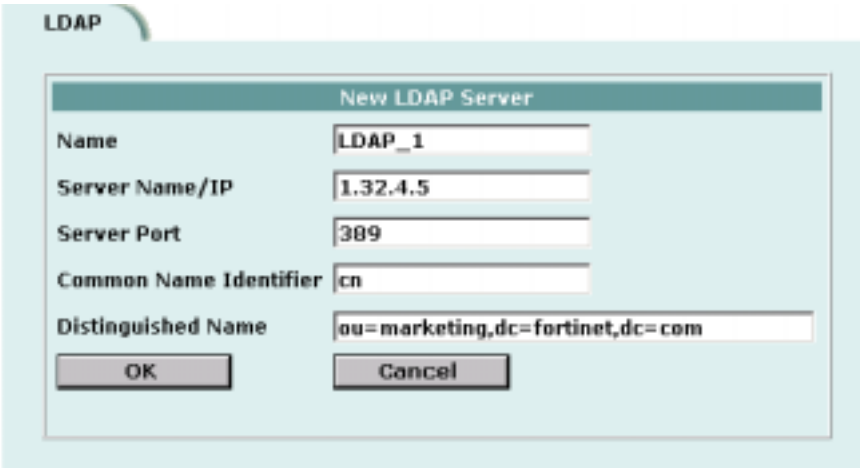
5 输入与 LDAP 服务器通讯的端口。
默认的 LDAP 使用 389 端口。

6 为这个 LDAP 服务器输入一个通用标识符。
大多数 LDAP 服务器的通用标识符是 cn。然而有些服务器可能会使用其他标识符例如 uid。

7 输入用于在 LDAP 服务器上搜索条目的名称。
使用适当的 X.509 或 LDAP 格式为服务器输入一个基本名称。FortiGate 设备会将这个名称不加修改直接发送到服务器。
例如，您可以使用以下基本名称：
ou= 行销，dc=fortinet,dc=com
其中 ou 是机构单位的缩写，dc 是域成员的缩写。
您还可以在基本名称中指定同一域名的多个实例。例如，要指定多个机构单位：
ou= 帐目 ,ou= 行销 ,dc=fortinet,dc=com

8 单击确定。

图 19: LDAP 配置举例



删除 LDAP 服务器

您不能删除已经添加到用户组的 LDAP 服务器。

1 进入**用户 > LDAP**。

2 对您要删除的 LDAP 服务器，单击服务器名旁边的 **删除** 图标。

3 单击 **确定**。

配置用户组

要启用认证，您必须在一个或多个用户组中添加用户名和 / 或 RADIUS 服务器。当您需要认证时，可以选择一个用户组。您可以对以下情况选择一个用户组：

- 需要认证的策略。只有被选中的组中的用户和可以被添加到这个用户组的 RADIUS 服务器认证的用户才能使用这些策略认证。
- 拨号用户的 IPSec VPN 第一阶段配置。只有选定用户组中的用户可以通过认证使用 VPN 通道。
- IPSec VPN 第一阶段配置的 XAuth 。只有选定用户组中的用户可以通过认证使用 VPN 通道 XAuth。
- FortiGate PPTP 配置。只有选定用户组中的用户可以使用 PPTP。
- TFortiGate L2TP 配置。只有选定用户组中的用户可以使用 L2TP。

当您将用户名、RADIUS 服务器和 LDAP 服务器添加到用户组中时，您添加它们的顺序决定了 FortiGate 设备使用他们请求认证的顺序。如果用户名在前，FortiGate 设备在本地用户中检索匹配的用户名。如果没有找到匹配的用户名，FortiGate 设备将检索 RADIUS 服务器或 LDAP 服务器。如果先添加的是 RADIUS 服务器或 LDAP 服务器，FortiGate 设备将先在服务器中检索，如果没有找到匹配的用户名才在本地用户中检索。

如果用户组包含用户名，RADIUS 服务器和 LDAP 服务器，FortiGate 设备根据他们被添加时的顺序在其中检索用户。

本节描述了以下内容：

添加用户组

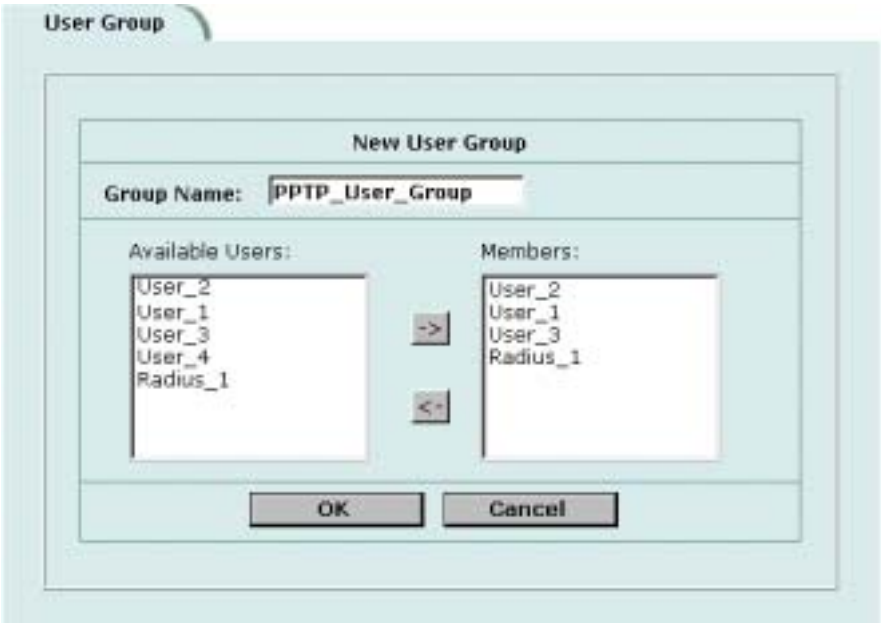
使用以下信息在 FortiGate 配置中添加用户组。可以在用户组中添加用户名、RADIUS 服务器或 LDAP 服务器。

按以下步骤添加用户组：

1 进入 **用户 > 用户组**。

2 单击 **新建** 以添加新的用户组。

图 20: 添加用户组



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

7 要从用户组中删除用户、RADIUS 服务器或 LDAP 服务器，选中 **成员列表** 中要删除的用户、RADIUS 服务器或 LDAP 服务器，然后单击右箭头将用户名或者 RADIUS 服务器从组中删除。

8 单击 **确定** 。

删除用户组

您不能删除已经被策略、远程网关、PPTP 或 L2TP 配置选用的用户组。

按以下步骤删除用户组：

1 进入 **用户 > 用户组。**

2 单击您要删除的用户组右侧的 **删除** 。

3 单击 **确定** 。

IPSec VPN

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。

可以将通道、数据加密和认证结合起来以实现安全的 VPN 连接。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）。这些信息根据已知的密钥使用数学算法加密和解密。

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 功能算法计算校验和。

本章提供了关于如何配置 FortiGate IPSec VPN 的概述。关于 FortiGate VPN 的详细信息，请见 *FortiGate VPN 指南*。

密钥管理

任何加密系统都有三个基本的元素：

- 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 IKE 自动密钥管理。

- “手工密钥”
- “使用预置密钥或证书的自动互联网密钥交换（自动 IKE)”

手工密钥

当选择了手工密钥之后，通道两端的安全参数必须互相匹配。包括加密和认证密钥在内的这些设置必须保密，从而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。

使用预置密钥或证书的自动互联网密钥交换（自动 IKE)

为了便于部署多个通道，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 IKE 和证书 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。

手工密钥 IPSec VPN

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 VPN 的一般配置步骤

一个手工密钥 VPN 的配置由手工密钥通道、通道两端的源和目的地址、以及用于控制对这个 VPN 通道访问的加密策略组成。

按以下步骤创建手工密钥 VPN 配置：

1 添加一个手工密钥 VPN 通道。请见 第 177 页 “ 添加一个手工密钥 VPN 通道” 。

2 配置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 188 页 “ 配置加密策略” 。

添加一个手工密钥 VPN 通道

配置手工密钥通道可以在 FortiGate 和同样使用手工密钥的远程 IPSec VPN 客户或网关之间建立 IPSec VPN 通道。

按照以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 VPN 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 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 到 9， 字母 a 到 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。

远程安全参数索引是一个不多于八位的一个十六进制数 （数字 0 到 9， 字母 a 到 f）。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。

在通道的两端选择相同的算法。

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 193 页 “添加一个 VPN 集中器”。

12 单击 **确定** 保存手工密钥 VPN 通道。

自动 IKE IPSec VPN

Fortinet 支持用自动密钥互联网密钥交换（自动 IKE）以两种方式建立 IPSec VPN 通道：预置密钥的自动 IKE 和数字认证的自动 IKE。

自动 IKE VPN 的一般配置步骤

一个自动 IKE VPN 的配置内容包括 第一阶段和第二阶段参数、通道两端的源地址和目的地址，以及一个控制对这个通道的访问的加密策略。

按以下步骤创建一个自动 IKE VPN 配置：

注意：您在配置一个使用数字证书的自动 IKE VPN 之前，必须为 FortiGate 设备添加一个 CA 和本地证书。关于详情请见 第 184 页 “管理数字证书”。

1 添加第一阶段参数，请见 第 179 页 “为自动 IKE VPN 添加第一阶段配置”。

2 添加第二阶段参数，请见 第 182 页 “为自动 IKE VPN 添加第二阶段配置”。

3 配置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 188 页 “配置加密策略”。

为自动 IKE VPN 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。

按以下步骤添加第一阶段配置：

1 进入 **VPN > IPSEC > 第一阶段。**

2 单击新建以添加新的第一阶段配置。

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 2。

5 选择进取模式或主模式 （ID 保护）。

当使用进取模式时，VPN 双方使用明文交换识别信息。当使用主模式时，识别信息是隐藏的。

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。

VPN 通道的两端必须使用相同的 P1 阶段提议设置。

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。

一般来说，VPN 双方应当使用相同的 DH 组设置。

8 输入密钥寿命。

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 认证方式可以设置为预置密钥或者 RSA 签名。

- 如果您选择了预置密钥，输入一个由 VPN 双方共享的密钥。这个密钥可以包含任何字符但是长度不能少于 6 个字符。只有网络管理员有权知道这个密钥。要防御密码猜测攻击，一个好的预置密钥应当包含至少 16 个随机选择的字符。
- 如果您选择了 RSA 签名，选择一个由认证中心 （CA）进行数字签名的本地认证。要为 FortiGate 设备添加一个本地认证，请见 第 184 页 “ 获得签名的本地证书” 。

10 （可选的）输入 FortiGate 设备的本地 ID。

只有当 FortiGate 设备作为客户并用它的本地 ID 对 VPN 远端认证它自己的时候，才需要输入本地 ID。（如果您没有添加本地 ID，FortiGate 设备将发送它的 IP 地址。）

只能在预置密钥和进取模式下配置本地 ID，不要在证书或者主模式下配置本地 ID。

配置高级选项

1 单击高级选项。

2 （可选的）选择对等选项。

选择对等选项可以使用远程 VPN 端点在第一阶段发送的 ID 对它们进行认证。

接受任何端点 ID	选择接受任何端点 ID（从而不认证远程 VPN 端点的 ID）。
接受这个端点 ID	选择使用一个共享的用户名 （ID）和密码 （预置密钥）认证指定的 VPN 端点或一组 VPN 端点。同时还需要输入端点 ID。
接受拨号组的端点 ID	选择使用唯一的用户名 （ID）和密码 （预置密钥）认证每一个远程 VPN 端点。还需要选择一个拨号组 （用户组）。 在配置这一选项之前先配置这个用户组。

3 （可选的）配置 XAuth。

XAuth （IKE 扩展认证）在用户层认证 VPN 双方。如果 FortiGate 设备 （本地 VPN 端点）被配置为一个 XAuth 服务器，它将通过在用户组中查询来验证远程 VPN 端点。包含在用户组中的这个用户可以是 FortiGate 设备中配置的本地用户，或者远程的 LDAP 或 RADIUS 服务器中的用户。如果 FortiGate 设备被配置为 XAuth 客户端，当它被查询的时候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 端点认证它自己的用户名。
密码	输入本地 VPN 端点用于对远程 VPN 端点认证它自己的密码。

XAuth：作为服务器

加密方法 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。

4 （可选的） NAT 跨越。

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。

5 （可选的）配置端点失效检测。
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。

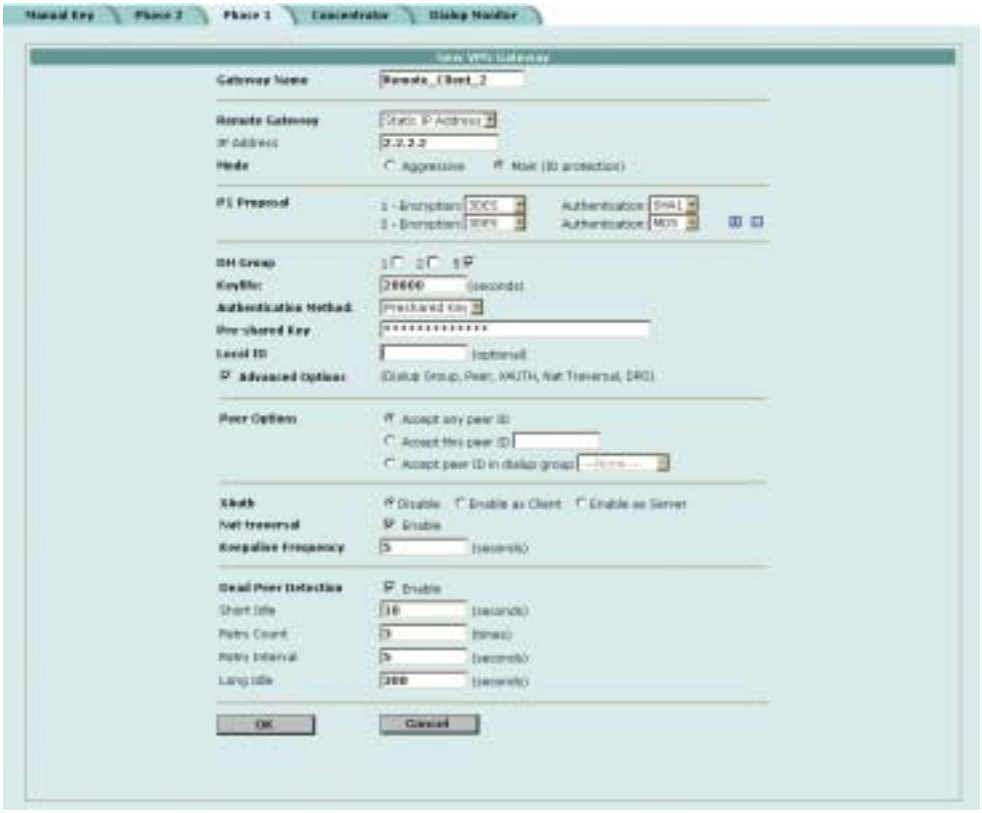
重试累计 设置本地 VPN 端点认为通道已经失效并断开安全联结之前使用 DPD 探测的重复次数。根据您的网络的具体情况，将重试累计设置得足够高可以避免网络拥塞或其他传输问题带来的影响。

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。

6 单击确定以保存第一阶段参数。

图 21: 添加第一阶段配置



为自动 IKE VPN 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。

注意：使用预置密钥 VPN 和证书 VPN 的第二阶段配置相同。

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 179 页 “ 为自动 IKE VPN 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。关于 IPSec 冗余的详细信息，请见 第 195 页 “ 冗余 IPSec VPN” 。

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。
VPN 通道的两端必须使用相同的 P2 提议设置。

6 （可选的）启用重放检测。
重放检测可以保护 VPN 通道以抵御重放攻击。

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。

7 （可选的）启用向前保密 （PFS）。
PFS 通过在密钥过期时启动一个新的 Diffie-Hellman 交换提高了安全性。

8 选择 DH 组。
VPN 双方必须使用相同的 DH 组设置。

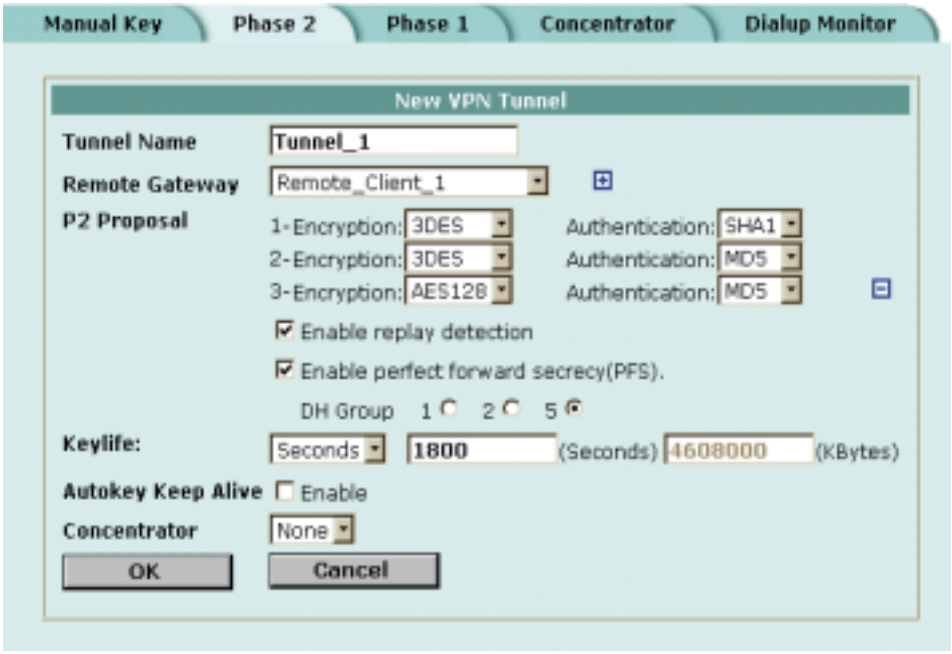
9 输入密钥有效期。
密钥有效期限制第二阶段的密钥在一定时间内，或者千字节的数据被 VPN 通道处理过之后过期，或者两者都有。如果您选择两者都是，则直到经过了指定的时间并且处理了指定量的数据之后，密钥才会过期。
当密钥过期之后，无须中断服务就可以生成一个新的密钥。P2 提议中的密钥有效期可以从 120 秒到 172800 秒或者从 5120 千字节到 99999 千字节。

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）是否指定一个集中器。
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 193 页 “ 添加一个 VPN 集中器” 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 22: 添加第二阶段配置



管理数字证书

在一个 IPSec 通讯会话的参与双方建立一个加密的 VPN 通道之前，数字证书可以用来保证参与双方是可信的。

Fortinet 使用手工操作获得证书。这包括从您的本地电脑将文本文件复制和粘贴到认证中心，或从认证中心到您的本地电脑。

- 获得签名的本地证书
- 获得一个 CA 证书

注意： 配置 fortiGate VPN 无须数字证书。数字证书是一项高级功能，它为系统管理提供了便利。这一操作假定用户具有如何在他们的应用中配置数字证书的有关知识。

获得签名的本地证书

签名的本地证书可以为 FortiGate 设备提供其他设备鉴别它的能力。

注意： VPN 端点的数字证书必须遵从 X.509 标准。

生成证书请求

您可以按照如下步骤生成一个公钥 / 私钥对。公钥是证书请求的基本元素。

按照如下步骤生成证书请求：

1 进入 **VPN > 本地证书。**

2 单击生成。

3 输入一个证书名称。

输入的名称。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 配置要认证的对象的主题信息。

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

主机 IP	输入被认证的 FortiGate 设备的 IP 地址作为主机 IP。
域名	输入被人证的 FortiGate 设备的完整的域名。不包括协议标识（http://）或任何端口号或路径名。
E-Mail	输入被认证的 FortiGate 设备的所有者的电子邮件地址。典型情况下，只有客户才需要电子邮件地址，网关不需要。

5 配置要认证的对象的用于进一步识别的可选信息。

组织单位	输入请求这个 FortiGate 设备的证书的组织中的部门或单位的识别名称（例如制造商或 MF）。
组织	输入请求这个 FortiGate 设备的证书的组织的依法登记的名称 （例如 Fortinet）。
位置	输入这个 FortiGate 设备所在的城市或城镇的名称 （例如北京）。
州 / 省	输入 FortiGate 设备所在的省 / 市 / 自治区的名称 （例如河北省）。
国家	选择这个 FortiGate 设备所在的国家。
电子邮件	输入这个 FortiGate 设备的联络电子邮件地址。通常电子邮件地址仅用于客户，而不是网关。

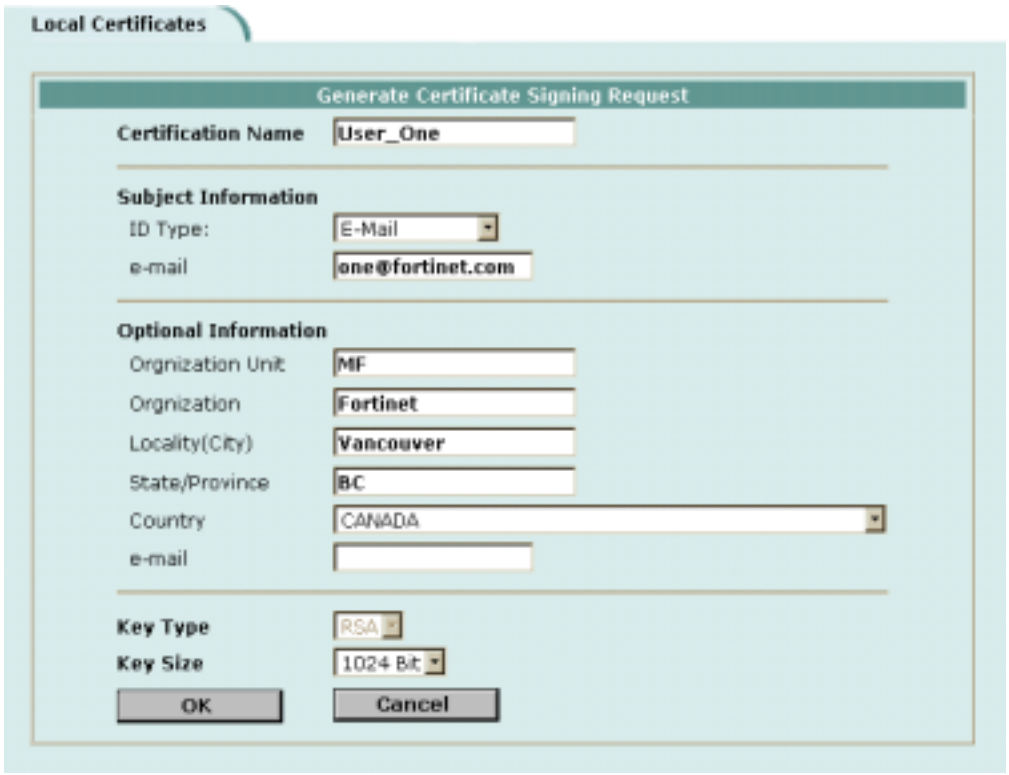
6 配置密钥。

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。
密钥大小	选择 1024 比特，1536 比特或 2048 比特。越大的密钥生成得越慢，但是也更加安全。不是所有的产品都支持这三种密钥尺寸。

7 单击确定以生成公钥 / 私钥对和证书请求。

将生成公钥 / 私钥对并在本地证书列表中显示一个带有未决状态的证书请求。

图 23: 添加本地证书



下载证书请求

您可以使用如下操作将证书请求从 FortiGate 设备下载到管理员电脑。

按照如下步骤下载证书请求：

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。

3 单击保存。

4 命名这个文件并将它保存到管理员电脑中。

请求签名的本地证书

在下面的操作中，您可以从管理员电脑中将证书请求复制和粘贴到 CA 网页服务器。

按照如下步骤请求签名的本地证书：

1 在管理员电脑中使用一个文本编辑器打开本地证书请求。

2 复制证书请求。

3 连接到 CA 网页服务器。

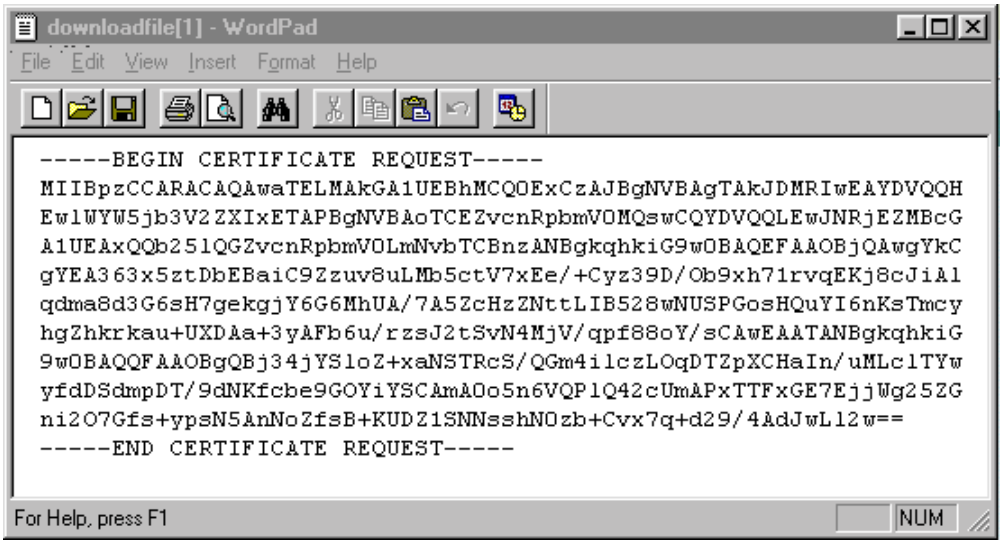
4 申请一个签名了的本地证书。

按照 CA 网页服务器的指令进行如下操作：

- 将一个 base64 编码的 PKCS#10 认证请求添加到 CA 网页服务器，
- 将证书请求粘贴到 CA 网页服务器，
- 在 CA 网页服务器上提交证书请求。

现在证书请求已经提交到 CA 以进行签名。

图 24: 在文本编辑器中打开证书请求



领取一个签名的本地证书

在下面的操作中，您可以连接到 CA 网页服务器并将一个签名的本地证书下载到管理员电脑（在 CA 已经对证书请求签名之后再领取证书）。

按照如下步骤领取一个签名了的本地证书：

1 连接到 CA 网页服务器。

2 按照 CA 网页服务器的指示下载签名了的本地证书。

将显示文件下载对话框。

3 单击保存。

4 在管理员电脑中的一个目录中保存文件。

导入签名的本地证书

在下面的操作中，您可以从管理员电脑中将签名的本地证书导入 FortiGate 设备中。

按照如下步骤导入签名的本地证书：

1 进入 **VPN > 本地证书。**

2 单击导入。

3 输入路径或通过浏览在管理员电脑中定位签名的本地证书。

4 单击确定。

在本地证书列表中将显示签名的本地证书，其状态为 OK。

获得一个 CA 证书

VPN 双方为了让对方认证自己，必须从同一个证书授权获得 CA 证书。CA 认证为 VPN 双方提供了坚定他们从其他设备中收到的数字证书是否有效的方法。

FortiGate 设备为了验证它从远程 VPN 端点获得的数字证书而获取 CA 证书。远程 VPN 端点为了验证它从 FortiGate 设备收到的数字证书而获取 CA 证书。

注意：CA 证书必须遵循 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。

按以下操作恢复 CA 证书：

1 连接到 CA 网页服务器。

2 跟随 CA 网页服务器的指示下载 CA 证书。

将显示文件下载对话框。

3 单击保存。

4 在管理员电脑的一个目录中保存 CA 证书。

导入一个 CA 证书

从管理员电脑将一个 CA 证书导入到 FortiGate 设备。

按以下步骤导入 CA 证书：

1 进入 **VPN > CA 证书。**

2 单击导入。

3 输入路径或浏览以在管理员电脑中定位 CA 证书。

4 单击确定。

现在 CA 证书将显示在 CA 证书列表中。

配置加密策略

VPN 将本地的内部网络连接到远程的外部网络。加密策略的主要角色是定义（和限制）这些网络上的哪些地址可以使用这个 VPN。

一个 VPN 只需要一个加密策略，它可以同时控制向内和向外的连接。根据您对加密策略所做的配置，它可以控制您的内部网络中的用户是否可以建立到远程网络的通道（向外连接），以及远程网络中的用户是否可以建立一个通道以连接到您的内部网络（向内连接）。这种灵活性使得一个加密策略就可以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，它必须被配置成为一个向外的策略。一个向外的策略具有一个内部网络的源地址和一个外部网络上的目的地址。源地址标识 VPN 在内部网络中的部分。目的地址标识了 VPN 在远程网络中的部分。典型的向外策略包括内部到外部的策略和 DMZ 到外部的策略。

注意：目的地址可以是互联网上的一个 VPN 客户端地址或是一个远程 VPN 网关后边的一个网络中的地址。

除了用定义 VPN 成员的地址之外，您可以配置加密策略的服务，例如 DNS、FTP 和 POP3，以及根据预定义的时间表 （根据一天当中的时间或者一周、月或年当中的日期）来接受连接。您还可以配置加密策略的以下内容：

- 向内 NAT 可以转换进入的数据包的源地址。
- 向外 NAT 可以转换向外发出的数据包的源地址。
- 流量控制 可以控制 VPN 可用的带宽和 VPN 的优先级。
- 内容配置文件 可以对 VPN 中的网页、文件传输和电子邮件服务应用防病毒保护、网页过滤和电子邮件过滤。
- 日记记录 可以使 FortiGate 设备对所有使用 VPN 的连接记录日志。

策略必须包含您所创建的用来和远程 FortiGateVPN 网关通讯的 VPN 通道。当您的内部网络中的用户试图连接到远程 VPN 网关后面的网络中的时候，加密策略截获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连接到远程 VPN 网关。当远程 VPN 网关接收到连接请求时，它检查自己的策略，网关和通道配置。如果配置允许，将在这两个 VPN 端点之间协商一个 IPSec VPN 通道。

- 添加源地址
- 添加目的地址
- 添加一个加密策略

添加源地址

源地址是本地 VPN 端点所在的网络中的地址。它可以是一个单独的电脑的地址或是一个网络的地址。

1. 进入 **防火墙 > 地址。**
2. 选择一个内部接口。（根据 FortiGate 型号的不同，方法稍有差别。）
3. 单击新建以添加一个地址。
4. 输入本地 VPN 端点的内部接口上的单独电脑或是整个子网的地址名，IP 地址和网络掩码。
5. 单击确定以保存源地址。

添加目的地址

目的地址可以是互联网上的一个 VPN 客户端或是远程 VPN 网关后边的一个网络的地址。

1. 进入 **防火墙 > 地址。**
2. 选择一个外部接口。（根据 FortiGate 型号的不同，方法稍有差别。）
3. 单击新建以添加一个地址。

4 输入互联网上的一个 VPN 客户端或是远程 VPN 网关后边的一个网络的地址名，IP 地址和网络掩码。

5 单击确定以保存目的地址。

添加一个加密策略

1 进入 **防火墙 > 策略。**

2 选择您要添加策略的策略列表。

例如，内部 -> 外部或 DMZ-> 外部。

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 VPN 连接的服务。

您可以选择 任意 以允许所有支持的类型的服务通过 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 将动作设置为接受。

8 配置加密的参数。

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。

关于配置策略有关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。

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 25: 添加一个加密策略

IPSec VPN 集中器

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提供同样的处理效率，特别是在辐条上。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，它需要一个 VPN 配置以将它连接到每个辐条 （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）。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。

- VPN 集中器（集线器） 一般配置步骤
- 添加一个 VPN 集中器
- VPN 辐条一般配置步骤

VPN 集中器（集线器） 一般配置步骤

作为集线器的中心 FortiGate 设备需要以下配置：

- 每个辐条一个通道（自动 IKE 第一阶段和第二阶段或手工密钥配置）。
- 每个辐条一个目的地址。
- 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。选择手工通道或者 IKE 通道。

- 一个手工密钥通道包括通道名、通道另一端的辐条 （客户端或网关）的 IP 地址，以及这个通道所用的加密和认证算法。

  请见 第 176 页 “ 手工密钥 IPSec VPN” 。
- 一个自动 IKE 通道，包括第一阶段和第二阶段参数。第一阶段参数包括辐条 （客户或网关）的名称，辐条如何接收它的 IP 地址 （静态）的指示，加密和认证算法，以及认证方法，可以是预置密钥或着 PKI 证书。第二阶段参数包括通道名，在第一阶段中选择的辐条 （客户或网关）的配置，加密和认证算法，以及一些安全参数。

  请见 第 178 页 “ 自动 IKE IPSec VPN” 。

2 为每个辐条添加一个目的地址。这个目的地址是辐条 （可以是互联网上的客户或者一个网关后边的网络）的地址。

请见 第 189 页 “ 添加源地址” 。

3 添加集中器配置。这一步将 FortiGate 设备上的通道彼此分组。这些通道将辐条连接到集线器上。这些通道是作为自动 IKE 第二阶段配置或手工密钥配置的一部分添加的。

请见 第 193 页 “ 添加一个 VPN 集中器” 。

注意：为所有辐条添加完通道后再为中心 FortiGate 设备 （集线器）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 VN 连接。每个辐条的加密策略必须包括这个辐条的通道名。源地址必须是内部 _ 全部。在加密策略中使用以下配置：

源	内部 _ 全部。
目的	VPN 辐条地址。
动作	加密。
VPN 通道	VPN 辐条通道名。
允许向内	选择允许向内的通讯。
允许向外	选择允许向外的通讯。
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 190 页 “ 添加一个加密策略” 。

5 按以下顺序排列策略：

- 加密策略
- 默认的非加密策略 （内部 _ 全部 -> 外部 _ 全部）

添加一个 VPN 集中器

按以下步骤添加一个 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。

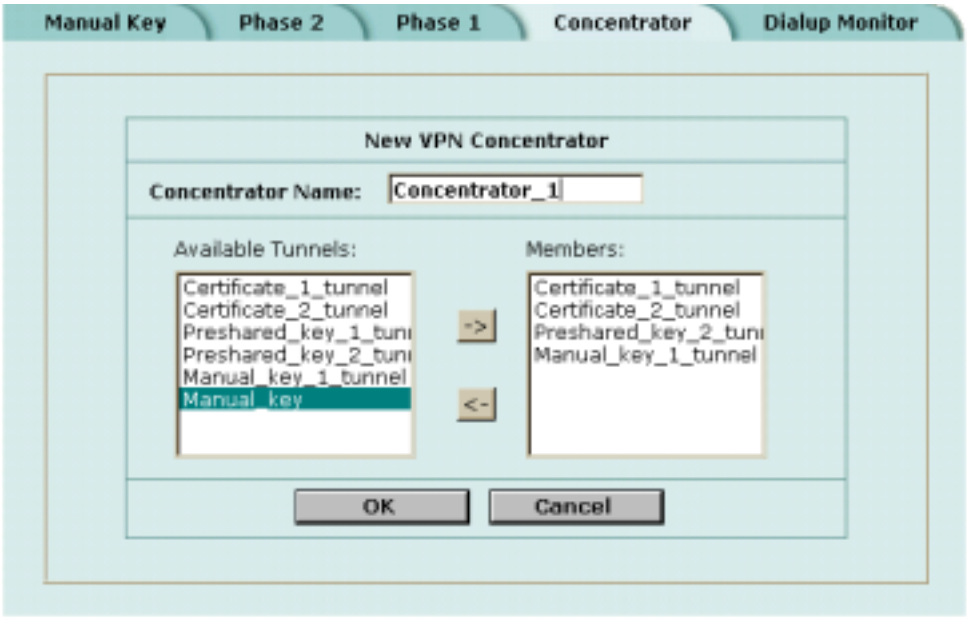
3 在 集中器名称 一栏输入新集中器的名称。

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 26: 添加 VPN 集中器



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 176 页 “ 手工密钥 IPSec VPN” 。
- 要添加一个自动 IKE 通道，请见 第 178 页 “ 自动 IKE IPSec VPN” 。

2 添加源地址。需要一个本地 VPN 辐条的源地址。

请见 第 189 页 “ 添加源地址” 。

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 189 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 190 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址。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 190 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。

冗余 IPSec VPN

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。

配置冗余 IPSec VPN

在配置 VPN 之前，确保两个 FortiGate 设备都有到互联网的多重连接。对于每个设备，首先添加多个 （两个或更多）外部接口。然后将每个接口分配到一个外部区域。最后，为每个接口添加到互联网的路由。

使用对称的设置配置两个 FortiGate 设备到互联网的连接。例如，如果远程 FortiGate 设备有两个外部接口并被分组到同一区域内，那么本地的 FortiGate 设备应当也有两个在同一区域内的外部接口。

类似地，如果远程 FortiGate 设备有两个外部接口并且在不同的区域中，那么本地 FortiGate 设备应当也有两个在不同区域中的外部接口。

如果所有的外部接口都分组在同一区域内，配置将比接口在不同区域内简单。然而，处于安全角度考虑，或者其他原因，可能无法这样配置。

当您定义完了两个 FortiGate 设备到互联网的连接后，您可以开始配置 VPN 通道。

按如下步骤配置 IPSec 冗余：

1 最多可以为三个 VPN 连接添加第一阶段参数。

除了网关名和 IP 地址以外，为每个 VPN 连接输入一样的数值。确保远程 VPN 端点 （远程网关）有静态 IP 地址。

请见 第 179 页 “ 为自动 IKE VPN 添加第一阶段配置” 。

2 最多为三个 VPN 连接添加第二阶段参数 （VPN 通道）。

- 如果到互联网的连接在同一区域内，添加一个 VPN 通道和到它的远程网关。您最多可以添加三个远程网关。
- 如果到互联网的连接在不同的区域内，或分配到了单独的接口，为输入的每个远程网关添加一个 VPN 通道。

请见 第 182 页 “ 为自动 IKE VPN 添加第二阶段配置” 。

3 添加源地址和目的地址。

请见 第 189 页 “ 添加源地址” 。
请见 第 189 页 “ 添加目的地址” 。

4 最多为三个 VPN 连接添加加密策略。

- 如果 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 VPN 连接在不同区域，为每个连接添加一个单独的向外加密策略。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。为每个策略添加不同的自动 IKE 密钥通道。

请见 第 190 页 “ 添加一个加密策略” 。

VPN 监视和问题解答

本节提供了一些常见的 VPN 维护和监视手段。

本节叙述了以下内容：

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。

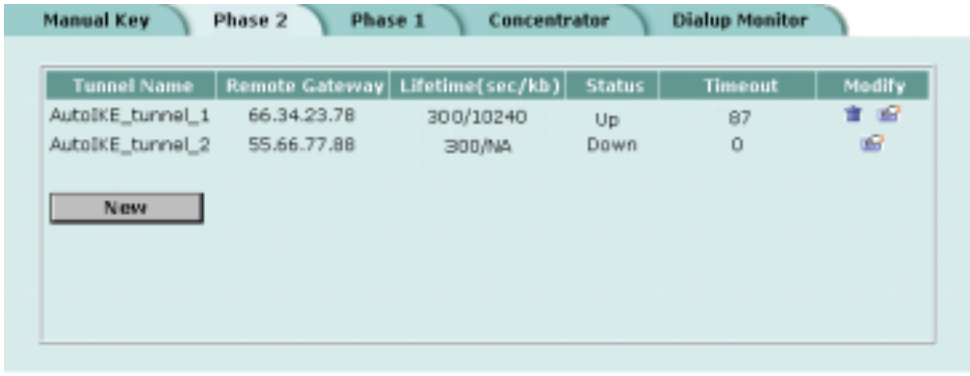
以下操作用于查看通道状态

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。

PPTP 和 L2TP VPN

您可以使用点对点隧道协议 （PPTP）和第二层隧道协议 （L2TP）在运行 Windwos 操作系统的远程客户电脑和您的内部网络之间建立一个虚拟专用网络 （VPN）。PPTP 和 L2TP 不需要第三方软件即可在客户电脑上运行，因为它们一种 Windows 标准。只要互联网服务供应商支持 PPTP 和 L2TP 连接，您只要在客户电脑和 FortiGate 设备上做一些必要的简单设置即可创建一个安全的连接。

本章提供了一个关于如何配置 FortiGate PPTP 和 L2TP VPN 的概述。关于 FortiGate PPTP 和 L2TP 的详细描述请见 FortiGate VPN 指南。

本章描述了以下内容：

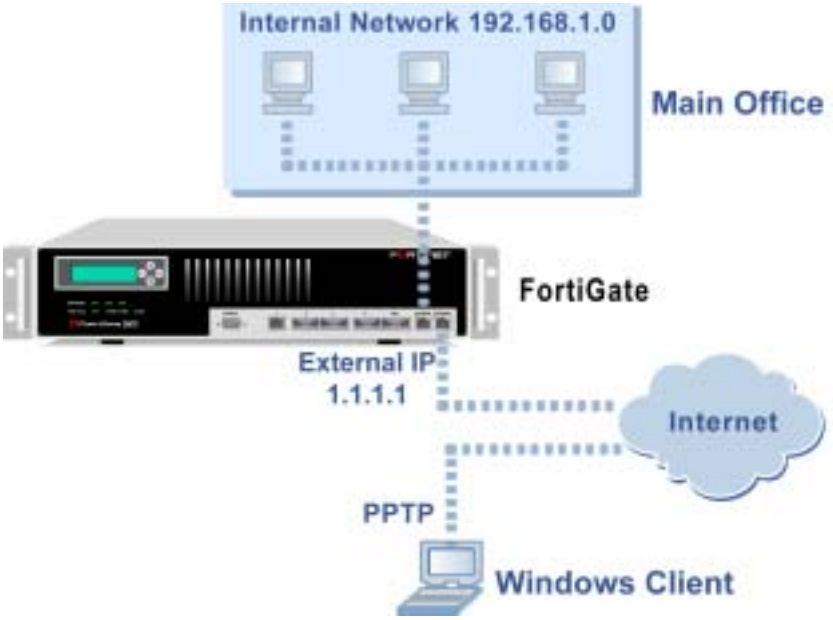
配置 PPTP

顾名思义，PPTP 包括点对点通讯协议。PPTP 使用 PPP 包将数据封包并使用 IP 包压缩 PPP 包以使得它能通过 VPN 通道传输。

注意：只有在 NAT/ 路由模式下才支持 PPTP VPN。

本节叙述了以下内容：

图 29: Windows 客户和 FortiGate 之间的 PPTP VPN



把 FortiGate 配置为 PPTP 网关

按照以下步骤将 FortiGate 设备配置问 PPTP 网关：

添加用户名和组

按以下步骤为每个 PPTP 客户端添加一个用户：

1 进入 **用户 > 本地**。

2 添加并配置 PPTP 用户。
请见 第 168 页 “ 添加用户名并配置认证” 。

3 进入 **用户 > 用户组。**

4 添加并配置 PPTP 用户组。
请见 第 172 页 “ 配置用户组” 。

启用 PPTP 并指定一个地址范围

1 进入 **VPN > PPTP > PPTP 范围。**

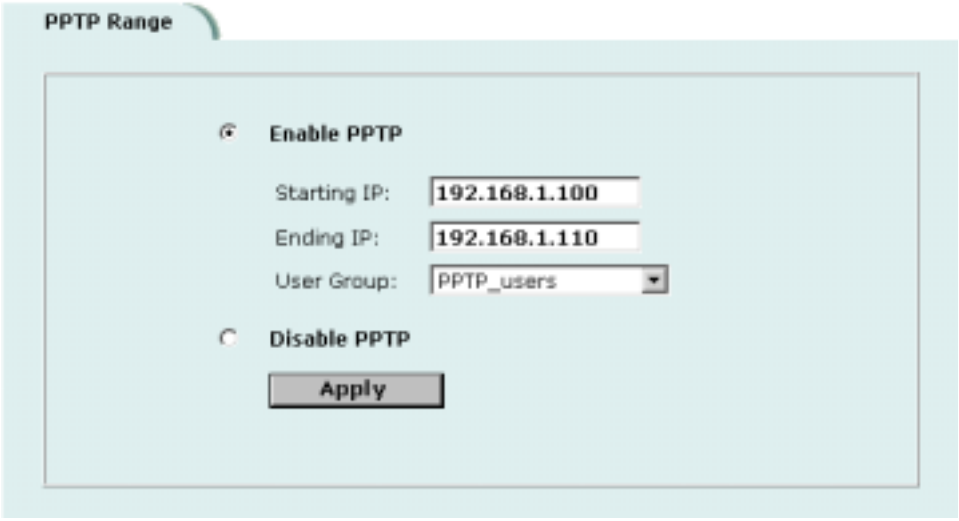
2 单击启用 PPTP。

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 200 页 “ 添加用户名和组” 中添加的用户组。

5 单击 **应用** 以启用通过 FortiGate 的 PPTP。

图 30: PPTP 地址范围配置的例子



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。

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。

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。

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。

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。

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。
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。

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。

L2TP VPN 配置

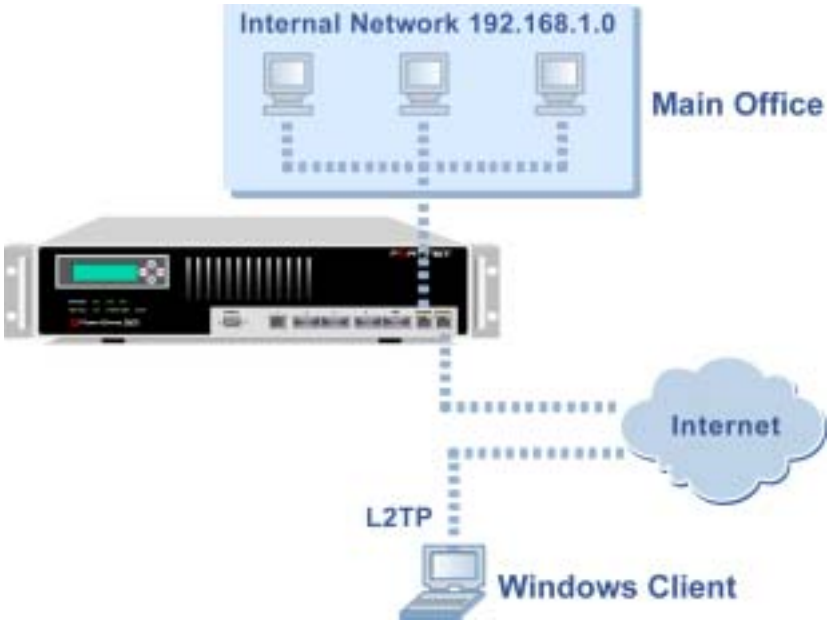
有些 L2TP 的应用支持 IPSec 元素。在 FortiGate 设备中使用 L2TP 时必须禁用这些 IPSec 元素。

注意：只有在 NAT/ 路由模式下才支持 L2TP VPN。

本节叙述了以下内容：

- 把 FortiGate 配置为 L2TP 网关
- 配置 Windows2000 客户的 L2TP
- 配置 WindowsXP 客户的 L2TP

图 31: Windows 客户和 FortiGate 之间的 L2TP VPN



把 FortiGate 配置为 L2TP 网关

按以下步骤将 FortiGate 设备配置为 L2TP 网关：

添加用户和用户组

为每个 L2TP 客户端添加一个用户：

1 进入 **用户 > 本地。**

2 添加并配置 L2TP 用户。
请见 第 168 页 “ 添加用户名并配置认证” 。

3 进入 **用户 > 用户组。**

4 添加并配置 L2TP 用户组。
请见 第 172 页 “ 配置用户组” 。

启用 L2TP 并指定地址范围

1 进入 **VPN > L2TP > L2TP 范围。**

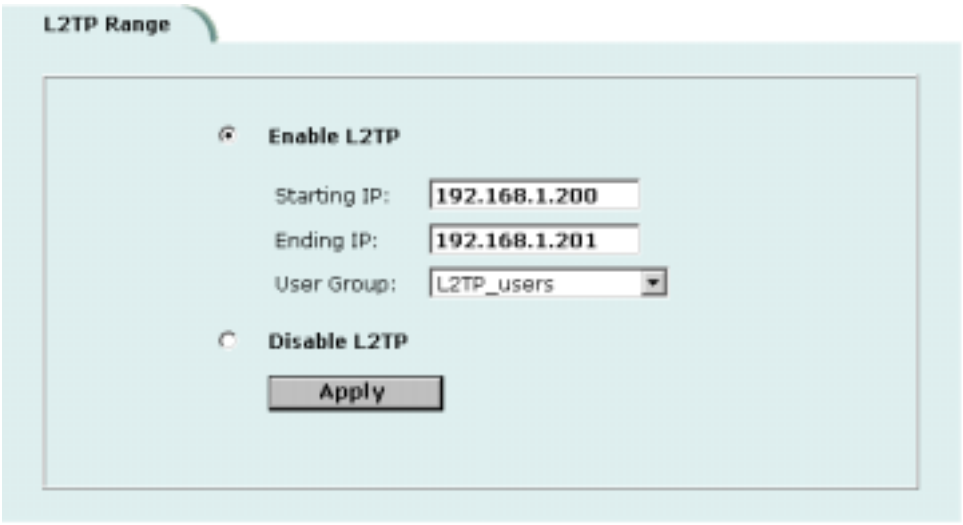
2 选择启用 L2TP。

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 206 页 “ 添加用户和用户组” 添加的用户组。

5 单击**应用** 以启动通过 FortiGate 的 L2TP。

图 32: L2TP 地址范围配置的例子



6 把 L2TP 地址范围中的地址添加到外部接口地址列表。这些地址可以放进一个外部地址组里。

7 在连接到目的接口中添加 L2TP 用户可以连接的网络地址。这些地址可以放进一个地址组里。
例如，如果您希望 L2TP 用户可以连接到内部网络中，您可以在防火墙 -> 地址 -> 内部的内部接口地址列表里添加这个地址。

8 添加一个允许 L2TP 用户通过 FortiGate 连接的策略。

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。
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 L2TP 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。

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。
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。

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。

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。

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。

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。

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。

10 选择 **网络** 属性页。

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。

网络入侵检测系统（NIDS）

FortiGate NIDS 是一个实时的网络入侵探测器，它使用攻击定义库来检测和阻止各种各样的可疑的网络数据流和基于网络的直接攻击。此外，当发生攻击时，NIDS 可以将事件写入攻击日志并向系统管理员发送报警邮件。

本章叙述了以下内容：

检测攻击

NIDS 检测模块可以检测到大多数可疑的网络通讯和基于网络的攻击。按照以下步骤配置 NIDS 的通用设置和 NIDS 检测模块特征列表。

对于 NIDS 通用设置，您需要选择要监视基于网络攻击的网络接口。您还需要决定是否启用校验和检验功能。校验和检验功能测试被监视的接口接收到的数据包的完整性。

本节描述了以下内容：

选择要监视的网络接口

1. 进入 **NIDS > 检测 > 通用**。
2. 选择要检测网络攻击的网络接口。
   您可以选择一个或多个网络接口。
3. 单击**应用**以保存您所做的修改。

禁用 NIDS

1. 进入 **NIDS > 检测 > 通用**。
2. 删除全部网络接口。

3 单击 **应用** 以保存您所做的修改。

验证校验和的配置

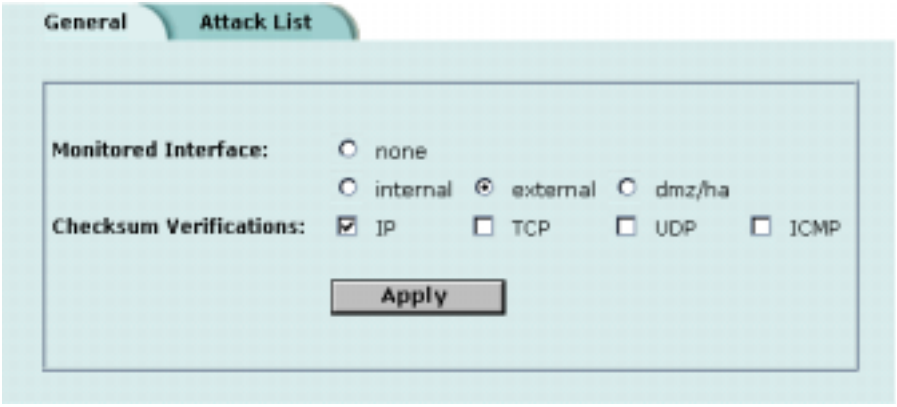
校验和验证测试通过 FortiGate 的文件，确保他们在传送过程中没有被篡改。NIDS 可以在 IP、TCP、UDP 和 ICMP 数据流上进行校验和检查。如果要进行最大限度的检查，您可以启用所有类型数据流的校验和检查。然而，如果 FortiGate 不需要进行校验和验证，您可以关掉部分或者全部类型的数据流的校验和验证，这样可以提高网络传输性能。如果您的 FortiGate 是安装在一个同样进行校验和验证的路由器后面，您就没有必要再进行校验和验证。

1 进入 **NIDS > 检测 > 通用**。

2 选中要验证校验和的数据流类型。

3 单击 **应用** 以保存您所做的修改。

图 33: NIDS 检测配置举例



查看攻击特征列表

按以下操作显示当前的攻击特征组和特征组成员列表：

1 进入 **NIDS > 检测 >特征列表**。

2 查看列表中的特征组的名称和活动状态。
NIDS 根据列表中所有修改列或细节列被选中的特征组进行攻击检测。

注意：用户定义的特征组是特征列表中的最后一项。请见 第 217 页 “ 添加 用户定义的特征” 。

3 单击查看细节 以查看特征组的成员。
特征组成员列表显示了每个成员的攻击 ID，名称和修订版本。

查看攻击描述

Fortinet 提供了所有 NIDS 攻击的在线信息。按照如下步骤查看特征列表中的某一种攻击对应的 Forti 响应攻击分析网页：

1 进入 **NIDS> 检测 > 特征列表**。

2 单击查看细节可以显示一个特征组的成员。
选择一个特征并复制它的攻击 ID。

3 打开网页浏览器并输入以下 URL：

`http://www.fortinet.com/ids/ID<攻击 ID>`

记住要包括这个攻击 ID。

例如，要查看 ssh CRC32 overflow /bin/sh 攻击（ID101646338）的 Fortinet 攻击分析网页，使用如下 URL：

`http://www.fortinet.com/ids/ID101646338`

注意：每个攻击日志消息包含一个直接连到这个攻击的 Forti 响应攻击分析网页的 URL。这个 URL 可以从攻击日志消息和报警邮件消息中直接访问。关于日志消息内容和格式的详细信息，以及有关日志位置的信息，请见*日志配置和参考指南*。要记录攻击日志消息，请见 第 220 页“记录 NIDS 攻击日志”。

图 34: 特征组成员的例子

exploit		
ID	Rule Name	Revision
101646337	gobbles SSH exploit attempt	16
101646338	ssh CRC32 overflow /bin/sh	16
101646339	ssh CRC32 overflow NOOP	16
101646340	ssh CRC32 overflow	16
101646341	x86 linux samba overflow	16
101646342	Solaris x86 nlps overflow attempt	16
101646343	nlps x86 solaris overflow	16
101646344	LPRng overflow	16
101646345	redhat 7.0 lprd overflow	16

启用和禁用 NIDS 攻击特征

默认情况下，所有的 NIDS 攻击特征都已经启用。您可以使用 NIDS 攻击特征列表禁用对某些攻击的检测。禁止检测不常见的攻击方式可以提高系统的性能，减少 NIDS 生成的攻击日志中消息的数目和报警邮件的数量。例如，NIDS 检测大量的网页服务器攻击。如果您没有提供对您的防火墙后面的 Web 服务器的访问，则可以禁用所有对 Web 服务器攻击类型的攻击检测。

注意：为了保存您的 NIDS 攻击特征设置，Fortinet 建议您在更新固件和在更新之后恢复保存过的配置之前先备份您的 FortiGate 设置。

禁用 NIDS 攻击特征

1 进入 **NIDS > 检测 > 特征列表**。

2 卷动特征列表，找到要禁用的攻击特征。

攻击日志和报警邮件中的攻击名称和 ID 号与攻击列表中的相对应。您可以很容易地通过 ID 号在攻击列表中找到特定的攻击定义库。

3 取消对攻击特征旁边的活动选项的选中就可以禁用对这个攻击的检测。

4 单击确定。

5 对您要禁用的每个攻击特征重复步骤 2 到 4。

单击全部选中 可以启用攻击特征列表中的全部的 NIDS 攻击特征组。

单击全部取消 可以禁用攻击特征列表中的全部的 NIDS 攻击特征组。

添加 用户定义的特征

您可以在一个文本文件中创建用户定义特征列表然后将它从管理员电脑中上载到 FortiGate 设备。

关于如何编写用户定义的攻击特征的详细信息，请见 *FortiGate NIDS 指南*。

1 进入 **NIDS > 检测 > 用户定义特征列表。**

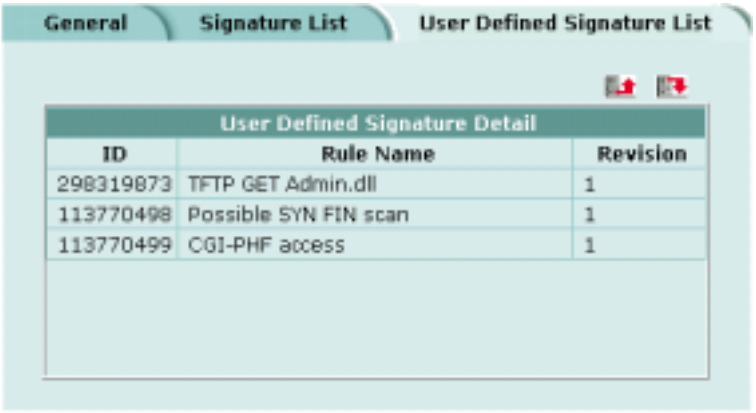
2 单击上载。

3 输入用户定义特征列表的文本文件的文件名和路径，或者单击浏览并定位文件。

4 单击确定以上载用户定义攻击特征列表的文本文件。

5 单击确定以显示上载的用户定义攻击特征列表。

图 35: 用户定义攻击特征列表的例子



下载用户定义攻击特征列表

您可以将用户定义攻击特征列表备份到管理员电脑中，保存成文本文件。

1 进入 **NIDS > 检测 > 用户定义攻击特征列表。**

2 单击下载。

FortiGate 设备将用户定义的攻击特征列表下载到管理员电脑中保存为文本文件。您可以指定文本文件保存时的文件名和路径。

NIDS 攻击预防

NIDS 攻击预防功能可以保护 FortiGate 设备和所连接的网络不受一般 TCP、ICMP、UDP 和 IP 攻击的威胁。您可以使用默认的攻击检测临界值启用 NIDS 攻击预防功能。或者也可以根据您的需要启用攻击预防并调整攻击检测的临界值。

注意：FortiGate 设备重新启动后，NIDS 攻击预防和握手信号淹没预防功能始终是关闭的。

启用 NIDS 攻击预防

1 进入 **NIDS > 预防。**

2 单击左上角的启用。

启用 NIDS 攻击预防特征

NIDS 预防模块包括了各种常见攻击的特征，以保护您的网络不受这些攻击的威胁。默认情况下只启用了部分特征，您可以根据需要手工启用其他的。 关于 NIDS 预防特征的完整列表和详细描述，请见 *FortiGate NIDS 指南*。

1 进入 **NIDS > 预防。**

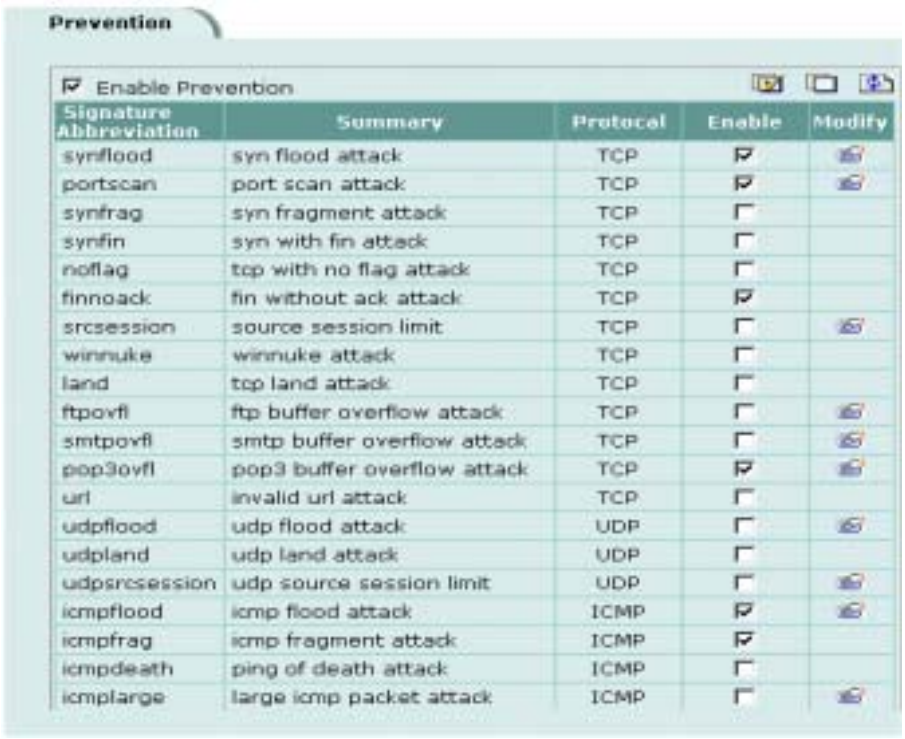
2 选中您要启用的每个特征旁边的核选框。

3 单击全部选中  可以启用 NIDS 攻击预防特征列表中的全部特征。

4 单击全部取消  可以禁用 NIDS 攻击预防特征列表中的全部特征。

5 单击恢复默认值  可以只启用默认的 NIDS 攻击预防特征，并恢复到默认的临界值。

图 36: NIDS 攻击预防特征列表的条目举例



设置特征临界值

您可以表 6 中列出的 NIDS 攻击预防特征的默认的临界值。临界值取决于攻击的类型。对于淹没攻击，临界值是每秒接收到的包的最大数目。对于溢出攻击，临界值是命令的缓冲区大小。对于超大 ICMP 包攻击，临界值是允许传输的 ICMP 包的尺寸限制。

例如，将 ICMP 淹没特征的临界值设置为 500 可以允许从单一源地址发出 500 个回音请求，而系统将发送回音响应。如果收到 501 个或更多的回音请求，FortiGate 设备将阻塞攻击者以预防对操作系统的攻击。

如果您输入的临界值是 0 或超过了允许的范围，FortiGate 设备将使用默认的临界值。

表 6： NIDS 预防特征的临界值

特征缩写	临界值的单位	默认临界值	最小临界值	最大临界值
握手淹没	每秒接收到的 SYN 包的最大数目	200	30	3000
端口扫描	每秒接收到的 SYN 包的最大数目	128	10	256
会话淹没	来自同一源地址的会话初始化请求的最大数目。	2048	128	10240
FTP 溢出	一个 FTP 命令的最大缓冲区大小 （字节）	256	128	1024
SMTP 溢出	一个 SMTP 命令的最大缓冲区大小 （字节）	512	128	1024
POP3 溢出	一个 POP3 命令的最大缓冲区大小 （字节）Maximum buffer size for a POP3 command (bytes)	512	128	1024
UDP 淹没	每秒从同一源地址接收到的或发送到同一目的地址的最大 UDP 包数目	2048	512	102400
UDP 会话淹没	来自同一源地址的 UDP 会话初始化请求的最大数目	1024	512	102400
ICMP 淹没	每秒从同一源地址接收到的或发送到同一目的地址的最大 ICMP 包数目	256	128	102400
ICMP 源会话淹没	来自同一源地址的 ICMP 会话初始化请求的数目	128	64	2048
ICMP 攻击	每秒从同一源地址收到的 ICMP 包的最大数量	32	16	2048
超大 ICMP 包	ICMP 包的最大尺寸 （字节）	32000	1024	64000

按以下步骤设置预防特征的临界值：

1 进入 **NIDS > 预防。**

2 单击您要设置临界值的特征旁边的修改  图标。

不具备临界值设置功能的特征旁边没有修改  图标。

3 输入临界值。

4 单击启用核选框。

5 单击确定。

配置握手溢出特征值

您可以设置对握手溢出特征进行检测的临界值、队列长度和有效期。

值	描述	最小值	最大值	默认值
临界值	每秒发送到目的主机或服务器的建立连接请求（握手）的数量。如果握手请求是发送到目的主机的所有端口的，而不是仅仅发送到一个端口，那么临界值将提高为原来的四倍。	30	3000	200
队列长度	FortiGate 设备能控制的代理连接的最大值。FortiGate 设备将丢弃更多的代理请求。	10	10240	1024
超时	一个代理连接的握手请求（SYN）的以秒为单位的有效时间。此值限制了代理连接表的大小	3	60	15

1 进入 **NIDS > 预防。**
2 单击握手淹没特征旁边的修改  。
3 输入临界值。
4 输入队列长度。
5 输入超时时间。
6 单击启用核选框。

或者，单击预防特征列表中的启用握手淹没。

7 单击确定。

记录 NIDS 攻击日志

当 NIDS 检测或者预防一个攻击的时候，它会生成一条攻击消息。您可以配置系统以将这个消息添加到攻击日志。

- 将攻击消息记录到攻击日志
- 减少 NIDS 攻击日志消息和报警邮件的数量

将攻击消息记录到攻击日志

按照如下步骤将攻击消息记录到攻击日志。

1 进入 **日志和报告 > 日志设置。**
2 对您设置的日志位置单击配置策略。
3 单击 IDS 日志。
4 单击 IDS 检测和 IDS 预防。
5 单击确定。

注意：关于日志消息的内容和格式，以及日志位置的详细信息，请见*日志配置和参考指南*。

减少 NIDS 攻击日志消息和报警邮件的数量

入侵企图可能产生大量的攻击消息。为了帮助您从无关的警报中找到真正有用的信息，FortiGate 设备提供了减少没必要的消息的数量的方法。根据消息生成的频率，FortiGate 设备能自动删除重复的消息。如果您还收到大量的虚假警报，您可以手工禁用有关的特征组的消息生成。

自动减少消息

NIDS 生成的攻击日志和报警邮件消息中的内容包括被检测到的攻击的 ID 编号和名称。消息中的攻击 ID 编号和名称对应于 NIDS 特征组成员列表中的 ID 编号和名称。

FortiGate 设备有一个报警邮件队列，它将每个新生成的消息与队列中已有的消息比对。如果新的消息没有重复，FortiGate 设备将立刻发送这个消息，并将消息的一个副本放进队列。如果新消息是重复的，FortiGate 设备会删除它并将队列中对应的消息内部的计数器加一。

FortiGate 设备将报警邮件消息的副本保存 60 秒。如果一个消息副本在队列中的时间超过了 60 秒，FortiGate 设备删除这个消息并将副本计数器加一。如果副本数大于一，FortiGate 设备将发送一个标题为 “重复 x 次”的统计信息邮件，邮件内容为“以下邮件在过去的 y 秒中重复了 x 次”和原始信息。

手工减少信息

如果您希望减少 NIDS 生成的警报的数量，您可以查看以下攻击日志消息的内容和报警邮件的内容。如果有大量的无效警报 （例如，网页攻击警报，而您根本没有运行网页服务器），您可以禁用攻击列表中对应的那些类型的攻击。使用攻击日志和报警邮件中消息所显示的攻击 ID 编号可以很容易地在特征列表中找到对应的项目。见 第 216 页 “ 启用和禁用 NIDS 攻击特征” 。

防病毒保护

在防火墙策略中启用了防病毒保护功能。当您启用一个防火墙策略中的防病毒保护功能时，您可以选择一个内容配置文件来决定防病毒保护的程度。内容配置文件可以控制通讯保护的类型 (HTTP, FTP, IMAP, POP3, SMTP)，防病毒保护的类型以及如何处理邮件片段、超大型的文件和电子邮件。

本章描述了以下内容：

一般配置步骤

防病毒保护功能的配置一般包括以下几步。

1 在一个新的内容配置文件或现有的内容配置文件中选择防病毒保护选项。请见 第 163 页 “ 添加一个内容配置文件” 。

2 在防火墙策略中选中防病毒保护和网页过滤选项，以允许网页 (HTTP), FTP, 和电子邮件 (IMAP, POP3, 和 SMTP) 连接通过 FortiGate 设备。对防火墙策略选择一个内容配置文件以提供您所希望的防病毒保护功能。请见 第 165 页 “ 将内容配置文件添加到策略” 。

3 配置防病毒保护设置，以控制 FortiGate 设备应用到该策略所接受的网页、FTP 和电子邮件通讯上的防病毒保护功能。请见

- 第 224 页 “ 防病毒扫描” ，
- 第 225 页 “ 文件阻塞” ，
- 第 229 页 “ 阻塞过大的文件和电子邮件” ，
- 第 229 页 “ 对邮件片段免除阻塞” 。

4 配置文件隔离设置可以控制要实施隔离的被感染的文件或被阻塞的文件的通讯类型、时间和文件大小。请见 第 229 页 “ 配置隔离选项” 。

5 配置当 FortiGate 设备阻塞或删除一个被感染的文件时用户收到的消息。请见 第 133 页 “ 定制替换信息” 。

6 配置 FortiGate 设备在阻塞或删除被感染的文件时发送的报警邮件，请见 *日志和消息参考指南*中的 “配置报警邮件”。

注意：要接收病毒日志消息，请见*日志配置和参考指南*中的 “配置日志”，关于日志消息的内容和格式的信息，请见*日志配置和参考指南*中的 “病毒日志消息”。

防病毒扫描

病毒扫描可以从启用了防病毒保护功能的内容流中截取大多数的文件 （包括使用 ZIP、RAR、GZIP、UPX 和 OLE 压缩了 12 层的文件）。病毒扫描功能将测试每个文件的文件类型和使用最有效的方法在文件中扫描病毒。例如，使用二进制病毒扫描功能扫描二进制文件，使用宏病毒扫描功能扫描含有宏的 Microsoft Office 文件。

FortiGate 病毒扫描功能不扫描以下类型的文件：

- cd 映像
- 软盘映像
- 扩展名为 .ace 的文件
- 扩展名为 .bzip2 的文件
- 扩展名为 .Tar+Gzip+Bzip2 的文件

一旦发现某个文件含有病毒，它将被从内容流中删除，并用一条替换信息提示用户。

如果您的 FortiGate 设备配备了硬盘并启用了对匹配的通讯协议中的感染的文件隔离的功能，FortiGate 设备会把文件加入隔离列表。

以下方法用于在 FortiGate 防火墙通讯中扫描病毒

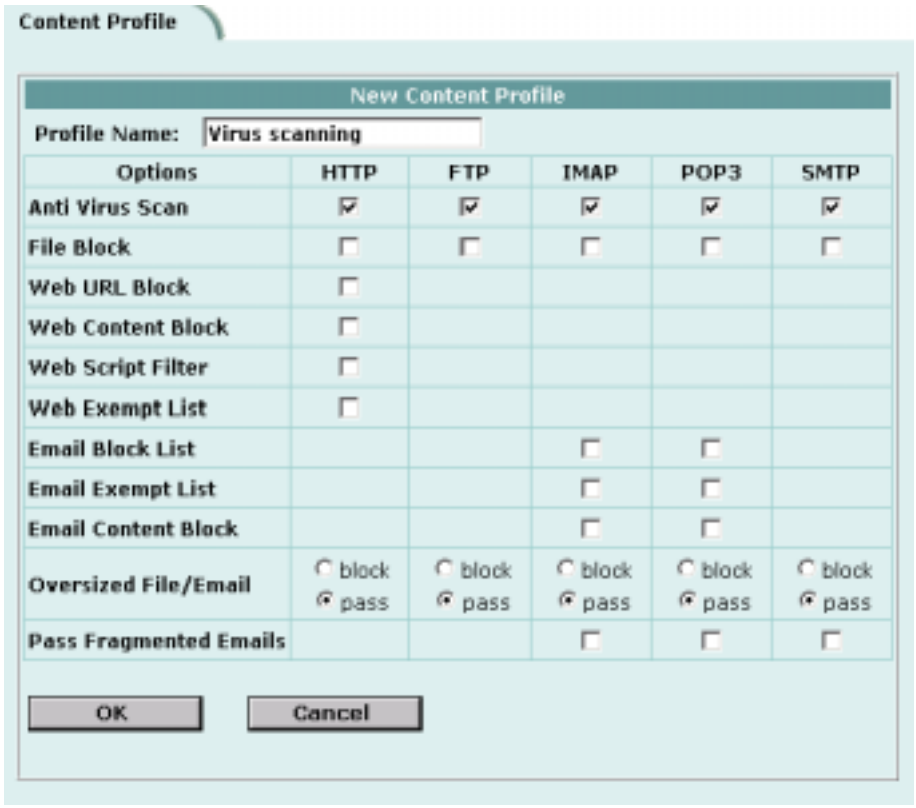
1 在一个内容配置文件中选择防病毒扫描。
见 第 163 页 “ 添加一个内容配置文件” 。

2 可以在这个内容配置文件中选择隔离。

3 将这个内容配置文件添加到防火墙策略以对防火墙策略接受的通讯应用病毒扫描。
见 第 165 页 “ 将内容配置文件添加到策略” 。

4 配置文件隔离设置以控制如何隔离被感染的文件。见 第 229 页 “ 配置隔离选项” 。

图 37: 病毒扫描的内容配置文件的例子



文件阻塞

启用文件阻塞删除所有的文件以阻止潜在的威胁，并对计算机病毒攻击提供最好的保护。只有出现防病毒扫描功能不能发现的新病毒的时候才有必要使用文件阻塞功能提供对病毒的防护。通常情况下您没有必要启用 FortiGate 设备的文件阻塞功能。然而，在极度危险的情况下，当没有其它的方式能够保护您的网络免受文件型病毒的危害的时候，文件阻塞是唯一有效的方法。

在配备了硬盘的 FortiGate 设备中，如果启用了对应通讯协议的文件阻塞的隔离功能，FortiGate 设备会将文件添加到隔离列表。

文件阻塞功能会删除所有与文件样板列表匹配的文件。FortiGate 设备会用一条警告消息替换掉文件并转发给用户。同时，如果做了相应的配置，FortiGate 设备还会在病毒日志中写入一条消息，并发送一封报警邮件。

注意：如果同时启用了阻塞和扫描，FortiGate 设备直接阻塞与文件名样板列表匹配的文件，而不对它们进行病毒扫描。

默认情况下，当阻塞功能启用时，FortiGate 按照以下文件名样板阻塞文件：

- 可执行文件 (*.bat, *.com, 和 *.exe)
- 压缩或存档文件 (*.gz, *.rar, *.tar, *.tgz, 和 *.zip)
- 动态链接库文件 (*.dll)
- HTML 应用程序 (*.hta)
- Microsoft Office 文件 (*.doc, *.ppt, *.xl?)
- Microsoft Works 文件 (*.wps)
- Visual Basic 文件 (*.vb?)
- 屏幕保护程序 (*.scr)

在防火墙通讯中阻塞文件

使用内容配置文件可以在防火墙策略接受的 HTTP, FTP, POP3, IMAP, 和 SMTP 通讯中应用文件阻塞。

1 在一个内容配置文件中选择文件阻塞。

请见 第 163 页 “ 添加一个内容配置文件” 。

2 把这个内容配置文件添加到防火墙策略，以在这个防火墙策略接受的通讯中应用内容阻塞。

请见 第 165 页 “ 将内容配置文件添加到策略” 。

添加用于阻塞的文件名样板

1 进入 **防病毒 > 文件阻塞**

2 单击新建。

3 在文件名样板栏输入新的样板。

输入文件名样板所需的字符，您可以使用星号来代表任何字符，用问号来代表任何单个字符。例如， *.dot 阻塞 Microsoft Word 模板文件，*.do? 阻塞 Microsoft Word 模板文件和文档文件。

4 选中要启用对这个文件样板的阻塞的通讯协议旁边的核选框。

5 单击确定。

隔离

配备了硬盘的 FortiGate 可以配置为隔离被阻塞或被感染的文件。被隔离的文件将被从内容流中删除，并存储到 FrotiGate 的硬盘上。用户会收到一条信息提醒他们被删除的文件已经被隔离了。

在 FortiGate 设备中，被隔离的文件的文件名显示在隔离列表里。列表显示每个被隔离的文件的状态、副本数和时间信息。您可以根据这些条件对列表进行排序和过滤。您也可以从这个列表中删除或下载文件。

- 隔离被感染的文件
- 隔离被阻塞的文件
- 查看隔离列表
- 隔离列表排序
- 过滤隔离列表
- 从隔离区中删除文件
- 下载被隔离的文件
- 配置隔离选项

隔离被感染的文件

使用内容配置文件可以隔离在由防火墙策略控制的 HTTP, FTP, POP3, IMAP, 和 SMTP 通讯中发现的被感染的文件。

1 进入 **病毒防护 > 隔离 > 隔离配置**。

2 选择要隔离被感染的文件的内容协议。

3 在内容配置文件中选择防病毒扫描。

请见 第 163 页 “ 添加一个内容配置文件” 。

4 选择隔离以将任何已发现被病毒感染的文件隔离。

5 将这个内容配置文件添加到防火墙策略，以隔离由这个防火墙策略控制的通讯中发现的被感染的文件。

请见 第 165 页 “ 将内容配置文件添加到策略” 。

隔离被阻塞的文件

使用内容配置文件可以隔离在由防火墙策略控制的 HTTP, FTP, POP3, IMAP, 和 SMTP 通讯中被阻塞的文件。

1 进入 **病毒防护 > 隔离 > 隔离配置**。

2 选择要隔离被阻塞的文件的内容协议。

3 要隔离被阻塞的文件，在内容配置文件中选择文件阻塞。

见 第 163 页 “ 添加一个内容配置文件” 。

4 选择隔离以将被阻塞的文件放入隔离区。

5 将这个内容配置文件添加到防火墙策略，以隔离由这个防火墙策略控制的通讯中发现的阻塞的文件。

请见 第 165 页 “ 将内容配置文件添加到策略” 。

查看隔离列表

1 进入 **病毒防护 > 隔离**。

隔离列表提供了以下信息。

文件名	被隔离的文件的文件名。文件名中的空格将被删除。当文件被隔离时，它会被添加一个 32 比特的校验和并用以下格式存贮在 FortiGate 硬盘上： <32bit CRC>.< 被处理过的文件名 > 例如，一个名为 Over Size.exe 的文件按以下格式存储： 3fc155d2.oversize.exe。
隔离日期	文件被隔离时的日期和时间，按如下格式存储：天天 / 月月 / 年年年年 时时 : 分分。如果这个文件存在多个副本，这个时间指的是第一个被隔离的文件被存储的时间。
服务	被隔离的文件所用的协议 (HTTP, FTP, IMAP, POP3, SMTP)。
状态	用颜色表示的状态指示： t 红：文件被感染 t 黄：文件被启发式扫描捕获 t 绿：文件被阻塞样板所阻塞 t 蓝：文件大小超过了限制 Fortinet 建议您将状态为黄色的文件发送到 Forti 响应中心，因为这些文件可能含有新的病毒或已知病毒的变种。
状态描述	指出与状态相关的信息。例如 “文件被 ‘W32/Klez.h’ 病毒感染”或 “文件被文件阻塞样板所阻塞”。
DC	副本数统计。统计出文件一共被重复地隔离了多少次。如果 DC 迅速地增加则很有可能是某种病毒发作了。
TTL	以 时时 : 分分 表示的剩余时间。当 TTL 耗尽时，FortiGate 设备自动删除文件。对于重复的文件，每新发现一个副本都将刷新 TTL。
修改	您可以删除或下载这个文件。当您下载一个文件时，它将以原始的格式传输。

注意：在文件存在副本的情况下，除了 TTL 之外，所有的项目只与最初被隔离的文件有关。TTL 则在每次发现一个新的副本的时候被刷新一次。重复文件 （基于校验和）不被存储，但是每个文件的内部计数器将记录文件重复的次数。

隔离列表排序

您可以根据状态 （感染或阻塞）、服务 (IMAP, POP3, SMTP, FTP, 或 HTTP)，文件名的字母顺序、隔离日期、剩余时间 (TTL) 或副本数将隔离列表排序。

1 进入 **病毒防护 > 隔离**。

2 在列表排序中选择一个列标题以将列表排序。

3 单击应用。

过滤隔离列表

您可以将隔离列表过滤以控制它的显示：

- 只显示被阻塞的文件
- 只显示被感染的文件
- 只显示在 IMAP, POP3, SMTP, FTP, 或 HTTP 通讯中被阻塞和被感染的文件

从隔离区中删除文件

1 进入 **病毒防护 > 隔离**。

2 单击删除  以从列表中删除被隔离的文件。

下载被隔离的文件

1 进入**病毒防护 > 隔离**。

2 单击下载  以原始格式下载被隔离的文件。

配置隔离选项

您可以指定 FortiGate 设备是否隔离被感染的文件、被阻塞的文件或两者都隔离。您可以指定从网页、FTP 和电子邮件通讯中进行隔离。您还可以设置文件的有效期限，文件的最大尺寸和当 FortiGate 设备的硬盘满时如何处理文件。

1 进入**病毒防护 > 隔离 > 隔离配置**。

2 对于每种通讯协议，单击隔离被感染的文件和隔离被阻塞的文件核选框。
FortiGate 设备在选定的通讯中隔离被感染和被阻塞的文件。

注意：隔离阻塞文件的选项不适用于 HTTP 或 FTP，因为在文件名在请求时已经被阻塞了并且这个文件不被下载到 FortiGate 设备。

3 输入以小时为单位的有效期限（TTL）以指定文件在隔离区中保存的时间。
最大时间是 480 小时。当 TTL 达到 00:00 时 FortiGate 设备自动删除文件。

4 输入隔离区中被隔离文件尺寸的最大值（兆字节）。FortiGate 设备保留现有的大小超过了这一限制的被隔离的文件。FortiGate 设备不再隔离任何新的大小超过这一限制的文件。文件大小范围是 1-499 兆字节。输入零将不限制文件的大小。

5 选择硬盘空间过低复选框以指定当 FortiGate 设备的硬盘将满的时候如何处理要被隔离的文件。
您可以选择覆盖最老的文件或丢弃新的被隔离的文件。

6 单击应用。

阻塞过大的文件和电子邮件

您可以将 FortiGate 配置为使用 1% 到 15% 的可用内存来缓冲过大的文件和电子邮件。FortiGate 设备将阻塞超过这一大小限制的文件和电子邮件，而不是对它们进行病毒扫描和直接发送服务器或用户。FortiGate 设备会将过大的文件替换为一条替换信息发送给 HTTP 或电子邮件代理客户端。

配置文件或电子邮件大小限制

1 进入 病毒防护 > 配置 > 配置。

2 以兆字节为单位输入大小限制。

3 单击应用。

对邮件片段免除阻塞

分割的邮件是一个很大的邮件，通常被分割成多个部分分别发送，在接收端再重新组合起来。默认情况下当防病毒保护被启用的时候，FortiGate 阻塞被分割的邮件，把他们替换为邮件阻塞信息发送给接收方。建议您禁用电子邮件客户端软件的邮件分割功能。

为了避免病毒防护功能自动阻塞被分割的邮件，您可以启用邮件内容协议（SMTP、POP3 和 IMAP）的传递邮件碎片功能。

警告：FortiGate 不能扫描邮件碎片中的病毒或者使用文件名样板从这些邮件中删除文件。

按以下方法将 FortiGate 设备配置为传递邮件片段：

1 在内容配置文件中启用邮件片段传递。

2 在防火墙策略中选种 病毒防护和网页过滤。例如，要传递由内部网络用户到外部网络的邮件片段，选择一个内部到外部的策略。

3 对您希望 FortiGate 设备扫描的策略，选择一个已经启用了邮件片段传递的内容配置文件。

查看病毒列表

使用以下操作可以显示当前病毒定义库列表中的病毒和蠕虫列表。

1 要显示病毒列表，进入 **病毒防护 > 配置 > 病毒列表。**

2 卷动病毒和蠕虫列表可以查看列表中的所有病毒和蠕虫名称。

网页内容过滤

在防火墙策略中可以启用网页内容过滤功能。您在一个防火墙策略中启用了防病毒和网页过滤功能后，可以选择一个内容配置文件以控制对 HTTP 通讯的网页过滤方式。内容配置文件控制以下类型的内容过滤：

- 阻塞不受欢迎的 URL，
- 阻塞不受欢迎的内容，
- 从网页中删除脚本，
- 从阻塞列表中排除 URL。

您还可以使用 Cerberian URL 阻塞功能阻塞不受欢迎的 URL。详细信息请见 第 235 页 “ 使用 Cerberian 网页过滤器” 。

本章描述了以下内容：

一般配置步骤

配置网页内容过滤功能通常包括以下两个步骤：

1 在一个新的或现有的内容配置文件中选中网页过滤选项。请见 第 163 页 “ 添加一个内容配置文件” 。

2 对于允许 HTTP 连接通过 FortiGate 设备的防火墙策略，选中该策略的防病毒和网页过滤选项。

- 对您希望应用网页过滤功能的防火墙策略选择一个能提供网页过滤功能的内容配置文件。请见 第 165 页 “ 将内容配置文件添加到策略” 。

3 配置网页过滤的设置，以控制 FortiGate 设备将网页过滤功能应用到该防火墙策略接受的 HTTP 通讯的方式。请见：

- 第 233 页 “ 阻塞对 URL 的访问” ，
- 第 235 页 “ 使用 Cerberian 网页过滤器” ，
- 第 232 页 “ 内容阻塞” ，
- 第 238 页 “ 脚本过滤” ，
- 第 239 页 “ URL 排除列表” 。

4 配置当 FortiGate 设备阻塞不受欢迎的内容或不受欢迎的 URL 的时候用户收到的信息。请见 第 133 页 “ 定制替换信息” 。

5 配置 FortiGate 设备在阻塞或删除一个受感染的文件的时候发送一封报警邮件。请见 *日志配置和参考指南*中的 “配置报警邮件”。

注意：要接收网页过滤日志消息，请见 *日志配置和参考指南*中的 “配置日志记录”关于日志消息的内容和格式，请见 *日志配置和参考指南*中的 “网页过滤日志消息”。

内容阻塞

当 FortiGate 阻塞某个网页时，对那个被阻塞了的网页发出请求的用户会收到一个阻塞信息，同时 FortiGate 会在网页过滤日志中写入一条消息。

您可以使用多种语言在禁忌词汇列表中添加词汇和短语。可以使用西方语言、简体中文、繁体中文、日文或者韩文字符集。.

在禁忌词汇列表中添加单词或短语

1 进入 **Web 过滤器 > 内容阻塞**。

2 单击 **新建** ，在禁忌词汇列表中添加新的词汇或短语。

3 选择禁忌词汇或短语使用的语言或字符集。

您可以选择西方语言、简体中文、繁体中文、日文或是韩文。

您的电脑和网页浏览器必须也被配置为支持您所选择的字符集。

4 输入禁忌词汇或者短语。

如果您输入的是单个词汇 （例如，**禁忌**），FortiGate 将阻塞所有包含了这个词汇的网页。

如果输入的是一个短语 （例如，**禁忌 短语**），FortiGate 将阻塞所有同时包含这两个词汇的网页。当这个短语出现在禁忌词汇列表中时，FortiGate 将在两个词汇之间的空格处插入一个加号 (+) （例如，**禁忌 + 短语**）。

如果输入了一个被引号包围的短语 （例如，**“禁忌 词汇”**），FortiGate 将阻塞所有内容中包含这两个词汇并以一个短语的形式出现的网页。

内容过滤并不区分大小写字母。您也不能在禁忌词汇中包含特殊字符。

5 单击 **确定**。

这个词汇或短语就被添加进禁忌词汇列表了。

6 在禁忌词汇列表中的修改列上，选中新增加的条目旁边的核选框，FortiGate 将阻塞所有包含了这个词汇或短语的网页。

您可以输入多个禁忌词汇或者短语，然后单击 全部选中  从而一次激活禁忌词汇列表中的所有条目。

注意：要阻塞含有禁忌词汇的网页，内容配置文件的启用禁忌词汇一项必须被选中。

图 38: 禁忌词汇列表举例

阻塞对 URL 的访问

您可以使用 FortiGate 网页过滤功能或 Cerberian 网页过滤器阻塞不受欢迎的内容。

- 使用 FortiGate 网页过滤器
- 使用 Cerberian 网页过滤器

使用 FortiGate 网页过滤器

您可以阻塞某个网站的所有页面，只需要把顶级 URL 或者 IP 地址添加到阻塞列表。或者，您可以单独阻塞某个页面，方法是在阻塞列表里添加这个页面的整个路径和文件名。

本节讨论了：

- 在阻塞列表中添加 URL 或者 URL 样板
- 清除 URL 阻塞列表
- 下载 URL 阻塞列表
- 上载 URL 阻塞列表

在阻塞列表中添加 URL 或者 URL 样板

1 进入 **Web 过滤器** > **URL 阻塞**。

2 单击 **新建** ，在 URL 阻塞列表中添加新的条目。

3 输入要阻塞的 URL。

输入一个顶级 URL 或者 IP 地址可以阻塞对一个站点上所有网页的访问。例如，`www.badsite.com` 或者 `122.133.144.155` 阻塞了对这个站点上所有网页的访问。

输入一个顶级 URL 后面加上路径和文件名可以阻塞对这个站点中单个页面的访问。例如， `www.badsite.com/news.html` 或者 `122.133.144.155/news/html` 阻塞了对这个站点中 news 页面的访问。

要阻塞一个含有 `badsite.com` 结尾的 URL 中的所有页面，把 `badsite.com` 添加进阻塞列表。例如，添加 `badsite.com` 阻塞了对 `www.badsite.com,mail.badsite.com,www,finace,badsite.com` 等等站点的访问。

注意： 不要在要阻塞的 URL 中包含 http://。 不要使用星号 （*）来代表任意字符。您可以输入一个顶级域名的后缀（例如，不带前边的 “.” 的 “com”）以阻塞所有带有这个后缀的 URL 的访问。

注意： URL 阻塞不能阻塞用户可以用网页浏览器访问的其它服务。例如，URL 阻塞不能阻塞对 `ftp://ftp.badsite.com` 的访问。在这种情况下，您可以使用防火墙策略来拒绝 FTP 连接。

4 选择 **启用** 以阻塞 URL/URL 样板。

5 单击 **确定** 把这个 URL/ 样板添加到 URL 阻塞列表。

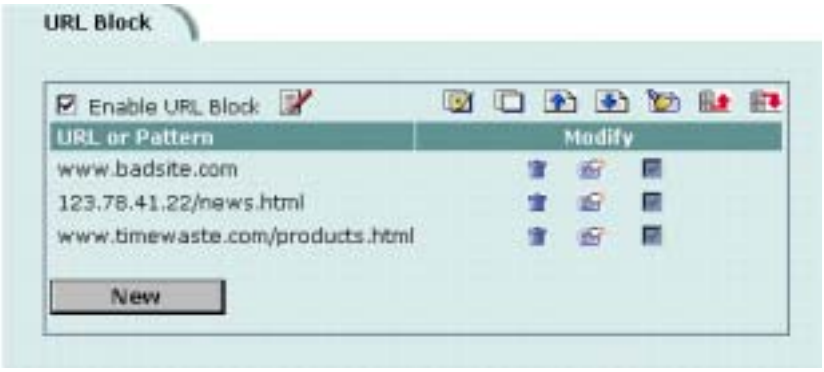
您可以输入多个 URL 然后单击**全部选中** 一次激活 URL 阻塞列表中的所有条目。

URL 阻塞列表的每一页可以显示 100 个 URL。

6 您可以使用 **向下翻页** 和 **向上翻页** 在 URL 阻塞列表中翻页浏览。

注意： 内容配置文件的启用 URL 阻塞必须被选中，对 URL 阻塞列表中的 URL 的阻塞才能生效。

图 39: URL 阻塞列表的例子



清除 URL 阻塞列表

1 进入 **Web 过滤器 > URL 阻塞**

2 选择 **清除 URL 阻塞列表** 以删除 URL 阻塞列表中的所有 URL。

下载 URL 阻塞列表

您可以将 URL 阻塞列表备份，方法是将它下载到管理员电脑上保存为文本文件。

1 进入 **Web 过滤器** > **URL 阻塞**。

2 选择 **下载 URL 阻塞列表**  。

FortiGate 将把 URL 阻塞列表下载到控制电脑上保存为一个文本文件。您可以指定保存文本文件的位置和文件名。

上载 URL 阻塞列表

您可以用一个文本编辑器创建一个 URL 阻塞列表然后把这个文本文件上载到 FortiGate。在文本文件中每个 URL 占独立的一行。您可以在 URL 后面加上一个空格然后加上一个 1 来启用它或者一个零 （0）来禁用这个 URL。如果您不添加不在文本文件中添加这些信息，FortiGate 将自动启用您所上载的文本文件中的所有的 URL。

图 40: URL 阻塞列表的文本文件举例

```
www.badsite.com/index 1
www.badsite.com/products 1
182.63.44.67/index 1
```

您可以创建您自己的 URL 阻塞列表，也可以使用由第三方 URL 阻塞或者黑名单服务创建的 URL 阻塞列表。例如，您可以从 http://www.squidguard.org/blacklist/ 下载 squidGuard 的黑名单，以此作为起点创建您自己的 URL 阻塞列表。 squidGuard 的机器人每周三次搜索万维网并在黑名单中添加新的 URL。您可以把 squidGuard 的黑名单作为文本文件上载到 FortiGate，仅仅需要做一点儿小改动：删除每个名单顶部的注释并把您需要的名单组合成一个单独的文本文件。

注意：当您上载一个新的 URL 阻塞列表时，用基于 Web 的管理程序对 URL 阻塞列表所做的任何改动都将丢失。但是您可以先下载当前的 URL 阻塞列表，使用文本编辑器修改它，添加一些新的 URL 然后再把它上载到 FortiGate。

1 在文本编辑器中，创建要阻塞的 URL 和样板列表。

2 使用基于 Web 的管理程序，进入 **Web 过滤器** > **URL 阻塞**。

3 选择 **上载 URL 阻塞列表**  。

4 输入您的 URL 阻塞列表文件的路径和文件名，或者单击浏览然后在浏览器中定位文件。

5 单击 **确定** 以上载文件到 FortiGate。

6 单击 **返回** 以显示更新过的 URL 阻塞列表。

URL 阻塞列表的每一页可以显示 100 个 URL。

7 您可以使用 **向下翻页**  和 **向上翻页**  按钮在 URL 阻塞列表中浏览。

8 您可以继续维护 URL 列表，修改文本文件然后再次上载它。

使用 Cerberian 网页过滤器

FortiGate 设备支持 Cerberian 网页过滤器。关于 Cerberian 网页过滤器的更进一步信息请见 www.cerberian.com。

注意：如果您的 FortiGate 设备运行于主动 - 被动 HA 模式，在这个簇中的每个 FortiGate 设备必须有它自己的 Cerberian 许可证。在主动 - 主动 HA 模式下不支持 Cerberian 网页过滤器。有关 HA 的信息请见 第 55 页 “ 高可用性” 。

如果您为您的 FortiGate 设备购买了 Cerberian 网页过滤功能，按照以下步骤为 FortiGate 设备配置 Cerberian 网页过滤器。

一般配置步骤

要使用 Cerberian 网页过滤器，您需要：

1 安装 Cerberian 网页过滤器许可密钥。请见 第 236 页 “ 在 FortiGate 设备上安装 Cerberian 许可密钥” 。

2 添加要使用 Cerberian 网页过滤器的用户。请见 第 236 页 “ 在 FortiGate 设备中添加一个 Cerberian 用户” 。

3 配置 Cerberian 网页过滤器。请见 第 235 页 “ 使用 Cerberian 网页过滤器” 。

4 启用 Cerberian URL 过滤。请见 第 235 页 “ 使用 Cerberian 网页过滤器” 。

注意：要使用 Cerberian 网页过滤，FortiGate 设备必须能够访问互联网。

在 FortiGate 设备上安装 Cerberian 许可密钥

在您使用 Cerberian 网页过滤之前，您必须安装一个许可密钥。许可密钥决定了可以通过这个 FortiGate 设备使用 Cerberian 网页过滤功能的最终用户数。

1 进入 **网页过滤 >URL 阻塞。**

2 选择 Cerberian URL 过滤。

3 输入许可证号。

4 单击应用。

在 FortiGate 设备中添加一个 Cerberian 用户

Cerberian 网页过滤策略只能应用到用户组。您可以在 FortiGate 设备上添加用户，然后将用户添加到 Cerberian 管理网页站点的用户组。

当最终用户试图访问某个 URL 的时候，FortiGate 设备将检查用户的 IP 地址是否在 FortiGate 设备的 IP 地址列表中。如果用户 IP 地址在列表中，这个 URL 访问请求将被发送到 Cerberian 服务器。否则，将发送给这个用户一条错误信息，声明这个用户没有访问 Cerberian 网页过滤器的许可。

1 进入 **网页过滤 >URL 阻塞**。

2 选择 Cerberian URL 过滤。

3 单击新建。

4 输入用户的 IP 地址和网络掩码。您可以输入单一用户的 IP 地址。例如，192.168.100.19/255.255.255.255。也可以输入一组用户的一个子网地址。例如，192.168.100.0/255.255.255.0。

5 输入用户的别名。当您在 Cerberian 服务器的用户组中添加用户的时候可以使用这个别名。如果您不输入别名，用户的 IP 将被作为别名并添加到 Cerberian 服务器的默认组里。

6 单击确定。

配置 Cerberian 网页过滤

您在 FortiGate 设备中添加了 Cerberian 网页过滤用户之后，可以将用户添加到 Cerberian 网页过滤服务器的用户组中。然后您可以创建策略并将策略应用到这个用户组。

关于默认组和策略

在 Cerberian 网页过滤器中存在一个默认用户组，并和默认策略关联。

您可以在默认组中添加用户，并将任何策略应用到这个组。

默认组可以用于：

- 所有在 FortiGate 设备中没有指派别名的用户。
- 所有没有添加到其他用户组的用户。

Cerberian 网页过滤器将网页分成 53 类。默认的策略阻塞 12 类的 URL。您可以修改默认策略并将他应用到任何用户组。

按以下方法配置 Cerberian 网页过滤

1. 根据您添加到 FortiGate 设备的别名将用户添加到 Cerberian 服务器的用户组。因为网页策略只能应用到用户组。如果您没有为 FortiGate 设备中的用户 IP 输入别名，用户 IP 自动添加到默认组中。
2. 选择您要阻塞的网页类别，创建您册策略。
3. 将策略应用到包含这个用户的用户组。

详细的步骤，请见 Cerberian 网页过滤页面的在线帮助。

启用 Cerberian URL 过滤

您添加了 Cerberian 用户 / 用户组并配置了 Cerberian 网页过滤之后，可以启用 CerberianURL 过滤功能。您必须在以下三个地方启用它：

- Cerberian URL 过滤页面。
- 内容配置文件。
- 使用内容配置文件的策略。

1. 进入 **网页过滤 >URL 阻塞。**
2. 选择 Cerberian URL 过滤。
3. 单击 Cerberian URL 过滤选项。
4. 进入 **防火墙 > 内容配置文件。**
5. 创建新的内容配置文件或选择现有的内容配置文件，启用网页 URL 阻塞。
6. 进入 **防火墙 > 策略。**
7. 创建一个新的策略或选择现有的策略以应用内容配置文件。
8. 选择病毒防护和网页过滤。
9. 从内容配置文件列表中选择内容配置文件。
10. 单击确定。

脚本过滤

使用以下方法可以将 FortiGate 配置为从网页中删除脚本。您可以将 FortiGate 配置为阻塞 java 小程序、cookies 和 ActiveX。

注意：阻塞这些内容中的任何一项都可能会使得某些网页无法正常工作。

启用脚本过滤

1 进入 **防火墙 > 内容配置文件。**
2 选择您要启用脚本过滤的内容配置文件。
3 单击脚本过滤。
4 单击确定。

选择脚本过滤选项

1 进入 **Web 过滤器 > 脚本过滤**。
2 选择您要启用的脚本过滤选项。
您可以阻塞 java 小程序、cookies 和 ActiveX。
3 单击 **应用** 。

图 41: 脚本过滤设置为阻塞 java 小程序和 ActiveX 的例子

URL 排除列表

在 URL 排除列表中添加的 URL 是为了避免正常的数据流被内容过滤或 URL 过滤功能意外地阻塞掉。例如，如果内容过滤被设置为阻塞含有关于色情描写的词汇而一个著名的站点上有一个色情故事，那么这个站点上的全部网页就会被阻塞。把这个站点的 URL 添加到 URL 排除列表里就可以避免内容阻塞功能对这个站点上的网页的阻塞。

注意：从被排除的 URL 上下载的内容将不会被防病毒保护功能扫描或阻塞。

在 URL 排除列表中添加 URL

1 进入 **Web 过滤器** > **排除 URL**。

2 选择 **新建** 在 URL 排除列表中添加新的 URL。

3 输入要排除的 URL。

输入一个包括路径和文件名的完整的 URL，可以排除对这个站点上的这个网页的阻塞。例如， `www.goodsite.com/index.html` 可以排除对这个站点的主页的阻塞。您也可以指定 IP 地址，例如， `122.63.44.67/index.html` 可以免除对这个地址的站点上的主页的阻塞。不要在排除的 URL 前面加上 `http://`。

排除一个顶级的 URL，例如 `www.goodsite.com`，可以排除任何内容阻塞规则和 URL 阻塞规则对这个站点上的任何网页 （例如， `www.goodsite.com/badpage`）的阻塞。

注意：排除一个顶级的 URL 不能从所有内容阻塞规则和 URL 阻塞规则中排除诸如 `mail.goodsite.com` 这类的页面，除非您把 `goodsite.com` 添加到 URL 排除列表里去。

4 选择 **启用** 以排除这个 URL。

5 单击 **确定** 把 URL 添加到 URL 排除列表。

您可以输入多个 URL 然后单击 全部选中 一次激活 URL 排除列表中的所有 URL。URL 排除列表中的每页可以显示 100 个 URL。

6 使用 **向下翻页** 和**向上翻页** 可以浏览整个 URL 排除列表。

图 42: URL 排除列表的例子

电子邮件过滤

防火墙策略中可以使用电子邮件过滤。当您在一个防火墙策略中启用了病毒防护和网页过滤，您可以选择一个内容配置文件用来控制电子邮件过滤功能如何处理邮件（IMAP 或 POP3）通讯。内容配置文件用以下方式识别不受欢迎的电子邮件并提供保护：

- 过滤不受欢迎的发件人地址模板，
- 过滤不受欢迎的内容，
- 从阻塞中排除发件人地址模板。

本章叙述了如下内容：

一般配置步骤

配置邮件过滤包括通常如下步骤：

1. 在一个新的或现有的内容配置文件中选择邮件过滤选项。请见 第 163 页 “添加一个内容配置文件”。
2. 对允许通过通过 FortiGate 设备传输 IMAP 和 POP3 连接的防火墙策略选择病毒防护和网页内容过滤选项。选择一个提供了您所需要的电子邮件过滤功能的内容配置文件应用到防火墙策略中。请见 第 165 页 “将内容配置文件添加到策略”。
3. 对不受欢迎的电子邮件添加一个主题标签，使邮件接收者可以使用他们的邮件客户软件根据这个标签对邮件进行过滤。请见 第 244 页 “添加一个主题标签”。

注意：要接收电子邮件过滤日志消息，请见 *FortiGate 日志配置和参考指南*中的“配置日志”。关于电子邮件过滤日志消息的分类和格式的详细信息，请见 *FortiGate 日志配置和参考指南*中的“日志消息”。

电子邮件禁忌词汇列表

当 FortiGate 设备检测到在电子邮件中含有禁忌词汇列表中的词汇或短语时，FortiGate 设备将在这封电子邮件的主题中添加一个标签，并在事件日志中写入一条消息。接收者可以使用他们的电子邮件客户端软件根据主题中的标签过滤邮件。

您可以用西方字符集、简体中文、繁体中文、日文、或韩文字符集使用多种语言在列表中添加禁忌词汇。

在禁忌词汇列表中添加单词或短语

1 进入 **Web 过滤器 > 内容阻塞**。

2 单击 **新建** ，在禁忌词汇列表中添加新的词汇或短语。

3 输入禁忌词汇或者短语。

如果您输入的是单个词汇 （例如，**禁忌**），FortiGate 将标记所有包含了这个词汇的 IMAP 和 POP3 电子邮件。

如果输入的是一个短语 （例如，**禁忌 短语**），FortiGate 将标记所有同时包含这两个词汇的 IMAP 和 POP3 电子邮件。当这个短语出现在禁忌词汇列表中时，FortiGate 将在两个词汇之间的空格处插入一个加号 (+) （例如，**禁忌 + 短语**）。

如果输入了一个被引号包围的短语 （例如，**“禁忌 词汇”**），FortiGate 将标记所有内容中包含这两个词汇并以一个短语的形式出现的 IMAP 和 POP3 电子邮件。

内容过滤并不区分大小写字母。您也不能在禁忌词汇中包含特殊字符。

4 选择禁忌词汇或短语使用的语言或字符集。

您可以选择西方语言、简体中文、繁体中文、日文或是韩文。

您的电脑和网页浏览器必须也被配置为支持您所选择的字符集。

5 单击启用。

6 单击确定。

这个词汇或短语就被添加进禁忌词汇列表了。

您可以输入多个禁忌词汇或者短语，然后单击 全部选中  从而一次激活禁忌词汇列表中的所有条目。

注意：必须选中 IMAP 或 POP3 邮件的内容配置文件的邮件内容阻塞功能以对含有禁忌词汇的邮件添加标记。

电子邮件阻塞列表

您可以将 FortiGate 设备配置为对所有不受欢迎的地址发来的 IMAP 和 POP3 协议的通讯添加标记。当 FortiGate 设备检测到一封邮件的发件人符合不受欢迎地址模板时，FortiGate 设备将在这封邮件的主题中添加一个标签，并在邮件过滤日志中写入一条消息。接收者可以使用他们的邮件客户端软件根据主题中的标签过滤邮件。

您可以根据指定的发件人地址标记邮件，或者添加一个顶级域名以阻止所有子域的地址。或者，您可以添加子域名以标记从单一子域发来的邮件。

在邮件阻塞列表中添加地址模板

1 进入**邮件过滤器 > 阻塞列表。**

2 单击新建在邮件阻塞列表中添加新的模板。

3 输入一个阻塞模板。
- 要标记来自一个特定地址的所有邮件，只需输入这个邮件的地址。例如，sender@abccompany.com。
- 要标记从特定域来的邮件，输入域名。例如，abccompany.com。
- 要标记从特定子域来的邮件，输入子域名。例如，mail.abccompany.com。
- 要标记从某一类地址来的全部邮件，输入顶级域名。例如，输入 com 可以标记所有使用 .com 作为顶级域名的组织。

模板可以包含数字 (0-9)，大写或小写字母 (A-Z，a-z)，以及特殊字符 - 和 _，还有 @。不能使用其他特殊字符和空格。

4 单击启用以标记与阻塞模板匹配的电子邮件。

5 单击确定在邮件阻塞列表中添加地址。

您可以输入多个地址模板然后单击全部选中  一次启用邮件阻塞列表中的所有模板。

您还可以单击启用列的核选框以启用邮件阻塞列表中的任意模板。

邮件排除列表

在排除列表中添加地址模板可以避免合法的 IMAP 和 POP3 通讯被阻塞或添加标记。例如，如果邮件禁忌词汇列表中设置了阻塞含有与色情相关的词汇，而一个著名的公司发送的邮件中含有这些词汇，FortiGate 设备将在这封邮件中添加标签。将这个著名的公司的域名添加到排除列表可以避免这个公司的 IMAP 和 POP3 通讯被阻塞或添加标签。

在邮件排除列表中添加地址模板

1 进入 **邮件过滤器 > 排除列表。**

2 单击新建在邮件排除列表中添加地址模板。

3 输入要排除的地址模板。
- 要排除来自一个特定地址的所有邮件，只需输入这个邮件的地址。例如，sender@abccompany.com。
- 要排除从特定域来的邮件，输入域名。例如，abccompany.com。
- 要排除从特定子域来的邮件，输入子域名。例如，mail.abccompany.com。
- 要排除从某一类地址来的全部邮件，输入顶级域名。例如，输入 com 可以标记所有使用 .com 作为顶级域名的组织。

模板可以包含数字 (0-9)，大写或小写字母 (A-Z，a-z)，以及特殊字符 - 和 _，还有 @。不能使用其他特殊字符和空格。

4 单击启用以排除地址模板。

5 单击确定将地址模板添加到邮件排除列表。

您可以输入多个地址模板然后单击全部选中  一次启用邮件排除列表中的所有模板。

您还可以单击启用列的核选框以启用邮件排除列表中的任意模板。

添加一个主题标签

当 FortiGate 设备从一个不受欢迎的地址收到电子邮件、或收到含有邮件禁忌词汇列表中的词汇的邮件的时候，FortiGate 设备将在主题中添加一个标签并将消息发送到邮件的目的地址。邮件用户可以使用他们的电子邮件客户端软件根据主题中的标签过滤电子邮件。

按以下方法添加主题标签

1 进入 **电子邮件过滤 > 配置。**

2 输入您希望在主题栏显示的标签。这一标签将显示在从不受欢迎的地址受到的邮件或含有禁忌词汇的邮件的主题栏中。例如，输入 “不受欢迎的邮件”。

注意：不要在主题标签中使用引号。

3 单击应用。

FortiGate 设备将在所有不受欢迎的邮件的主题栏中添加这一标签。

日志和报告

您可以将 FortiGate 设备配置为记录网络的各种活动，从常规配置的改变和通讯会话直到紧急事件。您还可以将 FortiGate 设备配置为发送警报邮件消息以提醒系统管理员当前发生的事件，例如网络攻击，病毒入侵以及防火墙和 VPN 事件。

本章描述了以下内容：

记录日志

通过配置日志可以在以下一个或多个地点记录日志：

- 运行系统日志服务的电脑。
- 运行 WebTrends 防火墙报告服务的电脑。
- FortiGate 的硬盘 （如果您的 FortiGate 内装有硬盘）。
- 控制台。

如果您的 FortiGate 设备没有配备硬盘，您也可以将日志配置为将事件、攻击、防病毒、网页过滤和电子邮件过滤日志记录到 FortiGate 系统内存里。把日志记录到内存允许快速地访问最近记录的日志条目。如果 FortiGate 重新启动，所有的日志条目都会丢失。

您可以将不同级别的日志记录到不同的位置。例如，您可能希望只将紧急消息和警报消息记录到 FortiGate 内存，而将其他级别的消息记录到一个远程计算机上。

关于过滤日志类型和 FortiGate 设备记录日志的方式的详细信息，请见 第 248 页 “ 过滤日志消息” 。关于通讯日志的信息，请见 第 249 页 “ 配置通讯日志” 。

本节描述了以下内容：

在远程电脑上记录日志

以下操作用于将 FortiGate 配置为将日志消息记录到一台远程电脑上。这台远程电脑必须配置为一个系统日志服务器。

1 进入 **日志与报告 > 日志设置**。

2 选择 **记录日志到远程主机** 以发送日志到一个日志服务器上。

3 输入运行系统日志服务器软件的远程主机的 **IP 地址** 。

4 输入系统日志服务器的端口号。

5 选择您希望记录到日志的消息的紧急程度。

FortiGate 会将所有不低于您所选择的级别的消息记录进日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误。

6 单击配置策略。

- 选择您希望 FortiGate 设备记录的日志的类型。
- 对于每一种日志类型，选择选择您希望 FortiGate 设备进行的记录操作。
- 单击确定。

关于日志类型和记录活动的详细信息请见 第 248 页 “ 过滤日志消息” 和 第 249 页 “ 配置通讯日志” 。

7 单击应用。

在 NetIQ WebTrends 服务器上记录日志

以下操作可以将 FortiGate 配置为在一台远程的 NetIQ 防火墙报告服务器上记录日志，以供存储和分析之用。FortiGate 日志的格式服从 Web Trends Enhanced Log（WELF）格式规范，并与 Web Trends NetIQ 安全报告中心 2.0 和防火墙套件 4.1 兼容。可以从安全报告中心和防火墙套件的文档中获得更详细的信息。

注意：FortiGate 通讯日志消息包括发送和接收域，这些内容是在日志记录中可选的，但是是绘制 WebTrends 图表所必须的内容。

以下操作将日志记录到一台 NetIQ Web Trends 服务器上：

1 进入 **日志与报告 > 日志设置**。

2 选择 **以 Web Trends Enhanced 日志格式记录日志**。

3 输入 NetIP WebTrends 防火墙报告中心的 **IP 地址**。

4 选择您希望记录到日志的消息的紧急程度。

FortiGate 会将所有不低于您所选择的级别的消息记录进日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误。

5 单击配置策略。

要对 FortiGate 过滤的日志类型和记录的事件进行配置，按照 第 248 页 “ 过滤日志消息” 和 第 249 页 “ 配置通讯日志” 中的步骤操作。

6 单击应用。

将日志记录到 FortiGate 硬盘

如果您的系统中安装了硬盘，您可以将日志文件记录到硬盘里。

以下操作设置日志的记录方式为记录到硬盘：

1 进入**日志与报告 > 日志设置**。

2 选择 记录到本地 。

3 输入一个日志文件的 最大值（以兆字节为单位）。
当日志文件的大小达到这一最大值的时候，当前日志文件将被保存并关闭。系统将创建一个新的当前日志文件用来记录日志。默认的最大系统日志文件的大小是 10M 字节，您可以设置的最大值为 2G 字节。

4 输入一个创建日志的 时间间隔 （以天为单位）
在达到指定的时间间隔后，当前日志文件将被保存和关闭，一个新的文件被创建。默认的时间间隔是 10 天。

5 选择您希望记录到日志的消息的紧急程度。
FortiGate 会将所有不低于您所选择的级别的消息记录进日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误。

6 单击配置策略。
要对 FortiGate 过滤的日志类型和记录的事件进行配置，按照 第 248 页 “过滤日志消息” 和 第 249 页 “配置通讯日志” 中的步骤操作。

7 设置当磁盘被写满时的日志选项：

覆盖	当硬盘满的时候删除最早的日志文件。覆盖是默认的选项。
阻塞数据流	当硬盘被写满的时候阻塞所有的网络流通。
不记录日志	当硬盘被写满的时候停止记录日志消息。

8 单击 应用 保存您的日志设置。

将日志记录到系统内存

如果您的 FortiGate 没有安装硬盘，您可以使用以下操作将 FortiGate 配置为保留一些系统内存用来记录当前的事件日志、攻击日志、防病毒、网页过滤、电子邮件日志消息。将日志记录到内存允许对近期的日志条目进行快速访问。FortiGate 可以在系统内存中保留有限的日志消息。一旦所有的可用内存都被用掉了，FortiGate 会删除最早的日志消息。如果 FortiGate 重新启动，所有的记录都会丢失。

注意：FortiGate 设备只能在系统内存中记录事件日记和攻击日志。

以下操作可以将日志设置为记录到内存：

1 进入 **日志与报告 > 日志设置**。

2 选择 **在内存中记录日志**。

3 选择您希望记录到日志的消息的紧急程度。
FortiGate 会将所有不低于您所选择的级别的消息记录进日志。例如，如果您希望记录紧急、警报、危险和错误消息，选择错误。

4 单击配置策略。
要对 FortiGate 过滤的日志类型和记录的事件进行配置，按照 第 248 页 “过滤日志消息” 中的步骤操作。

5 单击应用。

过滤日志消息

您可以选择记录哪种日志和在每种日志中记录哪类消息。

1 进入 **日志和报告 > 日志设置。**

2 选择配置策略设置您在 第 245 页 “ 记录日志” 选择的日志记录位置。

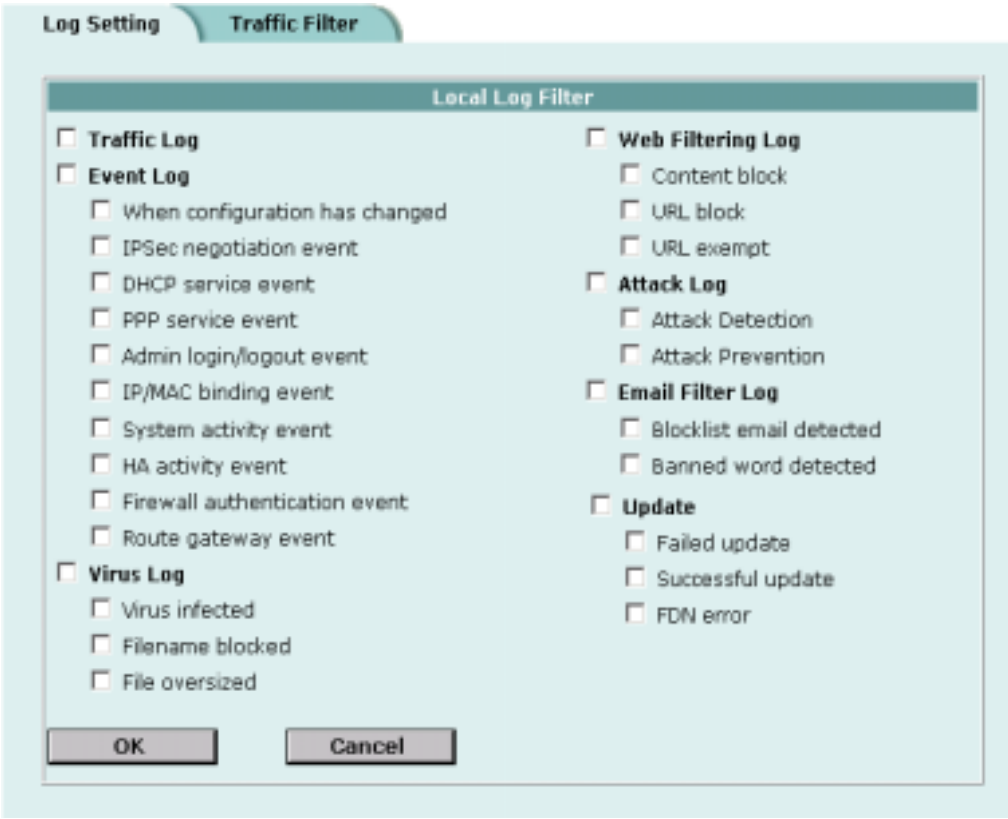
3 选择您希望 FortiGate 设备记录的日志类型。

通讯日志	记录所有到该接口和通过该接口的连接。 要配置通讯过滤，请见 第 251 页 “ 添加通讯过滤的条目” 。
事件日志	将管理和活动事件记录到事件日志里。 管理事件包括系统配置的修改、管理员和用户的登录和注销。活动日志包括系统活动，例如建立 VPN 通道，HA 失效恢复事件。
病毒日志	记录病毒入侵事件，例如当 FortiGate 设备检测到一个病毒阻塞某个类型的文件，或者阻塞一个超大型的文件或电子邮件的时候，发生此事件。
网页过滤日志	记录系统活动事件，例如 URL 和内容阻塞，以及从阻塞的 URL 中排除指定的 URL。
攻击日志	记录由 NIDS 检测到的攻击和 NIDS 预防功能阻止的攻击企图。
电子邮件过滤日志	记录活动事件，例如检测到包含有不受欢迎的内容的邮件或者由不受欢迎的发件人发送的邮件。
更新	当 FortiGate 连接到 FDN 下载病毒防护和攻击更新的时候记录一条日志消息。

4 如果您在步骤 3 中选择了事件日志、病毒日志、网页过滤日志、攻击日志、电子邮件过滤日志或更新，您还需要选择希望 FortiGate 设备记录的消息的类型。

5 单击确定。

图 43: 日志过滤配置的例子



配置通讯日志

您可以将 FortiGate 设备配置为记录以下连接的通讯日志消息：

- 任意接口
- 任意防火墙策略

FortiGate 设备可以根据任何源地址、目的地址或服务类型对通讯日志进行过滤。您还可以起用以下全局设置：

- 将 IP 地址解析为主机名，
- 记录会话或包信息，
- 显示端口号或服务。

通讯过滤列表显示了过滤的通讯的名称、源地址、目的地址和协议类别。

本节描述了以下内容：

启用通讯日志

您可以对任何接口和任何防火墙策略启用日志记录。

在网络接口上启用通讯日志

如果您对某个网络接口启用了通讯日志记录，所有到此接口和通过此接口的网络连接将被记录进通讯日志。

1 进入 **系统 > 网络 > 接口**。
2 在你要启用日志记录的接口的一侧，单击修改列上的编辑  。
3 对日志，单击 启用。
4 单击确定。
5 对每个您希望启用日志记录功能的接口重复这一操作。

对防火墙策略启用通讯日志

如果您启用了某个防火墙策略的通讯日志记录，这个防火墙策略接受的全部连接都将被记录进通讯日志。

1 进入 防火墙 > 策略。
2 选择一个策略标签。
3 选择记录通讯日志。
4 单击确定。

配置通讯过滤设置

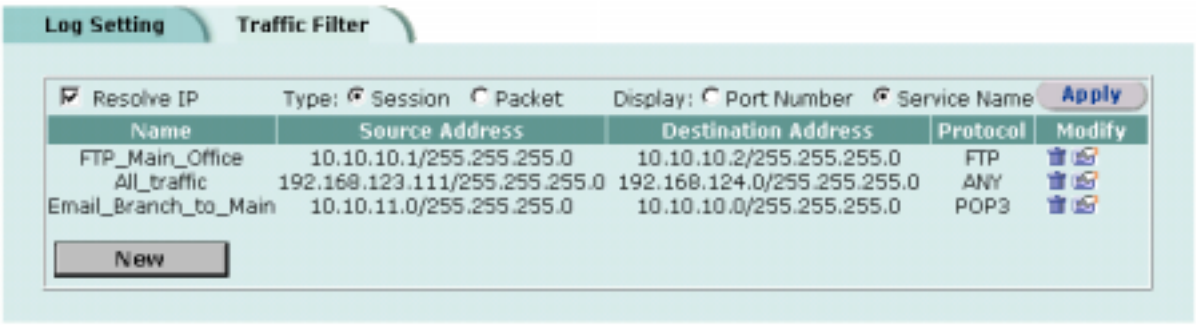
按照如下步骤配置在全部通讯日志消息中记录的信息。

1 进入 日志和报告 > **日志设置 > 通讯过滤。**
2 选择您要应用到所有通讯日志消息的设置。

解析 IP	如果您希望通讯日志消息列如 IP 地址和 DNS 服务器上所存储的域名，则选中解析 IP。如果您还没有添加由您的 ISP 提供的主 DNS 服务器和辅助 DNS 服务器的地址，请进入**系统 > 网络 >DNS** 并添加地址。
类型	选择 会话或包。如果您选择了会话，FortiGate 设备将每个会话发送和接收的包的数量。如果您选择了包，FortiGate 设备将记录每个会话的包的平均长度 （以字节为单位）。
显示	如果您希望通讯日志消息列出端口号，例如，80/TCP，则选择端口号。如果您希望通讯日志消息列出服务的名称，例如，TCP，则选择服务名称。

3 单击应用。

图 44: 通讯过滤列表的例子



添加通讯过滤的条目

在通讯过滤列表中添加条目可以过滤通讯日志记录的消息。如果您不在通讯过滤列表中添加任何条目，FortiGate 记录所有的通讯日志消息。您可以在通讯过滤列表中添加条目来限制通讯日志记录的内容。您可以选择记录来自某个指定源 IP 地址和网络掩码、到某个指定目的地址和掩码以及某个特定类型服务的通讯日志。通讯过滤条目可以包含源地址、目的地址和服务类型的任意组合。

按照以下步骤在通讯过滤列表中添加条目。

1 进入 **日志和报告 > 日志设置 > 通讯过滤**。

2 单击新建。

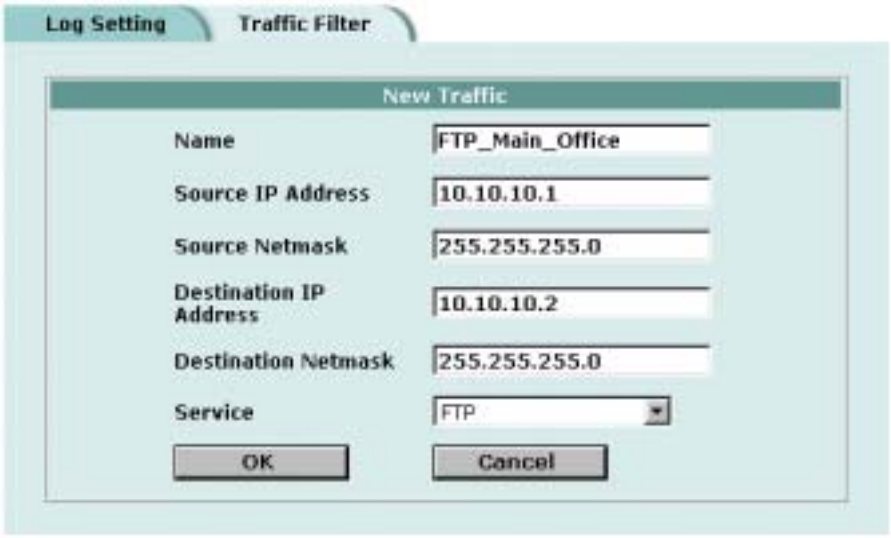
3 配置通讯过滤，选择您希望通讯日志记录的通讯的类型。

名称	输入一个名称以识别这个通讯过滤条目。 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 _。不能使用其他特殊字符和空格。
源 IP 地址 **源网络掩码**	输入您希望 FortiGate 设备记录通讯日志消息的源 IP 地址和网络掩码。地址可以是一个独立的主机、一个子网或者一个网络。
目的 IP 地址 **目的网络掩码**	输入您希望 FortiGate 设备记录通讯日志消息的目的 IP 地址和网络掩码。地址可以是一个独立的主机、一个子网或者一个网络。
服务	选择您希望 FortiGate 设备记录的通讯日志消息的服务组或单独的服务类型。

4 单击确定。

通讯过滤列表根据您在 第 250 页 “ 启用通讯日志” 中选择的设置显示新的通讯地址条目。

图 45: 新通讯地址条目的例子



查看记录到内存的日志

如果 FortiGate 被配置为在内存中记录日志。您可以使用基于 Web 的管理程序来查看、搜索和清除日志中的消息。本节讨论了：

- 查看日志
- 搜索日志

查看日志

在日志消息列表中，消息按照时间顺序排列，生成时间晚的消息排在上面。以下操作用于查看保存在系统内存中的日志消息：

1 进入**日志与报告 > 记录日志**。

2 选择 事件日志、攻击日志、防病毒日志、网页过滤日志或电子邮件过滤日志。
基于 Web 的管理程序列出保存在系统内存中的日志消息。

3 滚动窗口可以查看到更多的日志消息。

4 要查看日志中的某一行，只需在转到某行的空白处填写行号，然后单击 Go。

5 要在日志消息中翻页，单击 向下翻页 或 向上翻页 。

搜索日志

使用以下操作可以搜索保存在系统内存里的日志消息。

1 进入 **日志与报告 > 记录日志**。

2 选择 事件日志、攻击日志、防病毒日志、网页过滤日志或电子邮件过滤日志。

3 单击 可以在选定的日志中搜索消息。

4 选择 与 可以搜索与所有给定条件匹配的消息。

5 选择 或 可以搜索与某个或多个给定条件匹配的消息。

6 选择以下一个或多个搜索条件：

关键词	可以搜索包含在消息中的任何文字。关键词搜索中区分大小写字母。
时间	搜索日志中创建时间符合给定的年、月、日、小时条件的日志。

7 单击 确定 开始搜索

基于 Web 的管理程序 会显示出符合给定搜索条件的日志消息。您可以卷动窗口查看消息或者进行另一次搜索。

注意：在进行了一次搜索之后，如果想再次显示所有的日志消息，只需清空所有的搜索条件并再次执行搜索。

查看和管理保存在硬盘上的日志

如果您的 FortiGate 的日志是记录在硬盘上的，您可以用以下方法查看、搜索和维护日志：

- 查看日志
- 搜索日志
- 将日志文件下载到管理员电脑
- 删除当前日志中的全部消息
- 删除一个保存了的日志文件

查看日志

在日志消息列表中，最近生成的消息被排在最上面。您可以用以下操作查看活动的或者保存了的日志：

1 进入**日志与报告 > 记录日志**。

2 选择 事件日志、攻击日志、防病毒日志、网页过滤日志或电子邮件过滤日志。

基于 Web 的管理程序 列出选定类型的日志中已保存的全部消息，在列表顶部的是当前日志。对于每一个日志，列表显示了添加到日志的最后一个条目的添加时的日期和时间，日志文件的大小和文件名。

3 要查看日志文件，单击查看  。

4 基于 Web 的管理程序 显示了被选中的日志中的消息。

5 您可以将每一页中显示的日志消息的数量设置为 30、50 或 1000。您可以通过卷动浏览日志条目。

6 要查看日志文件中的指定行，只需在转到行字段填写要查看的行号。然后单击  。

7 要在日志消息中翻页，单击 向下翻页  或 向上翻页  。

8 要在您所查看的日志中搜索某条消息，单击搜索  。

搜索日志

以下操作用于在被保存的日志或当前日志中搜索消息：

1 进入 **日志与报告 > 记录日志**。

2 选择 事件日志、攻击日志、防病毒日志、网页过滤日志或电子邮件过滤日志。

3 对要查看的日志文件，单击查看  。

4 单击  在您正在查看的日志文件中搜索消息。

5 选择 与 可以搜索与所有给定条件匹配的消息。

6 选择 或 可以搜索与某个或多个给定条件匹配的消息。

7 选择以下一个或多个搜索条件：

关键词	用于搜索日志消息里包含的任何文字。关键词搜索是区分大小写的。
源	用于搜索任何源 IP 地址。
目的	用于搜索任何目的 IP 地址。
Time	用于搜索在给定的年、月、日和时间内记录的消息。

8 单击确定以执行搜索。

基于 Web 的管理程序会显示出符合给定搜索条件的日志消息。您可以卷动窗口查看消息或者进行另一次搜索。

注意：在进行了一次搜索之后，如果想再次显示所有的日志消息，只需清空所有的搜索条件并再次执行搜索。

将日志文件下载到管理员电脑

您可以将日志文件下载到管理员电脑并保存为纯文本文件或者逗号分隔值 （CSV）文件。下载完之后，您可以使用任何文本编辑器查看文本文件，或者使用一个电子表格软件查看 CSV 文件。按照如下步骤下载日志文件：

1 进入**日志和报告 > 记录日志。**

2 选择流量日志，事件日志，攻击日志，病毒防护日志，网页过滤日志，或者电子邮件日志。

3 要将日志文件下载到管理员电脑，单击下载  。

4 为这个日志文件选择格式：

- 选择以普通格式下载文件可以将日志消息下载保存为文本文件。文本文件的每一行是一条日志消息，消息的格式和它们杂基于 Web 的管理程序中的格式相同。
- 选择以 CSV 格式下载文件可以将日志消息以逗号分隔值格式保存到文本文件中。用这种格式，每个消息的每个字段以逗号分隔。如果您使用一个电子表格软件打开这个文件，每个消息字段显示为一个单独的列。

5 单击保存。

删除当前日志中的全部消息

按照如下步骤可以删除当前日志中的全部消息：

1 进入**日志和报告 > 记录日志。**

2 选择流量日志，事件日志，攻击日志，病毒防护日志，网页过滤日志，或者电子邮件日志。

3 要删除所有消息，单击清空日志  。

4 单击确定以删除消息。

删除一个保存了的日志文件

按照如下步骤操作可以删除一个保存了的日志文件：

1 进入**日志和报告 > 记录日志。**

2 选择流量日志，事件日志，攻击日志，病毒防护日志，网页过滤日志，或者电子邮件日志。

基于 Web 的管理程序列出了符合选定的类型的全部日志，在列表的顶部是当前日志。对于每个日子后，列表显示了添加到这个日志的最后一个条目的日期和时间，日志文件的大小和文件名。

3 要删除一个保存了的日志文件，单击删除  。

单击确定以删除这个日志文件。

配置报警邮件

您可以为 FortiGate 的报警邮件配置最多三个发送地址。您可以为病毒事件、阻塞事件、入侵事件和防火墙或者 VPN 事件或者异常事件的启用报警邮件发送功能。在您设置完邮件地址之后，可以通过发送测试邮件来测试您的设置是否正确。

- 添加报警邮件地址
- 测试报警邮件
- 启用报警邮件

添加报警邮件地址

因为 FortiGate 设备使用 SMTP 服务器名来连接邮件服务器，所以它必须能够在您的 DNS 服务器上解析这个服务器名。因此，在您配置报警邮件之前确保您已经配置了至少一个 DNS 服务器。

按以下方法添加 DNS 服务器

1 进入 **系统 > 网络 >DNS**。

2 如果还没有添加 DNS 服务器，则输入您的 ISP 提供的主 DNS 和辅助 DNS 的地址。

3 单击应用。

按以下方法添加报警邮件地址

1 进入 **日志和报告 > 报警邮件 > 配置**。

2 如果您的邮件服务器要求 SMTP 口令，选中 认证。

3 在 SMTP 服务器栏填写 SMTP 服务器的名字。这个 SMTP 服务器即是 FortiGate 设备用来发送报警邮件的服务器，名字按以下格式填写：smtp. 域名 .com。

SMTP 服务器可以位于连接到 FortiGate 设备的任意网络中。

4 在 **SMTP 用户** 栏，按照以下格式输入一个有效的电子邮件地址：用户名 @ 邮件服务器域名。

这个地址将出现在报警邮件的表单标题上。

5 在密码栏输入 SMTP 用户用来访问 SMTP 服务器的密码。

如果您选择了认证，则必须要输入密码。

6 在 **邮件发送到** 一栏最多可以输入三个目的地址。
这个地址是 FortiGate 将报警邮件实际发送到的电子邮件地址。

7 单击 **应用** 以保存您的报警邮件设定。

测试报警邮件

您可以通过发送测试邮件的方法测试报警邮件设置是否正确：

1 进入 **日志与报告 > 报警邮件 > 配置**。

2 单击 **测试** ，从 FortiGate 发送测试邮件到您所配置的邮件地址。

启用报警邮件

您可以配置 FortiGate 发送报警邮件来响应以下事件：病毒事件、入侵企图、以及防火墙或者 VPN 事件。如果您已经配置了将日志存储到本地硬盘，则可以启用当硬盘快被写满时发送报警邮件的功能。按照以下步骤启用报警邮件：

1 进入 **日志与报告 > 报警邮件 > 分类**。

2 选中**启用病毒事件的报警邮件** 可以使 FortiGate 在防病毒扫描功能发现病毒时发送报警邮件。
当病毒文件阻塞功能删除一个文件时不会发送此邮件。

3 选中**启用阻塞事件报警邮件**可以使 FortiGate 在阻塞被病毒感染的文件时发送报警邮件。

4 选中**启用入侵报警邮件** 可以使 FortiGate 发送报警邮件通知系统管理员 NIDS 检测到了攻击活动。

5 选中**启用防火墙 /VPN 紧急事件或者异常** 可以使 FortiGate 在出现防火墙或 VPN 的紧急事件时发送报警邮件。
防火墙关键事件包括失败了的认证企图。
VPN 关键事件包括重放检测功能检测到一个重放的数据包。重放检测功能可以配置在自动密钥 VPN 通道或者手工密钥 VPN 通道里。

6 选中 **在硬盘满时发送报警邮件** 可以使 FortiGate 在硬盘快被写满时发送报警邮件。

7 单击 **应用** 。

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

D

E

F

G

H

I

J

K

L

M

N

P

Q

R

S

T

U

V

W

X

Y

Z