# WatchGuard® System Manager 用户指南

Fireware® v8.3
Fireware® Pro v8.3

## 用户须知

本指南中的信息如有变更，恕不另行通知。本指南中的示例所使用的公司、名称和数据若未另外注明，均为虚构。未经 WatchGuard Technologies, Inc. 公司的明确书面许可，不得因为任何目的以任何形式或方式（无论电子或机械）复制或传播本指南的任何部分。

## 版权、商标及专利信息



完整的版权、商标、专利和许可信息请参阅本用户指南的附件。



管理软件：8.3
设备软件：Fireware® 8.3 and Fireware Pro 8.3
文档版本：8.3-352-2671-001

**地址**：
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

**技术支持**：
www.watchguard.com/support
support@watchguard.com
美国及加拿大 +877.232.3531
所有其他国家 +1.206.613.0456

**销售电话**：
美国及加拿大 +1.800.734.9905
所有其他国家 +1.206.521.8340

### 关于 WATCHGUARD

WatchGuard 是业界领先的专门针对全球中小型企业的网络安全解决方案提供商，提供功能强大且购买、部署和管理简便的集成产品和服务。公司的 Firebox X 系列可扩展集成安全设备可随着使用单位的发展而进行充分升级，提供业界最佳的安全、性能、直观界面和价值的组合。 WatchGuard 智能分层安全引擎结构能有效防御新出现的威胁，灵活整合 WatchGuard 产品提供的其他安全功能和服务。各项 WatchGuard 产品均附赠首次 LiveSecurity 服务订购，通过安全漏洞预警、软件升级、专家安全指导和优质客户关怀帮助客户在安全领域始终处于主动地位。详情请致电 (206) 521-8340 或访问网站 www.watchguard.com.

# 目录

# 第 1 章　简介

WatchGuard® System Manager (WSM) 让用户能够轻松高效地进行网络安全管理。只需一台电脑作管理工作站，就能显示、管理和监控网络中的每一台 Firebox® 设备。

WSM 支持混合环境。您可管理使用不同版本设备软件的不同型号的 Firebox 设备，还能对 Firebox X Edge 设备进行集中管理。

WSM 有三个服务器进行 Firebox 管理：

*Management Server （管理服务器）*

管理服务器在 Windows 电脑上运行。用户可以用此服务器管理所有防火墙设备，并通过简单的下拉式功能创建 VPN （虚拟专用网）隧道。管理服务器的基本功能如下：

– 对 VPN 隧道配置进行集中管理

– 认证中心（certificate authority）向网络协议安全（IPSec）隧道分发证书

– 支持 WatchGuard SOHO 和 Firebox X Edge 产品的协议转换

*Log Server （日志服务器）*

日志服务器收集来自每台 WatchGuard Firebox 设备的日志消息。日志消息发送至日志服务器时进行了加密，其格式为 XML （纯文本）。从防火墙设备收集的信息包括流量日志消息、事件日志消息、告警和诊断消息。

*WebBlocker Server （WebBlocker 服务器）*

WebBlocker 服务器与 Firebox HTTP 代理服务器一起运行，阻止用户访问特定类别的网站。管理员在配置 Firebox 时，设置允许或阻止的网站类别。

## 关于 Fireware 和 Fireware Pro

WatchGuard® Fireware® 是 WatchGuard 的下一代安全设备软件。设备软件是保存在防火墙硬件内存中的软件应用程序。 Firebox® 通过带配置文件的设备软件来运行。

贵单位的安全策略是一套定义如何保护电脑网络和网络所传输信息的规则。 Fireware 设备软件具有管理最复杂网络的安全策略的高级功能。

WatchGuard® 为客户推出了两种版本的 Fireware：

- Fireware® — 这是 Firebox X Core e 系列设备上安装的缺省设备软件。
- Fireware® Pro— 这是 Firebox X Peak e 系列设备上安装的缺省设备软件。如果您已有 Firebox X Core 设备，可购买 Fireware Pro 进行升级。此设备软件具有针对更复杂网络的以下高级功能：
  - High Availability
  - 高级网络选项，包括 QoS（服务质量）和动态路由

WSM 还包括用来配置和管理采用 WFS 设备软件的 Firebox X 设备的必备软件工具。WFS 设备软件是早期型号的 Firebox X Core 和 Peak 设备配备的缺省设备软件。有关 WFS 设备软件的详情，请参阅“*WFS 配置指南*”。

Firebox 被 WSM 纳入管理后，软件将自动识别 Firebox 使用的设备软件。如果您选择 Firebox，然后点击工具栏上的图标，就会启动正确的管理工具。工具包括：

- Firebox System Manager
- Policy Manager
- HostWatch

例如，如果您将一台使用 WFS 设备软件的 Firebox X700 添加到 WFS 的 **Device tab（设备条）**，然后点击 WSM 工具栏上的 Policy Manager（策略管理器）图标，就会自动启动 WFS 的 Policy Manager。如果您添加了一台使用 Fireware 设备软件的 Firebox X700，点击 Policy Manager 图标将自动启动 Fireware 的 Policy Manager。

# Fireware 的功能与工具

WatchGuard® Fireware® 和 Fireware Pro 包括能提高网络安全程度的众多功能。

## Fireware 的 Policy Manager

Policy Manager（策略管理器）提供一个用于执行基本的防火墙配置任务的用户界面。 Policy Manager 包括一整套预先配置的数据包过滤器和代理服务器。例如，要对所有 Telnet 流量应用数据包过滤器，可添加 Telnet 包过滤器。您也可自定义数据包过滤器，为其设置端口、协议和其他参数。严密的 IPS 选项配置可阻止 SYN 洪水攻击、欺骗攻击、端口或地址空间扫描等攻击。

## Firebox System Manager

Firebox® System Manager 提供一个可监控 Firebox 所有组件的界面。用户可利用 Firebox System Manager 监控 Firebox 的当前状态或直接连接获取配置的更新。

## 网络地址转换

网络地址转换（NAT）指一种或多种用于 IP 地址和端口地址转换的方法。网络管理员常用 NAT 来增加共用一个公共 IP 地址的电脑的数量。 NAT 还可隐藏用户网络中电脑的专用 IP 地址。

## 多广域网

Fireware 最多可将四个 Firebox 接口配置为外部或广域网接口。您可通过多个广域网接口控制流量，实现外发带宽共享。

### Firebox 与第三方验证服务器

WSM 与 Fireware 一起支持五种不同的验证协议：Firebox、 RADIUS、 SecurID、 LDAP 和 Active Directory。

### 基于特征的入侵侦测与防范

某病毒或攻击的一组特殊属性称为特征。当发现新的入侵攻击时，病毒或攻击的特殊属性就会被识别并记录下来，据此创建和分发新的特征。 WatchGuard 网关防病毒和入侵防范服务利用此类特征发现病毒和侦测入侵攻击。订购此项服务的用户可安排自动或手动进行特征代码更新。所有WatchGuard代理服务器均可使用入侵防范服务。网关防病毒服务的进行基于SMTP和HTTP代理服务器。

### VPN 创建和管理

Fireware 技术能更轻松地实现分支机构和终端用户的众多 IPSec VPN 隧道的配置、管理和监控。

### 高级网络功能

Fireware Pro 的 QoS 功能可为每项策略设置优先级和带宽限制。Firebox 也可使用动态路由协议 RIP、OSPF 和 BGP，这些协议能减少网络维护，提供路由冗余。

**注释**

仅 Fireware® Pro 支持 QoS 以及 OSPF 和 BGP 协议。Fireware 和 Fireware Pro 均支持 RIP 协议。

### 网络流量控制

WebBlocker 功能利用 HTTP 代理服务器将过滤器应用到网络流量。您可设置一天内用户可访问不同类型网站内容的小时数，也可设置用户不能浏览的网站类别。

### High Availability

High Availability 为防火墙连接提供状态故障转移功能。您可将一台运行中的 Firebox 设置为备用模式，另一台 Firebox 继续运行。如果主 Firebox 无法连接互联网，则备用 Firebox 将自动接管防火墙操作。

**注释**

仅 Fireware® Pro 支持 High Availability。

## WatchGuard System Manager (WSM) 用户界面

WSM 用户界面的基本组件是 WatchGuard 工具栏和 WSM 窗口。本节介绍用户界面的基本信息。详情见后续章节。

### 关于 WatchGuard 工具栏

可以用 WatchGuard 工具栏启动、停止和配置下列服务器：

- 管理服务器
- 日志服务器

- WebBlocker 服务器

WatchGuard 工具栏是电脑屏幕底端的其中一个工具栏。如果管理工作站没有安装任何 WatchGuard 服务器软件，则不会显示 WatchGuard 工具栏。


工具栏上从左到右的图标分别管理下列服务器：

- 日志服务器 — 此服务器收集来自 Firebox® X Edge、FSM 和安装有 Fireware® 设备的 XML（纯文本）格式的日志消息、事件消息、告警和诊断消息。有关日志服务器的详情，请参阅本指南“*日志与通知*”章节。
- 管理服务器 — 管理服务器在一台 Windows 电脑上运行。若要将 DVCP 服务器从 Firebox 迁移至您的电脑上，请参阅 “*迁移指南*”。
- WebBlocker 服务器— 此服务器与 Firebox HTTP 代理服务器一起运行，限制用户访问该服务器禁止的网站。有关 WebBlocker 的信息，请参阅 “*通过 WebBlocker 控制网站访问*”章节。

## 关于 WatchGuard System Manager 窗口

WSM 窗口有两个选项卡（tab），可用于监控和管理网络：

WSM 窗口在显示屏幕顶端有两个选项卡：

***设备状态***

此选项卡显示连接到 WSM 的设备的状态。显示信息包括状态、 IP 地址和每个以太网接口的 MAC 地址以及已安装的证书，还包括 WSM 中配置的所有 VPN 隧道的状态。

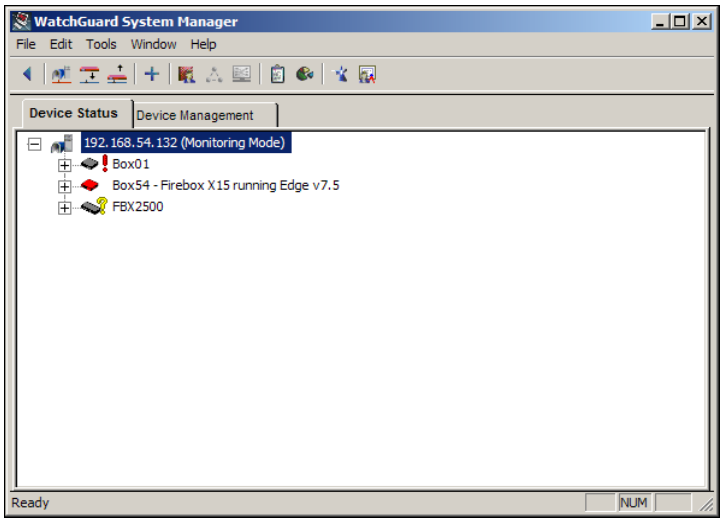
此选项卡中显示的设备与 WSM 直接连接。

***设备管理***

此选项卡显示导航栏和信息栏。导航栏显示连接的 WatchGuard 管理服务器及其设备、托管 VPN 和托管 Firebox® X Edge 的配置。信息栏显示在导航栏中选择的任何项目的详细信息。

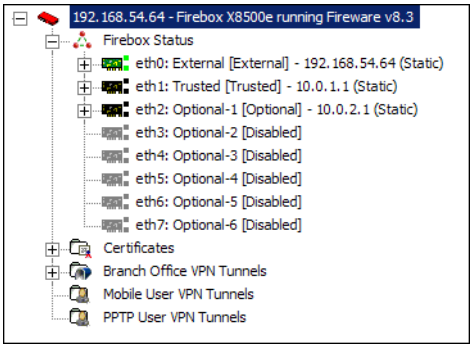
**Device Management （设备管理）**选项卡显示直接连接 WSM 的管理服务器和连接这些服务器的设备。管理服务器所管理的设备如果也与 WSM 直接连接，也可显示在 **Device Status （设备状态）**选项卡上。

WSM 窗口也有可用来启动其他工具的菜单和图标。




## 设备状态

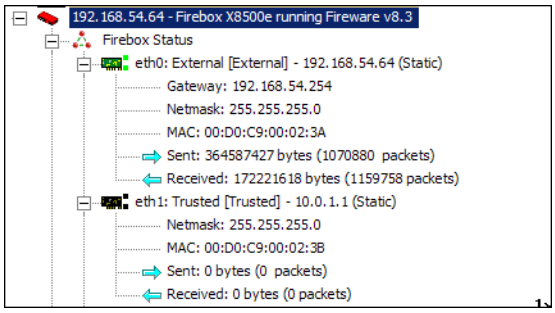
WSM 的 **Device Status( 设备状态 )** 选项卡显示连接的设备的信息。




### Firebox 状态

Firebox 的展开信息包括每个 Firebox 接口的 IP 地址和子网掩码。接口的展开信息包括：

- 缺省网关的 IP 地址和子网掩码 （ 仅针对外部接口 ）。




- 接口的媒体访问控制 （ MAC ）地址。
- 最后一次重启 Firebox 后每个接口发送和接收的数据包数量。

### 分支机构 VPN 隧道数量

Firebox Status （ Firebox 状态 ）下方是关于分支机构虚拟专用网 （ BOVPN ）隧道的内容。共有两种类型的 IPSec BOVPN 隧道：使用 Policy Manager （ 策略管理器 ）手动创建的 VPN 隧道和使用管理服务器创建的 VPN 隧道。

**BOVPN 隧道的展开条目显示以下信息：**

- 隧道名称、目标 IPSec 设备的 IP 地址、及隧道类型。若隧道由管理服务器进行管理，则 IP 地址指完整的远程网络地址。
- 以字节和数据包统计的隧道上收发的数据量。
- 密钥过期前的时间以及再次创建隧道的时间，显示为时间限制或字节数。如果使用管理服务器将隧道配置为根据时间和数据量限制判定过期，则将显示两项过期值。
- 为隧道设置的验证和加密层。
- 隧道的路由策略。

### 移动用户 VPN 隧道

分支机构 VPN 隧道条目之后为移动用户 VPN 隧道条目。此条目显示的信息与分支机构 VPN 隧道相同，包括隧道名称、目标 IP 地址及隧道类型，此外还显示数据包信息、密钥到期日、验证和加密数据。

### PPTP VPN 隧道

对于 PPTP RUVPN 隧道， WSM 只显示已收发数据包的数量。字节数和总字节数不适用于 PPTP 隧道。

## 连接状态

每台设备的树型图显示四种可能状态中的一种。状态描述如下：

*无感叹号和灰色图标*

设备正被首次联系或尚未被联系。

*正常图标*

正常操作。设备正成功地向 WSM 发送数据。

*黄色问号*

设备有一个动态 IP 地址，尚未联系管理服务器。

*红色感叹号和灰色图标*

WSM 此时无法与该设备建立网络连接。

# 第 2 章　开始使用

过去，各公司机构曾使用过多种工具、系统和人力来控制网络安全。不同的电脑系统控制访问、验证、虚拟专用网络和网络控制。这些价格不菲的系统配合使用及更新并不方便。 WatchGuard® System Manager (WSM) 提供管理网络和控制安全问题的集成解决方案。本章讲述如何在网络中安装 WSM。

## 安装 WatchGuard System Manager

WatchGuard® System Manager (WSM) 包括防火墙设备软件和管理软件。用 WSM 软件配置和监控 Firebox® 设备。

要安装 WSM，必须：

- 收集您的网络地址和信息
- 选择网络配置模式
- 选择将管理服务器、日志服务器和 WebBlocker 服务器与管理软件安装在同一台电脑或不同的电脑上
- 配置管理工作站
- 用 Quick Setup Wizard （ 快速安装向导 ）创建基本配置文件
- 在网络中运行 Firebox 设备

**注释**

本章介绍三接口配置的 Firebox 的缺省信息。如果您的 Firebox 有三个以上接口，请使用 “*网络配置*”章节所述的配置工具和程序。

### 安装要求

安装 WatchGuard System Manager 前，请确认是否有下列各项：

- WatchGuard Firebox 安全设备
- 一根串口连接线 （ 蓝色 ）

- 三根以太网交叉网线（红色）
- 三根以太网直通网线（绿色）
- 电源线
- LiveSecurity 服务授权码

## 收集网络信息

### 授权码

获取授权码证书。您购买的 WatchGuard Firebox 附有 LiveSecurity 授权码，可启用 Firebox 的功能。购买任何可选产品时，均附送授权码。

### 网络地址

建议您配置 Firebox 时接上两条连接线，使用 Firebox 前将第一条用于网络 IP 地址。
WatchGuard 用斜线记法表示子网掩码。

未使用 Firebox 时的网络 IP 地址

| | |
|---|---|
| 广域网 | _____._____._____._____ / ____ |
| 缺省网关 | _____._____._____._____ |
| 局域网 | _____._____._____._____ / ____ |
| 第二网（若适用） | _____._____._____._____ / ____ |
| 公共服务器（若适用） | _____._____._____._____ |
| | _____._____._____._____ |
| | _____._____._____._____ |

开始运行 Firebox 后，将第二条线用于网络 IP 地址。

*外网接口*
连接非受信外部网络（通常是互联网）。

*受信接口*
连接要保护的专用局域网或内部网络。

*可选接口*

通常连接用户网络的 DMZ （隔离区）或混合信任区。购买的型号不同， Firebox 可选接口的数量也不同。使用可选接口在网络中创建具有不同访问级别的区域。

Firebox 的网络 IP 地址

| | |
|---|---|
| 缺省网关 | _____._____._____._____ |
| 外部网络 | _____._____._____._____ / ____ |
| 受信网络 | _____._____._____._____ / ____ |
| 可选网络 | _____._____._____._____ / ____ |
| 第二网 （若适用） | _____._____._____._____ / ____ |

## 选择防火墙配置模式

安装 WSM 之前，必须确定如何将 Firebox 安装到网络中。如何安装 Firebox 决定了接口配置。要将 Firebox 安装到网络中，请选择符合当前网络需要的配置模式 – 路由模式 ( routed ) 或透明模式 ( drop-in )。

许多网络在路由配置模式下运行效果最佳，但在下列情况下，我们建议使用透明模式。

- 您已指定了大量静态 IP 地址
- 无法用专用 IP 地址配置拥有公共 IP 地址的受信网络和可选网络中的电脑

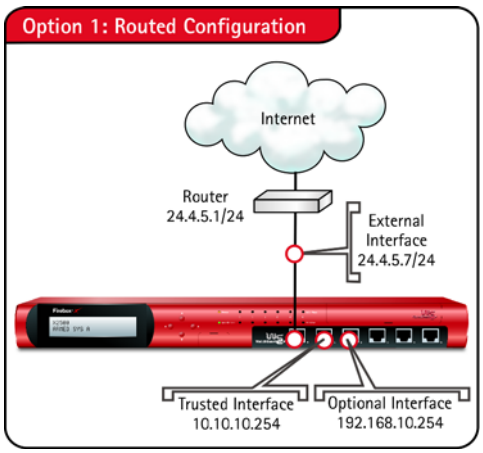
下列表格及其后的描述列出了可帮助您选择防火墙配置模式的三种情况。

| 路由配置模式 | 透明配置模式 |
|---|---|
| Firebox 的所有接口在不同網絡中。 | Firebox 的所有接口在相同网络中并拥有相同 IP 地址。 |
| 受信接口和可选接口必须在不同网络中。各接口在其网络中各有一个 IP 地址。 | 受信接口或可选接口的电脑可以有一个公共 IP 地址。 |
| 使用静态 NAT （网络地址转换）将公共地址映射到受信接口或可选接口后的专用地址。 | 可供公共访问的电脑拥有公共 IP 地址。因此无需静态 NAT。 |

### 路由配置模式

当只有少量公共 IP 地址或 Firebox 通过 PPPoE （以太网点对点协议）或 DHCP （动态主机配置协议）获得外部 IP 地址时，使用路由配置模式。

在路由配置模式下， Firebox 的各个接口对应不同子网。 Firebox 后面的公共服务器可使用专用 IP 地址。 Firebox 使用网络地址转换将数据流从外部网络路由至公共服务器。




路由配置模式要求如下：

- Firebox 的所有接口必须配置在不同子网中。最低配置包括外网接口和受信接口，也可配置一个或多个可选接口。
- 连接受信接口和可选接口的所有电脑必须拥有您网络分配的一个 IP 地址。例如，上图中受信接口上的一台电脑可拥有 10.10.10.200 的 IP 地址，但不能是 192.168.10.200，后者分配给可选接口。

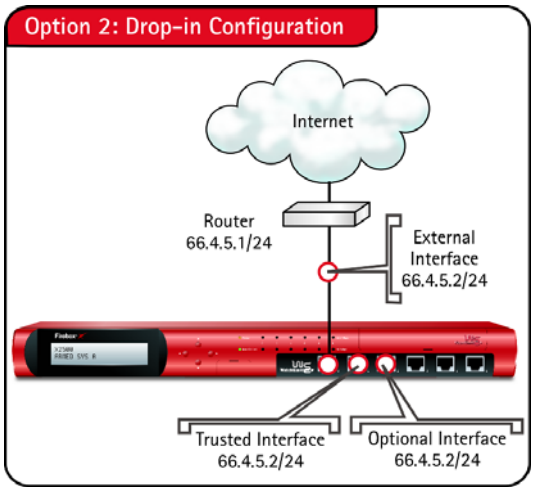
### 透明配置模式

在透明配置模式下， Firebox 在所有接口上的 IP 地址相同。透明配置模式在 Firebox 接口中分配网络逻辑地址范围。您可以将 Firebox 安装在路由器和局域网之间，而无须修改任何本地电脑的配置。此配置称为 “drop-in” 是因为 Firebox 可被 “随意插入” 到网络中。

在透明模式下：

- 必须为 Firebox 的所有接口 （ 外网接口、受信接口和可选接口 ） 分配相同的主 IP 地址。
- 您可将第二网分配至任意接口。
- 您可为受信网络和可选网络中的主机保留相同的IP地址和缺省网关，并为Firebox接口添加第二网地址，以便 Firebox 能向上述网络中的主机正确发送信息流。

Firebox 后面的公共服务器可继续使用公共 IP 地址。Firebox 不使用网络地址转换选择从网络外到公共服务器的流量路径。




透明配置模式的属性如下：

- 必须为 Firebox 指定一个静态外部 IP 地址。
- 所有接口使用同一个逻辑网络。
- 透明模式不支持轮流平均或备份顺序的多广域网。有关上述选项的详情，请参阅 “*网络设置与配置*”章节。

有时需要清除受信网络中每台电脑的 ARP 高速缓存，但并非经常有此必要。

## 选择服务器软件安装位置

在安装过程中，可在同一台电脑上安装管理工作站和三个 WatchGuard System Manager 服务器组件；或者，可以用相同的安装步骤在其他电脑上安装日志服务器和 WebBlocker 服务器组件，以分配服务器负载或提供冗余。管理服务器在没有安装 WSM 软件的电脑上不能正确运行。要确定服务器软件的安装位置，必须先检查管理工作站的容量，并选择符合需要的安装方式。

如果要在已启动 Windows 防火墙以外的桌面防火墙的电脑上安装管理服务器、日志服务器或 WebBlocker 服务器，必须打开服务器需要通过防火墙连接的端口。 Windows 防火墙用户无需修改桌面防火墙配置，因为安装程序会自动通过 Windows 防火墙打开所需端口。详情请参阅第 20 页的 “*在装有桌面防火墙的电脑上安装 WatchGuard 服务器*”。

## 安装管理工作站

在管理工作站上安装 WatchGuard System Manager (WSM) 软件。此软件显示通过防火墙的流量。WSM 还显示连接和隧道状态。WatchGuard 日志服务器记录从 Firebox 收到的信息，您可以用管理工作站中的工具访问这些数据。

选择网络中的一台电脑作为管理工作站，并安装管理软件。您必须拥有管理权限才能够在基于 Windows 的管理工作站上安装 WSM 软件。安装完成后，您可以用 Windows XP 或 Windows 2003 超级用户权限进行操作。

您可以随时从 https://www.watchguard.com/archive/softwarecenter.asp 网页上下载最新的 WSM 软件，但必须用 LiveSecurity 用户名和密码登录。如果您是新用户，在下载 WSM 软件前请先创建用户配置文件并在 http://www.watchguard.com/activate 网页上激活您的产品。

1 下载最新的 WSM 软件。您还必须下载并在管理工作站上安装最新的 Fireware® 设备软件。通过 Web Quick Setup Wizard （网络快速安装向导）使用此软件为 Firebox 创建基本配置文件。
将文件保存到硬盘上时，请务必记下文件名称和路径。

2 打开文件，遵照安装指导的指示进行安装。
安装程序包括选择要安装的软件组件或更新的页面。安装某些软件组件时，需要不同的授权码。.

**注释**

如果管理工作站运行时有 Windows 工具栏，部分用户认为有必要关闭并重启工具栏，才能看见为 WatchGuard 管理系统安装的新组件。

### 软件加密等级

管理工作站软件有两种加密等级。

*基本型*
支持 PPTP RUVPN 隧道的 40 位加密。此加密等级无法创建 IPSec VPN 隧道。

*加强型*
支持 PPTP RUVPN 的 40 位和 128 位加密，也支持 56 位和 168 位 DES 以及 128 位、 192 位和 256 位 AES。

要在虚拟专用网应用 IPSec，必须下载强大的加密软件。

强大的加密软件具有强大的输出限制功能，但有可能不提供下载。

## 备份以前的配置

如果有旧版本的 WSM，在安装新版本前，请先备份安全策略配置。要创建配置的备份，请参阅“*升级指南*”。

# 快速安装向导

您可以使用快速安装向导 ( Quick Setup Wizard ) 为 Firebox X 创建基本配置文件， Firebox 首次启动时将使用该基本配置文件。这样 Firebox 就可作为基本防火墙使用。如果因恢复或其他原因要为 Firebox 重新设定新的基本配置，可按此相同步骤进行。

## Firebox X Core 和 Peak e 系列网络快速安装向导

如果您购买了 Firebox X Core 或 Peak e 系列设备，可使用新的网络快速安装向导对 Firebox 进行配置。如果您以前曾经配置过 Firebox X Core 或 X Peak，您必须了解，网络快速安装向导的使用不同于 Firebox X 以前硬件型号所配的快速安装向导。对于以前的 Firebox X Core 和 Peak 设备，快速安装向导使用设备搜索来查找网络中要配置的 Firebox ； 而对于 Firebox X Core、 Peak e 系列和网络快速安装向导，则必须与 Firebox 建立直接网络连接并使用网页浏览器来启动向导。 Firebox 使用来自以太网接口 Eth1 的 DHCP 向管理工作站分配配置中要使用的新 IP 地址。

运行网络快速安装向导前，请确认：

- 已为 Firebox 注册 LiveSecurity 服务
- 已将一份 Firebox 密钥保存在管理工作站上的一个文本文件中
- 已将 WSM 和 Fireware® 软件从 LiveSecurity 服务网站下载到管理工作站
- 已在管理工作站上安装可执行的 Fireware
- 已将管理工作站配置为自动接受 IP 地址（通过 DHCP）

### 使用网络快速安装向导

1 用 Firebox 所配的红色以太网交叉网线连接管理工作站的以太网端口和 Firebox 的 Eth1 端口。

2 将电源线分别插入 Firebox 的电源输入口和电源。

3 打开 Firebox 电源时，按下 Firebox X 正面的向上箭头按钮。
Firebox X 启动到安全模式。出现“调用恢复”（Invoking Recovery）提示时，可松开向上箭头按钮。

4 请确认管理工作站配置为接受 DHCP 分配的 IP 地址。
例如，在管理工作站使用 Windows XP 的情况下：
从 Windows Start（启动）菜单中选择 **All Programs（所有程序）> Control Panel（控制面板）> Network Connections（网络连接）> Local Area Connections（本地连接）**。单击 **Properties（属性）**。选择 **Internet Protocol (TCP/IP)（网络协议 TCP/IP）**，单击 **Properties（属性）**。请确认选择了 **Obtain an IP Address Automatically（自动获取 IP 地址）**。

5 **打开网页浏览器，输入：http://10.0.1.1:8080/**
这将打开管理工作站和 Firebox X e 系列设备之间的 HTTP 连接，网络快速安装向导将自动启动。

Firebox 配置了此基本配置后，可使用 Policy Manager（策略管理器）扩展或修改 Firebox 的配置。

### 使用网络快速安装向导进行恢复

首次配置 Firebox X e 系列设备时，可使用网络快速安装向导。如果因忘记密码或在一个新的网络中部署 Firebox 而需要为 Firebox 重新设定新配置，也可使用网络快速安装向导。

如果要使用网络快速安装向导进行恢复且已购买了 Firebox 硬件型号升级，必须确认在向导中输入的密钥就是型号升级所配的密钥。

### 网络快速安装向导疑难解答

如果网络快速安装向导无法在 Firebox 上安装 Fireware 设备软件，向导将在六分钟后超时。如果使用向导时出现问题，请查看以下事项：

- 从 LiveSecurity 网站上下载的 Fireware 应用程序软件文件可能已被破坏。如果软件图像被破坏，有时在液晶显示屏界面上会出现提示：“文件截取错误”。请重新下载软件并再次启动向导。
- 如果使用 IE6，请清除网页浏览器中的文件缓存后再重试。要清除缓存，请在 IE 工具栏中选择 **Tools（工具）> Internet Options（Internet 选项）> Delete Files（删除文件）**。

## 快速安装向导

如果使用旧型号的 Firebox X Core 或 Peak（非 e 系列 Firebox），则必须使用作为 Windows 应用程序运行的快速安装向导创建基本配置文件， Firebox 首次启动时将使用该基本配置文件，这样 Firebox 就可作为基本防火墙使用。

Firebox 配置了此基本配置后，可使用 Policy Manager（策略管理器）扩展或修改 Firebox 的配置。.

快速安装向导使用设备搜索程序来查找正在配置的 Firebox X 型号，此程序使用 UDP 广播。软件防火墙，包括 Microsoft Windows XP SP2 的防火墙，可能会造成设备查找问题。

可从 Windows 桌面或 WSM 启动快速安装向导。在桌面上选择 **Start（开始）> All Programs（所有程序）> WatchGuard System Manager 8.3 > Quick Setup Wizard（快速安装向导）**。在 System Manager 中，选择 **Tools（工具）> Quick Setup Wizard（快速安装向导）**。

**注释**

在快速安装向导中，必须为 Firebox 设置状态和配置密码短语。准备配置从 Firebox 收集日志消息的日志服务器时，使用在快速安装向导中设置的状态密码短语作为缺省日志密钥。日志服务器配置完成后，如有必要可修改日志密钥。详情请参阅 “*日志与通知*”章节。

## 运行 Firebox

完成任意一个快速安装向导后，即完成了 Firebox® 的安装。 Firebox 可作为基本防火墙使用，允许所有外发的 TCP、 DNS 和 ping 流量。

完成下列步骤，即可在网络中运行 Firebox:

- 将 Firebox 安装在固定的物理位置。
- 在 WSM 中，用 **File（文件）> Connect To Device（连接设备）**将管理工作站连接至 Firebox。
- 如果使用路由配置模式，请修改连接到 Firebox 受信 IP 地址的所有电脑上的缺省网关。
- 安装管理服务器。请参阅本指南中的 “*管理服务器安装和管理*”章节。
- 配置日志服务器，开始记录日志消息。请参阅本指南中的 “*日志与通知*”章节。
- 安装 WebBlocker 服务器。请参阅本指南中的 “*通过 WebBlocker 控制网站访问*”章节。
- 打开 Policy Manager，修改配置。

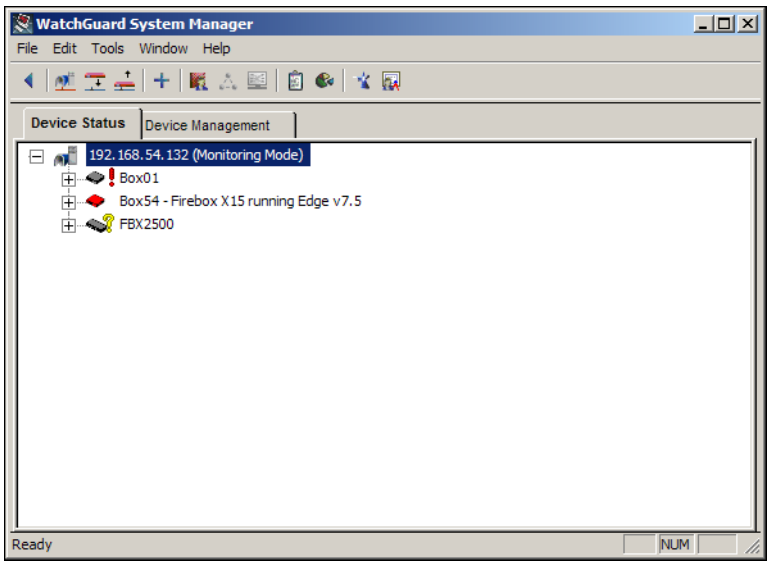
**注释**

如果要在已启动 Windows 防火墙以外的桌面防火墙的电脑上安装管理服务器、日志服务器或 WebBlocker 服务器，必须打开服务器需要防火墙连接的端口。Windows 防火墙用户无需修改配置。详情请参阅第 20 页的 “*在装有桌面防火墙的电脑上安装 WatchGuard 服务器*”章节。

## 开始使用 WatchGuard System Manager

本节介绍了开始使用 WatchGuard System Manager 的基本步骤，还介绍了首次连接到 Firebox 时页面上出现的信息。

在 Windows 桌面上选择 **Start （开始）> All Programs （所有程序）> WatchGuard System Manager 8.3 > WatchGuard System Manager**。

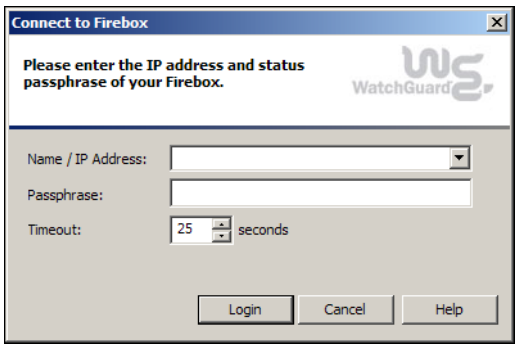



有关 WSM 的基本信息，请参阅第 4 页的 “*WatchGuard System Manager (WSM) 用户界面*”。您可在此主页面访问本手册中介绍的 WSM 所有功能。

## 连接 Firebox

1 选择 **File （文件）> Connect to （连接到）> Device （设备）**。
或
右键点击 **Device Status （设备状态）**键，选择 **Connect to （连接到）> Device （设备）**。

或
点击 WSM 工具栏上的 Connect to Device （连接到设备）图标，该图标位于屏幕左边。
出现 **Connect to Device （连接到设备）**对话框。




2 在 **Firebox** 下拉列表中，根据 IP 地址或主机名称选择 Firebox®。
您也可以输入 IP 地址或主机名称。输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

3 输入 Firebox 状态 （只读）密码短语。
使用状态密码短语监控流量和 Firebox 状态。向 Firebox 保存新配置时，必须输入配置密码短语。

4 必要时，请修改 **Timeout（超时）**字段值，该值设置管理工作站在发送显示无法从 Firebox 获取数据的消息之前等待 Firebox 发送数据的时间 （单位为秒）。
如果连接到设备的网络或互联网连接速度较慢，可增大超时字段值。如果连接到了不可用的 Firebox，减小该值就意味着减少了等待出现超时提示的时间。

5 单击 **Login（登录）**。
WSM 窗口将显示 Firebox。

### 断开与 Firebox 的连接

要断开连接，请右键点击要断开的 Firebox 的信息首行，选择 **File（文件）> Disconnect（断开连接）**；或者选择 Firebox，然后单击左边的 Disconnect（断开连接）图标。

### 启用安全应用程序

您可使用任务栏和菜单选项上的图标，从 WatchGuard® System Manager 启动以下工具：

*Policy Manager（策略管理器）*

Policy Manager 让用户安装、配置和自定义网络安全策略。要为 Firebox® X Edge 或 Firebox SOHO 配置或自定义安全策略，必须使用网络用户界面连接到该设备。

*Firebox System Manager（Firebox 系统管理员）*

WatchGuard Firebox System Manager 让用户通过一个简单的用户界面启动多项不同的安全工具。您也可以用 Firebox System Manager 监控通过防火墙的实时流量。有关使用 Firebox System Manager 的详情，请参阅 “*监控 Firebox 状态*”章节。

*HostWatch*

HostWatch 显示受信网络通过 Firebox 接到外部网络的连接，它显示当前连接，也可用日志文件显示历史连接。有关使用 HostWatch 的详情，请参阅 “*监控 Firebox 状态* “章节。

*Log Viewer*

Log Viewer 显示日志文件的静态视图，可以：

– 按数据类型应用过滤器
– 搜索字和字段
– 打印并保存到文件

有关使用 Log Viewer 的详情，请参阅本指南中的 “*日志与通知*”章节。

*Historical Reports（历史报表）*

这些 HTML 报表提供监控网络或排除网络故障之时所使用的数据，数据包括：

– 会话类型
– 最活跃主机
– 最常用服务
– URL

有关使用历史报表的详情，请参阅本指南中的 “*生成网络活动报表*”章节。

## 安装完成后

您已妥善安装和配置新的 WSM 软件并将其加入到网络运行中。以下是一些基本程序和注意事项。

### 自定义安全策略

安全策略控制进出网络的人员和访问位置。 Firebox® 的配置文件创建了安全策略。

通过快速安装向导创建的配置文件只是基本配置，您可创建使安全策略符合自身要求的配置文件。为此，需添加被过滤和被代理的策略（ proxied policies ），设置对网络的访问控制。每项策略都可能对网络产生影响。增强网络安全性的策略会减少对网络的访问量，而增加网络访问量的策略会降低网络的安全性。选择策略时，必须根据所在单位和所保护电脑设备的情况选择一系列平衡的策略。若属于新安装，我们建议，只采用数据包过滤策略，直到所有系统正常运行为止。可根据需要添加被代理策略。

### LiveSecurity 服务的功能

购买 Firebox，我们就附送 LiveSecurity® 服务。订购该服务可：

- 确保您获得最新软件版本的最新网络防护
- 用全面的技术支持资源，为您的问题提供解决方案
- 利用有关最新安全问题的消息和配置帮助，防止服务中断
- 我们的培训资源可帮助您了解更多有关网络安全的知识
- 通过软件和其他功能，增进您的网络安全
- 通过高级替换安排，延长硬件的保修期

## 升级至新版 Fireware

有时，我们会向订购了 LiveSecurity 服务的 Firebox® 用户提供新版本的 WSM 和 Fireware® 设备软件。要从 Fireware 的一个 WSM 8.x 版本升级到 Fireware 的 WSM 8.x 新版本：

1 备份当前的 Firebox 配置文件和管理服务器配置文件
有关如何备份 Firebox 配置的详情，请参阅第 72 页的 “*关于 Firebox 备份*”。
要备份管理服务器上的设置，请使用 Management Server Backup and Restore Wizard（ 管理服务器备份和恢复向导 ）。有关此向导的详情，请参阅 “*管理服务器安装和管理*”章节。

2 用 Windows 控制面板中的 “添加或删除程序”来卸载现有的 WatchGuard Fireware 程序。
没有必要卸载 WSM。

3 启动从 LiveSecurity 网站下载的文件，按屏幕指示程序进行操作。

4 要将更新保存到设备，请用 Policy Manager 打开 Firebox X Core 或 Firebox X Peak 配置文件，并按照屏幕指示将配置文件转换为新版本，并保存到 Firebox。
如果并未显示屏幕指示或此程序出现问题，请打开 Policy Manager，选择 **File （ 文件 ）> Upgrade （ 升级 )**。浏览安装目录或 C:\Program Files\Common Files\WatchGuard\resources\Fireware，选择 WGU file （ WGU 文件 )。点击 **OK （ 确定 )**。

升级程序将自动重启 Firebox。

## 安装内容

本节介绍了有关安装 Firebox® 的更多信息。

## 在装有桌面防火墙的电脑上安装 WatchGuard 服务器

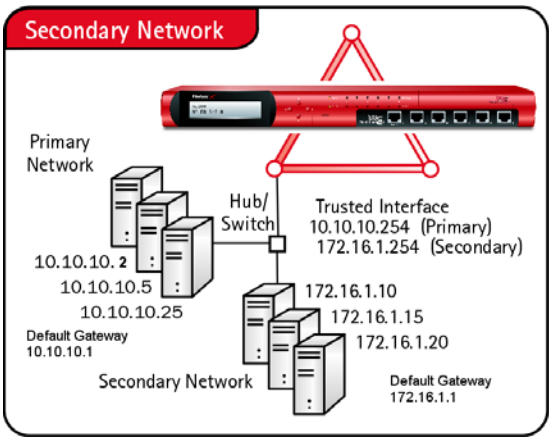
桌面防火墙可能阻隔 WatchGuard® 服务器组件运行所需的端口。在已启动桌面防火墙的电脑上安装管理服务器、日志服务器或 WebBlocker 服务器之前，可能需要打开桌面防火墙上的必要端口。Windows 防火墙用户无需修改配置，因为安装程序会自动打开 Windows 防火墙中的必要端口。

下表列出了必须在桌面防火墙中打开的端口。

| 服务器类型 / 设备软件 | 协议 / 端口 |
|---|---|
| 管理服务器 | TCP 4109, TCP 4110, TCP 4112, TCP 4113 |
| 日志服务器<br>有 Fireware® 设备软件<br>有 WFS 设备软件 | <br>TCP 4115<br>TCP 4107 |
| WebBlocker 服务器 | TCP 5003, UDP 5003 |

## 在配置中添加第二网

第二网是通过交换机或集线器连接到 Firebox 接口的另一个不同网络。




添加第二网时，将一个第二 IP 地址映射到 Firebox 接口。这样，您就为网络接口创建（或添加）了一个 IP 别名。您设置的第二网络地址是第二网中所有电脑的缺省网关。第二网还通知 Firebox 在 Firebox 接口上存在另一个网络。

要添加第二网，可按下列程序之一进行操作：

### 在安装过程中使用快速安装向导

如果将 Firebox 配置为透明模式，可在网络快速安装向导中为第二网输入 IP 地址，该地址即为第二专用网络的缺省网关。

### Firebox 安装完成后添加第二网

如果将 Firebox 配置为路由模式，或使用快速安装向导后的任何时候，可以用 Policy Manager 向接口添加第二网。有关如何使用 Policy Manager 的详情，请参阅本指南中的 “*策略配置*”章节。

## 外网接口上的动态 IP 支持

如果使用动态 IP 地址，则必须在使用快速安装向导时，将 Firebox 配置为路由模式。

如果选择 DHCP， Firebox 将通知 Internet 服务提供商（ISP）控制的 DHCP 服务器为 Firebox 分配 IP 地址、网关和子网掩码。该服务器还为 Firebox 提供 DNS 服务器信息，如果没有提供该信息，则必须手动添加到配置中。必要时可修改 ISP 提供的 IP 地址。

您也可使用 PPPoE。同 DHCP 一样， Firebox 将创建接到您的 ISP PPPoE 服务器的 PPPoE 连接，该连接自动配置您的 IP 地址、网关和子网掩码。

如果在外网接口上使用 PPPoE，配置网络时必须拥有 PPP 用户名和密码。如果 ISP 提供了使用的域名，请在使用快速安装向导时以 “用户名 @ 域名”的格式输入用户名。

如果要 Firebox 执行某些功能，则需要有一个静态 IP 地址。如果将 Firebox 配置为接收动态 IP 地址，则 Firebox 不能使用以下功能：

- High Availability（Firebox 500 无此功能）
- 透明模式
- 1 对 1 网络地址转换
- MUVPN
- 应用 PPTP 的 RUVPN

**注释**

如果您的 ISP 使用 PPPoE 连接提供一个静态 IP 地址，则 Firebox 将由于 IP 地址是静态的而允许启用应用 PPTP 的 MUVPN 和 RUVPN。

如果您安装的 Firebox 是 PPPoE 客户端，则不能使用外部别名和一对一网络地址转换。

## 输入 IP 地址

在快速安装向导或 WSM 对话框中输入 IP 地址时，请以正确顺序输入数字和句点。不要使用 TAB 键、箭头键、空格键或鼠标将光标移至句点后。例如，如果要输入 IP 地址 172.16.1.10，输入 “16”后不要输入空格。不要将光标移到下一句点后以输入 “1”，直接在 “16”后输入句点，然后输入 “1.10.”按斜杠（/）键移动到子网掩码。

### 关于斜线记法

用斜线记法输入子网掩码。在斜线记法中，一个数字表示 IP 地址的多少位标识主机所在的网络。子网掩码 255.255.255.0 的斜线记法值相当于 8+8+8=24。例如， IP 地址 192.168.42.23/24 等于子网掩码为 255.255.255.0. 的 IP 地址 192.168.42.23。

下表列出了子网掩码及其斜线记法：

| 子网掩码 | 斜线记法 |
|---|---|
| 255.0.0.0 | /8 |
| 255.255.0.0 | /16 |
| 255.255.255.0 | /24 |
| 255.255.255.128 | /25 |
| 255.255.255.192 | /26 |
| 255.255.255.224 | /27 |
| 255.255.255.240 | /28 |
| 255.255.255.248 | /29 |
| 255.255.255.252 | /30 |

## 安装 Firebox 线缆

将电源线的两端分别连接到 Firebox 的电源输入口和电源。

建议您用一条以太网直通网线（绿色）将管理工作站连接至 Hub（集线器）或交换机，用另一条以太网直通网线（绿色）将 Firebox 连接到同一个集线器或交换机。

您也可以用红色交叉网线将 Firebox 受信端口连接到管理工作站的以太网端口。

# 第 3 章　服务和支持

若无定期更新和安全信息，互联网安全解决方案是不完善的。新的威胁每天都会出现 —从最新黑客到操作系统中的最新 bug，均会对网络系统造成损害。 LiveSecurity® 服务直接向您发送安全解决方案，使您的安全系统始终保持最佳状态。 WatchGuard® 网站提供培训和技术支持，帮助您深入了解网络安全和 WatchGuard® 产品。

## LiveSecurity 服务解决方案

安全问题越来越多，有关网络安全的信息也越来越多。我们知道，防火墙只是整套安全解决方案中的首要组件。 WatchGuard® 快速响应小组由专门的网络安全人员组成，帮助您控制安全信息量过大的问题；他们通过监控互联网安全网站来发现新的安全问题。

### 威胁应对、预警和专家建议

发现新的威胁后， WatchGuard 快速响应小组会通过电子邮件将问题通知您。每封邮件都提供全面信息，让你了解有关的安全问题类型和为防止网络被攻击而必须采取的措施。

### 简单方便的软件升级

发布 WSM 软件新版本后， LiveSecurity® 服务团队很快就会向您发出电子邮件，大大节省了您的时间。安装向导、发布说明和软件升级链接使安装快捷简便。持续更新功能使您无需耗时寻找新的软件。

### 使用技术支持和培训

用户可以利用我们提供的多种网上资源，迅速查找关于 WatchGuard 产品的信息，也可直接咨询 WatchGuard 技术支持人员。用户可以利用我们提供的在线培训深入了解 WSM 软件、Firebox® 和网络安全，或利用用户所在地区的 WatchGuard 认证的培训中心。

# LiveSecurity 服务广播

WatchGuard® 快速响应小组会定期通过电子邮件向用户的电脑桌面发送消息和软件信息，消息按类划分，以便用户即时识别和利用收到的信息。

*信息预警（Information Alert）*

信息预警使用户能够快速掌握最新信息和互联网安全威胁。 WatchGuard 快速响应小组会经常建议用户针对新出现的威胁修改安全策略。必要时，信息预警会包括修改步骤指示。

*威胁应对*

针对新出现的安全威胁，如果有必要， WatchGuard 快速响应小组会为用户的 Firebox® 发送软件更新。威胁应对包括关于安全威胁的信息和如何下载并在 Firebox 和管理工作站上安装软件更新的指示。

*软件升级*

必要时， WatchGuard 会更新 WSM 软件。产品升级包括新功能和补丁。我们发布软件更新时，会向用户发送电子邮件，指导用户如何下载和安装更新。

*评论*

每个星期，高层网络安全人员都会与 WatchGuard 快速响应小组开会，撰写网络安全评论文章，这源源不绝的信息可帮助确保用户的网络安全。

*知识基础*

WatchGuard 快速响应小组还会专门为安全管理员、员工和不熟悉此技术的其他人员编写资料。

*环回（Loopback）*

LiveSecurity® 服务每个月末会向用户发送一封电子邮件，总结该月发送的信息。

*技术支持动画*

这些短小的培训信息可帮助用户使用 WSM，是对其他网上资源的补充 :

– 在线帮助
– 常见问题
– 技术支持网站上的已知问题页面

*病毒预警*

WatchGuard 与防毒厂商 McAfee 联手，为用户提供有关电脑病毒的最新信息。每个星期，我们都会向用户发送一条关于互联网上病毒流量的摘要。当黑客在互联网上发布危险病毒时，我们会发出特殊病毒警告，以帮助用户对网络进行防护。

WatchGuard *新品发布*

每当 WatchGuard 推出新产品，我们会首先通知您—我们的客户，您用户可以了解到新功能和新服务、产品更新、硬件发布及促销活动。

## 激活 LiveSecurity 服务

用户可以在 LiveSecurity 网站的 “激活”栏目激活 LiveSecurity® 服务。快速启用指南和本指南中的“*开始使用*”章节对激活和 Quick Start Guide （ 快速安装向导 ）做了说明。

**注释**

要激活 LiveSecurity 服务，必须启用浏览器中的 JavaScript。

**要通过 Internet 激活 LiveSecurity 服务，请按以下步骤操作：**

1 确认已获得 Firebox® 序列号，这在 LiveSecurity 激活程序中必须用到。
   - Firebox 序列号位于 Firebox 背面通用产品代码（UPC）下方的标签上，或在 Firebox 底部的标签上。
   - 授权码可在 WatchGuard LiveSecurity 授权码证书中找到。注意一定要用大写输入授权码，并且不要遗漏连字符。

2 用网页浏览器进入：
www.watchguard.com/account/register.asp
将出现客户页面。

3 填写 LiveSecurity Activation（LiveSecurity 激活）页面。用 TAB 键或鼠标在页面的字段间移动。
必须填写所有字段才能正确激活，填写的信息有助于 WatchGuard 向您发送针对您购买产品的信息和软件更新。

4 确认您的电子邮件地址正确无误，关于产品更新和威胁应对的 LiveSecurity 邮件将发至此邮箱。完成以上程序后，您将会收到一封邮件，通知您已成功激活 LiveSecurity 服务。

5 **点击 Register（注册）**。

## LiveSecurity 服务自助工具

在线自助工具（Online Self Help Tools）有助于用户购买的 WatchGuard® 产品发挥最佳性能。

**注释**

访问网上资源之前，必须先激活 LiveSecurity® 服务。

*Instant Answers（快速解答）*

Instant Answers 是快速提供针对产品问题的解决方案的指导性帮助工具，它向您提出问题，然后根据您的回答提供最佳解决方案。

*Basic FAQs（基本常见问题）*

基本常見問題提供關于 Firebox® 和 WSM 軟件的綜合信息，爲對網絡安全和 WatchGuard 産品不熟悉的客户編寫。

*Advanced FAQs（高级常见问题）*

高级 FAQs（常见问题）提供关于配置选项和系统或产品使用的重要信息，是对本用户指南和在线帮助系统中的信息的补充。

*Fireware® "How To"'s*

Fireware How To 文档能帮助用户快速查找 Fireware 设备软件的配置任务程序。

*Known Issues（已知问题）*

"已知问题"工具可监控 WatchGuard 产品问题和软件更新。

*WatchGuard Users Forum（WatchGuard 用户论坛）*

WatchGuard 技术支持小组创办的网站，客户可就 WatchGuard 产品互相提供帮助。技术支持小组对该论坛实行监控，确保用户所获信息的准确性。

*Online Training（在线培训）*

通过浏览在线培训，用户可以了解网络安全和 WatchGuard 产品的更多资料。用户可以阅读培训资料并获得 WatchGuard 产品的认证。培训包括大量有关网络安全的文档和网站链

接。培训分为多个部分，用户可以根据需要有选择地进行学习。有关在线培训的详情，请浏览：
www.watchguard.com/training/courses_online.asp

*Learn About*

Learn About 是关于特定产品或功能的所有可用资源的一个列表，是有关功能的网站地图。

*Product Documentation （产品文档）*

WatchGuard 网站提供全部产品用户指南，包括已不再支持的软件版本的用户指南。用户指南为 PDF 格式。

*Firebox X Edge 和 Fire box SOHO 综合资源*

网站的此部分为 Firebox X Edge 和 Firebox SOHO 客户提供基本信息和链接，帮助用户安装和使用 Firebox X Edge 和 SOHO 硬件。

要使用 LiveSecurity 服务自助工具：

1 请打开网页浏览器，在地址栏中输入：
http://www.watchguard.com/support

2 点击 **Self Help Tools （自助工具）**。
需登录。

3 点击选择。

## WatchGuard 用户论坛

WatchGuard® 用户论坛是一个在线用户群组，采用 WatchGuard 产品的用户可相互交流以下产品信息：

- 配置
- 连接 WatchGuard 产品和其他公司的产品
- 网络策略

论坛内容按类划分，可供用户查询不同信息。技术支持小组在正常工作时间对论坛实行控制管理，用户在使用论坛时技术支持小组不会提供特殊帮助。如要直接从网上联系技术支持小组，请登录用户的 LiveSecurity 帐户，点击 **Incidents （事件）**链接，发送技术支持事件。

### 使用 WatchGuard 用户论坛

要使用 WatchGuard 用户论坛，必须先创建帐户。请在 http://www.watchguard. com/forum 查看说明。

## 在线帮助

WatchGuard® 在线帮助是可在大多数电脑操作系统中运行的网上系统，我们每发布一项软件产品都会同时推出整套在线帮助系统。

在安装 WSM 软件时，将自动安装帮助的静态版本，用户可以在安装文件夹的 Help 子目录中找到。

### 启用 WatchGuard 在线帮助

要在 WSM 软件中启动在线帮助系统，请按 **F1**。浏览器将会打开，显示在线帮助页面，页面将显示有关用户正在使用的功能的信息。

### 搜索信息

在 WatchGuard 在线帮助系统中，搜索信息有三种方法：

*Contents （内容）*

**Contents （内容）**表格显示帮助系统中的类别列表，双击书本图标，打开类别。点击页标题，查看该类别的内容。

*Index （索引）*

**Index （索引）**显示帮助系统中的文字列表，输入文字，列表将自动跳转至用户输入的字母开头的文字。点击页标题查看内容。

*Search （搜索）*

搜索功能可在帮助系统中进行纯文本搜索。输入文字，按 ENTER （回车），将会显示包含该字的类别列表。搜索功能不能使用 AND、 OR 和 NOT 操作符。

### 将在线帮助系统复制到更多电脑上

用户可以将 WatchGuard 在线帮助从管理工作站复制到第二台电脑上。执行此操作时，请复制管理工作站上 WatchGuard 安装目录中的整个在线帮助文件夹，必须包括所有子目录。

#### 软件要求

- IE 4.0 或更新版本
- Netscape Navigator 4.7 或更新版本

#### 操作系统

- Windows NT 4.0、 Windows 2000 或 Windows XP
- Sun Solaris
- Linux

## 产品文档

所有用户指南均可在此网址上找到：http://www.watchguard.com/help/documentation.

## 技术支持

LiveSecurity® 服务订购包括对 WSM 软件和 Firebox® 硬件的技术支持。有关 WatchGuard 技术支持的详情，请浏览 WatchGuard 网站：

http://www.watchguard.com/support

**注释**

如要寻求技术支持，必须先激活 LiveSecurity® 服务。

## LiveSecurity 服务技术支持

只要购买任何一款新的 Firebox 产品，就获得了 WatchGuard LiveSecurity 技术支持服务。如果安装、管理或配置 Firebox 时出现问题，用户可以与 WatchGuard 技术支持小组成员联系。

*办公时间*

WatchGuard 技术支持小组办公时间为用户当地时间的周一至周五的早上 6 点到下午 6 点。

*电话号码*

美国和加拿大：877.232.3531（选 #2）
其他国家：+1.206.613.0456

*网址*

http://www.watchguard.com/support

*服务时间*

我们尽力在四小时内给出回复。

另提供单一事件优先响应升级（SIPRU）和非办公时间单一事件升级（SIAHU）服务。有关上述升级服务的详情，请浏览 WatchGuard 网站：

http://www.watchguard.com/support

## LiveSecurity 金牌服务

WatchGuard 金牌 LiveSecurity 技术支持是对标准 LiveSecurity 服务的补充，如果用户在工作中经常使用互联网或 VPN 隧道，建议用户选择此项升级服务。

WatchGuard 金牌 LiveSecurity 技术支持为用户提供：

- 每周七天每天 24 小时技术支持，节假日不休。
- 技术支持小组工作的支持中心，周日晚上 7 点至周五晚上 7 点（太平洋标准时间）。周末如遇重要问题需要支持，请使用在线寻呼系统。
- 我们尽力在一小时内回复。
- 要创建支持事件，请呼叫 WatchGuard LiveSecurity 技术支持，客户服务代表将记录问题并为用户分配事件号，优先支持技术人员会尽快联系用户。如果在支持中心非工作时间用户遇到重要问题，请拨打 LiveSecurity 技术支持电话号码呼叫技术人员，也可在网站上发送事件：http://www.watchguard.com/support/ incidents/newincident.asp

## Firebox 安装服务

WatchGuard 远程 Firebox 安装服务帮助用户安装和配置 Firebox，用户可以安排两小时的时间，享受 WatchGuard 技术支持小组成员为用户提供的服务。技术人员将帮助用户：

- 分析网络和安全策略
- 安装 WSM 软件和 Firebox 硬件
- 根据用户公司的安全策略调整配置

此项服务不包括 VPN 安装。

### VPN 安装服务

WatchGuard 远程 VPN 安装服务全程帮助用户进行 VPN 安装，用户可以安排两小时的时间，享受 WatchGuard 技术支持小组成员为用户提供的服务，在此期间，技术人员将帮助用户：

- 分析 VPN 策略
- 配置 VPN 隧道
- 测试 VPN 配置

用户可以在正确安装和配置 Firebox 后使用此项服务。

## 培训和认证

WatchGuard® 提供在线产品培训，帮助用户了解网络安全和 WatchGuard 产品的更多资料。技术支持网站提供培训资料，可供用户准备认证考试之用，培训资料包括有关网络安全的书籍和网站链接。用户所在地区附近还有众多 WatchGuard 认可培训合作伙伴（WCTPs）为用户提供 WatchGuard 产品培训，培训合作伙伴使用经认可的培训教材和 WatchGuard 硬件提供培训。有高级讲师和系统管理员帮助用户学习如何安装和配置产品。查询培训合作伙伴信息，请浏览 http://www.watchguard.com/training/partners_locate.asp

# 第 4 章　监控 Firebox 的状态

WatchGuard® Firebox® System Manager (FSM) 为你提供监控 Firebox 所有组件及其工作情况的界面，你可以利用 FSM 监控 Firebox 的当前状态，或直接连接 Firebox 获取配置更新。你可以查看：

- Firebox 界面和通过界面流量的状态
- VPN 隧道和管理证书的状态
- Firebox 带宽使用情况或特定端口连接的实时图表
- Firebox 上使用的任何其他安全设备的状态

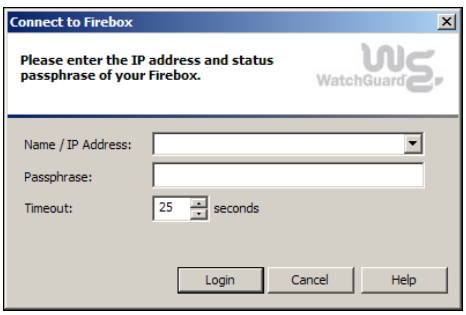
## 开始使用 Firebox System Manager

开始使用 Firebox® System Manager 前，必须先连接 Firebox。

### 连接 Firebox

1　在 WatchGuard System Manager 中，点击 Connect to Device （连接到设备）图标。

或者选择 File （文件）> Connect To Device （连接到设备）。
将出现 Connect to Firebox （连接到 Firebox）对话框。




2　在 **Name/IP Address （名称 /IP 地址）**下拉菜单中，选择一个 Firebox。
你可以输入 IP 地址或 Firebox 名称。

3 在 **Passphrase （口令）**框中输入 Firebox 状态 （只读）口令。

4 单击 **Login （登录）**。
WatchGuard System Manager 窗口将显示 Firebox。

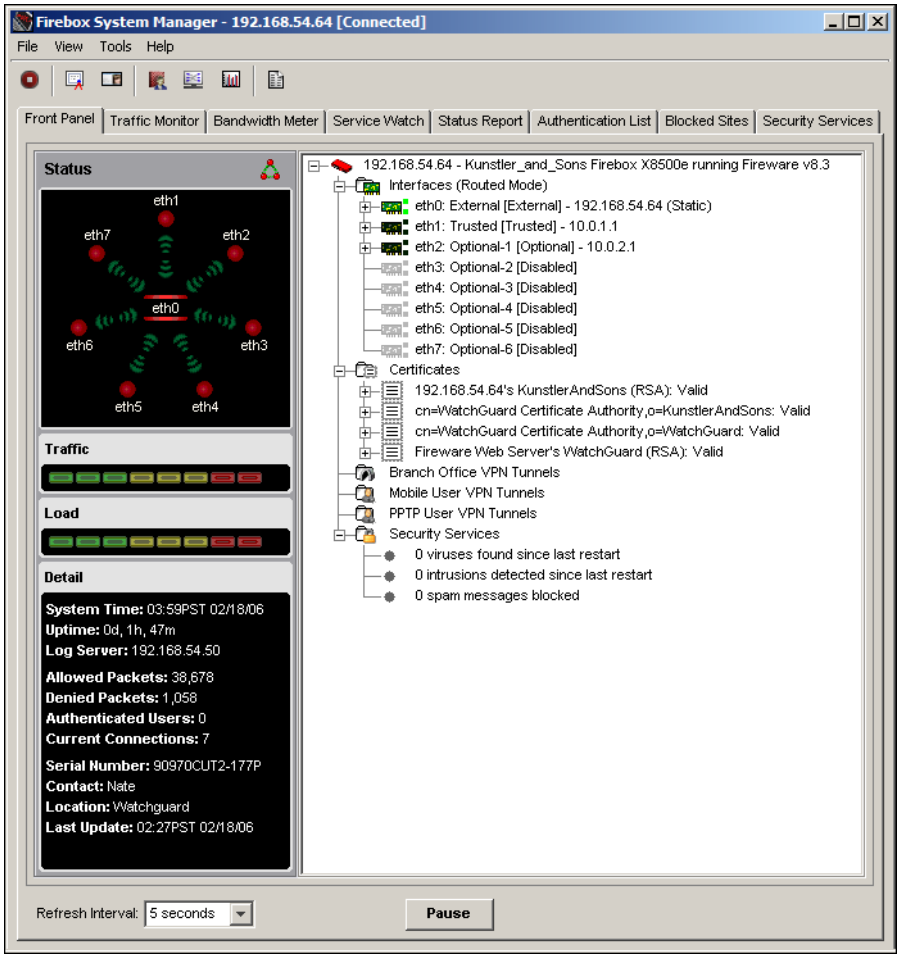
### 打开 Firebox System Manager

1 在 WatchGuard System Manager 中选择 **Device Status （设备状态）**选项卡。

2 选择要用 Firebox System Manager 查看的 Firebox。

3 点击 Firebox System Manager 图标。

出现 Firebox System Manager，然后连接至 Firebox 获取关于状态和配置的信息。




## Firebox System Manager 菜单和工具栏

Firebox® System Manager (FSM) 命令在窗口顶端的菜单中。工具栏中还有最常用任务的按钮。下表列出了菜单和工具栏按钮的功能。

## Firebox System Manager 菜单

| 菜单 | 命令 | 功能 |
|---|---|---|
| 文件 | Settings（设置） | 修改 Firebox System Manager 显示状态信息的方式 |
| | Disconnect（断开连接） | 保持 Firebox System Manager 的开启状态，但断开与被监控 Firebox 的连接 |
| | Reset（复位） | 停止并重新启动 Firebox 上运行的系统组件（软启） |
| | Reboot（重启） | 重新启动当前 Firebox |
| | Shutdown（关机） | 关闭 Firebox |
| | Close（关闭） | 关闭 Firebox System Manager 窗口 |
| 视图 | Certificates（证书） | 列出 Firebox 上的证书 |
| | Licenses（许可证） | 列出 Firebox 当前许可证 |
| | （通信日志） | 打开通信日志，日志中包含登录和握手等成功或失败等信息，是 Firebox 与 Firebox System Manager 之间的连接 |
| 工具 | Policy Manager | 打开具有所选 Firebox 配置的 Policy Manager |
| | HostWatch | 打开当前 Firebox 连接的 HostWatch |
| | Performance Console（性能控制台） | 打开显示 Firebox 性能图表的性能控制台 |
| | Synchronize Time（时间同步） | 使 Firebox 时间与系统时间同步 |
| | Clear ARP Cache（清除 ARP 高速缓存） | 清空所选 Firebox 的 ARP 高速缓存 |
| | Clear Alarm（清除告警） | 清空所选 Firebox 的告警列表 |
| | High Availability | 配置 High Availability 选项 |
| | Change Passphrases（修改口令） | 修改状态和配置口令 |
| 帮助 | Firebox System Manager Help（FSM 帮助） | 打开此应用程序的在线帮助文件 |
| | About（关于） | 显示版本和版权信息 |

## Firebox System Manager 工具栏

| 图标 | 功能 |
|---|---|
|  | 再次启动显示，此图标仅在未连接 Firebox 时显示。 |
|  | 停止显示，此图标仅在连接 Firebox 时显示。 |
|  | 显示 Firebox 上保存的管理和 VPN 证书。 |
|  | 显示此 Firebox 注册和安装的许可证。 |
|  | 启动 Policy Manager，使用 Policy Manager 创建或修改配置文件。 |

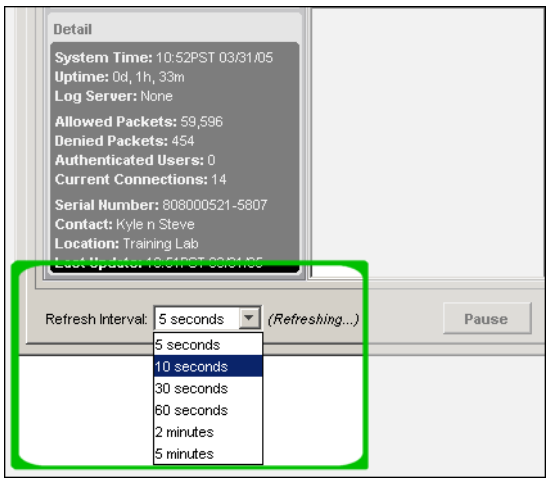
| 图标 | 功能 |
| --- | --- |
|  | 启动显示此 Firebox 连接的 HostWatch。 |
|  | 启动性能控制台，可配置显示 Firebox 状态的图表。 |
|  | 启动通信日志对话框，显示 Firebox System Manager 与 Firebox 的连接。 |

### 设置刷新时间与暂停显示

Firebox System Manager 的所有选项卡在页面顶端都有可设置刷新时间的下拉菜单和可停止显示的 **Pause( 暂停 )** 按钮 :

*刷新时间*

刷新时间是轮询间隔，刷新与显示之间的时间。你可以修改 Firebox System Manager 收到你必须平衡收取信息频率和 Firebox 负载。请务必检查各选项卡上的刷新时间。当选项卡收到要显示的新信息时， **Refresh Interval （ 刷新时间 ）**下拉列表旁将显示 “正在刷新 …” 字样。间隔时间越短，显示更精确，但会使 Firebox 负载更重。在 Firebox System Manager 中，使用 **Refresh Interval （ 刷新时间 ）**下拉列表选择窗口刷新之间的新时间。你可以选择 5 秒、 10 秒、 30 秒、 60 秒、 2 分钟或 5 分钟，也可在框中输入自定义值。




*暂停 / 继续*

你可以点击 **Pause （ 暂停 ）**按钮让 Firebox System Manager 暂时停止页面刷新。点击 **Pause （ 暂停 ）**按钮后，此按钮即变为 **Continue （ 继续 ）**按钮。点击 **Continue （ 继续 ）**可继续刷新页面。

## 查看 Firebox 和网络基本状态

Firebox® System Manager 的 **Front Panel （ 前面板 ）**选项卡显示 Firebox、网络和网络流量的基本信息。

## 使用安全流量显示

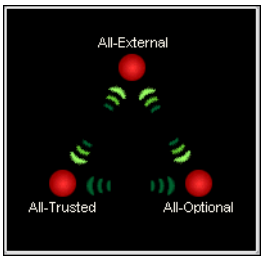
Firebox System Manager 开始有一组指示灯显示 Firebox 接口间流量的方向和大小，显示可为三角形（左下图）或星形（正下和右下图）。

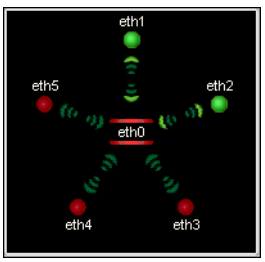
*三角形显示*

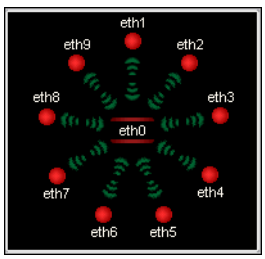
如果 Firebox 只有三个配置接口，三角形的每个角代表一个接口。如果 Firebox 有三个以上的配置接口，三角形的每个角代表一类接口。例如，如果你有六个配置接口，一个外网口，一个受信口，四个可选口，则三角形的 All-Optional（所有可选）一角代表所有四个可选接口。

*星形显示*

星形显示所有进出中心接口的流量。从中心接口向节点接口移动的箭头显示 Firebox 有流量通过。流量从中心接口进入，从节点接口流出。例如，如果 eth1 在中心， eth2 在节点，绿色箭头显示流量从 eth1 流向 eth2。共有两种星形显示 – 一种是六个接口的 Firebox X Core，另一种是十个接口的 Firebox X Peak。




要修改显示，请右键点击，选择 **Triangle Mode（三角模式）**或 **Star Mode（星形模式）**。

## 监控状态信息

星形和三角形的各点显示通过接口的流量。绿色点表示该接口允许流量通过，红色点表示拒绝流量通过，或该接口拒绝部分流量，允许部分流量通过。每个点用不同的箭头表示进出的连接。当流量在两个接口间流动时，箭头朝流量的方向亮起。

在星形图中，多点集中的位置可表示下列情况：

- 红色（拒绝）–– Firebox 拒绝在该接口的连接。
- 绿色（允许）–– 此接口与星形的另一接口（非中心接口）之间存在流量。当此接口与中心接口存在流量时，它们之间的点显示为绿色箭头。

在三角形中，网络流量以三角形的各点显示，只显示空闲或拒绝状态，但存在大量 VPN 隧道交换流量时则例外。隧道交换流量指通过 VPN 向配置为 VPN 网络默认网关的 Firebox 发送的数据包。在这种情况下， Firebox System Manager 流量指示灯可能显示超高流量，但不显示绿灯，因为有更多隧道交换流量进出同一接口。

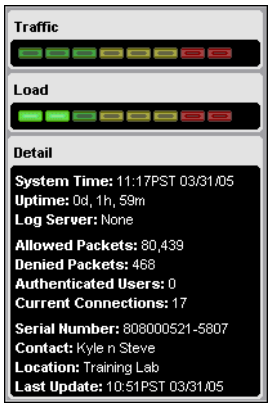
## 设置中心接口

如果使用星形图，可自定义中心显示的接口。点击接口名称或所在点，接口将移动到星形中心，所有其他接口将顺时针移动。如果将某接口移到星形中心，可看见该接口与所有其他接口间的所有流量。默认显示位于中心的外网接口。

## 监控流量、负载和状态

下图 **Security Traffic Display （安全流量显示）**为流量大小指示、处理器负载指示和基本状态信息（详细内容）。

两个条形图表示流量大小和 Firebox 容量。




## Firebox 和 VPN 隧道状态

Firebox System Manager 前面板的右边部分显示以下信息：

- Firebox 状态
- 证书
- 分支办公室 VPN 隧道
- 移动用户和 PPTP VPN 隧道
- 已发现的病毒、入侵和垃圾邮件信息

### Firebox 状态

在 Firebox 状态部分，打开条目可查看以下内容：

- High Availability 功能的状态如果配置正确并可用，将显示备用 Firebox 的 IP 地址。如果安装了 High Availability 但与第二 Firebox 无网络连接，将显示 “无响应” 提示。
- 每个 Firebox 接口的 IP 地址和外网接口的配置模式。
- CA （根）证书和 IPSec （客户端）证书的状态。

在 Firebox System Manager 主窗口中再次打开条目，可查看以下内容：

- 各配置接口的 IP 地址和子网掩码
- 各接口的媒体访问控制 （MAC）地址
- 最后一次重启 Firebox 后收发的数据包数量
- CA 和 IPSec 证书的结束日期和时间
- CA 指纹
- 物理链接 （彩色接口或链接图标表示接口或链接已配置，暗色图标表示接口或链接关闭）状态

### 分支办公室 VPN 隧道

Firebox 状态下方是 BOVPN 隧道内容，共有两种类型的 IPSec BOVPN 隧道: 手动创建的隧道和用管理服务器创建的隧道。

### 移动用户 VPN 隧道

当分支办公室 VPN 隧道变为移动用户 VPN 隧道条目时，显示与分支办公室 VPN 类似的信息。

### PPTP 用户 VPN 隧道

对于 PPTP 用户 VPN 隧道， Firebox System Manager 显示用户名和收发数据包数量。

### 安全服务

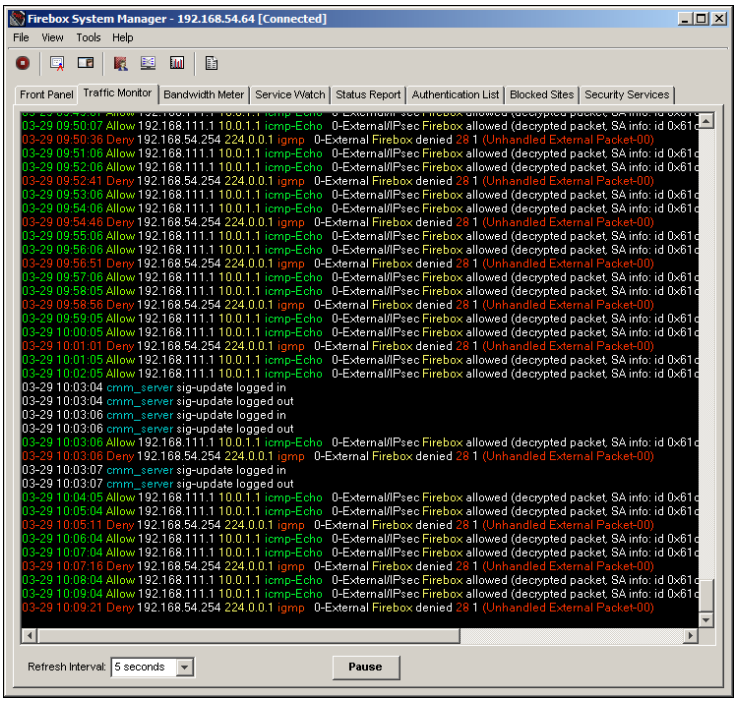
在安全服务项下， Firebox System Manager 显示已检测到的病毒数量、入侵数量和最后一次重启后拦截并有效隔离的垃圾邮件数量。

### 打开和关闭树型视图

要打开显示的某部分，点击条目旁的加号（ + ）或双击条目名称。要关闭某部分，点击条目旁的减号（ – ）。若无加号或减号图标，则表示没有更多信息。

# 监控 Firebox 流量

要查看 Firebox® 日志消息，请点击 **Traffic Monitor （流量监控器）**选项卡。




## 设置日志消息最大数量

你可以修改 Traffic Monitor （流量监控器）上可保存和查看的日志消息的最大数量。当消息已达最大数量时，最新日志消息将覆盖上一条消息。如果处理器速度较慢或 RAM 容量较小，此字段赋值过大会降低管理系统的速度。若需要查看大量日志消息，建议你使用 Log Viewer （日志查看器），见第 91 页 “*开始使用 LogViewer*”。

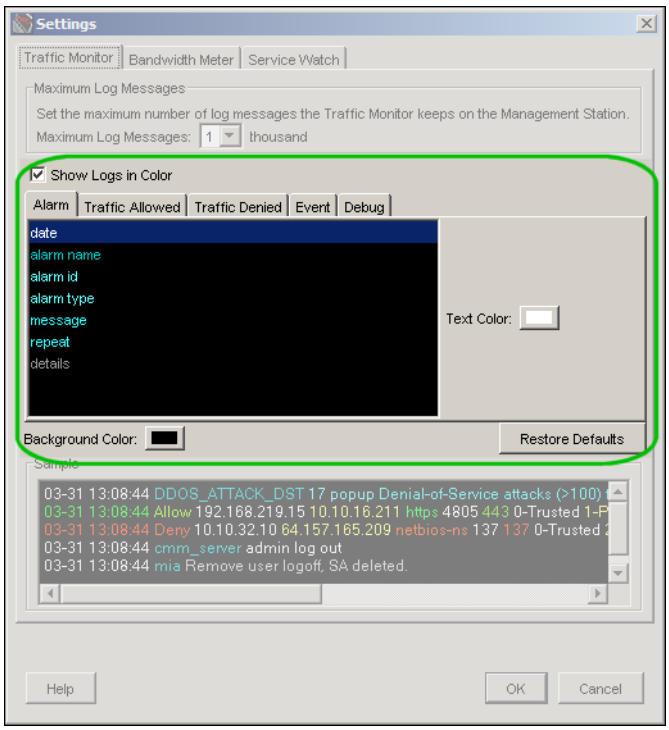
1 在 Firebox System Manager 中，选择 **File （文件）> Settings （设置）**。
出现 Settings （设置）对话框。

2 在 **Maximum Log Messages （日志消息最大数量）**下拉列表中选择希望在 Traffic Monitor （流量监控器）中显示的日志消息数量。点击 **OK （确定）**。
输入的数值使日志消息的数量以千计。

## 用颜色标记日志消息

在 Traffic Monitor （流量监控器）中，你可以使消息显示为不同颜色，每种颜色代表不同类型的信息。

1 在 Firebox System Manager 中，选择 **File （文件）> Settings （设置）**。点击 **Traffic Monitor （流量监控器）**选项卡。




2 要启用或禁用显示颜色，请清除或选择 **Show Logs in Color （用颜色显示日志）**复选框。

3 在 **Alarm （告警）**、**Traffic Allowed （允许流量）**、**Traffic Denied （拒绝流量）**、**Event （事件）**、或 **Debug （调试）**选项卡中，点击要用颜色显示的字段。
选项卡右边的 Text Color （文本颜色）字段显示该字段使用的颜色。

4 要修改颜色，请点击 **Text Color （文本颜色）**旁的颜色控制，选择颜色，点击 **OK （确定）**关闭颜色控制对话框。再点击 **OK （确定）**关闭 **Settings （设置）**对话框。
此字段的信息将在 Traffic Monitor （流量监控器）中以新的颜色显示。对话框底部将显示 Traffic Monitor （流量监控器）的外观示例。

5 你也可为流量监控器选择背景颜色。点击 **Background Color （背景色）**旁的控制箭头，选择颜色，点击 **OK （确定）**关闭颜色控制对话框，再点击 **OK （确定）**关闭 **Settings （设置）**对话框。

你可以取消在此对话框中所做的修改，点击 **Restore Defaults （恢复默认值）**。

## 复制日志消息

要将日志消息复制并粘贴到另一软件程序中，请右键点击消息，选择 **Copy Selection （复制选择）**。若选择 **Copy All （全选）**， Firebox System Manager 将复制所有日志消息。打开另一工具，将消息粘贴进去。

要复制一条以上但非全部日志消息，请使用 Log Viewer （ 日志查看器 ）打开日志文件，然后使用 Log Viewer 复制功能，见 “*日志与通知*”章节。

### 深入了解流量日志消息

要深入了解流量日志消息，你可以 :

*复制源或目的 IP 地址*

制流量日志消息的源或目的 IP 地址，粘贴到另一软件程序中。要复制源 IP 地址，右键点击消息，选择 **Source IP Address （ 源 IP 地址 ）> Copy Source IP Address （ 复制源 IP 地址 )**。要复制目的 IP 地址，右键点击消息，选择 **Destination IP Address （ 目的 IP 地址 ） > Copy Destination IP Address （ 复制目的 IP 地址 )**。

*Ping 源地址或目的地址*

要 ping 流量日志消息的源或目的 IP 地址，请右键点击消息，选择 **Source IP Address （ 源 IP 地址 ）> Ping** 或 **Destination IP Address （ 目的 IP 地址 ）> Ping**，弹出窗口将显示结果。

*跟踪源地址或目的地址路径*

要使用流量日志消息的源或目的 IP 地址跟踪路径命令，请右键点击消息，选择 **Source IP Address （ 源 IP 地址 ）> Trace Route （ 跟踪路径 )** 或 **Destination IP Address （ 目的 IP 地址 ） > Trace Route （ 跟踪路径 )**，弹出窗口将显示跟踪路径结果。

*暂时受禁源或目的 IP 地址*

要暂时封禁流量日志消息的源或目的 IP 地址，请右键点击消息，选择 **Source IP Address （ 源 IP 地址 ）> Block**: [IP address] （ 封禁：IP 地址 ）或 **Destination IP Address （ 目的 IP 地址 ）> Block** [IP address] （ 封禁：IP 地址 )。在 Policy Manager 中，用此命令设置 IP 地址暂时受禁的时间。要使用此命令，必须输入配置密码。

## 清除 ARP 高速缓存

Firebox® 上的 ARP（ 地址解析协议 ）高速缓存保留 TCP/IP 主机的硬件地址（ 亦称 MAC 地址 )。ARP 请求开始前，系统先确认高速缓存中是否存在硬件地址。当网络为透明配置模式时，在安装完成后必须清除 Firebox 上的 ARP 高速缓存。

1 在 Firebox System Manager，选择 **Tools （ 工具 ）> Clear ARP Cache （ 清除 ARP 高速缓存 )**。

2 输入 Firebox 配置口令，点击 **OK （ 确定 )**。
高速缓存即被清空。

当 Firebox 处于透明模式时，此程序仅清除 ARP 表中的内容，并不清除 MAC 表中的内容。如果 MAC 表中的条目超过 2000 条，则最早的 MAC 条目会被删除。若要清除 MAC 表，必须重新启动 Firebox。

## 使用性能控制台

性能控制台是用来绘制显示运行中的 Firebox 不同部分的图表的 Firebox® 工具。要获取信息，需定义确认绘制图表所需信息的计数器。

## 计数器类型

你可以监控以下类型的性能计数器：

*系统信息*
显示 CPU 的使用情况

*接口*
监控并报告所选接口的事件。例如，可设置监控指定接口收到数据包数量的计数器

*策略*
监控并报告所选策略的事件。例如，可设置监控指定策略检测到的数据包数量的计数器。

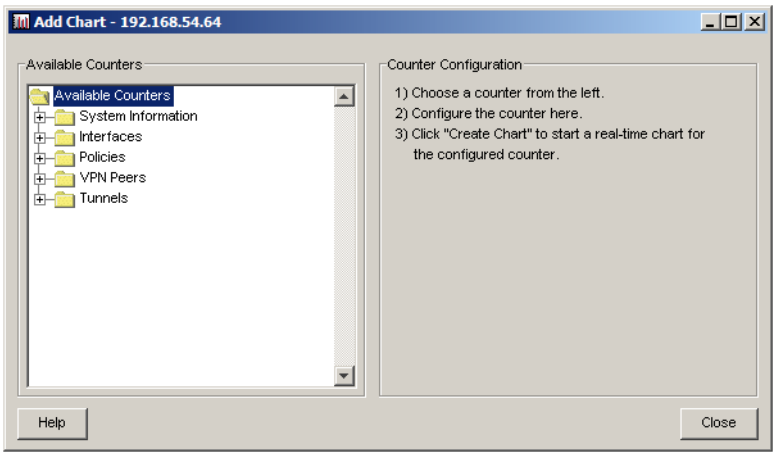
*VPN 对等端*
监控并报告所选 VPN 策略的事件。

*隧道*
监控并报告所选 VPN 隧道的事件。

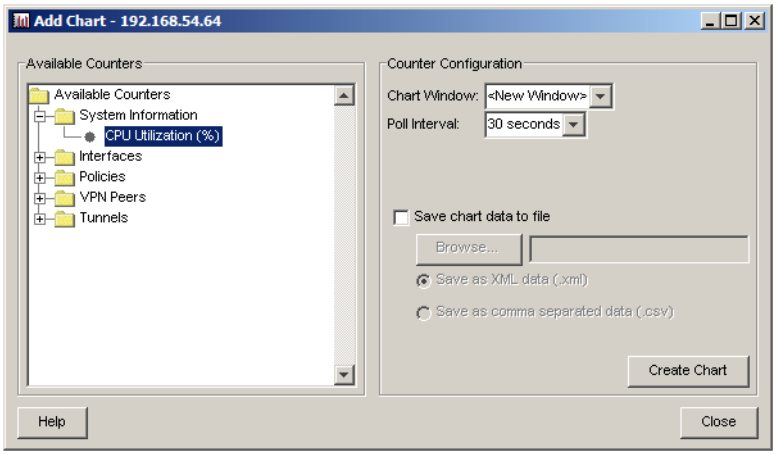
## 定义计数器

要确定任何类别的计数器，按以下步骤操作：

1 在 Firebox System Manager 中，选择 Performance Console （性能控制台）图标，或选择 **Tools（工具）> Performance Console （性能控制台）**。
出现 Add Chart （添加图表）窗口。



2 在 **Add Chart（添加图表）**窗口，打开 **Available Counters（可用计数器）**下方的一个计数器类别。
点击类别名称旁的加号，查看该类中可使用的计数器。点击计数器时， Counter Configuration（计数器配置）字段会自动刷新为与所选计数器相关。



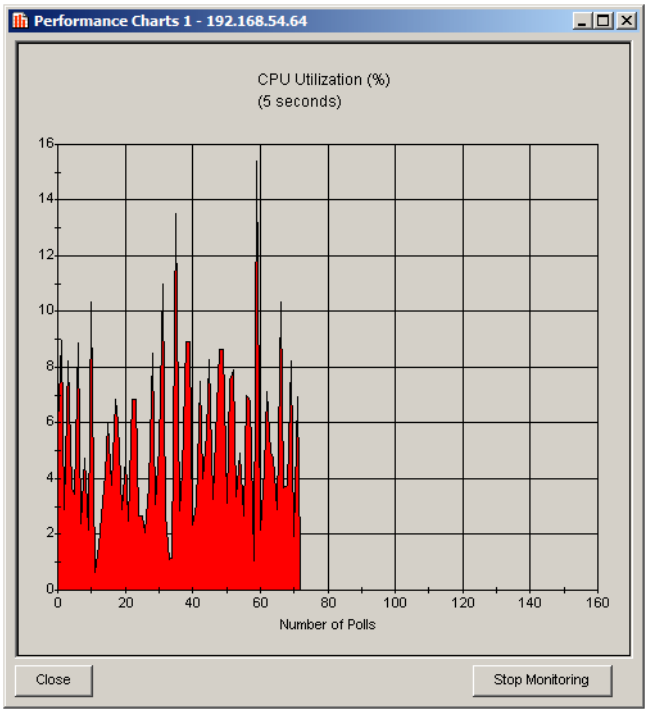

3 如果希望在新窗口中显示图表，请在 **Chart Window（图表窗口）**下拉列表中选择 **New Window（新窗口）**，或选择一个打开窗口的名称，将图表添加到打开的窗口中。

4 在 **Poll Interval**（**轮询间隔**）下拉列表中选择 5 秒和 1 小时之间的时间间隔。
这是性能控制台检查 Firebox 更新信息的频率。

5 添加应用于指定计数器的配置信息。选择指定计数器后，将自动显示以下字段：
- **类型** — 使用下拉列表选择要创建图表的类型。
- **接口** — 使用下拉列表选择图表所用数据的接口。
- **策略** — 使用下拉列表从 Firebox 配置选择图表所用数据对应的策略。若选择策略计数器，点击 **Refresh Policy List（刷新策略列表）**按钮时可更新性能控制台中显示的策略列表。
- **对端 IP** — 使用下拉列表选择图表所用数据对应的VPN端点IP地址。若选择VPN对等端计数器，点击 **Refresh Peer IP List（刷新对端 IP 列表）**按钮可更新性能控制台中显示的策略列表。
- **隧道 ID** — 使用下拉列表选择图表所用数据对应的 VPN 隧道名称。若选择隧道计数器，点击 **Refresh Tunnel ID List（刷新隧道 ID 列表）**按钮时可更新性能控制台中显示的策略列表。如果不知道 VPN 隧道的隧道 ID，可查看 Firebox System Manager Front Panel（前面板）选项卡。

6 选择 **Save Chart Data to File（保存图表数据到文件）**复选框，将性能控制台收集的数据保存到 XML 数据文件或用逗号分隔的数据文件中。
例如，可用 Microsoft Excel 打开 XML 数据文件，查看每次轮询间隔记录的计数器值。可使用其他工具合并多个图表的数据。

7 点击 **Create Chart（创建图表）**为此计数器创建实时图表。




**注释**

能图显示了 CPU 的使用情况。你可以同样的方法为其他功能创建图表。

## 查看性能图表

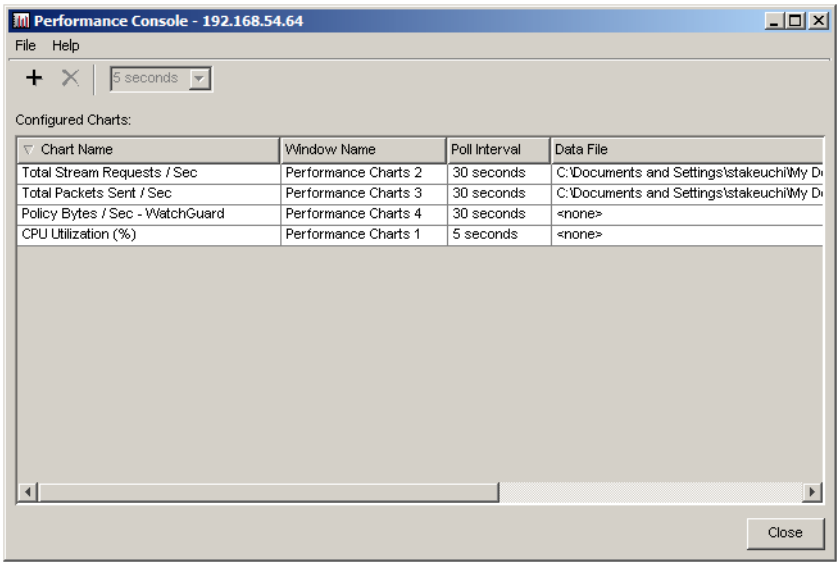
图形显示在实时图表窗口中。你可以在每个窗口显示一个图表，或在同一窗口显示多个图表。图表会根据数据自动缩放至合适大小。

点击 **Stop Monitoring（停止监控）**使性能控制台停止从此计数器获取数据。你可以停止监控器以节省资源，另找时机再重启。

点击 **Close（关闭）**关闭图表窗口。

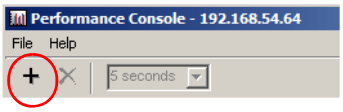
## 使用多个性能控制台图表

主性能控制台窗口显示所有配置和活动性能计数器表。在此窗口中，可为配置的计数器添加新图表或修改轮询间隔。



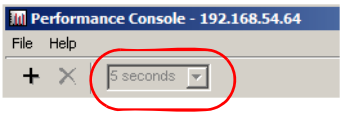

### 添加新图表

要添加新图表，请点击性能控制台工具栏上的加号按钮或选择 **File（文件）> Add Chart（添加图表）**。



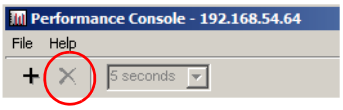

### 修改轮询间隔

要修改性能控制台的轮询间隔，请从列表中选择图表名称。用性能控制台工具栏上的轮询间隔下拉列表修改轮询频率。



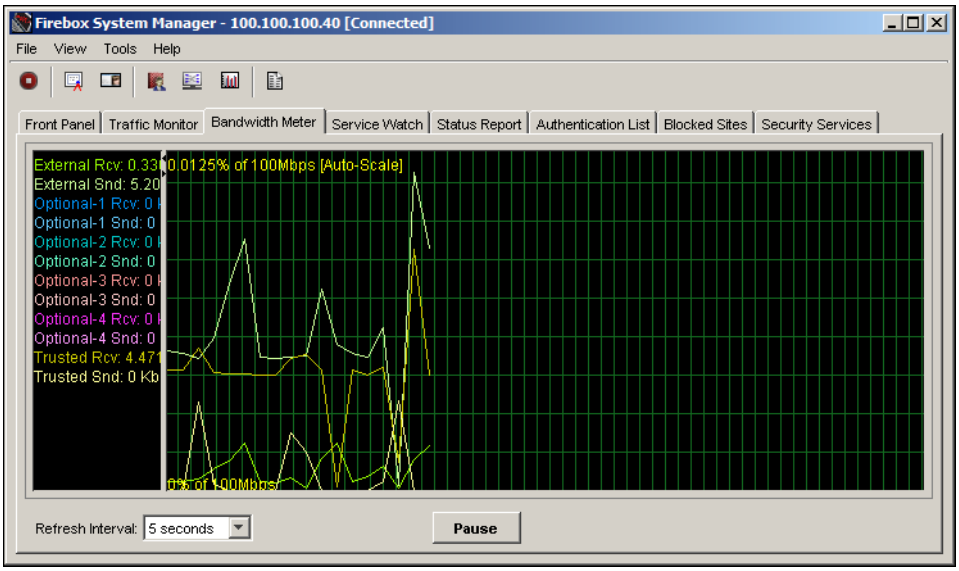

### 删除图表

要删除图表，请从列表中选择图表名称，用性能控制台工具栏上的 X 按钮或选择 **File（文件）> Delete Chart（删除图表）**。



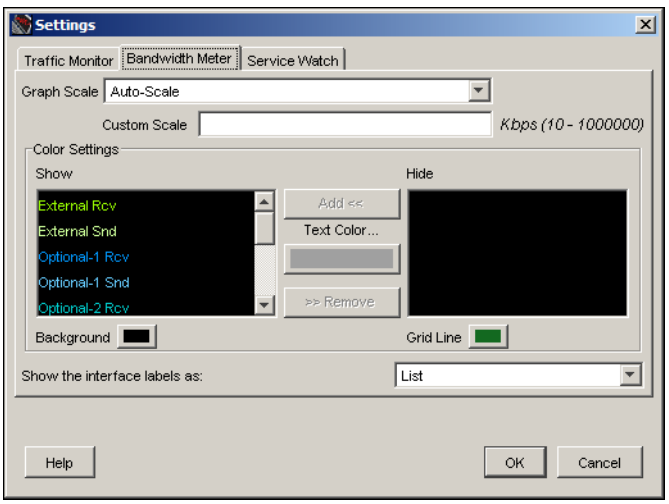
# 查看带宽使用情况

选择 **Bandwidth Meter （带宽计量器）**选项卡查看所有 Firebox® 接口的实时带宽。Y 轴（垂直）表示连接的数量，X 轴（水平）表示时间。点击图表的任何部位，会出现弹出窗口，显示该时刻该点带宽使用情况的详细信息。




要修改带宽显示方式：

1 在 Firebox System Manager 中，选择 **File （文件）> Settings （设置）**，点击 **Bandwidth Meter （带宽计量器）**选项卡。




2 按图中显示的下面步骤操作。

### 修改带宽显示的比例

你可以修改 **Bandwidth Meter （带宽计量器）**选项卡的比例。用 **Graph Scale （图表比例）**下拉列表选择与网络速度的最佳匹配值；也可设置自定义比例，在 **Custom Scale （自定义比例）**文本框中输入每秒千字节的数值。

### 在带宽显示中添加和删除行

- 要在 **Bandwidth Meter（带宽计量器）**选项卡中添加行，请从 Color Settings（颜色设置）的 Hide（**隐藏**）列表中选择接口。用 **Text Color（文本颜色）**控制选择行的颜色，点击 **Add（添加）**，接口名称将以所选颜色显示在 **Show（显示）**列表中。
- 要在 **Bandwidth Meter（带宽计量器）**选项卡中删除行，请从 Color Settings（颜色设置）的 **Show（显示）**列表中选择接口，点击 **Remove（删除）**，接口名称将显示在 **Hide（隐藏）**列表中。

### 修改带宽显示的颜色

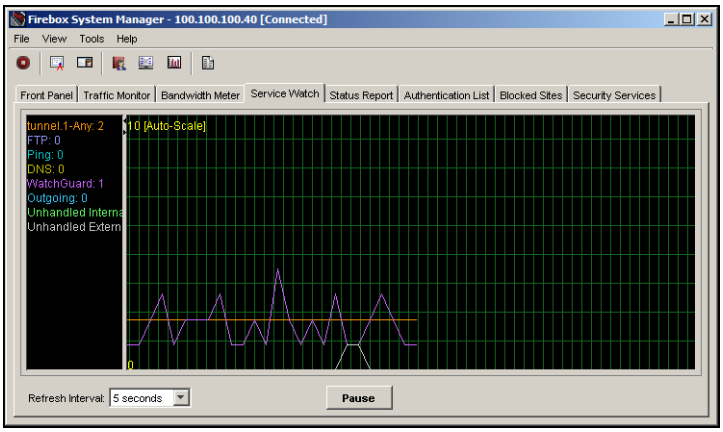
你还可修改 **Bandwidth Meter（带宽计量器）**选项卡显示的颜色。用 **Background（背景）**和 **Grid Line（网格线）**颜色控制框选择新颜色。

### 修改带宽显示中接口显示的方式

一种选择是修改接口名称在 **Bandwidth Meter（带宽计量器）**选项卡左边的显示方式，名称可显示为列表，也可将接口名称显示在对应行旁边。用 **Show the interface（显示接口）**文本作为下拉列表选择 **List（列表）**或 **Tags（选项卡）**。

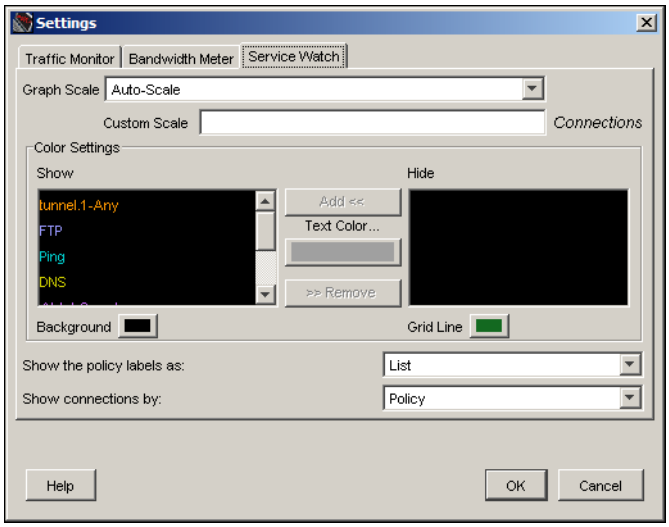
## 按策略查看连接数量

选择 Firebox® System Manager 的 **Service Watch（业务查看）**选项卡查看 Policy Manager 中为 Firebox 配置的策略图表。Y 轴（垂直）表示连接的数量，X 轴（水平）表示时间。点击图表的任何部位，会出现弹出窗口，显示该时刻该点策略使用情况的详细信息。




1 要修改策略显示的方式，请选择 **File（文件）> Settings（设置）**，点击 **Service Watch** 选项卡。

2 按图中显示的下面步骤操作。




### 修改策略显示的比例

你可以修改 **Service Watch** 选项卡的比例。用 **Graph Scale （图表比例）**下拉列表选择与网络流量大小的最佳匹配值；也可设置自定义比例，在 **Custom Scale （自定义比例）**文本框中输入连接数量。

### 在策略显示中添加和删除行

- 要在 **Service Watch** 选项卡中添加行，请从 Color Settings（颜色设置）对话框中的 **Hide（隐藏）**列表中选择策略。用 **Text Color （文本颜色）**控制器选择行的颜色，点击 **Add （添加）**，接口名称将以所选颜色显示在 **Show （显示）**列表中。
- 要在 **Service Watch** 选项卡中删除行，请从 Color Settings（颜色设置）对话框中的 **Show（显示）**列表中选择策略，点击 **Remove** （**删除**），接口名称将显示在 **Hide （隐藏）**列表中。

### 修改策略显示的颜色

你可以修改 **Service Watch** 选项卡显示的颜色。用 **Background （背景）**和 **Grid Line （网格线）**颜色控制框选择新颜色。

### 修改策略显示中策略名称显示的方式

你可以修改策略名称在 **Service Watch** 选项卡左边的显示方式。名称可显示为列表，也可将接口名称显示在对应行旁边。用 **Show the policy labels as （将策略标签显示为）**下拉列表选择 **List**（**列表**）或 **Tags**（标签）。

### 按策略或规则显示连接

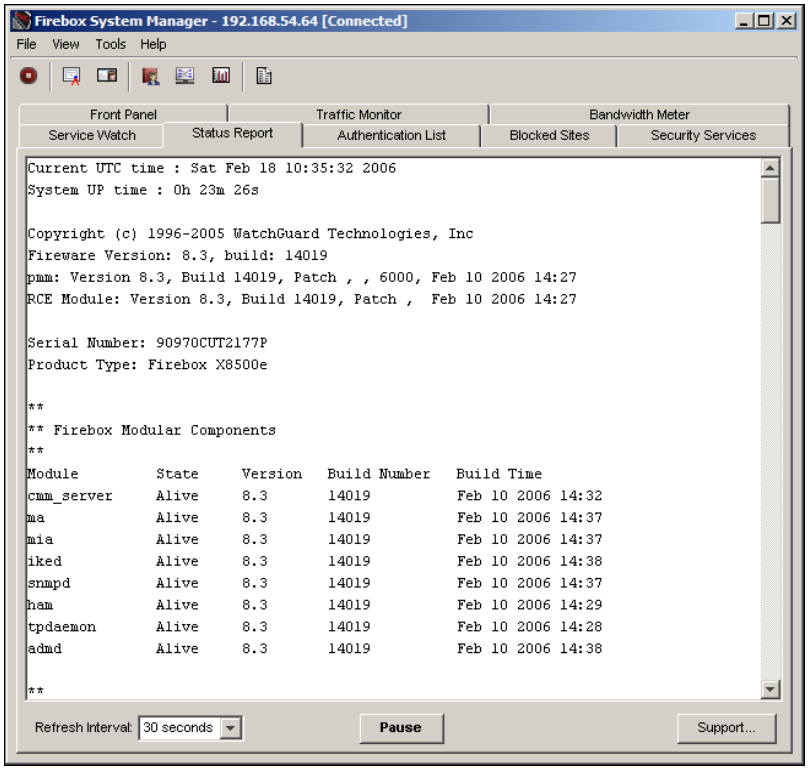
**Service Watch** 选项卡可按策略或规则显示连接数量。若按策略显示，则一行会显示多个规则。用 **Show connections by （按…显示连接）**下拉列表选择显示设置。

# 查看 Firebox 状态信息

共有四个选项卡显示 Firebox® 状态和配置：**Status Report （状态报告）**、 **Authentication List （验证列表）**、 **Blocked Sites （受禁站点）**和 **Security Services （安全服务）**。

## 状态报告

**Status Report （状态报告）**选项卡显示 Firebox 流量和性能的统计信息。




Firebox 状态报告包含以下信息：

*正常运行时间和版本信息*
Firebox 正常运行时间、 WatchGuard® Firebox 系统软件版本、 Firebox 型号和设备软件版本。此外，还有 Firebox 产品组件状态和版本列表。

*日志服务器*
所有已配置日志服务器的 IP 地址。

*日志选项*
用快速安装向导或 Policy Manager 配置的日志消息选项。

*内存和平均负载*
Firebox 内存使用（以内存字节数显示）和平均负载的统计信息。平均负载有三个值，通常显示最后一分钟、 5 分钟和 15 分钟的平均值。数值超过 1.00 (100%) 表示部分线程正在排队等候，直到资源可用为止。（系统负载超过 1.00 并不意味着系统过载。）

*进程*
进程 ID、进程名称及进程状态。

*网络配置*

Firebox 的网卡信息：接口名称及其软硬件地址和子网掩码。显示信息还包括本地路由信息和 IP 别名。

*受禁网站列表*

当前手动受禁站点和任何当前例外。暂时受禁站点显示在永久 **Blocked Sites**（**受禁站点**）选项卡中。

*接口*

此部分显示每个 Firebox 接口，以及配置接口类型（外部、受信或可选）及其状态和封包数量的信息。

*路由*

Firebox 核心路由表。可使用这些路由查找各目的地址使用的 Firebox 接口。
此处还显示动态路由程序接受的动态路由。

*ARP 表*

Firebox 上的 ARP 表，用于匹配 IP 地址和硬件地址。（如果设备处于透明模式，只将 ARP 表的内容用于排除通过接口连接第二网的连接故障。）

*动态路由*

显示 Firebox 使用的动态路由组件（若有）。

*刷新时间*

显示更新信息的频率。

*支持*

点击 **Support**（**支持**）打开 **Support Logs**（**支持日志**）对话框，可设置诊断日志文件的保存位置。支持日志保存为 *.tgz 格式。按支持代表要求创建此文件用于故障排除。

## 验证列表

Firebox System Manager 的 **Authentication List**（**验证列表**）选项卡显示经过身份验证可使用 Firebox 的所有人员的信息。共有四列显示每位经过身份验证用户的信息：

*用户*

身份验证时提供的用户名。

*类型*

经身份验证的用户类型：防火墙、 MUVPN 或 PPTP。

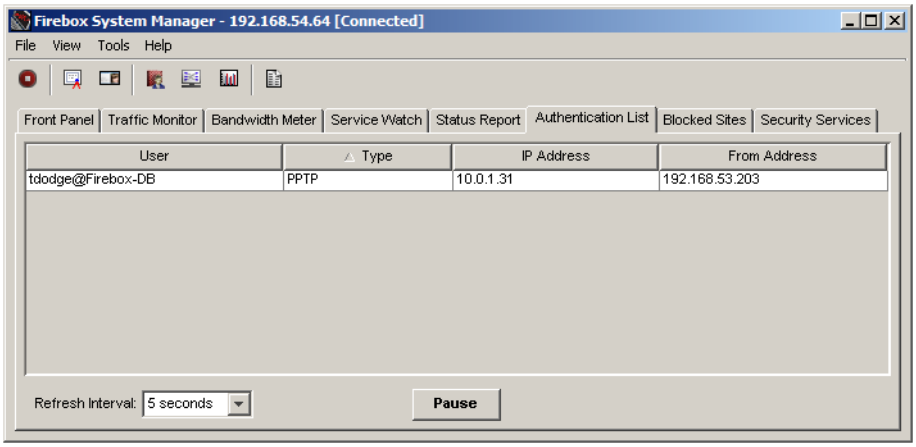
*IP 地址*

用户使用的内部 IP 地址。对于 MUVPN 和 PPTP 用户，此处显示的 IP 地址为 Firebox 分配的 IP 地址。

*来源地址*

用户验证身份的计算机的 IP 地址。对于 MUVPN 和 PPTP 用户，此处显示的 IP 地址为其连接 Firebox 的计算机的 IP 地址。对于防火墙用户， IP 地址和来源地址为同一地址。

可单击列标题对用户进行排序，也可将经过身份验证的用户从列表中删除，要删除用户，请右键点击用户名，然后停止其验证的会话。




## 受禁站点

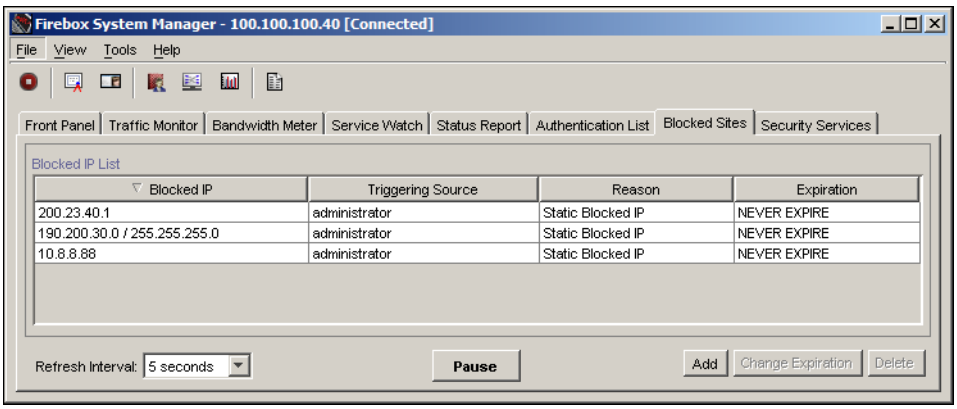
Firebox System Manager 的 **Blocked Sites List（受禁站点列表）**选项卡显示所有暂时受禁的外部 IP 地址的 IP 地址。许多事件都可能导致 Firebox 将 IP 地址添加到 **Blocked Sites （受禁站点）**选项卡中：如端口空间探测、欺骗式攻击、地址空间探测或配置的事件。

每个 IP 地址旁边是其从 **Blocked Sites （受禁站点）**选项卡中被删除的时间。你可以使用 Policy Manager 中的 **Blocked Sites （受禁站点）**对话框来调整 IP 地址保留在列表中的时间。

### 添加和删除站点

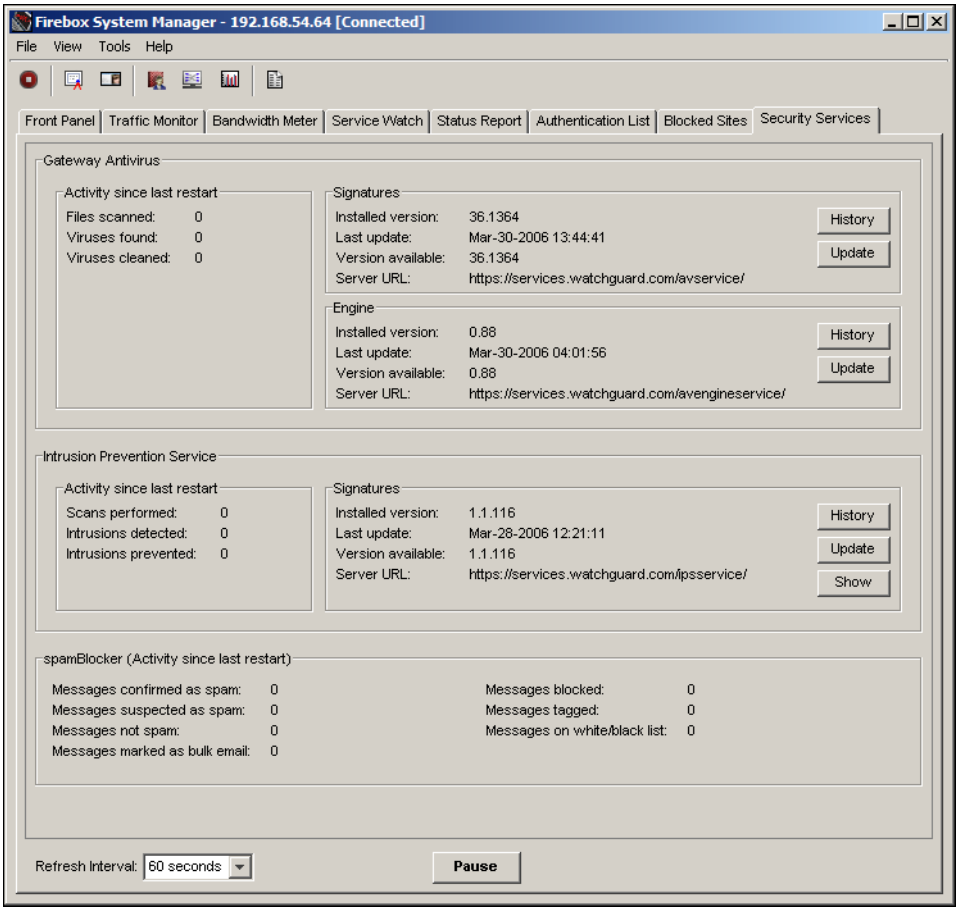
**Add （添加）**可将站点暂时添加到受禁站点列表。点击 **Change Expiration （修改到期时间）**可修改从列表中删除该站点的时间。 **Delete （删除）**可将站点从受禁站点列表中删除。

只有在用配置口令打开 Firebox 的情况下才能从列表中删除站点。




## 安全服务

**Security Services(安全服务)**选项卡包括Gateway AntiVirus(网关防毒)和Intrusion Prevention(入侵防范)信息。




### 网关防毒

此对话框提供有关网关防毒功能的信息。

*上一次重启后的操作*

- 已扫描文件： 最后一次重启 Firebox 后进行病毒扫描的文件数量。
- 已发现病毒： 最后一次重启 Firebox 后扫描文件中检测到的病毒数量。
- 已清除病毒： 最后一次重启 Firebox 后删除的病毒感染文件数量。

*特征*

- 安装版本： 已安装特征的版本号。
- 上次更新日期： 上次特征更新的日期。
- 可用版本： 是否推出新版本的特征。
- 服务器 URL：Firebox 用于查看是否可更新的 URL 以及用于下载更新的 URL。
- 历史记录： 单击可显示所有特征更新列表。
- 更新： 单击可更新病毒特征。此按钮只在推出病毒特征新版本时才可用。

*引擎*

- 安装版本： 已安装引擎的版本号。
- 上次更新日期：上次引擎更新的日期。
- 可用版本：是否推出新版本的引擎。
- 服务器 URL：Firebox 用于查看是否可更新的 URL 以及用于下载更新的 URL。
- 历史记录：单击可显示所有引擎更新列表。
- 更新：单击可更新防毒引擎。此按钮只在推出引擎新版本时才可用。

### 入侵防范服务

此对话框提供有关基于特征的入侵防范服务功能的信息。

*上一次重启后的操作*

- 已进行的扫描：最后一次重启 Firebox 后进行病毒扫描的文件数量。
- 已检测到的入侵：最后一次重启 Firebox 后扫描文件中检测到的病毒数量。
- 已防范的入侵：最后一次重启 Firebox 后删除的病毒感染文件数量。

*特征*

- 安装版本：已安装特征的版本号。
- 上次更新日期：上次特征更新的日期。
- 可用版本：是否推出新版本的特征。
- 服务器 URL：Firebox 用于查看是否可更新的 URL 以及用于下载更新的 URL。
- 历史记录：单击可显示所有特征更新列表。
- 更新：点击此按钮可更新入侵防范特征。此按钮只在推出入侵防范特征新版本时才可用。
- 显示：点击此按钮可下载并显示所有当前 IPS 特征的列表。下载特征后，可按特征 ID 查找特征。

### spamBlocker

*上一次重启后的操作*

- 被确认为非垃圾邮件、群发或可疑邮件的消息数量。

– 拦截和标识的消息数量。
– 你创建的 spamBlocker 例外列表拦截或允许的消息的数量（你创建的拒绝其他站点的例外有时称为黑名单；你创建的允许其他站点的例外有时称为白名单）。

# 使用 HostWatch

HostWatch 是显示受信网络与外部网络之间的网络连接的图形用户界面，并显示有关用户、连接和网络地址转换等信息。

连接源主机和目的主机的行使用颜色来表示连接类型。你可以对颜色进行修改。默认颜色如下：

- **红色** — Firebox® 拒绝连接。
- **蓝色** — 连接使用代理服务器。
- **绿色** — Firebox 使用网络地址转换进行连接。
- **黑色 —** 正常连接（连接被接受，未使用代理服务器或网络地址转换）。

显示服务类型的图标位于 HTTP、 Telnet、 SMTP 和 FTP 的服务器条目旁边。

启动 HostWatch 后不会立即出现域名服务器（DNS）解析。当 HostWatch 配置为 DNS 解析时，将用主机或用户名代替 IP 地址。如果 Firebox 无法识别主机或用户名， IP 地址将保留在 HostWatch 窗口中。

如果 HostWatch 使用 DNS 解析，管理工作站可通过 Firebox 发送大量 NetBIOS 数据包（UDP 137），阻止此现象的唯一方法是在 Windows 中关闭 NetBIOS over TCP/IP。

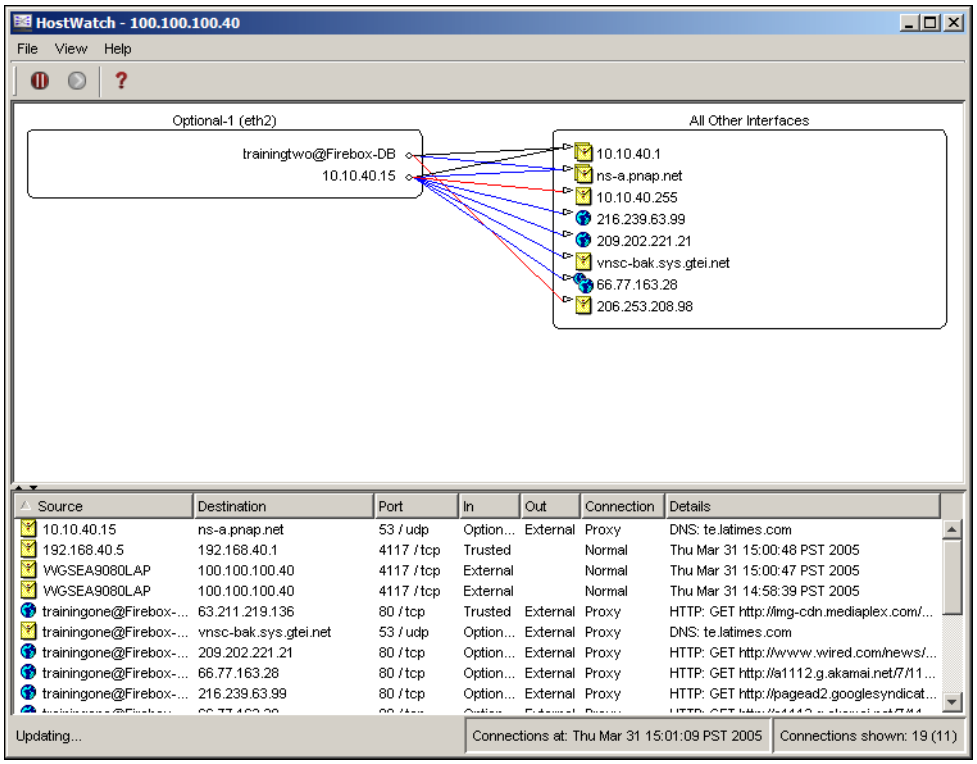
要启用 **HostWatch**，请点击 Firebox System Manager 中的 **HostWatch** 图标，或选择 **Tools（工具）> HostWatch**。

## HostWatch 窗口

HostWatch 窗口的上部分为左右两部分。左边可设置接口，右边显示所有其他接口。 HostWatch 在左边显示配置接口上进行的连接。要选择接口，请右键点击当前接口名称。选择新接口。

双击其中一边中的某项，打开包含该项的连接的 **Connections For** 对话框，对话框显示连接信息，包括 IP 地址、端口号、时间、连接类型和方向。

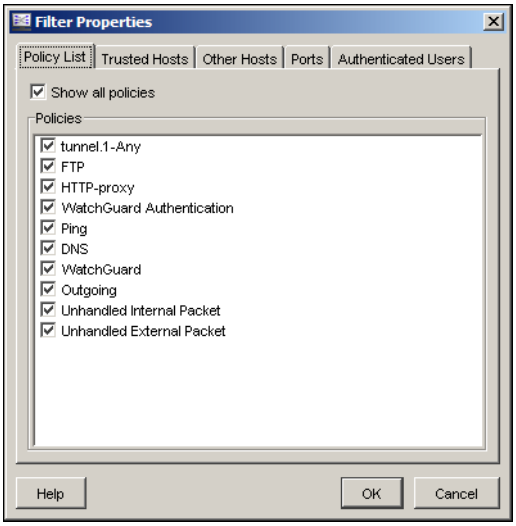
窗口上部只显示所选接口上进行的连接， HostWatch 窗口下部则显示所有接口上进行的所有连接。信息以表格显示，并显示端口和连接创建的时间。




## 控制 HostWatch 窗口

你可以将 HostWatch 窗口修改为只显示必要的项目。可利用此功能监控指定主机、端口或用户。

1 在 HostWatch 中选择 **View （视图）> Filter （过滤）**。



2 点击选项卡可监控 **Policy List （策略列表）**、 **External Hosts （外部主机）**、 **Other Hosts （其他主机）**、 **Ports （端口）**或 **Authenticated Users （通过身份验证的用户）**。

3 在不希望显示的项目选项卡中，取消对话框中的复选框的选择。

4 在希望显示的项目选项卡中，输入要监控的 IP 地址、端口号或用户名。点击 **Add （添加）**，对 HostWatch 必须监控的每一项目重复此操作。

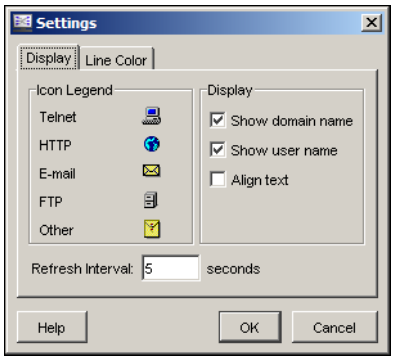
5 点击 **OK （确定）**。

## 修改 HostWatch 视图属性

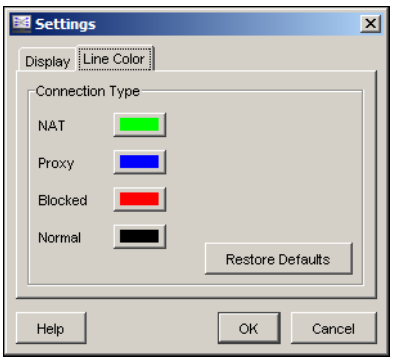
你可以修改 HostWatch 显示信息的方式。例如， HostWatch 可用主机名代替地址显示。

1 在 HostWatch 中选择 **View （视图）>Settings （设置）**。

2 用 **Display （显示）**选项卡修改主机在 HostWatch 窗口中的显示方式。




3 用 **Line Color （行颜色）**选项卡修改 NAT （网络地址转换）、 proxy （代理服务器）、 blocked （受禁）和 normal （正常）连接的行的颜色。




4 点击 **OK （确定）**关闭 **Settings （设置）**对话框。

## 从 HostWatch 添加受禁站点

要从 HostWatch 添加 IP 地址到受禁站点列表，请右键点击连接，使用弹出窗口从连接选择要添加到受禁站点列表的 IP 地址。要封禁 IP 地址，必须设置时间并输入配置口令。

## 暂停 HostWatch 显示

你可以使用工具栏上的 **Pause （ 暂停 ）**和 **Continue （ 继续 ）**图标来暂时停止和重新启动显示。也可使用 **File （ 文件 ）> Pause （ 暂停 ）and File （ 文件 ）> Continue （ 继续 ）**。

# 第 5 章　Firebox 基本管理

Firebox® 要正确运行，就必须具备将安全策略应用于网络流量的必要信息。除安全策略外， Policy Manager （ 策略管理器 ）还提供配置 Firebox 基本设置的用户界面。本章介绍如何：

- 添加、删除和查看许可证
- 设置使用 NTP 服务器的 Firebox
- 设置 Firebox 时区
- 对 Firebox 进行 SNMP 配置
- 修改 Firebox 口令
- 为 Firebox 命名以方便标识 （ 非 IP 地址 ）
- 恢复 Firebox

## 使用许可证

如果您购买了可选服务并将授权码添加到配置文件中，就增加了 Firebox® 的功能。获得新授权码时，请务必按与授权码一同提供的指示说明在 LiveSecurity 网站上激活新功能，将新密钥添加到 Firebox。

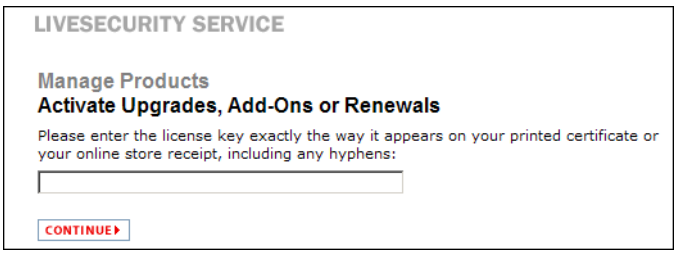
### 激活新功能

激活新功能前，必须取得未在 LiveSecurity 网站上注册的 WatchGuard® 授权码证书。此授权码位于书面授权码证书上或您的网上购物收据上 （ 若您通过 WatchGuard 网上商店购得 ）。

1　打开网页浏览器，连接 https://www.watchguard.com/activate。

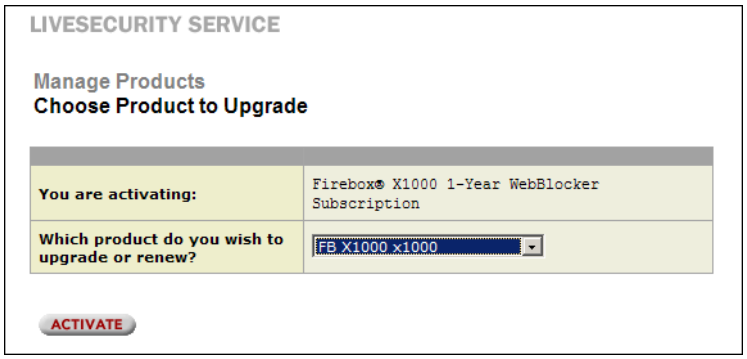
2　如果您尚未登录 LiveSecurity，将进入 LiveSecurity 登录页面。输入您的 LiveSecurity 用户名和口令。

3 在 **Options**（选项）下，选择 **Upgrades**（更新）、**Renewals**（续订）、**Services**（服务），点击 **Continue**（继续）。
将显示 Activate Upgrades, Add-Ons, or Renewals（激活更新、 Add-Ons 或续订）页面。




4 输入证书上的产品授权码，包括连字符。

5 点击 **Continue**（继续）。
将显示 Choose Product to Upgrade（选择要升级的产品）页面。

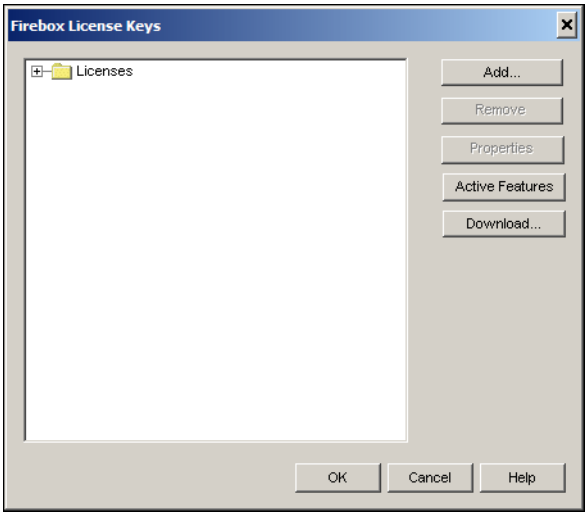



6 从下拉列表中选择要升级或续订的 Firebox。如果注册 Firebox 时已添加了 Firebox 名称，则列表中会显示该名称。选择 Firebox 后，点击 **Activate**（激活）。

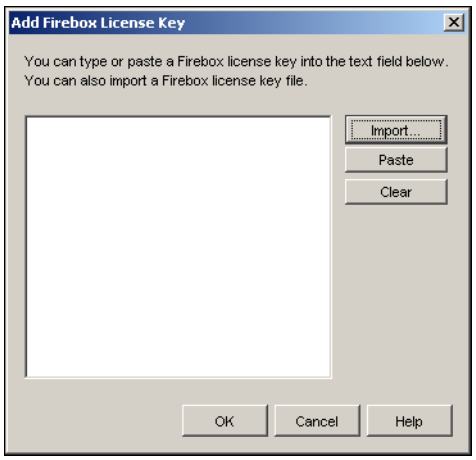
7 将显示 Retrieve Feature Key（取回密钥）页面。在 Windows Start（开始）菜单中，打开 Notepad（写字板）或可保存文本的任何程序，将完整的密钥从本页面复制到文本文件中，保存在您的电脑上，点击 **Finish**（完成）。

## 添加许可证

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> Licensed Features（授权功能）**。
将出现 Firebox License Keys（Firebox 授权码）对话框，显示可用的许可证。




2 点击 **Add（添加）**。
将出现 Add Firebox License Keys（添加 Firebox 授权码）对话框。建议您添加新密钥之前先删除旧密钥。




3 点击 **Import（导入）**查找密钥文件或将密钥文件内容粘贴到对话框中。

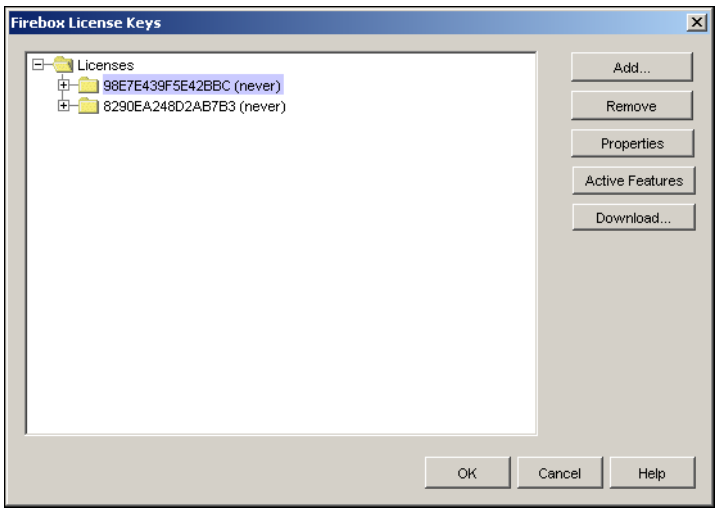
4 双击 **OK（确定）**。
此时，管理工作站已可使用上述功能。在某些情况下，配置功能的新对话框和菜单命令会显示在 Policy Manager（策略管理器）中。

5 将配置保存到 Firebox。
配置文件保存到 Firebox 后才可在 Firebox 上使用功能。

## 删除许可证

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> Licensed Features（授权功能）**。
将出现 Firebox License Keys（Firebox 授权码）对话框，

2 展开 **Licenses**（**许可证**），选择要删除的许可证 ID，然后点击 **Remove**（**删除**）。

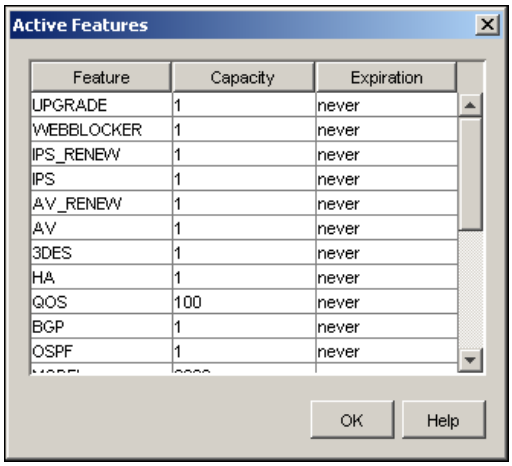



3 点击 **OK**（**确定**）。

4 将配置保存到 Firebox。

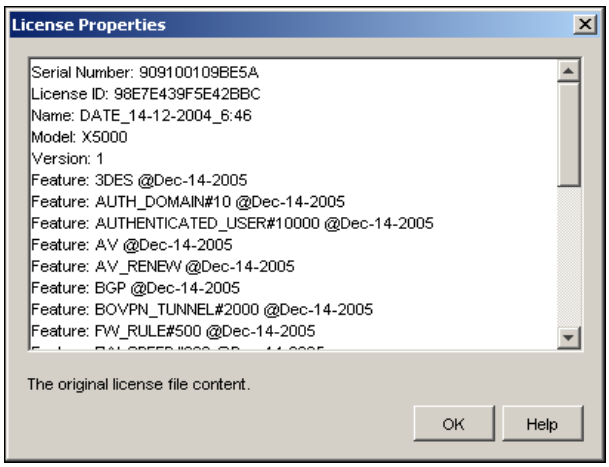
## 查看活动功能

要查看所有授权功能列表，请选择授权码，点击 **Active Features**（**活动功能**）。**Active Features** 对话框将显示各功能及其容量和到期日。



### 查看许可证属性

要查看许可证属性，请选择授权码，点击 **Properties （属性）**。**License Properties （许可证属性）**对话框将显示该许可证对应的 Firebox 序列号、许可证 ID 和名称、 Firebox 型号和版本号以及 Firebox 可用功能。



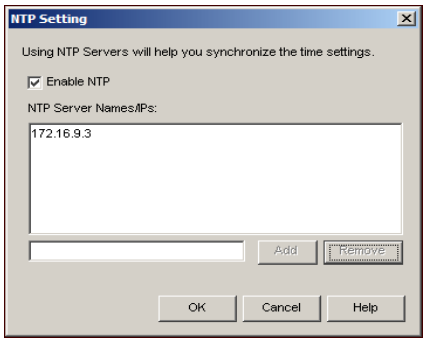

### 下载授权码

如果您的许可证文件不是最新版本，可从 Firebox 下载任何一份许可证文件到管理工作站上。要从 Firebox 下载授权码，请选择授权码，点击 **Download（下载）**，将显示对话框，提示您输入 Firebox 的状态口令。

## 设置 NTP 服务器

时钟时间。 Firebox® 可将其时钟与 Internet NTP 服务器同步。

1 在 Policy Manager （策略管理器）中，选择 **Setup （设置）> NTP**。
出现 NTP Settings （NTP 设置）对话框。




2 选择 **Enable NTP （启用 NTP）**复选框。

3 在 **NTP Server Names/IPs（NTP 服务器名称 /IPs）**列表下的框中输入要使用的 NTP 服务器的 IP 地址。点击 **Add （添加）**。
Firebox 最多可使用三个 NTP 服务器。

4 点击 **OK （确定）**。

## 设置友好名称和时区

您可为 Firebox® 命名，以便在日志文件和报告中使用。若不进行此操作，日志文件和报告将使用 Firebox 外网接口的 IP 地址。许多客户若在 DNS 系统中注册了全称域名，则使用该名称。如果使用管理服务器为 Firebox 配置 VPN 隧道和证书，则必须为 Firebox 命名。

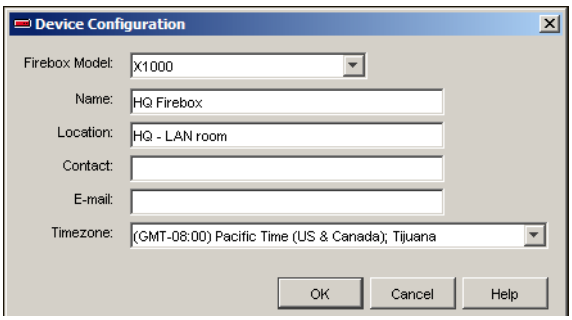
Firebox 时区控制日志文件和 LogViewer、Historical Reports（历史报告）和 WebBlocker 等工具中显示的日期和时间。将 Firebox 实际位置的时区设置为 Firebox 时区，此时区设置使日志消息能显示正确时间。 Firebox 系统时间默认设置为格林威治标准时间（GMT）。

1 在 Policy Manager （策略管理器）中，点击 **Setup （设置）> System （系统）**。
出现 Device Configuration （设备配置）对话框。

2 在 **Name （名称）**文本框中输入要为 Firebox 命名的特殊名称，点击 **OK （确定）**。
如果使用了不允许的字符，弹出通知将给出提示。

3 在 **Location（位置）**和 **Contact（联系人）**字段中输入有助于识别和维护 Firebox 的任何信息。

4 在 **Time zone （时区）**下拉列表中选择时区，点击 **OK （确定）**。



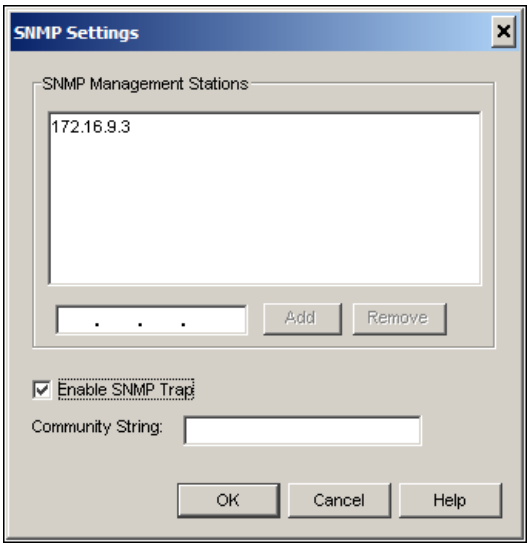

## 使用 SNMP

简单网络管理协议（SNMP）是一组监控和管理网络的工具，运用提供 SNMP 服务器所管理或监控设备的配置信息的管理信息库（MIBs）。通过 Fireware® 设备软件， Firebox® 支持 SNMPv1 和 SNMPv2c。

您可将 Firebox 设置为接受来自 SNMP 服务器的 SNMP 轮询，也可设置为向 SNMP 服务器发送陷阱。

## 启用 SNMP 轮询

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> SNMP**。




2 输入 Firebox 连接 SNMP 服务器时必须使用的 **Community String（社群字符串）**，点击 **OK（确定）**。
社群字符串允许访问设备的统计信息，其作用相当于无线 SSID 或群组 ID。所有 SNMP 请求都必须包含此社群字符串。如果社群字符串正确，设备将提供所请求的信息。如果社群字符串不正确，设备将丢弃请求，不作响应。

3 点击 **OK（确定）**，将配置保存到 Firebox。
现在 Firebox 即可接收 SNMP 轮询。

## 启用 SNMP 陷阱

SNMP 陷阱是 Firebox 向 SNMP 管理系统发送的事件通知。陷阱确定条件何时产生，如超过预设临界值的数值。要启用 Firebox 发送 SNMP 陷阱的功能，请按以下步骤操作：

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> SNMP**。

2 在 **SNMP Settings（SNMP 设置）**对话框中选择 **Enable SNMP Trap（启用 SNMP 陷阱）**复选框。

3 在 **SNMP Management Stations（SNMP 管理工作站）**列表下方的框中输入 SNMP 服务器的 IP 地址，点击 **Add（添加）**。

4 输入 Firebox 连接 SNMP 服务器时必须使用的 **Community String（社群字符串）**，点击 **OK（确定）**。
社群字符串的作用如同允许访问设备统计信息的用户 ID 或密码。所有 SNMP 请求都必须包含此社群字符串。如果社群字符串正确，设备将提供所请求的信息。如果社群字符串不正确，设备将丢弃请求，不作响应。

5 向 Firebox 添加 SNMP 策略。在 Policy Manager（策略管理器）中，选择 **Edit（编辑）> Add Policy（添加策略）**（或点击加号图标），展开 **Packet Filters（数据包过滤器）**，选择 **SNMP**，然后点击 **Add（添加）**。
将显示 New Policy Properties（新策略属性）对话框。

6 在 **From（从）**框下，点击 **Add（添加）**。在出现的 **Add Address（添加地址）**对话框中，点击 **Add Other（添加其他）**。
出现 Add Member（添加成员）对话框。

7 在 **Choose Type**（**选择类型**）下拉列表中，选择 **Host IP**（**主机 IP**）。在 **Value**（**值**）字段中输入 SNMP 服务器计算机的 IP 地址。

8 点击 **OK**（**确定**）两次，返回新策略的 **Policy**（**策略**）选项卡。

9 在 **To**（**至**）框下，点击 **Add**（**添加**）。

10 在出现的 **Add Address**（**添加地址**）对话框中，选择 **Available Members**（**可用成员**）下的 **Firebox**，点击 **Add**（**添加**）。

11 点击 **OK**（**确定**）、**OK**（**确定**）和 **Close**（**关闭**），将配置保存到 Firebox。

您可将 Firebox 设置为发送 Policy Manager（策略管理器）中任何策略的陷阱。编辑触发陷阱的策略。双击 Policy Manager（策略管理器）中显示的策略图标，编辑配置。在 **Edit Policy Properties**（**编辑策略属性**）对话框中，选择 **Properties**（**属性**）选项卡，点击 **Logging**（**日志**），选择 **Send SNMP Trap**（**发送 SNMP 陷阱**）复选框。

### 使用 MIBs

具有 Fireware® 设备软件的 WatchGuard® System Manager 支持两种管理信息库（MIBs）：

- 公共 MIBs 用于 Fireware 产品，安装 Fireware 时复制到 WatchGuard 管理工作站上，此类 MIBs 包括 IETF 标准和 MIB2。
- 专用 MIBs 是 WatchGuard 创建的 MIBs，提供 Firebox 指定组件的基本监控信息，包括 CPU 和内存使用情况以及接口和 IPSec 量度。

安装 WatchGuard System Manager 时， MIBs 即安装到 My Documents\My WatchGuard\Shared WatchGuard\SNMP。

Firebox 支持以下只读对象 MIBs：

- RFC1155-SMI
- SNMPv2-SMI
- RFC1213-MIB
- RAPID-MIB
- RAPID-SYSTEM-CONFIG-MIB

## 修改 Firebox 口令

Firebox® 使用两个口令：

- 状态口令
  允许访问 Firebox 的只读密码或口令
- 配置口令
  允许管理员为创建安全口令而完全访问 Firebox 的可读写密码

建议您：

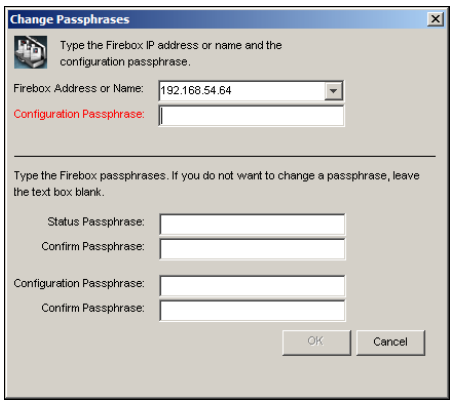
- 使用大小写字符、数字和特殊字符的组合作密码（如 Im4e@tiN9）。
- 不要使用标准字典里的词作密码，即使以不同顺序或以另一种语言来使用。造一个只有您自己认识的新缩略词。
- 不要使用名字，因为攻击者很容易查找到企业名称、熟悉的名称或名人的名字。

另一项安全措施就是定期修改 Firebox 口令。要进行修改，您必须拥有配置口令。

1 在 Policy Manager （策略管理器）中，打开 Firebox 上的配置文件。

2 点击 **File （文件）> Change Passphrases （修改口令）**。
将显示 Open Firebox （打开 Firebox）对话框。

3 在 **Firebox** 下拉列表中，选择 Firebox 或输入 Firebox 的 IP 地址或名称。输入 Firebox 配置（可读写）口令，点击 **OK （确定）**。
出现 Change Passphrases （修改口令）对话框。




4 输入并确认新的状态 （只读）和配置 （可读写）口令。状态口令必须不同与配置口令。

5 点击 **OK （确定）**。
新的 flash 图像和新口令保存到 Firebox。 Firebox 将自动重新启动。

# 恢复 Firebox

如果要将 Firebox® 恢复为出厂默认设置或用全新配置对 Firebox 进行重新设置，可使用 Firebox 恢复程序。 Firebox X Core 或 Peak e 系列恢复程序不同与旧版 Firebox X Core 或 Peak 的恢复程序。请确认对 Firebox 使用正确的程序。

## 重新设置 Firebox X e 系列设备

要用新配置对 Firebox X Core 或 Peak e 系列设备进行重新设置，请使用网络快速安装向导。有关网络快速安装向导的详细信息请参阅 “入门”章节。

## 重新设置 Firebox X Core 或 Peak （非 e 系列）

重新设置早期型号的 Firebox X Core 或 Peak 时，即用新图像代替 Firebox 上的现有图像。您可使用快速安装向导对 Firebox 进行重新配置，这是重新设置 Firebox 的最简便方法，也是最常用的方法。

但有时也不能使用快速安装向导对 Firebox 进行重新设置。使用快速安装向导时，必须要能创建管理工作站与 Firebox 的网络连接，并在网络中 “搜索到” Firebox ；如果不行，可使用本手册中介绍的手动重置程序。

开始此程序前必须拥有最新 Firebox 密钥。

要手动重新设置 Firebox：

1 关闭 Firebox，按下 Firebox 正面的向上箭头。

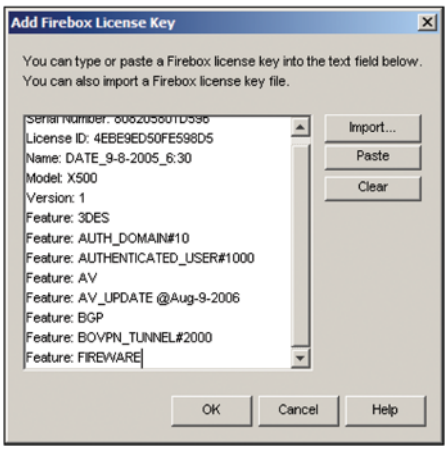

2 打开Firebox时一直按住向上箭头按钮，直到液晶显示屏显示Firebox正在系统B或安全模式下运行。
当 Firebox 在系统 B 模式下运行时，处于出厂默认设置模式。在出厂默认模式下， Firebox 受信接口设置为 10.0.1.1。

3 用以太网交叉网线连接 WatchGuard 管理工作站和 Firebox 的受信接口。
受信接口在 Firebox 上标为接口 1。

4 将管理工作站上的 IP 地址改为 10.0.1.2（或可连接到 Firebox 受信接口 10.0.1.1 的其他 IP 地址）。
最好从管理工作站 ping 受信接口，确认有可用的网络连接。

5 打开 Policy Manager （策略管理器），您可打开已有配置文件，或使用 **File （文件）**下拉菜单中的可用选项创建新的配置文件。

6 选择 **Setup （设置）> Licensed Features （授权功能），点击 Add （添加）**，如有必要，将密钥复制到文本框中。




7 准备就绪后，选择 **File （文件）> Save （保存）> To Firebox （至 Firebox）**。将配置保存到 Firebox 的 10.0.1.1IP 地址，管理口令为 “admin”。

8 Firebox 使用新配置重启后，最好修改其口令。选择 **File（文件）> Change Passphrases（修改口令）**设置新口令。

9 现在您可将 Firebox 重新接回到网络中，用新配置中设置的 IP 地址和口令进行连接。
如果没有修改 IP 地址或口令，可用口令 “admin”连接到受信 IP 地址 10.0.1.1。

## 用 fbxInstall 重新设置 Firebox

如果快速安装向导和手动重置程序不能解决问题，可用命令行工具 fbxinstall 将 Firebox 恢复到出厂设置。

此程序在 Firebox 闪存盘上安装新的文件系统和操作系统，在闪存盘损坏时很有必要。开始前请确认管理工作站上已安装了 Fireware®。

要使用 fbxinstall：

1 用串口连接线连接 Firebox 和管理工作站。
如果有多个 COM 端口，请留意所使用的端口。

2 打开命令提示符窗口。

3 输入 fbxinstall <temporary eth0 IP address>。
此处输入的虚拟 IP 地址必须为与串口连接线连接 Firebox 的计算机位于同一网络中的未使用的 IP 地址。例如，您的 IP 地址为 172.168.1.35，则输入：fbxinstall 172.168.1.36。此 IP 地址用于连接 Firebox，完成重新设置操作，但并非实际分配给 Firebox。

4 Fbxinstall 过程完成后，启动快速安装向导，对 Firebox 进行新配置。

# 第 6 章　基本配置设定

在网络中安装了 Firebox® 并通过基本配置文件开始运行后，即可根据贵单位要求添加自定义配置设定。本章介绍了如何执行部分基本配置和维护任务，有些任务在使用 Firebox 过程中需完成数次，其他任务则只需执行一次。

上述基本配置任务包括：

- 打开本地机或 Firebox 上的配置文件
- 将配置文件保存到本地机或 Firebox 上
- 创建和恢复 Firebox 备份镜像
- 使用别名
- 配置 Firebox 全局设置
- 设置策略中将使用的基本计划表
- 远程管理 Firebox

## 打开配置文件

Fireware 或 Fireware Pro 的 Policy Manager（策略管理器）是可用来创建、修改和保存配置文件的软件工具。配置文件扩展名为 .xml，包括所有配置数据、选项、 IP 地址及购成 Firebox® 安全策略的其他信息。使用 Policy Manager，可轻松查看并修改配置文件。

您可利用 Policy Manager 进行下列操作：

- 打开 Firebox 上的当前配置文件
- 打开保存在本地硬盘上的配置文件
- 创建新的配置文件

### 打开可用的配置文件

网络管理员的一项常见工作是对当前安全策略进行修改。例如，贵公司购买了一套新的软件程序，则必须为软件厂商的服务器开启一个端口和协议。为此，必须用 Policy Manager （策略管理器）修改配置文件。

## 使用 WatchGuard System Manager

1 在 Windows 桌面上点击 **Start（开始）> All Programs（所有程序）> WatchGuard System Manager 8.3 > WatchGuard System Manager**。
WatchGuard® System Manager 8.3 是 Start（开始）菜单图标文件夹的默认名称，安装时可修改此文件夹名称。

2 在 WatchGuard System Manager 中选择 **File（文件）> Connect To Device（连接到设备）**。

或，
点击 WatchGuard® System Manager 工具栏上的 Connect to Device（连接到设备）图标，将出现 Connect to Firebox（连接到 Firebox）对话框。

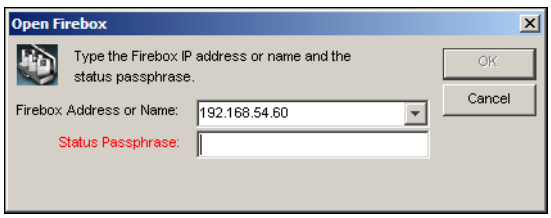
3 使用下拉列表选择 Firebox，或输入其受信 IP 地址。输入状态口令，点击 **OK（确定）**。
设备将显示在 WatchGuard System Manager 的 Device Status（设备状态）选项卡中。

4 在 **Device Status（设备状态）**选项卡中选择 Firebox，然后选择 **Tools（工具）> Policy Manager（策略管理器）**。

或，
点击 WatchGuard System Manager 工具栏上的 Policy Manager 图标， Policy Manager 将打开，并将正在使用的配置文件放置到所选 Firebox 上。

## 使用 Policy Manager（策略管理器）

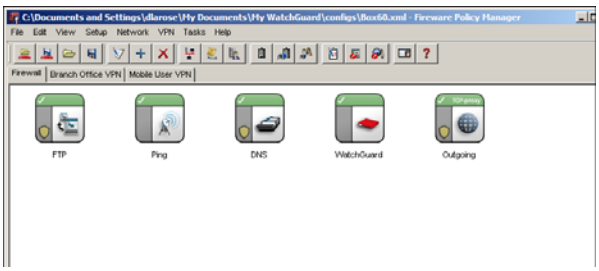
1 在 Policy Manager 中，点击 **File（文件）> Open（打开）> Firebox**。
将显示 Open Firebox（打开 Firebox）对话框。
如果出现 “无法连接” 的错误提示，请再重试。




2 在 **Firebox Address or Name（Firebox 地址或名称）**下拉列表中，选择一个 Firebox。
您也可输入 IP 地址或主机名称。

3 在 **Passphrase（口令）**文本框中输入 Firebox status (read-only) 口令。
此处请使用状态口令。向 Firebox 保存新配置时必须使用配置口令。

4 点击 **OK（确定）**。
Policy Manager（策略管理器）将打开配置文件并显示设置。




若无法打开 Policy Manager，请尝试以下步骤：

- 如果输入口令后马上又出现 **Connect to Firebox（连接到 Firebox）**对话框，请检查大写锁定键是否关闭，输入的口令是否正确。请记住口令是要区分大小写的。

- 如果 **Connect to Firebox（连接到 Firebox）**对话框超时，请检查受信接口和计算机是否有链接。请确认 Firebox 输入的受信接口 IP 地址是否正确，并检查您的计算机 IP 地址是否与 Firebox 受信接口处于同一网络。

### 打开本地配置文件

有些网络管理员认为保存多个版本的 Firebox 配置文件较为有用。例如，如果要使用新的安全策略，建议您先将旧的配置文件保存到本地硬盘上。如果以后不想使用新的配置，就可以恢复旧版本。用户可打开管理工作站可连接的任何网络驱动器上的配置文件。

1 在 WatchGuard System Manager 中，选择 **Tools（工具）> Policy Manager（策略管理器）**（或点击 Policy Manager 图标）。

2 选择 **File（文件）> Open（打开）> Configuration File（配置文件）**。

或，
点击 WatchGuard System Manager 工具栏上的 Open File（打开文件）图标，将出现标准 Windows 打开文件对话框。

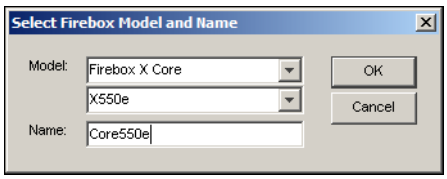
3 使用 **Open（打开）**对话框查找并选择配置文件。点击 **Open（打开）**。
Policy Manager 将打开配置文件并显示设置。

### 创建新的配置文件

快速安装向导可为 Firebox 创建基本配置文件，建议您将其作为各配置文件的基础，但您也可使用 Policy Manager 创建新的只有默认配置属性的配置文件。

1 在 WatchGuard System Manager 中，选择 **Tools（工具）> Policy Manager（或点击 Policy Manager 图标）**。

2 在 Policy Manager 中，选择 **File（文件）> New（新建）**。
将出现 Select Firebox Model and Name（选择 Firebox 型号和名称）对话框。




3 使用 **Model（型号）**下拉列表选择 Firebox 型号。由于每个型号都有其独特的功能，请选择与硬件设备相同的型号。

4 输入 Firebox 名称，该名称将显示为配置文件名称。

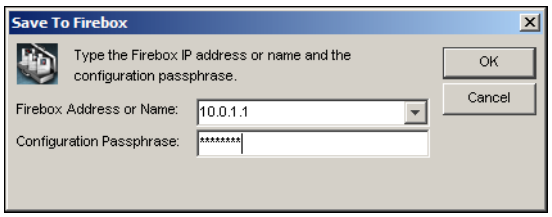
5 点击 **OK（确定）**。
Policy Manager 将创建文件名为 < 名称 >.xml 的新配置文件，其中 < 名称 > 即为前面输入的 Firebox 名称。

## 保存配置文件

创建新配置文件或修改当前配置文件后，可将其直接保存到上 Firebox®，也可保存到本地硬盘。

### 将配置保存到 Firebox

1 在 Policy Manager （策略管理器）中，点击 **File （文件）> Save （保存）> To Firebox （至 Firebox）**。
将出现 Save to Firebox （保存到 Firebox）对话框。




2 在 **Firebox Address or Name（Firebox 地址或名称）**下拉列表中，输入 IP 地址或名称，或选择一个 Firebox。如果使用 Firebox 名称，该名称必须通过 DNS 解析。
输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

3 输入 Firebox 配置口令，向 Firebox 保存文件时必须使用配置口令。

4 点击 **OK （确定）**。

### 将配置保存到本地硬盘

1 在 Policy Manager 中，点击 **File （文件）> Save （保存）> As File （存为文件）**。
也可使用 CTRL-S 命令，将出现标准 Windows 打开文件对话框。

2 输入文件名称。
默认程序是将文件保存到 WatchGuard 目录下，您也可浏览任何从管理工作站可连接到的文件夹。出于安全考虑，建议您将文件保存到其他用户无法访问的安全文件夹中。

3 点击 **Save （保存）**。
配置文件即保存到本地硬盘上。

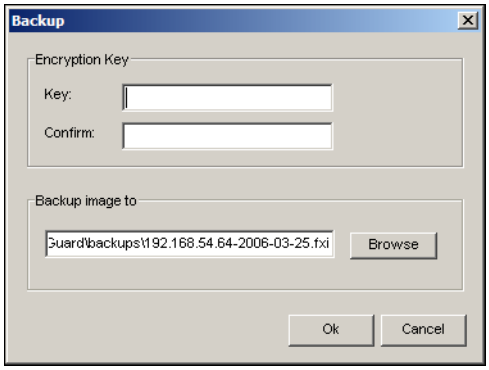
## 关于 Firebox 备份镜像

Firebox 备份镜像是加密并保存的 Firebox 闪存盘镜像的备份，包括 Firebox 设备软件、配置文件、许可证和证书。您可将备份镜像保存到管理工作站上或网络中的目录下。建议您对 Firebox 镜像进行定期备份，并在对 Firebox 配置进行重大修改或升级 Firebox 或其设备软件前先创建 Firebox 的备份镜像。

### 创建 Firebox 备份镜像

1 在 Policy Manager 中，选择 **File （文件）> Backup （备份）**。

2 输入 Firebox 配置口令，
出现 Backup（备份）对话框。




3 输入并确认密钥。
此密钥用于为备份文件加密。如果丢失或遗忘此密钥，则无法恢复备份文件。

4 选择要保存备份文件的目录，点击 **OK（确定）**。
扩展名为 “.fxi” 的备份文件的默认位置为 C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address> - <date>.fxi。

### 恢复 Firebox 备份镜像

1 在 Policy Manager 中，选择 **File（文件）> Restore（恢复）**。

2 输入 Firebox 配置口令，点击 **OK（确定）**。

3 输入创建备份镜像时使用的密钥。
Firebox 将恢复备份镜像并重新启动，重启时将使用备份镜像。请等待两分钟再重新连接到 Firebox。

如果无法成功恢复 Firebox 镜像，可按第 65 页 “*恢复 Firebox*” 中的程序重新设置 Firebox。

## 使用别名

别名是标识一组主机、网络或接口的快捷方式。使用别名可轻松创建安全策略，因为 Firebox® 允许在创建策略时使用别名。

以下是 Policy Manager 中包含的部分默认别名，可供用户使用：

*Any-Trusted*
这是所有配置为 “受信” 接口的 Firebox 接口的别名（在 Policy Manager 中定义时，选择 **Network（网络）> Configuration（配置）**）以及通过此类接口可访问的任何网络。

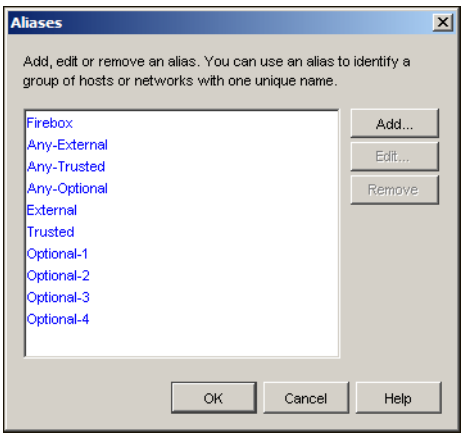
*Any-External*
这是所有配置为 “外网” 类型的 Firebox 接口的别名（在 Policy Manager 中定义时，选择 **Network（网络）> Configuration（配置）**）以及通过此类接口可访问的任何网络。

*Any-Optional*
这是所有配置为 “可选” 类型的 Firebox 接口的别名（在 Policy Manager 中定义时，选择 **Network（网络）> Configuration（配置）**）以及通过此类接口可访问的任何网络。

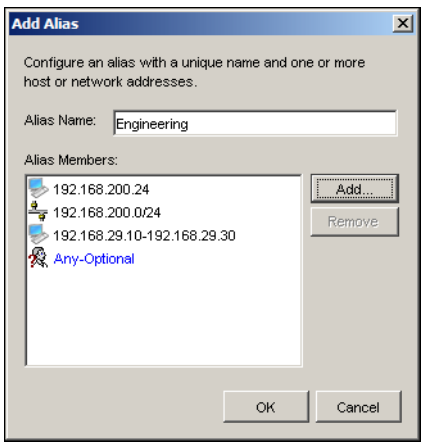
别名不同于用户验证时使用的用户名或群组名。通过用户验证，用户可利用名称而非 IP 地址监控连接。用户可使用用户名和密码验证身份，访问互联网协议。有关用户验证的详情，请参阅第 111 页的 “*如何进行用户验证*”。

## 创建别名

1 在 Policy Manager 中，选择 **Setup （设置）> Aliases （别名）**。
出现 Aliases （别名）对话框。




2 点击 **Add （添加）**。
出现 Add Alias （添加别名）对话框。




3 在 **Alias Name （别名）**文本框中，输入标识别名的特殊名称。
配置安全策略时此名称将显示在列表中。
4 点击 **Add （添加）**向别名成员列表添加主机 IP 地址、网络 IP 地址、主机 IP 地址范围或别名。
该成员将显示在别名成员列表中。
5 双击 **OK （确定）**两次。

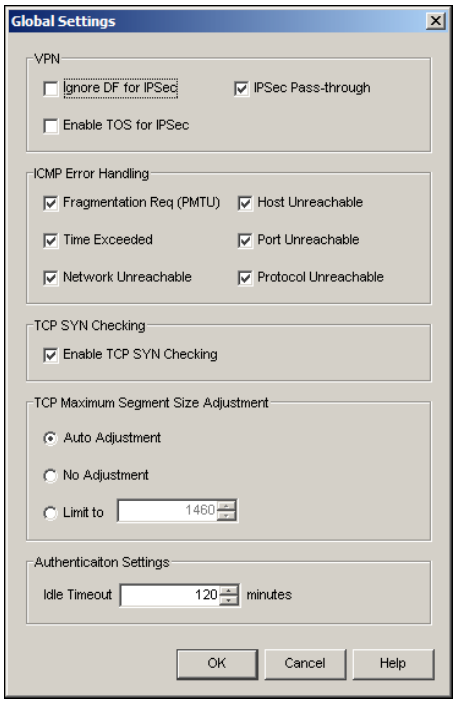
# 使用全局设置

在 Policy Manager 中，用户可选择控制多项 Firebox® 功能的设置。要设置的基本参数如下：

- IPSec VPN
- ICMP 错误处理
- TCP SYN 检查
- TCP 最大长度调整
- 验证空闲超时

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> Global Settings（全局设置）**。
出现 Global Settings（全局设置）对话框。

2 对下图中的各类全局设置进行配置。




## VPN

全局 VPN 设置如下：

*忽略 IPSec 的 DF 位（不分段位）*

忽略 IP 报头的 **Don't Fragment bit（不分段位）**设置。如果设置为忽略， Firebox 将数据桢分割成可在 IPSec 数据包中插入 ESP 或 AH 报头的片段。

*IPSec 隧道连接*

如果用户必须创建从一台 Firebox 后到另一台 Firebox 的 IPSec 连接，则不要选择 **IPSec Pass–through** 复选框，以启用 IPSec 隧道连接功能。例如，若移动员工处于配有 Firebox 的客户位置，可使用 IPSec 创建到其网络的 IPSec 连接。本地 Firebox 若要正确允许外发 IPSec 连接，也必须向 Policy Manager 添加 IPSec 策略。

*启用 IPSec 的 TOS 位*

TOS（服务类型）位是 IP 报头中的一组四位标志，可指示路由设备提供优先级高于或低于其他数据报的 IP 数据报。 Fireware® 用户可选择允许 IPSec 隧道让带有 TOS 标志的数据包通过，部分互联网服务提供商丢弃所有设置了 TOS 标志的数据包。

如果不选择 **Enable TOS for IPSec（启用 IPSec 的 TOS 位）**复选框，所有 IPSec 数据包均无 TOS 位。如果以前曾设置了 TOS 位，Fireware 封锁 IPSec 报头中的数据包时， TOS 位将被清除。

如果选择了 **Enable TOS for IPSec（启用 IPSec 的 TOS 位）**复选框，且原始数据包设置了 TOS 位，Fireware 在封锁 IPSec 报头中的数据包时将保留 TOS 位。如果原始数据包没有设置 TOS 位， Fireware 在封锁 IPSec 报头中的数据包时将不会设置 TOS 位。

## ICMP 错误处理

互联网控制信息协议（ICMP）控制连接中出现的错误，用于两种类型的操作：

- 将错误情况通知客户端主机。
- 进行网络探测，查找关于网络的一般特征。

每次事件发生时， Firebox 均发送一条与所选参数之一相匹配的 ICMP 错误信息。如果拒绝上述 ICMP 信息，可通过防止网络探测来增强安全性，但也可能造成不完整连接的超时延迟及应用程序问题。全局 ICMP 错误处理参数及其描述如下：

*分段请求（PMTU）（路径最大传输单元）*

IP 数据报必须分段，但由于 IP 报头中设置了 Don't Fragment bit（不分段位）而使此操作被禁止。

*超时*

因 Time to Live（生存期）字段过期，数据报被丢弃。

*网络不可达*

数据报无法送达网络。

*主机不可达*

数据报无法送达主机。

*端口不可达*

数据报无法送达端口。

*协议不可用*

数据报的协议片段无法发送。

## TCP SYN 检查

全局 TCP SYN 设置如下：

*启用 TCP SYN 检查*

此功能确保在 Firebox 允许数据连接之前进行 TCP 三次握手。

## TCP 最大报文段长度调整

TCP 报文段可设置为指定长度，用于 TCP/IP 第三层网络负担（如 PPPoE、 ESP、 AH 等）较重的连接。若此长度未正确配置，用户将无法访问部分网站。全局 TCP 最大报文段长度调整设置如下：

*自动调整*
Firebox 检查所有最大报文段长度（MSS）协商并将 MSS 更改为相应值。

*不调整*
Firebox 不修改 MSS。

*仅限于*
用户可设置长度调整限制。

### 验证设置

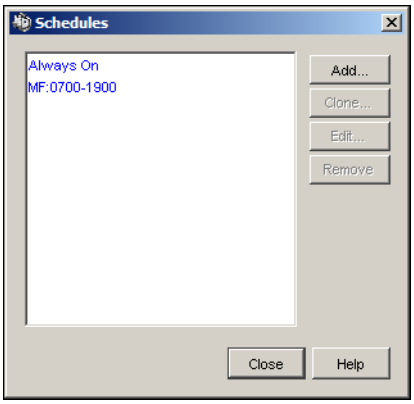
全局验证设置如下：

*空闲超时*
将验证空闲超时的单位设置为分钟：如果经过身份验证的用户在超时前未使用验证创建连接，对话将自动停止。

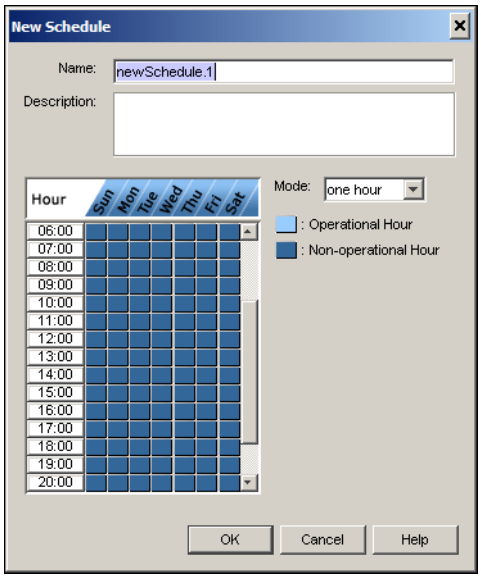
## 创建计划表

务等部分 Firebox® 操作。可为一周每天创建同一计划表，也可为一周每天创建不同的计划表。用户可在策略中应用所创建的上述计划表。有关如何在策略中使用计划表的信息，请参见 “策略配置” 章节。

1 在 Policy Manager 中，选择 **Setup（设置）> Actions（操作）> Schedules（计划表）**。
出现 Schedules（计划表）对话框。



2 点击 **Add （添加）**。
出现 New Schedules （新建计划表）对话框。




3 输入计划表名称及描述。计划表名称将显示在 **Schedule （计划表）**对话框中，输入的名称应便于记忆。

4 在 **Mode （模式）**下拉列表中，选择计划表的时间增量：1 小时、 30 分钟或 15 分钟。
New Schedule （新计划表）对话框左边的图表将显示用户在下拉列表中输入的内容。

5 对话框中的图表的 X 轴（水平）表示一周内各天， Y 轴（垂直）表示一天内的时间增量。点击图表中的方格可在运行时间（策略生效时）和非运行时间（策略未生效时）之间进行切换。

6 点击 **OK （确定）**关闭 **New Schedule （新建计划表）**对话框。点击 **OK （确定）**关闭 **Schedules （计划表）**对话框。

要编辑计划表，请在 **Schedule （计划表）**对话框中选择计划表名称，然后点击 **Edit （编辑）**。要根据已有计划表创建新的计划表，请选择计划表名称，然后点击 **Clone （复制）**。

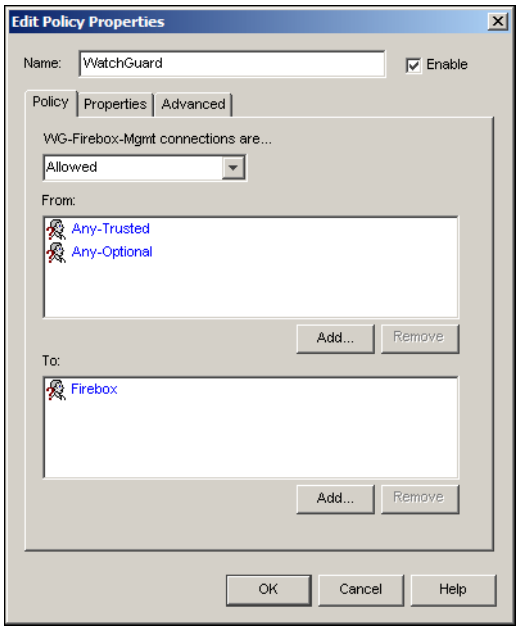
## 远程管理 Firebox

使用快速安装向导配置 Firebox® 时，将自动创建允许用户从受信或可选网络中的任一台计算机连接并管理 Firebox 的策略。如果要对 Firebox 进行远程（Firebox 外部的任何位置）管理，则必须将配置修改后允许进行远程管理连接。
控制到 Firebox 的管理连接的策略本身在 Policy Manager 中称为 WatchGuard® 策略，该策略控制通过以下四个 TCP 端口对 Firebox 的访问：4103, 4105, 4117, 4118。如果用户允许 WatchGuard 策略中的连接，则允许对上述四个端口的连接。
将策略修改为允许从网外计算机到 Firebox 的连接之前，建议考虑以下方面：

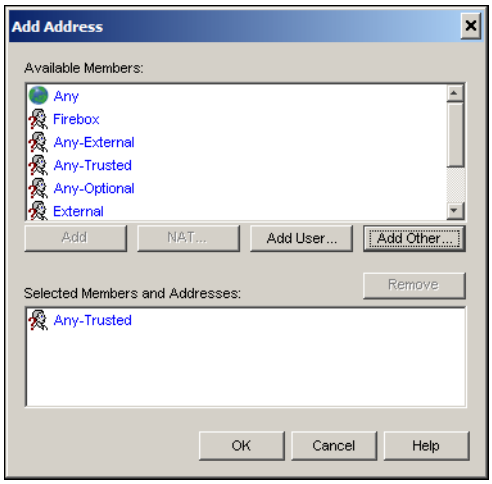
- 通过用户验证限制对 Firebox 的连接。

- 最好尽量限制外部网络对计算机的访问。例如，允许来自单台计算机的连接比允许来自别名“Any-External”的连接更加安全。

1 在 Policy Manager 中，双击 **WatchGuard** policy （**WatchGuard** 策略）。
也可右键点击 WatchGuard policy （WatchGuard 策略），然后选择 Edit （编辑），将显示 Edit Policy Properties （编辑策略属性）对话框。




2 在 **From** （从）列表中，点击 **Add** （添加）。




3 要输入连接 Firebox 的外部计算机的 IP 地址，请点击 **Add Other**（**添加其他**）。确认 **Host IP**（**主机 IP**）是所选类型，输入 IP 地址。
要添加用户名，请点击 **Add User** （**添加用户**）。选择用户类型及其使用的验证方法。在 **User/Group** （**用户 / 群组**）下拉列表中，选择 **User** （**用户**），输入要连接到 Firebox 的用户的名称。

4 点击 **OK** （**确定**）。

# 第 7 章　日志与通知

事件是 Firebox® 上发生的活动。例如，拒绝数据包通过 Firebox 即为一个事件。日志是在日志主机上对此类事件所作的记录。通知是当发生可能威胁网络安全的事件时 Firebox 向管理员发送的消息，可以是电子邮件或弹出窗口的形式，或通过 SMTP trap 发送。

例如， WatchGuard® 建议用户将默认数据包处理配置为当 Firebox 发现端口空间探测时发送通知。此时，日志主机向网络安全管理员发送关于被拒绝数据包的通知。网络安全管理员可检查日志文件，确定如何增强公司网络安全。可考虑以下措施：

- 封锁使用探测的端口
- 封锁发送数据包的 IP 地址
- 通知经其发送数据包的互联网服务提供商

日志与通知对于完善的网络安全策略具有重要意义，两者结合起来可监控网络安全、识别攻击和黑客以及应对安全威胁和挑战。

用户可在使用管理工作站的计算机上安装日志服务器，也可通过 WatchGuard System Manager 安装程序将日志服务器软件安装在另一台计算机上，并可选择只安装日志服务器组件。用户还可添加更多日志服务器用作备份。

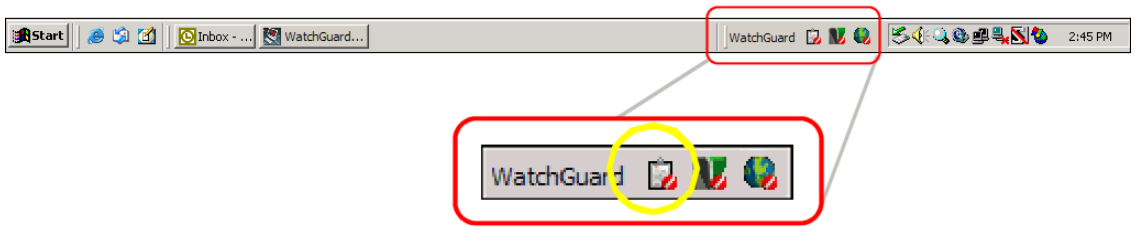
**注释**

如果要在装有防火墙而不是 Windows 防火墙的计算机上安装管理服务器、日志服务器或 WebBlocker 服务器，必须打开服务器通过防火墙连接所需的端口。 Windows 防火墙用户无需修改配置。详细信息请参见第 20 页的 “*在装有桌面防火墙的计算机上安装 WatchGuard 服务器*”。

# 设置日志服务器

日志服务器从 WSM 管理的每台 WatchGuard® Firebox® 上收集日志。

1 在已安装日志服务器软件的计算机上，选择 WatchGuard 工具栏中的 Log Server（日志服务器）图标。
如果没有显示 WatchGuard 工具栏，请右键点击系统托盘，选择 Toolbars（工具栏）> WatchGuard。




将显示 **WatchGuard Log Server Configuration**（**WatchGuard 日志服务器配置**）对话框。


2 输入 Firebox 和日志服务器安全连接所需的密钥。日志服务器密钥最小长度为 8 个字符。

3 确认密钥。

4 选择用于保存所有日志、报告和报告定义文件的目录，建议您使用默认位置。

5 点击 **OK**（**确定**）。

6 点击 **Start**（**开始**）> **Control Panel**（**控制面板**），进入电源选择页面。选择 **Hibernate**（**休眠**）选项卡，禁用休眠功能，这样当电脑休眠时日志服务器就不会关闭。

7 请务必将日志服务器和 Firebox 的系统时间设置为相同。有关设置系统时间的信息，请参见“*Firebox 基本管理*”章节。

## 修改日志服務器密鑰

要修改日志服务器密钥，请按以下步骤操作：

1 右键点击 WatchGuard 工具栏上的 Log Server（日志服务器）图标，选择 **Status/Configuration**（**状态 / 配置**）。

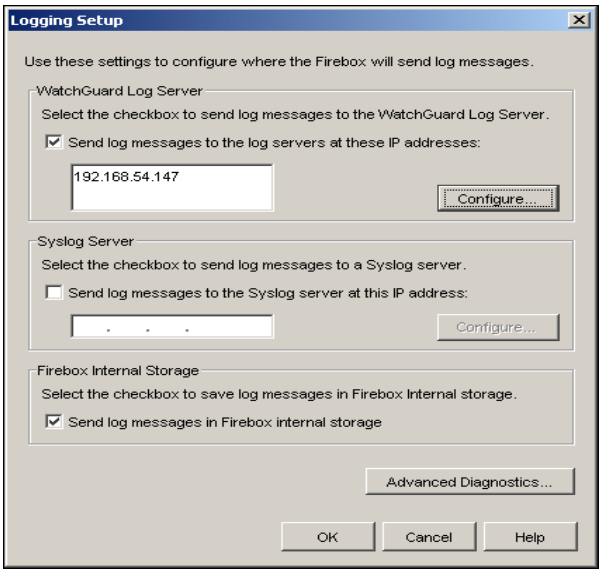
2 选择 **File**（**文件**）> **Set Log Encryption Key**（**设置日志密钥**）。

3 输入新的日志密钥两次。
4 在 Policy Manager（策略管理器）中，选择 **Logging（日志）**，输入新的日志密钥。
5 点击 **OK（确定）**。
6 对 Firebox 进行相同操作。

## 设置指定日志服务器的 Firebox

建议用户要使用 WatchGuard System Manager 则至少需设置一台日志服务器。用户可选择一台不同的主日志服务器以及一台或多台备份日志服务器。

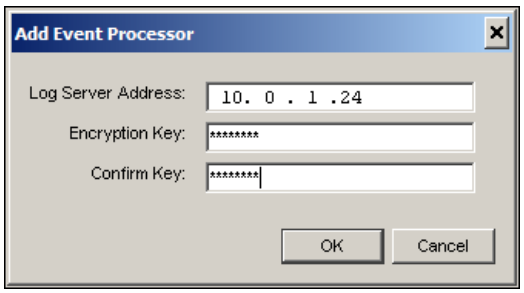
1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> Logging（日志）**。
出现 Logging Setup（日志设置）对话框。
2 选择要使用的一台或多台日志服务器。点击 **Send log messages to the Log Servers at these IP addresses（发送日志消息到这些 IP 地址的日志服务器）**复选框。




### 向 Firebox 添加日志服务器

1 在 Policy Manager（策略管理器）中，选择 **Setup（设置）> Logging（日志）**。
出现 Logging Setup（日志设置）对话框。

2 点击 **Configure**（**配置**），再点击 **Add**（**添加**）。
出现 Add Event Processor（添加事件处理器）对话框。




3 在 **Log Server Address**（**日志服务器地址**）框中，输入要使用的日志服务器的 IP 地址。

4 在 **Encryption Key**（**密钥**）和 **Confirm**（**确认**）框中，输入日志服务器密钥。密钥允许长度范围为 8-32 个字符，可使用除空格和斜线（/ 或 \）以外的所有字符。

5 点击 **OK**（**确定**）。点击 **OK**（**确定**）关闭 **Configure Log Servers**（**配置日志服务器**）对话框。点击 **OK**（**确定**）关闭 **Logging Setup**（**日志设置**）对话框。

6 将修改保存到 Firebox，开始执行日志功能。

用户可检验 Firebox 日志功能是否正常。在 WSM 中，选择 **Tools**（**工具**）**> Firebox System Manager**。在左边 **Log Server**（**日志服务器**）旁的 **Detail**（**详情**）部分，将显示日志主机的 IP 地址。

## 设置日志服务器优先级

如果 Firebox 无法连接到优先级最高的日志服务器，将连接到优先级列表中次一级优先级别的日志服务器。如果 Firebox 依次检查了列表中的所有日志服务器但无法连接，则将尝试再次连接列表中的第一台日志服务器。用户可为日志服务器创建优先级列表。

1 在 Policy Manager（策略管理器）中，选择 **Setup**（**设置**）**> Logging**（**日志**）。
出现 Logging Setup（日志设置）对话框。

2 点击 **Configure**（**配置**）。
将显示 Configure Log Servers（配置日志服务器）对话框。

3 从 **Configure Log Servers**（**配置日志服务器**）对话框的列表中选择一台日志服务器。使用 **Up**（**上**）、**Down**（**下**）按钮修改优先顺序。

## 激活 syslog 日志

Syslog 是为 UNIX 开发的日志接口，但也用于许多其他计算机系统。用户可将 Firebox 配置为向 syslog 服务器发送日志消息。Firebox 可同时向日志服务器和 syslog 服务器发送日志消息，或向其中一个发送日志消息。Syslog 日志消息不加密，建议您不要选择外网接口上的主机。

1 在 Policy Manager（策略管理器）中，选择 **Setup**（**设置**）**> Logging**（**日志**）。
出现 Logging Setup（日志设置）对话框。

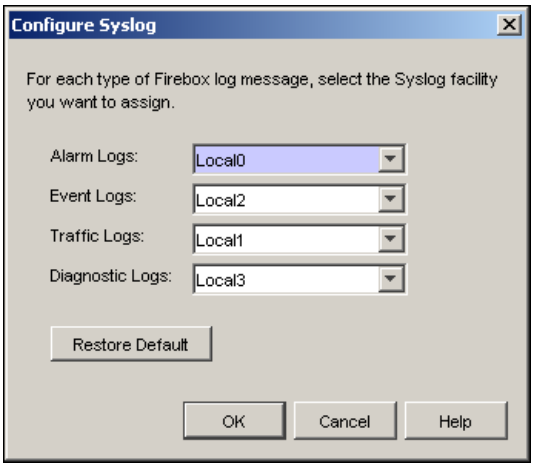
2 点击 **Send Log Messages to the Syslog server at this IP address**（**发送日志消息到此 IP 地址的 Syslog 服务器**）复选框。

3 在地址框中，输入 syslog 服务器的 IP 地址。

4 点击 **Configure （配置）**。
将显示 Configure Syslog Servers （配置 Syslog 服务器）对话框。

5 为各种类型的日志消息选择要分配的 syslog 工具。有关日志消息类型的信息，请参见第 90 页的“*日志消息类型*”。
Syslog 工具指 syslog 数据包中的某一字段及 syslog 发送到的文件。用户可将 Local0 用于优先级高的 syslog 消息，如告警；可使用 Local1- Local 7 为其他类型的日志消息指定优先级（少数日志消息拥有较高优先级）。有关日志工具的详情，请参阅 syslog 文件。

6 点击 **OK （确定）**。点击 **OK （确定）**关闭 **Logging Setup （日志设置）**对话框。



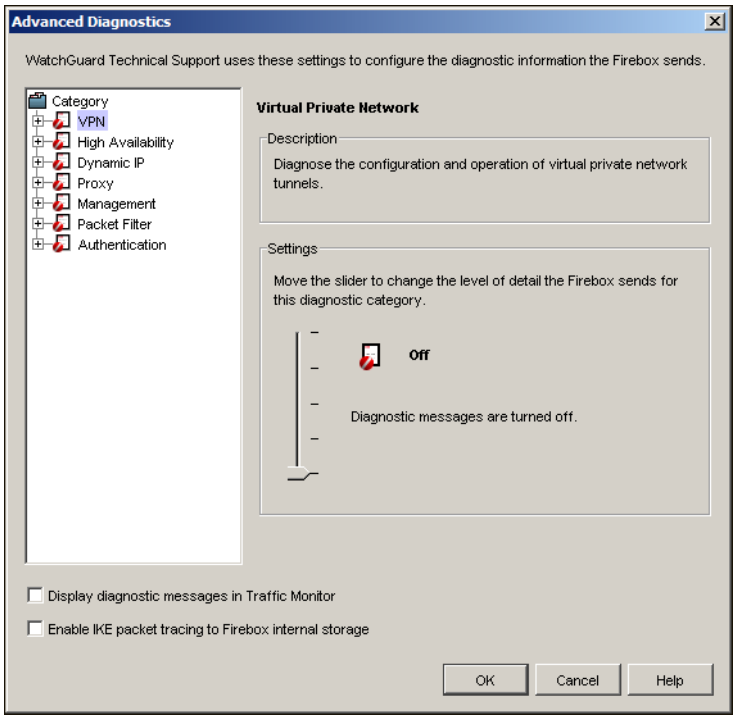

7 将修改保存到 Firebox。

## 启用高级诊断

用户可选择写至日志文件或 Traffic Monitor （流量监控器）的诊断日志级别，但不建议用户将日志级别设置为最高级，除非为排除故障在技术支持代表指示下作此设置，因为这可能造成日志文件迅速填满，还可能造成 Firebox 负载过重。

1 在 Policy Manager （策略管理器）中，选择 **Setup （设置）> Logging （日志）**。
出现 Logging Setup （日志设置）对话框。

2 点击 **Advanced Diagnostics（高级诊断）**。
出现 Advanced Diagnostics（高级诊断）对话框。




3 从类别列表中选择一种类别。
Description（描述）框中将显示类型描述。

4 使用 **Settings（设置）**下的滑块设置每类日志在其日志消息中包含的信息等级。若设置为最低等级，该类别的诊断消息将关闭。若设置为最高等级，用户可设置诊断日志消息的详情等级。

5 要在 Traffic Manager 中显示诊断消息，请选择 **Display diagnostic messages in Traffic Monitor（在流量监控器中显示诊断消息）**复选框，这有助于快速诊断问题。

6 要使Firebox收集IKE数据包的数据包追踪，请选择**Enable IKE packet tracing to Firebox internal storage（启用 IKE 数据包追踪至 Firebox 内部存储设备）**复选框。要查看 Firebox 收集的数据包追踪信息，请启动 Firebox System Manager，点击 **Status（状态）**选项卡。点击 **Support（支持）**使 Firebox System Manager 从 Firebox 获取数据包追踪信息。

7 完成后请关闭诊断日志。

## 设置全局日志和通知优先权

要查看日志服务器状态和配置，请点击 WatchGuard® 工具栏上的 Log Server（日志服务器）图标，选择 **Status/Configuration（状态 / 配置）**，将显示状态和配置信息。窗口中共有三个控制区：

*日志文件选项卡*
设置滚动日志文件的选项。

*报告选项卡*
计划日志条目定期报告。

*通知选项卡*

配置电子邮件通知。

以上三项控制共同设置事件和通知的一般配置。

## 日志文件大小和切换频率

用户可按文件大小或时间来切换日志。当进行切换时，日志服务器将关闭当前日志文件，打开另一个新日志文件。关闭的日志文件可用于报告，请将其复制或移动到另一位置，并保存归档。

要设置适合贵公司的最佳切换大小，须考虑以下因素：

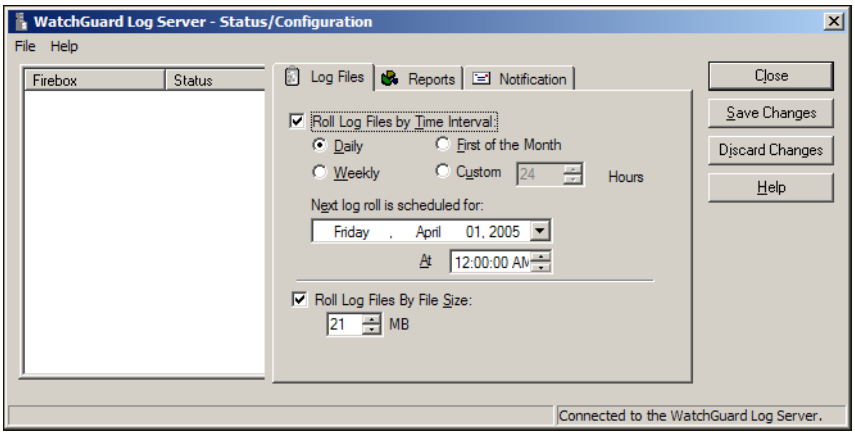
- 可用的存储空间
- 希望可用的天数
- 保留、打开和查看的最佳大小
- 已记录事件类型的数量
  例如，一家小公司两周的条目数为 10,000 条，而一家实施多项策略的大公司一天内就能轻易达到 100,000 条。
- Firebox® 上的流量
- 要创建报表的数量
  要创建周报，则需要 8 天或 8 天以上的数据，如果日志文件在同一位置，则此数据可从多个日志文件中获得。

建议监控新日志文件并根据需要调整配置。

## 设置日志文件切换时间

用户可在日志服务器配置界面的 **Log Files**（**日志文件**）选项卡中控制何时进行日志文件切换，也可手动开始当前日志文件的切换。请选择 **Status/Configuration**（**状态 / 配置**）窗口中的 **File**（**文件**）**> Roll current log file**（**切换当前日志文件**）。

1 要设置何时切换日志文件，请点击 **Log Files**（**日志文件**）选项卡。




2 要按一定时间间隔切换日志文件，请选择 **Roll Log Files By Time Interval**（**按时间间隔切换日志文件**）复选框，设置时间间隔。在 **Next Log Roll is Scheduled For**（**下次日志切换时间**）下拉列表中选择日志文件切换日期。

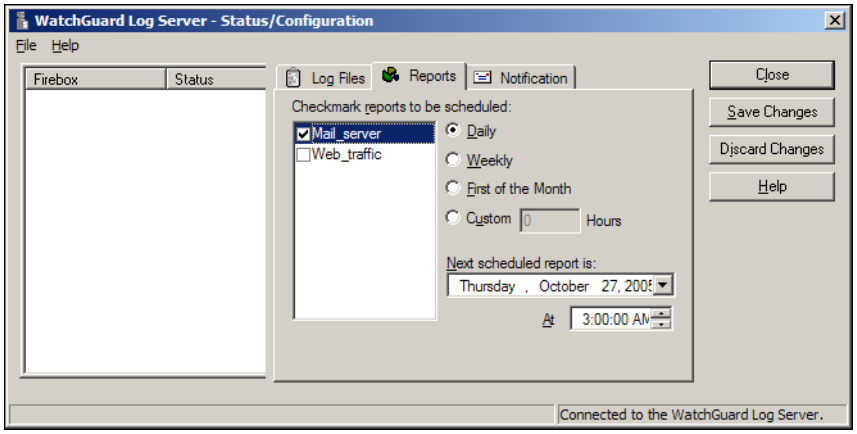
3 要根据日志文件大小切换日志文件，请选择 **Roll Log Files By File Size（按文件大小切换日志文件）**复选框，输入文件切换前的日志文件最大长度，或使用数值调节钮控件来设置数字。

4 点击 **Save Changes（保存修改）**或 **Close（关闭）**。
将关闭 Log Server（日志服务器）界面并保存条目。新配置将立即启用，日志服务器将自动重新启动。

## 安排自动报告

如果已使用 Historical Reports（历史报告）创建了网络活动报告，则可安排日志服务器组件自动生成报告。首先必须在 Historical Reports（历史报告）中创建一份报告，否则报告不会显示在日志服务器界面上。

1 点击 **Reports（报告）**选项卡。




2 使用单选按钮设置报告的时间间隔：每日、第周、每月第一天或自定义时间。

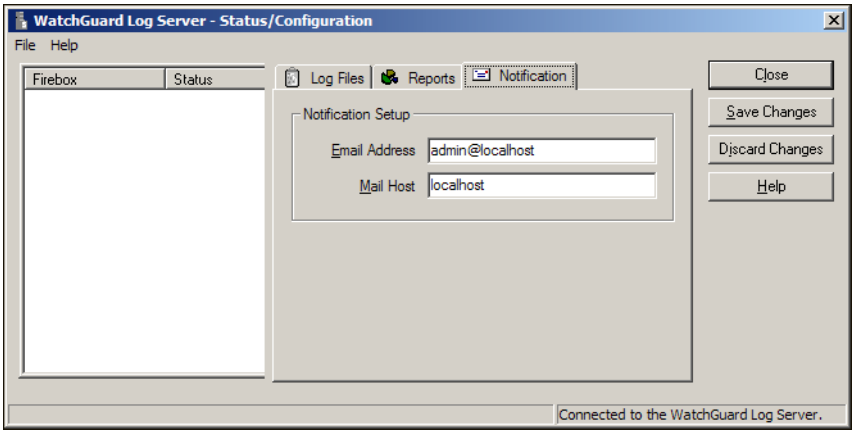
3 在 **Next Scheduled Report（下次计划报告）**下拉列表中选择下一次计划报告的日期和时间。

4 点击 **Save Changes（保存修改）**或 **Close（关闭）**。
将关闭 Log Server（日志服务器）界面并保存条目。新配置将立即启用，日志服务器将自动重新启动。

### 控制通知

用户可将 Firebox 配置为在发生特定事件时发送电子邮件消息。使用 **Notification （通知）**选项卡配置目的邮件地址。

1 点击 **Notification （通知）**选项卡。




2 输入通知邮件消息的邮件地址和邮件主机。

通知邮件消息格式为 firebox_name@[firebox_ip_address]（firebox_ 名称 @[firebox_ip_ 地址 ]，请确认 SMTP 服务器可处理此种格式。

考虑是否需要修改默认值。如果日志主机不能明确相应的 FQDN，而且接收 MX 服务器进行了反向查找（reverse lookup），则电子邮件可能被丢弃（discarded）。

3 点击 **Save Changes （保存修改）**或 **Close （关闭）**。

将关闭 Log Server（日志服务器）界面并保存条目。新配置将立即启用，日志服务器将自动重新启动。

### 启动及停止日志服务器

用户可手动停止或启动日志服务器：

- 要启动日志服务器，右键点击工具栏上的 Log Server（日志服务器）图标，选择 **Start Service （启动服务）**。
- 要停止日志服务器，右键点击工具栏上的 Log Server（日志服务器）图标，选择 **Stop Service （停止服务）**。

## 关于日志消息

WatchGuard® System Manager 具有强大而灵活的日志消息工具。完善的网络安全策略的重要功能即是将来自安全系统的消息记入日志，经常检查这些记录并妥善归档保存。用户可使用日志监控网络安全和活动、识别任何安全网络并进行相应处理。

WatchGuard® Firebox X Core 和 Firebox X Peak 可向称为 “日志服务器”的共享日志管理系统发送日志消息，也可向 syslog 服务器发送日志消息或将日志保存在本地 Firebox 上，用户可选择将日志发送到上述任一位置或同时发送到上述两个位置。

用户可使用 Firebox System Manager 在 **Traffic Monitor （流量监控器）**选项卡中记录日志消息。详情请参阅 “*监控 Firebox 状态*”章节。用户还可用 Log Viewer 检查日志消息。日志消息以扩展名为 .wgl.xml 的 XML 文件形式保存在日志服务器的 WatchGuard 目录下。有关日志消息格式的详情，请参阅 “*参考指南*”中的 “*日志消息*”章节。

# 日志消息类型

Firebox® 可发送四种类型的日志消息。消息类型将显示在消息的正文中。日志消息的四种类型如下：

- 流量
- 告警
- 事件
- 诊断

### 流量日志消息

Firebox 向通过 Firebox 的流量应用数据包过滤和代理服务器规则时发送流量日志消息。

### 告警日志消息

当发生促使 Firebox 执行命令的事件时发送告警日志消息。当满足告警条件时， Firebox 向流量监控器和日志服务器发送告警日志消息，然后进行指定操作。

用户可设置部分告警日志消息。例如，可使用 Policy Manager （策略管理器）配置当指定值等于或大于临界值时即产生告警。其他告警日志消息由设备软件进行设置，用户不得修改其值。例如，当 Firebox 某个接口上的网络连接失败或出现拒绝服务攻击时， Firebox 发送告警日志消息。有关告警日志消息的详情，请参阅 “*参考指南*”。

告警日志消息分为八类：系统、 IPS、 AV、策略、代理服务器、计数器、拒绝服务及流量。

Firebox 在 15 分钟内针对相同条件发送的告警不超过 10 个。

### 事件日志消息

Firebox 会针对用户操作发送事件日志消息。可能引起 Firebox 发送事件日志消息的操作包括：

- 启动和关闭 Firebox
- Firebox 和 VPN 验证
- 启动和关闭进程
- Firebox 硬件组件的问题
- Firebox 管理员执行的任何任务

### 诊断日志消息

诊断日志消息包括可帮助用户排除故障解决问题的信息。共有 27 种不同的产品组件可发送诊断日志消息。用户可选择是否根据第 85 页 “*启用高级诊断*”中的说明将诊断日志消息显示在流量监控器中。

# 日志文件名及位置

Firebox® 可向主日志服务器或备份日志服务器发送日志消息。日志文件的默认位置为 My Documents （我的文档）> My WatchGuard （我的 WatchGuard）> Shared WatchGuard （共享 WatchGuard）> logs （日志）。

日志文件名称显示：

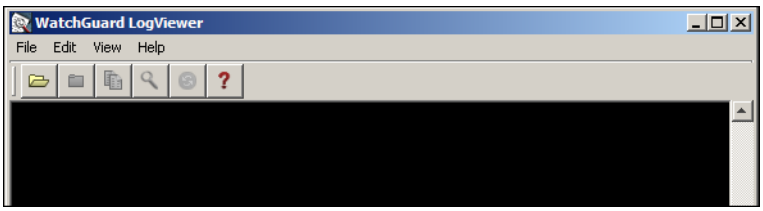
- 如果 Firebox 已命名，日志文件名称的格式为 FireboxName-date . wgl . xml（Firebox 名称 - 日期 .wgl . xml ）。
- 如果 Firebox 未命名，日志文件名称的格式为 FireboxIP–date . wgl . xml（FireboxIP- 日期 . wgl . xml ）。

## 开始使用 LogViewer

LogViewer是用于查看日志文件数据的WatchGuard® System Manager工具，可按页显示日志数据页，或按关键字或指定日志字段进行搜索和显示。

1 在 WatchGuard System Manager，选择 **Tools（工具）> Logs（日志）> Log Viewer（日志查看器）**。

或
点击 WatchGuard System Manager 工具栏上的 LogViewer 图标，该图标位于屏幕左边。



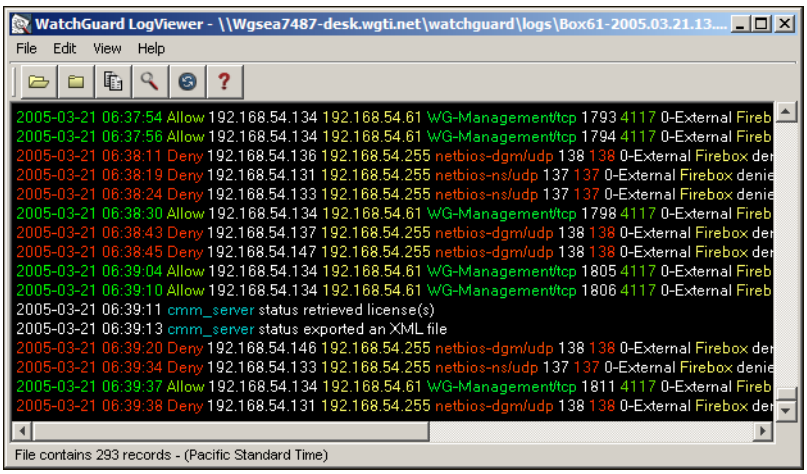

2 在 Log Viewer 中，选择 **File（文件）> Open（打开）**。

或
点击 Log Viewer 工具栏上的 Open File（打开文件）图标，该图标位于屏幕左边。

日志的默认位置为 My Documents（我的文档）> My WatchGuard（我的 WatchGuard）> Shared WatchGuard（共享 WatchGuard）> logs（日志）。

3 浏览并查找日志文件，点击 **Open（打开）**。

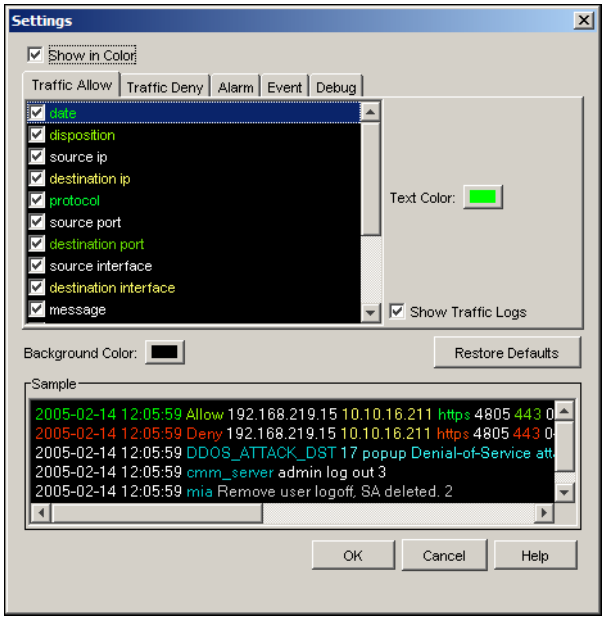
LogViewer 将显示所选的日志文件。示例如下。



# LogViewer 设置

用户可调整 Log Viewer 窗口的内容和格式。

1 在 Log Viewer 中选择 **View （视图）>Settings （设置）**。
出现 Settings （设置）对话框。




**Settings （设置）**对话框有五个选项卡，每个选项卡的字段相同。用户可利用这些选项卡设置日志文件中显示的四类消息的属性：告警、流量、事件及诊断。

*以不同颜色显示日志*
用户可设置根据日志消息类型以不同颜色显示消息。如果禁用颜色，日志消息将显示为黑色背景白色文本。

*显示列*
用户可为各种类型的日志消息选择要在 LogViewer 窗口中显示的列。选择各字段旁的复选框即可。

*文本颜色*
点击 **Text Color （文本颜色）**设置各类日志消息的颜色。

*背景颜色*
用户可设置背景色。如果背景和文本设置为相同颜色，则无法看见文本。

*恢复默认设置*
点击可将日志消息的格式设置为默认颜色。

*示例*
显示修改格式的日志消息示例。

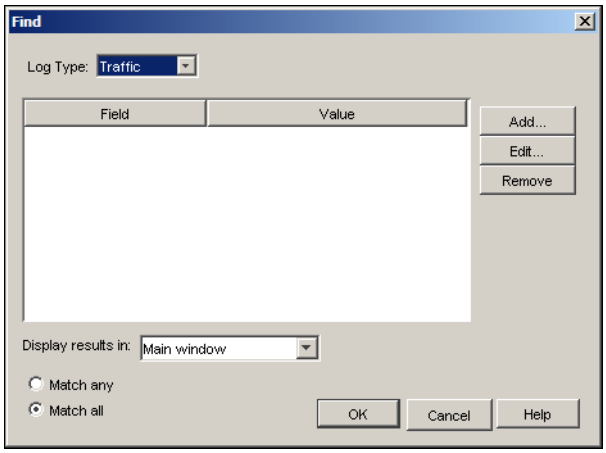
*显示日志*
每个选项卡上都有此复选框。如果选择某选项卡上的该复选框，该类日志消息将显示在 LogViewer 窗口中。若不要在窗口中显示该类日志消息，请取消该日志类型对应选项卡上的复选框的选择。

# 使用 LogViewer

## 创建搜索规则

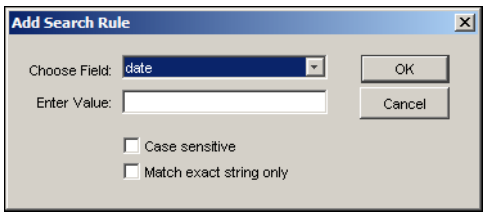
用户可创建搜索 LogViewer 中显示数据的规则。

1 选择 **Edit（编辑）> Find（查找）**（或点击放大镜图标）。
出现 Find（查找）对话框。




2 使用 **Log Type（日志类型）**下拉列表选择要应用搜索规则的日志消息类型，可选择：流量、事件、告警、调试或全部。

3 点击 **Field（字段）**列标题，选择 **Add（添加）**。
出现 Add Search Rule（添加搜索规则）对话框。




4 在 **Choose Field（选择字段）**下拉列表中选择要搜索的字段。

5 在 **Enter Value（输入值）**文本框中，输入要搜索的文本或值。

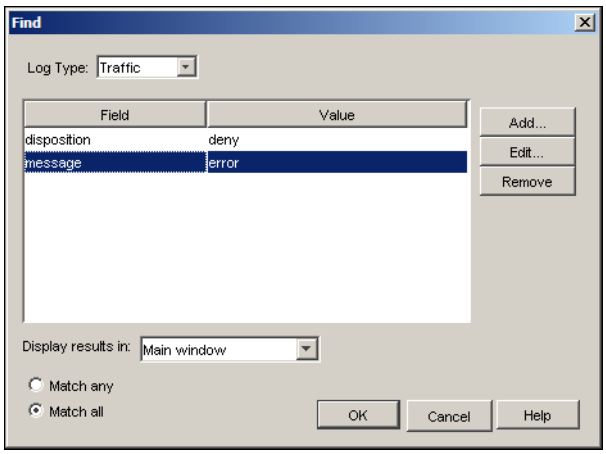
6 如果在 **Enter Value（输入值）**文本框中输入的文本要区分大小写，请选择 **Match Case（区分大小写）**复选框。如果只需查找与输入值精确匹配的条目，请选择 **Match exact string only（只查找准确匹配串）**复选框。

7 点击 **OK（确定）**。

## 在 LogViewer 中进行搜索

创建搜索规则后，可用于搜索 Log Viewer 中显示的数据。

1 使用 **Log Type （日志类型）**下拉列表选择要在窗口中显示的日志消息类型。




2 使用 **Display Results （显示结果）**下拉列表选择搜索结果的显示方式，有以下几种选择：
   - *在主窗口中突出显示* — Log Viewer 窗口显示设置的相同日志消息，但颜色与符合标准的日志消息不同。使用 F3 键在指定条目中移动。
   - *主窗口* — Log Viewer 主窗口只显示符合搜索标准的日志消息。
   - *新窗口* — 在新窗口中显示符合搜索标准的日志消息。

3 从以下两项中进行选择：
   - *匹配任何* — 显示符合任一搜索标准的日志消息。
   - *匹配全部* — 只显示符合所有搜索标准的日志消息。

4 点击 **OK （确定）**开始搜索。

## 在 LogViewer 查看当前日志文件

用户可在 LogViewer 中打开当前日志文件，检查写入日志文件的日志。 Log Viewer 每隔 15 秒会自动更新，显示新日志消息。如果打开了当前日志文件和 LogViewer 搜索窗口，也会每隔 15 秒更新一次。

## 复制 LogViewer 数据

用户可将日志文件数据从 Log Viewer 复制到另一工具中。使用 **copy （复制）**将指定日志消息移动到另一工具中。

1 选择要复制的日志消息。
   使用 Shift 键选择一组条目。使用 Ctrl 键选择多条条目。

2 选择 **Edit （编辑）> Copy （复制）**。

3 将数据粘贴到任何文本编辑器中。

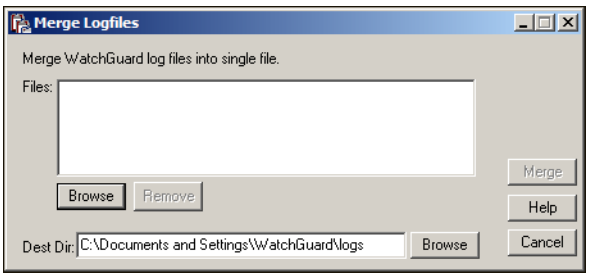
## 合并日志文件

用户可将两个或多个日志文件合并为一个文件，然后可将此文件用于历史报告、 LogViewer 或其他工具中，进行长时间间隔的日志数据检查。要合并日志文件：

- 日志文件必须来自同一台 Firebox。
- 文件中的日志消息必须按日期和时间排序。
- 日志文件必须是用相同的设备软件所创建。WFS 设备软件创建的日志文件不同与 Fireware® 设备软件创建的日志文件合并，即使文件来自同一台 Firebox。

右键点击 Windows 工具栏上的 Log Server （ 日志服务器 ）图标，选择 **Merge Log Files （ 合并日志文件 )**。或在 Log Server Status/Configuration （ 日志服务器状态 / 配置 ）界面上：

1 点击 **File （ 文件 ）> Merge log files （ 合并日志文件 )**。
出现 Merge Logfiles （ 合并日志文件 ）对话框。




2 点击 **Browse （ 浏览 )** 查找要合并的文件。

3 点击 **Merge （ 合并 )**。
日志文件将合并并作为一个新文件保存到指定目录下。

## 将 .wgl 日志文件更新为 .xml 格式

当用户从旧版本的 WatchGuard System Manager 升级为 WSM 8.3 时，可将日志文件从 .wgl 格式转换为 .xml 格式。这有助于管理使用不同 WSM 版本的混合网络。转换后，用户可将 WSM 8.3 LogViewer 或报告工具用于 WatchGuard Management System 7.3 或更早版本所创建的日志文件。

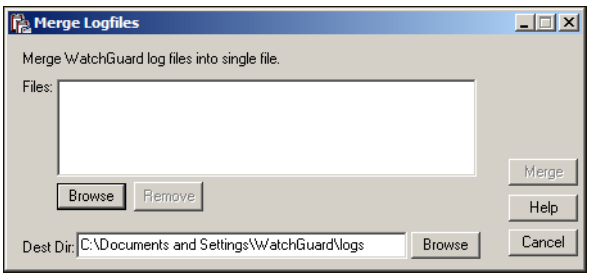
为帮助用户理解新日志结构或将 .xml 格式的日志纳入第三方应用程序中，请参阅以下 Advanced FAQ （ 高级常见问题 )，它介绍了新 WatchGuard 日志文件的 XML 方案和文件类型定义 （ DTD )：
https://www.watchguard.com/support/AdvancedFaqs/wsm8_xmlschema.asp

将日志文件从 .wgl 转换为 .xml 时：

- XML 文件通常小于 .wgl 文件。
- 如果用 XML 编辑器打开新 XML 文件，可能会出现重复的条目。这是 Historical Reports （ 历史报告 ）在 WSM 7.3 及更早版本中创建报告方式的功能，不会在 LogViewer 或 WSM 8.3 的 Historical Reports （ 历史报告 ）中造成问题。

要将日志文件从 .wgl 转换为 .xml：

1 右键点击 Windows 桌面托盘上的 Log Server（日志服务器）图标，选择 **Merge Log Files（合并日志文件）**。
出现 Merge Logfiles （合并日志文件）对话框。此对话框控制日志文件的合并和更新。




2 点击 **Browse（浏览）**查找要转换为 XML 格式的 .wgl 日志文件的位置。如果一次选择多个日志文件，该工具将所选的全部文件合并为一个文件，新文件为 .xml 格式。

3 点击 **Merge （合并）**。
该工具将日志文件合并，然后保存到指定文件夹中。

# 第 8 章　网络设置与配置

将 Firebox® 安装到网络中并完成快速安装向导后，即有了基本配置文件。然后可利用 Policy Manager（策略管理器）创建新的配置文件或修改快速安装向导创建的文件。

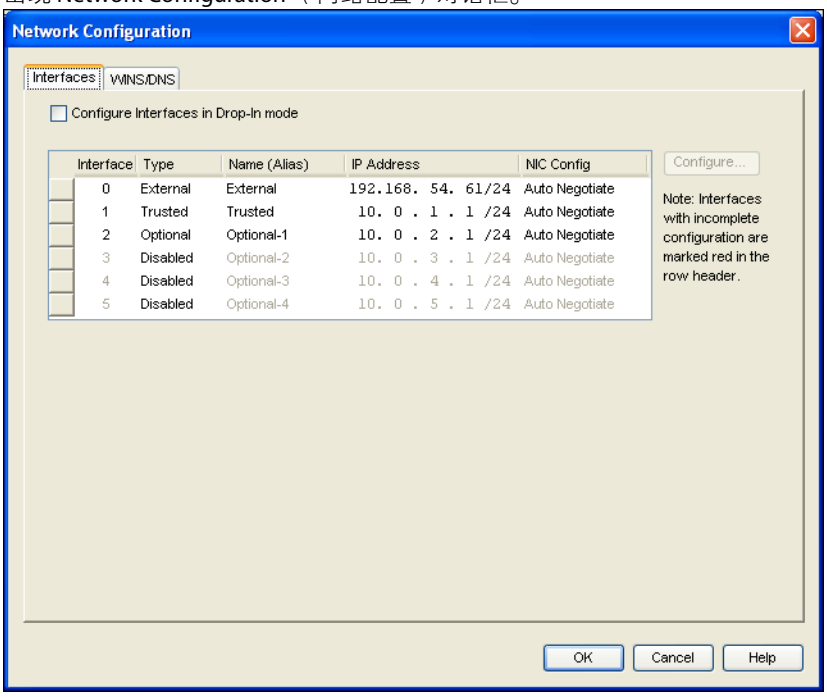
如果您对网络安全尚不熟悉，建议您完全按照本章的所有程序进行操作，以确保对网络中的所有组件进行配置。本章将介绍如何使用 Policy Manager（策略管理器）来：

- 配置 Firebox 接口
- 配置多广域网支持
- 添加第二网
- 添加 DNS 和 WINS 服务器信息
- 配置动态 DNS
- 配置网络和主机路由
- 设置 Firebox 接口速度和双工模式
- 配置相关主机

用户还可使用 Policy Manager（策略管理器）将四个 Firebox 接口配置为外网接口或广域网接口。用户可通过多个广域网接口控制流量，实现外发流量负载共享。

# 修改 Firebox 接口 IP 地址

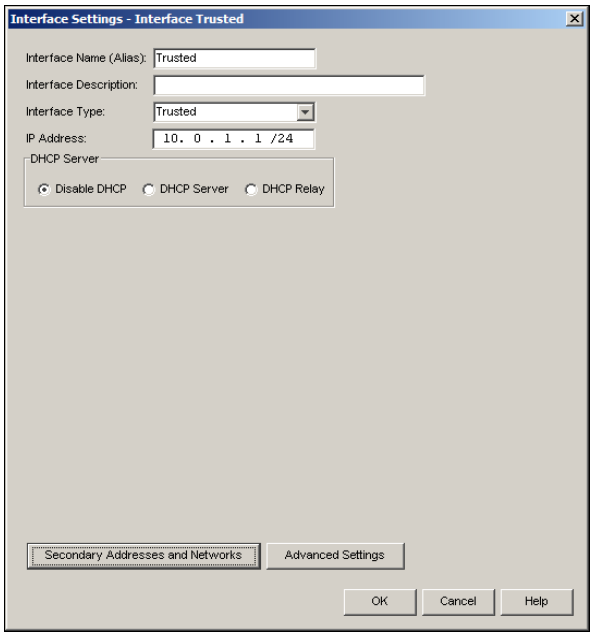
1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> Configuration（配置）**。
出现 Network Configuration（网络配置）对话框。




2 选择要配置的接口，点击 **Configure（配置）**。
出现 Interface Settings（接口设置）对话框。

3 （可选）在 **Interface Description（接口描述）**字段中输入接口描述。

4 可从 **Interface Type（接口类型）**下拉列表中修改接口类型。



5 您可修改接口 IP 地址，在斜线标记框中输入 IP 地址。
输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

6 如果要配置受信或可选接口，请选择 **Disable DHCP, DHCP Server（禁用 DHCP、 DHCP 服务器）**或 **DHCP Relay（DHCP 中继）**。
DHCP 服务器选项见“将 Firebox 配置为 DHCP 服务器”，DHCP 中继选项见第 99 页的“配置 DHCP 中继”。如果要配置外网接口，请参见第 100 页的 “*配置外网接口*”。

7 点击 **OK（确定）**。

## 将 Firebox 配置为 DHCP 服务器

动态主机配置协议（DHCP）是能帮助用户轻松控制大型网络的互联网协议。配置为 DHCP 服务器的计算机会自动为网络中的计算机分配 IP 地址。用户设置地址范围，并可将 Firebox® 配置为 Firebox 背后网络的 DHCP 服务器。

如果已配置了 DHCP 服务器，建议您继续将该服务器作为 DHCP 服务器使用。

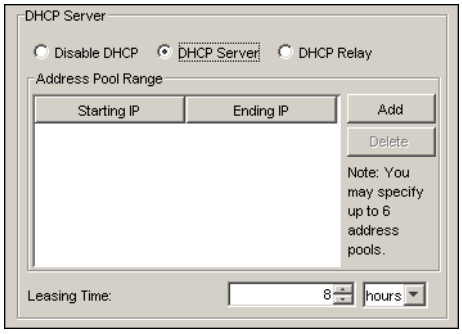
1 选择 **Network（网络）> Configuration（配置）**。
出现 Network Configuration（网络配置）对话框。

2 选择受信或可选接口。

3 点击 **Configure（继续）**，选择 **DHCP Server（DHCP 服务器）**。

4 要添加 IP 地址范围，请点击 **Add（添加）**，输入第一个和最后一个 IP 地址。
最多可配置六个地址范围。

5 可使用箭头按钮修改 **Default Lease Time（默认租期时间）**。
这是 DHCP 客户端可使用 DHCP 服务器分配的 IP 地址的时间间隔。当该时间即将结束时，客户端向 DHCP 发送数据，以重新获得租用期。




## 配置 DHCP 中继

为 Firebox 受信或可选网络中的计算机分配 IP 地址的一种方法即是使用另一网络中的 DHCP 服务器。 Firebox 可向另一位置的 DHCP 服务器而非 DHCP 客户端发送 DHCP 请求。 Firebox 收到回复后，即发送到 Firebox 受信或可选网络中的计算机。

1 选择 **Network（网络）> Configuration（配置）**。
出现 Network Configuration（网络配置）对话框。

2 选择受信或可选接口。

3 点击 **Configure（继续）**，选择 **DHCP Relay（DHCP 中继）**。

4 在相关字段中输入 DHCP 服务器的 IP 地址，必要时务必添加到 DHCP 服务器的路由。

5 点击 **OK（确定）**。要完成修改，必须重新启动 Firebox。


## 配置外网接口

Firebox 可通过动态主机配置协议（DHCP）或 PPPoE（以太网点对点协议）获得外网接口的动态 IP 地址。通过 DHCP， Firebox 使用互联网服务提供商（ISP）控制的 DHCP 服务器获得 IP 地址、网关和子网掩码。通过 PPPoE， Firebox 将创建到用户 ISP 的 PPPoE 服务器的 PPPoE 协议连接。Fireware® 支持无编号和静态 PPPoE。

**注释**

如果将多个接口配置为外网接口，只有最低位外网接口可作为 IKE 网关或 IPSec 隧道端点。如果该接口关闭，则 Firebox 连接的所有 IPSec 隧道都将无法工作。

### 使用静态 IP 地址

1 在 **Interface Settings（接口设置）**对话框中，选择 **Static（静态）**。

2 输入默认网关的 IP 地址

3 点击 **OK（确定）**。

### 使用 PPPoE

一些互联网服务提供商通过以太网点对点协议（PPPoE）分配 IP 地址。 PPPoE 扩展了标准拨号连接，加入了以太网和 PPP 的部分功能。该系统允许互联网服务提供商通过 DSL 调制解调器和线缆调制解调器产品使用计费、验证和拨号基础设施的安全系统。
如果您的互联网服务提供商使用 PPPoE，您必须将 PPPoE 信息输入 Firebox， Firebox 才能通过外网接口发送数据流。

1 在 **Interface Settings（接口设置）**对话框中，选择 **PPPoE**。

2 选择下列之一的选项：
- 自动获得 IP 地址
- 使用 IP 地址（互联网服务提供商分配的地址）

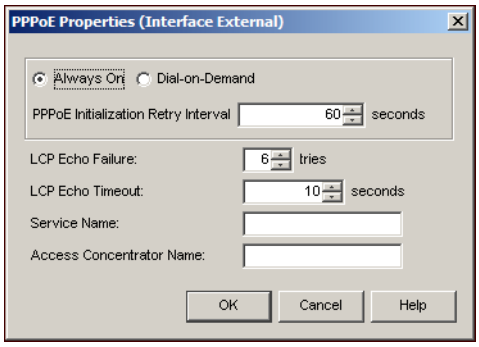
3 如果选择 **Use IP Address（使用 IP 地址）**，请在右边的文本框中输入 IP 地址。

4 输入 **User Name（用户名）和 Password（密码）**。密码必须输入两次。
互联网服务提供商经常使用邮件地址格式作用户名，如 myname@ispdomain.net。


5 点击 **Property（属性）**配置 PPPoE 参数。
出现 PPPoE 参数对话框。互联网服务提供商可告知您是否需要修改超时或 LCP 值。

6 使用单选按钮选择 Firebox 何时连接 PPPoE 服务器。

- **始终保持连接** — Firebox 一直保持 PPPoE 连接。网络数据流无需经过外网接口。
- **按需拨号** — Firebox 只在收到向外网接口上的 IP 地址发送数据流的请求时才连接 PPPoE 服务器。如果互联网服务提供商定期进行连接重置，请选择 Dial-on-Demand（按需拨号）。如果不选择 Dial-on-Demand（按需拨号），则每次连接重置后需手动重新启动 Firebox。




7 在 **PPPoE Initialization Retry Interval（PPPoE 初始化重试间隔）**字段中，使用箭头设置 PPPoE 在超时前进行初始化重试的秒数。

8 在 **LCP echo failure（LCP 回应失败）**字段中，使用箭头设置在认为 PPPoE 连接停止并关闭前允许 LCP 回应请求失败次数。

9 在 **LCP echo timeout（LCP 回应超时）**字段中，使用箭头设置每次回应超时必须收到响应的时间长度（单位为秒）。

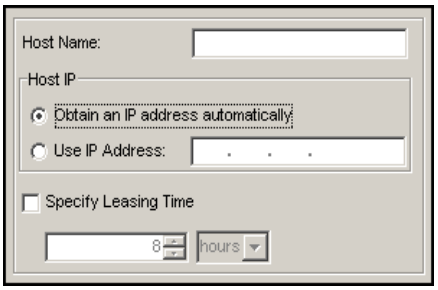
10 （可选）在 **Service Name（服务名称）**字段中，输入 PPPoE 服务名称，既可以是 ISP 名称，也可以是 PPPoE 服务器上配置的一类服务。通常不使用此选项，仅当存在多个访问集中器或用户知晓必须使用指定服务名称时才使用此字段。

11 （可选）在 **Access Concentrator Name（访问集中器名称）**字段中，输入 PPPoE 访问集中器名称，即 PPPoE 服务器。通常不使用此选项，仅当用户知晓存在多个访问集中器时才使用此项。

### 使用 DHCP

1 在 **Interface Settings（接口设置）**对话框中，选择 **DHCP**。

2 如果 DHCP 服务器让用户在 DHCP 交换中使用可选标识符，请在 **Host Name（主机名称）**文本框中输入该标识符。




3 如果希望 DHCP 为 Firebox 分配 IP 地址，请在 **Host IP（主机 IP）**下，选择 **Obtain an IP address automatically（自动获取 IP 地址）**复选框。如果希望手动分配 IP 地址并只使用 DHCP 将该地址

分配给 Firebox，请选择 **Use IP address （使用 IP 地址）**复选框，并在旁边的字段中输入该 IP 地址。

4 DHCP 服务器分配的 IP 地址租期为一天，即地址有效期为一天。如果要修改租期时间，请选择 **Specify Leasing Time （指定租期时间）**复选框，选择复选框下字段中的值。

# 关于多广域网支持

用户通过 Fireware® 设备软件可选择配置多个外网接口（最多四个），每个位于不同子网。这样，用户可将 Firebox® 连接到多个互联网服务提供商（ISP）。第二个外网接口配置完成后，多广域网支持自动启用，轮流平均多广域网为默认设置。控制外发数据包使用的接口有三种方式。

请注意：

- 如果有策略配置了单独的外网接口别名，必须将配置修改为使用 “Any-External” 别名。
- 如果使用多广域网功能，请将贵公司的全称域名映射到最低位的外网接口 IP 地址。如果向管理服务器配置添加多广域网 Firebox，必须添加使用最低位外网接口进行标识的 Firebox。
- 多广域网配置中不得使用一对一网络地址转换。如果 Firebox 后存在公共 SMTP 服务器，必须设置允许访问公共 SMTP 邮件服务器的静态网络地址转换规则。然后才能设置多个 MX 记录，每个 Firebox 外网接口各一个。
- 如果配置了多广域网，则不能使用基于策略的动态网络地址转换 **Set Source IP （设置源 IP）**选项。只有在 Firebox 使用单个外网接口时才能使用 **Set Source IP （设置源 IP）**选项。
- 多广域网支持不应用于分支机构或移动用户 VPN 数据流。分支机构和移动用户 VPN 数据流总是使用为 Firebox 配置的首个外网接口。应用 PPTP 的 RUVPN 在多广域网配置下可正常工作。
- 透明模式不支持多广域网功能。

## 关于轮流平均多广域网

如果选择 “轮流平均”，可按如下方式共享外网接口上的外发数据流负载：

- IP 地址为 x.x.x.x 的第一台主机向互联网发送 HTTP 请求。该会话中的数据包通过最低位外网接口发送。
- IP 地址为 y.y.y.y 的第二台主机向互联网发送 HTTP 请求。该会话中的数据包通过次高位外网接口发送。
- IP 地址为 z.z.z.z 的第三台主机向互联网发送 HTTP 请求。该会话中的数据包通过最低位外网接口（如果只配置了两个外网接口）或第三高位的外网接口发送。
- 由于每台主机均发起连接， Firebox 使用上文所述方式在外网接口中进行循环。

**注释**

如果使用轮流平均多广域网，可通过 DNS 提供商设置轮流平均 DNS，在多个外网接口中实现负载平衡。

## 关于广域网容错

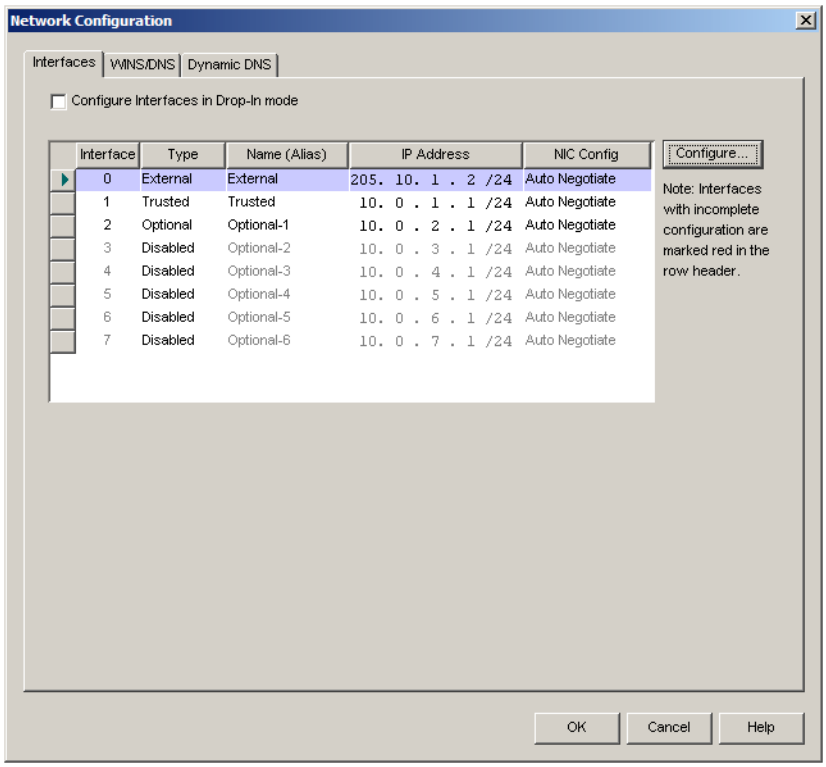
此选也只用于外发流量。如果选择此选项，列表中配置的最低位外网接口将成为主外网接口，所有其他外网接口将成为备用外网接口。 Firebox 将所有外发流量发送到主外网接口。如果主外网接口未启用，则 Firebox 将流量发送到第一个备用外网接口。 Firebox 通过两个程序监控主外网接口的状态。首先检查接口的实际连接状态，并 ping 每 20 秒为每个接口配置的外网主机的 IP 地址或域名。如果对该主机连 ping 三次均失败， Firebox 将转移至配置的下一个外网接口。
如果 Firebox 检测到主外网接口再次启用，将自动开始向主外网接口发送新连接。

## 关于具有路由表的多广域网

当用户为多广域网配置选择路由表选项时， Firebox 使用其内部路由表中设置的路由通过正确的外网接口发送数据包。用户可在 Policy Manager （策略管理器）中设置网络或主机路由， Firebox 会检查这些路由，确定数据包是否会发送到指定接口。如果 Firebox 没有找到指定路由， Firebox 将使用其路由表中的第一个默认路由。如果 Firebox 配置为使用动态路由，将根据其路由表中记录的动态信息发送数据流。要查看 Firebox 上的路由表，请连接 Firebox System Manager，选择 **Status**（**状态**）选项卡。

## 配置多广域网支持

1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> Configuration（配置）**。
出现 Network Configuration（网络配置）对话框。

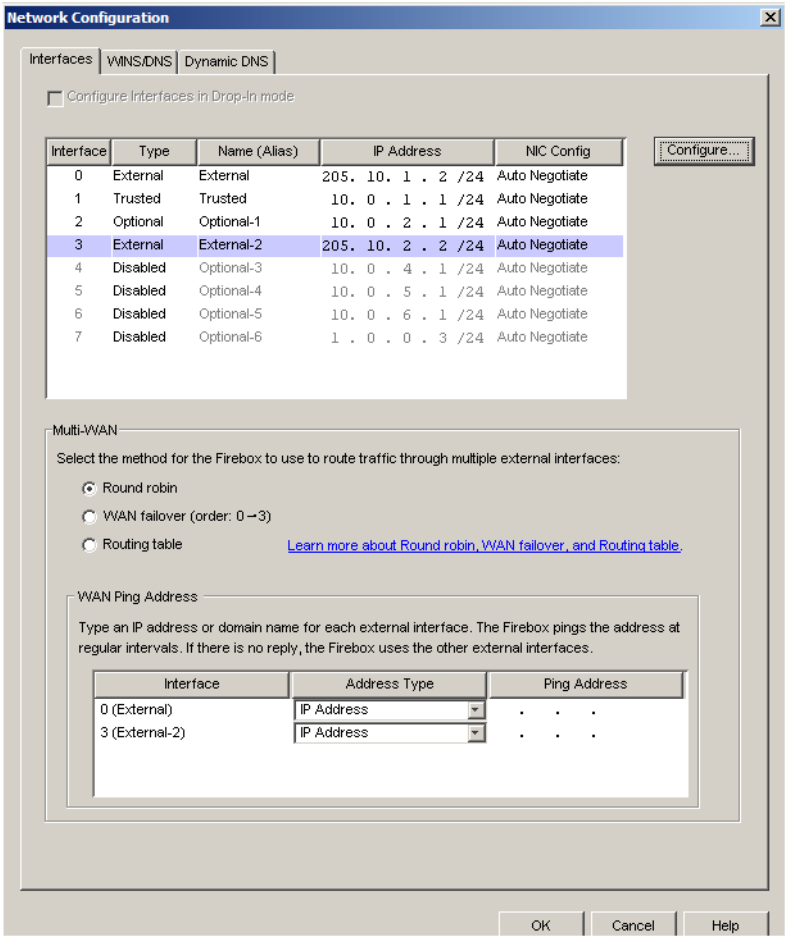



2 选择要配置为外网接口的接口，点击 **Configure（配置）**。从 **Interface Type（接口类型）**下拉列表中选择 **External（外网接口）**调出对话框，输入接口名称及描述。
必须至少配置了两个外网接口才能查看和配置多广域网设置。

3 输入该接口的 IP 地址和默认网关，点击 **OK（确定）**。

输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

第二个外网接口配置完成后， Network Configuration （网络配置）对话框将显示多广域网配置选项。 .




4 选择控制多个外网接口中流量要使用的程序。

共有三个程序，上文已有表述。

5 在 **WAN Ping Address（广域网 Ping 地址）**对话框中，右键点击 **Ping Address（Ping 地址）**列，为每个外网接口添加 IP 地址或域名。建议使用公司外部的计算机的 IP 地址。

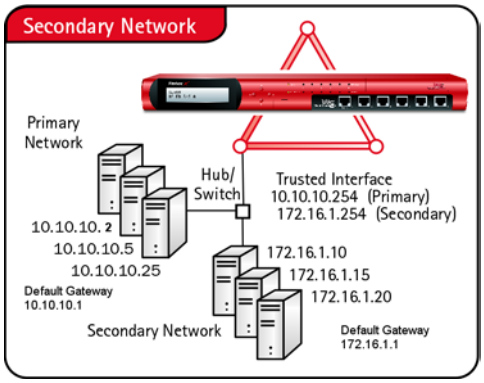
如果某外网接口已启用， Firebox 每隔 20 秒 ping 一次此处设置的 IP 地址或域名，检查接口运行是否正常。如果连 ping 三次均无响应， Firebox 将开始使用配置的下一个外网接口，然后开始 ping 用户为该接口设置的广域网 ping 地址，检查连接情况。

6 点击 **OK（确定）**，将修改保存到 Firebox。

## 添加第二网

第二网是共享与 Firebox® 某一接口同一物理网络的网络。添加第二网时，就为接口创建（或添加）了一个 IP 别名，此 IP 别名是第二网中所有计算机的默认网关。第二网通知 Firebox 在 Firebox 接口上存在另一个网络。

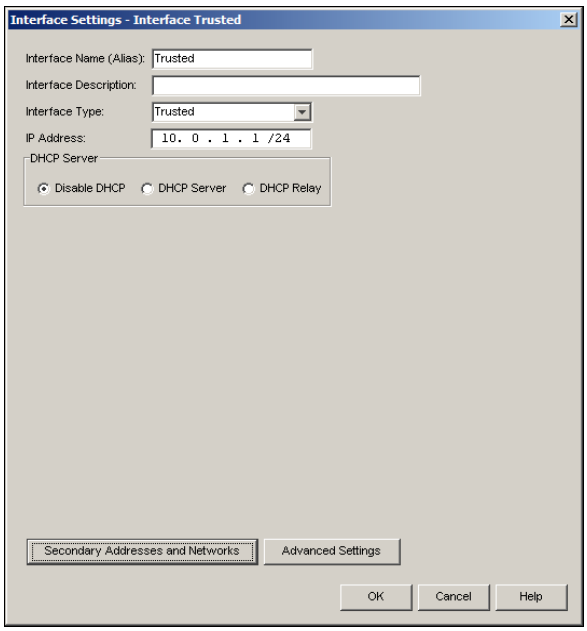
如果 Firebox 配置了静态 IP 地址，可在与主外网接口相同的子网中添加 IP 地址作为第二网。然后可为多个相同类型的服务器配置静态 NAT。例如，如果有两个公共 SMTP 服务器且希望为每个服务器配置静态 NAT 规则，则可为外部第二网配置第二个公共 IP 地址。



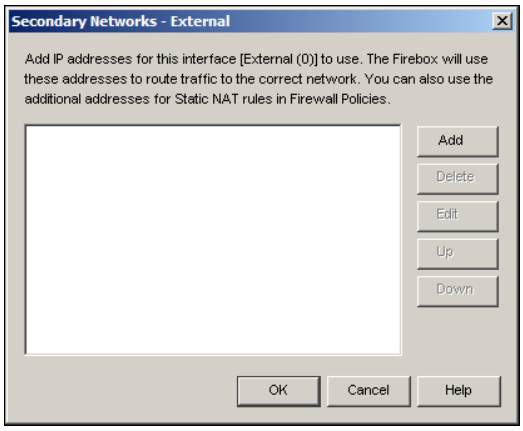

要使用 Policy Manager（策略管理器）配置第二网：

1 选择 **Network（网络）> Configuration（配置）**。
出现 Network Configuration（网络配置）对话框。

2 选择第二网的接口，点击 **Configure（配置）**。
出现 Interface Settings（接口设置）对话框。



3 点击 **Secondary Addresses and Networks （第二地址和网络）**。
出现 Secondary Networks （第二网）对话框。




4 点击 **Add （添加）**，输入来自第二网的未分配 IP 地址。
输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

5 点击 **OK （确定）**，再次点击 **OK （确定）**。

**注释**

需注意要正确添加第二网地址。如果地址不正确， Policy Manager （策略管理器）不会给出提示。建议用户不要在作为另一不同接口上的大型网络中的组件的接口上创建子网作为第二网，否则可能出现欺骗，网络无法正常运行。

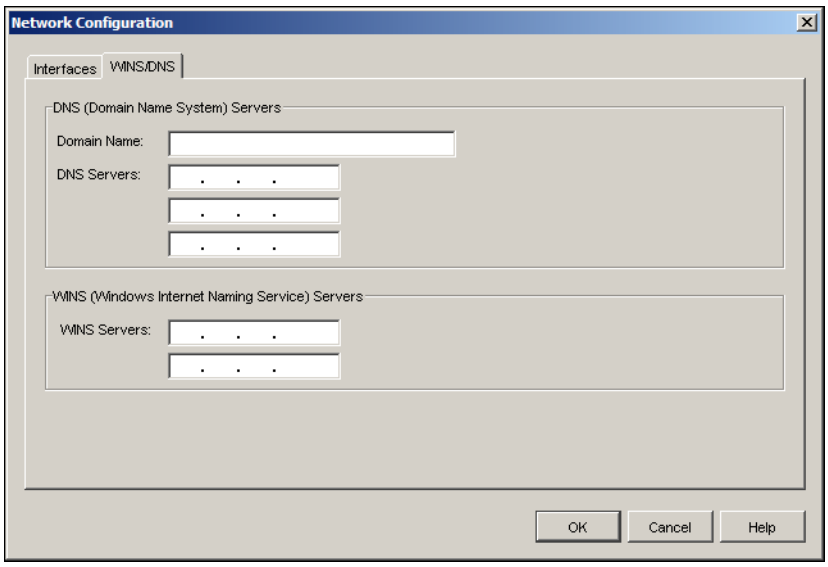
## 添加 WINS 和 DNS 服务器地址

Firebox® 的许多功能必须使用共享 Windows 网络名称服务器（WINS）和域名系统（DNS）服务器 IP 地址，这些功能包括 DHCP 和远程用户 VPN。必须要能从 Firebox 的受信接口访问这些服务器。此信息用于两种用途：

- Firebox 利用此处所示的 DNS 服务器将名称解析为 IP 地址，以使 IPSec VPN、 spamBlocker、GAV 和 IPS 功能可正常运行。
- 受信或可选网络中的 DHCP 客户端、MUVPN 用户和 PPTP RUVPN 用户使用 WINS 和 DNS 项目来解析 DNS 请求。

请一定注意 DHCP 和 RUVPN 只使用一个内部 WINS 和 DNS 服务器，这有助于确认没有创建配置属性阻止用户连接到 DNS 服务器的策略。

1 在 Policy Manager （策略管理器）中，选择 **Network （网络）> Configuration （配置）**。点击 **WINS/DNS** 选项卡。
将显示 WINS/DNS 选项卡中的信息。




2 输入 WINS 和 DNS 服务器的主地址和第二地址，也可在 **Domain Name（域名）**文本框中输入域名后缀，以使 DHCP 客户端可使用 kunstler_mail 等不合格名称。

## 配置动态 DNS

用户可向动态域名服务器 （DNS）服务注册 Firebox® 的外部 IP 地址。动态 DNS 服务确保互联网服务提供商为 Firebox 分配新 IP 地址时域名相连的 IP 地址也相应修改。 Firebox 支持一个动态 DNS 提供商：

DynDNS。有关动态 DNS 的详情，请登录 DynDNS 网站 http://www.dyndns.com

**注释**

WatchGuard® 与 DynDNS 没有联营关系。

### 创建 DynDNS 帐户

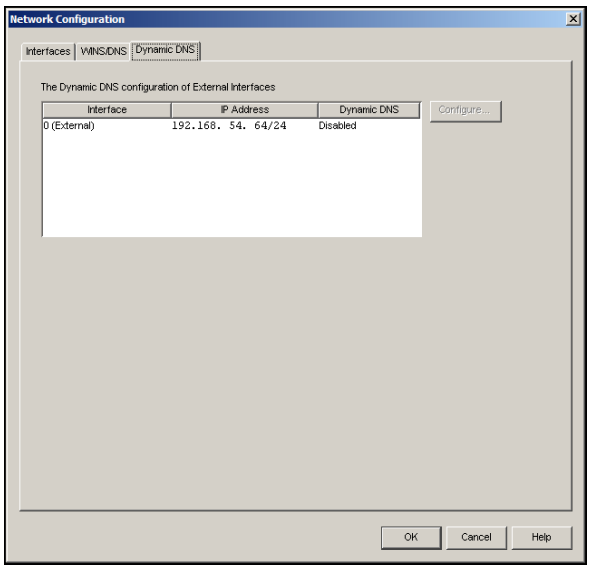
要设置帐户，请访问网站：

http://www.dyndns.com

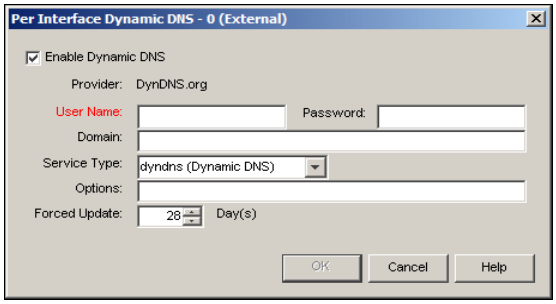
请按 DynDNS 网站上的指示激活帐户，必须完成该操作才能对 Firebox 进行动态 DNS 配置。

## 对 Firebox 进行动态 DNS 设置

1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> Configuration（配置）**。点击 **Dynamic DNS（动态 DNS）**选项卡。
将显示 Dynamic DNS（动态 DNS）选项卡中的信息。




2 选择要配置动态 DNS 的外网接口，点击 **Configure（配置）**。
出现 Per Interface Dynamic DNS（每个接口动态 DNS）对话框。




3 要启用动态 DNS，选择 **Enable Dynamic DNS（启用动态 DNS）**复选框。

4 输入用户名、密码和设置动态 DNS 帐户时使用的域名。

5 在 **Service Type（服务类型）**下拉列表中选择要应用此更新的系统：
- **dyndns** 发送动态 DNS 主机名称的更新。
- **statdns** 发送静态 DNS 主机名称的更新。
- **custom** 发送自定义 DNS 主机名称的更新。

有关各项的详情，请访问 http://www.dyndns.com/services/。

6 在 **Options（选项）**字段，可输入如下所示的任一选项。添加的每个选项前后必须输入一个“&”字符。如果添加多个选项，必须用 “&”字符将各选项隔开。例如：
&backmx=NO&wildcard=ON&
mx=mailexchanger
backmx=YES|NO

wildcard=ON|OFF|NOCHG
offline=YES|NO

有关各选项的详情，请访问：
http://www.dyndns.com/developers/specs/syntax.html

7 使用箭头设置强制更新 IP 地址的时间间隔（单位为天）。

# 配置路由

*路由*是网络流量从数据源到目的地必须经过的设备的顺序。*路由器*是路由中查找下一网络点的设备，网络流量通过该设备发送到目的地。每台路由器至少连接两个网络。数据包可通过一系列装有路由器的网络点，最后到达目的地。

Firebox® 可创建将数据流从接口发送到路由器的静态路由，路由器即可将数据流从指定路由发送到正确目的地。如果不添加到远程网络的路由，所有到该网络的数据流都将发送到 Firebox 默认网关。

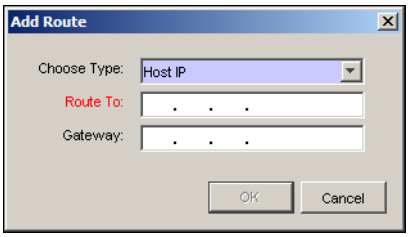
WatchGuard® 用户论坛也提供有关网络路由和路由器的丰富信息。用户可利用 LiveSecurity 服务查询更多信息。

## 添加网络路由

如果用户本地网络中某路由器后存在完整网络，可添加网络路由器。输入网络 IP 地址，并用斜线标注。

1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> Routes（路由）**。
出现 Setup Routes（设置路由）对话框。

2 点击 **Add（添加）**。
出现 Add Route（添加路由）对话框。




3 从下拉列表中选择 **Network IP（网络 IP）**。

4 在 **Route To（路由至）**文本框中输入网络地址，使用斜线标记。
例如，输入 10.10.1.0/24。/24 网络最后八位字节总有一个零。

5 在 **Gateway（网关）**文本框中输入路由器的 IP 地址。
输入的 IP 地址必须与 Firebox 位于同一网络中。

6 点击 **OK（确定）**关闭 **Add Route（添加路由）**对话框。
Setup Routes（设置路由）对话框将显示配置的网络路由。

7 再次点击 **OK（确定）**关闭 **Setup Routes（设置路由）**对话框。

### 添加主机路由

如果路由器后只有一台主机或用户希望数据流只经过一台主机，可添加主机路由。输入指定主机的 IP 地址，不用斜线标记。

1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> Routes（路由）**。
出现 Setup Routes（设置路由）对话框。

2 点击 **Add（添加）**。
出现 Add Route（添加路由）对话框。

3 从下拉列表中选择 **Host IP（主机 IP）**。

4 在 **Route To（路由至）**文本框中输入主机 IP 地址。

5 在 **Gateway（网关）**文本框中输入路由器的 IP 地址。
输入的 IP 地址必须与 Firebox 位于同一网络中。

6 点击 **OK（确定）**关闭 **Add Route（添加路由）**对话框。
Setup Routes（设置路由）对话框将显示配置的主机路由。

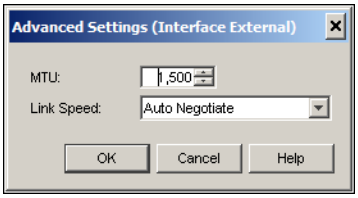
7 再次点击 **OK（确定）**关闭 **Setup Routes（设置路由）**对话框。

## 设置 Firebox 接口速度和双工模式

用户可将 Firebox® 接口的速度和双工参数配置为自动或手动配置。建议用户将速度和双工参数设置为与 Firebox 连接的设备相匹配。必须覆盖自动 Firebox 接口参数时请使用手动配置选项，以与网络中的其他设备相配合。

1 选择 **Network（网络）> Configuration（配置）**。点击要配置的接口，再点击 **Configure（配置）**。

2 点击 **Advanced Settings（高级设置）**。
出现 Advanced Settings（高级设置）对话框。




3 在 **MTU** 值控制中，选择可通过该接口发送的数据包最大长度（单位为字节）。
如果使用 PPPoE，必须将该值修改为 1492，或 ISP 支持的 MRU。如果不使用 PPPoE，建议不要修改 MTU 值。

4 如果希望 Firebox 选择最高网络速度，请在 **Link Speed（链接速度）**下拉列表中选择 **Auto Negotiate（自动协商）**，也可选择一个与用户设备兼容的半双工或全双工速度。

5 点击 **OK（确定）**关闭 **Advanced Settings（高级设置）**对话框。再次点击 **OK（确定）**关闭 **Network Configuration（网络配置）**对话框。

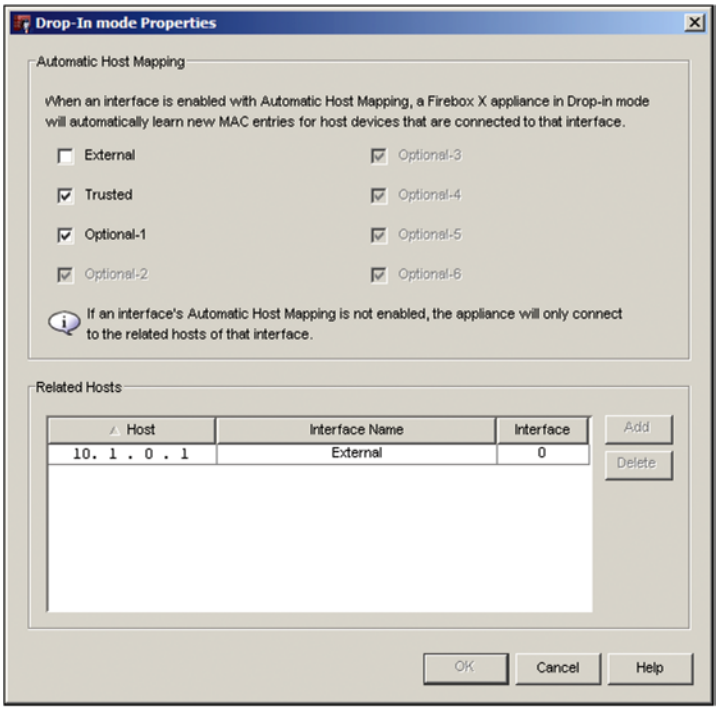
## 配置相关主机

在透明配置模式下， Firebox® 在所有接口上的 IP 地址相同。透明配置模式在 Firebox 接口中分配网络地址范围。当 Firebox 已配置为透明模式且自动主机映射运行不正常时，有时需要用到相关主机。由于对试图查找接口上的设备的 Firebox 的干扰，这种情况有时会发生。如果发生此情况，请

关闭自动主机映射，将为与 Firebox 共享网络地址的计算机添加相关主机项目，这样就在相关主机 IP 地址和为该 IP 地址指定的接口之间建立了静态路由关系。当动态 / 自动主机映射出现问题时，必须使用相关主机项目。

1 在 Policy Manager （策略管理器）中，选择 **Network （网络）> Configuration （配置）**。
出现 Network Configuration （网络配置）对话框。

2 单击 **Properties （属性）**。
出现 Drop-In Mode Properties （透明模式属性）对话框。




3 禁用自动主机映射运行不正常的任何接口上的自动主机映射。

4 点击 **Add （添加）**。输入要从 Firebox 建立静态路由的计算机的 IP 地址。

5 点击 **Interface Name （接口名称）**列，选择相关主机连接的接口。

6 所有相关主机项目添加完成后，点击 **OK （确定）**。将配置保存到 Firebox。

# 第 9 章 使用防火墙 NAT

网络地址转换（NAT）原是为无法从互联网地址注册处获得足够的注册 IP 网络号以满足其日益增加的主机和网络数量的需要的机构开发的解决方案。

NAT 一般用于描述 IP 地址和端口转换的形式。在其最基础层，NAT 修改数据包的 IP 地址值。NAT 的主要目的是增加能不通过可在公网上路由的 IP 地址运行的计算机数量，并隐藏用户局域网中主机的专用 IP 地址。

使用 NAT 有多种不同方式。 WatchGuard® System Manager 支持三种形式的 NAT。

*动态网络地址转换*

动态 NAT 也称为 IP 伪装。 Firebox® 可将此公共 IP 地址应用到所有连接或指定服务的外发数据包，这样就隐藏了作为外网数据包数据源的计算机的真实 IP 地址。动态 NAT 通常在内部主机可访问公共服务时用于隐藏内部主机的 IP 地址。

*1 对 1 网络地址转换*

1对1 NAT绑定可选或受信网络后的主机绑定到内部IP地址。此类NAT用于为外部计算机提供对公共内部服务器的访问权。

*针对策略的静态 NAT*

也称为端口转发。如第 65 页 “*配置策略*”中所述，用户配置策略时配置静态 NAT。静态 NAT 是端口对主机的 NAT。主机从外网发送数据包到外网接口上的端口，静态 NAT 将此 IP 地址修改为防火墙后的 IP 地址和端口。

在配置中有可能使用多种类型的 NAT。用户可将 NAT 用作普通防火墙设置或策略中的设置。请注意防火墙 NAT 设置不用于 BOVPN 或 MUVPN 策略。

## 使用动态 NAT

动态 NAT 是最常用的 NAT，可将外发连接的源 IP 地址修改为 Firebox® 的公共 IP 地址。在 Firebox 外部，只能看到 Firebox 在外发数据包上的 IP 地址。

多台计算机可从同一个公共 IP 地址连接到互联网。动态 NAT 可隐藏用户网络中的主机 IP 地址，因此可为上网的内部主机提供更强大的安全保护。配置了动态 NAT，所有连接都必须从 Firebox 后开始启动。当 Firebox 配置了动态 NAT，恶意主机无法建立与 Firebox 之后的计算机的连接。

在多数网络中，建议使用的安全策略是对所有外发数据包均应用 NAT。使用 Firebox®， **Network（网络）> NAT** 对话框中默认启用动态 NAT，用户创建的每个策略也默认启用动态 NAT。用户可覆盖各自安全策略中的动态 NAT 的防火墙设置。

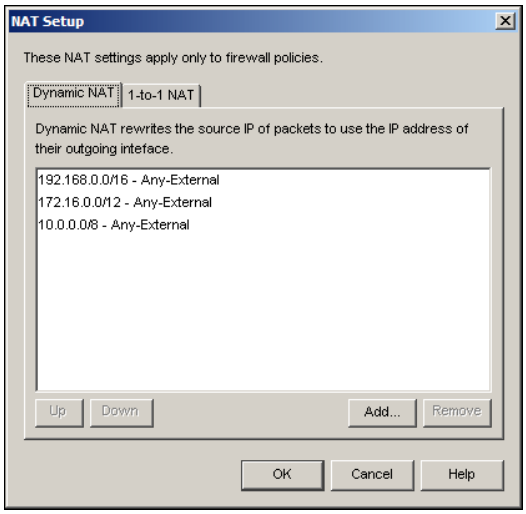
## 添加防火墙动态 NAT 项目

动态 NAT 的默认配置为从所有专用 IP 地址到外部网络均启用动态 NAT。默认项目如下：

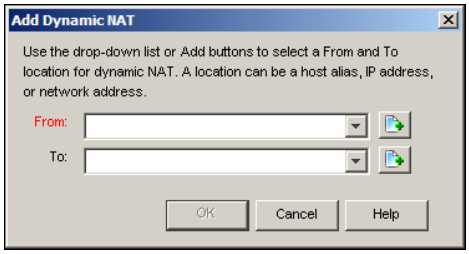
- 192.168.0.0/16 - Any-External
- 172.16.0.0/12 - Any-External
- 10.0.0.0/8 - Any-External

以上三个网络地址是互联网工程工作小组（IETF）保留的专用网络，通常用于局域网的 IP 地址。要对以上地址之外的专用 IP 地址启用动态 NAT，必须添加项目。 Firebox 按动态 NAT 项目列表中的顺序应用动态 NAT 规则，建议用户将规则按符合规则所应用流量的顺序来排列。

1 在 Policy Manager（策略管理器）中，选择 **Network（网络）> NAT**。
出现 NAT Setup（NAT 设置）对话框。




2 在 **NAT Setup (NAT 设置)** 对话框的 **Dynamic NAT (动态 NAT)** 选项卡中，点击 **Add (添加)**。
出现 Add Dynamic NAT（添加动态 NAT）对话框。




3 使用 **From（从）**下拉列表选择外发数据包的数据源。
例如，使用受信主机别名从所有受信网络启用 NAT。有关内置 Firebox 别名的详情，请参见第 73 页的 “*使用别名*”。

4 使用 **To（至）**下拉列表选择外发数据包的目的地。

5 要添加主机或网络 IP 地址，请点击右边的 **Add Device（添加设备）**按钮。使用下拉列表选择地址类型，输入 IP 地址或范围，输入的网络地址必须使用斜线标记。

输入 IP 地址时，请输入所有数字和句点，不要使用 TAB 键或箭头键。

6 点击 **OK（确定）**。
新项目将显示在动态 NAT 项目列表中。

## 对动态 NAT 项目重新排序

要修改动态 NAT 项目的顺序，请选择要修改的项目，然后点击 **Up（上）或 Down（下）**。

用户不能修改动态 NAT 项目。如果定要修改，则必须使用 **Remove（删除）**删除该项，然后再使用 **Add（添加）**重新输入。

## 基于策略的动态 NAT 项目

如果配置了此类 NAT， Firebox 将发出接口的主 IP 地址用于此策略的外发数据包。每个策略均默认启用动态 NAT，使用全局动态 NAT 表。用户可对某策略中的所有数据流禁用动态 NAT。

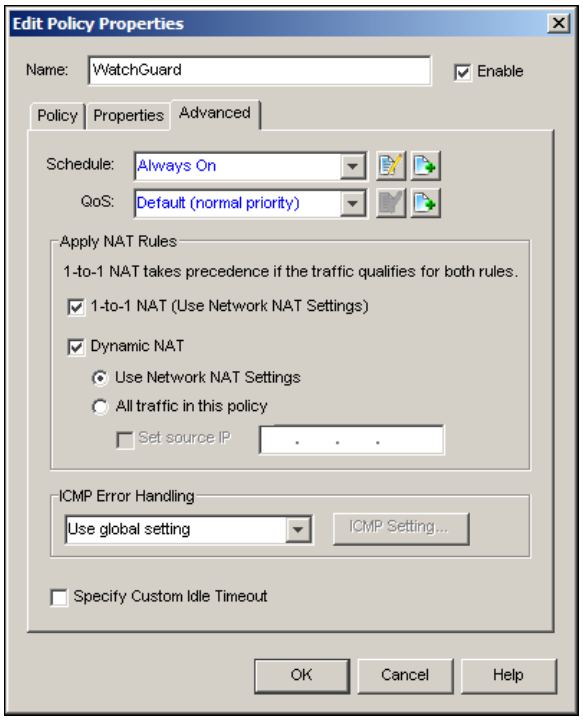
### 禁用基于策略的动态 NAT

1 在 Policy Manager（策略管理器）中，右键点击策略，选择 **Edit（编辑）**。
将显示 Edit Policy Properties（编辑策略属性）窗口。

2 点击 **Advanced（高级）**选项卡。

3 取消对 **Dynamic NAT（动态 NAT）**前的复选框的选择，对该策略所控制数据流关闭 NAT。

4 点击 **OK**（**确定**）。将修改保存到 Firebox。




# 使用一对一 NAT

启用 1 对 1 NAT 后， Firebox® 将修改所有从一组地址范围发送到另一组地址范围的进入和外发数据包，并对其进行路由。用户最多可配置 64 个一对一 NAT 地址，这样就可为单个 /26 网络配置一对一 NAT 规则或在所有一对一 NAT 规则项目中配置 64 个 IP 地址。一对一 NAT 规则始终优先于动态 NAT。

如果一组内部服务器的专用 IP 地址必须转换成公共地址，则常会使用一对一 NAT。用户可使用一对一 NAT 将公共 IP 地址映射到内部服务器，而无需修改内部服务器的 IP 地址。如果用户有一组相似服务器（例如一组邮件服务器），使用一对一 NAT 进行配置比使用静态 NAT 更容易。

为帮助用户理解如何配置一对一 NAT，现举例如下：

ABC 公司的 Firebox X Peak 的受信接口后有一组（五台）专用地址的邮件服务器，地址如下：

10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
10.1.1.5

ABC 公司从与 Firebox 外网接口相同的网络地址中选择了五个公共 IP 地址，并创建了邮件服务器要解析的 DNS 记录，地址如下：

50.1.1.1
50.1.1.2
50.1.1.3

50.1.1.4
50.1.1.5

ABC 公司为邮件服务器配置了一对一 NAT 规则，该规则在对应 IP 地址对之间建立了静态双向关系，关系如下：

10.1.1.1 <--> 50.1.1.1
10.1.1.2 <--> 50.1.1.2
10.1.1.3 <--> 50.1.1.3
10.1.1.4 <--> 50.1.1.4
10.1.1.5 <--> 50.1.1.5

应用一对一 NAT 规则时， Firebox 将在专用 IP 地址池和公共地址池之间创建双向路由和 NAT 关系。

## 定义一对一 NAT 规则

在每个一对一 NAT 策略，用户可配置一台主机、一组主机或一个子网，还必须配置：

*接口*

应用一对一 NAT 的 Firebox® 以太网接口名称。 Firebox 将一对一 NAT 应用到通过接口发送出入的数据包。在上面的示例中，规则应用到外网接口。

*NAT base*

配置一对一 NAT 策略时，用 “从”和 “至”范围的 IP 地址配置策略。 NAT base 是 “至”地址范围中可用的第一个 IP 地址。 NAT base IP 地址是应用一对一 NAT 时 real base IP 地址转变成的地址。在上面的示例中，NAT base 为 50.1.1.1。

*Real base*

配置一对一 NAT 策略时，用 “从”和 “至”范围的 IP 地址配置策略。 Real base 是 “从”地址范围中可用的第一个 IP 地址，是分配给将应用一对一 NAT 策略的计算机的物理以太网接口的 IP 地址。当配置了 real base 地址的计算机的数据包通过指定接口时，即应用了一对一 NAT 操作。在上面的示例中， Real base 为 10.1.1.1。

*应用 NAT 的主机数量（仅针对范围）*

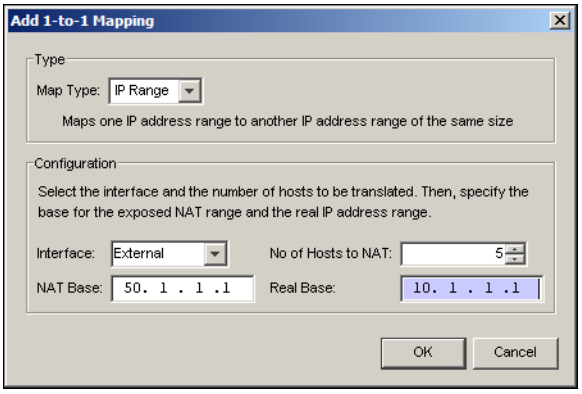
某范围内应用了一对一 NAT 规则的 IP 地址数量。应用一对一 NAT 时，第一个 real base IP 地址转换为第一个 NAT Base IP 地址。应用一对一 NAT 时，范围中的第二个 real base IP 地址转换为第二个 NAT Base IP 地址。一直重复操作，直到达到 “应用 NAT 主机数量”。在上面的示例中，应用 NAT 的主机数量为五。

如果必须在使用相同专用网络地址的两个网络之间创建 VPN 隧道，用户也可利用一对一 NAT 解决问题。创建 VPN 隧道时， VPN 隧道一端的网络必须拥有不同的网络地址范围。如果远程网络的网络范围与本地网络相同，用户可将两个网关配置为使用一对一 NAT。然后可创建 VPN 隧道，无需修改隧道一端的 IP 地址。配置 VPN 隧道时即为 VPN 隧道配置一对一 NAT，而非在 **Network（网络）> NAT** 对话框中进行配置。

## 配置防火墙一对一 NAT

1 在 Policy Manager（策略管理器）中，点击 **Network（网络）> NAT**，再点击 **1-to-1 NAT（一对一 NAT）**选项卡。

2 点击 **Add（添加）**。
出现 1-1 Mapping（一对一映射）对话框。




3 如果要映射到一台主机、一组主机或一个子网，请在 **Map Type（映射类型）**下拉列表中，选择 **Single IP（单个 IP）**、**IP range（IP 地址范围）**或 **IP subnet（IP 子网）**。

4 在 **NAT base** 文本框中输入外部可见的 NAT 范围地址。

5 填完所有信息，点击 **OK（确定）**。

6 对每个一对一 NAT 项目重复 2 – 4 的步骤。完成后，点击 **OK（确定）**关闭 **NAT Setup（NAT 设置）**对话框。将修改保存到 Firebox。

配置全局一对一 NAT 规则后，必须在相应策略中配置 NAT base IP 地址。在上面的示例中，必须将 SMTP 策略配置为允许从 Any 到 50.1.1.1-50.1.1.5 的 SMTP 流量。

## 配置基于策略的一对一 NAT

如果配置了此类 NAT， Firebox 将使用用户配置全局一对一 NAT 时设置的专用和公共 IP 地址，但规则将应用于每个单独的策略。各项策略的默认配置为启用一对一 NAT。如果流量符合一对一 NAT 和动态 NAT 策略，则一对一 NAT 优先。一对一 NAT 不会对该策略禁用动态 NAT。

### 禁用基于策略的一对一 NAT

1 在 Policy Manager（策略管理器）中，右键点击策略，选择 **Edit（编辑）**。

2 将显示 **Edit Policy Properties（编辑策略属性）**窗口。

3 点击 **Advanced（高级）**选项卡。

4 取消对 **1-to-1 NAT（一对一 NAT）**复选框的选择，对该策略所控制数据流关闭 NAT。

5 点击 **OK（确定）**。将修改保存到 Firebox。

## 配置基于策略的动态 NAT

如果配置了此类 NAT， Firebox 将专用 IP 地址映射到公共 IP 地址。各项策略的默认配置为启用动态 NAT。如果要使用为 Firebox 设置的动态 NAT 规则，请选择 **Use Network NAT Settings（使用网络 NAT 设置）**。如果要将 NAT 应用到此策略中的所有流量，请选择 **All traffic in this policy（此策略中所有流量）**。如果流量符合一对一 NAT 和动态 NAT 策略，则一对一 NAT 优先。一对一 NAT 不会对该策略禁用动态 NAT。

用户还可选择为使用动态 NAT 的任何策略设置动态 NAT 源 IP 地址，这确保了使用此策略的任何流量显示来自用户公共或外部 IP 地址范围为源地址。当 Firebox 外网接口的 IP 地址不同于 MX 记录 IP 地址时，用户要强制外发 SMTP 流量显示用户域的 MX 记录地址，会最常用到此操作。

一对一 NAT 规则优先级高于动态 NAT 规则。

**注释**

如果使用多广域网，则不能使用 **Set Source IP（设置源 IP）**选项。只有在 Firebox 使用单个外网接口时才能使用此选项。

### 禁用基于策略的动态 NAT

1 在 Policy Manager（策略管理器）中，右键点击策略，选择 **Edit（编辑）**。

2 将显示 **Edit Policy Properties（编辑策略属性）**窗口。

3 点击 **Advanced（高级）**选项卡。

4 取消对 **Dynamic NAT（动态 NAT）**复选框的选择，对该策略所控制数据流关闭动态 NAT。

## 配置针对策略的静态 NAT

静态 NAT 也称为端口转发，是端口对主机的 NAT。主机发送外网数据包到外网接口上的端口。静态 NAT 将此 IP 地址修改为防火墙后的 IP 地址和端口。如果软件应用程序使用多个端口且动态选择端口，用户必须使用一对一 NAT 或检查 Firebox® 上是否存在管理此类数据流的代理服务器。

使用静态 NAT 时，用户使用 Firebox 的外部 IP 地址，而非公共服务器的 IP 地址，如果用户希望或者公共服务器无公共 IP 地址，可进行此操作。例如，用户可将 SMTP 邮件服务器装于配置了专用 IP 地址的 Firebox 后面，在 SMTP 策略中配置静态 NAT。Firebox 收到端口 25 上的连接，确认任何 SMTP 数据流发送到 Firebox 后的真正 SMTP 服务器。

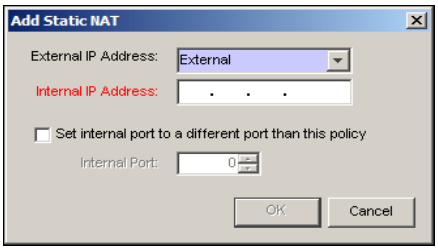
由于静态 NAT 的工作方式，这只对使用指定 TCP 或 UDP 端口的策略才可行。配置其他协议的策略无法使用流入静态 NAT。如果用户有使用 TCP 或 UDP 之外的其他协议的策略，该策略的 **Properties（属性）**对话框中的 **NAT** 按钮将被禁用。静态 NAT 也不能用于 Any 策略。

1 双击 Policies（策略）选项中的策略图标。

2 在 **Connections are（连接）**下拉列表中选择 **Allowed（允许）**。
要使用静态 NAT，策略必须允许流入数据流通过。

3 在 **To（至）**列表中，点击 **Add（添加）**。
出现 Add Address（添加地址）对话框。

4 点击 **NAT**。
出现 Add Static NAT（添加静态 NAT）对话框。




5 在 **External IP Address（外部 IP 地址）**下拉列表中选择此服务要使用的公共 IP 地址。

6 输入内部 IP 地址。
内部 IP 地址是受信或可选网络中的目的地。

7 如有必要，请选择 **Set internal port to different port than this policy（将内部端口设置到此策略外的不同端口）**复选框，这将启用端口地址转换（PAT）。
通常不使用此功能。此功能可将数据包目的地修改至指定内部主机和不同端口。如果选择此复选框，请输入不同端口号或使用 Internal Port（内部端口）框中的箭头按钮。

8 点击 **OK（确定）**关闭 **Add Static NAT（添加静态 NAT）**对话框。
静态 NAT 路由将显示在 Members and Addresses（成员和地址）列表中。

9 点击 **OK（确定）**关闭 **Add Address（添加地址）**对话框。点击 **OK（确定）**关闭该服务的 **Properties（属性）**对话框。

# 第 10 章 实施身份验证

用户身份验证将用户名与通过 Firebox 的连接相对应。通过用户身份验证之后， Firebox 管理员在监控通过 Firebox 的连接时使用用户名和 IP 地址。若不经过身份验证，用户只能看见各连接的 IP 地址。不经过身份验证，用户虽然可从任何计算机登录网络，但只能看见允许其查看的信息。用户从该 IP 地址发起的所有连接在用户进行身份验证时也传输会话名称。

Firebox 允许用户创建包含群组和用户名的策略，因此，策略应用于用户登录的任何计算机。在下列情况下，通过用户名进行监控 :

- 如果使用动态主机配置协议（ DHCP ）。 DHCP 可使计算机的 IP 地址发生变化。
- 如果多个不同用户使用在同一天内使用相同的 IP 地址，如在大学或计算机实验室。

在上述情况下，身份验证可提供关于员工操作的更多信息。

## 如何进行用户身份验证

HTTPS 服务器在 Firebox® 上运行，接受验证请求。要进行身份验证，用户必须连接到 Firebox 上的验证网页，地址为 :

https://*Firebox 接口 IP 地址* : *4100*

或

https://*Firebox*: *4100 主机名称*

出现身份验证电子表单。用户必须输入用户名和密码。 Firebox 使用 PAP （ 密码验证协议 ）将名称和密码发送到验证服务器。用户通过身份验证后，可使用允许的网络资源。用户关闭最后一次通过验证的连接后，用户身份验证可保留一段时间。此身份验证超时由 Firebox 管理员在 **Policy Manager （ 策略管理器 ） > Setup （ 设置 ）> Global Settings （ 全局设置 ）中进行设置**。

要在身份验证超时前关闭经过验证的会话，用户可点击验证页面的 **Logout （ 登出 )**。如果该页面已关闭，用户必须重新打开，断开连接。要阻止用户进行身份验证，管理员必须在验证服务器上禁用该用户的帐户。

## 从外部网络进行身份验证

验证工具的主要功能是对外发数据流进行验证，用户也可将其用于限制流入的网络流量。如果在 Firebox 上有帐户，可一直使用外部验证。例如，用户可于家中在浏览器中输入以下地址：
https://Firebox 外部接口 IP 地址：4100

完成身份验证后，用户可使用 Firebox 上配置的策略。

可通过此程序让远程用户从外部网络进行身份验证，这样该用户可通过 Firebox 使用资源。

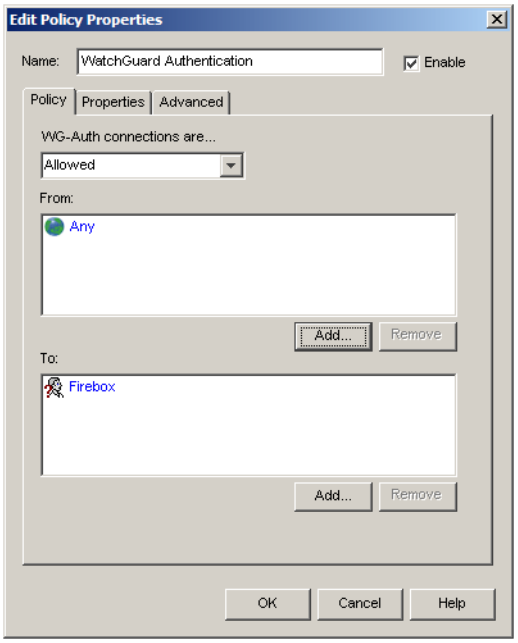
1 在 Policy Manager 中，双击 **WatchGuard Authentication** policy（**WatchGuard 验证策略**）图标，用户为策略配置添加用户或群组后将显示该策略。
编辑自动配置的策略时将出现警告，提示用户小心操作。

2 点击 **Policy**（**策略**）选项卡。

3 在 **WG-Auth Connections are**（**WG-Auth 连接**）下拉列表中选择 **Allowed**（**允许**）。

4 在 **From**（**从**）框下，点击 **Add**（**添加**）。在列表中选择 **Any**（**任何**），点击 **Add**（**添加**），再点击 **OK**（**确定**）。

5 在 **To**（**至**）框下，点击 **Add**（**添加**）。在列表中选择 **Firebox**，点击 **Add**（**添加**），再点击 **OK**（**确定**）。




## 使用通过网关 Firebox 到另一 Firebox 的验证

要通过网关 Firebox 向另一 Firebox 发送验证请求，必须添加在网关 Firebox 上允许验证流量的策略。在网关 Firebox 上，使用 Policy Manager（策略管理器）添加 WatchGuard 身份验证策略，该策略控制 TCP 端口 4100 上的流量。将该策略配置为允许到目的 Firebox 之 IP 地址的流量。

### 验证服务器类型

Fireware® 有五种身份验证方法 :

- Firebox
- RADIUS
- SecurID
- LDAP
- Active Directory

用户可为 Firebox 配置一种或多种验证服务器类型。对不同服务器类型的验证对于用户来说几乎相同。对于 Firebox 管理员来说，差别在于用户数据库可能在 Firebox 上，也可能在专用验证服务器上。

使用验证服务器时，根据厂家的指示说明进行配置，出于安全考虑，将可访问 Firebox 的服务器安装在 Firebox 之后。

### 使用备用验证服务器

用户可配置具有所有类型第三方验证的备用验证服务器。如果 Firebox 无法连接到主验证服务器（三次尝试失败），将连接到备用验证服务器。如果 Firebox 无法连接到备用验证服务器，将等待 10 分钟，然后再次尝试连接主验证服务器。如此循环，直到 Firebox 连接到验证服务器为止。

## 将 Firebox 配置为验证服务器

如果不使用第三方验证服务器，可使用 Firebox® 作为验证服务器。该程序将用户公司分为若干群组和用户进行身份验证。用户指定了人员的群组由其执行的任务和使用的信息进行控制。例如，用户可拥有一个财务组，一个营销组和一个研发组，也可设置一个新员工组，对互联网有受控访问权。

在群组中，可设置用户身份验证程序、系统类型以及用户可访问的信息。用户可以是网络或计算机。如果用户公司发生变化，可添加或删除群组中的用户或系统。

可使用 Policy Manager（策略管理器）:

- 添加、修改或删除配置中的群组
- 添加或修改群组中的用户

### 关于 Firebox 验证

用户可将 Firebox 配置为对用户进行三种不同类型的身份验证 :

- 防火墙验证
- PPTP 连接
- MUVPN 连接

验证成功后， Firebox 将在以下各项间创建映 :

- 用户名称
- 该用户所在的 Firebox 用户组
- 用户进行身份验证时用户计算机的 IP 地址
- 用户连接 RUVPN 时用户计算机的虚拟 IP 地址

### 防火墙验证

要在 Policy Manager （策略管理器）中创建 Firebox 用户帐户，请选择 **Setup （安装）> Authentication Servers（验证服务器）**。创建用户帐户后，可创建 Firebox，将该用户设置在该 Firebox 用户组中。

然后创建只允许进出 Firebox 用户名列表或 Firebox 群组列表的流量的策略，该策略只在数据包来自或发往通过身份验证用户的 IP 地址时应用。

用户输入 https://Firebox 接口 IP 地址 :4100，用通过端口 4100 到 Firebox 的 HTTPS 连接进行身份验证。

如果用户名和密码有效，则该用户通过身份验证。

用户通过身份验证后，其计算机上的用户信任信息和 IP 地址将用于查找是否有策略应用于进出该用户计算机的流量。

### PPTP 连接

要将 Firebox 配置为可主持 PPTP VPN 会话，请选择 **VPN > Remote Users （远程用户）**，点击 **PPTP** 选项卡。如果不选择 **Use RADIUS Authentication to authenticate remote users （对远程用户使用 RADIUS 进行身份验证）**复选框，Firebox 将对 PPTP 会话进行验证。Firebox 检查用户在 VPN 连接框中输入的用户名和密码是否与 Firebox 用户数据库中的用户名和密码相匹配。如果用户提供的信任信息与 Firebox 用户数据库中的帐户相匹配，该用户通过 PPTP 会话验证。

然后创建只允许进出 Firebox 用户名列表或 Firebox 群组列表的流量的策略， Firebox 不看此策略，除非流量来自或发往通过验证的用户虚拟 IP 地址。

用户使用其计算机操作系统中的 PPTP 功能创建 PPTP 连接。由于 Firebox 允许来自任何提供正确信任信息的 Firebox 用户的 PPTP 连接，请务必创建 PPTP 会话策略，只包括准备允许其通过 PPTP 会话发送数据流的用户；或将这些用户设置在 Firebox 用户组中，并创建只允许来自该群组的数据流的策略。 Firebox 为此配置了一个群组，名为 “PPTP-Users”。

### MUVPN 连接

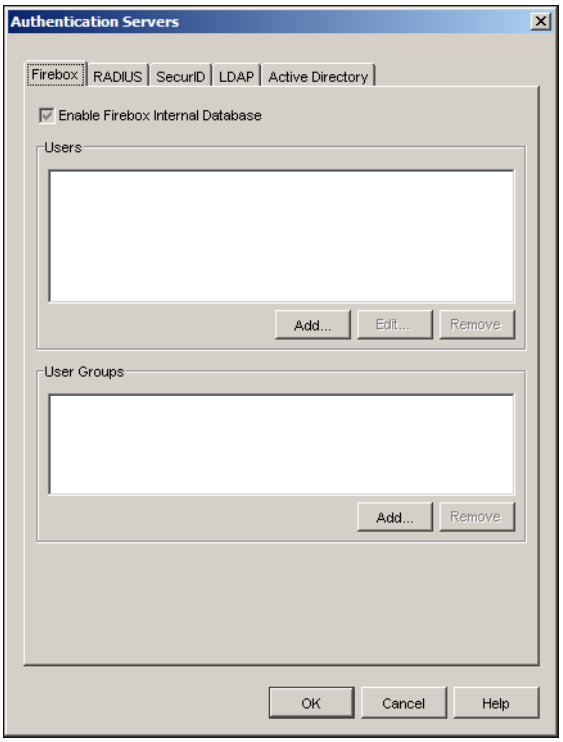
用户可将 Firebox 配置为主持移动用户 VPN （ MUVPN ） IPSec 会话。选择 **VPN > Remote Users （远程用户）**，点击 **Mobile User VPN （移动用户 VPN）**选项卡。用户可使用 Add Mobile User VPN （添加移动用户 VPN ）向导创建 MUVPN 群组。向导完成后， Policy Manager （策略管理器）进行以下两项操作 :

- 创建客户端配置文件（称为 .wgx 文件）并置于创建 MUVPN 帐户的管理工作站计算机上。用户要配置 MUVPN 客户端计算机，必须使用该 .wgx 文件。
- 在 **Mobile User VPN （移动用户 VPN）**选项卡中自动添加 “Any” 策略，允许流量进出通过身份验证的 MUVPN 用户。

用户计算机正确配置后，用户可创建 MUVPN 连接。如果用户在 MUVPN 验证对话框中输入的用户名和密码与 Firebox 用户数据库中的相匹配，且该用户属于您创建的 MUVPN 群组，则 MUVPN 会话通过验证。 Policy Manager （策略管理器）将自动创建策略，允许来自通过身份验证用户的任何数据流。要限制 MUVPN 客户端可访问的端口，请删除 Any （任何）策略，在 **Mobile User VPN （移动用户 VPN）**选项卡中添加该等端口的策略。有关如何添加策略，请参见第 146 页的 “*添加策略*”。

## 将 Firebox 设置为验证服务器

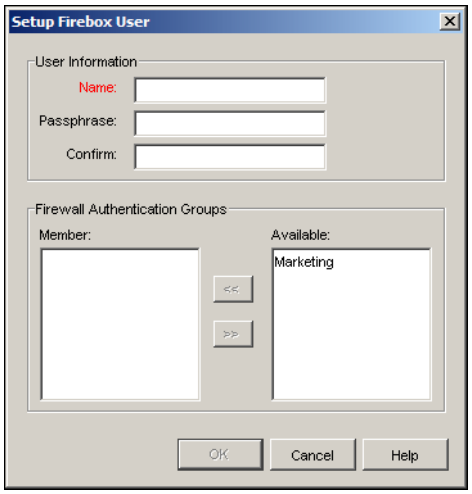
1 在 Policy Manager 中，选择 **Setup**（设置）> **Authentication Servers**（验证服务器）。
将显示 Authentication Servers（验证服务器）对话框，默认配置为启用 Firebox 验证服务器。




2 要添加新用户群组，请点击 **User Groups**（用户组）列表下的 **Add**（添加）。
出现 Add Firebox Group（添加 Firebox 群组）对话框。


3 输入群组名称，点击 **OK**（确定）。

4 要添加新用户，请点击 **User（用户）**列表下的 **Add（添加）**。
出现 Setup Firebox User（设置 Firebox 用户）对话框。




5 输入希望进行 Firebox 验证的人员使用的名称和密码短语。
此密码短语设置后，就无法再看见简单文本形式的密码短语。如果此密码短语丢失，必须重新设置新密码短语。
6 要在群组中添加用户，请在 **Available（可用）**列表中选择群组名称，点击指向左边的双箭头，将名称移至 **Member（成员）**列表中。
也可双击群组名称。
7 如果要在服务中使用 PPTP-Users 群组，请将该用户添加到 PPTP-Users 群组中。
8 将用户添加到所选群组后，点击 **OK（确定）**。
用户已添加到用户列表中，可接着添加更多用户。
9 要关闭 **Setup Firebox User（设置 Firebox 用户）**对话框，请点击 **OK（确定）**。
出现 Firebox Users（Firebox 用户）选项卡，显示新用户列表。
10 添加所有必要用户和群组完成后，点击 **OK（确定）**。现在即可使用用户和群组对策略和验证进行配置。

## 对防火墙用户、PPTP 和 MUVPN 验证使用本地用户帐户

任何用户均可作为防火墙用户、 PPTP 用户或 MUVPN 用户进行身份验证，如果设备上启用了 PPTP 或 MUVPN，还可创建 PPTP 或 MUVPN 隧道。但身份验证或隧道成功确立后，用户只能在 Firebox 策略允许数据流的情况下通过 VPN 隧道发送数据流。例如，只使用 MUVPN 的用户可通过 MUVPN 隧道发送数据流，但不能通过 PPTP 隧道发送数据流，即使该用户可进行身份验证并创建 PPTP 隧道。

1 启用防火墙用户身份验证、 MUVPN 和 PPTP，并配置为使用本地帐户。
2 为这些验证类型创建相应策略。
3 为各验证群组（防火墙用户、 PPTP 用户及 MUVPN 用户）关联一用户帐户，并创建一个不属于以上任何群组的帐户。
4 将配置部署到 Firebox。

5 使用网页浏览器、PPTP 客户端和 MUVPN 客户端向具有一个或多个上述用户帐户的 Firebox 进行身份验证。

## 配置 RADIUS 服务器验证

远程身份验证拨入用户服务（RADIUS）对公司网络中的本地用户和远程用户进行身份验证。RADIUS 是客户 / 服务器系统，将用户身份验证信息、远程访问服务器、VPN 网关和其他资源保存在中央数据库中。

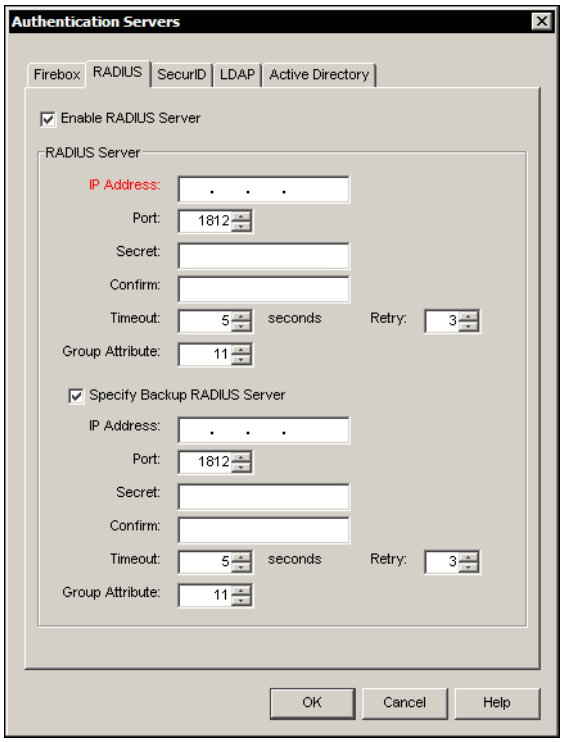
RADIUS 服务器收发的验证消息始终使用验证码。RADIUS 客户端和服务器上的该验证码或共享密钥必须相同。黑客无此验证码就无法攻击验证消息。请注意， RADIUS 在身份验证过程中，发送的是验证码，并非密码。对于网页和 MUVPN 验证， RADIUS 只支持 PAP（非 CHAP）验证。对于 PPTP 验证， RADISU 只支持 MSCHAPv2。

要使用 Firebox® 的 RADIUS 服务器身份验证，必须：

- 按 RADIUS 文件中的要求，将 Firebox 的 IP 地址添加到 RADIUS 服务器。
- 启用并在 Firebox 配置中指定 RADIUS 服务器。
- 在 Policy Manager（策略管理器）的策略中添加 RADIUS 用户名或群组名。

要启用 RADIUS 服务器身份验证：

1 在 Policy Manager 中，选择 **Setup（设置）> Authentication Servers（验证服务器）**。点击 **RADIUS Server（RADIUS 服务器）**选项卡。
显示 RADIUS 配置。




2 在 **IP Address（IP 地址）**框中输入 RADIUS 服务器的 IP 地址。

3 在 **Port（端口）**框中，请一定选择 RADIUS 进行身份验证使用的端口号。
默认端口号为 1812，较早版本的 RADIUS 服务器可能使用端口 1645。
4 在 **Secret（密钥）**框中，输入 Firebox 和 RADIUS 服务器共享的密钥。
共享密钥是区分大小写的密码， Firebox 和 RADIUS 服务器的密钥必须相同。
5 要设置超时值，请使用 **Timeout（超时）**值控制箭头设置需要的数值。
这将设置 Firebox 尝试再次连接之前等待验证服务器响应的时间。
6 要设置 Firebox 尝试连接的次数，请使用 **Retry（重试）**值控制箭头设置需要的数值。
这是 Firebox 在报告验证连接失败之前尝试连接验证服务器的次数（使用上面指定的超时）。
7 要设置群组属性，请使用 **Group Attribute（群组属性）**值控制箭头设置需要的属性。
群组属性值用于设置携带用户群组信息的属性。 RADIUS 服务器向用户通过身份验证的 Firebox 发送消息时，也同时发送用户群组字串，如 “engineerGroup”或 “financeGroup”，该信息用于访问控制。
8 要添加备用 RADIUS 服务器，请选择 **Specify Backup RADIUS Server（指定备用 RADIUS 服务器）**复选框。如果选择该复选框，请输入备用 RADIUS 服务器的 IP 地址和端口。主 RADIUS 服务器和备用 RADIUS 服务器上的共享密钥必须相同。
9 点击 **OK（确定）**。

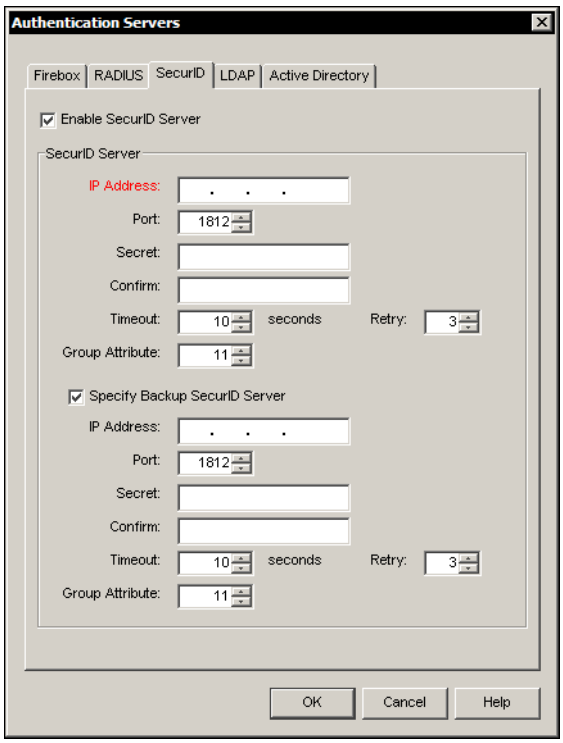
## 配置 SecurID 验证

要使用 SecurID 验证，必须正确配置 RADIUS 和 ACE/ 服务器。用户还必须具有经认可的 SecurID 令牌和 PIN 码（个人识别码）。详情请参阅 “*SecurID 说明*”。

**注释**

SecurID 验证不要使用 Steel Belted RADIUS。将 RADIUS 软件应用程序配合 RSA SecurID 软件使用。

1 在 Policy Manager 中，选择 **Setup**（**设置**）> **Authentication Servers**（**验证服务器**）。点击 **SecurID Server**（**SecurID 服务器**）选项卡。




2 在 **IP Address**（**IP 地址**）框中输入 SecurID 服务器的 IP 地址。

3 在 **Port**（**端口**）框中，使用数值控制箭头选择用于 SecurID 验证的端口号。
默认号为 1812。

4 在 **Secret**（**密钥**）框中，输入 Firebox® 和 SecurID 服务器共享的密钥。
共享密钥是区分大小写的密码， Firebox 和 SecurID 服务器的密钥必须相同。

5 在 **Timeout**（**超时**）框中，使用数值控制箭头选择要设置的超时值。
这将设置 Firebox 尝试再次连接之前等待验证服务器响应的时间。

6 要设置 Firebox 尝试连接的次数，请使用 **Retry**（**重试**）值控制箭头。
这是 Firebox 在报告验证连接失败之前尝试连接验证服务器的次数（使用上面指定的超时）。

7 选择群组属性。建议用户不要修改此值。
群组属性值用于设置携带用户群组信息的属性。 SecurID 服务器向用户通过身份验证的 Firebox 发送消息时，也同时发送用户群组字串，如 “engineerGroup”或 “financeGroup”，该信息用于访问控制。

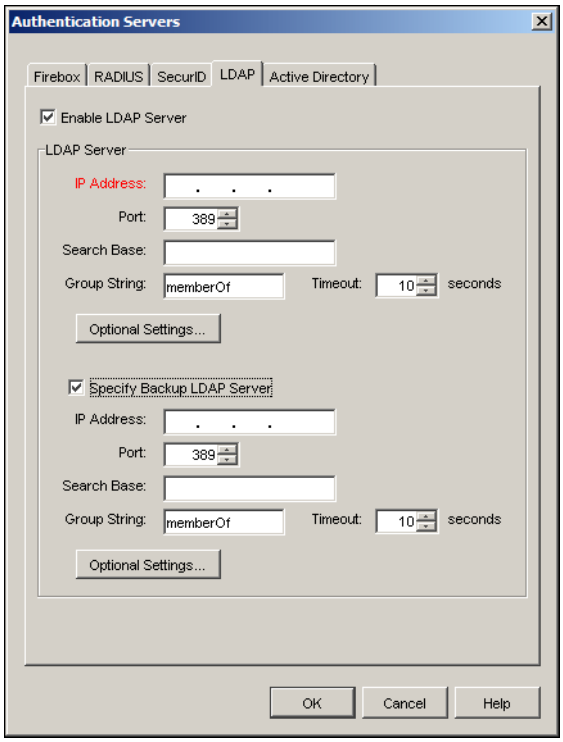
8 输入备用 SecurID 服务器的 IP 地址和端口。主 SecurID 服务器和备用 SecurID 服务器上的共享密钥必须相同。

9 点击 **OK**（**确定**）。

# 配置 LDAP 验证

可使用 LDAP （轻量级目录访问协议）验证服务器对 Firebox® 用户进行身份验证。 LDAP 是针对使用网上目录服务的开放式标准协议，与 TCP 等网络传输协议共同使用。可利用 LDAP 访问独立目录服务器或 X.500 目录。

1 在 Policy Manager 中，选择 **Setup （设置）> Authentication Servers （验证服务器）**。选择 **LDAP** 选项卡。




2 选择 **Enable LDAP Server （启用 LDAP 服务器）**复选框。

3 在 **IP Address （IP 地址）**框中，输入 Firebox 联系验证请求所需的主 LDAP 服务器的 IP 地址。
LDAP 服务器可安装在任何 Firebox 接口上或通过 VPN 隧道进行使用。

4 在 **Port（端口）**下拉列表中，选择 Firebox 用于连接 LDAP 服务器的 TCP 端口号，默认端口号为 389。
不支持 SSL 绑定到端口 636。

5 输入 **Search Base （搜索库）**。搜索库设置的标准格式为：ou=organizational unit （组织单位）， dc= 服务器专有名称第一部分， dc= 服务器专有名称在点之后的任何部分。
例如，如果用户帐户在称为 “accounts” 的 OU （组织单位）中，且域名为 kunstlerandsons.com，则搜索库为 : “ou=accounts,dc=kunstlerandsons,dc=com”.
可设置搜索库，对 Firebox 用来搜索验证匹配的验证服务器上的目录施以限制。

6 输入 **Group String （群组字串）**。
这是用于在 LDAP 服务器上保存用户群组信息的属性字串。在许多 LDAP 服务器上，默认群组字串是 “uniqueMember”，而在其他服务器上则是 “member”。

7 如有必要，可修改超时值，该值为 Firebox 等待验证服务器响应的时间。

8 如果有备用 LDAP 服务器，请添加该服务器的信息。

9 要将 MUVPN 用户配置为从 LDAP 服务器接收配置信息，可修改目录方案，使用可通过 **Optional Settings（可选设置）**按钮使用的设置。可在 LDAP 服务器的用户属性中输入 MUVPN 客户端信息，包括 IP 地址、子网掩码或 DNS 和 WINS 服务器。然后可将这些字段映射到 Optional Settings（可选设置）中显示的字段。MUVPN 用户通过 Firebox 启动 VPN 隧道后，Firebox 将使用 LDAP 用户属性中的信息为用户设置 IP 地址、子网掩码或 DNS 和 WINS 服务器。

IP *属性字串*
输入包含指定 IP 地址的 LDAP 用户属性字段名。

*子网掩码属性字串*
输入包含指定子网掩码的 LDAP 用户属性字段名。

*DNS 属性字串*
输入包含 DNS 服务器 IP 地址的 LDAP 用户属性字段名。

*WINS 属性字串*
输入包含 WINS 服务器 IP 地址的 LDAP 用户属性字段名。

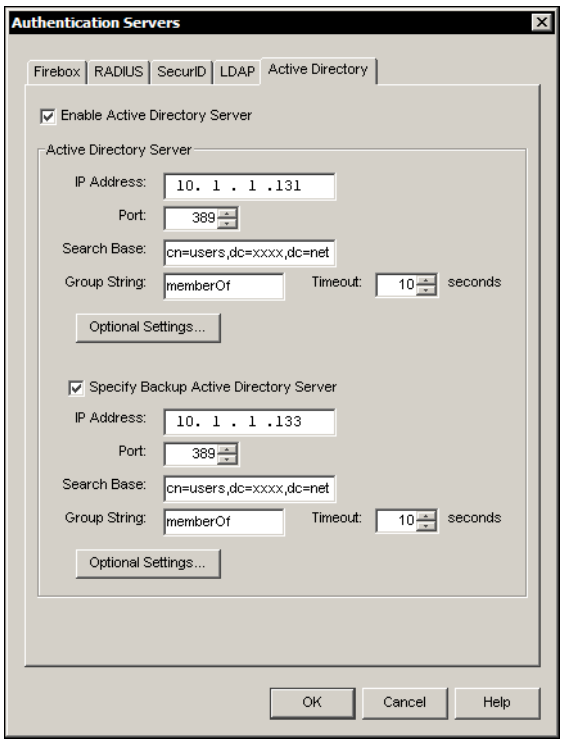
*租期属性字串*
输入包含 MUVPN 连接会话允许总时间的 LDAP 用户属性字段名。

*空闲超时属性字串*
输入包含指定空闲超时的 LDAP 用户属性字段名。

# 配置 Active Directory 验证

可使用 Active Directory 验证服务器对 Firebox® 用户进行身份验证。必须对 Firebox® 和 Active Directory 服务器进行配置。

1 在 Policy Manager 中，选择 **Setup（设置）> Authentication Servers（验证服务器）**。选择 **Active Directory** 选项卡。




2 选择 **Enable Active Directory Server（启用 Active Directory 服务器）**复选框。

3 输入主 Active Directory 服务器的 IP 地址。
Active Directory 服务器可安装在任何 Firebox 接口上或通过 VPN 隧道进行使用。

4 选择 Firebox 用于连接 Active Directory 服务器的 TCP 端口号，默认端口号为 389。
如果 Active Directory 服务器为全局编录服务器，则可用于修改默认端口。详情请访问 https://www.watchguard.com/support/Fireware_H owto/H owTo_U seG lobal Catalog Port.pdf。

5 输入 **Search Base（搜索库）**。搜索库设置的标准格式为：ou=organizational unit（组织单位），dc= 服务器专有名称第一部分，dc= 服务器专有名称在点之后的任何部分。
例如，如果用户帐户在称为 “accounts” 的 OU（组织单位）中，且域名为 HQ_main.com，则搜索库为 : “ou=accounts,dc=HQ_main,dc=com”。
可设置搜索库，对 Firebox 用来搜索验证匹配的验证服务器上的目录施以限制。

6 输入 **Group String（群组字串）**。
这是用于在 Active Directory 服务器上保存用户群组信息的属性字串。如果未修改 Active Directory 方案，群组字串始终为 “memberOf”。

7 如有必要，可修改超时值，该值为 Firebox 等待验证服务器响应的时间。

8 如果有备用 Active Directory 服务器，请添加该服务器的信息。

9 要将 MUVPN 用户配置为从 Active Directory 服务器接收配置信息，可修改目录方案，使用可通过 **Optional Settings（可选设置）**按钮使用的设置。可在 Active Directory 服务器的用户属性中输

入 MUVPN 客户端信息，包括 IP 地址、子网掩码或 DNS 和 WINS 服务器。然后可将这些字段映射到 Optional Settings（可选设置）中显示的字段。MUVPN 用户通过 Firebox 启动 VPN 隧道后，Firebox 将使用 Active Directory 用户属性中的信息为用户设置 IP 地址、子网掩码或 DNS 和 WINS 服务器。

IP *属性字串*
输入包含指定 IP 地址的 Active Directory 用户属性字段名。

*子网掩码属性字串*
输入包含指定子网掩码的 Active Directory 用户属性字段名。

*DNS 属性字串*
输入包含 DNS 服务器 IP 地址的 Active Directory 用户属性字段名。

*WINS 属性字串*
输入包含 WINS 服务器 IP 地址的 Active Directory 用户属性字段名。

*租期属性字串*
输入包含指定租期的 Active Directory 用户属性字段名。

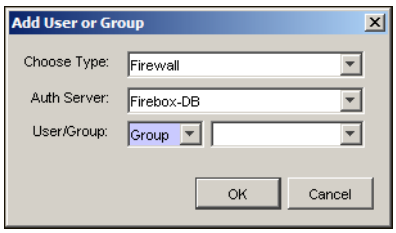
*空闲超时属性字串*
输入包含指定空闲超时的 Active Directory 用户属性字段名。

## 使用用户身份验证配置策略

如果将 Firebox 配置为使用验证服务器，在 Policy Manager（策略管理器）中创建策略时就可以开始使用用户名了。例如，你可以将所有策略设置为仅允许通过验证的用户可以建立连接。操作如下：

1 在包含所有用户帐户的第三方验证服务器上创建一个群组。

2 在 Policy Manager（策略管理器）中，添加或启用 Outgoing（外发）策略。点击 **From（从）**字段下的 **Add（添加）**，再点击 **Add User（添加用户）**。
出现 Add User or Group（添加用户或群组）对话框。




3 在 **Choose Type（选择类型）**下拉列表中，选择防火墙、MUVPN 或 PPTP 验证。

4 在 **Auth Server（验证服务器）**下拉列表中，选择要使用的验证服务器类型。

5 在 **User/Group（用户 / 群组）**下拉列表中，选择 **User（用户）**或 **Group（群组）**。

6 输入在验证服务器上创建的用户或群组名称。点击 **OK（确定）**。

7 在 Policy Manager（策略管理器）中以相同方式配置所有策略的 **From（从）**字段。

8 在策略配置中添加用户或群组后，WSM 会自动添加一条 WatchGuard 验证策略到 Firebox 配置，该策略用于控制对验证网页的访问。

# 第 11 章　防火墙入侵检测及防御

WatchGuard® Fireware® 和用户在 Policy Manager （ 策略管理器 ）中创建的策略严格控制对用户网络的接入。严格的接入政策使黑客不能进入您的网络。但是，这样严格的政策也有不能击败的其它类型攻击。认真配置 Firebox® 缺省包处理选项能阻止下列攻击：SYN flood attack、欺骗攻击及端口或地址空间探测 （ address space probe ）。

配置缺省包处理后，防火墙将检查接收到的每个数据包的源头和目的地。它查看 IP 地址及端口号并监视数据包，并对比表明网络受到威胁的模式。如果有威胁存在，您可以配置 Firebox，以自动阻挡可能受到的攻击。这种先发制人的入侵检测方法将黑客置于您的网络之外。您也可以购买 Firebox 的升级版本以使用基于特征的入侵防御。如需了解更多详情，请参阅本手册中 “*基于特征的入侵检测和防御*”一章。

## 使用缺省包处理选项

防火墙检查接收到的每个数据包的源头和目的地。它查看 IP 地址及端口号。防火墙也监视数据包，并对比表明网络受到威胁的模式。

缺省包处理 :

- 拒绝可能是安全威胁的数据包，包括可能是欺骗攻击或 SYN flood attack 的一部分的数据包
- 能自动阻挡前往及源自某个源 IP 地址的所有流量
- 将事件添加至日志文件
- 将 SNMP 陷阱 （ SNMP trap ）发送至 SNMP 管理服务器
- 发送疑似安全威胁的通知

用 **Default Packet Handling （ 缺省包处理 ）**对话框设置所有的缺省数据包处理选项。

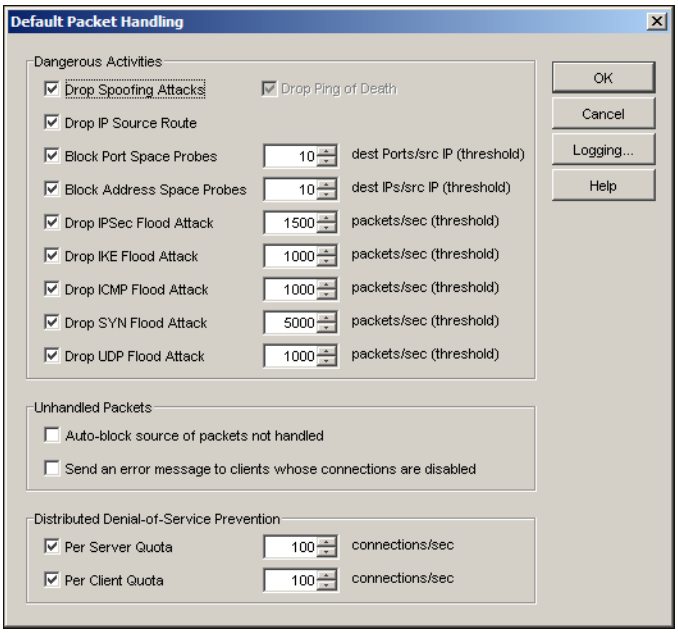
1　从 Policy Manager （ 策略管理器 ）中选择 **Setup （ 设置 ） >Intrusion Prevention （ 入侵防御 ） >Default Packet Handling （ 缺省包处理 ）**。

或

点击 Policy Manager （ 策略管理器 ）工具栏上的缺省包处理选项图标。

弹出 Default Packet Handling （ 缺省包处理 ）对话框。

2 选择您想要阻止的流量模式复选框（见下一节中的解释）。如果发生了这些事件中的一件，缺省配置将发送一条日志信息。如需配置 SNMP trap 或缺省包处理通知，点击 **Logging（日志）**。




## 欺骗攻击

黑客进入您的网络的惯用方法之一就是制作 “电子假身份”。利用这种 “IP 欺骗”程序，黑客发送一个 TCP/IP 数据包，使用与主机首次发送的 IP 地址不同的 IP 地址。

阻止 IP 欺骗的功能启用后， Firebox® 进行检测并核实数据包是否真实反映访客接口所在网络的源 IP 地址。

为防止这种欺骗攻击，可在 **Default Packet Handling（缺省包处理）**对话框中选择 **Drop Spoofing Attacks（禁止欺骗攻击）**复选框。

## IP 源路由攻击

黑客使用 IP 源路由攻击发送一个 IP 数据包，以查找数据包经过的网络路由。然后，黑客能看到对数据包的应答，并获得关于目标计算机或网络的操作系统的信息。

为防御 IP 源路由攻击，在 **Default Packet Handling（缺省包处理）**对话框中选择 **Drop IP Source Route（禁止 IP 源路由）**复选框。

## “Ping of death”攻击

“Ping of death”是一种拒绝服务（DoS）攻击，是黑客发送 IP 协议允许的大于 65,535 个字节的 IP 数据包引起的，它导致一些操作系统的崩溃或重启。

为防御 Ping of death 攻击，必须始终打开 **Drop Ping of Death（禁止 Ping of Death）**功能。不可禁用本功能。

## 端口空间和地址空间攻击

黑客使用探测器寻找关于局域网及其主机的信息。端口空间探测器探查主机以找到其使用的服务。地址空间探测器探查网络以查看该网络上有哪些主机。

为防御端口及地址空间攻击，在 **Default Packet Handling （缺省包处理）**对话框中选择 **Block Port Space Probes （阻止端口空间探测器）**和 **Block Address Space Probes （阻止地址空间探测器）**复选框。然后，用箭头为每个源 IP 地址选择允许的 IP 地址或端口探测器最大数量。

## 洪水攻击

在洪水攻击中，黑客向系统发送巨大的数据流，使系统不能检查和允许获得许可的网络流量。例如，如果系统收到足够的 ICMP ping 命令（使用所有资源发送回复命令），即为 ICMP 洪水攻击。Firebox 能防御下列洪水攻击：

- IPSec 洪水攻击
- IKE 洪水攻击
- ICMP 洪水攻击
- SYN 洪水攻击
- UDP 洪水攻击

洪水攻击也称为拒绝服务（DoS）攻击。您可以用 **Default Packet Handling （缺省包处理）**对话框配置 Firebox 从而阻止这些攻击。选择您想要防御的洪水攻击的复选框。用箭头选择每秒钟处理的数据包最大允许数量。

### 关于 SYN flood attack 的设置

对于 SYN flood attack，您可以为 Firebox 设置阈值以报告可能发生的 SYN flood attack。但如果仅收到阈值量的数据包，尚不会有数据包被禁止。如果为阈值的两倍，所有 SYN 数据包都会被禁止。在您定义的阈值与两倍阈值之间的任何水平，如果一个数据包的 src_IP、 dst_IP 和总长度与之前收到的数据包一致，则该数据包将被禁止。其它情况下， 25% 的收到的新数据包将被禁止。

例如，假如您将阈值定义为每秒 18 个数据包，当您收到这个数量的数据包时， Firebox 会向您发出警告：可能发生了 SYN flood attack，但不会禁止数据包。如果您每秒收到 20 个数据包， Firebox 将禁止 25% 的数据包（即 5 个数据包）。如果您每秒收到 36 个或更多的数据包，最后收到的 18 个或更多的数据包将被禁止。

## 未经处理的数据包

“未经处理的数据包”是不符合 Policy Manager（策略管理器）中创建的任何规则的数据包。Firebox 将拒绝该数据包，但您也可以选择始终自动阻止其源头，这个操作将把发送该数据包的 IP 地址添加至临时受禁网站列表。 Firebox 收到未经处理的数据包时，您也可以将 TCP 重设或 ICMP 错误送回至客户端。

## 分布式拒绝服务攻击

分布式拒绝服务（DDoS）攻击几乎与洪水攻击等同。在分布式拒绝服务攻击中， ICMP ping 命令来自许多电脑。您可以用 **Default Packet Handling （缺省包处理）**对话框配置 Firebox 以防御分布式拒绝服务攻击。用箭头键设置您的服务器和客户端每秒钟收到的最大容许连接数量。

# 设置受禁网站

受禁网站功能帮助防御您从系统了解到的或认为是危险或安全威胁的网络流量。发现可疑的数据流源头后，您可以阻止与该 IP 地址的所有连接，也可以配置 Firebox 在该源头每次试图连接您的网络时就发送一条日志消息。从日志文件中，您可以看到它们经常攻击的服务。

受禁网站是不能通过 Firebox 的检查从而建立连接的 IP 地址。如果一个数据包来自受禁的系统，则不能通过 Firebox®。

有两种不同的受禁 IP 地址：

- 永久受禁网站 — 被纳入您手动设置的配置文件中的一个列表，称为受禁网站列表。
- 自动受禁网站 — Firebox 在临时受禁网站列表上添加或拦截的 IP 地址。Firebox 采用为每项服务制订的数据包处理规则。例如，您可以配置 Firebox 以阻止企图连接到受禁端口的 IP 地址，然后这些地址被隔离一段特定的时间，因此被称为临时受禁网站列表。

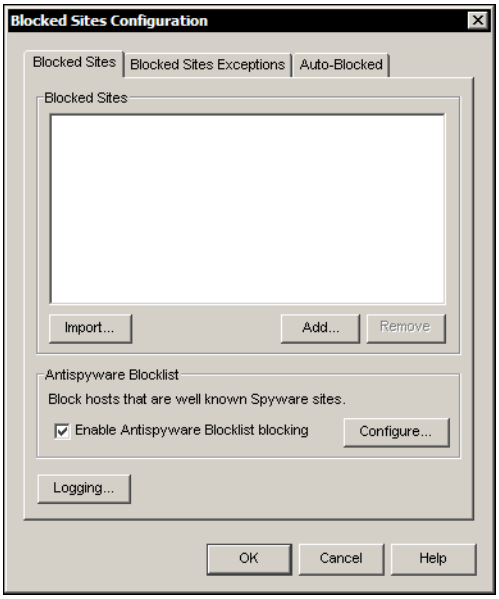
您可以使用临时受禁网站列表及日志文件帮助您决定哪些 IP 地址应永久受禁。

## 永久性隔离一个网站

您可以用 Policy Manager（策略管理器）永久地隔离您知道属于安全威胁的一个主机。例如，一台黑客频繁使用的大学里的计算机就是一台很应该隔离的主机。

1 在 Policy Manager（策略管理器）中选择 **Setup（设置）>Intrusion Prevention（入侵防御）>Blocked Sited（受禁网站）。**

弹出 Blocked Sites Configuration（受禁网站配置）对话框。




2 点击 **Add（添加）**

弹出 Add Site（**添加网站对话框**）。

3 用 **Choose Type（选择类型）**下拉列表选择受禁类型。选项为：**Host IP（主机 IP）**、**Network IP（网络 IP）**、或 **Host Range（主机范围）**。

4 输入受禁值

如果是一个 IP 地址或一个 IP 地址范围，将显示受禁类型。您输入一个 IP 地址时，应输入所有数值和受禁时期。勿使用 tab 键或箭头键。

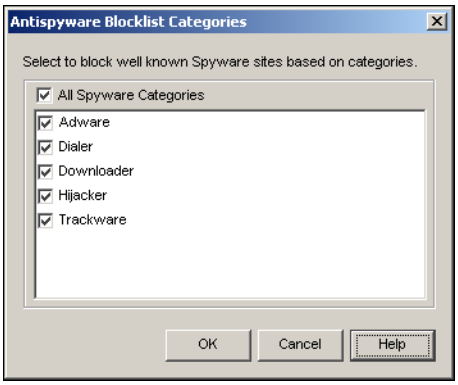
5 点击 **OK（确认）**
新网站出现在受禁网站列表中。

## 隔离间谍软件网站

通过配置要隔离的间谍软件网站的类型，可以隔离间谍软件。

1 在 **Blocked Sites（受禁网站）**对话框中，选择 **Enable Antispyware Blocklist blocking（启用反间谍软件隔离列表功能）**对话框。

2 默认状况下，如果您在上一步中选择了复选框， Firebox 将阻止所有类型的间谍软件。如需选择您想要隔离的间谍软件类型，点击 **Configure（配置）**。
弹出 Antispyware Blocklist Categories（反间谍软件隔离类型）对话框。




3 选择或清除下列复选框，为这些类型启用或禁用反间谍软件隔离功能。如需启用或禁用所有类型，选择或清除 **All Spyware Categories（所有间谍软件类型）**复选框：

*广告软件*
指程序运行时显示广告条的软件应用程序。有时候，广告软件包含记录用户个人信息的代码，并在未获得用户授权及用户不知情的情况下将其发送给第三方。

*拨号软件*
指能劫持用户的调制调解器，并且拨打可接入不良网站的收费号码的软件应用程序。

*下载软件*
指获得并安装其它文件的程序，大多数被配置为从指定的网站或 FTP 网站上获取文件。

*劫持软件（Hijacker）*
一种恶意软件，它能改变计算机的浏览器设置并将引导您到您并不想浏览的网站。

*行为记录（Trackware）*
指未获得用户许可而使用计算机互联网连接发送个人信息的任何软件。

## 使用受禁网站的外部列表

您可以在外部文件中创建一张受禁网站列表。该文件必须是一个 .txt 文件。要将外部文件添加至您的受禁网站列表中：

1 在 **Blocked Sites Configuration（受禁网站配置）**对话框中选择 **Import（导入）**。

2 找到文件，并双击该文件，或选中该文件并选择 **Open （ 打开 ）**。
文件中的网站将出现在受禁网站列表中。

## 创建受禁网站列表的例外

如果某台主机是受禁网站的例外项，则该主机不会出现在受禁列表中。自动规则不适用于这台主机。

1 从 Policy Manager （ 政策管理器 ）中选择 **Setup （ 设置 ）>Intrusion Prevention （ 入侵防御 ）>Blocked Sites （ 受禁网站 ）**。

2 点击 **Blocked Sites Exception （ 受禁网站例外 ）**选项卡，再点击 **Add （ 添加 ）**。

3 使用 **Choose Type （ 选择类型 ）**下拉列表选择受禁类型。选项为：**Host IP （ 主机 IP ）**、Network **IP （ 网络 IP ）**、或 **Host Range （ 主机范围 ）**。

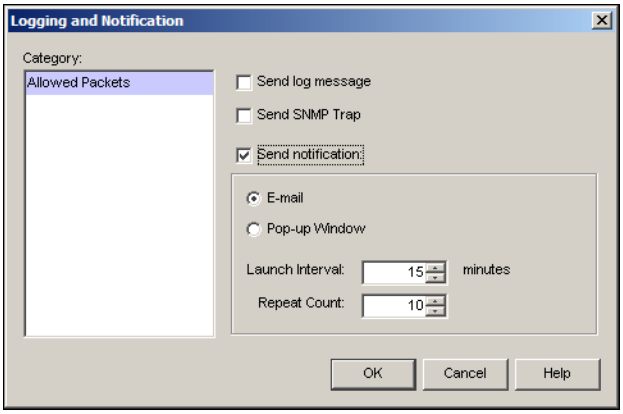
4 输入受禁值。
受禁类别将显示此地址是单一的 IP 地址还是一系列 IP 地址。您输入 IP 地址时，应输入所有数字和句点。请勿使用 TAB 键或箭头键。

5 选择 **OK （ 确认 ）**。

## 设置日志和通知参数

可以对 Firebox 进行配置，使其在某一主机尝试访问任何受禁网站时生成一条日志记录，也可以将其配置为在某一主机尝试访问任何受禁网站时发出通知。

1 从 **Blocked Sites （ 受禁网站 ）**中选择 **Logging （ 日志 ）**。
弹出日志和通知对话框。




2 设置符合安全政策的参数及通知：

*Enter it in the log （ 在日志中将其输入 ）*
启用此复选框后，如果一个数据包因受禁端口的设置而遭到拒绝， Firebox 将发送一条日志消息。所有服务的默认设置为：Firebox 在拒绝数据包时发送一条日志消息。

*Send SNMP trap （ 发送 SNMP trap ）*
启用本复选框后， Firebox 发送一个事件通知至 SNMP 管理系统。 SNMP trap 将确定数据流与允许值相匹配。阈值限制就是它检查的一个标准范例。

*Send notification （发送通知）*

启用本复选框后，如果一个数据包因受禁端口的设置而遭拒绝， Firebox 将发出一份通知。您可以设置 Firebox 以完成下列操作之一：

- **E-mail （电子邮件）**：事件发生时， Firebox 发出一封电子邮件消息。请在日志服务器用户界面中的 **Notification （通知）**选项卡中设置电子邮件地址。
- **Pop-up Window （弹出窗口）**：事件发生时，Firebox 以对话框的形式在管理站上做出提示。

### 设置发送间隔和重复计数

您可以控制通知时间及重复计数，如下所示：

*Launch Interval （发送间隔）*

指不同通知之间相隔的最短时间（以分钟计算）。本参数防止在短时间内为同一事件发送多份通知。

*Repeat count （重复计数）*

计算事件发生的频率。当它达到设定值时，一个专用通知器将被激活。该通知器将对指定通知进行重复性日志输入。达到事件数量后，通知再次开始。

下面是如何使用这两个值的例子。如果将这两个值设为：

- 发送间隔 = 5 分钟
- 重复计数 = 4

端口空间探测器从早上 10 点开始运行，并且时时都在继续。这样，日志和通知机制开始了。下面是时间和发生的事件：

1 10:00— 最初的端口空间探测器（首次事件）

2 10:01— 首次通知开始（一件事件）

3 10:06— 第二次通知开始（报告五件事件）

4 10:11— 第三次通知开始（报告五件事件）

5 10:16— 第四次通知开始（报告五件事件）

发送间隔控制了事件 1、 2、 3、 4、 5 之间的时间间隔。时间间隔设置为 5 分钟。将重复计数与发送间隔相乘，即为事件必须继续开始重复通知器的时间间隔。

## 用政策设置临时隔离网站

您可以使用政策设置隔离企图使用拒绝服务的网站：

1 在 Policy Manager（政策管理器）中，双击政策图标。
弹出 Properties（属性）对话框。

2 在 **Policy（策略）**选项框中，确保将 **Connections Are（连接为）**下拉列表设置为 **Denied（拒绝）**。

3 在 **Properties （属性）**选项卡中，选择复选框 **Automatically block sites that attempt to connect （自动隔离企图连接的网站）**。
遭拒数据包的 IP 地址将被添加至 Blocked Sites（受禁网站）列表，并在默认状态下持续 20 分钟。

# 隔离端口

可以将已知的可被用来攻击用户网络的端口隔离起来。此操作也将停止特定的外部网络服务。隔离一个端口后，将覆盖所有的服务设置。

您可以隔离一个端口，因为：

- 通过隔离端口，可以保护最敏感的服务。本功能有助于使您免受 Firebox® 设置错误的影响。
- 当敏感服务遭到刺探时，系统将生成独立的日志记录。

在默认配置状态下， Firebox 将隔离一些目的站端口。如此即可生成通常无需更改的基本配置。它将隔离如下端口的 TCP 和 UDP 数据包：

*X Window System （端口 6000 – 6005）*

X Window System （或 X–Windows）客户端连接未加密，所以在互联网上使用很危险。

*X Font Server （端口 7100）*

很多版本的 X–Windows 运行 X Font Server。 X Font Server 在一些主机上作为超级用户运行。

*NFS （端口 2049）*

NFS （网络文件系统）是一种频繁使用的 TCP/IP 服务。在该项服务中，许多用户在网路上使用同样的文件。但新版本具有严重的认证及安全问题。

在互联网上提供 NFS 是非常危险的。

**注释**

在使用 NFS 的系统中，端口映射器将频繁使用 2049 端口。如果您使用 NFS，确保 NFS 在您所有的系统上均使用端口 2049。

*rlogin、 rsh、 rcp （端口 513、 514）*

这些服务用于实现与其它计算机的远程接入。他们存在安全风险，而且经常遭到黑客的刺探。

*RPC 端口映射器 （端口 111）*

RPC 服务通过端口 111 查找给定 RPC 服务器所使用的各个端口。RPC 服务很容易通过互联网遭到攻击。

*端口 8000*

许多供应商使用本端口，但有许多与此有关的安全问题。

*端口 1*

TCPmux 服务使用端口 1，但使用频率不高。您可以将其隔离，使检查端口的工具难以将其发现。

*端口 0*

此端口经常被 Firebox 隔离。您不能将本端口添加至受禁网站列表，并且不能允许端口 0 上的流量通过 Firebox。

**注释**

如果必须允许使用推荐的受禁端口的软件程序中的数据流通过，建议您仅允许流量通过 IPSec VPN 隧道或接入使用 ssh 的端口，以达到更安全的目的。

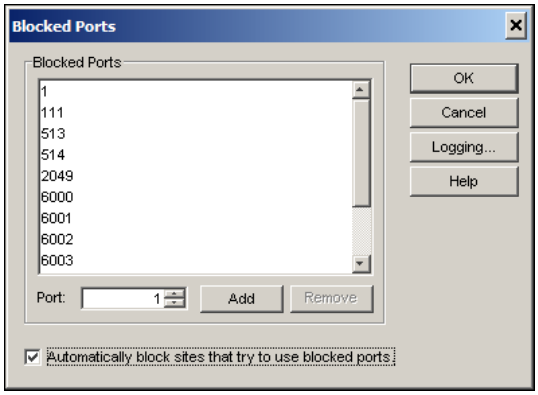
### 避开受禁端口的问题

受禁端口可能会给你带来麻烦。您在隔离高于 1023 的端口号码时必须十分小心。客户频繁地使用这些源端口号码。

## 永久性隔离一个端口

1 从 Policy Manager（政策管理器）中选择 **Setup（设置）>Intrusion Prevention（入侵防御）>Blocked Ports（受禁端口）**。
弹出受禁端口对话框。

2 输入端口号码。点击 **Add（添加）**。
新端口号码显示在受禁端口列表中。




## 自动隔离试图使用受禁端口的 IP 地址

可以设置 **Firebox** 以自动隔离试图访问受禁端口的外部主机。在 **Blocked Ports（受禁端口）**对话框中，选择 **Automatically block sites that try to use blocked ports（自动隔离试图使用受禁端口的站点）**对话框。

## 为受禁端口设置日志和通知

你可以对 Firebox 进行设置，使其在某一主机试图使用受禁端口时，生成日志记录。当主机试图访问受禁端口时。您也可以对 Firebox 进行设置，使其在某一主机试图使用受禁端口时，发出通知或让 Firebox 将 SNMP trap 发送至 SNMP 管理服务器。

设置受禁端口日志和通知参数的步骤与设置受禁网站的步骤相同，请参阅第 140 页 “*设置日志和通知参数*”。

# 第 12 章　配置策略

在 Policy Manager（策略管理器）中，有两种策略：数据包过滤器和代理服务器。

数据包过滤器检查每个数据包的 IP 报头，是防火墙最基本的功能。它控制进出 Firebox® 的网络流量。如果数据包报头信息合法，则 Firebox 接受该数据包；如果数据包报头信息不合法，则 Firebox 丢弃该数据包。它还可以记录日志消息或向源头发送错误信息。

代理服务器采用与数据包过滤器同样的步骤检查报头信息，同时它还检查内容。如果该内容不符合设置的标准，则代理服务器拒绝该数据包。代理服务器在应用程序层上运行，而数据包过滤器在网络和传输协议层上运行。激活代理服务器后， Firebox 将：

- 拦截删除所有网络数据
- 检查内容是否符合 RFC 标准及内容类型
- 再次添加网络数据
- 发送数据包至其目的地

与数据包过滤器相比，代理服务器使用更多的资源和带宽。但代理服务器能找到数据包过滤器不能发现的危险内容。

在本用户指南中，数据包过滤器和代理服务器统称为策略。除非另有说明，相关步骤均适用于代理服务器和数据包过滤器。

Policy Manager（策略管理器）将每个数据包过滤器和代理服务器显示为一个图标。可以接受或拒绝流量，您可以设置源头和目的地，也可以为日志和通知设置规则，并且配置数据包过滤器或代理服务器的端口、协议和其它参数。

WatchGuard® Fireware® 包括许多预设的数据包过滤器和代理服务器。例如，如果想为所有 Telnet 流量设置一个数据包过滤器，则可添加 Telnet 策略，还可以创建自定义数据包过滤器并为其设置端口、协议和其它参数。

## 为网络创建策略

公司的安全策略是规定如何保护计算机网络和通过该网络的信息的一套规则。 Firebox® 拒绝未经特殊批准的所有数据包。该安全策略有助于使网络免遭：

- 使用新的或不同的 IP 协议的攻击

- 未知的应用程序

用 Quick Setup Wizard （快速安装向导）配置 Firebox 时，您只需要设置基本的策略（DNS 客户端、 FTP 和 TCP 外发代理服务器）及接口 IP 地址。如果有多个软件应用程序和网络流量需要 Firebox 进行检查，必须：

- 在 Firebox 上配置策略，让必需的流量通过
- 为每项策略设置获批准的主机和属
- 平衡保护网络的要求与用户访问外部资源的要求

配置 Firebox 时，建议设置对外访问的限制。

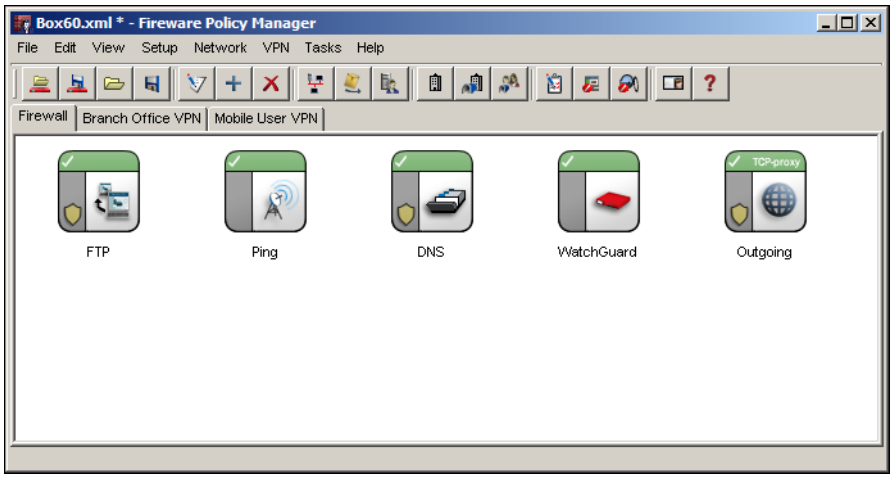
# 添加策略

您可使用 Policy Manager （策略管理器）添加策略。 Policy Manager （策略管理器）显示图标或一个列表以标识 Firebox® 上配置的策略。对于每项策略，您可以：

- 设置允许的流量源和目的地
- 制订过滤规则和策略
- 启用或禁用策略
- 配置 QoS、 NAT、计划和日志等属性

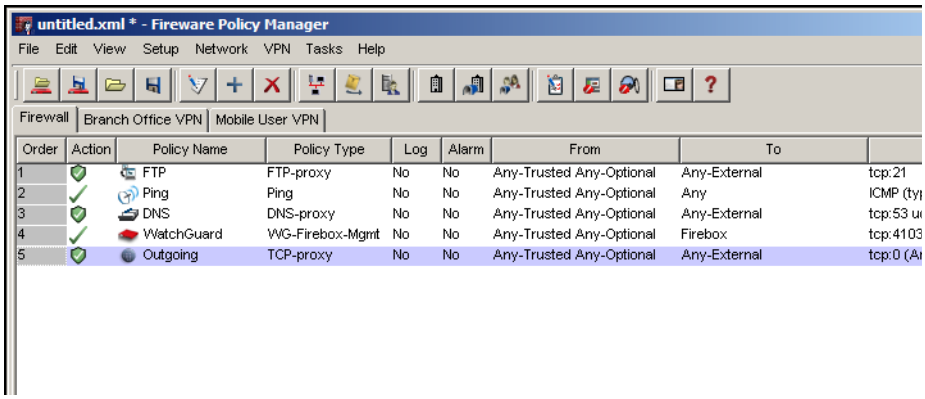
## 更改 Policy Manager （策略管理器）视图

Policy Manager （策略管理器）有两种视图：大图标和详细视图。大图标视图将每项策略显示为一个图标。如需更改大图标视图，在 **View （视图）**菜单中选择 **Large Icons （大图标）**。




大图标视图

如需改为详细视图，在 **View （视图）**菜单中选择 **Details （详细视图）**。在详细视图中，每项策略显示成一行信息，您可以查看配置信息，包括源头和目的地、日志和通知参数。



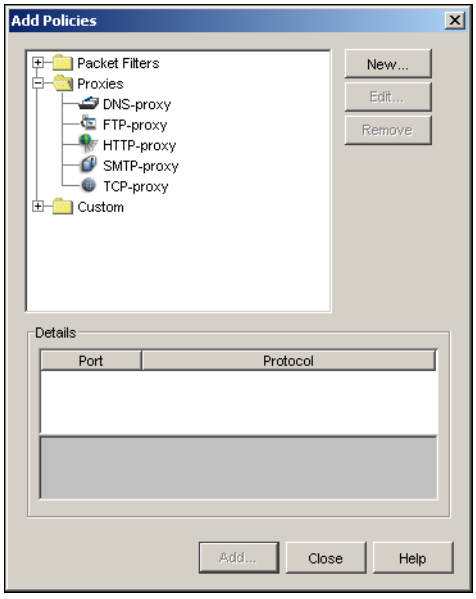

详细视图

## 添加策略

可使用 Policy Manager （策略管理器）将数据包过滤器或代理服务器添加至配置中。如需添加策略：

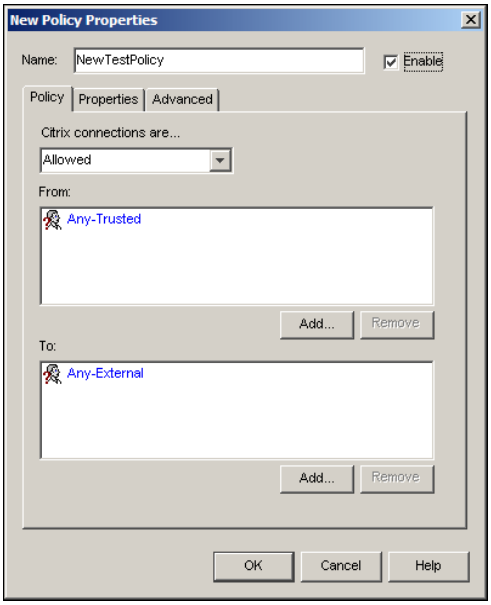
1 在 Policy Manager （策略管理器）中，点击 Policy Manager （策略管理器）工具栏上的加号（+）。
也可以选择 Edit （编辑）>Add Policies （添加策略），然后弹出 Add Policies （添加策略）对话框。

2 点击文件夹左侧的加号（+），打开 **Packet Filter （数据包过滤器）**或 **Proxies （代理服务器）**文件夹。
显示数据包过滤器或代理服务器列表。




3 点击策略名称进行添加。
选择一项策略后，策略图标将显示在 New （新建）、 Edit （编辑）和 Remove （删除）按钮下。此外，Details（详细视图）将显示策略的基本信息。

4 点击 **Add（添加）**。
将显示 New Policy Properties（新建策略属性）对话框。




5 可以在此修改策略名称，此信息将显示在 Policy Manager（策略管理器）详细视图中。如需修改名称，请在 **Name（名称）**文本框中输入新名称。

6 点击 **OK（确认）**关闭 **Properties（属性）**对话框。
策略对话框打开状态下可添加多项策略。

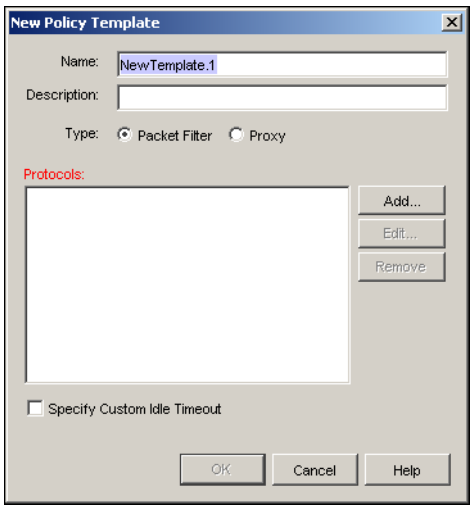
7 点击 **Close（关闭）**。
新建策略将显示在 Policy Manager（策略管理器）中。现在您可以按照第 150 页的 “配置策略属性”设置策略属性。

## 创建自定义策略模板

Policy Manager（策略管理器）包括多个数据包过滤器策略模板。您也可以创建自定义策略模板。模板包括只对应一种网络流量的端口和协议。如果想在防火墙后添加新的软件应用程序，就有必要创建自定义策略模板。

1 在 Policy Manager（策略管理器）中，点击 Policy Manager（策略管理器）工具栏上的加号（+）。
还可以选择 Edit（编辑）>Add Policies（添加策略），然后弹出 Add Policies（添加策略）对话框。

2 点击 **New （新建）**。
弹出 New Policy Template （新建策略模板）对话框。

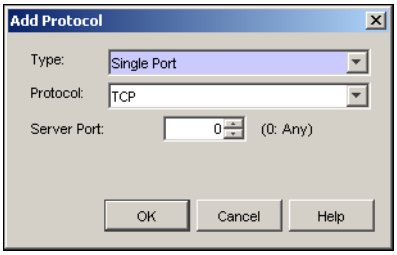



3 在 **Name （名称）**文本框中，输入策略模板名称。
该名称不能与 Add Policy( 添加策略 ) 对话框列表中的任何名称相同。该名称作为策略类型显示在 Policy Manager （策略管理器）中。如果您想更改或删除某个策略，该名称有助于您查找策略。

4 在 **Description （描述）**文本框中输入策略的描述信息。
点击 User Filters( 用户过滤器 ) 列表中的策略名称时，该信息将显示在 Details （详细情况）一栏中。

5 选择策略类型：**Packet Filter （数据包过滤器）**或 **Proxy （代理服务器）**。
代理服务器有如下几个选项：
- DNS
- FTP
- HTTP
- TCP
- SMTP

6 如需为本策略添加协议，点击 **Add （添加）**。
弹出 Add Protocol （添加协议）对话框。




7 在 **Type （类型）**下拉列表中选择 **Single Port （单个端口）**或 **Port Range （端口范围）**。

8 在 **Protocol （协议）**下拉列表中为新建策略选择协议。有关网络协议的详细信息，请参阅参考指南或在线帮助系统。如果选择了 **Single Port （单个端口）**，可选择：
- TCP
- UDP
- GRE
- AH

- ESP
- ICMP
- IGMP
- OSPF
- IP
- Any

选中 **Port Range（端口范围）**后，可选择 **TCP 或 UDP**。

9 在 **Server Port（服务器端口）**下拉列表中为新建策略选择端口。如果选中 **Port Range（端口范围）**，则选择起始服务器端口和结束服务器端口。

10 点击 **OK（确认）**。
Policy Manager（策略管理器）将相关值添加入 New Policy Template（新建策略模板）对话框。请检查本策略的名称、信息和配置是否正确。如有必要，点击 Add（添加）为本策略配置更多端口。再次执行 Add Port（添加端口）操作，直到为本策略配置了所有端口。

11 点击 **OK（确认）**。
Add Policy（添加策略）对话框与新建策略一同显示在 Custom（自定义）文件夹中。

## 添加多项同类策略

如果安全策略允许，可以多次添加同类策略。例如，可以在网页访问上对大多数用户设限，但赋与管理层完全网页访问权。为执行本操作，须为外发流量创建具有不同属性的两种策略：

1 添加首项策略。

2 更改策略名称，在安全策略中创建功能并添加相关信息。
在本例中，可将首项策略命名为“restricted_web_access”。

3 点击 **OK（确认）**，弹出本策略的 **Properties（属性）**对话框。按照第 150 页的“*配置策略属性*”设置属性。

4 添加第二项策略。

5 点击 **OK（确认）**，弹出本策略的 **Properties（属性）**对话框。设置属性。

## 删除策略

随着安全策略的变化，有时必须删除一项或多项策略。如需删除一项策略，首先将其从 Policy Manager（策略管理器）中删除，然后将新配置保存至 Firebox。

1 在 Policy Manager（策略管理器）中，点击 **Policy（策略）**。

2 在 Policy Manager（策略管理器）中，点击 Policy Manager（策略管理器）工具栏上的 **X** 按钮。
还可以选择 Edit（编辑）>Delete Policy（删除策略）。

3 要求确认时，点击 **Yes（是）**。

4 将配置保存至 Firebox，并重新启动 Firebox。选择 **File（文件）> Save（保存）> To Firebox（至 Firebox）**输入配置密码短语。选择 **Save to Firebox（保存至 Firebox）**复选框。点击 **Save（保存）**。

# 配置策略属性

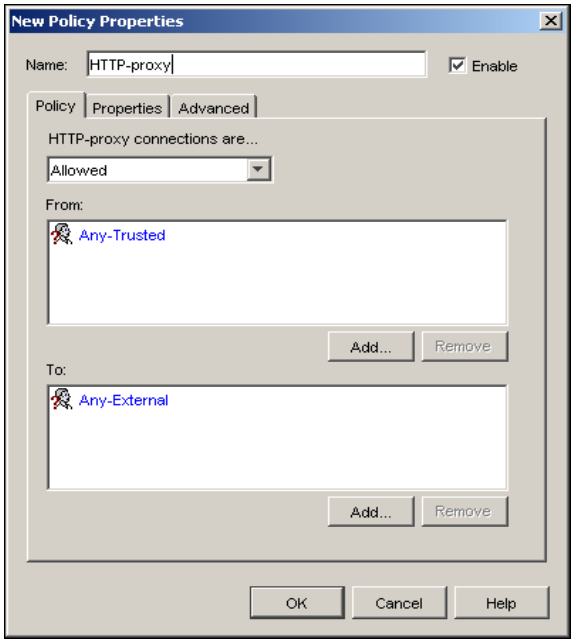
如果添加了一项策略后，想改变其属性，双击策略图标，打开 **Edit Policy Properties （编辑策略属性）**对话框。

## 设置访问规则、源头和目的地

可使用 **Policy （策略）**选项卡为特定策略设置访问规则。

**Policy （策略）**选项卡显示：

- 是否允许或拒绝使用本策略的流量。
- 谁使用本策略通过 Firebox® 与可达到的用户、主机和网络开始连接。
- 本策略流量的目的地。




在 **From （从）**列表中，添加能使用本策略发送（或不能发送）网络流量的计算机和网络；在 **To （至）**列表中，如果 Firebox 路由的流量符合策略规格，则添加 Firebox 路由该流量的计算机和网络。例如，您可以设置一个 ping 数据包过滤器，允许外部网络中所有计算机的 ping 流量到达可选网络的网页服务器。有关别名（显示为 From （从）和 To （至）列表选项）的详细信息，请参见第 73 页中的 “*使用别名*”。

您可以使用这些设置以配置流量的处理方式：

*允许*

如果流量符合在策略中设置的规则，则 Firebox 允许该流量。

*拒绝*

Firebox 拒绝所有符合本策略的流量。当计算机试图使用本策略时，您可以将其设置为记录一条日志消息。它还可以自动添加试图将本策略与封禁站点列表（**Properties （属性）**选项卡中配置）开始连接的计算机或网络。

*拒绝（发送重设）*

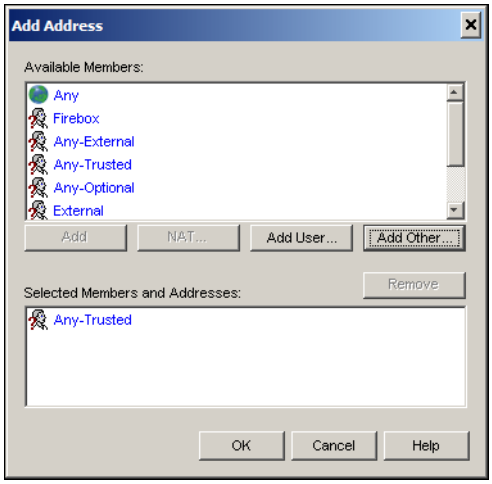
Firebox 拒绝所有符合本策略的流量。它还可以自动添加试图将本策略与封禁站点列表（**Properties（属性）**选项卡中配置）开始连接的计算机或网络。此外， Firebox 还将发送重设（RST）数据包，通知客户会话被拒绝和关闭。

1 在 **Policy（策略）**选项卡中，配置是否允许、拒绝或拒绝（发送重设）连接。

2 如需为策略添加成员，为 **From（从）**或 **To（至）**成员列表点击 **Add（添加）**。

3 使用 **Add Address（添加地址）**对话框为策略添加网络、 IP 地址或特定用户。点击 **Add User（添加用户）**或 **Add Other（添加其它）**。

还可以在 Available Member（可用成员）窗口中选择一个项目，点击 **Add（添加）**或双击该窗口中的项目。 Available Member（可用成员）列表包括您添加的别名和 Policy Manager（策略管理器）预设的别名。




4 如果选中 **Add Other（添加其它）**，则在 **Choose Type（选择类型）**下拉列表中选择主机范围、主机 IP 地址或网络 IP 地址进行添加。在 **Value（值）**文本框中，输入正确的网络地址、范围或 IP 地址。点击 **OK（确认）**。

成员或地址显示在 Selected Members and Addresses（所选成员和地址）列表中。

5 如果选中 **Add User（添加用户）**，则选择用户或群组类型、验证服务器及是否要添加用户或群组。

再次执行本操作以添加其他成员和地址。策略在 **From（从）**或 **To（至）**字段中可有多个对象。

6 点击 **OK（确认）**。

## 设置代理服务器操作

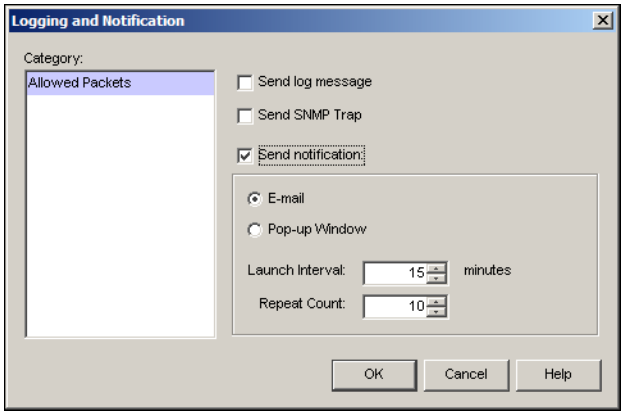
如需创建代理策略，可使用 **Policy Properties（策略属性）**对话框中的 **Properties（属性）**选项卡设置代理服务器操作。详情请参阅 “*配置代理策略*”一章。

如果创建了数据包过滤器策略，该字段显示为灰色（即不可用）。

## 设置日志属性

使用 **Policy Properties （策略属性）**对话框中的 **Properties （属性）**选项卡为策略设置日志属性。可将 Firebox 配置为当策略拒绝数据包时记录一条日志消息，也可以在允许或拒绝数据包时设置通知。

1 在 **Properties （属性）**选项卡中，点击 **Logging （日志）**。
弹出 Logging and Notification （日志和通知）对话框。




2 设置参数和通知：

*Enter it in the log （在日志中输入）*

选择此复选框后，如果 Firebox 发现 **Category （类型）**列表中所选类型的流量，将发出一条日志消息。 Firebox 上的域名解析能延缓 Firebox 将日志消息发送至日志文件的时间。所有策略的默认设置旨在让 Firebox 在拒绝数据包时发送日志消息。

*Send SNMP 陷阱 （发送 SNMP 陷阱）*

选择此复选框后， Firebox 将向 SNMP 管理系统发送事件通知。该 Trap 识别条件的发生，例如超过预设值的阈值。

*Send notification （发送通知）*

选择此复选框后，如果 Firebox 发现 **Category （类型）**列表中所选类型的流量，将发出通知。在日志服务器设置通知参数。有关日志服务器的详细信息，请参阅 “日志和通知” 一章。

*可配置 Firebox 完成下列操作之一：*

– **E-mail （电子邮件）**事件发生时， Firebox 发送一封电子邮件。在日志服务器用户界面的 **Notification （通知）**选项卡中设置电子邮件地址。

– **Pop-up Window （弹出窗口）**事件发生时， Firebox 将在管理工作站上弹出一个对话框。您可以控制通知时间及重复次数。有关于如何使用 Launch Interval and Repeat Count （发送间隔和重复次数）设置的详细信息，请参阅后续章节。

### 设置发送间隔和重复次数

您可以通过下列参数控制通知时间及重复次数：

*Launch Interval （发送间隔）*

指不同通知之间相隔的最短时间 （以分钟计算）。本参数防止在短时间内为同一事件发送多个通知。

*Repeat count （重复次数）*

计算事件发生的频率。当达到所选值时，一个特殊的重复事件通知器将开始启用。该通知器对特定的通知进行反复的日志输入。达到事件数量后，通知再次开始。

下面举例说明如何使用这两个值。数值设置为：

- 发送间隔 = 5 分钟
- 重复次数 = 4

端口空间探测从早上 10 点开始，并一直继续。这样即启动了日志和通知机制。下面是时间和发生的事件：

1 10:00 – 初始端口空间探测（首次事件）

2 10:01 – 首次通知开始（一个事件）

3 10:06 – 第二次通知开始（报告五个事件）

4 10:11 – 第三次通知开始（报告五个事件）

5 10:16 – 第四次通知开始（报告五个事件）

发送间隔控制了事件 1、2、3、4、5 之间的时间间隔。时间间隔设置为 5 分钟。将重复次数与发送间隔相乘，即为事件必须继续以启动重复通知器的时间间隔。

如果配置的策略是代理服务器，则 **Proxy（代理服务器）**下拉列表将同 View/Edit Proxy（查看 / 编辑代理服务器）和 Clone Proxy（复制代理服务器）图标一起显示。有关如何使用这些选项的详细信息，请参阅本指南中的 “*配置代理策略*”一章。

**注释**

一项策略可分别管理允许的流量或拒绝的流量，但不会同时管理这两种流量。如果想要 Firebox 为允许和拒绝的流量发送日志消息，必须为每种流量使用不同的策略。

## 配置静态 NAT

静态 NAT 也称为端口转发，是端口对主机的 NAT。主机从外部网络发送数据包至特定的公共地址和端口。静态 NAT 将该地址更改为防火墙后的地址和端口。有关 NAT 的详细信息，请参阅本指南中 “*使用防火墙 NAT*”一章。

由于静态 NAT 的运行方式，因此仅有使用特定端口（包括 TCP 和 UDP）的策略才可利用它。使用不同协议的策略不能使用流入的静态 NAT。该策略 **Properties（属性）**对话框中的 **NAT** 按钮不能使用， Any 策略也不能使用静态 NAT。

为防止垃圾邮件，许多接收电子邮件的服务器对邮件的源 IP 地址进行反向查看。接收服务器执行此操作以确保发送服务器（发送邮件的服务器）为该域名获授权的邮件服务器。因此，建议使用 Firebox 的外部 IP 地址作为域名的 MX 记录。MX（Mail exchange）记录是一种设置让电子邮件如何通过互联网的 DNS 记录。 MX 记录显示接收电子邮件的服务器，以及按优先顺序首先接收邮件的服务器。

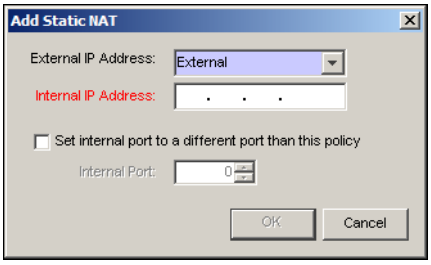
通常，始于受信或可选网络并到达互联网的连接显示 Firebox 的外部 IP 地址，作为数据包源 IP 地址。如果 Firebox 外部 IP 地址不是域名的 MX 记录 IP 地址，一些远程服务器将拒绝您发送的电子邮件。之所以如此，是因为 SMTP 会话并不显示您的 MX DNS 记录作为连接的源 IP 地址。如果 Firebox 不使用 MX 记录的 IP 地址作为外部接口 IP 地址，您可以使用一对一 NAT 映射，使外发电子邮件连接显示出正确的源 IP 地址。有关一对一 NAT 的详细信息，请参阅 “*使用防火墙 NAT*”一章。

1 双击 Policy Manager（策略管理器）中的策略图标。

2 在 **Connections are（连接为）**下拉列表中选择 **Allowed（允许）**。
如需使用静态 NAT，策略必须允许流入的流量通过。

3 在 **To（至）**列表下，点击 **Add（添加）**。
弹出 Add Address（添加地址）对话框。

4 点击 **NAT**。
弹出 Add Static NAT（添加静态 NAT）对话框。




5 在 **External IP Address（外部 IP 地址）**下拉列表中，选择本策略要使用的 “公共”地址。

6 输入内部 IP 地址。
内部 IP 地址是受信网络中的目的地址。

7 如有必要，选择 **Set internal port to different port than service（设置内部端口为服务以外的不同端口）**复选框。
一般情况下无需使用本功能。它不仅能将数据包目的地更改至特定的内部主机，而且可将其更改至一个不同的端口。如果选择此复选框，则输入不同的端口号或使用 Internal Port（内部端口）框中的箭头键。

8 点击 **OK（确认）**关闭 **Add Static NAT（添加静态 NAT）**对话框。
Members and Addresses（成员和地址）列表中将显示静态 NAT 路由。

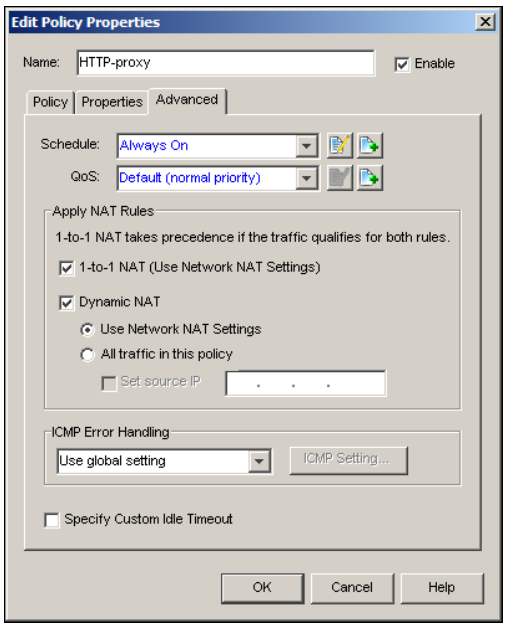
9 点击 **OK（确认）**关闭 **Add Address（添加地址）**对话框；点击 **OK（确认）**关闭策略的 **Properties（属性）**对话框。

**注释**

一些公司拥有多个使用相同协议（如两台 SMTP 服务器）的服务器，并希望每台服务器都使用静态 NAT。如果您的 Firebox 配置为路由模式，并有中设置的且有多个公共 IP 地址可分配给 Firebox，则可以实现此目标。在 Policy Manager（策略管理器）中设置两项策略：第一项策略在 Firebox的主外部IP地址与您的第一个服务器之间设置静态NAT；第二项策略在Firebox外部接口的第二 IP 地址与您的第二个服务器之间设置静态 NAT。

## 设置高级属性

可使用 **Edit Policy Properties**（**编辑策略属性**）对话框中的 **Advanced**（**高级**）选项卡设置策略计划表，执行服务质量（QoS）设置，应用 NAT 规则，为本策略配置 ICMP 错误处理，并设置自定义空闲超时。




### 设置计划表

可以为策略设置操作计划表。可使用 **Schedule**（**计划表**）下拉列表中的计划表模板或创建自定义计划表。相关信息请参阅本指南中 “*基本配置设置*” 一章。

注意：这些计划表可供多项策略共享。

### 应用服务质量（QoS）操作

如果 Firebox 上安装了 Fireware® Pro，您可以为策略分配一项服务质量操作。使用最右边的按钮创建一项新的 QoS 操作。创建新的 QoS 操作后，该操作将显示在 **QoS** 下拉列表中。详细信息请参阅第 209 页的 “*创建 QoS 操作*”。

注意：这些操作可供多项策略共享

### 应用 NAT 规则

可将网络地址转换（NAT）规则应用于策略：

*一对一 NAT*

应用此类 NAT，Firebox 将使用设定的专用和公共 IP 范围，请参阅第 105 页的 “*使用一对一 NAT*”。

*动态 NAT*

应用此类 NAT， Firebox 将专用 IP 地址映射至公共 IP 地址。如果要使用为 Firebox 设置的动态 NAT 规则，则选择 **Use Network NAT Settings**（**使用网络 NAT 设置**）；如果要将

NAT 应用至本策略中的所有流量，则选择 **All traffic in this policy（本策略中的所有流量）**。还可以选择为使用动态 NAT 的任何策略设置一个动态 NAT 源 IP 地址。

这样能确保使用本策略的任何流量显示公共或外部 IP 地址范围中的一个特定地址作为源地址。当 Firebox 外部接口上的 IP 地址与 MX 记录 IP 地址不同时，您通常需要执行此操作以强制外发 SMTP 流量显示出域的 MX 记录地址。

一对一 NAT 规则比动态 NAT 规则具有更高的优先权。

**注释**

如果使用多广域网，则不能使用 **Set Source IP （设置源 IP）**选项。仅在 Firebox 使用单个外部接口时才能使用该选项。

### 设置 ICMP 错误处理

可以设置与策略相关的 ICMP 错误处理设置。

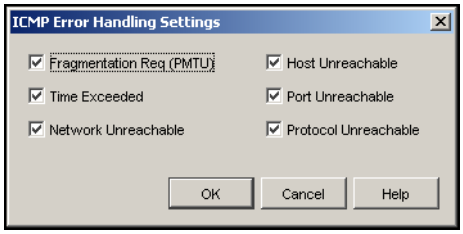
在下拉列表中选择：

*Use global setting （使用全局设置）*

使用为 Firebox 设定的全局 ICMP 错误处理设置。有关全局设置的详细信息，请参阅第 40 页的 “*ICMP 错误处理*”设置。

*Specify setting （指定设置）*

配置覆盖全局设置的参数。点击 **ICMP Setting （ICMP 设置）**。在 **ICMP Error Handling Settings （ICMP 错误处理设置）**对话框中，选择复选框配置单个设置。有关这些设置的详细信息，请参阅第 40 页的 “*ICMP 错误处理*”。




### 设置自定义空闲超时

如需设置空闲超时，点击 **Specify Custom Idle Timeout （指定自定义空闲超时）**，再点击箭头设置超时前的秒数。此设置将覆盖策略的空闲超时。

## 设置策略优先权

优先权是 Firebox® 检查网络流量和应用策略规则的顺序。 Firebox 按路由发送为首项策略 （与流量匹配）使用规则的流量。 Fireware® Policy Manager （策略管理器）按最详细至最普通的顺序自动为策略排序。也可以手动设置优先权。

## 使用自动顺序

Fireware Policy Manager（策略管理器）按最详细至最普通的顺序自动为策略排序。每添加一项策略后， Policy Manager（策略管理器）将新规则与配置文件中的所有规则进行比较。 Policy Manager（策略管理器）使用以下标准设置优先权：

1 为策略类型设置的协议
2 **To**（至）字段的流量规则
3 **From**（从）字段的流量规则
4 防火墙操作
5 计划表
6 基于策略类型的字母数字顺序
7 基于策略名称的字母数字顺序

### 比较策略类型

Policy Manager（策略管理器）使用这些标准依次比较两种策略，直到发现策略相同或其中一项策略比另一项更详细：

1 Any 策略的优先权通常最低。有关 Any 策略的详细信息，请参阅第 233 页的“*Any（任何）*”一节。
2 检查 TCP0（任何）或 UDP0（任何）协议的数量。数字较小的策略享有较高的优先权。
3 检查 TCP 和 UDP 协议唯一端口的数量。数字较小的策略享有较高的优先权。
4 计算 TCP 和 UDP 协议唯一端口的数量。数字较小的策略享有较高的优先权。
5 根据 IP 协议值给协议计分。分数较少的策略享有较高的优先权。

如果 Policy Manager（策略管理器）在比较策略类型时不能设置优先权，将检查流量规则。

### 比较流量规则

Policy Manager（策略管理器）使用这些标准依次将一项策略最普通的流量规则与第二项策略最普通的流量规则进行比较。它将更高的优先权分配给流量规则最详细的策略。从最详细到最普通的流量规则列表如下：

1 主机地址
2 IP 地址范围（小于相比较的子网）
3 子网
4 IP 地址范围（大于相比较的子网）
5 验证用户
6 验证群组
7 接口， Firebox
8 任何 – 外部的、任何 – 受信的、任何 – 可选的
9 任何

例如，比较如下两项策略：
HTTP-1
源自：受信的，用户 1
HTTP-2

源自：10.0.0.1，任何 – 受信的

“受信的”是 HTTP – 1 最普通的条目。“任何 – 受信的”是 HTTP – 2 最普通的条目。由于 “受信的”在 “任何 – 受信的”范围内。HTTP – 1 是更详细的流量规则。尽管 HTTP – 2 包括一个 IP 地址，这仍是正确的，因为 Policy Manager（策略管理器）依次使用这些标准将一项策略最普通的流量规则与第二项策略最普通的流量规则进行比较。如果 Policy Manager（策略管理器）在比较流量规则时不能设置优先权，将检查防火墙操作。

### 比较防火墙操作

Policy Manager（策略管理器）通过比较两项策略的防火墙操作来设置优先权。防火墙操作的优先权从高到低的顺序为：

1 拒绝或拒绝（发送重设）

2 允许的代理服务器

3 允许的过滤器

如果策略服务器在比较防火墙操作时不能设置优先权，将检查计划表。

### 比较计划表

Policy Manager（策略管理器）通过比较两项策略的计划表来设置优先权。计划表的优先权从高到低的顺序为：

1 始终关闭

2 有时打开

3 始终打开

如果 Policy Manager（策略管理器）在比较列表时不能设置优先权，则检查策略名称。

### 比较类型和名称

如果两项策略与任何其它优先权标准不匹配，则 Policy Manager（策略管理器）按字母数字顺序为策略排序。首先使用策略类型，然后使用策略名称。由于没有两项策略的类型和名称均相同，因此这是优先权的最后标准。

## 手动设置优先权

要切换至手动顺序模式，选择 **View（查看）>Auto-order mode（自动顺序模式）**，勾选符将消失，系统提示您确认是否切换至自动顺序模式。

要修改策略的顺序：

- 选择要修改顺序的策略。点击 Policy Manager（策略管理器）工具栏上较右边的 “向上”或“向下”箭头。

或

- 选择要修改顺序的策略并将其拖至新位置。

# 第 13 章　设置代理策略

代理服务器过滤器比数据包过滤器的功能强大得多。代理服务器检查数据包的内容，而不仅仅检查数据包报头。因此，代理服务器能找到隐藏或嵌入在数据净荷中的受禁内容。例如， SMTP 代理服务器检查所有流入的 SMTP 数据包（ 电子邮件 ）是否含有受禁内容，比如以脚本语言编写的可执行程序或文件。黑客频繁地使用这些方法发送计算机病毒。 SMTP 代理服务器知道这些内容类型是不允许的，而数据包过滤器不能检测到数据包数据净荷中未经许可的内容。

WatchGuard® 代理服务器还检测应用程序协议的异常，并阻止错误形成的数据包。如果 SMTP 数据包创建不正确或包含预料之外的内容，则不能通过 Firebox®。

代理服务器策略在应用程序、网络和传输协议层运行，而数据包过滤器策略仅在网络及传输协议层运行。换言之，代理服务器获得一个数据包后，即删除网络层并检查其净荷，然后将网络信息放回至数据包上，再将信息发送至受信和可选网络中的目的地。这样，同样的网络流量给防火墙增加了更多的工作量。但代理服务器使用数据包过滤器不能采用的方法可捕捉到危险的数据包。

## 定义规则

规则集是基于代理服务器一项功能的一组规则。配置代理服务器时，可以在 **Categories （ 类别 ）** 列表中看到该代理服务器的规则集。在代理服务器配置窗口的 **Properties （ 属性 ）** 选项卡中修改代理服务器操作后，您看到的规则集就随之变化。

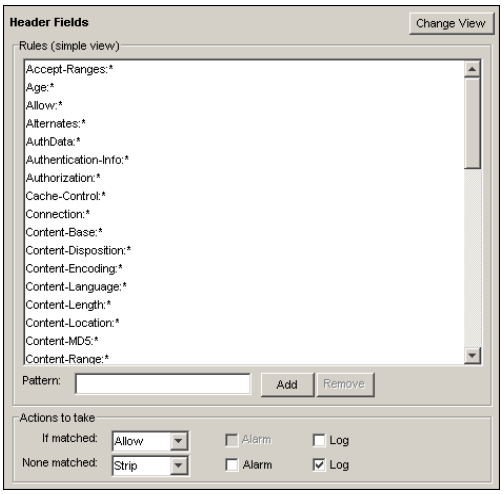
一台代理服务器可对应多个代理服务器操作。例如，您可以对发送至 Firebox® 保护的电子邮件服务器的数据包使用一个规则集，而对正通过 Firebox 发送到互联网的电子邮件使用另一规则集。可以使用现有的代理服务器操作，或复制一个现有的代理服务器操作，将其修改为一个新的代理服务器操作。

如果数据包的内容与一条规则匹配，则该规则包括一种内容、模式或表达式以及 Firebox 执行的操作。当 Firebox 发送告警或它向日志文件发送事件时，规则还包括设置。

对于大多数代理服务器功能而言， Firebox 有一个预装的规则集。但可以编辑规则集中的规则，修改规则的操作，也可以添加自己的规则。

这些规则定义所使用的字段在每类规则集中均相同。下面是一个简单的视图。也可以选择 **Change View （ 更改视图 ）** 以查看高级视图。

使用高级视图提高代理服务器的匹配功能。在高级视图中，可以配置精确匹配和 Perl 兼容正则表达式。在简单视图中，可以配置与简单正则表达式匹配的通配符模式。




## 添加规则集

在简单视图下，执行以下操作以添加新规则：

1 在 **Pattern （ 模式 ）**文本框中输入使用简单正则表达式语法的模式。
0 或多个字符的通配符是 “*”。
一个字符的通配符是 “?”。

2 点击 **Add （ 添加 ）**。
新建规则显示在 Rules （ 规则 ）框中。

3 在 **Actions to take （ 要执行的操作 ）**选项中，如果数据包的内容与列表中的一项规则相匹配，**If matched （ 若匹配 ）**下拉列表将设置要进行的操作。如果数据包的内容与列表中的任何规则均不匹配， **None matched （ 不匹配 ）**下拉里表将设置要进行的操作。下面列出了所有可能执行的操作。 **Strip （ 删除 ）和 Lock （ 锁定 ）**操作仅适用于基于特征的入侵防护操作。

*Allow （ 允许 ）*
允许连接。

*Deny （ 拒绝 ）*
拒绝特定请求，但在可能的情况下保持连接。

*Drop （ 中断 ）*
拒绝特定请求并中断连接。

*Block （ 禁止 ）*
拒绝请求，中断连接，并将源主机添加至受禁站点列表中。有关受禁站点的详细信息，请参阅第 135 页的 “*设置受禁站点*”一节。

*Strip （ 删除 ）*
删除并丢弃数据包中的附件。数据包的其它部分则通过 Firebox 发送至其目的地。

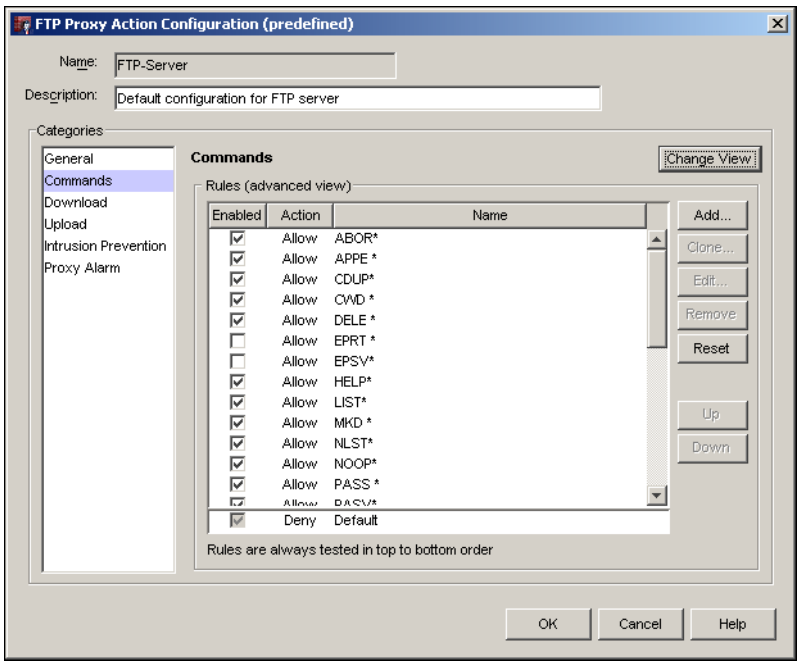
*Lock （ 锁定 ）*
锁定并包起附件，使用户不能打开，只有管理员可打开此文件。

4 告警是一种机制，在一条代理服务器规则适用于网络流量时，将提醒用户。使用 **Alarm （告警）**复选框为本事件配置告警。要设置告警选项，在代理服务器配置窗口左侧的 Categories （**类别**）列表中选择 **Proxy Alarm （代理服务器告警）**。您可以发送 SNMP 陷阱和电子邮件，或打开一个弹出窗口。

5 使用 **Log （日志）**复选框为本事件编写流量日志。

## 使用高级规则视图

如需查看当前规则的详细视图，点击 **Change View （更改视图）**。高级视图显示每条规则的操作，还包括可用于编辑、复制（使用现有的规则定义创建新规则）、删除或重设的按钮。要返回简单视图，再次点击 **Change View （更改视图）**即可。如果启用的规则有不同的操作、告警和日志设置，则不能返回简单视图。在此情况下，您必须继续使用高级视图。




### 更改规则的优先权

Firebox 应用规则时遵循以下原则：

- 从窗口的顶部至底部依次执行规则。
- 当过滤项目与规则匹配时， Firebox 即进行相关流量操作。
- 内容可与多条规则或默认规则匹配，但仅使用第一条规则。
- 如果无其它规则适用， Firebox 就使用默认规则。 Firebox 始终将最后一条规则应用于内容。

要更改规则的顺序，必须使用高级视图：

1 点击 **Change View （更改视图）**，查看所创建规则的高级视图。

2 选择一条规则，在列表中上下移动。点击 **Up （向上）或 Down （向下）**按钮，将此规则在列表中上移或下移。

# 为代理服务器规则自定义日志和通知

告警、日志消息或通知是一种机制，网络管理员通过这种机制可知悉与允许流量标准不匹配的网络流量。例如，如果流量大于阈值，您可以将 Firebox® 配置为向您发送一封电子邮件。您可以为每个数据包过滤器和代理服务器策略设置告警、日志消息和通知属性，还可以为代理服务器规则设置告警和日志消息属性。

## 为代理服务器策略配置日志消息和通知

1 双击策略图标，打开 **Policy Properties**（**策略属性**）对话框。

2 点击 **Properties**（**属性**）选项卡，然后点击 **Logging**（**日志**）。
弹出 Logging and Notification（日志和通知）对话框。

3 设置符合安全策略要求的参数。

## 为代理服务器规则配置日志消息和告警

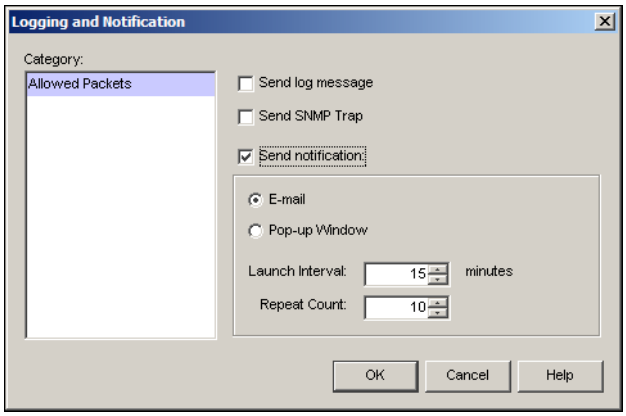
1 双击策略图标，打开 **Policy Properties**（**策略属性**）对话框。

2 点击 **Properties**（**属性**）选项卡。从 **Proxy**（**代理服务器**）下拉列表中选择要配置的代理服务器操作。

3 从 **Categories**（**类别**）列表中选择 **Proxy Alarms**（**代理服务器告警**）。有关参数的详细信息，请参阅后续章节。
还有更多日志消息和通知选项提供基于特征的入侵防护服务。
这些选项详见 “使用基于特征的安全服务”一章。

## 使用告警、日志消息和通知对话框

代理服务器定义中的告警、日志消息和通知对话框具有大多数或所有如下字段：




*Enter it in the log（在日志中输入）*

选择此复选框后，如果事件发生， Firebox 将发送一条流量日志消息至日志服务器。所有策略的默认设置使 Firebox 在拒绝数据包时发送一条日志消息。

*Send SNMP Trap （发送 SNMP 陷阱）*

选择此复选框后， Firebox 将向 SNMP 管理系统发送事件通知。如果流量与一项条件匹配（比如超出其阈值的属性），将显示 SNMP trap。 SNMP 开始或停止（比如重设、重启或出现故障）时，如果 trap 发生了，则 SNMP trap 中的绑定部分为空白。

*Send notification （发送通知）*

选择此复选框后，如果事件发生，日志服务器将发送通知。您可以将日志服务器配置为执行下列任一操作：

- **E-mail（电子邮件）**事件发生时，日志服务器发送一封电子邮件。在日志服务器用户界面中的 **Notification（通知）**选项卡中设置电子邮件地址。
- **Pop-up Window （弹出窗口）**事件发生时，日志服务器将在管理工作站上弹出一个对话框。

### 设置发送间隔和重复次数

您可以控制通知时间及重复次数，如下所示：

*Launch Interval （发送间隔）*

指不同通知之间相隔的最短时间（以分钟计算）。此参数防止在短时间内为同一事件发送多个通知。

*Repeat Count （重复次数）*

计算事件发生的频率。当达到所选值时，将启用特殊的重复事件通知器。该事件通知器对特定的通知进行反复的日志输入。达到事件数量后，通知再次开始。

下面举例说明如何使用这两个值，数值设为：

- 发送间隔 = 5 分钟
- 重复次数 = 4

端口空间探测从早上 10 点开始运行，并一直持续。这样即启动了日志和通知机制。下面是时间和发生的事件：

1 10:00— 初始端口空间探测（首次事件）

2 10:01— 首次通知开始（一个事件）

3 10:06— 第二次通知开始（报告五个事件）

4 10:11— 第三次通知开始（报告五个事件）

5 10:16— 第四次通知开始（报告五个事件）

发送间隔控制了事件 1、 2、 3、 4、 5 之间的时间间隔。时间间隔设置为 5 分钟。将重复次数与发送间隔相乘，即为事件必须继续以启动重复通知器的时间间隔。

## 配置 SMTP 代理服务器

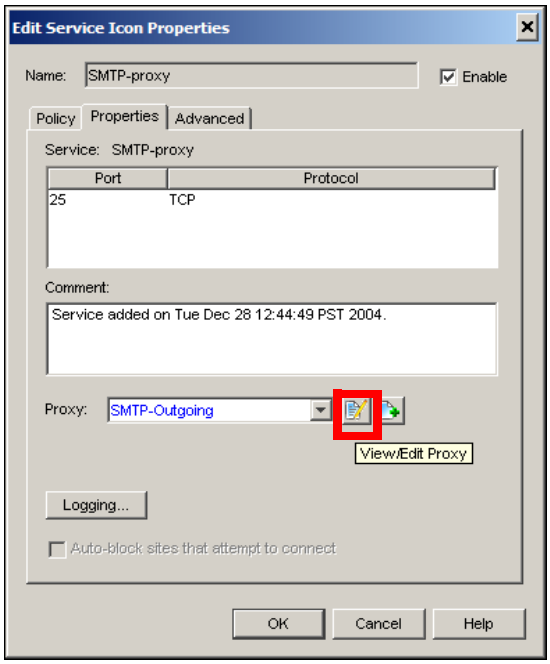
使用 SMTP 代理服务器控制电子邮件及其内容。代理服务器扫描 SMTP 信息的大量过滤参数，并将其与代理服务器配置中设定的规则进行比较。要配置 SMTP 代理服务器：

1 添加 SMTP 代理服务器至 Policy Manager（策略管理器）中。如需了解如何将策略添加至 Policy Manager （策略管理器）中，请参阅第 66 页的 “添加策略” 一节。

2 双击 SMTP 图标，选择 **Properties （属性）**选项卡。
弹出 Edit Policy Properties （编辑策略属性）对话框，并显示出关于 General Settings （一般设置）信息。

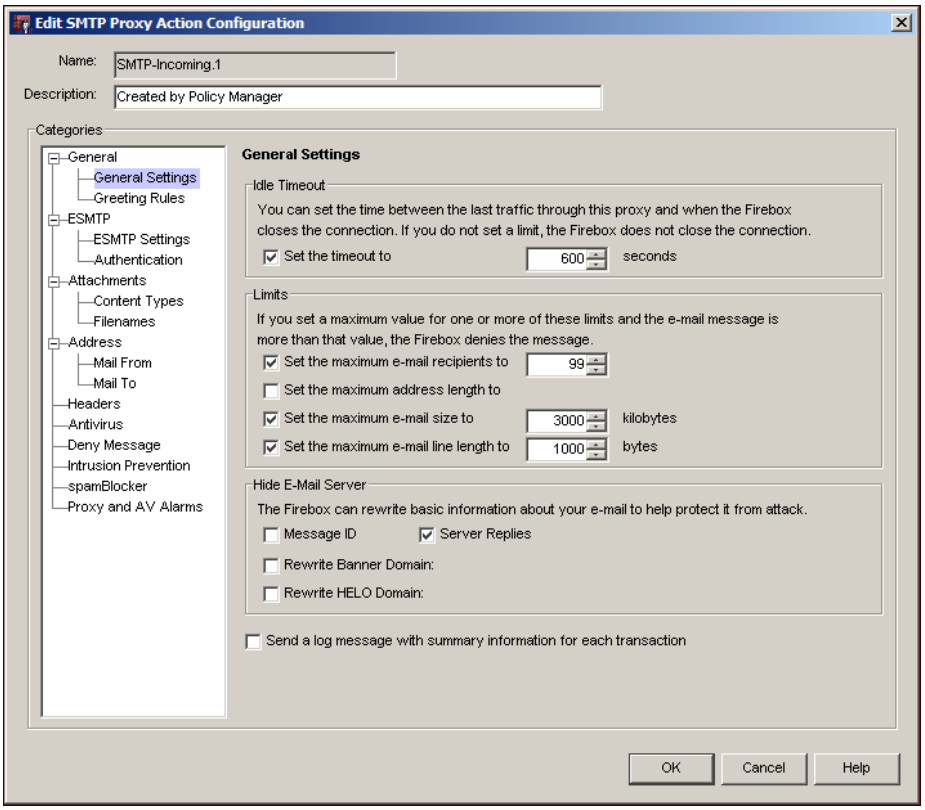
3 在 **Proxy**（**代理服务器**）下列列表中，选择配置接收的 SMTP 或外发的 SMTP。
也可以复制一项代理服务器操作以创建新的代理服务器操作。

4 点击 **View/Edit Proxy**（**查看 / 编辑代理服务器**）图标。



## 配置一般设置

使用 **General Settings （一般设置）**字段配置基本 SMTP 代理服务器参数，比如空闲超时和消息限制。




*Idle timeout （空闲超时）*

可以设置传入 SMTP 连接在未超时之前的空闲时间长度。默认值为 600 秒 （ 10 分钟 ）。如不需要超时设置，则取消对 **Set the timeout to （设置超时为）**复选框的选择。

*Maximum e-mail recipients （电子邮件收件人最大人数）*

**Set the maximum e-mail recipients to （设置电子邮件收件人最大人数为）**复选框可以设置发出的一封电子邮件最多的接收人数。 Firebox® 计数并允许特定数量的地址通过，然后禁止其它地址。例如，如果采用的默认值为 50，但有一条信息发向 52 个地址，那么前 50 个地址将收到这封电子邮件，而最后两个地址却不能收到此信息。一个分配列表作为一个 SMTP 电子邮件地址显示 （ 例如， support@watchguard.com ）。 Firebox 将它计为一个地址。

您可以使用本功能减少垃圾邮件，因为垃圾邮件通常包括庞大的收件人列表。进行此项设置时，请认真操作，因为该设置同时也可能会拒绝合法的电子邮件。

*Maximum address length （最大地址长度）*

**Set the maximum address length to （设置最大地址长度为）**复选框可以设置电子邮件地址的最大长度。

*Maximum e-mail size （最大电子邮件大小）*

**Set the maximum e-mail size to（设置最大电子邮件大小）**复选框可以设置接收 SMTP 消息的最大长度。大多数电子邮件以 7– 位 ASCII 文本长度发送。但 Binary MIME 和 8– 位 MIME

例外。 8– 位 MIME 的内容（例如， MIME 附件）以标准算法（Base64 或 QP 编码）进行编码，使它们可通过 7– 位电子邮件系统进行发送。编码可增加三分之一的文件长度。为允许 1000 字节大的信息，您必须将此字段设置为至少 1334 字节，以确保所有电子邮件都能通过。默认值为 3,000,000 字节（三百万字节）。

*Maximum e-mail line length（电子邮件行最大长度）*

**Set the maximum e-mail line length to（设置电子邮件行最大长度为）**复选框可以为 SMTP 消息行设置最大行长度。如果行长度过长，将会在一些电子邮件系统上导致缓存溢出。大多数电子邮件客户和系统发送较短的行长度，但一些基于网页的电子邮件系统则发送很长的行长度。默认值为 1024。

*Hide E-mail Server（隐藏电子邮件服务器）*

选择 **Message ID（信息 ID）**和 **Server Replies（服务器回复）**复选框，代替 MIME 边界及电子邮件消息中的问候字符串。黑客通过这些来识别 SMTP 服务器供应商和版本。

如果您有一个电子邮件服务器并使用传入 SMTP 的代理服务器操作，则可以使 SMTP 代理服务器以所选域名取代 SMTP 服务器横幅中显示的域。为进行该操作，选择 **Rewrite Banner Domain（重写横幅域）**复选框，并在弹出的文本框中输入横幅中要使用的域名。此外，还必须选择 **Server Replies（服务器回复）**复选框。

如果使用外发 SMTP 代理服务器操作，可让 SMTP 代理服务器取代 HELO 或 EHLO 问候中显示的域。当电子邮件服务器宣布自己为一台接收电子邮件的服务器时， HELO 或 EHLO 问候成为 SMTP 事务的第一部分。为执行此操作，选择 **Rewrite HELO Domain（重写 HELO 域）**复选框，并在弹出的文本框中输入在 HELO 或 EHLO 中想用的域。

*Send a log message（发送日志消息）*

选择 **Send a log message（发送日志消息）**复选框，通过 SMTP 为每个连接请求发送一条日志消息。如需 Historical Reports（历史报告）创建关于 SMTP 流量的精确报告，则必须选择此复选框。

*Greeting rules（问候语规则）*

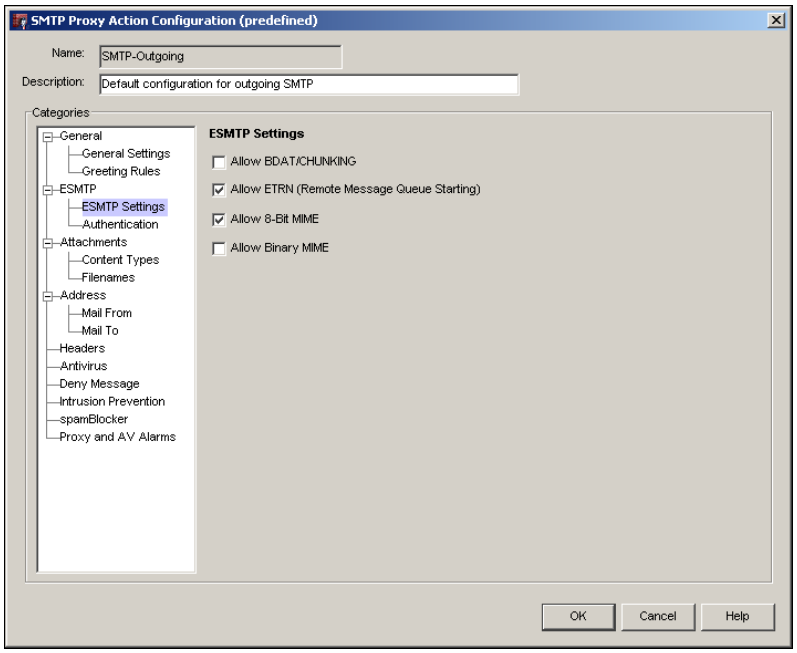
代理服务器在 SMTP 会话初始化期间检查初始 HELO/EHLO 响应。传入 SMTP 代理服务器操作的默认规则确保拒绝带有超长问候语、或包括错误或意料之外的字符的数据包。

## 配置 ESMTP 参数

使用 **ESMTP Setting（ESMTP 设置）**字段为 ESMTP 内容设置过滤功能。尽管 SMTP 被广为接受并应用，但一些互联网社区已发现有必要扩展 SMTP，使其具有更多功能。

ESMTP 提供了功能扩展至 SMTP 的方法，使支持扩展功能的客户端能相互认识。

1 在 **Categories**（类别）中选择 **ESMTP Setting（ESMTP 设置）**。




*Allow BDAT/CHUNKING（允许 BDAT/ CHUNKING）*

选择 Allow BDAT/CHUNKING（允许 BDAT/ CHUNKING）。这样，通过 SMTP 连接可轻松发送大型消息。

*Allow ETRN （远程消息队列启动）*

扩展至 SMPT，允许 SMPT 客户端及服务器交互作用，为特定主机启动消息队列交流。

*Allow 8-Bit MIME（允许 8– 位 MIME）*

如果客户端和主机支持扩展，则选择 Allow 8-Bit MIME（允许 8– 位 MIME）。8– 位 MIME 扩展允许客户端和主机交流由八位字节文本组成的消息。该八位字节不在使用 SMTP 的 US-ASCII 八位字节范围（十六进制 00-7F，或 7– 位 ASCII）内。

*Allow Binary MIME（允许二进制 MIME）*

如果发送器和接收器接受二进制 MIME，则选择允许二进制 MIME 扩展。二进制 MIME 防止被发送的二进制对象（使用有 SMTP 的消息格式） base64 和 QP 编码的开销。建议不要选择此选项，因为它有可能成为安全威胁。

## 配置验证规则

此规则集允许多种 ESMTP 验证类型。默认规则拒绝所有其它验证类型。说明 SMTP 验证扩展的 RFC 为 RFC 2554。

1 在 **Categories（类别）**栏中选择 **Authentication（身份验证）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

## 定义内容类型规则

使用传入 SMTP 代理服务器操作的规则集为传入 SMTP 内容过滤设置值。使用外发 SMTP 代理服务器操作的规则集为外发 SMTP 内容过滤设置值。

1 在 **Categories（类别）**栏中选择 **Content Types（内容类型）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

## 定义文件名规则

使用传入 SMTP 代理服务器操作的规则集对传入的电子邮件附件文件名设置限制。使用外发 SMTP 代理服务器操作的规则集为外发的电子邮件附件文件名设置限制。

1 在 **Categories（类别）**栏中选择 **Filenames（文件名）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

## 配置 Mail From（邮件发自）和 Mail To（邮件发至）规则

**Mail From（邮件发自）**规则集能对电子邮件设置限制，仅允许来自特定发件人的电子邮件进入您的网络。默认设置则允许来自所有发件人的电子邮件。

**Mail To（邮件发至）**规则集能对电子邮件设置限制，仅允许发至特定收件人的电子邮件发出网外。默认设置则允许将发至所有收件人的电子邮件发出网外。对于传入 SMTP 代理服务器操作，可用 Mail To（邮件发至）规则集防止他人使用您的电子邮件服务器传递电子邮件。为此，请确保电子邮件服务器接受电子邮件的所有域名显示在规则列表中。然后，如果 **None Matched（不匹配）**，确保将 **Action to Take（要执行的操作）**设置为 **Deny（拒绝）**。任何地址与所列的域名不匹配的电子邮件都将被拒绝。

还可以使用包含在此规则配置对话框中的 **Rewrite As（重写为）**功能要求 Firebox 将电子邮件地址的 From（发自）和 To（发至）组件修改为不同的值。本功能也称为 “SMTP 伪装”。

1 在 **Categories（类别）**栏中选择 **Mail From（邮件发自）**和 **Mail To（邮件发至）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “定义规则”。

## 定义报头规则

报头规则集允许您为传入或外发 SMTP 报头过滤设置值。

1 在 **Categories（类别）**栏中选择 **Header（报头）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

## 定义防病毒措施

如果在电子邮件中发现病毒，此对话框中的字段将设置必要的操作。另外，电子邮件包含超大附件或 Firebox 不能扫描的附件时，也可设置相应的操作。

尽管可使用代理服务器定义页面激活和配置 Gateway Antivirus（网关防病毒），但用 Policy Manager（策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行本操作或在代理服务器定义中使用防病毒页面，请参阅 “*使用基于特征的安全服务*”。

## 修改拒绝消息

Firebox 能发出代替被拒绝内容的默认拒绝消息。您可用自己写入的消息取代拒绝消息，还可以用标准 HTML 编写自定义拒绝消息。拒绝消息的首行是 HTTP 报头的一部分。首行和消息正文之间必须有一空行。

1 在 **Categories（类别）**栏中选择 **Deny Message（拒绝消息）**。

2 在拒绝消息框中输入拒绝消息。可以使用以下变量：

*%（原因）%*
输入 Firebox 拒绝内容的原因。

*%（类型）%*
输入被拒绝内容的类型。

*%（文件名）%*
输入被拒绝内容的文件名。

*%（病毒）%*
仅为 Gateway Antivirus（网关防病毒）用户输入病毒名称或状态。

*%（操作）%*
输入所执行操作的名称：锁定、删除等。

*%（恢复）%*
可以设置文本，直到出现如下句子：“您的网络管理员%（恢复）%了本附件”。

## 为 SMTP 配置 IPS（入侵防御系统）

黑客使用多种方法攻击互联网上的计算机。这些攻击的目的是破坏网络、获取敏感信息，或利用您的计算机攻击其它网络。因此，这些攻击被称为 Intrusions（入侵）。

尽管可使用代理服务器定义页面激活和配置 IPS，但用 Policy Manager（策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何执行此操作或在代理服务器中使用防病毒页面，请参阅 “*使用基于特征的安全服务*”。

## 配置 spamBlocker

不请自来的电子邮件，也称为垃圾邮件，会以惊人的速度塞满普通邮箱。大量的垃圾邮件减少带宽、降低员工工作效率并浪费网络资源。 WatchGuard® spamBlocker™ 选项可在垃圾邮件企图进入系统时，增强捕获网络边缘的垃圾邮件的能力。

尽管可使用代理服务器定义页面激活和配置 spamBlocker，但用 Policy Manager（策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行该操作或使用代理服务器定义中的 spamBlocker 页面，请参阅 “*使用 spamBlocker*”一章。

## 为 SMTP 配置代理服务器和防病毒告警

代理服务器或防病毒（AV）告警事件发生时，可设置 Firebox 的相关操作：

1 在 **Categories（类别）**栏中选择 **Proxy and AV Alarm（代理服务器和 AV 告警）**。

2 有关 **Proxy/AV Alarm Configuration（代理服务器 / 防病毒告警配置）**中字段的信息，请参阅第 164 页的 “*使用告警、日志消息和通知对话框*”。

# 配置 FTP 代理服务器

文件传输协议（FTP）是在互联网上传输文件的协议。就如 SMTP 和 HTTP 一样， FTP 使用 TCP/IP 协议进行数据传输。通常使用 FTP 从互联网上的服务器下载文件或将文件上传至服务器。

1 添加 FTP 至 Policy Manager（策略管理器）。如需了解如何将策略添加至 Policy Manager（策略管理器），请参阅第 66 页的 “*添加策略*”。

2 双击 FTP 图标，选择 **Policy（策略）**选项卡。

3 在 **FTP proxy connections are（FTP 代理服务器连接为）**下拉列表中选择 **Allowed（允许）**。

4 选择 **Properties（属性）**选项卡。

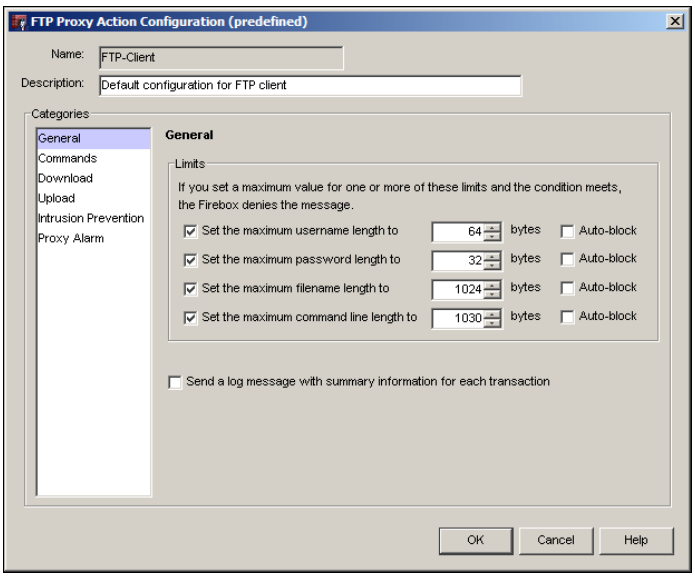
5 在 **Proxy（代理服务器）**下拉列表中，选择为 FTP– 客户端或 FTP– 服务器设置代理服务器操作。

6 点击 **View/Edit Proxy（查看 / 编辑代理服务器）**图标。

## 配置常规设置

用 **General（常规）**字段配置基本 FTP 参数（包括用户名最大长度）。

1 在 **Categories（类别）**栏中选择 **General（常规）**。




2 如需为 FTP 参数设置限制，则选择相应的复选框。这些设置有助于防止网络遭受缓存溢出攻击。如果将复选框设置为 0 字节，则 Firebox® 不会使用该参数。用箭头设置限制：

*Maximum user name length（用户名最大长度）*
为 FTP 网站上的用户名设置最大长度。

*Maximum password length（密码最大长度）*
为用于登录 FTP 网站的密码设置最大长度。

*Maximum file name length（文件名最大长度）*
为上传或下载的文件设置文件名最大长度。

*Maximum command line length（命令行最大长度）*
为用于 FTP 网站上的命令行设置最大长度。

3 对于每项设置，您可以设置或清除旁边的 **Auto-block（自动阻断连线）**复选框。如果有人试图连接至 FTP 网站并超出所选 **Auto-block（自动阻断连线）**复选框的限制，发送该命令的计算机将被添加至临时 Blocked Sites（受禁站点）列表中。

4 如需为每件事务创建一条日志消息，则选择 **Send a long message with summary information for each transaction（为每件事务发送一条包含信息概要的日志消息）**复选框。

## 为 FTP 定义命令规则

FTP 有很多管理文件的命令。可以编写规则对一些 FTP 命令设置限制。用 FTP– 服务器代理服务器操作对一些命令设置限制，这些命令可用于 Firebox 保护下的 FTP 服务器。使用 FTP– 客户端代理服务器操作对另一些命令设置限制， Firebox 保护下的用户在连接至外部 FTP 服务器时可使用这些命令。 FTP– 客户端的默认配置允许所有 FTP 命令。

1 在 **Categories（类别）**栏中选择 **Commands（命令）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 FTP 设置下载规则

下载规则控制用户使用 FTP 进行下载的文件名、扩展名或 URL 路径。用 FTP– 服务器代理服务器操作为 Firebox 保护下的 FTP 服务器控制下载规则。用 FTP– 客户端代理服务器操作为连接至外部 FTP 服务器的用户设置下载规则。如需增加下载规则集：

1 在 **Categories（类别）**栏中选择 **Download（下载）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 FTP 设置上传规则

上传规则集控制用户使用 FTP 进行上传的文件名、扩展名或 URL 路径。用 FTP– 服务器代理服务器操作为 Firebox 保护下的 FTP 服务器控制上传规则。用 FTP– 客户端代理服务器操作为连接至外部 FTP 服务器的用户设置上传规则。 FTP– 客户端的默认配置允许所有要上传的文件。如需创建上传规则集：

1 在 **Categories（类别）**栏中选择 **Upload（上传）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 FTP 启用入侵防御

尽管可使用代理服务器定义页面激活和配置 IPS，但用 Policy Manager（策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行该操作或在代理服务器定义中使用 IPS 页面，请参阅 “*使用基于特征的安全服务*”一章。

## 为 FTP 配置代理服务器告警

告警是一种机制，在网络流量吻合可疑流量或内容时将提醒网络管理员。告警事件发生时，Firebox 执行用户设置的操作。例如，可以为文件长度设置一个阈值。如果文件大于阈值， Firebox 发送一条日志消息至日志服务器。

1 在 **Categories（类别）**栏中选择 **Proxy Alarm（代理服务器告警）**。

2 有关 **Proxy Alarm Configuration （代理服务器告警设置）**中字段的信息，请参阅第 164 页的 “*使用告警、日志消息和通知对话框*”。

# 配置 HTTP 代理服务器

HTTP 代理服务器是一种高性能内容过滤器。它检查网页流量以识别可能为病毒、间谍软件或其它入侵的可疑内容，还可以保护网络服务器免受来自外部网络的攻击。您可以将 HTTP 配置为：

- 仅允许符合网络服务器和客户端 RFC 要求的内容
- 选择 Firebox® 允许进入用户网络的 MIME 内容的类型
- 阻止 Java、 ActiveX 和其它代码类型
- 检查 HTTP 报头，确保其不是源自已知的可疑内容

1 添加 HTTP 代理服务器至 Policy Manager （策略管理器）。如需了解如何添加策略至 Policy Manager （策略管理器），请参见第 66 页的 “*添加策略*”。

2 选择 **Properties （属性）**选项卡。

3 在 **Proxy （代理服务器）**下拉列表中，选择配置 HTTP– 客户端或 HTTP– 服务器代理操作。用 HTTP– 服务器代理操作（或用户根据 HTTP– 服务器代理操作创建的传入代理服务器操作）保护网络服务器。用 HTTP– 客户端或外发代理服务器操作过滤来自 Firebox 之后用户的 HTTP 请求。

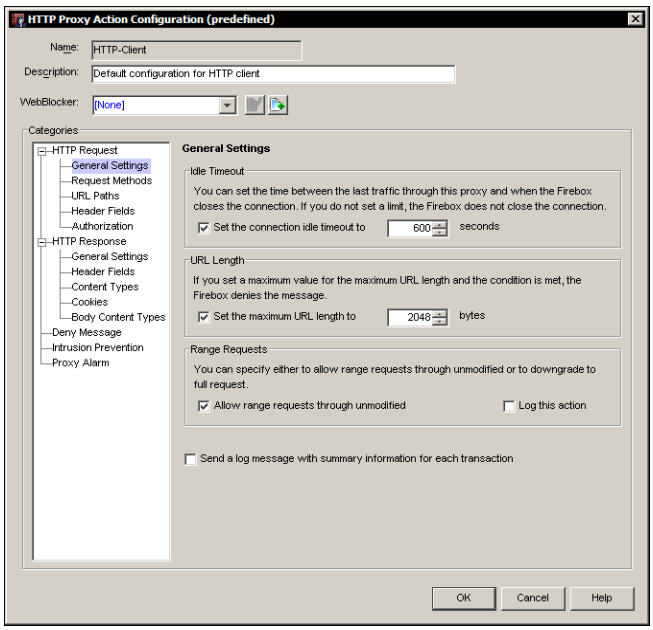
4 点击 **View/Edit Proxy （查看 / 编辑代理服务器）**图标。
也通过复制代理服务器操作来创建新的代理服务器操作。

## 为 HTTP 请求配置设置

可以为 HTTP 请求配置常规设置，还可以查看和编辑代理服务器操作中包含的 HTTP 请求规则集。为进行这些设置，点击代理服务器配置左边的 **Categories （类别）**列表中的 **HTTP Request （HTTP 请求）**。

## 为 HTTP 请求配置常规设置

可用 **General Settings（常规设置）**字段配置基本 HTTP 参数（包括空闲超时和 URL 长度）。




*Idle Timeout（空闲超时）*

控制 HTTP 代理服务器在开始 TCP/IP 连接后或对该连接所做的上一请求（若有）后，等待网络客户端为来自外部网络服务器的一些数据做出请求的时间。如果时间超出设置，HTTP 代理服务器将关闭该连接。默认值是 600 秒。

*URL Length（URL 长度）*

设置 URL 路径组件的最大长度，但不包括 “http: \\” 或主机名。控制 URL 的长度有助于防御缓存溢出攻击。

*Range requests（范围请求）*

Range request（范围请求）允许客户请求网络资源中的字节子集，而非全部内容。例如，如果您只需要一个大型 Adobe 文件的某些部分，此操作就会发挥作用。可以选择范围请求以防止下载多余的页面。如果允许范围请求通过 Firebox 并下载感染病毒的文件（其特征被分割，介于两页面之间），防病毒软件将不会发现病毒。允许范围请求可加快下载速度，但安全系数降低。

*Send a log message with summary information for each transaction（为每件事务发送包含信息概要的日志消息）*

为每件事务创建一条流量日志消息。此选项将创建大型日志文件，如果防火墙遭到攻击，则此信息就非常重要。如果不选择此复选框，则无法在 Historical Reports（历史报告）中看到关于 HTTP 代理连接的详细信息。

## 设置 HTTP 请求方法

大多数浏览器 HTTP 请求属于以下两个类型之一：GET 和 POST 操作。浏览器通常使用 GET 操作下载对象，比如图形、 HTML 数据或 Flash 数据。客户端电脑通常为每页发送多个 GET，因为网页通常包含不同的素材。这些素材集中在一起形成一个页面，显示为终端用户的页面。

浏览器通常使用 POST 操作向网站发送数据。许多网页从终端用户处获得位置、电子邮件地址和名称等信息。如果禁用 POST 命令， Firebox 将拒绝对外部网络中网络服务器的所有 POST 操作。此功能可防止用户向外部网络中的网站发送信息。

HTTP 支持的请求方法包括：HEAD、 GET、 POST、 OPTIONS、 PUT 和 DELETE。如果将规则配置为允许其它请求方法，将出现错误信息：“不支持的方法”。

1 在 **Categories（类别）**栏中选择 **Request Methods（请求方法）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

### 设置 HTTP 请求 URL 路径

用 URL 路径规则过滤 URL 主机、路径和查询字符串组件的内容。下面举例说明如何使用 HTTP 请求 URL 路径阻止内容：

- 如需阻止主机名为 www.test.com 的所有网页，则输入：www.test.com*
- 如需阻止所有网站上包含 “性”一词的所有路径，则输入：* 性 *
- 如需阻止所有网站上包含 “*.test”一词的 URL 路径，则输入：*.test

**注释**

一般情况下，如果用 HTTP 请求 URL 路径规则集过滤 URL，必须配置一个使用全部正则表达式语法和规则集高级视图的复杂模式。根据报头或正文内容类型进行过滤比按 URL 路径进行过滤更容易，效果也更好。

1 在 **Categories（类别）**栏中选择 **URL paths（URL 路径）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

### 设置 HTTP 请求报头字段

此规则集为全部 HTTP 报头提供内容过滤。默认状态下， Firebox 使用准确匹配规则删除 Via 和 From 报头，但允许所有其它报头。此规则集针对完整报头，而不仅仅是其名称。因此，如需匹配报头的所有值，输入模式：“[ 报头名称 ]:*”。如仅需匹配报头的部分值，则用一个模式取代星号（*）通配符。如果模式不是以星号（*）通配符开头，则在 **Pattern（模式）**文本框中输入时在冒号和模式之间插入一个空格。例如，输入：[ 报头名称 ]: [ 模式 ] 而不是 [ 报头名称 ]:[ 模式 ]。请注意，默认规则并不删除 Referer 报头，但包括删除本报头的禁用规则。如需启用该规则，请选择 **Change View（更改视图）**。一些网页浏览器和软件应用程序必须使用 Referer 报头才能正确运行。

1 在 **Categories（类别）**栏中选择 **Header Field（报头字段）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

### 设置 HTTP 请求授权

此规则为 HTTP 请求报头授权字段设置内容过滤标准。当网络服务器开始 “WWW-Authenticate” 质询时，即发送关于其可使用的验证方法的信息。代理服务器对在请求中发送的验证类型设置限制，仅使用网络服务器接受的验证方法。默认状态下， Firebox 允许 Basic、 Digest、 NTLM 和 Passport1.4 验证，而删除所有其它验证。

1 在 **Categories（类别）**栏中选择 **Authorization（授权）**。

2 执行用于创建规则的相关操作。详情请参阅第 79 页的 “*定义规则*”。

## 为 HTTP 响应配置常规设置

使用 General Settings （常规设置）字段配置基本 HTTP 参数，例如空闲超时、行长和总长度的限制。如果将复选框设置为 0 字节，则 Firebox 不会检查该参数。

1 在 **Categories （类别）**栏中选择 **General Settings （常规设置）**。

2 如需为 HTTP 参数设置限制，选择相应复选框。用箭头设置限制：

*Idle timeout （空闲超时）*

控制 Firebox HTTP 代理服务器等待网络服务器发送网页的时间。默认值是 600 秒。

*Maximum line length （最大行长度）*

控制 HTTP 响应报头中一行字符串的最大允许长度。使用此属性可保护计算机免受缓存溢出漏洞攻击。

*Maximum total length （最大总长度）*

控制 HTTP 响应报头的最大长度。如果报头总长度超过此限制， HTTP 响应将被拒绝。默认值是 0 （即无限制）。

## 为 HTTP 响应设置报头字段

此属性控制 Firebox 允许的 HTTP 响应报头字段。 RFC2616 包括许多默认配置中允许的 HTTP 响应。详情请参阅：

http://www.ietf.org/rfc/rfc2616.txt

1 在 **Categories （类别）**栏中选择 **Header Fields （报头字段）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 HTTP 响应设置内容类型

网络服务器发送 HTTP 流量时，通常向响应添加 MIME 类型。数据流上的 HTTP 报头包含该 MIME 类型。添加在数据发送前完成。

此规则集设置在 HTTP 响应报头中寻找内容类型 （MIME 类型）的规则。默认状态下， Firebox 允许部分安全内容类型，拒绝不含特定内容类型的 MIME 内容。

一些网络服务器提供错误的 MIME 类型以绕过内容规则。

1 在 **Categories （类别）**栏中选择 **Content Types （内容类型）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 HTTP 响应设置 cookies

HTTP cookies 是网络服务器置于网络客户端上的字母数字文本小文件。 Cookies 监视网络客户端正在浏览的网页，使网络服务器以正确的顺序发送更多网页。网络服务器也用 cookies 收集终端用户的有关信息。许多网站将 cookies 用于验证和其它合法功能，如果不使用 cookies 则无法正常运行。

此规则集使用户可控制 HTTP 响应中的 cookies。可根据网络要求配置规则删除 cookies。 HTTP– 服务器端和 HTTP– 客户端代理服务器操作的默认规则允许所有 cookies。

Cookies 规则集根据与其相关的域寻找数据包。该域可以在 cookies 中指明。如果 cookies 中无域，代理服务器将使用第一个请求中的主机名。

因此，如需阻止 nosy-adware-site.com 的所有 cookies，则添加一条带如下模式的规则：“*.nosy-adware-site.com”。

1 在 **Categories（类别）**栏中选择 **Cookies**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 设置 HTTP 正文内容类型

此规则集可控制 HTTP 响应中的内容。 Firebox 配置为拒绝 Java applet （小应用程序）、 Zip 档案、Windows EXE/DELL 文件和 Windows CAB 文件。外发 HTTP 请求（HTTP– 客户端）的默认代理服务器操作允许所有其它响应的正文内容类型。建议检查公司使用的文件类型，并仅允许网络必需的文件类型。

1 在 **Categories（类别）**栏中选择 **Body Content Types（正文内容类型）**。

2 执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

## 为 HTTP 定义防病毒措施

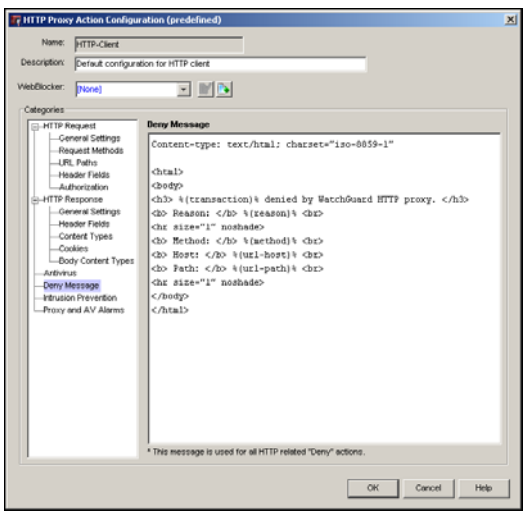
如果在电子邮件中发现病毒，此对话框中上的字段可设置必要的操作。电子邮件包含超大附件或 Firebox 不能扫描的附件时，也可设置相关操作。

尽管可使用代理服务器定义页面激活并配置 Gateway Antivirus （网关防病毒），但用 Policy Manager （策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行该操作或在代理服务器定义中使用防病毒页面的详细信息，请参阅 “*使用基于特征的安全服务*”一章。

## 更改拒绝消息

Firebox 发出默认拒绝消息，取代被拒绝的内容。您可以自己编写消息代替该拒绝消息，也可以用标准 HTML 自定义拒绝消息。拒绝消息的首行是 HTTP 报头的一部分。消息首行和正文之间必须有一空行。

1 在 **Categories（类别）**栏中选择 **Deny Message（拒绝消息）**。




2 在拒绝消息框中输入拒绝消息。可以使用如下变量：

*%（事务）%*
输入 “请求” 或 “响应” 显示事务的哪个方面使数据包遭到拒绝。

*%（原因）%*
输入 Firebox 拒绝内容的原因。

*%（方法）%*
输入来自被拒请求的请求方法。

*%（url– 主机）%*
输入来自被拒 URL 的服务器主机名。如果不包含主机名，则输入服务器的 IP 地址。

*%（url– 路径）%*
输入被拒 URL 的路径组件。

### 为 HTTP 启用入侵防御

尽管可使用代理服务器定义页面激活并配置 IPS，但用 Policy Manager（策略管理器）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行该操作或在代理服务器定义中使用 IPS 页面，请参阅 “使用基于特征的安全服务” 一章。

### 为 HTTP 定义代理服务器和防病毒告警

使用这些设置为通知事件设置标准：

1 在 **Categories（类别）**栏中选择 **Proxy and AV Alarms（代理服务器和 AV 告警）**。
2 执行第 164 页 “*使用告警、日志消息和通知对话框*” 中的相关操作。

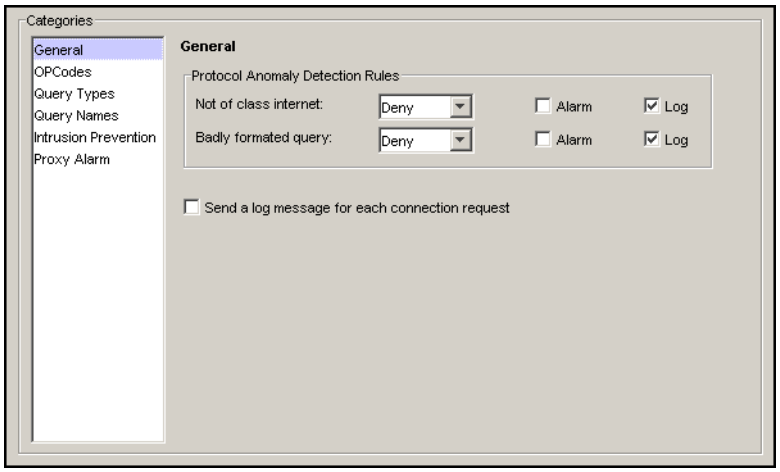
## 配置 DNS 代理服务器

利用域名系统（Domain Name System， DNS），可通过便于记忆的 “dot-com” 域名访问网站。DNS 发现互联网域名（例如：WatchGuard.com）并将其更改成 IP 地址。DNS 代理服务器保护 DNS 服务器免受 TSIG、 NXT 和其它 DNS 攻击。如需将 DNS 代理服务器添加至 Firebox® 配置：

1 添加 DNS 代理服务器至 Policy Manager（策略管理器）。如需了解如何添加策略至 Policy Manager（策略管理器），请参阅第 66 页的 “*添加策略*”。
2 双击 DNS 图标，选择 **Policy（策略）**选项卡。
3 在 **DNS proxy connections are（DNS 代理服务器连接为）**下拉列表中选择 **Allowed（允许）**。
4 选择 **Properties（属性）**选项卡。
5 在 **Proxy（代理服务器）**下拉列表中，选择设置 NS-Outgoing（NS– 外发）或 DNS-Incoming（DNS– 传入）代理服务器操作。
6 点击 **View/Edit Proxy（查看 / 编辑代理服务器）**图标。
也可以通过复制现有的代理服务器操作来创建新的代理服务器操作。

## 为 DNS 代理服务器配置常规设置

DNS 代理服务器常规设置包括两条协议异常检测规则。




*Not of class Internet*

代理服务器检查非互联网（IN）类 DNS 流量时，选择要执行的操作。默认操作为拒绝该流量。建议不要更改默认操作。用 **Alarm（告警）**复选框为此事件告警，并用 **Log（日志）**复选框将此事件写入日志文件。

*Badly formatted query（粗糙格式化查询）*

代理服务器检查格式不正确的 DNS 流量时，选择要执行的操作。用 **Alarm（告警）**复选框为此事件告警，并用 **Log check box（日志复选框）**复选框将此事件写入日志文件。

*Send a log message with summary information for each transaction（为每件事务发送一条包含信息概要的日志消息）*

选择此复选框为每个 DNS 连接请求记录一条日志消息。请注意，此操作将创建大量日志消息和流量。

## 配置 DNS OPcodes

DNS OPcodes 是向 DNS 服务器发出的命令，让其执行查询（Query）、反向查询（IQuery）或服务器状态查询（STATUS）等操作。可以允许、拒绝、中断或阻止指定的 DNS OPcodes。

1 在 **Categories（类别）**栏中选择 OPCodes。

2 从所列规则中选择 **Enabled（已启用）**复选框启用规则。取消对 **Enabled（已启用）**复选框的选择，则禁用规则。

**注释**

如果使用 Active Directory，且 Active Directory 配置要求动态更新，您必须允许传入 DNS 代理服务器规则中的 DNS OPcodes。此操作存在安全风险，但对 Active Directory 的正确运行却是必需的。

### 添加新 DNS OPcodes 规则

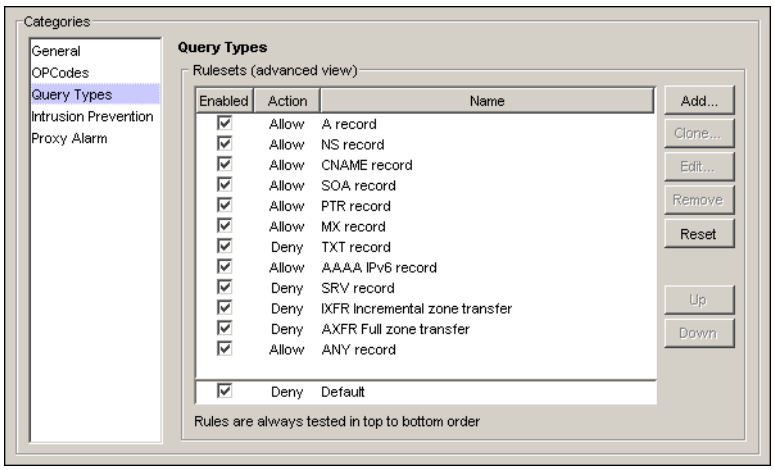
1 点击 **Add（添加）**。
弹出 New OPcodes Rule（新建 OPcode 规则）对话框。

2 输入规则名称。
规则不能超过 31 个字符。
3 DNS OPcodes 具有整数值。用箭头设置 OPcode 值。
有关 DNS OPcodes 整数值的详细信息，请参阅 RFC 1035。
4 为本规则设置一项操作，并配置发送告警或在日志文件中输入事件。详情请参阅第 80 页的“*添加规则*”。

## 配置 DNS 查询类型

DNS 查询类型可根据类型（例如 CNAME 或 TXT 记录）或查询操作的自定义类型（例如 AXFR 全区转移）配置资源记录。用户可以允许、拒绝、中断或阻止指定的 DNS 查询类型。

1 在 **Categories（类别）**栏中选择 **Query Types（查询类型）**。




2 如需启用一条规则，请选择规则操作及名称旁边的 **Enabled（已启用）**复选框。

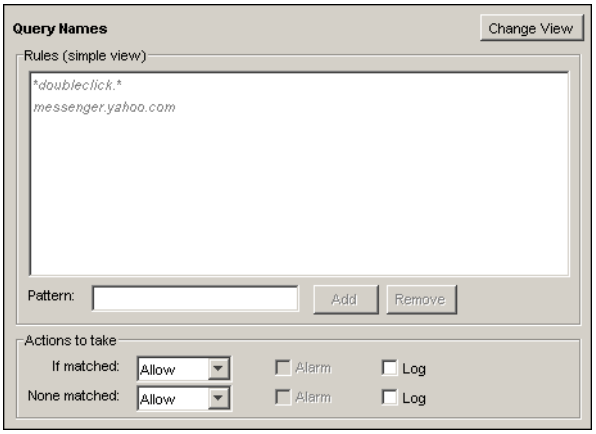
### 添加新的查询类型规则

1 如需添加新的查询类型规则，点击 **Add（添加）**。
弹出 New Query Types Rule（新建查询类型规则）对话框。
2 输入规则名称。
规则不能超过 31 个字符。
3 DNS 查询类型具有资源记录（RR）值。用箭头设置该值。
有关 DNS 查询类型的详细信息，请参阅 RFC 1035。
4 为本规则设置一项操作，并配置发送告警或在日志文件中输入事件。详情请参阅第 161 页的“*定义规则*”。

### 配置 DNS 查询名称

DNS 查询名称指指定的 DNS 域名。该域名显示为全称域名 （ FQDN ）。

1 在 **Categories （ 类别 ）**栏中选择 **Query Names （ 查询名称 )**。




2 如需添加更多名称，执行用于创建规则的相关操作。详情请参阅第 161 页的 “*定义规则*”。

### 为 DNS 启用入侵防护

尽管可使用代理服务器定义页面激活并配置 IPS，但用 Policy Manager （ 策略管理员 ）中的 **Tasks （任务 )**菜单可更轻松地完成该操作。有关如何进行该操作或在代理服务器定义中使用 IPS 页面的详细信息，请参阅 “*使用基于特征的安全服务*”一章。

### 配置 DNS 代理服务器告警

用这些设置为通知事件设定标准：

1 在 **Categories （ 类别 ）**栏中选择 **Proxy Alarm （ 代理服务器告警 )**。

2 执行第 164 页 “*使用告警、日志消息和通知的对话框*”中的操作。

## 配置 TCP 代理服务器

传输控制协议 （ TCP ）是 TCP/IP 网络中的主要协议。 IP 协议控制数据包， TCP 使主机开始连接并发送和接收数据。 TCP 代理服务器监视 TCP 握手，检查 TCP 会话是否合法。

### 为 TCP 代理服务器配置常规设置

*HTTP proxy action （HTTP 代理服务器操作 )*

选择用于 TCP 连接的 HTTP 代理服务器操作。 TCP 代理服务器将 HTTP 代理服务器规则集应用至所有确定为 HTTP 流量的流量。

*Send a log message with summary information for each transaction （为每件事务发送一条包含信息概要的日志消息）*

选择此复选框，将为所有 TCP 连接请求记录一条日志消息。此功能将创建大量日志消息和流量。

## 为 TCP 启用入侵防护

尽管可使用代理服务器定义页面激活并配置 IPS，但用 Policy Manager（策略管理员）中的 **Tasks（任务）**菜单可更轻松地完成该操作。有关如何进行该操作或在代理服务器定义中使用 IPS 页面，请参阅 “*使用基于特征的安全服务*”一章。

# 第 14 章　生成网络活动报告

Historical Reports（历史报告）是编制 Firebox® 日志文件摘要和报告的一种工具。可用这些报告了解因特网的使用情况，也可用于测量带宽及查看哪些用户及软件应用程序占用了主要带宽资源。Historical Reports（历史报告）是根据记录在 WatchGuard® Log Server（日志服务器）上的日志创建的。

用 Historical Reports（历史报告）的高级功能可：

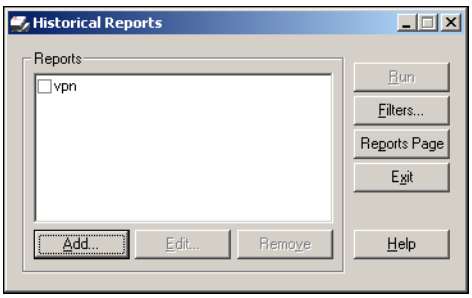
- 为一份报告设置特定的时间段。
- 用数据过滤器自定义报告。
- 将不同的日志文件合并起来，用于为一组 Firebox 创建一份报告。
- 显示不同格式的报告数据。

## 创建和编辑报告

编制报告时，设定一组设置，用于在选中的列表中创建一份报告。本栏说明如何创建、编辑及删除报告，以及如何为报告设置创建备份文件。

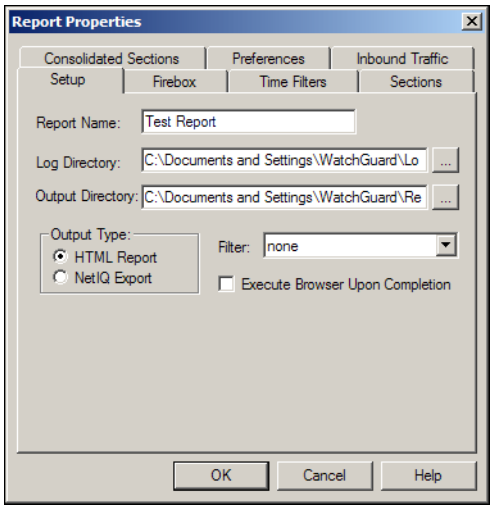
### 启用 Historical Reports（历史报告）

在 **Device Status（设备状态）**选项卡中点击 Historical Reports（历史报告）图标。



## 启用一份新报告

1 在 Historical Reports（历史报告）点击 **Add（添加）**。
弹出 Report Properties（报告属性）对话框。




2 输入报告名称。
报告名称显示在 Historical Reports（历史报告）及输出文件的名称中。

3 用 **Log Directory（日志目录）**中的文本框指定日志文件的位置。
日志文件默认位置的路径为：My Documents\My WatchGuard\Shared WatchGuard\Logs。

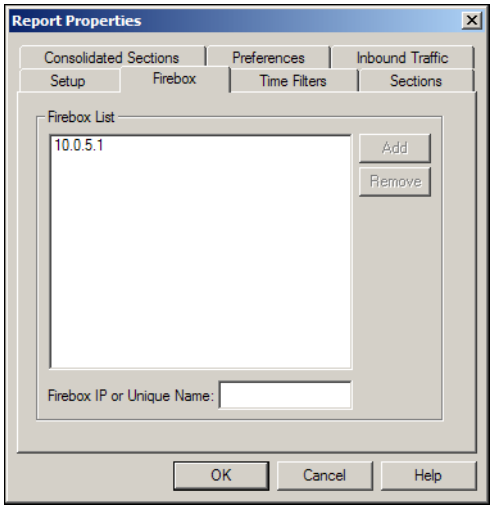
4 用 **Output Directory（输出目录）**中的文本框指定输出文件的位置。
日志文件默认位置的路径为 :My Documents\My WatchGuard\Shared WatchGuard\reports。

5 如需选择输出类型，点击 **HTML Report（HTML 报告）**或 **NetIQ Export（NetIQ 导出）**。
如需了解更多关于输出类型的信息，请参阅第 190 页的 “Exporting Reports（导出报告）”。

6 选择过滤器。
如需了解更多关于过滤器的信息，请参阅第 191 页的 “使用报告过滤器”。

7 如需在使用 HTML 输出时查看第一页，选择 **Execute Browser Upon Completion（一完毕后运行浏览器）**复选框。

8 点击 **Firebox** 选项卡。



9 输入 Firebox®IP 地址或主机名。点击 **Add（添加）**。
输入 IP 地址时，请输入所有的数字和句点。请勿使用 TAB 或箭头键。在合并栏创建报告时，只能使用 WFS Firebox 或采用 Fireware® Firebox。如果在一份报告中使用两个版本的 Firebox，则结果错误。

10 用其它选项卡设置报告首选项。详情请参阅本章后续章节。

11 完成报告设置后，点击 **OK（确认）**。
报告名称显示在报告列表中。

### 编辑现有的报告

可以更改报告的定义。

1 在 Historical Reports（历史报告）中选择要更改的报告。点击 **Edit（编辑）**。
弹出 Report Properties（报告属性）对话框。

2 更改报告定义。
如需查看项目功能，右击该项目，然后点击 What’s This?（这是什么？）。

### 删除报告

可以从现有报告的列表中删除报告。

在 Historical Reports（历史报告）中选择要更改的报告。点击 **Remove（删除）**，从 report-defs 目录下删除 <report name（报告名）>. rep 文件。

### 查看报告列表

如需查看所有报告，点击 **Reports Page（报告页面）**，所有报告将出现在默认浏览器中。可在列表中查看所有报告。

### 备份报告定义文件

报告定义文件包含用户创建的报告设置。我们建议为报告定义文件创建例常及经常性备份文件，如此，可在用户想将 **Log Server（日志服务器）**移至不同的电脑时为用户节省时间。如需创建报告定义的备份文件，需将 \Documents and Settings\WatchGuard\report-defs 文件夹复制到档案文件中，并将其保存到安全位置。

## 设置报告属性

可用 **Report Properties（报告属性）**对话框设置报告的众多属性。如需查看本对话框：

- 在 Historical Reports（历史报告）中选择一份报告，然后点击 **Edit（编辑）**。

或

- 在 Historical Reports（历史报告）中点击 **Add（添加）**。

### 指定报告时间间隔

如果在创建报告时用户未更改时间间隔，则该报告将包含整个日志文件的数据。在 **Time Filters（时间过滤器）**对话框中用下拉列表选择一项时间间隔，例如 “昨天” 或 “今天”。

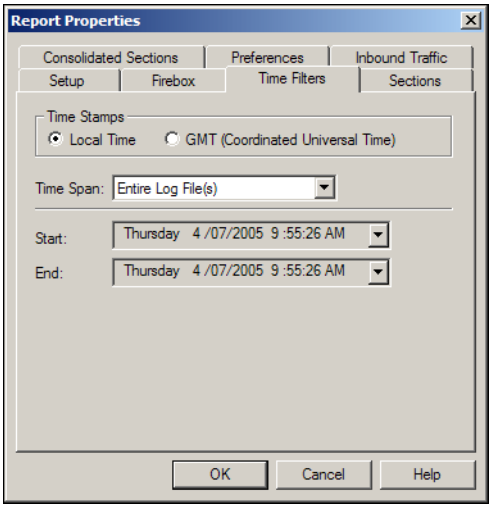
也可以手动设置开始和结束时间。如此，报告仅使用指定的时间间隔：

1 在 **Report Properties （报告属性）**对话框中点击 **Time Filters （时间过滤器）**选项卡。

2 选择显示在报告上的时间标志：**Local Time （本地时间）**或 **GMT （格林尼治标准时间）**。

3 在 **Time Span （时间跨度）**下拉列表中选择报告的时间间隔。

4 如果未在 **Time Span （时间跨度）**下拉列表中选择 **Specify Time Filters （指定时间过滤器）**，则点击 **OK （确认）**。
如果选择了 **Specify Time Filters （指定时间过滤器）**，则点击 **Start （开始）**和 **End （结束）**下拉列表并选择开始及结束时间，然后点击 **OK （确认）**。




## 指定报告区

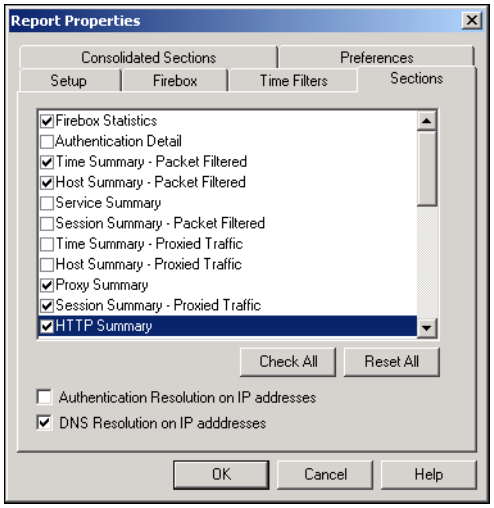
用户可通过使用 **Report Properties （报告属性）**对话框上的 **Sections （报告区）**选项卡，选择显示在报告中的信息。

1 在 **Report Properties （报告属性）**对话框中点击 **Sections （报告区）**选项卡。

2 选择要将其纳入报告的各个区复选框。
如需查看每个区的内容，请参阅第 193 页的 “*报告区和合并区*”。

3 （可选）如需纳入经验证Firebox®用户的IP地址的验证名称，选择**Authentication Resolution on IP address （IP 地址的验证解析）**复选框。
必须启用用户验证以用 IP 地址至用户名的决定创建报告。如需用已启用的决定创建报告，则需更长时间。

4 （可选）如需纳入IP地址的DNS名称，选择**DNS Resolution on IP address（IP地址的DNS解析）**复选框。
仅为从 Firebox 中解析 DNS 信息的 IP 地址纳入本信息。




## 合并报告区

在 **Sections（报告区）**选项卡中可选择将哪些信息纳入报告。用户可：

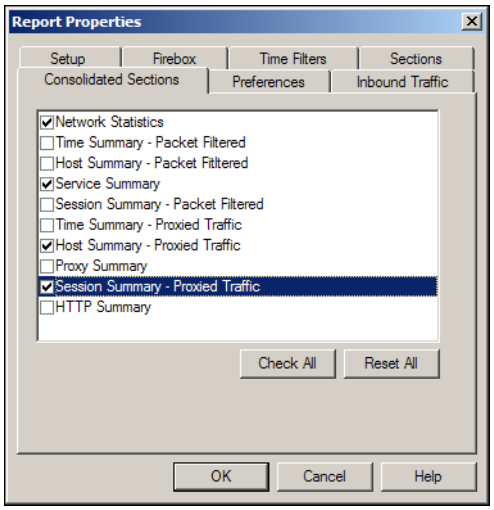
- 垂直查看每组 Firebox 的数据
- 平铺或层叠查看一组 Firebox® 设备的合并数据。

如需合并报告区：

1 在 **Report Properties（报告属性）**对话框中选择 **Consolidated Sections（合并区）**选项卡。
本选项卡带有一份用户可合并报告区列表。有关这些报告区内容的简短说明，请参阅本章末的 “报告区和合并区”。

2 选择报告区旁边的复选框将其纳入报告；清除无需纳入报告的报告区复选框。

3 点击 **OK（确认）**。



### 设置报告属性

报告可有 Summary sections （ 摘要区 ）或 Details sections （ 详情区 ）。用户可独立控制每个区的信息显示，以达到显示重要信息的最佳状态。报告摘要区显示包含用户所定义信息的文本和图像。

如需设置报告属性：

1 在 **Report Properties （ 报告属性 ）**对话框中选择 **Preferences （ 优选项 ）**选项卡。

2 输入作为图表显示在报告中的数据点 （ 项目 ）数量。
例如：如果有 45 台主机，则绘制前 10 台主机并将其余主机列为 “其它”。默认数量为 10。

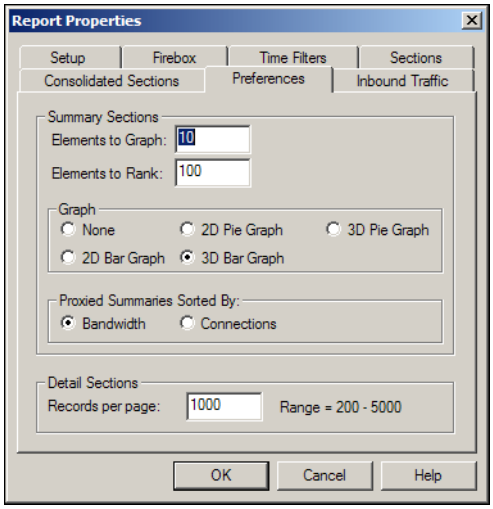
3 输入要在表格中输入的项目数量。
默认数量为 100。

4 选择将在报告中使用的图表类型。

5 选择如何对被代理摘要进行排序：按带宽或按连接。

6 输入将显示在详情区每页上的记录数量。
默认数量为 1,000 条记录。

7 点击 **OK （ 确认 ）**。




### 查看网络接口关系

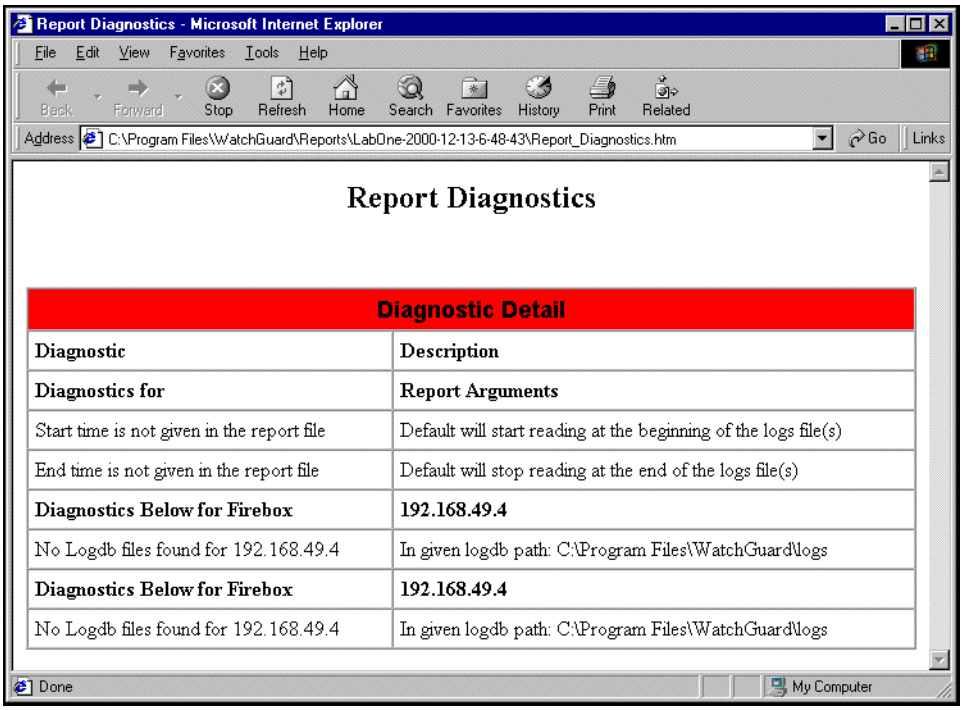
在 **Inbound Traffic （ 进向流量 ）**选项卡中，用户可以看到所有 Firebox 判断为进向的网络接口关系。例如，从可选网络至受信网络的流量可认为是进向流量。如果用户想从本列表中删除一项关系，点击 **Remove （ 删除 ）**。用户还自行将对应的源头和目的站添加到此列表。点击 **Add （ 添加 ）**并输入想要设定为进向的新源头和目的站。

## 导出报告

可以分两种格式导出报告：HTML 和 NetIQ。在 My Documents\My WatchGuard\Shared WatchGuard\reports\<export file> 路径中可找到所有的报告。报告目录带有每份报告的名称与时间子目录。

### 导出报告为 HTML 格式

如果从 **Report Properties （报告属性）**对话框上的 **Setup （设置）**选项卡上选择 **HTML Report （HTML 报告）**，则报告输出格式为 HTML。可以通过 JavaScript 菜单进入每个报告区。为此，用户必须在浏览器上启用 JavaScript。下图介绍如何将报告显示在浏览器中：




### 导出报告为 NetIQ 格式

NetIQ 提供系统和安全管理解决方案，包括公司如何使用因特网的所有报告，但 NetIQ 以不同与 WatchGuard Historical Reports （历史报告）的方式检测数据。为计算因特网使用报告的数据，Historical Reports （历史报告）计数 HTTP 协议事务的数量。 NetIQ 计算 URL 请求的数量。

**注释**

必须将 WatchGuard HTTP 代理服务器日志设为 “ON”，以向 NetIQ 提供必要的信息。

可在如下路径中找到报告：
My Documents\My WatchGuard\Shared WatchGuard\reports

## 使用报告过滤器

除非用户创建并使用报告过滤器，否则报告将包含整个日志文件的数据。可通过使用报告过滤器，仅显示指定主机、服务或用户的信息。该过滤器为如下两个类型中的一种：

*Include （包括型）*

编制一份报告，该报告也记载 **Host （主机）**、 **Service （服务）**或 **User Report Filters （用户报告过滤器）**选项卡中的属性设置记录。

*Exclude（不包括型）*

编制一份报告，该报告不记载 **Host（主机）**、**Service（服务）**或 **User Report Filters（用户报告过滤器）**选项卡中的属性设置记录。

可以将某一过滤器设置为在报告中 Include（包括）或 Exclude（不包括）如下三项属性的数据：

*Host（主机）*

主机 IP 地址。

*Port（端口）*

服务名或端口编号。

*User（用户）*

经验证的用户名。

## 创建新的报告过滤器

用 Historical Reports（历史报告）创建新的报告过滤器。可在 WatchGuard® 安装目录中找到过滤器，它位于子目录 report-defs 中，其扩文件展名为 .ftr。

1 在 Historical Reports（历史报告）中点击 **Filters（过滤器）**。

1 点击 **Add（添加）**。

2 输入过滤器名称。该名称显示在 **Report Properties Setup（报告属性设置）**选项卡上的 **Filters（过滤器）**下拉列表中。

3 选择过滤器类型。

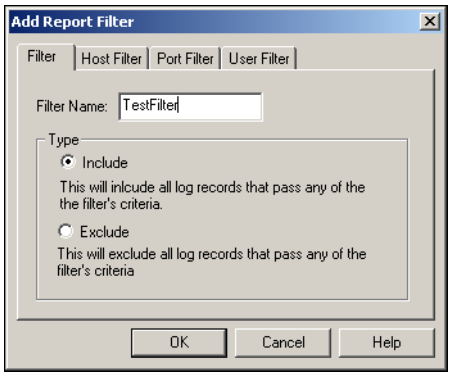
例如：如果有 45 台主机，则绘制前 10 台主机并将其余主机列为 “其它”。如需了解 Include（包括型）和 Exclude（不包括型）过滤器的相关信息，请参阅上述内容。

4 完成 **Filters（过滤器）**选项卡。

如需查看项目功能，右击该项目，然后点击 What’s This?（这是什么？）。

5 完成操作后，点击 **OK（确认）**。

过滤器名称显示在过滤器列表中。Filter Name（过滤器名称）.ftr 文件的路径为：My Documents\My WatchGuard\Shared WatchGuard\report-defs。




## 编辑报告过滤器

可以更改过滤器的属性。在 Historical Reports（历史报告）中的 **Filters（过滤器）**对话框中：

1 选择要更改的过滤器，然后点击 **Edit（编辑）**。

弹出 Report Filter（报告过滤器）对话框。

2 更改过滤器属性。
如需查看项目功能，右击该项目，然后点击 What’ s This？（这是什么？）。

### 删除报告过滤器

如需将过滤器从过滤器列表中删除，选择要删除的过滤器，再点击 **Delete（删除）**，将 . ftr 文件从 \report-defs 目录中删除。

### 应用报告过滤器

每份报告仅可有一个过滤器。如需应用该过滤器，打开报告属性。

1 在 Historical Reports（历史报告）中选择将要应用过滤器的报告，然后点击 **Edit（编辑）**。

2 用 **Filters（过滤器）**下拉列表选择一个过滤器。
只有用户在 Filters（过滤器）对话框中创建了过滤器，它才会显示在下拉列表中。如需了解更多相关信息，请参阅第 192 页的 “*创建新的报告过滤器*”。

3 点击 **OK（确认）**。
保存新建报告至 report-defs 目录中的 ReportName. rep 文件中。创建报告后，过滤器即开始应用。

## 运行报告

可用 Historical Reports（历史报告）创建一份或多份报告。

1 在 Historical Reports（历史报告）中选择所需报告旁边的复选框。

2 点击 **Run（运行）**。

**注释**

如果未选择 HTTP 代理服务器操作中的 **Send a log message with summary information for each transaction（为每件事务发送一条包含信息概要的日志消息）**复选框，用户就不会看到报告中 HTTP 代理连接的详细信息。

## 报告区和合并区

可用 Historical Reports（历史报告）创建带有一个或多个区域的报告。每个区包括不同类型的信息或网络流量。可将指定区域集中起来创建概要区，然后可为一组 Firebox® 设备的事件日志消息创建一份报告。

### 报告区

有两种基本的报告区类型：

- **Summary**（摘要）– 按带宽或连接排列数据的区域。
- **Detailed**（详情）– 显示所有流量和事件（但无简要图表或序列）的区域。

不同类型的报告区和合并区如下所述：

*Firebox Statistics （Firebox 统计数据）*

一个 Firebox 的一份或多份日志文件的简要统计数据。

*Authentication Detail （验证详情）*

按连接时间顺序排列的经验证用户的列表，其文本框包括：

– 经验证的用户
– 主机
– 经验证会话的开始日期和开始时间
– 经验证会话的结束时间
– 会话长度

*Time Summary （时间摘要） – Packet Filtered （已过滤的数据包）*

所有已接受连接的一张表格和可选图表，这些连接按照用户自定义的间隔和时间分开。默认的时间间隔为 “每天”，但用户可选择不同的时间间隔。

Host Summary （主机摘要） – Packet Filtered （已过滤的数据包）

按字节容量或连接数量顺序生成的一张所有内部和外部主机表格或可选图表，这些主机通过 Firebox 发送在数据包中经过滤的数据流。

*Service Summary （服务摘要）*

按连接计数顺序生成的一张每项服务的数据流表格和可选图表。

*Session Summary （会话摘要） – Packet Filtered （已过滤的数据包）*

按字节容量或连接数量顺序生成的一张顶级进向和外发会话表格和可选图表。会话的格式为：client （客户端）>server （服务器）：service （服务）。 Historical Report （历史报告）会尝试用一份表格查看服务器端口以显示服务名称。如果本操作不起作用，则 Historical Report （历史报告）将显示端口编号。

*Time Summary （时间摘要） – Proxied Traffic （被代理流量）*

所有已接受连接的一张表格和可选图表，这些连接按照用户自定义的间隔和时间分开。默认的时间间隔为 “每天”，但用户可选择不同的时间间隔。

*Host Summary （主机摘要） – Proxied Traffic （被代理流量）*

按字节容量或连接数量顺序生成的一张所有内部和外部主机表格和可选图表，这些主机通过 Firebox 发送在数据包中经过滤的数据流。

*Proxy Summary （代理服务器摘要）*

指按带宽或连接顺序运行的代理服务器。

*Session Summary （会话摘要） – Proxied Traffic （被代理流量）*

a) 按字节容量或连接数量顺序生成的一张顶级进向和外发会话表格和可选图表。该会话显示。会话的格式为：client （客户端）–>server （服务器）：service （服务）。服务以大写字母显示。

*HTTP Summary （HTTP 摘要）*

按字节容量或连接数量顺序生成的用户通过 HTTP 代理连接的顶级外部网域和主机表格和可选图表。

*HTTP Detail （HTTP 详情）*

按时标顺序生成的进向和外发 HTTP 数据流表格。这些字段为 Date （日期）、 Time （时间）、 Client （客户端）、 URL Request （URL 请求）和 Bytes Transferred （已传输的字节）。

*SMTP Summary （SMTP 摘要）*

按字节容量或连接数量顺序生成的顶级进向和外发电子邮件地址的一份表格和可选图表。

*SMTP Detail （SMTP 详情）*

按时标顺序生成的一份进向和外发 SMTP 代理服务器数据流表格。这些字段为 Date （日期）、 Time （时间）、 Sender （发件人）、 Recipient （收件人）和 Bytes Transferred （已传输的字节）。

*FTP Detail*

按时标顺序生成的多份进向和外发 FTP 数据流表格。这些字段为 Date （日期）、 Time （时间）、 Client （客户端）、 Server （服务器）、 FTP Request （FTP 请求）和 Bandwidth （带宽）。

*Denied Outgoing Packet Detail （被拒绝的外发数据包详情）*

按时间顺序生成的一份被拒绝的外发数据包列表。这些字段为 Date （日期）、 Time （时间）、 Type （类型）、 Client Port （客户端口）、 Server Port （服务器端口）、 Protocol （协议）、 Duration （持续时间）。

*Denied Incoming Packet Detail （被拒绝的进向数据包详情）*

按时间顺序生成的一份被拒绝的进向数据包列表。这些字段为 Date （日期）、 Time （时间）、 Type （类型）、 Client Port （客户端口）、 Server Port （服务器端口）、 Protocol （协议）、 Duration （持续时间）。

*Denied Packet Summary （被拒绝的数据包摘要）*

本区存在多张不同的表格。每张表格显示（拒绝数据包的）主机的数据。数据的内容包括第一次和最后一次尝试的时间、类型、服务器、端口、协议和尝试次数。如果仅有一次尝试，则最后一个字段无数据。

*Denied Service Detail （被拒绝的服务详情）*

一张用户被拒绝使用某项服务的事件列表。该列表包括进向和外发请求。

*WebBlocker Detail （WebBlocker 详情）*

按时间顺序生成的一张被 WebBlocker 拒绝的 URL 列表。这些字段为 Date （日期）、 Time （时间）、 User （用户）、 Web Site （网站）、 Type （类型）和 Category （种类）。

*Denied Authentication Detail （被拒绝的验证详情）*

按时间顺序生成的一张造拒绝验证列表。这些字段为 Date （日期）、 Time （时间）、 Host （主机）和 User （用户）。

*IPS Blocked Sites （IPS 受禁网站）*

IPS 受禁网站列表。

*Alarms （告警）*

仅供 Fireware® 用户使用，该报告显示所有设备告警及每次告警发现的问题。

*AV Summary （AV 摘要）*

电子邮件操作的 Gateway Antivirus （网关防病毒）摘要。这些字段包括 sender （发件人）、 virus detail （病毒详情）、 if the virus was cleaned （是否已清除病毒）和 attachment size of the e-mail （电子邮件的附件大小）。定购了防病毒服务的 Fireware 用户可获得本区功能。

*AV Detail （AV 详情）*

作为电子邮件对策提供的 Gateway Antivirus （网关防病毒）的源头、发件人及病毒详情的列表。本功能仅供定购了防病毒服务的 Fireware 用户使用。

*IPS Summary （IPS 摘要）*

入侵防御服务（IPS）的对策摘要，它显示（按百分比划分的）数据流类型、源 IP 地址和特征种类。本功能仅供定购了 IPS 服务的 Fireware 用户使用。

*IPS Detail （IPS 详情）*

所有入侵防御服务的对策列表，包括源头、协议和特征详情。本功能仅供定购了 IPS 服务的 Fireware 用户使用。

## 合并区

*Network Statistics （网络统计数据）*

受监控的所有 Firebox 的一张或多份日志文件统计摘要。

*Time Summary （时间摘要） – Packet Filtered （已过滤的数据包）*

所有已接受连接的一个表格和可选图表，这些连接被用户自定义的间隔和时间顺序分开。默认的时间间隔为 “每天”，但用户可选择不同的时间间隔。

*Host Summary （主机摘要） – Packet Filtered （已过滤的数据包）*

所有内部和外部主机的一个表格或可选图表，这些主机通过 Firebox 发送在数据包中经过滤的数据流。主机按字节容量或连接数量顺序显示。

*Service Summary （服务摘要）*

按连接计数顺序记录每项服务数据流的一个表格和可选图表。

*Session Summary （会话摘要） – Packet Filtered （已过滤的数据包）*

按字节容量或连接数量顺序生成的一张顶级进向和外发会话表格和可选图表。会话的格式为：client（客户端）>server（服务器）：service（服务）。Historical Report（历史报告）将尝试通过表格查看服务器端口，以显示服务名称。如果本操作不起作用，则 Historical Report（历史报告）显示端口编号。

*Time Summary （时间摘要） – Proxied Traffic （被代理流量）*

所有已接受连接的一张表格和可选图表，这些连接按照用户自定义的间隔和时间顺序分开。默认的时间间隔为 “每天”，但用户可选择不同的时间间隔。

*Host Summary （主机摘要） – Proxied Traffic （被代理流量）*

按字节容量或连接数量顺序生成的一张内部和外部主机表格和可选图表，这些主机使用一项代理策略通过 Firebox 发送数据流。

*Proxy Summary （代理服务器摘要）*

按带宽或连接顺序生成的代理服务器摘要。

*Session Summary （会话摘要） – Proxied Traffic （被代理流量）*

按字节容量或连接数量顺序生成的一张顶级进向和外发会话表格和可选图表。会话的格式为：client（客户端）–>server（服务器）：service（服务）。服务以大写字母显示。

*HTTP Summary （HTTP 摘要）*

按字节计数或连接数量顺序生成的用户通过 HTTP 代理连接到的顶级外部网域和主机表格和可选图表。

# 第 15 章　管理服务器设置与管理

WatchGuard® 管理服务器用一个简单易用的接口管理分布式的企业 VPN（虚拟专用网络）隧道。管理服务器还允许用户集中管理多个 Firebox® X Edge 设备。完成本章所述的设置操作后，可以用 WatchGuard® 管理服务器配置和管理连接至管理服务器的 Firebox 设备。用户可以在管理服务器设备页面上打开适当的工具来管理 Firebox X Core、 Firebox X Peak、 Firebox III、 Firebox X Edge 及 SOHO 6 设备。如需了解更多相关信息，请参阅后续章节。

用户可以用 WatchGuard® 管理服务器配置和管理多个 Firebox® X Edge 设备。如需了解更多相关信息，请参阅 “*管理 Firebox X Edge 和 Firebox SOHO*”一章。

用户可以在安装时在管理工作站上安装管理服务器，或者执行同样的安装程序将管理服务器安装到另一台使用 Windows 操作系统的电脑。建议将 Management Server （管理服务器）软件安装在带有静态 IP 地址（该静态 IP 地址位于 Firebox 之后，带有一个静态的外部 IP 地址）的电脑上。否则， Management Server （管理服务器）不会正常运行。

## WatchGuard 管理服务器口令

WatchGuard® 管理服务器采用许多密码以保护其硬盘上的敏感资料及客户端系统的数据。安装好 WatchGuard 管理服务器软件后，必须使用 Configuration Wizard （配置向导）设置管理服务器。此向导将对如下口令做出提示：

- 主加密密钥
- 管理服务器口令

管理服务器口令和其它自动创建的口令保存在口令文件中。

### 主加密密钥

用 Configuration Wizard （配置向导）设置的第一个口令是主加密密钥。该口令可以保护口令文件中的所有口令。

主加密密钥用于对管理服务器硬驱上的所有口令进行加密，防止可进入硬驱或其存档内容的人士获得口令及防止其使用获得的口令访问硬驱上的其它敏感资料。

认真选择并保护好主加密密钥，并确保主加密密钥和管理服务器口令不是同一密码。
在如下情况下可使用主加密密钥：

- 将管理服务器资料转移至新系统
- 恢复丢失的或被误用的主密钥文件
- 更改主加密密钥

不应频繁使用主加密密钥。建议用户将主加密密钥记下来并将其置于安全的位置。

### 管理服务器口令

Configuration Wizard（配置向导）提示的第二个口令是管理服务器口令。管理员频繁地使用该口令。用户可用本口令连接至 WatchGuard System Manager 中的管理服务器。

### 密码和密钥文件

管理服务器口令和所有自动创建的口令都保存在口令文件中。本文件中的口令由主加密密钥进行保护。主加密密钥并不保存在硬驱上。在主加密密钥上创建加密密钥。
密码文件和加密密钥的默认位置是：

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini
- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

请注意，这些文件由管理服务器软件使用，并且管理员不得直接对其进行修改。

### Miicrosoft SysKey 的应用

主密钥可用于保护密码文件，加密密钥可用于保护该主密钥，而 Windows 系统密钥又可用于保护该加密密钥。
Windows 操作系统用系统密钥保护安全账户管理（SAM）数据库。该数据库是电脑上的 Windows 账户和密码的数据库。默认状态下，系统密钥数据隐藏在注册表中。该系统受到保护，并且系统密钥是在启动过程中于注册表中生成。如果用户想拥有一个更安全的系统，则可从注册表中删除系统密钥，完全避免将敏感资料保存在系统上。
可用系统密钥实用程序：

- 将系统密钥移至一张软盘
- 让管理员在启动时输入密码
- 将系统密钥从软盘中移至系统

如果将启动密钥移至软盘，那么必须将该软盘插入系统中使系统启动。如果让管理员输入启动密码，管理员必须在每次系统启动时输入一次密码。
如需设置系统密钥选项，点击 **Start（开始）>Run（运行）**，输入系统密钥，然后点击 **OK（确认）**。

# 设置管理服务器

Management Server Setup Wizard （管理服务器安装向导）在工作站上创建新的 Management Server （管理服务器）。如果您曾使用 WatchGuard® System Manager 和 VPN Manager 的早期版本，也可使用本向导将安装在 Firebox® 上的 DVCP Server （DVCP 服务器）迁移至工作站上新的管理服务器。如需将 Management Server （管理服务器）从 Firebox 移开，请参阅 WFS to Fireware Migraion Guide （WFS Fireware 迁移指南）。

建议将 Management Server （管理服务器）软件安装在带有静态 IP 地址 （该静态 IP 地址位于 Firebox 之后，带有一个静态的外部 IP 地址）的电脑上。否则， Management Server （管理服务器）不会正常运行。

本程序说明了成功安装新 Management Server （管理服务器）所必须执行的操作步骤。如果此时您还没有 Management Server （管理服务器），则可采用本程序。

1 右击 Windows 任务栏上的 WatchGuard 工具条中的 Management Server （管理服务器）图标。
如果尚未安装 Management Server （管理服务器），您将不会看到该图标。


2 选择 **Start Service （开始服务）**。

3 Management Server Setup Wizard （管理服务器安装向导）开始运行，点击 **Next （下一步）**。

4 需要用主加密密钥控制对 WatchGuard 管理工作站的访问。输入至少有 8 位字符的口令并再次输入以确认。点击 **Next （下一步）**。
确保将此口令保存在安全的地方。

5 输入设置和监视 WatchGuard Management Server （WatchGuard 管理服务器）所需的 Management Server （管理服务器）密码。采用至少有 8 位字符的口令并再次输入以确认。点击 **Next （下一步）**。

6 输入网关 Firebox 的 IP 地址和口令。该网关 Firebox 可以对 Management Server（管理服务器）进行因特网安全保护。输入 IP 地址时，本向导完成如下三项操作：
   – 本向导用此 IP 地址设置网关 Firebox 以允许连接至 Management Server （管理服务器）。如果不在此处输入 IP 地址，您必须在 Management Server （管理服务器）与因特网之间设置一堵防火墙以允许连接至 TCP 端口 4110、 4112 和 4113 上的 Management Server （管理服务器）。
   – 如果拥有 WatchGuard System Manager 的早期版本，并将 Firebox 设置为 DVCP 服务器，本向导则从网关 Firebox 获得 DVCP 服务器信息并将这些设置移至 Management Server （管理服务器）。如需了解更多信息，请参阅 “*迁移指南*”。
   – 本向导为 Certificate Revocation List （证书撤销列表）设置 IP 地址。作为托管客户端添加的用户使用该 IP 地址连接至 Management Server （管理服务器）。本 IP 地址必须是 Management Server（管理服务器）向因特网显示的公共 IP 地址。如果不在此处输入 IP 地址，则本向导会将 Management Server （管理服务器）电脑上的当前 IP 地址用作 CRL IP 地址。如果由于你的电脑位于网络地址转换 （NAT）设备后区而使该 IP 地址不同于电脑向因特网显示的 IP 地址，那么您必须编辑 CRL 并输入 Management Server （管理服务器）使用的公共 IP 地址。如需了解更多相关信息，请参阅第 200 页的 “*更改管理服务器的设置*”。

7 输入 Management Server（管理服务器）的许可密钥，点击 **Next（下一步）**。
如需了解更多关于 Management Server（管理服务器）许可密钥的信息，请参阅 "*高级常见问题解答*"：
https://www.watchguard.com/support/AdvancedFaqs/wsm8_srvrkey.asp

8 输入公司名，点击 **Next（下一步）**。
本公司名用于 Management Server（管理服务器）上的 Certificate Authority（认证中心）。

9 弹出一个显示服务器信息的信息界面。点击 **Next（下一步）**。
本向导对服务器进行设置。

10 点击 **Finish（完成）**。

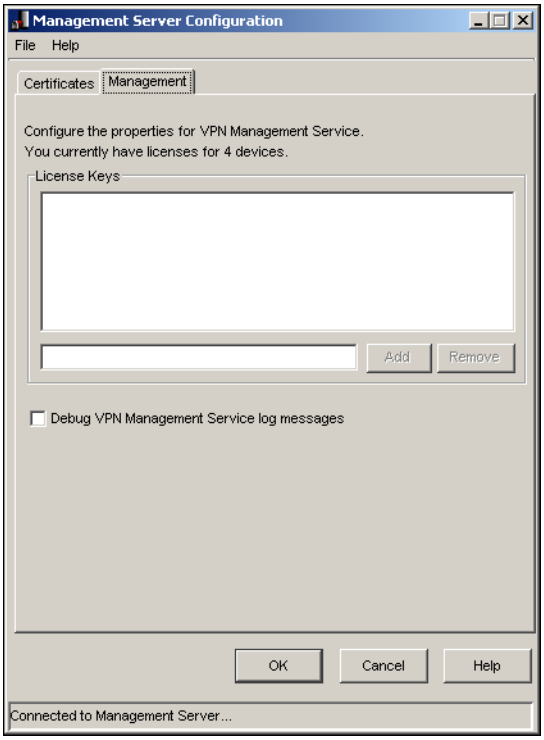
**注释**

IP 地址绑定至 Management Server（管理服务器）的接口下降并重新启动时，建议重新启动 Management Server（管理服务器）。

## 更改管理服务器设置

Management Server Setup Wizard（管理服务器安装向导）对 Management Server（管理服务器）进行设置。利用本向导进行配置后，无需经常更改 Management Server（管理服务器）的属性。如果必须更改 Management Server（管理服务器）的设置，用户可直接在 Management Server（管理服务器）上进行。

在配置为 Management Server（管理服务器）的电脑上，右击 WatchGuard® 工具条中的 Management Server（管理服务器）图标并选择 **Configure（配置）**，然后弹出 **Management Server Configuration（管理服务器配置）**对话框。



### 添加或删除管理服务器许可证

如需添加 Management Server（管理服务器）许可证，点击 **Management（管理）**选项卡。将 Management Server（管理服务器）许可证输入或粘贴至本字段，然后点击 **Add（添加）**。

如需删除 Management Server（管理服务器）许可证，点击 **Management（管理）**选项卡。选择要删除的许可证，然后点击 **Remove（删除）**。

完成本项设置后点击 **OK（确认）**。

如需了解更多关于 Management Server（管理服务器）许可密钥的信息，请参阅 Advanced FAQ（高级常见问题解答）：
https://www.watchguard.com/support/AdvancedFaqs/wsm8_srvrkey.asp

### 记录管理服务器的诊断日志消息

如需让 Management Server（管理服务器）发送诊断日志消息至 Windows Event Viewer（Windows 事件查看器），点击 Management（管理）选项卡。选择 **Debug VPN Management Service Log Messages（调试 VPN 管理服务日志消息）**复选框。

如需查看诊断日志消息，打开 Windows Event Viewer（Windows 事件查看器）。从 Windows 桌面上选择 **Start（启动）>Run（运行）**。在 Event Viewer（事件查看器）中的应用栏中输入 eventvwr 以查看日志消息。

## 设置认证中心

可在 WatchGuard Management Server（WatchGuard 管理服务器）上设置 Certificate Authority（认证中心）。用 Certificate Authority（认证中心）：

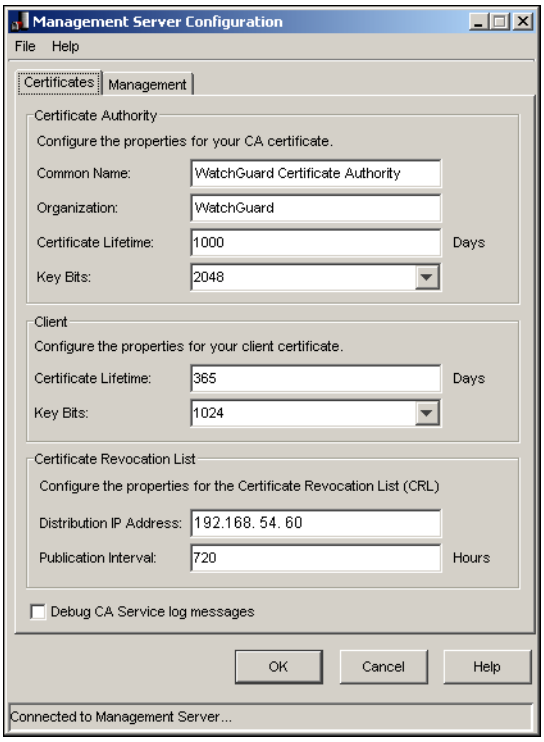
- 设置 CA 证书的属性
- 设置客户端证书的属性
- 设置 Certificate Revocation List（证书撤销列表）的属性
- 将 CA 服务诊断日志消息写入 Windows Event Viewer（Windows 事件查看器）

### 设置 CA 证书的属性

通常情况下， Firebox 的管理员不会更改 CA 证书的属性。如果必须更改这些设置：

1 在设置为 Management Server（管理服务器）的电脑上，右击 WatchGuard 工具条中的 Management Server（管理服务器）图标并选择 **Configure（设置）**。

2 点击 **Certificates**（证书）选项卡。




3 在 **Common Name**（通用名）文本框中输入想要将其显示在 CA 证书上的名称。

4 在 **Organization**（公司名）文本框中为 CA 证书输入公司名。

5 在 **Certificate Lifetime**（证书有效期）文本框中输入 CA 证书的有效天数。
如果证书有效期较长，则黑客可有更多时间进行攻击。

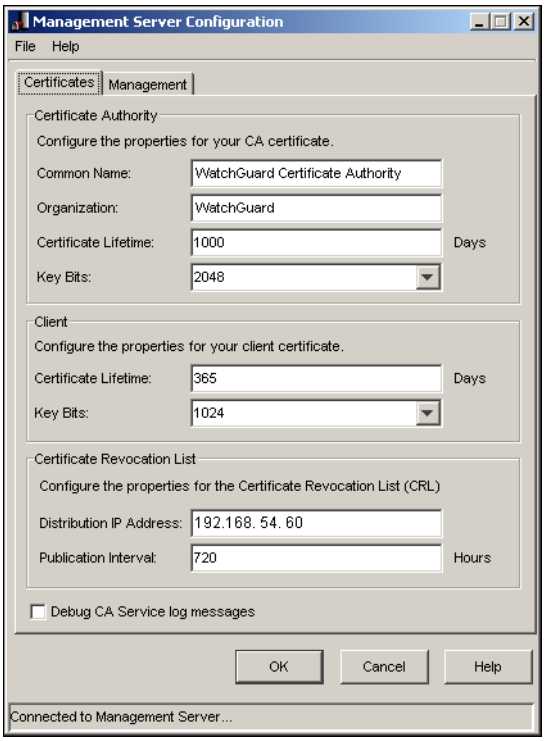
6 在 **Key Bits**（密钥位）下拉列表中选择证书的安全级别。
Key Bits（密钥位）设置中的数字越长，保护密钥的加密功能越强。

7 完成本项设置后点击 **OK**（确认）。

## 设置客户端认证的属性

1 在定义为 Management Server（管理服务器）的电脑上右击 WatchGuard 工具条中的 Management Server（管理服务器）图标并选择 **Configure**（配置）。

2 点击 **Certificates**（证书）选项卡。




3 在 **Certificate Lifetime**（证书有效期）文本框中输入客户端证书的有效天数。
如果认证有效期较长，则黑客可有更多时间进行攻击。

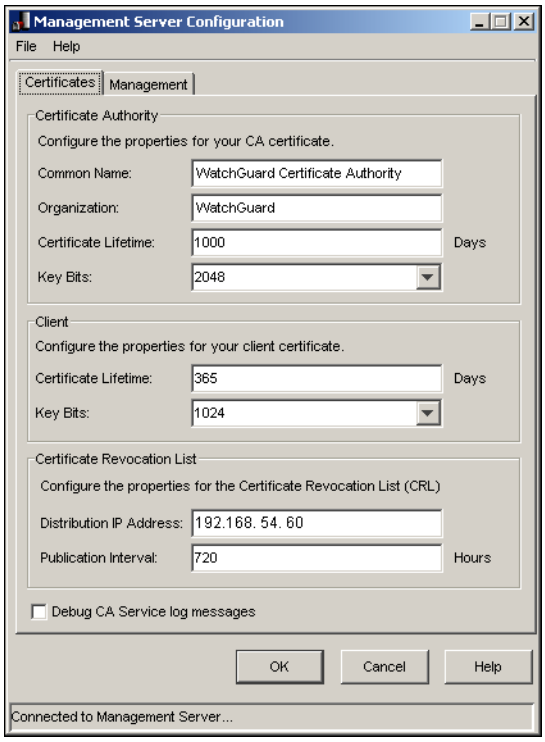
4 在 **Key Bits**（密钥位）下拉列表中选择证书的安全级别。
Key Bits（密钥位）设置中的数字越长，保护密钥的加密功能越强。

5 完成本项设置后点击 **OK**（确认）。

## 为 Certificate Revocation List（证书撤销列表，CRL）设置属性

1 在定义为 Management Server（管理服务器）的电脑上右击 WatchGuard 工具条中的 Management Server（管理服务器）图标并选择 **Configure**（配置）。

2 点击 **Certificates（证书）**选项卡。




3 为 Certificate Revocation List（证书撤销列表， CRL）输入 **Distribution IP Address（分配 IP 地址）**。
默认状态下，该地址为网关 Firebox 的地址，也是远程管理 Firebox 客户端用以连接至 Management Server（管理服务器）的 IP 地址。如果 Firebox 的外部 IP 地址更改，您必须更改此值。

4 为 CRL 输入以小时为单位的 **Publication Interval（公布时间间隔）**。该时间间隔为 CRL 自动公布的时间。
默认设置为零（0），表示 CRL 每隔 720 小时（30 天）进行公布。证书撤销后， CRL 也会更新。

5 完成本项设置后点击 **OK（确认）**。

### 记录认证中心服务的诊断日志消息

如需让 Management Server（管理服务器）发送诊断日志消息至 Windows Event Viewer（Windows 事件查看器），点击 **Certificates（证书）**选项卡。选择 **Debug CA Service log message（调试 CA 服务日志消息）**复选框。如需查看日志消息，打开 Windows Event Viewer（Windows 事件查看器）。

## 备份或恢复管理服务器设置

Management Server（管理服务器）载有所有托管 Firebox® X Edge 和 VPN 隧道的配置信息。建议经常为 Management Server 创建备份文件并将其妥善保管。万一硬件出现故障，用户可用此备份文

件恢复 Management Server。用户也可用此备份文件将 Management Server 转移至一台新电脑。如果使用已创建的备份文件，您必须知道主加密密钥。在您最初设置 Management Server 时即已设置了主加密密钥。

1 在 Windows 工具条中右击 Management Server 图标并选择 **Stop Service（停止服务）**。

2 在 Windows 工具条中右击 Management Server 图标并选择 **Backup（备份）/Restore（恢复）**。
Management Server Backup/ Restore Wizard（管理服务器备份 / 恢复向导）开始运行。按屏幕上的指示创建一份备份文件或从备份文件中恢复 Management Configuration（管理设置）。

3 完成本程序后，右击 Windows 工具条上的 Management Server 图标并选择 **Start Service（启动服务）**。

## 将 WatchGuard Management Server 转移至新的电脑

如需将 Management Server（管理服务器）转移至新的电脑，您必须知道主加密密钥，还必须确保新的 Management Server 获得与以前的管理服务器相同的 IP 地址。

1 用 Management Server Backup/ Restore Wizard（管理服务器备份 / 恢复向导）：
- 创建当前 Management Server 配置的备份文件
- 在新的 Management Server 上安装 Management Server 软件
- 用 WatchGuard® System Manager 安装文件并安装 Management Server 软件。

2 运行 Restore（恢复）向导并选择已备份的文件。

3 在 Windows 工具条中右击 Management Server 图标并选择 **Start Service（启动服务）**。

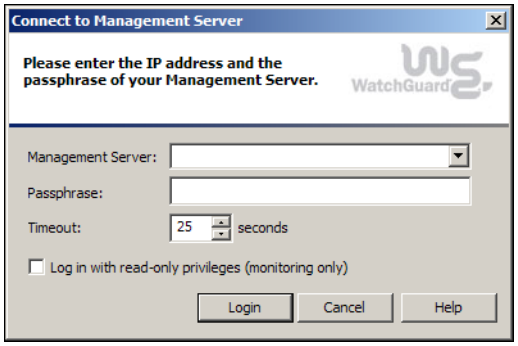
# 第 16 章 管理服务器的使用

完成对管理服务器的安装及配置后，你可以用管理服务器管理 VPN 隧道及多个 Firebox® 设备。你可以用管理服务器管理及配置 Firebox X Edge 设备。详情请检阅 “*管理 Firebox X Edge 及 Firebox SOHO*”章节。

## 连接到管理服务器

1 选择 **File（文件）>Connect to Server（连接到服务器）**。
或
右键点击 WSM 窗口的任何地方，选择 **Connect to（连接到）> Server（服务器）**。

或
点击 WSM 系统管理器工具条上的 Connect to Server （连接到服务器）图标。该图标将显示于左侧。




2 从 **Management Server （管理服务器）**下拉菜单中按照其名称及 IP 地址选择一台服务器。
如有必要，你也可以键入 IP 地址或主机名称。
在键入 IP 地址时，请键入所有的数字及期间。请勿使用 TAB 及箭头键。

3 为管理服务器键入口令。

4 如有必要，改变 **Timeout （超时间隔）**字段中的数值。该数值是指管理服务器在发出（指示不能连接）的消息之前 WSM 从管理服务器接收数据的时间（秒）。

如果你的网速或因特网与该设备的连接较慢，你可以增加超时间隔的数值。如果减小该数值，则你相应减小了在无法连接到一台管理服务器时，等待连接超时提示消息的时间。

5 如果你仅将服务器用作监控流量，请选择 **Monitoring Only （仅作监控用）**复选框。如果你必须配置服务器或其受管理的设备，请不要选择此复选框。

6 点击 **OK （确认）**。
服务器将出现在 WSM 窗口中。

**注释**

在某些先前版本的 WatchGuard 安全产品中， WSM 被称为 DVCP 服务器。

### 断开与服务器的连接

要断开与服务器的连接，请点击管理服务器名称并选择 **File （文件）>Disconnect**（断开）。或在树形图中选择管理服务器，然后点击左侧的 Disconnect （断开）图标。

## 用管理服务器管理各种设备

要用 Management Server （管理服务器）管理一台 Firebox，你必须：

- 确定 Firebox 允许与管理服务器进行管理连接；
- 对于任何带有动态外部 IP 地址的 Firebox，将 Firebox 相互激活为托管客户端；
- 将 Firebox 添加到管理服务器配置中。

如果你使用不同的 Firebox 应用软件或不同的 Firebox 型号，则你在将 Firebox 激活为托管 Firebox 客户端时所用到的指示也将有所不同。如果托管 Firebox 客户端带有动态 IP 地址，则上述指示也将有所不同。在阅读下述章节时，请确定与你的 Firebox 配置相匹配的内容。

### 将 Firebox X Core 或 X Peak Running Fireware 作为托管客户端进行配置

1 为你想将其作为托管客户端进行配置的 Firebox 打开 Policy Manager （策略管理器）。

2 双击 **WatchGuard** 政策，将其打开并进行编辑。
屏幕将出现为 WatchGuard 政策 Edit Policy Properties （编辑政策属性）对话框。

3 确定将 **WatchGuard-Firebox-Mgmt connections are （WatchGuard-Firebox-Mgmt 联接为）**下拉列表设置为 **Allowed （允许）**。

4 在 **From （从）**对话框下方，点击 **Add （添加）**。点击 **Add Other （添加其它）**。

5 确定将 **Choose Type （选择类型）**下拉列表设置为 **Host IP （主机 IP）**。在 **Value （数值）**字段，键入网关 Firebox 外部接口的 IP 地址，该网关 Firebox 用于向管理服务器提供因特网连接保护。
如果你没有向管理服务器提供因特网连接保护的网关 Firebox，则应键入管理服务器的静态 IP 地址。

6 点击 **OK （确认）**。再次点击 **OK （确认）**。

7 确定 **To （到）**对话框包括有 **Firebox** 或 **Any （任何）**条目。

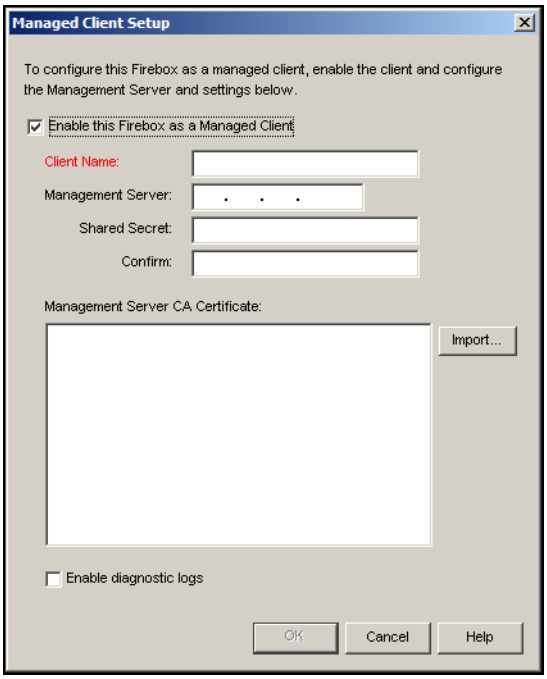
**注释**

如果你想管理的 Firebox 在其外部接口上有一条静态 IP 地址，则你可以于此停止。将配置保存到此 Firebox。此时，你可以将该设备添加到你的管理服务器配置中。当你将此 Firebox 添加到你的管理服务器配置中时，管理服务器将自动连接到静态 IP 地址，并将该 Firebox 配置为托管 Firebox 客户端。

如果你想管理的 Firebox 具有一条动态 IP 地址，则应按照步骤 8 操作。

8 在策略管理器中选择 **VPN>Managed Client（托管客户端）**。

屏幕将出现 Managed Client Setup（托管客户端安装）对话框。




9 要将一台 Firebox 设置为托管设备，应选择 **Enable This Firebox as a Managed Client（将此 Firebox 激活为托管客户端）**复选框。

10 在将 Firebox 添加到管理服务器配置后，在 **Client Name（客户端名称）**对话框中为此 Firebox 键入名称。

此名称为大小写敏感字段，因此必须与你在将该设备添加到管理服务器配置中时使用的名称完全匹配。

11 要启用托管客户端，让其向日志服务器发送日志消息，请选择 **Enable diagnostic logs（激活诊断日志）**复选框。（我们建议仅在排除故障时使用此选项）。

12 如果管理服务器有公开 IP 地址，在 **Management Server（管理服务器）**地址框中键入管理服务器的 IP 地址。或键入 Firebox（该 Firebox 用于保护管理服务器）的公开 IP 地址。

用于保护管理服务器的 Firebox 将自动监控管理服务器使用的所有端口，并将此等端口上的所有连接转接到经配置的管理服务器。在你运行管理服务器安装向导时，向导将提示你对用于保护管理服务器的 Firebox 进行上述配置。

如果你没有在管理服务器上使用管理服务器安装向导，或你在安装向导中跳过了“网关 Firebox”步骤，你需要对网关 Firebox 进行配置，使其将 TCP 端口 4110、4112 及 4113 转接到管理服务器的私有 IP 地址。

13 在 **Shared Secret（共享密钥）**框中键入共享密钥。再次键入，以兹确认。

你在此处键入的共享密钥必须与你在将 Firebox 添加到管理服务器配置中时键入的共享密钥完全匹配。

14 点击 **Import（导入）**按钮，将 CA-Adimin.pem 文件作为你的证书导入。

15 点击 **OK（确认）**。
将配置保存到 Firebox 中之后， Firebox 将作为托管客户端被激活。托管 Firebox 客户端将尝试连接到管理服务器在 TCP 端口 4110 上的 IP 地址。系统将允许从管理服务器到此托管 Firebox 客户端的管理连接。

## 将 Firebox III 或 Firebox X Core Running WFS 作为托管客户端进行配置

1 为你想将其作为托管客户端进行配置的 Firebox 打开 Policy Manager （策略管理器）。

2 双击 **WatchGuard** 服务，将其打开并进行编辑。
屏幕将出现为 WatchGuard 政策 Edit Service Properties （编辑服务属性）对话框。

3 在 **Incoming（来访）**选项卡中，确定来访 WatchGuard 连接被设置为 **Enabled and Allowed（已激活和允许）**。

4 在 **From（从）**对话框下方，点击 **Add（添加）**。点击 **Add Other（添加其它）**。

5 确定将 **Choose Type（选择类型）**下拉列表设置为 **Host IP Address（主机 IP 地址）**。在 **Value（数值）**字段，键入网关 Firebox 外部接口的 IP 地址，该网关 Firebox 用于向管理服务器提供因特网连接保护。
如果你没有向管理服务器提供因特网连接保护的网关 Firebox，则应键入管理服务器的静态 IP 地址。

6 点击 **OK（确认）**。再次点击 **OK（确认）**。

7 确定 **To（到）**对话框包括有 **Firebox 或 Any（任何）**条目。

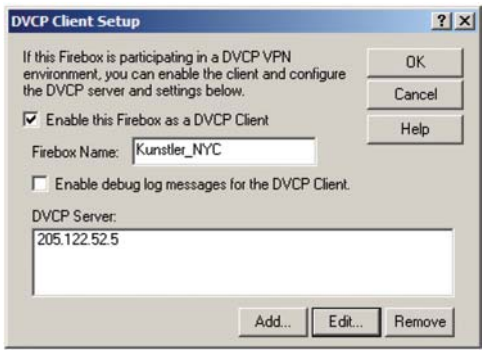
**注释**

如果你想管理的 Firebox 在其外部接口上有一条静态 IP 地址，则你可以于此停止。将配置保存到此 Firebox。此时，你可以将该设备添加到你的管理服务器配置中。当你将此 Firebox 添加到你的管理服务器配置中时，管理服务器将自动连接到静态 IP 地址，并将该 Firebox 配置为托管 Firebox 客户端。
如果你想管理的 Firebox 具有一条动态 IP 地址，则应按照步骤 8 操作。

8 在策略管理器中选择 **Network>DVCP Client（托管客户端）**。

9 选择 **Enable this Firebox as a DVCP Client（作为 DVCP 客户端激活此 Firebox）**复选框。

10 在 **Firebox Name（Firebox 名称）**字段，键入 Firebox 的名称。
此名称为大小写敏感字段，因此必须与你在将该设备添加到管理服务器配置中时使用的名称完全匹配。




11 要为托管客户端发送日志消息，请选择 **Enable debug log messages for DVCP Client（为 DVCP 客户端激活排除故障日志消息）**复选框。（我们建议仅在排除故障时使用此选项）

12 点击 **Add（添加）**，添加 Firebox 与其相连的管理服务器。在 **DVCP Server（DVCP 服务器）**地址框中键入管理服务器的 IP 地址（如果管理服务器有公开 IP 地址）。或键入 Firebox （该 Firebox 用于保护管理服务器）的公开 IP 地址。键入连接到 Firebox 时使用的 **Shared Secret（共享密钥）**。你在此处键入的共享密钥必须与你在将 Firebox 添加到管理服务器配置中时键入的

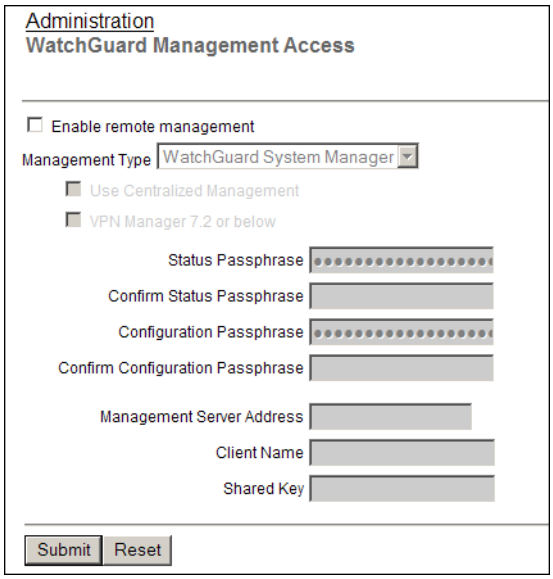
共享密钥完全匹配。
一台 Firebox 仅可作为一台管理服务器的一个客户端。
用于保护管理服务器的 Firebox 将自动监控管理服务器使用的所有端口，并将此等端口上的所有连接转接到经配置的管理服务器。在你运行管理服务器安装向导时，向导将提示你对用于保护管理服务器的 Firebox 进行上述配置。如果你没有在管理服务器上使用管理服务器安装向导，或你在安装向导中跳过了 “网关 Firebox” 步骤，你需要对网关 Firebox 进行配置，使其将 TCP 端口 4110、 4112 及 4113 转接到管理服务器的私有 IP 地址。

13 点击 **OK（确认）**。
将配置保存到 Firebox 中之后， Firebox 将作为托管客户端被激活。托管 Firebox 客户端将尝试连接到管理服务器在 TCP 端口 4110 上的 IP 地址。系统将允许从管理服务器到此托管 Firebox 客户端的管理连接。

## 将 Firebox X Edge 作为托管客户端进行配置

1 要进入 Firebox X Edge System Status （Firebox X Edge 系统状态）页面，请在浏览器地址条中键入 https:// 以及 Edge 受信网站的 IP 地址。
默认 URL 为 https://192.168.111.1。

2 在导航条中选择 **Administration（管理）>WSM Access（WSM 访问权限）**。
屏幕将出现 WatchGuard Management Access （WatchGuard 管理权限）页面。




3 选择 **Enable remote management（激活远程管理）**复选框。

4 从 **Management Type（管理类型）**下拉列表中选择 WSM。

5 点击 **Use Centralized Management（使用集中管理）**复选框，让 WSM Edge 集中管理系统控制 Firebox X Edge。如果你仅将 WSM 用作管理 VPN 隧道，请勿选择 **Use Centralized Management（使用集中管理）**复选框。
在 Firebox X Edge 受到集中管理后， Firebox X Edge 配置页面将被设置为只读模式。例外（非只读模式）仅限于 WSM Access （WSM 访问权限）配置页面。如果你选择禁用远程管理功能，则你再次获得读 – 写 Firebox X Edge 配置页面的权限。

6 为你的 Firebox X Edge 键入一条状态口令，然后在正确的字段再次键入该口令，以兹确认。

7 为你的 Firebox X Edge 键入一条配置口令，然后在正确的字段再次键入该口令，以兹确认。
此等口令必须与你在将设备添加到管理服务器时使用的口令完全匹配，否则连接将失败。

**注释**

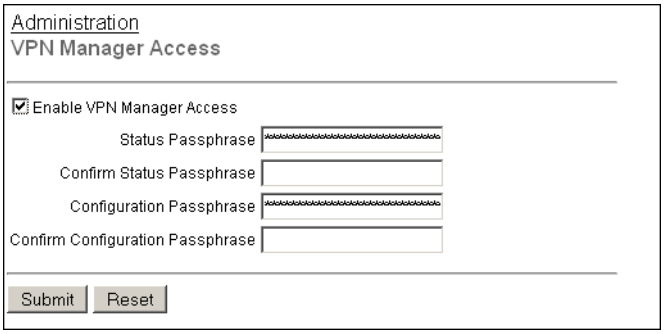
如果你想管理的 Firebox X Edge 在其外部接口上有一条静态 IP 地址，则你可以于此停止。将配置保存到此 Firebox。此时，你可以将该设备添加到你的管理服务器配置中。当你将此 Firebox 添加

到你的管理服务器配置中时，管理服务器将自动连接到静态 IP 地址，并将该 Firebox 配置为托管 Firebox 客户端。
如果你想管理的 Firebox 具有动态 IP 地址，则应按照步骤 8 操作。

8 如果管理服务器带有一条公开 IP 地址，在 **Management Server（管理服务器）**文本框中键入该管理服务器的 IP 地址。如果管理服务器带有一条私有 IP 地址，键入 Firebox （该 Firebox 用于保护管理服务器）的公开 IP 地址。
用于保护管理服务器的 Firebox 将自动监控管理服务器使用的所有端口，并将此等端口上的所有连接转接到经配置的管理服务器。在你运行管理服务器安装向导时，向导将提示你对用于保护管理服务器的 Firebox 进行上述配置，因此无需进行其它任何特殊配置。
9 为你的 Edge 键入 **Client Name （客户端名称）**，以便在管理服务器中识别 Edge。
此名称为大小写敏感字段，因此必须与你在将该设备添加到管理服务器配置中时使用的名称完全匹配。
10 键入 **Shared Key （共享密钥）**。
此共享密钥用于对管理服务器与 Firebox X Edge 之间的连接进行加密。此共享密钥必须与 Edge 及管理服务器上的密钥完全一致。你必须从你的 [ 管理服务器 ] 管理员处取得共享密钥。
11 点击 **Submit （提交）**将此配置保存到 Firebox X Edge。
将配置保存到 Edge 之后， Edge 将作为托管客户端被激活。托管 Firebox 客户端将尝试连接到管理服务器的 IP 地址。系统将允许从管理服务器到此托管 Firebox 客户端的管理连接。

## 将 Firebox SOHO 6 作为托管客户端进行配置

1 启动你的浏览器。键入 SOHO 6 的 IP 地址。
2 如果必须输入 SOHO 6 的用户名及口令，请键入用户名及口令。
3 在 Administration （管理）下方点击 **VPN Manager Access （VPN 管理器访问权限）**。
屏幕将出现 VPN Manager Access （VPN 管理器访问权限）页面。




4 在 VPN 下方的左导航窗格中，点击 **Managed VPN （托管 VPN）**。选择 **Enable VPN Manager Access （激活 VPN 管理器访问权限）**复选框。
5 为 VPN 管理器的访问权限键入状态口令。再次键入状态口令，以兹确认。
6 为 VPN 管理器的访问权限键入配置口令。再次键入状态口令，以兹确认。

**注释**

如果你想管理的 SOHO 在其外部接口上有一条静态 IP 地址，则你可以于此停止。将配置保存到此 SOHO。此时，你可以将该设备添加到你的管理服务器配置中。当你将此 SOHO 添加到你的管理服

务器配置中时，管理服务器将自动连接到静态 IP 地址，并将该 SOHO 配置为托管 Firebox 客户端。如果你想管理的 SOHO 具有一条动态 IP 地址，则应按照步骤 7 操作。

7 选择 **Enable Managed VPN（激活托管 VPN）**复选框。

8 从 **Configuration Mode（配置模式）**下拉列表中选择 **SOHO**。

9 如果管理服务器有一条公开 IP 地址，在 **DVCP Server Address（DVCP 服务器地址）**文本框中键入该管理服务器的 IP 地址。如果管理服务器有一条私有 IP 地址，键入 Firebox（该 Firebox 用于保护管理服务器）的公开 IP 地址。

用于保护管理服务器的 Firebox 将自动监控管理服务器使用的所有端口，并将此等端口上的所有连接转接到经配置的管理服务器，因此无需进行其它任何特殊配置。

10 为你的 Firebox SOHO 键入 **Client Name（客户端名称）**。

此名称为大小写敏感字段，因此必须与你在将此 Edge 添加到管理服务器配置中时使用的名称完全匹配。

11 键入 **Shared Key（共享密钥）**。

此共享密钥用于对管理服务器与 Firebox SOHO 之间的连接进行加密。此共享密钥必须与 SOHO 及管理服务器上的密钥完全一致。你必须从你的 Management Server 管理员处取得共享密钥。

12 点击 **Submit（提交）**。

将配置保存到 Firebox SOHO 之后， SOHO 将作为托管客户端被激活。托管 SOHO 客户端将尝试连接到管理服务器的 IP 地址。系统将允许从管理服务器到此托管 SOHO 客户端的管理连接。

## 将设备添加到管理服务器

你可以用 Management Server（管理服务器）配置及管理以下 Firebox® 设备之间的 VPN 隧道，包括各种使用 WFS 应用软件的 Firebox III 及 Firebox X Core 设备、使用 Fireware® 应用软件的 Firebox X 设备、 Firebox X Edge 设备以及 Firebox SOHO 设备。

如果是一台带有动态 IP 地址的设备，你也必须在该设备的策略管理器中将其配置为托管客户端（请参阅上一章）。

如果你的设备具有多个外部接口，请不要在将该设备添加到管理服务器之后改变该接口的配置。

**注释**

通过管理服务器，你也可以部署、管理及监控各个 Firebox X Edge 设备。详情请参阅 “*Managing the Firebox X Edge and Firebox SOHO（管理 Firebox X Edge 及 Firebox SOHO）*”章节。

1 在 WSM 中，建立与 Management Server（管理服务器）的连接。

选择 File（文件）>Connect to Server（连接到服务器），或选择 Device Status（设备状态）选项卡。

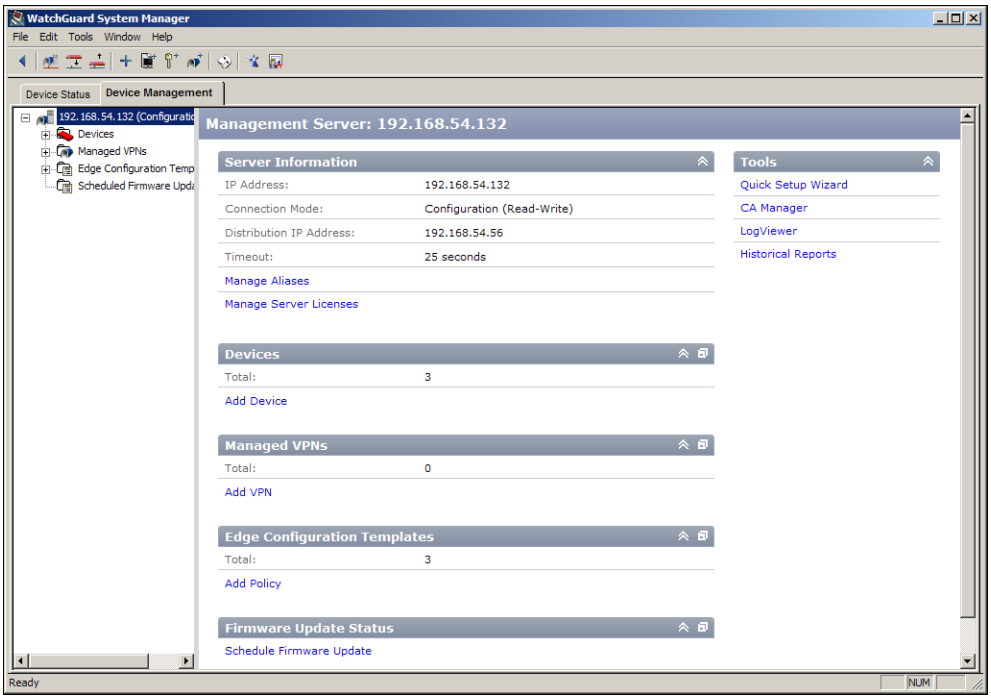
或

在窗口任意一处点击右键，然后选择 Connect to（连接到）>Server（服务器）。

2 键入或选择管理服务器的 IP 地址，键入口令，然后点击 **Login（登陆）**。

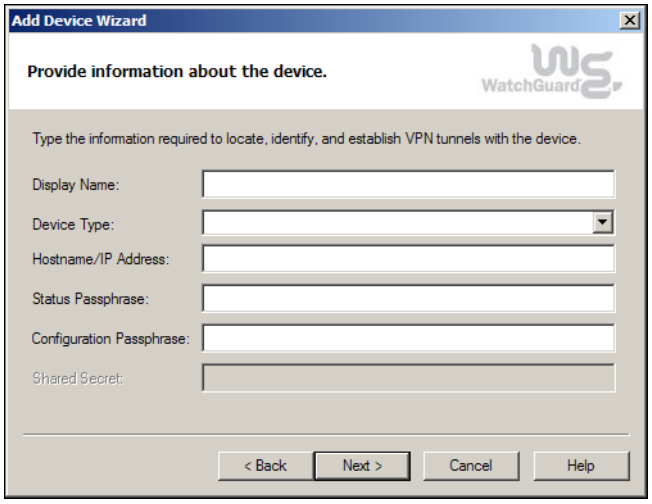
3 点击 **Device Management（设备管理）**选项卡。

4 从窗口左侧的列表中选择管理服务器。
屏幕将出现管理服务器页面。




5 展开 **Devices（设备）**文件夹。
由该管理服务器管理的设备均显示于此。

6 选择 **Edit（编辑）>Insert Device（插入设备）**，或右键点击该窗口的左边框，选择 **Insert Device（插入设备）**。
Add Device（添加设备）向导将被启动。




7 点击 **Next（下一步）**查看第一配置界面。

8 在 **Display Name（显示名称）**文本框中键入该设备的名称。
该名称不能包括任何空格或标点符号。

9 从 **Device Type（设备类型）**的下拉列表中选择你想将其添加到管理服务器配置中的 Firebox 型号。

10 在 **Hostname/IP address（主机名 /IP 地址）**文本框中键入 Firebox 的静态 IP 地址或主机名称。如果是使用动态 IP 地址的设备，请键入动态 DNS 服务客户端的名称。

如果该设备带有动态 IP 地址但未使用动态 DNS 服务，请为该设备键入一个唯一的用户名。你在此处键入的用户名必须与你在策略管理器中为该设备输入的用户名相匹配（如果该设备是 Firebox III、 Firebox X Core 或 X Peak）。如果该设备是 Firebox X Edge 或 SOHO，则该用户名必须与你在使用 web 配置管理器将该设备作为托管客户端激活时所赋予该设备的名称相匹配。

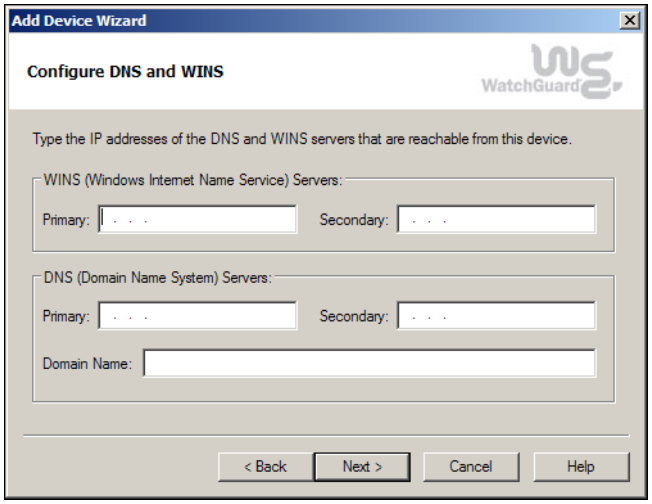
11 键入状态口令。该口令是你在将 Firebox 添加到管理服务器中时为该 Firebox 设置的状态（只读）口令。

12 键入配置口令。该口令是你在将 Firebox 添加到管理服务器中时为该 Firebox 设置的配置（读写）口令。

13 如果该 Firebox 使用动态 IP 地址，请键入共享密钥。你在此处键入的共享密钥必须与你键入到设备配置中的共享密钥完全一致（在你将该设备作为托管客户端激活时）。

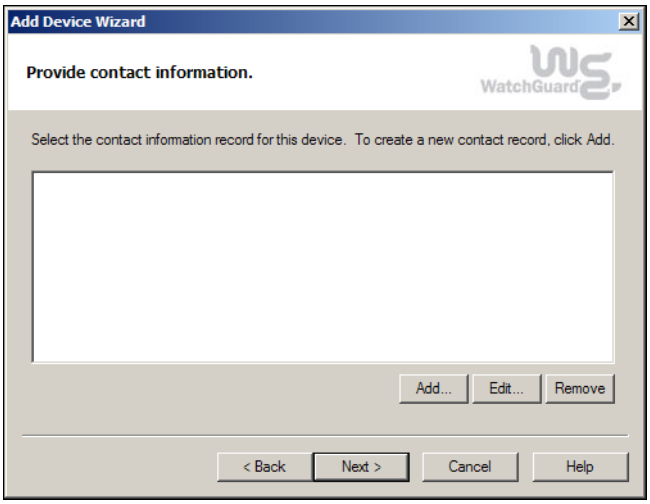
14 点击 **Next（下一步）**。

屏幕将出现 Configure WINS 及 DNS（配置 WINS 及 DNS）界面。




15 为此设备使用的 WINS 及 DNS 服务器键入第一及第二（如有）地址。

16 为此设备键入域名（如有）。点击 **Next（下一步）**。
屏幕将出现 Provide Contact Information（提供联系信息）界面。




17 你可以为此设备选择现有的联系记录，或点击 **Add（添加）**为此设备添加新的联系记录。你也可以删除一条现有的联系记录，具体操作为：选择该记录并点击 **Delete（删除）**。

18 点击 **Next（下一步）**。屏幕将出现 Configure Device（配置设备）界面。在该界面中点击 **Next（下一步）**，使用新的管理设置对该设备进行配置，并将其添加到管理服务器。如果该设备受另一个服务器管理，或已经通过本服务器进行了配置，则屏幕会弹出警告性对话框。点击 **Yes（是）**继续。

19 点击 **Close（关闭）**，关闭 Add Device（添加设备）向导。
在添加完一台使用动态 IP 地址的 Firebox 之后，你必须重启该 Firebox，以便 Firebox 可以连接到管理服务器并实现相应配置。

**注释**

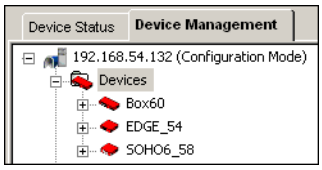
如果流量过大， Add Device（添加设备）向导可能由于 SSL 超时间隔而无法连接。在此情况下，请在系统荷载量降低后重新连接。

## 使用设备管理页面

在将一台 Firebox® 安装到一台管理服务器后，你可以使用 **Device Management（设备管理）**选项卡上的信息及字段对设备上的各项设置进行配置。有关如何将设备添加到管理服务器的更多信息，请参阅第 213 页的 “*将设备添加到管理服务器*”。

## 查看 Firebox 管理页面

1 在 WSM 的 **Device Management**（**设备管理**）选项卡中，展开 **Devices**（**设备**）。
屏幕将显示托管设备列表。



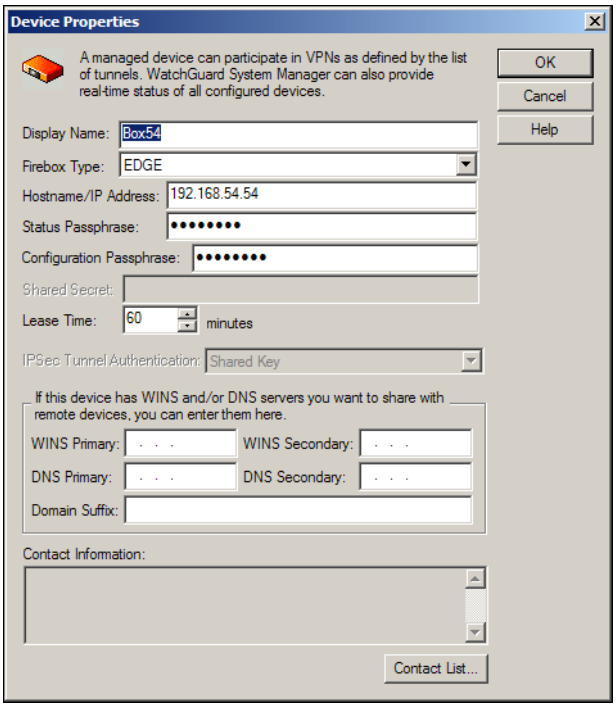

2 选择一台 Firebox X Edge。屏幕将出现该设备的管理页面。


**注释**

一台 Firebox X 设备的管理页面允许你访问各种不同的工具并配置更多的选项。有关 Firebox X Edge 管理的详情请参阅 “*管理 Firebox X Edge 及 Firebox SOHO*”章节。

## 配置 Firebox 管理属性

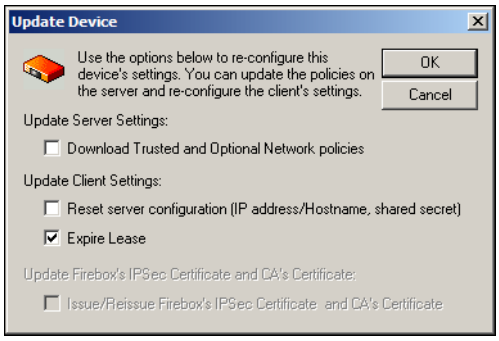
1 在 Firebox 管理页面上点击 **Configure （配置）**。
屏幕将弹出 Device Properties （设备属性）对话框。




2 为该设备配置管理属性。

## 设备更新

1 在 Firebox X Edge 管理页面之上点击 **Update Device （更新设备）**。
屏幕将出现 Update Device （更新设备）对话框。



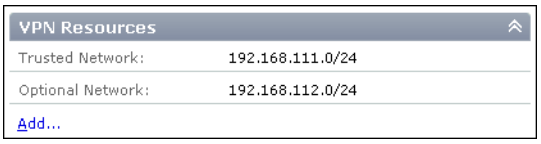

2 你可以通过使用该对话框从该设备中获得策略，为该设备重新设置管理服务器配置选项，并将管理协议作废。你也可以使用该对话框更新 Firebox 证书及 CA 证书 （如果该证书已被变更）。

3 点击 **OK （确认）**。

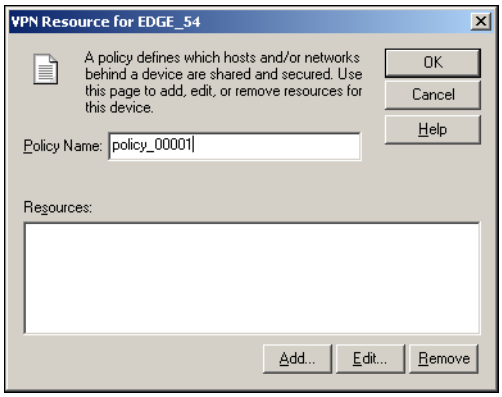
## 添加 VPN 资源

VPN 资源是指 VPN 用户可以连接的安全 IP 地址或网络地址。

1 在 **Device Management**（**设备管理**）选项卡中找见 **VPN Resources**（**VPN 资源**）。




2 点击 **Add**（**添加**）。




3 用相应的按钮添加、编辑或去除 VPN 资源。

4 点击 **OK**（**确认**）。
新的 VPN 资源将出现在列表上。

## 启用 Firebox 工具

**Device Management**（**设备管理**）选项卡允许你为 Firebox 的配置及监控启用四种工具：

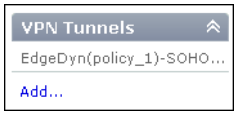
- 策略管理器
- Firebox 系统管理器
- HostWatch
- Ping

如需启用这些设备，则应在 Firebox 管理页面上的 Tools（工具）栏中点击工具连接。

### 添加 Firebox VPN 隧道

Firebox X Edge 管理页面将显示所有隧道（该设备为该等隧道的端点）。你也可以在此处添加一个 VPN 隧道。

1 在 Firebox 管理页面上找见 VPN Tunnels（VPN 隧道）。




2 点击 **Add（添加）**添加新的 VPN 隧道。
Add VPN（添加 VPN）向导将被启动。按照向导的提示配置 VPN。

## 监控 VPNs

手动配置的 VPN 列示于每一 Firebox® 的 Device Status（设备状态）选项卡中。在管理服务器中自动创建的托管 VPN 将出现在 **Device Management（设备管理）**选项卡中。

使用策略管理器手动创建的 VPN 政策将显示于 **Device Management（设备管理）**选项卡中。

# 第 17 章　管理证书及认证中心

在创建 VPN 隧道时，你可以对两种隧道认证方式进行选择：共享密钥或证书。共享密钥是一种用于在 VPN 中的各个电脑之间创建信任关系的一种认证方法。共享密钥与口令连用。与共享密钥相比，证书通常可以为整个认证流程提供更多安全保障。

证书是载有一把公共密钥的一份电子文件。认证中心（CA）是向客户提供证书的受信第三方。在 WSM 中，作为 Management Server（管理服务器）实现配置的工作站也充当认证中心的功能。在托管 Firebox® 客户端通过联系管理服务器而接收配置更新时，认证中心可以将证书发送给该等客户端。

认证中心是密钥生成、密钥管理及密钥认证系统的组成部分（名称为公共密钥基础结构 [PKI]）。PKI 提供可以创建、供应、保存及撤销（如有必要）各项证书的证书及目录服务。

## 公共密钥加密术及证书

公共密钥加密术是 PKI 的核心部分。此加密系统包括两条数字上相关联的密钥（又称非对称密钥对）。用户保存一把密钥，即私人密钥。用户可以向其它用户提供其它密钥，即公共密钥。

密钥对中的两把密钥相互依存。只有私有密钥的持有者才可以对公共密钥加密数据进行解密。任何公共密钥的持有者可以对私有密钥加密数据进行解密。

证书的作用是确定公共密钥仍然有效。证书包含于在生成认证中心（CA）证书的公共密钥时一同生成的数字签名中。你可以计算证书的数字签名，并与证书自身的数字签名进行比较。如果签名相互匹配，则该密钥为有效密钥。

证书在被创建时会取得证书有效期。但是证书经常在到达有效期之前被撤销。认证中心会保存一份作废证书的最新、在线列表。此列表称为作废证书列表（CRL）。

## WatchGuard VPN 中的 PKI

要使用证书认证 VPN 隧道，你必须首先配置管理服务器。在配置管理服务器时，认证中心会被自动激活。每一托管 Firebox® 客户端将连接到管理服务器，并从认证中心接收一份证书。在两个托

管客户端之间创建 VPN 隧道后，客户端将用证书认证该隧道。但是仅在上述两个托管 Firebox 客户端均被配置为使用证书认证时，上述功能方可实现。

### MUVPN 及证书

由于移动用户 VPN （ MUVPN ）客户端不是管理服务器的客户端，因此他们通过 Firebox 实现认证。用策略管理器中的 MUVPN Wizard （ MUVPN 向导 ）联通认证中心，并为 MUVPN 客户端生成一份证书。策略管理器将生成一个包括此证书及两分其它文件的文件包。

Firebox 管理员向每一 MUVPN 用户分发一个文件包。上述文件包和在一起就构成 MUVPN 终端用户的用户特征。通过共享密钥实现认证的用户将收到一份 .wgx 文件。通过证书实现认证的用户将收到一份 .wgx 文件、一份 .p12 文件 （ 该文件为客户端证书 ）及一份 cacert.pem 文件 （ 该文件包含根证书 ）。

通过证书实现认证的 MUVPN 用户将随后打开上述 .wgx 文件。包含自在 cacert.pem 及 .p12 文件中的根证书及客户端证书将被自动加载。

有关 MUVPN 的详情请参阅《MUVPN 管理员向导》。

## 管理认证中心

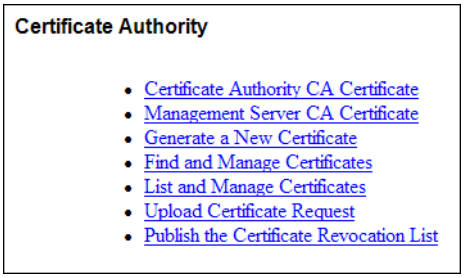
你可以用基于 web 的认证中心管理器控制认证中心的各种参数。

1 从 WSM 中连接到管理服务器。
你必须键入连接所需的配置口令。

2 为管理服务器点击 **Device Management （ 设备管理 ）**选项卡。

3 在 **Tools （ 工具 ）**菜单下方选择 **CA Manager （ 认证中心管理器 ）**。

或
在 WSM 工具条上点击认证中心管理器的图标。该图标位于左侧。
屏幕将出现 Certificate Authority Settings （ 认证中心设置 ）页面。




4 从菜单中选择正确的页面：

*认证中心 CA 证书*
将 CA （ 根 ）证书的一份拷贝件复制到屏幕上。你可以手动将其保存到客户端。

*管理服务器 CA 证书*
将一份管理服务器 CA 证书的拷贝件复制到屏幕。你可以手动将其保存到客户端。你可以在客户端访问认证 web 页面时使用此证书。

*生成新证书*

键入主题公用名、组织单位、密码及证书有效期，生成一份新证书。

– 如果是 MUVPN 用户，公用名必须与远程用户的用户名一致。

– 如果是 Firebox® 用户，公用名必须与 Firebox 的识别信息（通常是其 IP 地址）一致。

– 如果是普通证书，公用名应为用户的名称。

**注释**

请仅在为 MUVPN 用户生成证书时键入组织名称。请勿为其它类型的 VPN 隧道使用此选项。单位的名称必须符合以下格式：
GW:<*vpn gateway name*>
在此处，<vpn gateway name> 是 config.watchguard.id 在网关 Firebox 配置文件中的数值。

*搜索及管理证书*

提供可以在数据库中找见的一份证书的编号、公用名或组织单位。作为特殊证书的备选方案，你也可以仅搜索仍然有效的、已经撤销的或已经过期的证书。搜索结果将显示在 List Certificates（证书列表）页面。

*列示及管理证书*

查看数据库中的证书列表。选择要发放、撤销、恢复或移除的证书。有关如何管理证书的详情请参阅以下章节。

*上载证书请求*

使用此页签署并批准来自一台不同设备的证书请求。键入主题的公用名及组织单位，并点击 **Browse（浏览）**，查找 CSR（证书签批请求）文件。

*公布一份证书作废证书列表 (CRL)*

让认证中心向所有使用当前证书的客户端公布作废证书列表。如果托管 Firebox 客户端使用的证书包括在作废证书列表上，则该客户端无法创建 VPN 隧道。

## 用认证中心管理器管理证书

你可以用 List and Manage Certificate（列示及管理证书）页面公布、撤销、恢复或移除证书：

1 从 List and Manage Certificate（列示及管理证书）页面选择所要修改正书的编号。

2 从 **Choose Action（选择对策）**下拉列表中选择一种备选方案，然后选择 **GO（开始）**：

*Revoke Checked*

撤销一份证书。在 CRL 被公布之前，托管 Firebox 客户端不会将 CRL 视作已被撤销。

*Reinstate Checked*

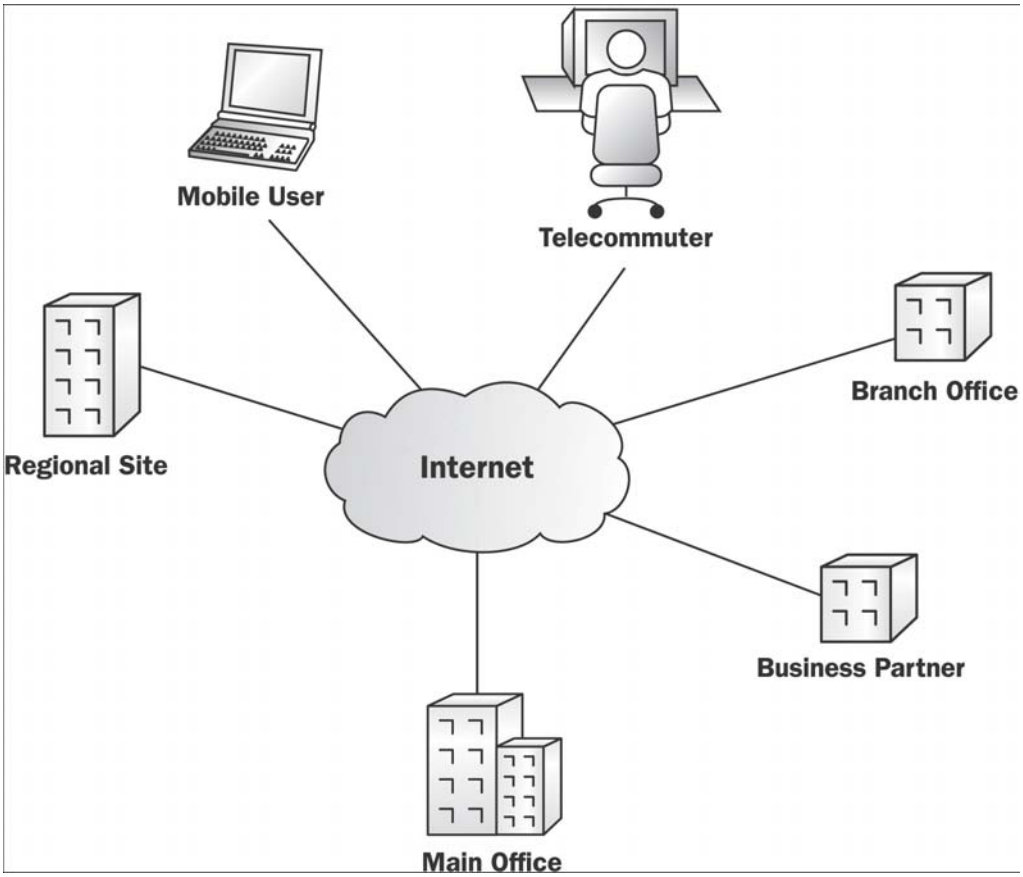
恢复先前已被撤销的证书。

*Destroy Checked*

移除一份证书。

# 第 18 章　VPN 简介

互联网是一种公共网络。在这个由电脑及网络组成的系统中，一台电脑可以从其它电脑取得各种信息。其他人有可能读取你在互联网上发送的未经安全处理的数据包。要在办公室、网络及用户之间通过互联网发送安全数据，你必须使用更为强大的安全防护功能。



虚拟专用网络（ VPN ）使用加密技术降低安全风险，并在互联网上保护专用信息的安全。虚拟专用网络可以让数据通过互联网在两个不同的网络之间安全流动。 VPN 可以确保主机与网络之间的安全连接。

位于 VPN 端点的网路及主机可以是公司总部、分支办事处以及远程用户。

VPN 隧道用认证方法检验消息发送人及接收人。如果认证信息正确，数据将被解密。只有消息发送人及接收人可以清晰读取该消息。

有关 VPN 技术的更多信息，请参阅 http://www.watchguard.com/support 的在线信息。

WatchGuard® 客服网站载有访问文档、基础性常见问题、高级常见问题以及 WatchGuard 用户论坛的各种链接。在使用某些功能时，你必须登陆技术支持网站。

# 隧道协议

隧道允许用户在不安全的网络（ 通常为互联网 ）上以安全数据包为载体发送数据。一条隧道是指一组安全协议、加密算法以及规则。隧道用此信息从一个端点到另一端点发送安全数据流。隧道允许用户从其它网络连接到资源及电脑。

隧道协议提供基础结构，并设置数据传输如何在隧道中发生。 WSM 支持的两条隧道协议分别为安全网络协议（ IPSec ）以及点对点隧道协议（ PPTP ）。装配 WatchGuard SSL VPN Firebox 系列产品后， WatchGuard 也可以支持 SSL VPN。

## IPSec

你可以用 IPSec 协议检验 IP 数据包并确定他们已获得认证。 IPSec 带有包括强大认证功能在内的多种安全功能，能够有效保护你在互联网上所传输信息的保密性。 IPSec 是一种适用于许多其它制造商系统的网络标准。

IPSec 两种保护数据完整性及保密性的协议。 AH （ 验证报头 ）协议是一种为数据完整性提供的解决方案。 ESP （ 封装安全载荷 ）协议可以确保数据的完整性及保密性。

## PPTP

点对点隧道协议（ PPTP ）是一种适用于不同厂家生产的多种系统的 VPN 安全标准。 PPTP 允许建立连接到公司网络及其它 PPTP 激活系统的隧道。 PPTP 的安全性不及 IPSec，而且不能同时确保两条网络的安全。 PPTP 只能用一个 IP 地址或网络确保另一 IP 地址的安全性。 PPTP 可以为公司网络提供比 IPSec 更便捷的低廉备选方案。

## 加密

在不安全的网络中，黑客可以很轻易就找到被传输的数据包。 VPN 隧道用加密方法确保数据安全。

加密密钥的长度连同所采用的加密方法将确定 VPN 的加密强度。密钥越长，加密级别就越高，安全性越强。你可以根据公司对网络性能及安全的实际要求，设定加密级别。通常，加密级别越高，安全性就越强，但网络性能就会有所降低。

如果传输的是非敏感数据，我们建议使用安全性较强、吞吐量适当的基础加密级别。如果是管理性或传输高度机密数据的连接，我们建议使用高强度加密级别。

通过隧道发送数据包的主机或 IPSec 设备将对数据包进行加密。隧道另一端的接收人将对数据包进行解密。两个端点的隧道配置参数必须完全一致，包括加密及认证方法、允许通过隧道发送数据的主机或网络、计算新密钥的时间间隔以及其它参数。

## 选择一种加密及保证数据完整性的方法

在选择加密及保证数据完整性的方法时，你需要衡量安全性及性能。我们建议为敏感数据采用最强加密方式 – 高级加密标准（AES）。 Fireware 采用 IPSec 的默认加密方法 – AES 256。

数据完整性确保 VPN 端点接收的数据与发送的数据完全一致。我们向两种类型的数据认证提供支持。一种是 128 比特 Message Digest 5（消息摘要 5）（MD5-HMAC）。第二种是 160 比特 Secure Hash Algorithm（安全散列算法）（SHA1-HMAC）。

## 认证

保证安全性的一个重要步骤是确保发件人及收件人均得到认证。共有两种方法：口令认证（又称共享密钥）以及数字证书。共享密钥是指隧道两端使用的同一口令。

数字证书使用公共密钥加密术识别及认证端点网关。你可以使用证书对 WSM 中创建的任何 VPN 隧道进行认证。有关证书的详情，请参阅 “*管理证书及认证中心*”章节。

## 扩展认证

对远程用户的认证可以通过保存到 Firebox 上的数据库或一台外部认证服务器实现。例如，拨入用户远程认证服务（RADIUS）即可作为一台外部认证服务器。认证服务器是认证网络上其它系统的安全第三方。如果是使用 IPSec 隧道协议的移动用户 VPN（MUVPN），远程用户必须在每次启动 VPN 时键入用户名及密码。

## 选择认证方法

VPN 的一个主要构成部分是用户认证方法。在安全使用共享密钥时，你必须确定：

- 让用户选择强密码。
- 经常变更密码。

在使用采用 PPTP 隧道协议或 MUVPN 的远程用户 VPN（RUVPN）时，使用强密码至关重要。如果 VPN 端点有风险，则整个网络也将有风险。例如，如果有人盗窃了一台笔记本电脑并破译了密码，则他可以直接访问你的网络。

数字证书是用于识别用户的电子记录。有关证书的详情请参阅 “*管理证书及认证中心*”章节。作为安全第三方的认证中心（CA）将管理各种证书。在 WSM 中，你可以将一台 Firebox 配置为认证中心。此类认证要比共享密钥更加安全。

## IP 寻址

在创建 VPN 隧道时，正确使用 IP 地址相当重要。我们建议不要在 VPN 隧道一端的电脑和 VPN 隧道另一端的电脑上使用同一专用 IP 地址。如果存在分支办事处，我们建议在每一处分支办事处采用不同于主办公网络的子网。如有可能，我们建议在设立分支办事处时采用与 Firebox® 子网基本相同的子网。

例如，如果主 Firebox 网络使用 192.168.100.0/24，则分支办事处应使用 192.168.101.0/24、192.168.102.0/24 等等。如此即可防止在扩展子网时可能产生的新问题，并帮助你记忆分支办事处的 IP 地址。

如果是 MUVPN 及 RUVPN 隧道， Firebox 将向每位远程用户提供一个虚拟 IP 地址。最方便的方法是提供源自主网络但未被其它电脑使用的虚拟 IP 地址。你不能为 RUVPN 及 MUVPN 远程用户提供相同的虚拟 IP 地址。你也不能使用可能被使用到主网络不同位置电脑上的虚拟 IP 地址。

如果主网络上的 IP 地址不能满足需要，最安全的解决方案是安装一个 “placeholder（占位器）”次级网络。为该次级网络选择一个地址范围，然后从地址范围内选择一条地址作为虚拟 IP 地址。如果你已经在主网络上建立了一个专用 IP 地址范围，你也可以扩展该网络范围。例如，你可以将 C 级网络 192.168.100.0/24 扩展为 B 级网络 192.168.0.0/16。

进行上述操作后，你可以从设定的地址范围内进行选择。此等地址与 Firebox 后台区使用的真实主机地址不存在任何冲突。如果你为 RUVPN 虚拟 IP 地址使用了上述操作流程，你必须配置客户端电脑，让其使用远程网络上的默认网关，或你必须在 VPN 隧道联通后手动添加路由，但该项并不适用于 MUVPN 客户端电脑。

## 互联网密钥交换（IKE）

随着网络中的 VPN 隧道数量不断增加，要管理各条隧道使用的大量会话密钥就显得越发困难。你必须经常更换密钥，以增强安全性。

互联网密钥交换（IKE）是 IPSec 使用的密钥管理协议。 IKE 使密钥协商及更换程序自动化。互联网安全协议及密钥管理协议（ISAKMP）是 IKE 密钥交换协议所依据的密码协议。 ISAKMP 使用双阶段程序创建 IPSec 隧道。在第一阶段，两台网关将为 VPN 数据流创建一条安全、经认证的隧道。在第二阶段，两台网关将交换密钥，就数据加密方法达成一致。

Diffie-Hellman 是 IKE 在为数据加密创建必要的密钥时使用的一种算法。Diffie-Hellman 群组是各种参数集。 Diffie-Hellman 群组可以让两条伙伴系统相互交换会话密钥并就此密钥达成一致。第 1 群组为 678 比特群组，而第 2 群组为 1024 比特群组。第 2 群组比第 1 群组更加安全，但在生成密钥时要耗费更多的处理机时间。

# 网络地址转化及 VPNs

通过网络地址转换（NAT），IP 数据包的源头及目标站将在 IP 数据包经过路由器或防火墙时得到修改。如果你在两台 VPN 网关之间使用 NAT，你必须在为各个设备之间创建 VPN 隧道时，将 ESP（而非 AH）用作认证协议。

如果你通过一台 Firebox®（IPSec 或 PPTP 通关）发送 IPSec 或 PPTP 数据流，则该 Firebox 可能会使用 1 对 1 NAT 发送数据流。

# 控制访问权限

由于 VPN 隧道可以让用户访问你计算机网络上的各种资源，因此你需要考虑特定类型的用户应该需要何种类型的资源。例如，你可以让一组合同雇员仅可以访问一条网络，而让你的销售员工能够访问所有网络。

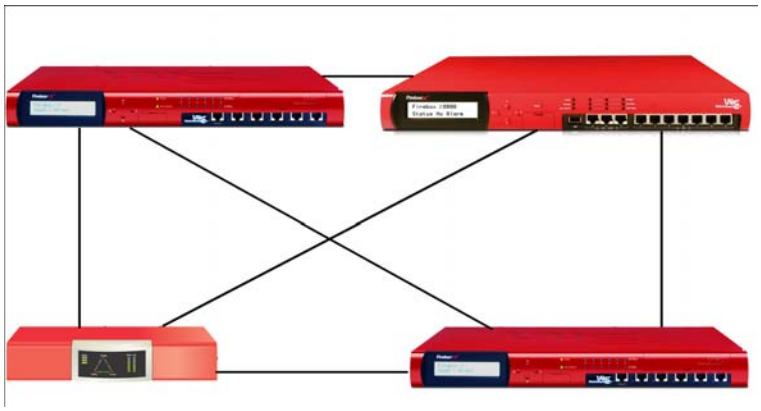
不同的 VPN 类型也可以设置你的受信级别。分支办事处的 VPNs（BOVPNs）在隧道的每一端点配备有一台防火墙设备。由于 MUVPN 及 RUVPN 仅在一端提供保护，因此它们比 MUVPN 及 RUVPN 更加安全。

# 网络拓扑

你可以配置 VPN，让其支持网状及中心辐射型配置。你选择的拓扑结构将设定连接的类型及数量，并设置数据流以及数据流的流量。

## 网状网络

在全网间拓扑结构中，所有服务器将被连接在一起，形成一个 web。每一设备仅作为另一 VPN 单元的一个中继点。如有必要，数据流可以在 VPN 的每一单元中流动。



网络拓扑

此拓扑结构能最大限度避免错误发生。如果一个 VPN 中断，只有该 VPN 与其受信站点之间的连接会被中断。但是此拓扑结构在建立时需要进行大量的工作。每一 VPN 单元必须与其它每一单元建立经配置的 VPN 隧道。如果稍有疏忽，就可能导致路由问题。

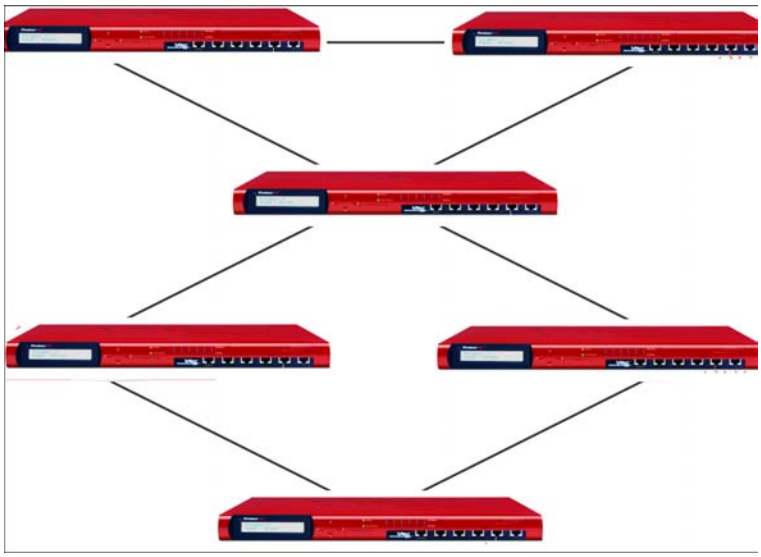
使用全网间拓扑结构的一个最大问题就是控制问题。由于网络中的每一单元都必须与其它单元建立连接，因此要建立隧道的数量将很快变得相当庞大。将要为此配置建立的隧道数量与设备数量的平方数相当。

[（设备数量）x（设备数量）] –1 ÷ 2= 隧道数量

如果所有 VPN 单元均为 WatchGuard 设备， WSM 可以让配置过程变得简短。管理服务器载有所有隧道所需的信息。通过 WSM，你可以通过拖放操作，用三个步骤创建一条两台设备之间的 VPN 隧道。通过一台 Firebox，你可以从多个位置监控整个系统的安全。大型公司采用此配置建立与其重要分支办事处之间的网络（每一分支办事处均使用较大容量的 Firebox® ）。小型办事处及远程用户可以通过 MUVPN、 RUVPN、 Firebox X Edge 或 SOHO 6 建立连接。

非全网间网络仅需要必要的辐射轴间 VPN 隧道（见下图）。因此，网络中的流量要优于全网间网络。所有网状网络均存在以下限制：

- 防火墙 CPU 可操控的 VPN 隧道数量。
- 此单元上 VPN 许可允许的 VPN 隧道数量。



部分网间网络

## 中心辐射型网络

在中心辐射型（hub-and-spoke）配置中，所有 VPN 隧道均停止于一个防火墙。小型公司通常通过主 Firebox 使用此配置。许多分布式远程用户通过 MUVPN、 RUVPN、 Firebox X Edge 或 SOHO 6 设备建立与此配置的连接。每一远程设备或远程用户仅创建连接到主 Firebox 的 VPN 隧道。

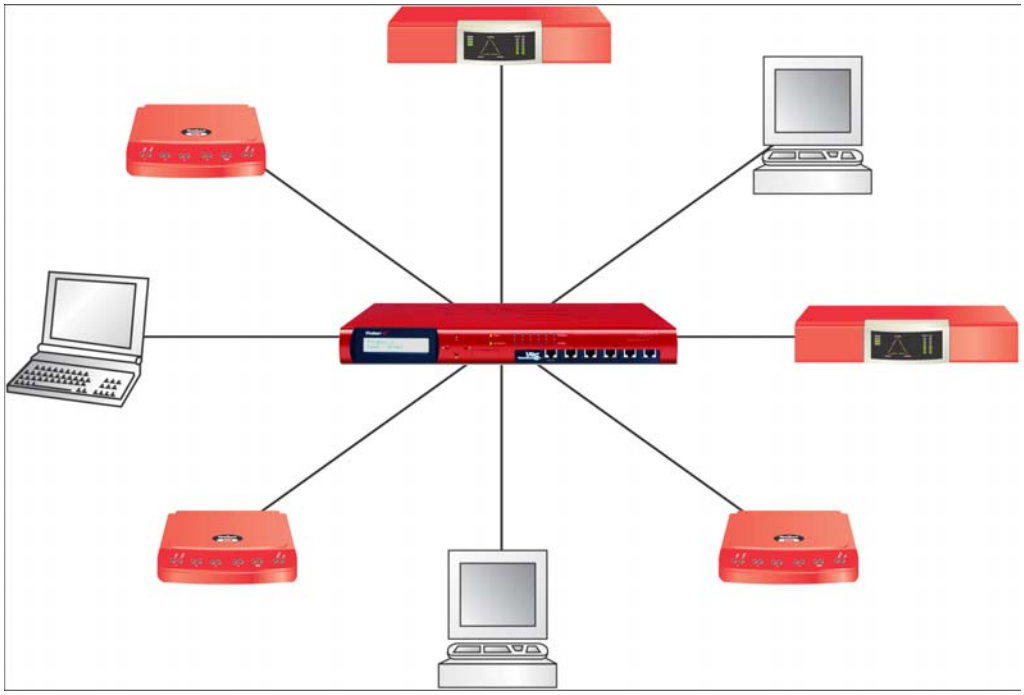
在简单的中心辐射型配置中，每一远程单元仅可以通过主 Firebox 之后的一条连接到网络的 VPN 隧道，发送及接收数据。你也可以将连接到主 Firebox 的 VPN 隧道配置为向一个不同的远程单元发送

或从该远程单元接收数据（隧道交换）。如果主 Firebox 从一个远程单元向另一远程单元发送数据包，则中心辐射结构中的流量密度可能增大。由于在简单的中心辐射结构中，远程单元仅可以通过一条 VPN 隧道将数据发送到主集线器单元，因此流量密度可能较低。由于主 Firebox 所有 VPN 隧道的端口所在，因此相当重要。如果主 Firebox 出现故障，你无法将任何 VPN 隧道连接到远程单元。

简单中心辐射型系统中的数据流流动轨迹要远比网状系统中的轨迹清晰。你可以更好控制隧道的数量。总数量如下：

[( 设备数量 )–1= 隧道数量 ]

如果需要增加中心辐射结构的容量，你需要扩展集线器单元。但是由于所有数据流都必须经过集线器，因此有必要分配更多带宽资源。



中心辐射型网络

## 隧道创建方法

当远程用户或端点可以在同一电脑上访问互联网时，可以用分割隧道法创建 VPN 连接。但是此用户无需让互联网数据流通过该隧道。远程用户直接通过 ISP 进行浏览。由于互联网数据流未经过滤或加密，因此采用分割隧道法的系统容易受到攻击。

如果该远程用户的所有互联网数据流都通过一条 VPN 隧道进入 Firebox®，此配置抵御攻击的能力将相对较强。然后，数据流将从 Firebox 发回到互联网（隧道交换）。通过此配置， Firebox 可以检验所有流量，提高网络安全性。在使用隧道交换功能时，动态 NAT 政策必须覆盖来自远程网络的向外数据流。如此，远程用户在将所有数据流发送到 Firebox 时就可以浏览互联网。

分割隧道法会降低网络安全性，而且不会提高网络性能。如果使用分割隧道法，远程用户必须为 VPN 端点后的电脑配备专用防火墙。

# WatchGuard VPN 解决方案

WSM 用此软件创建隧道：

- PPTP 远程用户 VPN （ RUVPN ）。
- IPSec 移动用户 VPN （ MUVPN ）。
- IPSec 分支办事处 VPN （ BOVPN ）（ 用策略管理器手动配置隧道设置 ）。
- IPSec 分支办事处 VPN （ BOVPN ）（ 用 WSM 手动配置隧道设置 ）。

WatchGuard 可以为你所创建的不同类型的 VPN 隧道提供不同类型的加密方法。BOVPN 允许采用各种级别的数据加密服务 （ DES ）：基础加密 （ 56 比特加密密钥 ）、中级加密 （ 112 比特密钥 ）以及强加密 （ 168 比特加密密钥 （ 3DES ））。 BOVPN 也允许采用高级加密标准 （ AES ），即一种使用 128 比特、 192 比特或 256 比特的数据块加密方法。

WatchGuard 也配备有一条单独的 SSL VPN Firebox 生产线。详情请参阅 WatchGuard 公共网站 http://www.watchguard.com/products/fb-ssl.asp。

## PPTP 远程用户 VPN

远程用户 VPN 允许远程用户或移动用户通过 PPTP 连接到 Firebox® 网络。 PPTP RUVPN 允许使用 RC4 40 比特或 128 比特密钥。

基础 WSM 套件包括 PPTP RUVPN。 PPTP RUVPN 可容纳 50 位用户并允许使用所有加密级别。有关如何创建 PPTP RUVPN 的详情请参阅 “*配置 PPTP RUVPN*” 章节。

## 移动用户 VPN

**注释**

有关如何配置及使用 MUVPN 的详情请参阅 MUVPN 管理员指南。

移动用户 VPN 是所有型号的 Firebox 都可以使用的可选软件组件。远程用户是指必须使用公司网络的流动性员工。 MUVPN 会在非安全性远程主机与你的公司网络之间创建一条 IPSec 隧道。远程用户首先用标准互联网拨号上网或宽带上网连接到互联网，然后通过 MUVPN 软件安全连接到 （ 受 Firebox 保护的 ）网络。使用 MUVPN 时，创建隧道仅需一台 Firebox。

MUVPN使用IPSec及DES或3DES对来访数据流进行加密，并使用MDS或SHA-1对数据包进行认证。你需要配置一项安全政策，然后将其连同 MUVPN 软件发送到每一远程用户。安全政策是一份扩展名为 wgx 的加密文件。在将软件安装到远程用户的电脑上之后，该等远程用户便可以安全连接到公司网络。 MUVPN 用户可以修改他们的安全政策，或者你也可以向他们提供只读安全政策。

## 分支办事处虚拟专用网络 （ BOVPN ）

许多公司在多处设有办事处。这些办事处经常使用其它办事处的数据，或者需要访问共享数据库。

由于分支办事处存在大量敏感数据，因此该等办事处之间的数据交换必须安全。在使用 WatchGuard 分支办事处 VPN 时，你可以在不降低安全性的情况下，通过互联网连接到两个或多个不同位置的办事处。 WatchGuard BOVPN 可以在两个不同的网络之间或一台 Firebox 与一台 IPSec 兼容设备之间提供加密隧道。你可以使用 WSM 或策略管理器配置 BOVPN。

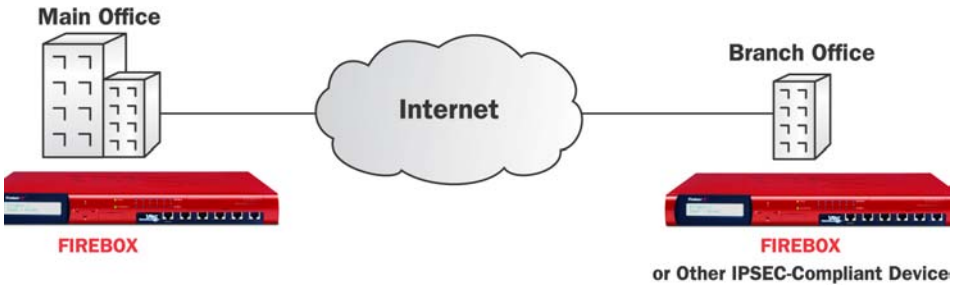
WatchGuard 允许 BOVPN 隧道使用基于证书的认证。如果你的 BOVPN 使用了基于证书的认证方式，则两个 VPN 端点都必须是 WatchGuard Firebox。如果是使用 SOHO 6 或 Firebox X Edge 设备的 BOVPN，你不能使用基于证书的认证。要使用此功能，你必须配置管理服务器及认证中心。详情请参阅第 169 页的 “*配置托管 VPN 隧道*”。有关如何使用策略管理器手动配置 BOVPN 隧道的详细信息，请参阅第 161 页的 “*用手动 IPSec 配置 BOVPN*”。

## 用策略管理器创建 BOVPN

在用策略管理器创建隧道时， Firebox 用 IPSec 创建连接到不同 IPSec 兼容安全设备的加密隧道。两个端点都必须具有一条共用静态 IP 地址。请在以下情况下用策略管理器创建 BOVPN：

- 在一台 Firebox 和一台非 WatchGuard IPSec 兼容设备之间创建隧道。
- 向不同的隧道提供不同路由政策。
- 限制通过隧道的数据流类型。

使用 IPSec 的 BOVPN 适用于 DES （ 56 比特 ）中等加密级别或更高加密解别的 3DES （ 168 比特 ）。BOVPN 也适用于 128 比特、192 比特以及 256 比特加密级别的 AES，其中 256 比特的 AES 最为安全。你可以在你的网络中为不同类型的流量创建不同的 VPN 隧道。例如，你可以为来自公司销售团队的数据流采用一条 DES 加密式 VPN 隧道，同时为来自公司财务部门的所有数据采用安全级别更高的 3DES 加密式 VPN 隧道。




使用手动 IPSec 的 BOVPN

## 用 WSM 创建 BOVPN

你可以在 WSM 中通过拖放操作或菜单界面创建全认证及全加密 IPSec 隧道。 WSM 通过管理服务器在两台 Firebox 设备之间安全传输 IPSec 配置信息。在使用管理服务器时，你需要设置每一 VPN 配置参数。管理服务器将保存此等信息。

请在以下情况下用 WSM 创建 BOVPN：

- 在两台或更多 Firebox 设备之间创建隧道。

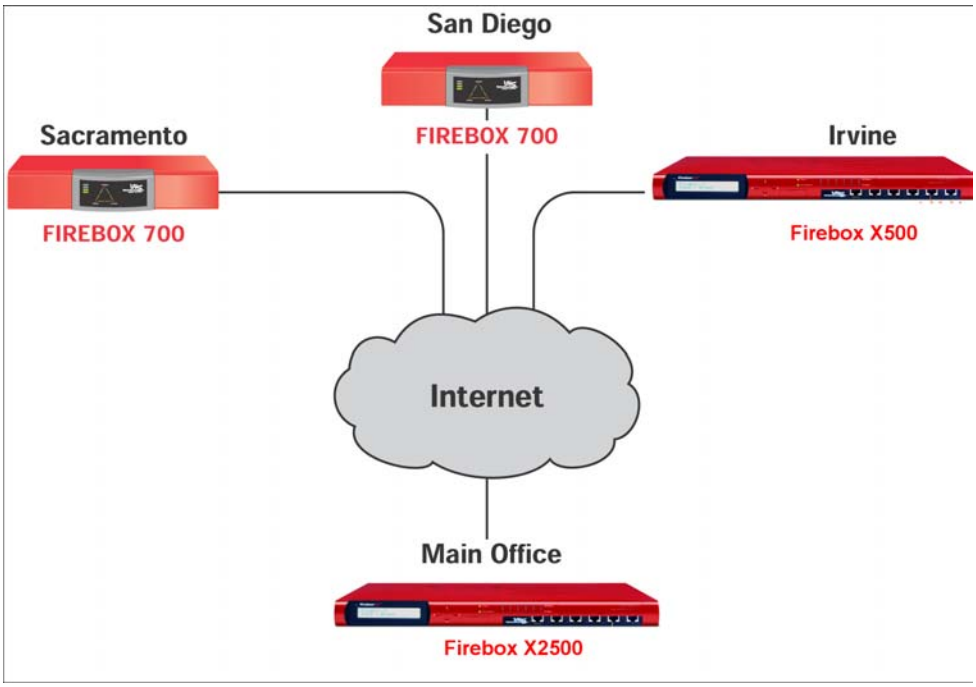
- 向不同的隧道提供不同的路由政策。
- 带有动态或静态共用 IP 地址的客户端单元。
- 需要创建数量庞大的隧道。

通过 WSM，你可以配置、管理及监控整个公司范围内的所有 WatchGuard 设备。你可以使用 WSM 向你提供的默认设置轻松配置两台远程设备之间的 VPN 隧道。你无需确定分支办事处及远程用户的互联网安全性。远程设备将连接到管理服务器，然后由管理服务器负责完成所有工作。如果为隧道采用证书认证方式，你可以将管理服务器配置为认证中心，由其自动生成证书。

# VPN 应用方法

本章节提供三种不同类型的公司及适用于每一类型公司的最佳 VPN 解决方案。

## 带有多个分支办事处的大型公司：WSM



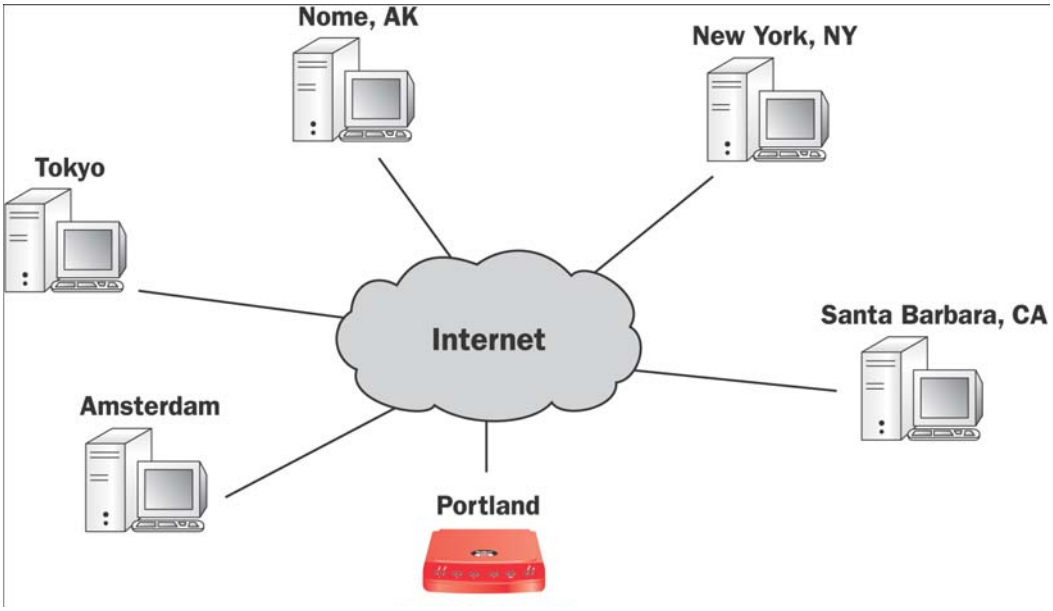

需要建立分支办事处 VPN 的大型公司

Gallatin 公司总部位于洛杉矶，约有 300 位用户，其分支办事处分别位于萨克拉曼多、圣地亚哥以及 Irvine，各自约有 100 位用户。所有办事处均可以快速连接到互联网，而且每一城市 / 地区的员工都必须建立能够访问其它地区办事处的安全连接。

此公司使用位于每一办事处的 WatchGuard Firebox® 以及 WSM 将所有办事处连接到一起。每一办事处都可以连接到所有其它办事处。每一办事处的员工都可以访问所有其它办事处的共享记录。管理服务器位于主办事处的 Firebox 的后台区，而分支办事处的 Firebox 为托管 Firebox 客户端。因此在 Gallatin 公司的互联网服务提供商停止提供服务时，公司总部的 Firebox 将停止运行，但其它办事处的隧道仍将处于运行状态。

## 使用 telecommuter （ 电传通信 ）的小型公司：MUVPN

River Rock Press 是一家专业市场中的小型出版社。该公司办事处设在俄勒冈波特兰，共有六名员工，而其它五名编辑都在其它位置。该公司总部使用一台 Firebox X Edge 作为防火墙及 VPN 网关。五名编辑各自使用 MUVPN 客户端建立与波特兰信息中心的安全连接。如果这些编辑的电脑能够连接到互联网，他们就可以安全地交换信息。



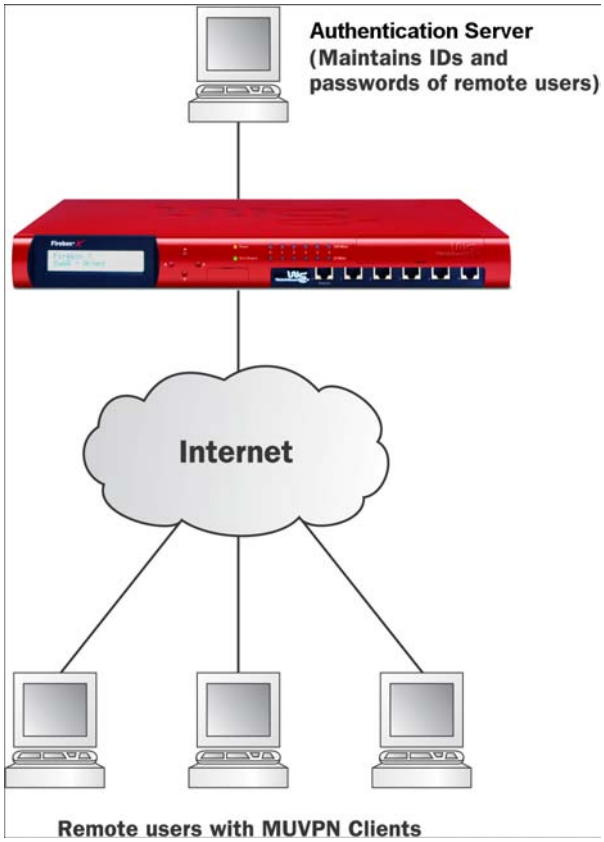

采用移动用户 VPN 的 Telecommuter 小型公司

## 存在远程雇员的公司：带有扩展认证功能的 MUVPN

BizMentors, Inc. 有 35 名讲师负责向不同地区的公司客户提供商业课程。BizMentors 的 75 名销售员工必须掌握所有讲师的最新课程表，以避免出现冲突。

BizMentors 数据中心的数据库负责保持这些信息处于最新状态。数据中心使用一台 Firebox，而每一销售人员使用一台 MUVPN 客户端访问库存及价格数据库。要认证所有远程用户， BizMentors 需要使用一台 RADIUS 认证服务器。

通常，你必须在 Firebox 及认证服务器中输入 ID 及密码。但是如果你使用扩展认证，所有 ID 及密码将被发送到认证服务器。你无需将它们置于 Firebox。所有销售人员都可以用他们经常用于进入公司网络的 ID 及密码登陆公司网络。 Firebox 会将 ID 及密码送往人证服务器，由认证服务器对 VPN 用户进行认证。




采用扩展认证的小型公司

# 第 19 章 配置托管 VPN 隧道

在你通过拖放操作流程、自动向导以及模版创建 IPSec VPN 隧道时， WSM 将提供快捷、可靠的服务。你可以在数分钟内创建采用认证及加密的 IPSec VPN 隧道。你可以确定此等隧道与其它隧道及安全政策相匹配。通过同一界面，你可以监控 VPN 隧道。

WSM 也允许客户从远端对 Firebox® X Edge 设备进行安全管理。详情请参阅 “*管理 Firebox X Edge 及 Firebox SOHO 6*”章节。

### 创建 VPN 的步骤

- 配置 WSM 及认证中心
- 将 Firebox 或 Firebox X Edge 或 SOHO 设备添加到管理服务器
- （仅供动态设备使用）将 Firebox 作为托管客户端进行配置
- 创建政策模版，并配置通过 VPN 隧道可以连接到那些网络
- 创建安全模版，并设置加密类型及认证类型
- 创建设备之间的隧道

## 将 Firebox 作为托管 Firebox 客户端进行配置

要允许 WSM 通过使用动态 IP 地址对 Firebox®、Edge 或 SOHO 进行管理，你必须将其作为托管 Firebox 客户端激活。有关如何将 Firebox 作为托管客户端激活的指导程序，请参阅第 16 章 “*使用管理服务器*”。

## 添加政策模版

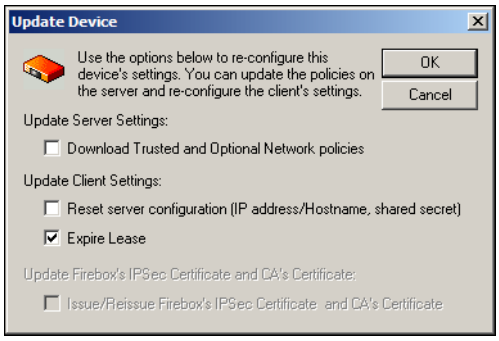
如果是 VPN，你可以配置 （并限定）通过隧道可以访问的网络。你可以在主机或网络之间创建一条 VPN。要配置通过一台给定的 VPN 设备可以访问的网络，你需要创建政策模版。如果该设备有

静态 IP 地址，则在默认状态下， WSM 将添加及提供一个可以在 VPN 设备后台区访问网络的网络政策模版。

## 从一台设备取得现有模版

在添加更多政策模版之前，请从该设备取得现有模版。由于 Firebox® 会自动为静态设备添加一份网络政策模版，因此此操作对动态设备至关重要。在对一份模版进行更新前，请确定将其作为托管 Firebox 客户端进行配置。

1 在 **Device Management （设备管理）**选项卡的 WSM 中选择一个托管客户端，然后点击 **Edit（编辑）>Update Device （更新设备）**。
屏幕将出现 Update Device （更新设备）对话框。




2 选择 **Download Trusted and Optional Network Policies （下载受信及可选网络政策）**复选框。

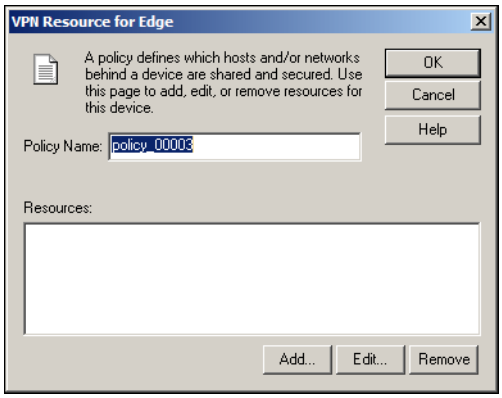
3 点击 **OK （确认）**。

## 创建一份新的政策模版

要创建一份政策模版，请在 **Device Management （设备管理）**选项卡中：

1 选择你想为其配置一份政策模版的设备

2 点击右键并选择 **Insert VPN Resource（插入 VPN 资源）**或点击 Insert VPN Resource （插入 VPN 资源）图标。
屏幕将出现该设备的 VPN Resource （VPN 资源）对话框。



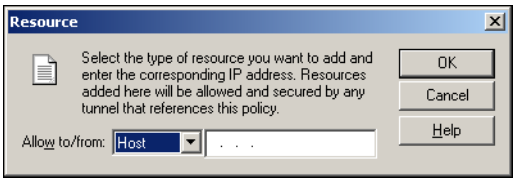

3 在 **Policy Name （政策名称）**对话框中键入你想选取的政策名称。

4 通过隧道政策添加、编辑或删除资源。点击 **Add（添加）**将一条 IP 地址或网络地址添加至隧道政策。点击 **Edit（编辑）**编辑你已经在列表中选中的一项资源。在 **Resource（资源）**列表中选择一项资源，并点击 **Remove（移除）**删除该资源。

5 点击 **OK（确认）**。
政策模版配置完毕。你可以在 VPN 配置区访问该模版。

### 将资源添加至政策模版

1 在 **VPN Resource（VPN 资源）**对话框中点击 **Add（添加）**。
屏幕将出现 Resource（资源）对话框。



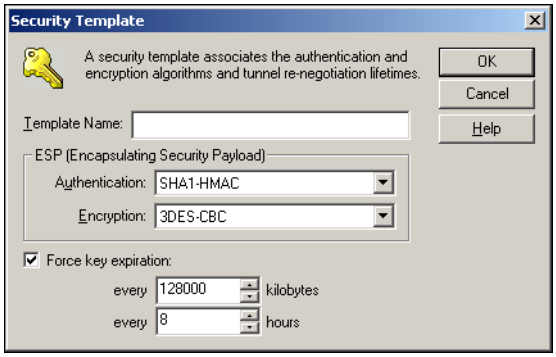

2 从 **Allow to/from（允许到 / 从）**下拉列表中选择资源类型，然后在相邻地址框中键入 IP 地址或网络地址。

3 点击 **OK（确认）**。

## 添加安全模版

安全模版为隧道提供加密类型及认证类型。
默认安全模版是为可以取得的加密类型提供的。你也可以创建新模版。通过配置向导中的隧道，安全模版能够让你轻松设置加密类型及认证类型。
要创建一份政策模版，请在 **Device Management（设备管理）**选项卡中：

1 在窗口中点击右键并选择 **Insert Security Template（插入安全模版）**或点击插入安全模版图标（见左侧）。
屏幕将出现 Security Template（安全模版）对话框。




2 在 **Template Name（模版名称）**对话框中键入你想选取的政策名称。从 **Authentication（认证）**及 **Encryption（加密）**下拉列表中选择认证方法及加密方法。

3 要为密钥设置截止日期，选择 **Force key expiration （强制密钥到期）**对话框，然后选择到期前的千字节或小时数。
如果你输入两种数值，密钥将在较早数值的到期日失效。

安全模版配置完毕。在你用该设备创建 VPN 隧道时，你可以在 VPN 向导中选择安全模版。

4 点击 **OK （确认）**。

# 在设备之间创建隧道

你可以通过拖放操作流程或 Add VPN （添加 VPN）向导配置一条隧道。

## 使用拖放操作流程

动态 Firebox 及 Firebox® X Edge 或 SOHO 设备必须有在你可以使用此流程前已经配置过的网络。在配置拖放隧道之前，你也必须从任何新的动态设备中获得政策（进行此操作时请使用第 238 页的流程 “*从一台设备取得现有模版*”）。

在 **Device Management （设备管理）**选项卡中进行以下操作：

1 在其中一个隧道端点中点击设备名称。将该名称拖放到其它隧道端点的设备名称。
Add VPN （添加 VPN）向导将被启动。

2 点击 **Next （下一步）**。

3 网关设备界面将显示你用拖放功能选择的两台端点设备以及隧道使用的政策模版。如果端点未予显示，请在此界面中选择该等端点。

4 从下拉列表中为每一设备选择一份政策模版。
政策模版将配置可以通过隧道获得的资源。资源可以是某一网络或某一主机。下拉列表将显示你已经添加到 WSM 中的政策模版。如果 VPN 端点设备存在静态 IP 地址，管理服务器会为该设备（包括所有受信网络）自动生成一份默认政策模版。如果该设备之后的受信网络存在许多经过配置的路由网络或次级网络，一些用户更倾向于创建一份自定义模版，对可从 VPN 隧道获得的资源加以限制。

5 点击 **Next （下一步）**。
向导将显示 Security Policy （安全政策）对话框。

6 选择适用于此隧道安全类型及认证类型的安全模版。
该列表将显示你添加到管理服务器中的模版。

7 点击 **Next （下一步）**。
向导将显示相应的配置。

8 选择 **Restart devices now to download VPN configuration（立即重启设备，下载 VPN 配置）**复选框。点击 **Finish （完成）**再次启动该等设备，并配置 VPN 隧道。

## 使用无拖放操作的 Add VPN （添加 VPN）向导

要用 Add VPN （添加 VPN）向导创建隧道，你需要进行以下操作：

1 从 **Device Management （设备管理）**选项卡中选择 **Edit （编辑）>Create a new VPN （创建新 VPN）**或点击 Create New VPN （创建新 VPN）图标。
Add VPN （添加 VPN）向导将被启动。

2 点击 **Next （下一步）**。
向导将显示两份列表，每份列表将显示已经注册到管理服务器中的所有设备。

3 从每一列表中选择将作为隧道端点的一台设备。

4 为每一设备的隧道端点选择政策模版。
列表将显示添加到管理服务器中的模版。
5 点击 **Next（下一步）**。
向导将显示 Security Template（安全模版）对话框。
6 为此 VPN 选择适用的安全模版，点击 **Next（下一步）**。
向导将显示相应的配置。
7 选择 **Restart devices now to download VPN configuration（立即重启设备，下载 VPN 配置）**复选框。点击 **Finish（完成）**再次启动该等设备，并配置 VPN 隧道。

## 编辑隧道

你可以在 WSM 的 **Device Management（设备管理）**选项卡中查看隧道。 WSM 允许你修改隧道名、安全模版、端点以及所使用的政策。

1 在 **Device Management（设备管理）**选项卡中拉伸树形图，查看要修改的设备及其政策。
2 选择你想修改的隧道。
3 点击右键，选择 **Properties（属性）**。
屏幕将出现 Tunnel Properties（隧道属性）对话框。
4 按照你的需要修改隧道。
5 点击 **OK（确认）**保存修改。
在隧道再次协商时，修改内容将被应用。

## 移除隧道及设备

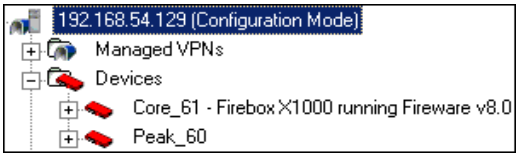
要从 WSM 移除某一设备，你必须首先移除该设备作为其端点的隧道。

### 移除隧道

1 在 WSM 中点击 **Device Management（设备管理）**选项卡。
2 拉伸 **Managed VPNs（托管 VPN）**文件夹，显示你想移除的隧道。
3 右键点击该隧道。
4 选择 **Remove（移除）**。点击 **Yes（是）**进行确认。
5 你可能需要重新启动你想移除其隧道的设备。点击 **Yes（是）**。

### 移除设备

1 在系统管理器中点击 **Device Status（设备状态）**或 **Device Management（设备管理）**选项卡。
屏幕将出现 Device Status（设备状态）选项卡（见左图下方）或 Device Management（设备管理）选项卡（见右图下方）。


2 如果使用 **Device Management**（**设备管理**）选项卡，你需要拉伸 **Devices**（**设备**）文件夹显示需要移除的设备。

3 右键点击该设备。

4 选择 **Remove**（**移除**）。点击 **Yes**（**是**）。

# 第 20 章 为 BOVPN 配置手动 IPSec 协议

您可以利用配置有手动 IPSec 协议的分支机构 VPN （ BOVPN ）在 Firebox® 和一台符合 IPSec 协议的安全设备之间创建加密隧道。该设备可保护分支机构或另一远程位置。配置有手动 IPSec 协议的 BOVPN 可以使用不同的加密方法：DES （ 56 位 ）、3DES （ 168 位 ）、AES128、AES192 和 AES256。

## 准备工作

要使用配置有手动 IPSec 协议的 BOVPN，您必须有以下信息：

- 策略端点- 在隧道上可以到达的主机或网络 IP 地址。
- 加密方法- 隧道两端必须使用相同的加密方法。
- 验证方法- 隧道两端必须使用相同的验证方法。

## 配置网关

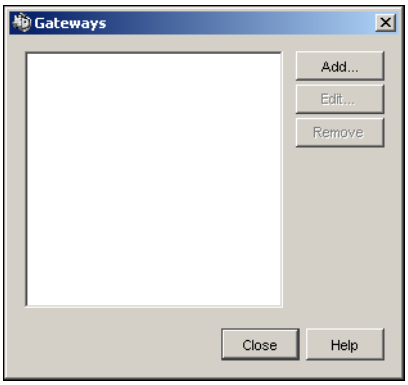
网关是一个或多个隧道的连接点。网关用来创建隧道的连接方法也就是隧道另一端必须使用的方法。 ISAKMP （ Internet 安全连接和密钥管理协议 ）就是一例。

### 添加网关

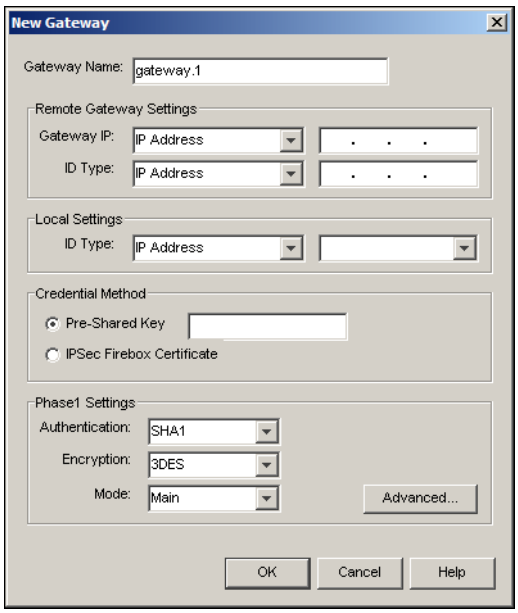
要启动 IPSec 隧道协商，对端必须连接到另一个对端。您可以用一个 IP 地址或 DNS 名连接这些对端。如果一个对端有一个动态 IP 地址，应为远端网关 IP 地址选择 **Any （ 任何 ）**。

要进行配置，将远端网关的 ID 类型设置为 **Domain Name（域名）**或 **User Domain Name（用户域名）**。将对端名设置为全称域名。 Firebox® 必须配置能够解析该域名的 DNS 服务器。

1 在 Policy Manager（策略管理器）中，点击 **VPN Branch Office Gateways（分支机构网关）**。
将显示 Gateways（网关）对话框。




2 要添加网关，点击 **Add（添加）**。
将显示 New Gateway（新建网关）对话框。




3 在 **Gateway Name（网关名）**文本框中，输入网关名。
此名称只在此 Firebox 的 Policy Manager（策略管理器）中标识网关。

4 在 **Gateway IP（网关 IP）**下拉列表中，选择 **IP Address(IP 地址)**或 **Any（任何）**。
如果远端网关地址是静态 IP 地址，则在旁边的地址框里输入该地址。如果远端 VPN 端点有动态 IP 地址，则选择 Any（任何）。

5 在 **Remote Gateway Setting ID Type（远端网关设置 ID 类型）**下拉列表中，选择 **IP Address（IP 地址）**, **Domain Name（域名）**, **User Domain Name（用户域名）**, 或 **X.500 Name（X.500 名）**。
如果远端 VPN 端点利用 DHCP 或 PPPoE 获取其外部 IP 地址，则将远端网关的 ID 类型设置为 Domain Name（域名）。将对端名称字段设置为远端 VPN 端点的全称域名。 Firebox 使用 IP 地址和 Domain Name（域名）去查找 VPN 端点。 Firebox 使用的 DNS 服务器必须应能识别该名称。

6 配置本地设置。在本地 **ID Type（ID 类型）**下拉列表中，选择 **IP address（IP 地址）**、**Domain Name( 域名 )** 或 **User Domain Name（用户域名）**。如果您选择了 **IP address（IP 地址）**，可从旁边的下拉列表中选择 IP 地址。将显示所有配置的 Firebox 接口 IP 地址。

7 点击 **Pre-shared Key( 预共享密钥 )** 或 **Firebox Certificate（Firebox 证书）**，确认要使用的验证程序。如果选择 **Pre-shared Key( 预共享密钥 )**，则输入该共享密钥。
在远端设备上，必须使用相同的共享密钥。该共享密钥只能使用 ASCII 字符。

**注释**

如果选择基于证书的验证，则必须启动 Certificate Authority（证书权限）。有关信息请参阅本手册前面的 “Certificate Authority”（证书权限）章节。此外，如果使用证书，您必须使用针对日志消息的 WatchGuard® 日志服务器。我们不支持第三方证书。

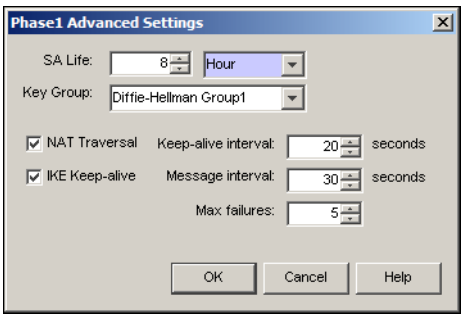
8 您可以使用默认的阶段 1 设置，也可修改设置。如果要使用默认设置，可直接执行第 19 步。
阶段 1 适用于 IKE 协商的初始阶段，包含验证、会话协商和密钥修改信息。

9 从 **Authentication（验证）**下拉列表中，选择 **SHA1** 或 **MD5** 为验证类型。

10 从 **Encryption（加密）**下拉列表中，选择 **None**、 **DES** 或 **3DES** 为加密类型。

11 从 **Mode（模式）**下拉列表中，选择 **Main** 或 **Aggressive**。
Main 模式不识别协商期间的 VPN 端点，并且比 Aggressive 模式更安全。Main 模式也支持 Diffie-Hellman 组 2。Main 模式比 Aggressive 模式慢，因为该模式必须在端点间发送更多的消息。

12 如果要修改 Diffie-Hellman 组设置和其它高级阶段 1 设置，点击 **Advanced（高级）**。
弹出 Phase 1 Advanced Settings（阶段 1 高级设置）对话框。




13 要修改 SA（安全关联）周期，在 **SA Life（SA 周期）**字段里输入一个数字，并从下拉列表中选择 **Hour（小时）**或 **Minute（分钟）**。

14 从 **Key Group( 密钥组 )** 下拉列表中选择您需要的 Diffie-Hellman 组。WatchGuard 支持组 1 和组 2。
Diffie-Hellman 组是属性组，用于在公共媒体上安全协商密钥。组 2 比组 1 更安全，但生成密钥所需时间更长。

15 如果要通过隧道使用 NAT 设备，选择 **NAT Traversal（NAT 穿越）**复选框。要设置 **Keep-alive interval（持续作用间隔）**，输入秒数，或利用数值控制选择您需要的秒数。
NAT 穿越或 UDP 封装允许流量到达正确目的地。如果要在 Firebox 和 NAT 设备后面的另一设备之间建立 BOVPN 隧道，则启用 NAT 穿越。

16 要让 Firebox 发送消息到其 IKE 对端以保持 VPN 隧道开放，选择 **IKE Keep-alive( IKE 持续作用 )** 复选框。要设置 **Message Interval（消息间隔）**，输入秒数，或利用数值控制选择您需要的秒数。

17 在试图再次协商阶段 1 之前，Firebox 会试图发送一条 IKE keep-alive 消息，要设置其发送消息的最大次数，在 **Max failure（最大失败次数）**框中输入所需数字。

18 完成高级配置后，点击 **OK（确定）**。

19 点击 **OK （确定）**保存网关。

20 点击 **Close （关闭）**关闭 **Gateway （网关）**对话框。

### 编辑和删除网关

要修改网关，选择 **VPN Branch Office Gateway （分支机构网关）**。也可在 Policy Manager （策略管理器）的 **BOVPN** 选项卡中，右键点击隧道图标，选择 **Gateway Property （网关属性）**。

1 选择所需网关，点击 **Edit （编辑）**。
弹出 Edit Gateway （编辑网关）对话框。

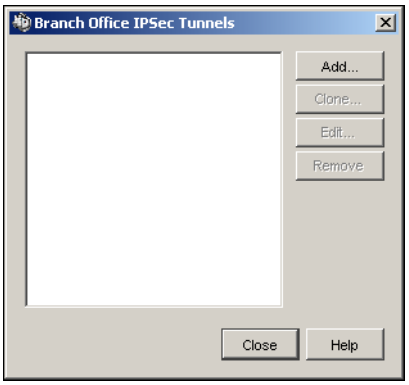
2 进行修改，点击 **OK （确定）**。

要删除网关，先选择网关，点击 **Remove （删除）**。

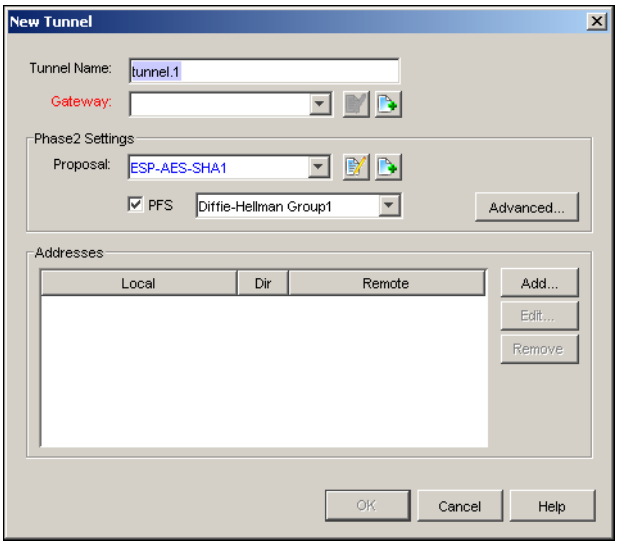
## 创建手动配置隧道

使用该方法配置手动隧道，该隧道使用配置有 ISAKMP 密钥协商类型的网关。 ISAKMP 是在两台设备间验证网络流量的协议。该程序包含设备如何控制安全 （包括加密）的信息，以及用于创建密钥的信息，密钥用于把加密数据修改为文本。

1 在 Policy Manager （策略管理器）中，选择 **VPN > Branch Office Tunnels （分支机构隧道）**。
弹出 Branch Office IPSec Tunnels （分支机构 IPSec 隧道）对话框。



2 点击 **Add（添加）**
弹出 New Tunnel（新建隧道）对话框。



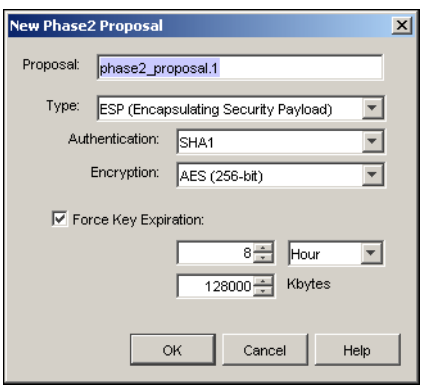

3 在 **Tunnel Name（隧道名）**框中，输入隧道名称。

4 从 **Gateway（网关）**下拉列表中，选择要连接该隧道的远端网关。您添加到配置中的网关都显示在该下拉列表中。
要编辑网关，选择名称，点击 **Edit（编辑）**按钮。要创建新网关，点击 **New（新建）**按钮。


Edit


New

5 从 **Proposal（提议）**下拉列表中，为隧道选择 IKE 阶段 2 提议。该下拉列表包含预先定义的阶段 2 安全提议。如果要使用默认的阶段 2 建议，并不创建或编辑阶段 2 建议，直接执行第 14 步。
您可以编辑您创建的任何阶段 2 提议，但不能编辑预定义的提议。您必须添加新的提议。要编辑您创建的阶段 2 提议，先选择提议名称，再点击 **Edit（编辑）**按钮。要创建新提议，点击 **New（新建）**按钮。
弹出 Phase2 Proposal（阶段 2 提议）对话框。




6 为新提议输入名称。

7 从 **Type （类型）**下拉列表中，选择 **ESP** 或 **AH** 为提议方法。
ESP 加密验证。 AH 只是验证。此外， ESP 验证不包括 IP 报头，但 AH 包括 IP 报头。 AH 很少使用。

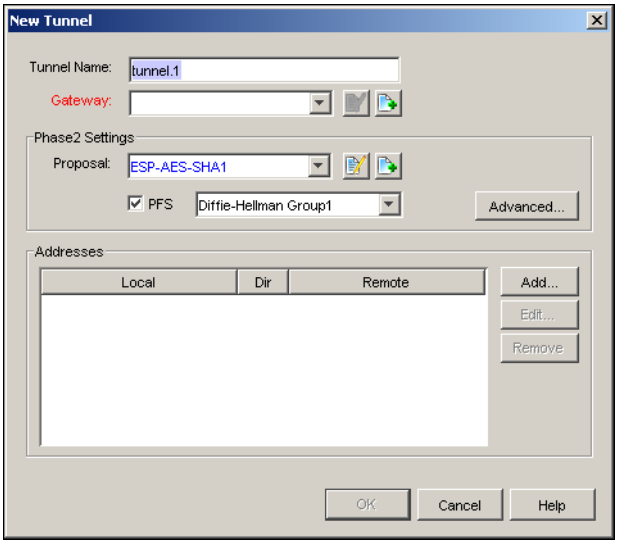
8 从 **Authentication （验证）**下拉列表中，为验证方法选择 **SHA1**， **MD5** 或 **NONE**。

9 （仅 ESP）从 **Encrption （加密）**下拉列表中，选择加密方法。
选项包括 DES、 3DES 和 AES 128、 192 或 256 位，其在列表中的排列顺序是从最简单和最不安全的到最复杂和最安全。

10 您可将密钥设置为在经过一定时间或流量后到期。要让密钥到期，选择 **Force Key Expiration （强迫密钥到期）**复选框。

11 输入时间和字节量，达到该值后密钥即到期。

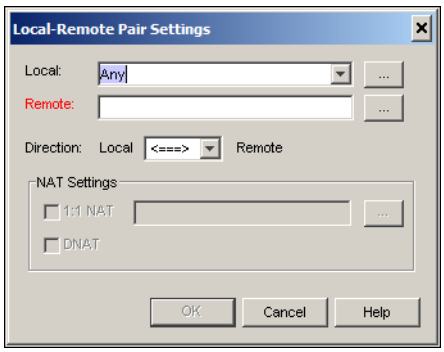
12 点击 **OK （确定）**关闭 **Phase 2 Proposal （阶段 2 提议）**对话框。



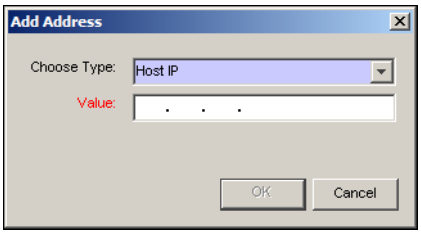

13 选择 **PFS** 复选框启用完整转发安全性 （PFS）。如果启用了 PFS，选择 Diffie-Hellman 组。
完整转发安全性 （PFS）为会话中创建的密钥提供更多保护。用 PFS 创建的密钥不是以前的密钥构成的。如果以前的密钥在会话后泄露，新会话密钥是安全的。 Diffie-Hellman 组 1 使用一个 768 位的组创建新的密钥交换， Diffie-Hellman 组 2 则使用一个 1024 位的组。

14 点击 **Advanced （高级）**配置高级设置。利用 **Phase 2 Advanced Settings （阶段 2 高级设置）**对话框将隧道配置对策略或地址使用 **Any （任何）**，完成后点击 **OK （确定）**。
如果没有选择 Use Any for Service （对服务使用 Any），就会为所用的每项策略中定义的每组定义端口 / 协议对创建一个安全关联 （SA）。如果没有选择 Use Any for Address （对地址使用 Any），就会根据隧道路由 （本地 – 远程对）创建一个安全关联。

15 在 **New Tunnel（新建隧道）**对话框的 **Address（地址）**块中，点击 **Add(添加)**，添加一对使用该隧道的地址。
弹出 Local-Remote Pair Setting( 本地 – 远程对设置 ) 对话框。




16 从 **Local（本地）**下拉列表中，选择所需的本地地址。
您也可以点击 Local（本地）下拉列表旁的按钮使用 IP 地址、网络地址或 IP 地址范围。
17 在 **Remote（远端）**框中，输入远端网络地址。点击 **Remote（远端）**框旁的按钮，打开 **Add Address（添加地址）**对话框。




18 从 **Choose Type（选择类型）**下拉列表中，选择要使用的地址类型。
选择 **Host IP（IP 地址）**、 **Network IP（网络 IP 地址，具有斜线计法掩码）**或 **Host Range（IP 地址范围）**。
19 在 **Value（数值）**文本框里，输入 IP 地址或网络地址。
20 点击 **OK（确定）**。
Add Address（添加地址）对话框关闭。
21 从 **Direction（方向）**下拉列表中，选择隧道方向。隧道方向决定了 VPN 隧道的哪个端点可以通过该隧道启动 VPN 连接。
22 您可以为隧道启用 NAT。选择 **1:1 NAT** 复选框或 **DNAT** 复选框。
不同类型的地址和不同隧道方向，可为 NAT 选择的选项就不同。对于 1:1NAT，输入地址，用字段中的 NAT 进行修改。
通过 VPN 也可以使用动态 NAT。必须设置从 LAN1 到 LAN2 的单向隧道，在该隧道里，您可以让所有的 LAN1 服务器连接到 LAN2 服务器，但只是作为一个 IP 地址显示在 LAN2 上。有关信息请参阅第 250 页的 “*通过 BOVPN 隧道设置外发动态 NAT*”。
23 配置完该对后，点击 **OK（确定）**。
24 完成隧道配置后， **OK（确定）**。

### 编辑和删除隧道

要修改隧道，选择 **VPN >Branch Office Tunnels（分支机构隧道）**；或在 Policy Manager（策略管理器）的 **Branch Office VPN（分支机构 VPN）**选项卡中，右键点击隧道光标，选择 **Tunnel Property（隧道属性）**。

1 选择隧道，点击 **Edit（编辑）**。
弹出 Edit Tunnel（编辑隧道）对话框。
2 进行修改，点击 **OK（确定）**。

要从 **Branch Office IPSec Tunnels（分支机构 IPSec 隧道）**对话框中删除隧道，先选择隧道，再点击 **Remove（删除）**。

## 创建隧道策略

隧道策略是应用于隧道连接的规则集。
在默认情况下，创建 VPN 隧道时就会创建 “Any” 策略。该策略允许所有的流量使用该隧道。您也可以删除该策略。接着，您可以创建自定义 VPN 策略，允许特定端口或使用代理服务器。

1 在 Policy Manager（策略管理器）中，点击 **Branch Office VPN（分支机构 VPN）**选项卡。
2 从 **Show（显示）**菜单中，选择要添加策略的隧道。
3 右键点击 Policy Manager（策略管理器），选择 **Add Policy（添加策略）**。
如果您没有从 **Show（显示）**菜单中选择 BOVPN 隧道，系统会弹出对话框提示您选择隧道。选择隧道，点击 **OK（确定）**。
4 配置策略。详情请参阅 “*为网络创建策略*”。
BOVPN 策略的地址信息不同于标准的 Firebox 策略。您可以用 Local-Remote Pairs（本地 – 远端对）对话框配置地址。

### 允许特定策略的 VPN 连接

要让只为特定策略下的来自 VPN 连接的流量通过，请添加并配置每项策略。有可能需要删除 “Any” 策略以创建必要的限制。

## 通过 BOVPN 隧道设置外发动态 NAT

您可以通过 BOVPN 隧道使用动态 NAT。动态 NAT 充当了单向 NAT，并且使 VPN 隧道仅在一个方向上保持开放状态。当您向远程站点创建 BOVPN（在该站点所有 VPN 流量均来自同一公共 IP 地址）时，这可能会有帮助。
例如，假设您要创建一个连接商业伙伴的 BOVPN 隧道，以便能够访问其数据库服务器，但不希望这家公司能访问您的任何资源。您的商业伙伴打算允许您的访问，但只能从单个 IP 地址进行访问，以便他们能够监控连接。
您必须拥有每个 VPN 端点的外部 IP 地址以及受信网络地址，才能完成该操作。

1 在您站点上的 Policy Manager（策略管理器）中，选择 **VPN>Branch Office Tunnels（分支机构隧道）**。选择 **Add（添加）**，添加新 BOVPN 隧道。
2 为 BOVPN 隧道命名。

3 选择 New Phase 2 Proposal（新建阶段 2 提议）图标（在 **Gateway（网关）**字段最右边的按钮）。
弹出 New Gateway（新建网关）对话框。
4 按照第 243 页 “*添加网关*”第 3 步开头的说明创建新网关。
5 点击 **OK（确定）**返回 **New Tunnel（新建隧道）**对话框。
6 点击 **Advanced（高级）**。取消对所有复选框的选择。点击 **OK（确定）**。
如果不修改这些 Phase 2 Advanced Settings（阶段 2 高级设置），BOVPN 隧道将无法正确协商。如果不做修改，在启用动态 NAT 后，第二个 VPN 端点将会查找第一个端点的受信网络，而非其外部接口。
7 点击 **Add（添加）**，添加隧道策略。按照第 249 页中以 “*从本地下拉列表中*”开头的说明进行操作。请务必选择 **DNAT** 复选框。
8 点击 **OK（确定）**，将修改保存到 Firebox® 中。
9 在远程站点的 Policy Manager（策略管理器）中，选择 **VPN> Branch Office Tunnels（分支机构隧道）**。选择 **Add（添加）**，添加新 BOVPN 隧道。
10 在远程站点上执行第 2 到第 8 步，但不要选择 **DNAT** 复选框。

当远程站点的 Firebox 重启时，两台 Firebox 设备进行 VPN 隧道协商。Firebox 将动态 NAT 应用到目的地是远程站点受信网络的所有流量上。流量到达远程站点时，作为源自外部接口的流量到达。

# 第21章 管理Firebox X Edge及Firebox SOHO

WSM 具备大量专门用于管理 Firebox® X Edge 设备的特殊功能。用户可以轻松管理大量的 Firebox X Edge 设备，一次性修改多个 Firebox X Edge 设备的安全策略，同时，仍然能够单独控制每一个 Firebox X Edge 设备的配置。通过管理服务器，你可以：

- 为一组 Firebox X Edge 设备创建 Edge Configuration Templetes（Edge 配置模版）。你可以在管理服务中创建一个配置模版，并将其安装到多个其他 Firebox X Edge 设备。在进行此操作前，首先从列表中选择一个 Edge Configuration Templetes （Edge 配置模版），或将 Firebox X Edge 设备拖放到模版之上。如果你对策略进行了修改，则该策略将被自动更新到所有定购的 Firebox X Edge 设备中。
- 用 WSM 即可对一组 Firebox X Edge 设备的网络设置进行管理这些。
- 通过 Quick Setup Wizard（快速安装向导）对 Firebox X Edge 设备的出厂设置进行修改，并通过管理服务器对设备进行管理设置。然后，只需一个步骤即可将设备导入管理服务器。
- 在一个简单的版面中查看多个 Firebox X Edge 设备的设置，并可以轻松修改设置。
- 查看一个 Firebox X Edge 的所有 VPN 隧道。
- 管理 Firebox X Edge 固件的更新。通过管理服务器，可以安排并安装固件更新。

你也可以用 WSM 对 Firebox SOHO 6 及 SOHO 5 设备进行管理。你无法为 Firebox SOHO 创建配置模版，或通过 WSM 对网络配置进行修改。你可以：

- 在一个简单的版面中查看一组 Firebox SOHO 设备的设置。
- 查看一个 Firebox SOHO 的所有 VPN 隧道。

**注释**

本章节介绍如何使用 WSM 对 Firebox X Edge 设备进行管理。有关 Firebox X Edge 配置的详情，请参阅《Firebox X Edge 使用向导》。

## 管理服务器的设备

你可以用安装在 WatchGuard® 管理服务器和 WSM 配置及管理众多的 Firebox® X Edge 设备及 Firebox SOHO 设备。

必须用管理服务器配置和管理每一 Firebox® X Edge 及 SOHO。然后，将各种设备 **Insert**（插入）或 **Import**（导入）到 管理服务器。

你可以将一个或多个已经用 Quick Setup Wizard（快速安装向导）配置好的 Firebox® X Edge 设备 **Import**（导入）管理服务器。这是将一组 Firebox® X Edge 设备添加到管理服务器中的最快步骤。

你可以 **Insert**（插入）一个已经用 Add Device Wizard（设备添加向导）配置或安装好的 Firebox® X Edge 设备。你必须配置好相应数值，使管理服务器能够识别该设备。你可以一次仅插入一个设备。

- 如果是一个新的或参数均为出厂默认值的 Firebox® X Edge 设备，你可以按照第 254 页的流程 "*对新的或参数为出厂默认值的 Firebox® X Edge 进行管理设置*"，然后按照第 255 页的流程 "*将 Firebox® X Edge 设备导入管理服务器*" 将设备导入。
- 如果是一个已经安装的 Firebox® X Edge 设备，按照第 255 页的流程 "*对已安装的 Firebox® X Edge 进行管理配置*" 对该设备进行管理配置，然后按照第 257 页的流程 "*将 Firebox® X Edg e 及 SOHO 6 设备添加至管理服务器*" 将该设备插入管理服务器。

在将一个 Firebox® X Edge 设备设置为由管理服务器进行管理之后，你必须将其重新设置为工厂默认值，使其恢复到原始状态。

**注释**

管理服务器通过 TCP 端口 4109 连接到受管控的 Firebox® X Edge 设备。确定你已取得相关策略，该策略允许受管控的数据流通过网关 Firebox 或其他防火墙（用于向管理服务器提供互联网连接保护）上的 TCP 端口 4109。

## 对新的或参数为出厂设置的 Firebox® X Edge 设备进行管理配置。

如果要将新的或参数为出厂设置的 Firebox® X Edge 设置为由管理服务器进行管理，你必须手动将 Firebox® X Edge 连接到你电脑上的以太网网接口。

准备 Firebox X Edge 设备时，你应该：

1 启动 WSM 并选择 **Tools（工具）>Quick Setup Wizard（快速安装向导）**。
Quick Setup Wizard（快速安装向导）将被启动。

2 阅读 Welcome（欢迎）页面并点击 Next（下一步）。

3 按照 Firebox 的型号选择 **Firebox® X Edge**，然后点击 **Next（下一步）**。

4 将你电脑上的网络接口连接到 Firebox® X Edge 上的 LAN（局域网络）端口，然后点击 **Next（下一步）**。
用与 Firebox X Edge 一起提供的绿色以太网电缆。（如果你的 Firebox X Edge 没有配备绿色电缆，请使用红色电缆。）查看 Edge 前面板指示屏显示的数字，该数字与 Edge 背部电缆所连接的以太网端口的数字相对应。如果指示屏不亮，则应换用不同的电缆。电缆有可能损坏或电缆为交叉线。通常要求使用直通电缆，但是你必须确定指示屏亮起并指示网络连接已接通。

5 按照向导后续页的指示，在安全模式下启动 Firebox X Edge。

6 遵守向导页的指示操作，然后点击 **Next（下一步）**。

7 遵守 **Wait for the Firebox（等待 Firebox）**及 **The Wizard found this Firebox（本 Firebox 中的向导）**页的指示。在完成每一页的指示后点击 **Next（下一步）**。

8 接受许可协议并点击 **Next（下一步）**。

9 对 Firebox X Edge 的外部（WAN1）界面进行配置。选择 **DHCP**、**PPPoE** 或 **Static IP addressing**（静态 IP 地址查询），然后点击 **Next（下一步）**。（有关如何配置 Edge 界面的详情，请参阅《Firebox X Edge 用户指南》。）

10 在对界面进行配置后，点击 **Next（下一步）**。

11 对 Edge 内部界面进行配置，并点击 **Next（下一步）**。

12 为你的 Edge 创建一个状态口令及一个配置口令，然后点击 **Next（下一步）**。
你必须将每一口令键入两次。该口令由 WSM 使用，用于连接至该设备并对其进行配置。

13 为设备键入用户名及口令，然后点击 **Next（下一步）**。
你必须将每一口令键入两次。你可以使用该用户名及口令连接到该设备，并使用 Web 浏览器对其进行配置。

14 选择时区设置，然后点击 **Next（下一步）**。

15 对管理服务器设置选项进行配置。键入网关 Firebox 的 IP 地址，该网关 Firebox 用于保护管理服务器、[ 管理服务器界面 ] 中用于识别 Firebox 的名称以及共用密钥。点击 **Next（下一步）**。
共用密钥由管理服务器使用，用于创建各个 Firebox 之间的 VPN 隧道。请你一定记住该密钥。

16 对 Edge 配置进行复查，然后点击 **Next（下一步）**。

17 如果需要对另一 Edge 进行设置，请选择复选框，然后点击 **Finish（完成）**。
如果选择另一 Edge， Quick Setup Wizard（快速安装向导）将用与该配置同样的数值设置各个字段，因此你可以轻松设置相似的 Edge 装置。

### 将 Firebox X Edge 导入管理服务器

用 Quick Setup Wizard（快速安装向导）配置的 Firebox X Edge 设备可以导入到管理服务器中。

1 启动 WSM，连接到你为其配置 Edge 设备的管理服务器。

2 选择 **File（文件）>Import Device（导入设备）**。
屏幕将出现 Import（导入设备）对话框。

3 选择你想导入的位于每一 Edge 前面的复选框。然后点击 **Import（导入）**。

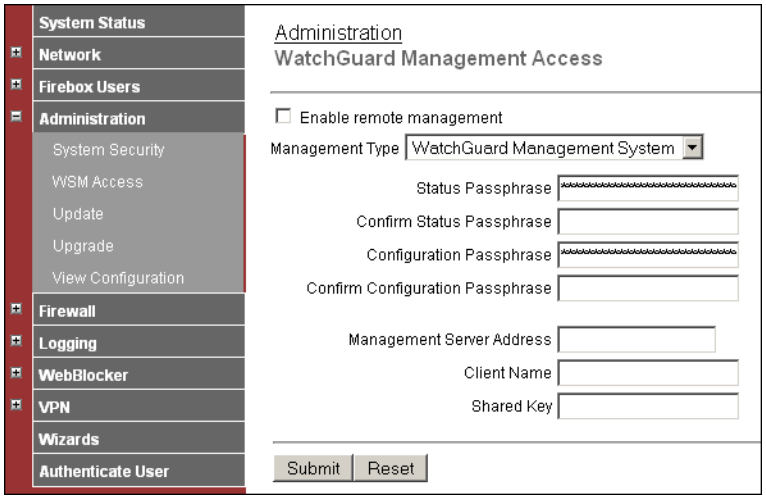
Firebox X Edge 设备将被导入至管理服务器。在管理服务器中，这些设备将出现在 **Imported Devices（导入设备）**文件夹中。

## 对已安装的 Firebox® X Edge 设备进行管理配置

1 启动你的 web 浏览器。键入 Firebox X Edge 的 IP 地址。

2 如有需要，键入一个用户名及口令，登入 Edge。

3 点击 **Administration**（**管理**）。点击 **WSM Access**（**WSM 访问权限**）
屏幕将出现 WatchGuard Management Access（WatchGuard 管理访问）页面。




4 选择 **Enable Remote Management**（**启用远程管理**）复选框。

5 从 **Management Type**（**管理类型**）下拉列表中选择 **WatchGuard Management System**（**WatchGuard 管理系统**）。

6 为 [WatchGuard 管理 ] 键入状态口令。再次键入状态口令进行确认。
WatchGuard 管理服务器将使用你创建的口令在只读模式下连接到该设备。

7 为 WatchGuard 管理键入配置口令。再次键入状态口令进行确认。
WatchGuard 管理服务器将使用你创建的口令对该设备进行配置。

8 （可选项，但推荐使用）键入管理服务器地址。该地址是管理服务器所依据的 Firebox IP 地址。
如果你没有键入管理服务器地址，则 Firebox X Edge 与管理服务器必须从管理服务器中启动。

9 （可选项）键入用户名
管理服务器使用该名称对 Edge 进行识别。

10 （可选项）如果已对其进行了配置，键入共用密钥。

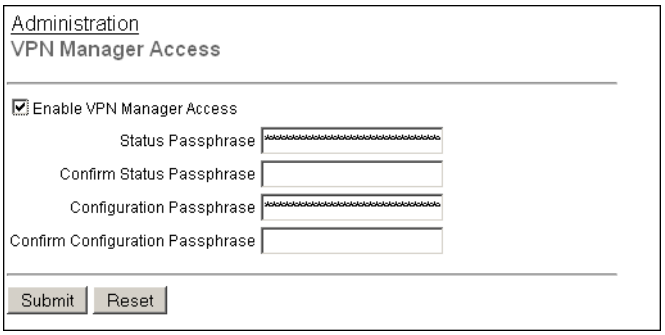
11 点击 **Submit**（**提交**）。
管理服务器将对 Edge 进行管理配置。

## 对 Firebox SOHO 6 进行管理设置

1 启动你的 web 浏览器。键入 SOHO 6 的 IP 地址。

2 如有需要，键入一个用户名及口令，登入 SOHO 6。

3 在 Administration （管理）项下，点击 **VPN Manager Access （VPN 管理器访问权限）**。
屏幕将出现 VPN Manager Access （VPN 管理器访问权限）页面。




4 选择 **Enable VPN Manager Access （启用 VPN 管理器访问权限）**复选框。

5 为 VPN 管理访问键入状态口令。再次键入状态口令进行确认。

6 为 VPN 管理访问键入配置口令。再次键入配置口令进行确认。

7 点击 **Submit （提交）**。
管理服务器将对 SOHO 6 进行管理配置。

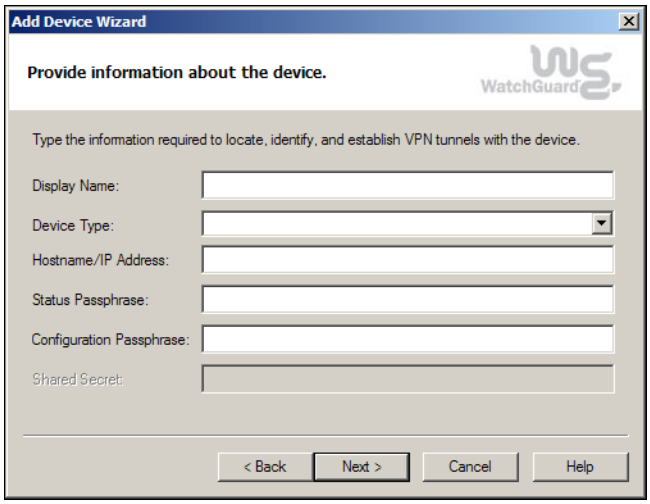
## 将 Firebox X Edge 及 SOHO 6 添加至管理服务器

1 在 WSM 中连接到管理服务器。
选择 File （文件）>Connect to Server （连接到服务器），或选择 Device Status （设备状态）或 Device Management （设备管理）选项卡 （Tab），点击右键，然后选择 Connect to （连接到）>Server （服务器）。

2 点击 **Device Management （设备管理）**选项卡。

3 详细显示 **Devices （设备）**文件夹。
由该管理服务器控制的设备均显示于此。

4 选择 **Edit （编辑）>Insert Device （插入设备）**，或右键点击该窗口的左边框，选择 **Insert Device （插入设备）**。
进入 Add Device Wizard （添加设备向导）。点击 Next （下一步）查看第一个配置页面。




5 为设备键入一个显示名称。
该名称不能包括任何空格或标点符号。

6 从 **Device Type （设备类型）**的下拉列表中选择 Firebox 型号。

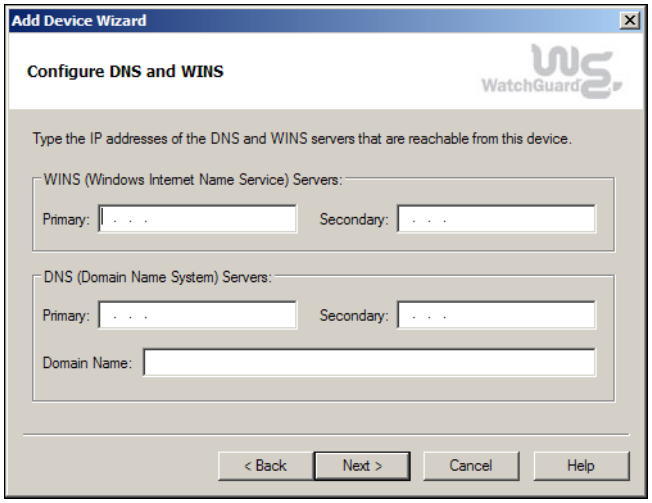
7 如果是不使用动态 IP 地址的设备，则键入 IP 地址或主机名称。如果是使用动态 IP 地址的设备，则键入动态 DNS 服务客户名称。

8 键入状态口令。该口令是你在设置VPN管理器访问权限或WatchGuard管理访问权限时为Firebox X Edge 或 SOHO 6 设置的状态口令。

9 键入配置口令。该口令是你在设置VPN管理器访问权限或WatchGuard管理访问权限时为Firebox X Edge 或 SOHO 6 设置的配置口令。

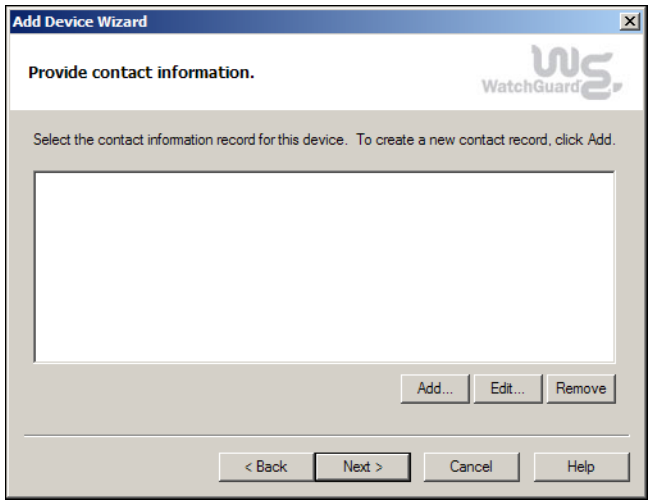
10 如果 Firebox X Edge 或 SOHO 6 使用动态 IP 地址，则键入动态 DNS 共用密钥。

11 点击 **Next （下一步）**。
屏幕将出现 Configure WINS 及 DNS （配置 WINS 及 DNS）界面。




12 为该设备使用 WINS 及 DNS 服务器键入第一及第二地址 （若有）。

13 为该设备键入域名 （若有）。点击 **Next （下一步）**。
屏幕将出现 Provide Contact Information （提供联系信息）界面。




14 你可以为该设备选择一个现有的联络记录，或点击 **Add （添加）**，为该设备添加一个新的联络记录。如果要删除现有的联络记录，则应选中该记录并将其 **Delete （删除）**。

15 点击 **Next（下一步）**。屏幕将出现 Configure Device（配置设备）界面。在该界面中点击 **Next（下一步）**，使用新的管理设置对该设备进行配置，并将其添加到管理服务器。如果该设备受另一个服务器管理，或已经通过本服务器进行了配置，则屏幕会弹出警告性对话框。点击 **Yes（是）**继续。
你无法通过管理服务器对 Firebox SOHO 设备进行配置。

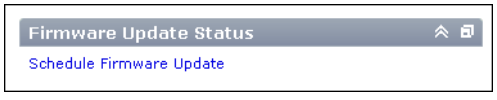
16 点击 **Close（关闭）**，关闭 Add New Device（添加新设备）向导。

## Firebox X Edge 固件的定期更新

Firebox® X Edge 设备必须具备适用于管理服务器高级功能的固件更新功能。今后，对固件进行更新的需求将越来越高。这些固件更新功能安装于管理服务器，而管理服务器可以将他们加载到各个 Edge 设备。WSM 可以轻松将各种固件更新安装到一组 Edge 设备中。仅需操作一次，你便可以立即或定期对各个设备组中的固件进行更新。

1 在 WSM 的 **Device Management（设备管理）**选项卡中选择管理服务器。
屏幕将弹出管理服务器设置界面。


2 下拉到 **Firmware Update Status（固件更新状态）**区。
如果有定期的固件更新功能，会在此处有所显示。




3 点击 **Schedule Firmware Update（安排固件更新）**。
Update Firmware（更新固件）向导将被启动。

4 阅读 Welcome（欢迎）页面并点击 **Next（下一步）**。

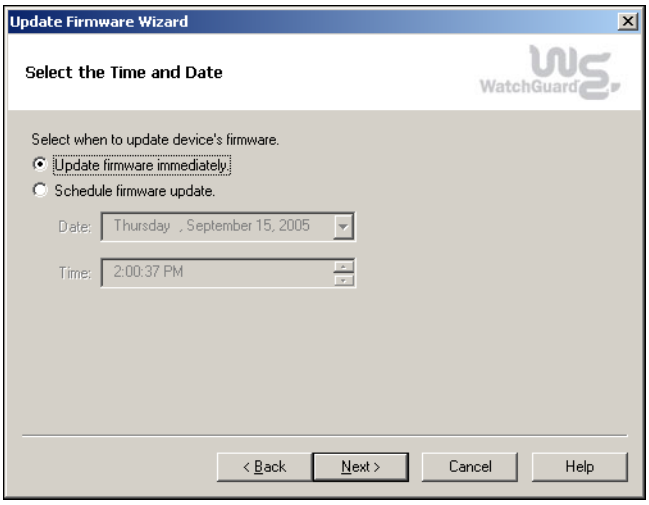
5 从列表中选择设备类型，然后点击 **Next（下一步）**。

**注释**

对于本版本的 WSM，你可以选择的设备类型仅限于 Firebox X Edge.

6 在每一你想对其进行更新的 Firebox X Edge 设备的前端选择复选框。点击 **Next（下一步）**。

7 选择固件版本，然后点击 **Next（下一步）**。
屏幕将弹出 Select the Time and Date（选择时间及日期）界面。




8 如需立即对固件进行更新，选择 **Update firmware immediately（立即更新固件）**。如需在今后某一特定时间进行更新，则应选择 **Schedule firmware update（安排固件更新）**。

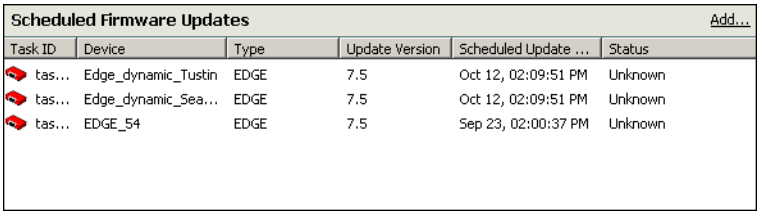
9 如果你选择了 **Schedule firmware update（安排固件更新）**，你需要在 **Date（日期）**字段选定日期，并在 **Time（时间）**字段设定更新时间。

10 点击 **Next（下一步）**。

11 点击 **Next（下一步）**。点击 **Close（关闭）**。
如果选择了 Update firmware immediately（立即更新固件），则固件更新将立刻进行。如果选择了 Schedule firmware update（安排固件更新），则固件更新被安排今后的某一具体时间。

## 查看及删除固件更新

1 在 **Device Management（设备管理）**选项卡中点击管理服务器项下的 **Scheduled Firmware Updates（定期固件更新）**。
屏幕将弹出 Scheduled Firmware Updates（定期固件更新）页面。



所有的定期固件更新均列示于此。即使同一固件更新涵盖多个设备，屏幕仍会分别显示每一设备的固件更新。因此，当你选择一个设备时，所有包括在该定期固件更新中的设备将全部被选中。

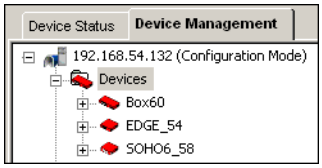
- 如需删除某一定期固件更新，则应右键点击一个设备，然后选择 **Remove Task（删除任务）**。
  该固件更新涵盖的所有设备将被从日程表中删除。
- 如需添加一个定期固件更新，则应点击 **Add（添加）**。
  Update Firmware（更新固件）向导将被启动。

# Firebox X Edge 管理页面的使用

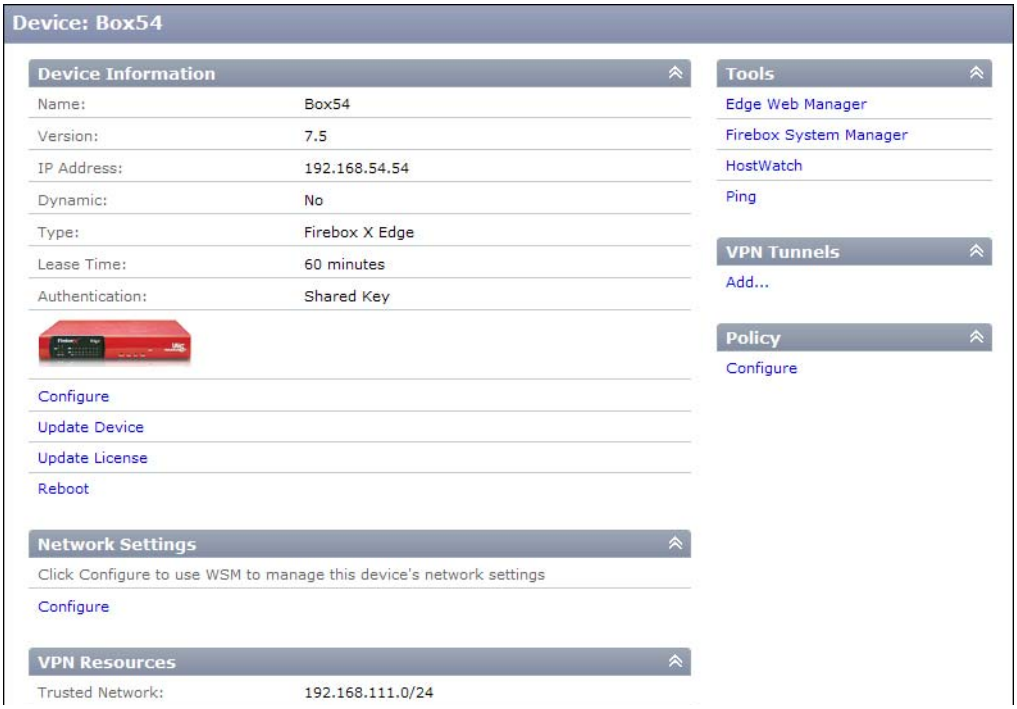
当 Firebox® X Edge 被添加至一个管理服务器之后，你可以使用管理页面对设备的设置选项进行配置。

## 查看 Firebox X Edge 管理页面

1 选择 **Device Management（设备管理）**选项卡，详细显示 WSM 中的 **Devices（设备）**。
屏幕将显示受管理的设备列表。

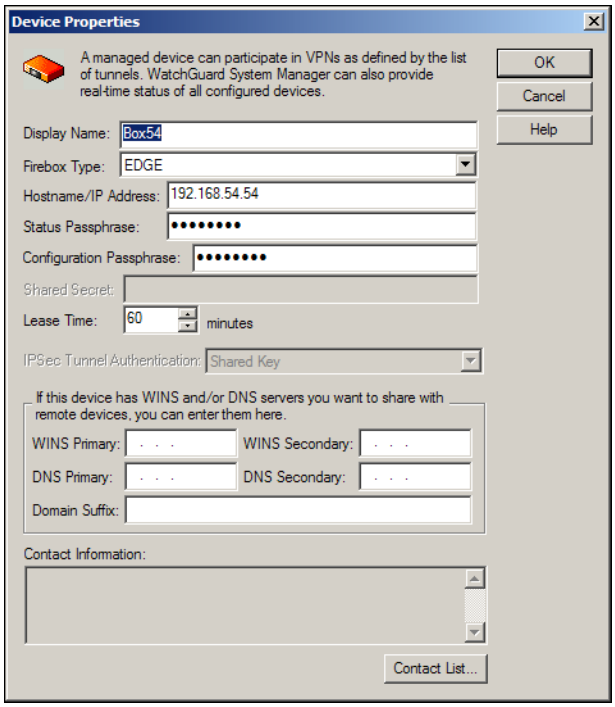



2 选择一个 Firebox X Edge。屏幕将出现该设备的管理页面。



## Firebox X Edge 管理属性的配置

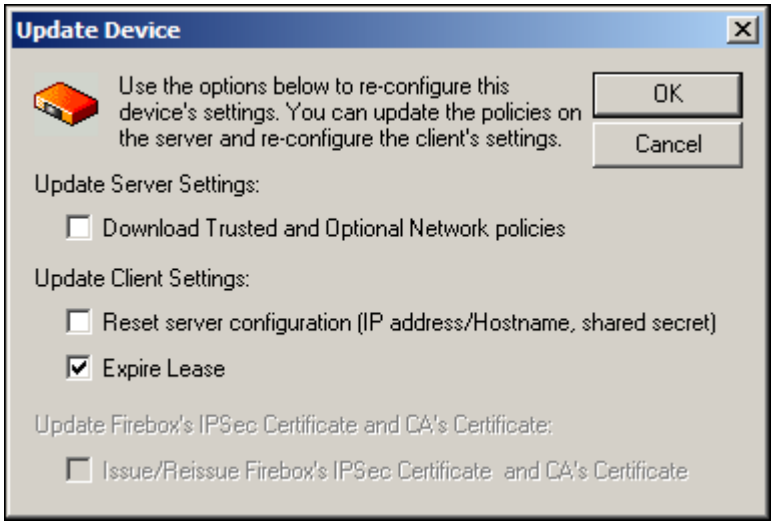
1 在 Firebox X Edge 管理页面上点击 **Configure （配置）**。
屏幕将弹出 Device Properties （设备属性）对话框。




2 为该设备配置管理属性。更多有关此对话框中各个单独字段的信息，请参阅《Firebox X Edge 用户指南》。

## 设备更新

1 在 Firebox X Edge 管理页面之上点击 **Update Device （更新设备）**。
屏幕将出现 Update Device （更新设备）对话框。

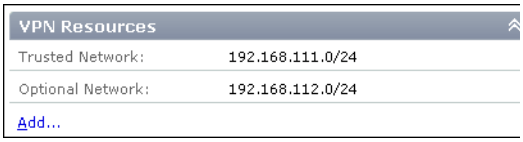


2 你可以通过使用该对话框从 Firebox X Edge 设备中获得策略，为该设备重新设置管理服务器配置选项，并将管理协议作废。你也可以使用该对话框更新 Firebox 证书及 CA 证书（如果该证书已被变更）。

3 点击 **OK（确认）**。

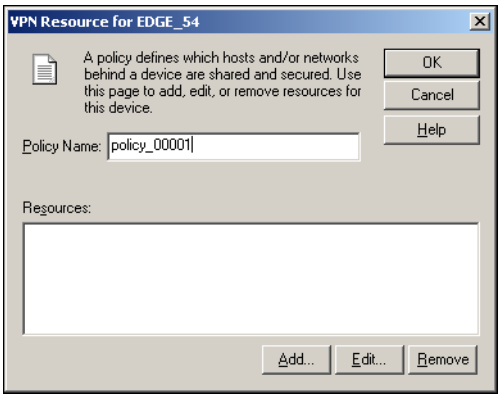
## 添加 VPN 资源

1 在 Firebox X Edge 管理页面找到 VPN Resources（VPN 资源）。




该设备的 VPN 资源如图所示。

2 点击 **Add（添加）**。




3 添加、编辑或去除 VPN 资源。
VPN 资源是指 VPN 用户可以安全连接的 IP 地址或网络地址。

4 点击 **OK（确认）**。
新的 VPN 资源将显示在列表上。

## Firebox X Edge 工具的启用

管理页面允许你为 Firebox X Edge 的配置及监控启用四种工具。

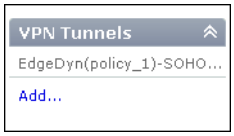
- HHostWatchEdge Web Manager（Edge Web 管理器）。你可以使用 Netscape 7.0（或更高版本）、Internet Explorer（互联网浏览器）6.0（或更高版本）、Mozilla Firefox 1.0（或更高版本）或同等浏览器。
- Firebox 系统管理器
- HostWatch
- Ping

如需启用这些设备，则应在 Firebox X Edge 管理页面上的 Tools （ 工具 ）栏中点击工具连接。


### 添加 Firebox X Edge VPN 隧道

Firebox X Edge 管理页面将显示所有隧道，包括 Tunnels （ 隧道 ）栏中的设备。你也可以在此隧道栏中添加一个 VPN 隧道。

1 在 Firebox X Edge 管理页面上选中 VPN Tunnels （ VPN 隧道 ）。




屏幕将显示所有隧道 （ 在这些隧道中，该设备是一个 VPN 端点 ）。

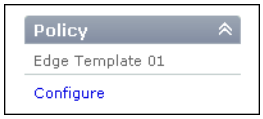
2 点击 **Add （ 添加 ）**添加新的 VPN 隧道。

Add VPN （ 添加 VPN ）向导将被启动。对 VPN 进行配置，使其符合你的 VPN 要求。

关于 Add VPN Wizard （ 添加 VPN 向导 ）的详情，请参阅 " *配置受管控的 VPN 隧道* " 章节。

### 使用 Firebox X Edge 策略界面

本界面介绍认购 Firebox X Edge 依据的 Edge Configuration Template （ Edge 配置模版 ）。你可以用本界面中的 **Configure （ 配置 ）**链接配置 Edge Configuration Template （ Edge 配置模版 ）。

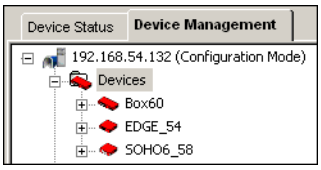



## Firebox SOHO 6 管理页面的使用

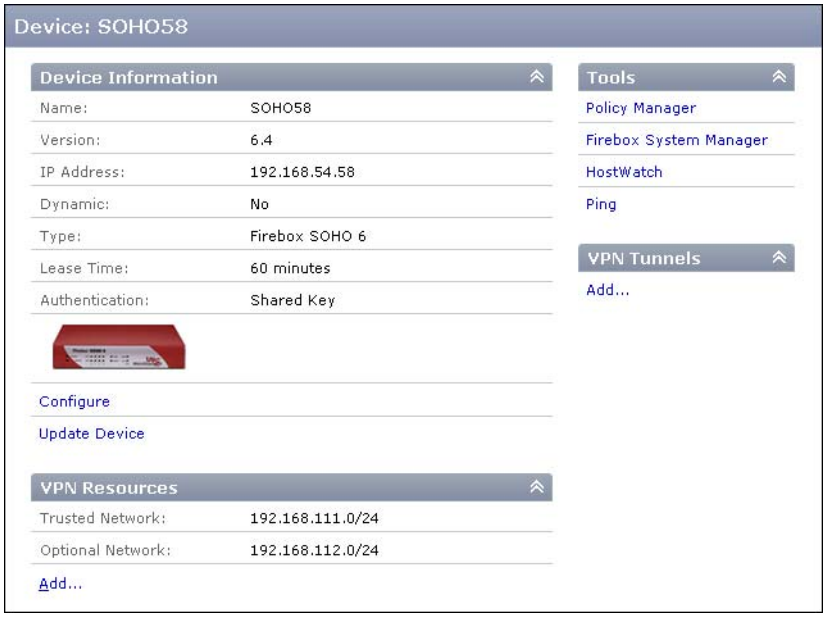
在将 Firebox ® SOHO 6 设备添加到一个管理服务器时，你可以使用管理页面对该设备的设置项进行配置。

## 查看 SOHO 6 管理页面

1 在 WSM 中点击 **Device Management**（**设备管理**）选项卡，展开 **Devices**（**设备**）。屏幕将显示受管理的设备列表。

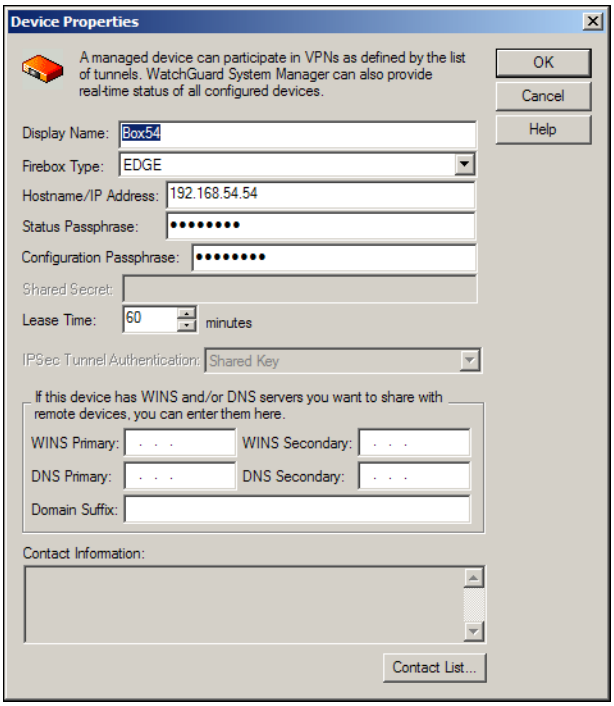



2 选择 Firebox SOHO 6。屏幕将出现该设备的管理页面。



## Firebox SOHO 6 管理属性的配置

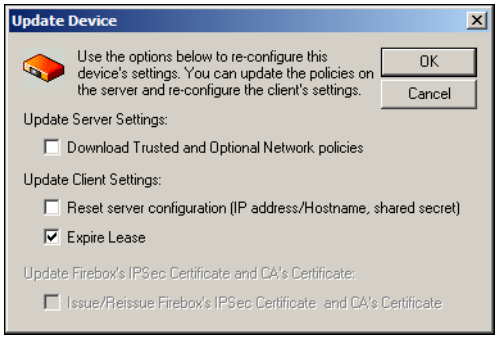
1 在 Firebox SOHO 6 管理页面中点击 **Configure （配置）**。
屏幕将出现 Device Properties （设备属性）对话框。




2 为该设备配置管理属性。更多有关本对话框中各个字段的信息，请参阅《Firebox SOHO 用户指南》。

## 设备更新

1 在 Firebox SOHO 6 管理页面中点击 **Update Device （更新设备）**。
屏幕将出现 Update Device （更新设备）对话框。

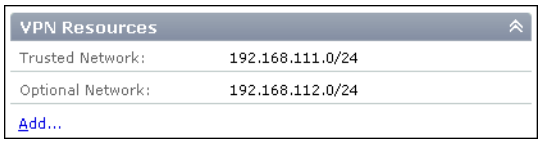



2 你可以通过使用该对话框从该设备中取得策略，为该设备重新设置管理服务器配置选项，并将管理协议作废。你也可以使用该对话框更新 Firebox 证书及 CA 证书 （如果该证书已被变更）。

3 点击 **OK （确认）**。

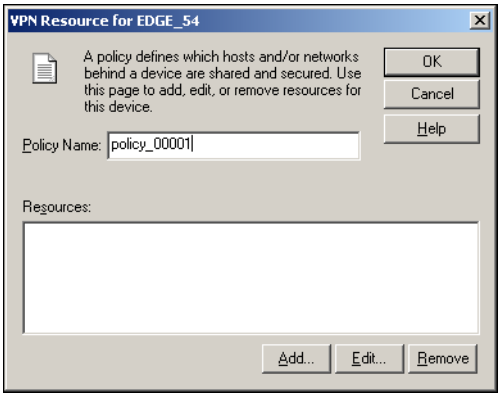
## 添加一个 VPN 资源

1 在 Firebox SOHO 6 管理页面中找见 VPN Resources （ VPN 资源 ）部分。




该设备的 VPN 资源如图所示。

2 点击 **Add （添加）**。




3 添加、编辑或去除 VPN 资源。

VPN 资源是指 VPN 用户可以安全连接的 IP 地址或网络地址。

4 点击 **OK （确认）**。

新的 VPN 资源将被显示在列表上。

## Firebox SOHO 6 工具的启用

管理页面允许你为 Firebox SOHO 6 的配置及监控启用四种工具 :

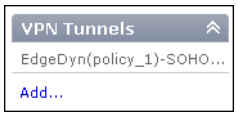
- 策略管理器 （ SOHO 6 配置 Web 页面 ）
- Firebox 系统管理器
- HostWatch
- Ping

如需启用这些设备，则应在 Firebox SOHO 6 管理页面上的 Tools （ 工具 ）栏中点击工具连接。

### 添加 Firebox SOHO 6 VPN 隧道

Firebox X Edge 管理页面将显示所有隧道，包括 Tunnels（隧道）栏中的设备。你也可以在此隧道栏中添加一个 VPN 隧道。

1 在 Firebox SOHO 6 管理页面上找出 VPN Tunnels （VPN 隧道）。




屏幕将显示包括该设备在内的所有隧道。

2 点击 **Add（添加）**添加新的 VPN 隧道。
Add VPN （添加 VPN）向导将被启动。对 VPN 进行配置，使其符合你的 VPN 要求。

## Edge 配置模版的创建及应用

当你使用带有 WatchGuard® 管理服务器的 Firebox® X Edge 设备时，你可以在管理服务器中创建 Edge Configuration Templetes（Edge 配置模版）。你可以将这些 Edge 配置模版应用到各个 Edge 设备。通过 Edge 配置模版，你可以轻松地对所有或部分受管理的 Edge 设备配置标准防火墙过滤器，修改受禁网站列表，修改你的 WebBlocker 配置，或修改其他策略设置。

**注释**

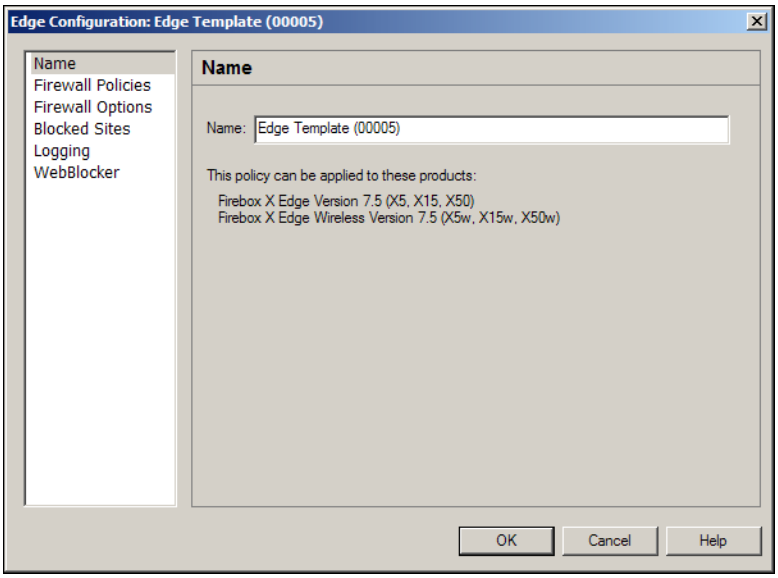
Edge 配置模版仅可以与 Firebox X Edge 一起使用。每一 Edge 设备仅可以有一个 Edge 配置模版。在使用 Edge 配置模版时，每一 Edge 必须配备有 7.5 或更高版本的固件。

你可以对已经应用了策略的 Edge 配置模版或设备列表进行修改。管理服务器将自动进行修改。

1 启动 WSM 并连接到管理服务器。

2 点击 **Device Management（设备管理）**选项卡。
你可以让系统详细显示 Edge 配置模版列表，查看所有已被创建的 Edge 配置模版。如果你没有创建任何 Edge 配置模版，则该列表为空。

3 点击右键，然后选择 **Insert Edge Configuration Template**（插入 **Edge** 配置模版）。




4 键入策略名。

5 如需对策略进行配置，则应依次点击对话框左窗口中的分类设置选项，并在弹出的字段中键入信息。上述类别包括：

- 防火墙策略
- 防火墙选项
- 受禁网站
- 日志（Logging）
- WebBlocker

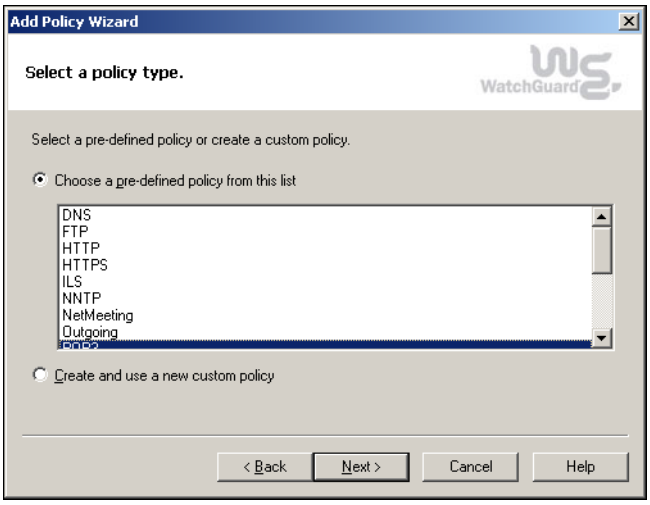
更多有关弹出字段的信息，请参阅 *《Firebox X Edge 用户指南》*。

6 点击 **OK**（**确认**），关闭 Edge 配置模版。
策略将被保存到管理服务器，而更新将被发送到所有适用本策略的 Firebox X Edge 设备。

## 使用 Add Policy（添加策略）向导添加预定义策略

1 在 **Device Management**（**设备管理**）选项卡中右键点击 **Edge Configuration Templates**（Edge **配置模版**）并选择 **Insert Edge Configuration Template**（插入 Edge **配置模版**）。选择 **Firewall Policies**（**防火墙策略**）并点击 **Add**（**添加**）。 **Add Policy**（**添加策略**）向导将被启动。

2 阅读 Welcome（欢迎）页面，然后点击 **Next（下一步）**。
屏幕将出现 Select a policy type（选择一个策略类型）页面。




3 如需使用预定义策略，应选择 **Choose a pre-defined policy from this list（从此列表中选择一个预定义策略）**，然后从该列表中选择所需的策略。

4 点击 **Next（下一步）**。

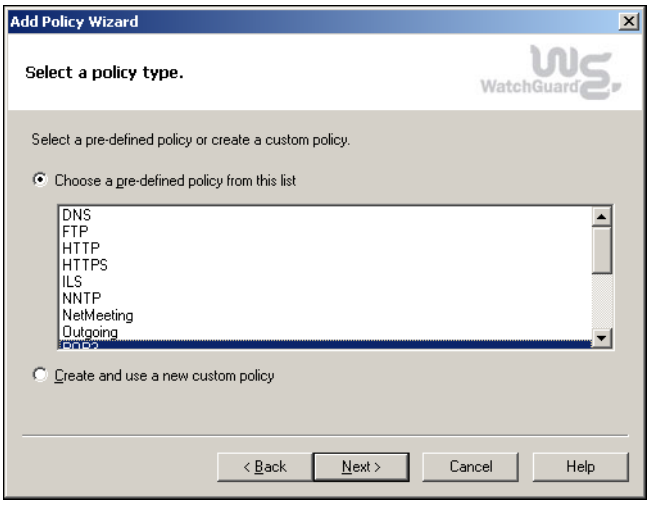
5 如需使用一个预定义策略，则应选择流量方向。

6 为此策略及方向选择拒绝或容许数据流。

## 使用添加策略向导添加一个自定义策略

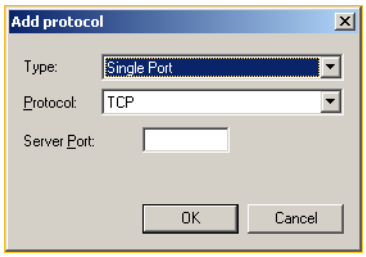
1 启动 Add Policy（添加策略）向导。启动该向导时需要在 Firewall Policies（防火墙策略）页面的 **Edge Configuration（Edge 配置）**对话框中点击 **Add（添加）**。

2 阅读 Welcome（欢迎）页面，然后点击 **Next（下一步）**。




3 选择 **Create and use a new custom policy（创建并使用一个新的自定义策略）**，创建并使用一个自定义策略。

4 点击 **Next（下一步）**。
屏幕将出现 Specify Protocols（指定协议）页面。
5 键入协议名称。
6 点击 **Add（添加）**，添加一个协议。
屏幕将出现 Add protocol（添加协议）对话框。




7 选择过滤 TCP、 UDP 或 IP 协议。
8 选择一个接口或范围。
9 键入端口编号或 IP 协议编号。点击 **OK（确认）**添加协议。
10 选择流量方向。选择 **Incoming（接收）**、 **Outgoing（外发）**或 **Optional（可选）**。
11 点击 **Add（添加）**添加另一协议。将该策略的所有协议添加完毕后，点击 **Next（下一步）**。
12 为过滤动作选择 **Allow（允许）**或 **Deny（拒绝）**。
如果过滤动作被设置为 **Allow（允许）**，则需要按要求 **From（从）**…**To（到）**…目的站。
13 点击 **Next（下一步）**。
14 点击 **Finish（完成）**，关闭向导并返回到 Edge 配置对话框。

## Edge 配置模版的复制

对于使用类似模版（仅需要做轻微改动）的同一类设备，对同一模版进行复制或拷贝非常实用。你可以制作一个 Edge 配置模版，然后为其他类似设备复制该模版，并对复制的模版进行相应修改。

1 在 Device Management（设备管理）窗口展开 **Edge Configuration Templetes（Edge 配置模版）**。
2 右键点击需要复制的 Edge 配置模版，然后选择 **Clone（复制）**。
在 Edge Configuration Templetes（Edge 配置模版）的列表中出现一个 Edge 配置模版 .
3 对复制的策略进行编辑。

## 将 Edge 配置模版应用到各个设备

你可以同时将同一 Edge 配置模版应用到一个 Firebox X Edge 或一组 Edge 设备。你无法将多个 Edge 配置模版应用到同一个 Edge 中。

### 通过拖放操作应用策略

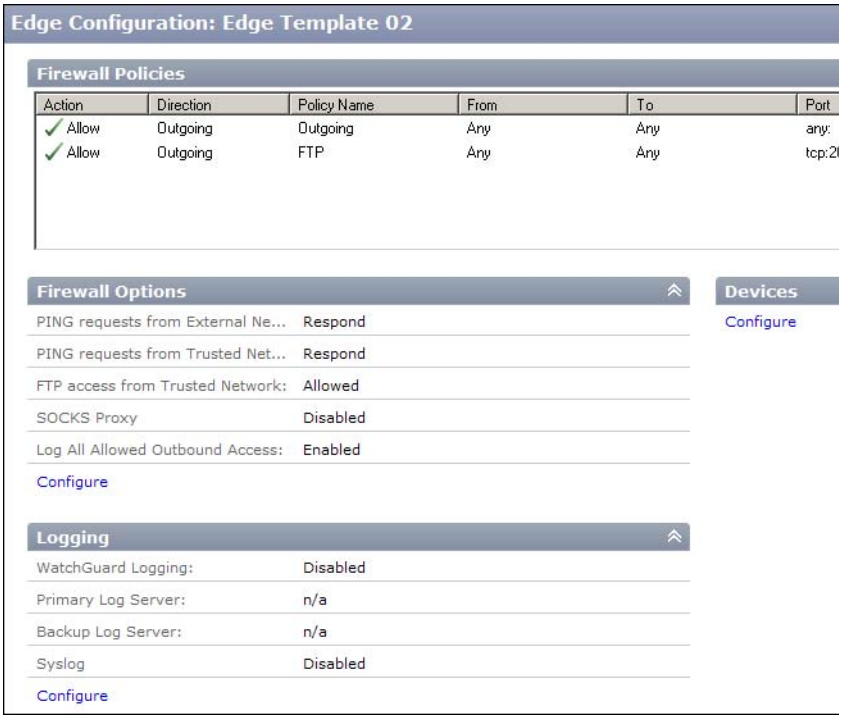
你可以通过拖放操作将一个 Edge 配置模版添加到 Firebox X Edge 设备。在设备列表中点击 Edge 设备。将 Edge 拖到 Edge 配置模版列表中的 Edge 配置模版上，然后将其放落到策略上。如此，该策略将被添加到该 Edge 中。

如果你有设备文件夹，你可以将此文件夹拖到 Edge 配置模版上方，将该 Edge 配置模版应用到文件夹中的所有 Edge 设备。所有其他类型的设备将被跳过。

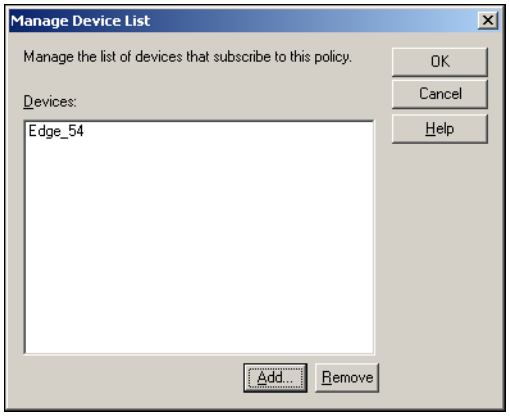
### 将策略应用到设备列表中的设备

1 选中 WSM 中的 **Device Management**（**设备管理**）选项卡，详细显示 Edge 配置模版列表。

2 选择策略，将其添加到一个设备。
策略配置将显示在窗口的右边框




3 点击 **Devices**（**设备**）区下面的 **Configure**（**配置**）链接。
屏幕将出现 Manage Devices（管理设备）界面。



4 点击 **Add（添加）**，将设备添加到列表。
屏幕将出现 Select Device（选择设备）对话框。


5 从下拉列表中选择 Firebox X Edge 设备。

6 点击 **OK（确认）**。再次点击 **OK（确认）**。
你选中的受管理设备将被输入 Edge 配置模版。

## Firebox X Edge 网络设置选项的管理

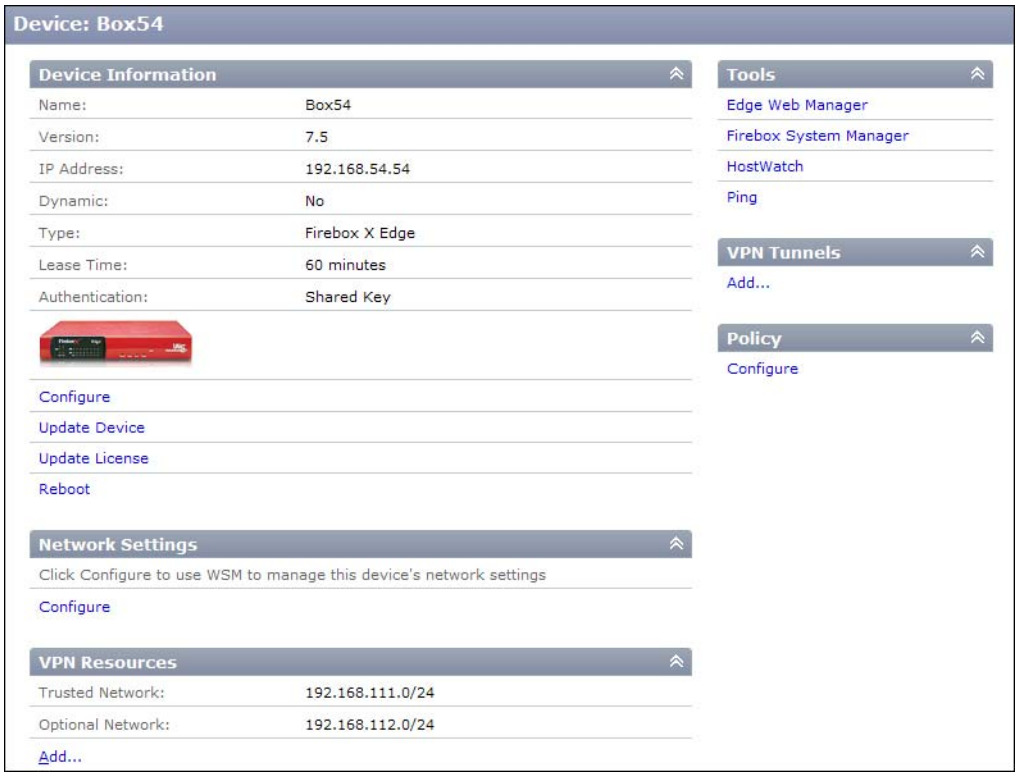
通过 WatchGuard® 管理服务器，你可以对一组使用 WSM 的 Firebox® X Edge 设备的网络设置选项进行配置。你可以使用 WSM 为每一 Firebox X Edge 配置特殊的网络设置。如果已经为 Edge 设定了正确的网络设置，你无需使用 WSM 对其进行修改（但如果你认为有必要，你可以对其进行修改）。

**注释**

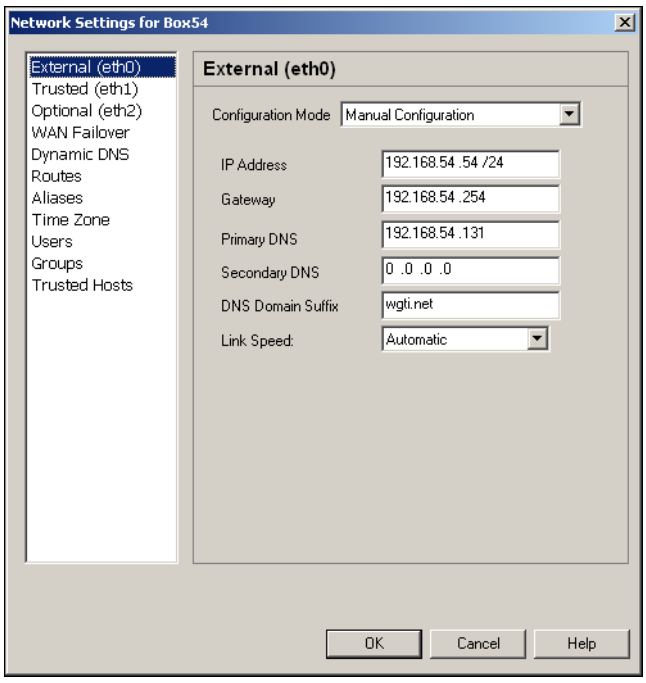
可以通过 Edge 的 Web 界面对所有 Firebox X Edge 网络设置选项进行配置。有关这些配置选项的详情，请参阅《Firebox X Edge 用户指南》。

1 点击 WSM 上的 **Device Management（设备管理）**选项卡。

2 详细显示 **Devices（设备）**，然后点击一个 Firebox X Edge 设备。
右窗口将出现 Edge 配置选项。




3 在 Network Settings（网络设置）项下点击 **Configure（配置）**。屏幕出现警示性提示后，点击 **OK（确认）**。
屏幕将出现 Edge 网络设置对话框。



4 在对网络设置选项进行配置时，需要点击对话框左窗口的每一设置类别并在屏幕上出现的字段填写信息。这些类别包括：
   - External (eth0)（外部站点）
   - Trusted (eth1)（受信站点）
   - Optional (eth2 )（可选站点）
   - WAN Failover（广域网故障转移）
   - Dynamic DNS（动态 DNS）
   - Routes（路由）
   - Aliases（别名）（更多有关 aliases 的信息，请参阅以下章节 “*Aliases 的使用*”）
   - Time Zone（时区）
   - Users（用户）
   - Groups（组）
   - Trusted Hosts（受信主机）

   更多有关字段的信息，请参阅《Firebox X Edge 用户指南》。
5 点击 **OK（确认）**，结束配置。

## Aliases 的使用

你可以通过 Firebox® X Edge 设备及 Aliases 为管理服务器上的策略配置功能定义一个普通目的站。例如，通过 Aliases，你可以为电子邮件创建一个 Edge 配置模版，并对策略进行定义，使其适用于你的电子邮件服务器。由于电子邮件服务器能在每一 Firebox X Edge 网络中拥有一个不同的 IP 地址，因此你可以在名称为 MailServer 的管理服务器中创建一个 Alias。当你为你的电子邮件服务器创建 Edge 配置模版时，你将该 Alias 用作目的站。然后你根据策略的判断，将该 Alias 定义为来源或目的站。在此示例中，你可以通过 MailServer 将输入的 [SMTP 允许 ] 策略配置到目的站。

要对使用该策略的各个 Edge 设备配置正确运行的 Edge 配置模版，你需要在 Network Settings（网络设置）中为每一 Firebox X Edge 设备配置 MailServer Alias（邮件服务器别名）。

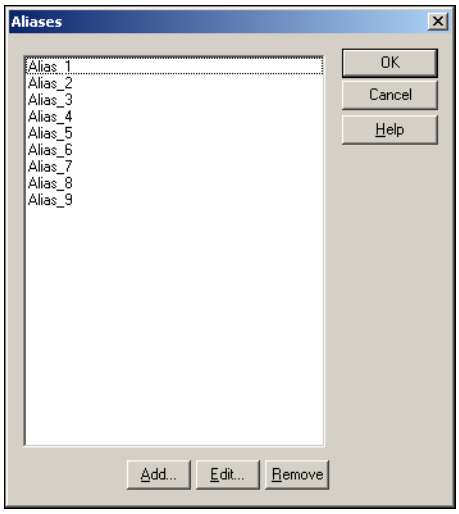
按以下步骤进行 Aliases 配置：

- 在管理服务器中为 Aliases 命名
- 在 Firebox X Edge 中定义 Alias IP 地址

## 在管理服务器中为 Aliases 命名

1 在 WSM 的 **Device Management**（**设备管理**）选项卡中，选择 Management Server（管理服务器）。
屏幕将弹出管理服务器页面。


2 点击 **Manage Aliases**（**管理 Aliases**）。
屏幕将出现 Aliases 对话框。




3 选择一个 Alias 并点击 **Edit**（**编辑**），对名称进行编辑。

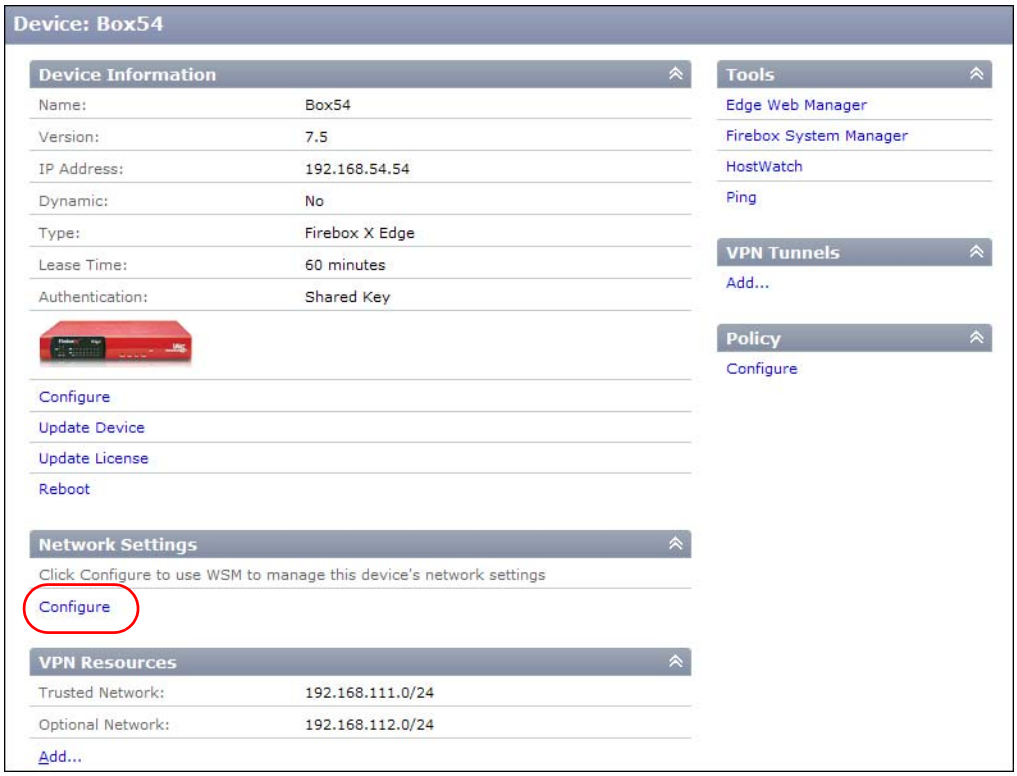
4 为 Alias 键入一个名称，然后点击 **OK**（**确认**）。

5 重复该步骤，直到将所有必须定义的 Aliases 定义完毕。

6 完成对所有 Aliases 的配置后，点击 **OK（确认）**。

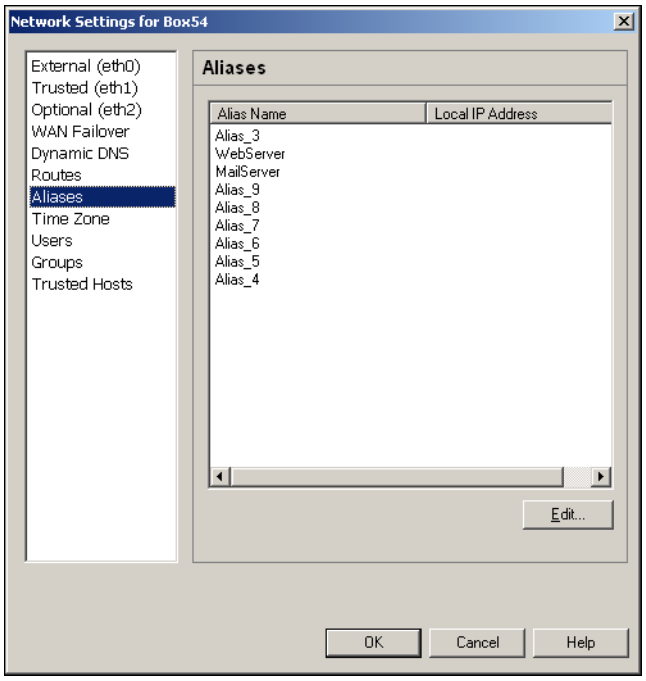
## 在 Firebox X Edge 中定义 Aliases

1 在 WSM 的 **Device Management（设备管理）**选项卡中，选择 Firebox X Edge。
屏幕将弹出管理服务器页面。




2 在 **Network Settings（网络设置）**项下点击 **Configure（配置）**。
屏幕将出现 Network Settings 对话框。

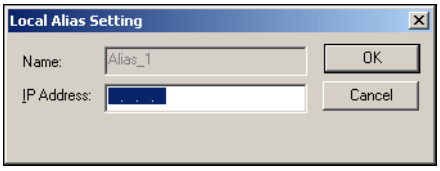
3 点击 **Aliases**




屏幕将出现 Aliases 对话框。你在管理服务器中命名的 Aliases 将与本对话框中的这些名称一起显示在界面中。

4 选择要定义的 Alias，然后点击 **Edit（编辑）**。

屏幕将出现 Local Alias Setting（本地 Alias 设置）对话框。




5 在此 Firebox X Edge 的网络中为本地 alias 键入 IP 地址。点击 **OK（确认）**。

6 重复此流程，直到将所有 Aliases 定义完毕。

7 在所有 Aliases 定义完毕后，点击 **OK（确认）**。

# 第 22 章 用 PPTP 配置 RUVPN

远程用户虚拟专用网（RUVPN）使用点对点隧道协议（PPTP）进行安全连接，可以支持 50 位用户同时使用每一 Firebox® 。 RUVPN 用户可以通过 Firebox 或 RADIUS 验证服务器获得验证。你必须对远程用户的 Firebox 及远程主机进行配置。

## 配置清单

在对 Firebox® 进行 RUVPN 配置之前，你需要记录以下信息：

- 远程用户使用的 RUVPN 隧道 IP 地址。**不可将这些 IP 地址设置为该 Firebox 所辖网络使用的地址。**向 RUVPN 用户提供地址的最快速方法是安装一个带有一系列 IP 地址的 “Placeholder（占位器）”二次网络。然后从该网络随带的地址范围内选择一个 IP 地址。例如，在你的受信网络 10.10.0.0/24 中创建一个新的子网，作为二次网络。在此子网选择需要的 IP 地址，将其作为你的 PPTP 地址。更多信息请参阅 152 页的 “**IP 寻址**”。
- DNS 及 WINS 服务器的 IP 地址，这些服务器可将主机名转化为 IP 地址。
- 用户的用户名及口令，这些用户被允许通过 RUVPN 连接到 Firebox。

### 加密级别

如果是使用 PPTP 的 RUVPN，你可以选用 128 比特的加密连接或 40 比特加密连接。如果是美国国内版本的 Windows XP，则可以使用 128 比特的加密连接。你可以从 Microsoft 为其他版本的 Windows 取得强大的加密补丁。你应该为 Firebox 首选 128 比特的加密连接。如果你的用户无法使用 128 比特的加密连接，则可以使用 40 比特（如果已被激活）的加密连接。

更多有关如何将 128 比特的加密连接降低至 40 比特，请参阅 284 页的 “*准备用户电脑*”。

如果你不再美国居住而且你必须为你的 LiveSecurity 服务账户取得强大的加密功能，请发送电子邮件至 supportid@watchguard.com，该电子邮件应包括：

- 你的 LiveSecurity 服务密钥号码
- 购买日期
- 公司名称

- 公司邮送地址
- 电话号码及名称
- 电子邮件地址

**如果你在美国居住，**你必须在 LiveSecurity™ 服务网站中，从你的档案页面下载强大的加密软件。登陆 www.watchguard.com，点击 **Support（支持）**，进入你的 LiveSecurity 服务账户，然后点击 **Latest Software（最新软件）**，然后下载具有强大加密功能的 WSM。

然后，你需要卸载原有的 WSM，并从已下载的文件中安装具有强大加密功能的 WSM。

**注释**

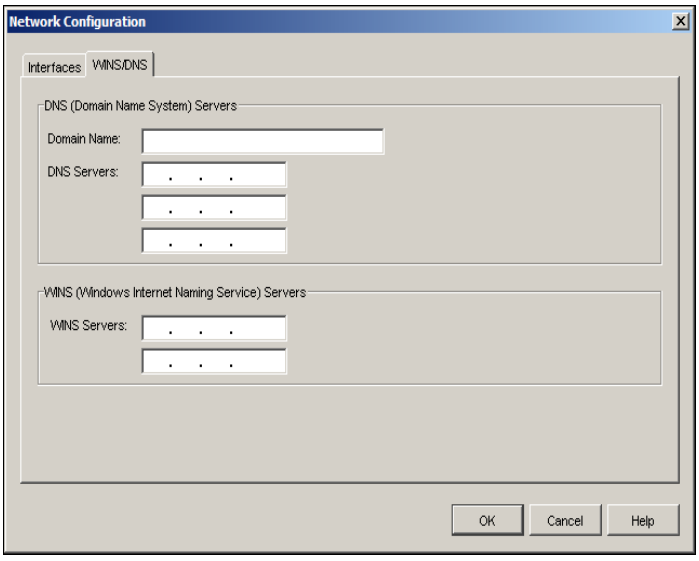
如果需要保留原有的 Firebox 配置，请不要在安装新的软件时使用 [ 快速安装向导 ]。打开 WSM，连接到 Firebox，然后保存你的配置文件。原有配置可与不同版本的加密软件相互兼容。

## WINS 及 DNS 服务器的配置

RUVPN 用户使用共享的 Windows 互联网名称服务（WINS）及域名系统（DNS）服务器地址。DNS 将主机名改变为 IP 地址，而 WINS 将 NetBIOS（网络输入输出系统）名称改变为 IP 地址。Firebox® 的受信接口必须能够接通这些服务器。

1 在 Policy Manager（策略管理器）中点击 **Network（网络）>Configuration（配置）**。点击 **WINS/DNS** 选项卡。
屏幕将出现 WINS 及 DNS 服务器相关。

2 在 IP 地址文本框中为 WINS 及 DNS 服务器键入地址。你可以为 DNS 服务器键入三个地址，并为 WINS 服务器键入两个地址。为 DNS 服务器键入一个域名。




## 激活使用 PPTP 的 RUVPN

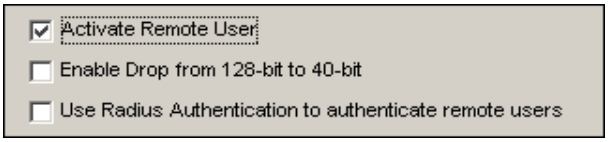
在对使用 PPTP 的 RUVPN 进行配置前，你必须激活该功能。使用 PPTP 的 RUVPN 会将

WatchGuard® PPTP 策略图标添加到 Policy Manager（策略管理器）。通过该步骤，系统将各个 PPTP 连接及这些连接中的输入 / 输出流设定为默认属性。我们建议你不要对 WatchGuard PPTP 策略的默认属性进行修改。

1 在 Policy Manager（策略管理器）中点击 **VPN>Remote Users（远程用户）**。点击 **PPTP** 选项卡。

2 选择 **Activate Remote User（激活远程用户）**复选框。

3 如有必要，选择 **Enable Drop From 128-bit to 40-bit（启用从 128 比特降低到 40 比特功能）**复选框。
通常，美国之外的客户才使用该复选框。




### 激活扩展认证

作为 Firebox® 的备选方案，带有扩展认证功能的 RUVPN 可以让用户在 RADIUS 认证服务器中取得认证。更多有关扩展认证的信息，请参阅 151 页的 “*扩展认证*”。

1 选择 **Use RADIUS Authentication to authenticate remote users（使用 RADIUS 认证对远程用户进行认证）**复选框。请参照先前部分的数值。

2 在 **Authentication Servers（认证服务器）**对话框中对 RADIUS 服务器进行配置。请参照 111 页的 “*实施配置*”。

3 在 RADIUS 服务器中创建一个 PPTP 用户组并添加 PPTP 用户的名称或组别。

## 为 RUVPN 隧道添加 IP 地址

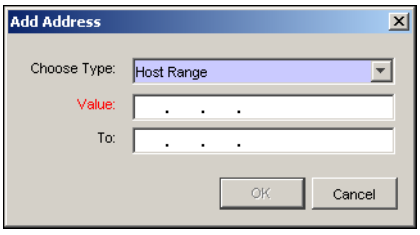
使用 PPTP 的 RUVPN 可以同时支持 50 位用户。 Firebox® 从一组可选地址中持续向每位入站的 RUVPN 用户提供一个开放 IP 地址，直到所有地址均被占用。在用户将一个隧道关闭之后，其地址将被收回到可选地址组中，并分配给下一位登陆的用户。

有关如何为 RUVPN 用户取得 IP 地址的详情，请参阅 152 页的 “*IP 寻址*”。

为了确保 PPTP 能正常运行，你必须配置两个或更多 IP 地址。

在 **Remote Users Configuration（远程用户配置）**对话框的 **PPTP** 选项卡中：

1 点击 **Add（添加）**。
屏幕将出现 Add Address（添加地址）对话框。



2 从 **Choose Type（选择类型）**下拉列表中选择 **Host IP（主机 IP）**（如果是单个 IP 地址）或 **Host Range （主机范围）**（如果是一系列 IP 地址）。
你可以配置 50 个地址。如果选择了 [ 主机地址 ]，你必须至少添加两个 IP 地址。如果选择了 [ 主机范围 ] 而且添加的 IP 地址数量超过了 50，使用 PPTP 的 RUVPN 将使用 [ 主机可选地址范围 ] 内的前 50 个 IP 地址。

3 在 **Value（数值）**文本框中键入主机 IP 地址。如果你选择了 **Host Range（主机范围）**，则应键入主机可选 IP 地址范围内的第一及最后一个 IP 地址，然后点击 **OK（确认）**。
键入未使用的而且 Firebox 可以在 RUVPN（使用 PPTP）会话期间为用户提供的 IP 地址。该 IP 地址将出现在可为远程用户提供的地址列表中。

4 重复上述步骤，直到将所有供 [ 使用 PPTP 的 RUVPN] 使用的地址配置完毕。

## 将新用户添加到 PPTP 用户认证组

要在 Firebox® 中创建 PPTP VPN 隧道，远程用户需要键入用户名及密码，获得认证。

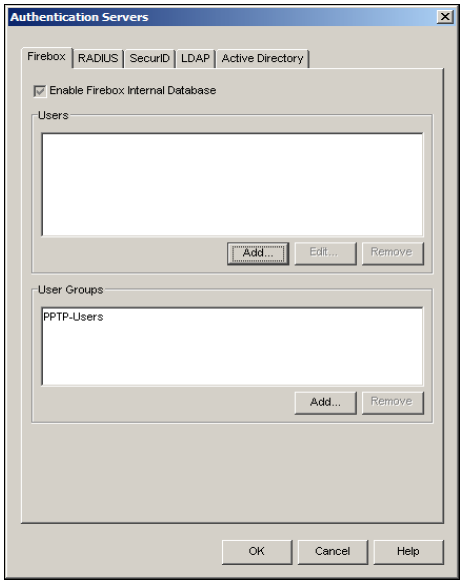
WatchGuard® 系统管理器软件使用该信息让用户在 Firebox 中获得认证。

你在 Firebox 配置中激活了 PPTP 后，系统将自动创建一个默认的用户组。该用户组被称为 pptp 用户。你在创建一个新用户或将用户名添加到策略时可以看到该用户组的名称。

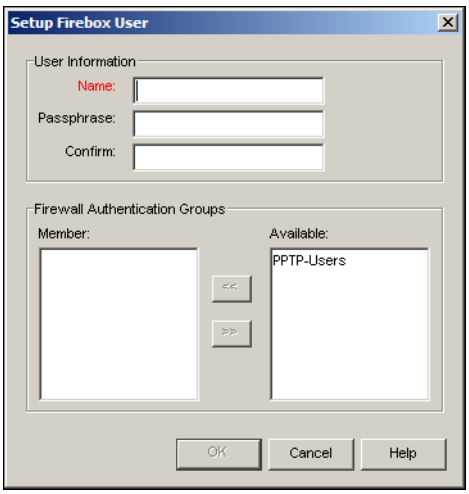
有关 Firebox 用户组的详情，请参阅 111 页的 “实施认证”。

1 在 Policy Manager（策略管理器）中点击 **Setup （设置）>Authentication Servers （认证服务器）**。
屏幕将出现 [ 认证服务器 ] 对话框。

2 点击 **Firebox** 选项卡。



3 点击 **Users （用户）**列表项下的 **Add （添加）**按钮，添加新的用户。
屏幕将出现 [ 设置 Firebox 用户 ] 对话框。




4 为新用户键入用户名及口令。再次键入口令，进行确认。
新用户将被置入 [ 用户列表 ]。[ 认证服务器 ] 对话框将保持打开状态，便于你添加更多用户。

5 关闭 **Authentication Servers （认证服务器）**对话框，点击 **OK （确认）**。
你可以使用用户及用户组对策略进行配置。请参阅下述章节。

## 对策略进行配置，使其允许入站的 RUVPN 数据流通过

RRUVPN 用户没有任何权限通过 Firebox 访问任何资源。你必须为策略添加用户名或完整的 PPTP 用户组，以便向远程用户提供访问具体网络资源的权限。

对于 RUVPN 数据流的策略配置， WatchGuard 推荐两种配置流程：individual policies （单个策略）或 Any policies （所有策略）。在对 RUVPN 数据流进行控制配置时，我们推荐使用 [ 单个策略 ]。[ 所有策略 ] 将为认证过的 RUVPN 用户在整个 Firebox 中开启一个缺口，使主机之间的流量完全不受防火墙规则的限制，因此 [ 所有策略 ] 存在一定的安全隐患。

### [ 单个策略 ]

在 Policy Manager （策略管理器）中，双击一项策略，为你的 VPN 用户启用该策略。推荐为 PPTP 数据流特别创建一项新的策略，使其与你的其他防火墙策略分离。属性设置：

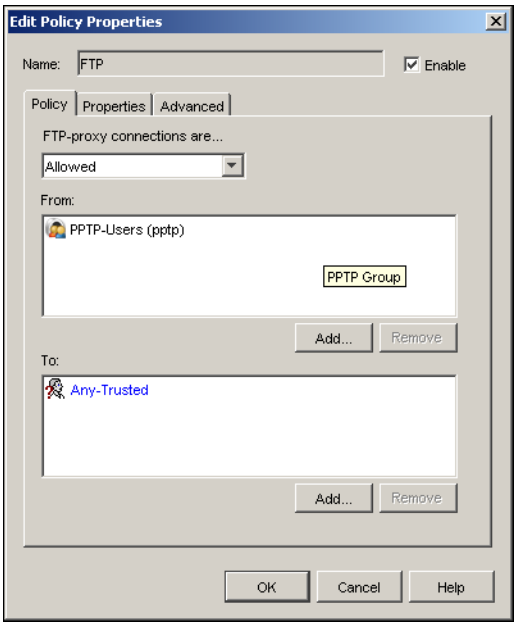
*入站数据流控制策略：*

- 允许
- 从：PPTP 用户或用户组
- 至：受信、可选、网络或主机 IP 地址或 alias

*出站数据流控制策略：*

- 允许
- 从：受信、可选、网络或主机 IP 地址或 alias

– 至：PPTP 用户或用户组




### Any policies[ 所有策略 ] 的使用

将下列属性添加到 Any policies （ 所有策略 ）：

*入站数据流控制策略：*

– 允许

– 从：PPTP 用户或用户组

– 至：受信、可选、网络或主机 IP 地址或 alias

*出站数据流控制策略：*

– 允许

– 从：受信、可选、网络或主机 IP 地址或 alias

– 至：PPTP 用户或用户组

修改之后，请务必将配置文件保存到 Firebox。

**注释**

如果需要使用 WebBlocker 对远程用户的访问权限进行控制，你应该将 PPTP 用户或用户组添加到控制 WebBlocker 的代理策略中 （ 如 HTTP 代理 ）。你应该使用此种类型的策略，并将包滤波器或代理策略作为 [ 所有策略 ] 的备选方案。

## 客户端电脑的准备

你必须首选将你使用的每一台电脑配置为可以访问互联网的 PPTP RUVPN 远程主机。然后，按照下后续章节中的指示进行以下操作：

- 安装可行版本的 Microsoft 拨号上网软件以及必要的服务包。

- 为各个 VPN 连接提供操作系统。
- 安装一个 VPN 适配器（无需为所有的操作系统安装）。

### 安装 MSDUN 及服务包

为使 RUVPN 达到正确配置，你有必要安装以下功能软件：

- MSDUN（Microsoft 拨号上网）升级程序
- 其他扩展软件
- 服务包

如果是使用 PPTP 的 RUVPN，你有必要安装以下升级程序：

| 加密 | 平台 | 应用 |
|---|---|---|
| 基础型 | Windows NT | 40 比特 SP4 |
| 增强型 | Windows NT | 128 比特 SP4 |
| 基础型 | Windows 2000 | 40 比特 SP2* |
| 增强型 | Windows 2000 | 128 比特 SP2 |

*40 比特加密功能是 Windows 2000 的默认功能。如果你的系统是从 Windows 98（带增强型加密功能）升级到 Windows 2000 的，系统将自动为新的安装程序设置增强型加密功能。

要安装这些升级程序或服务包，请访问 Microsoft 下载中心网站：

http://www.microsoft.com/downloads/search.asp

## 在 Windows XP 中创建及连接到 PPTP RUVPN

在准备 Windows XP 远程主机时，你必须对网络连接进行配置。

在客户端电脑的 Windows 桌面上进行以下操作：

1 点击 **Start（开始）>Control Panel（控制面板）>Network Connections（网络连接）**。
屏幕将出现 [ 网络连接 ] 向导。

2 在左侧的菜单中点击 **Create a new connection（创建一个新的连接）**。[ 新增连接 ] 向导将被启动。点击 **Next（下一步）**。

3 点击 **Connect to network at my workplace（连接到我的工作室网络）**。点击 **Next（下一步）**。

4 点击 **Virtual Private Network Connection（VPN 连接）**。点击 **Next（下一步）**。

5 为新增的连接命名，例如“与 RUVPN 的连接”。点击 **Next（下一步）**。

6 选择将此连接设置为非拨号上网（如果是宽带连接）或为自动拨号上网（如果是调制调解器连接）。点击 **Next（下一步）**。
如果你使用 Windows XP SP2，向导将显示此界面。不是所有的 Windows XP 用户可以看见此界面。

7 键入 Firebox 外部接口的主机名称或 IP 地址，并点击 **Next（下一步）**。

8 选择可以使用此连接简档的人员，并点击 **Next（下一步）**。

9 选择 **Add a shortcut to this connection to my desktop（将此连接的快捷方式添加到我的桌面）**，然后点击 **Finish（完成）**。

10 如果需要连接到你的新增 VPN 连接隧道，你需要首先通过拨号网络或直接通过 LAN 或 WAN 进行互联网连接。

11 双击你桌面上新增连接的快捷方式。
或选择 Control Panel（控制面板）>Network Connections（网络连接），然后在 Virtual Private Network（VPN 列表）中查找你创建的连接。.

12 为你的连接键入用户名及口令。
此信息应该在将用户添加至 pptp_users（pptp 用户）时输入。参阅 282 页的 “*将新用户添加到 PPTP 用户认证组*”。

13 点击 **Connect（连接）**。

# 在 Windows 2000 中创建及连接到 PPTP RUVPN

在准备 Windows 2000 远程主机时，你必须对网络连接进行配置。

在客户端电脑的 Windows 桌面上进行以下操作：

1 点击 **Start（开始）>Settings（设置）>Network Connections（网络连接）>Create a New Connection（创建新的连接）**。
屏幕将出现 New Connection [ 新增连接 ] 向导。

2 点击 **Next（下一步）**。

3 选择 **Connect to the network at my workplace（连接到我的工作室网络）**。点击 **Next（下一步）**。

4 点击 **Virtual Private Network connection（VPN 连接）**。

5 为新增的连接命名，例如 “与 RUVPN 的连接”。点击 **Next（下一步）**。

6 选择将此连接设置为非拨号上网（如果是宽带连接）或为自动拨号上网（如果是调制调解器连接）。点击 **Next（下一步）**。

7 键入 Firebox 外部接口的主机名称或 IP 地址，并点击 **Next（下一步）**。

8 选择 Add a shortcut to this connection to my desktop（将此连接的快捷方式添加到我的桌面），然后点击 **Finish（完成）**。

9 如果需要连接到你的新增 VPN 连接隧道，你需要首先通过拨号网络或直接通过 LAN 或 WAN 进行互联网连接。

10 双击你桌面上新增连接的快捷方式。
或选择 Control Panel（控制面板）>Network Connections（网络连接），然后在 Virtual Private Network（VPN 列表）中查找你创建的连接。

11 为你的连接键入用户名及口令。
此信息应该在将用户添加至 [pptp 用户 ] 时输入。参阅 282 页的 “*将新用户添加到 PPTP 用户认证组*”。

12 点击 **Connect（连接）**。

## 运行 RUVPN 并访问互联网

你可以让远程用户通过 RUVPN 隧道连接到互联网，但该操作对网络安全有一定影响。请参阅 155 页的 “*隧道的创建方法*”。

1 在客户端电脑设置你的连接时，你应该使用 **Advanced TCP/IP Settings（高级 TCP/IP 设置）**对话框，然后选择 **Use default gateway on remote network（在远程网络上使用默认网关）**复选框。

在 **Control Panel（控制面板）>Network Connections（网络连接）**中右键点击 VPN 连接，打开 Windows XP 或 Windows 2000 上的 Advanced TCP/IP Settings（高级 TCP/IP 设置）对话框。选择 **Properties（属性）**，然后点击 **Network（网络）**选项卡。在列表框中找见 **Internet Protocol（网络协议）**，然后点击 **Properties（属性）**。在 **General（普通）**选项卡中点击 **Advanced（高级）**。

2 确定你添加到 PPTP 地址库中的 IP 地址已被包括在你的动态 NAT 配置中。具体操作为：在 Policy Manager（策略管理器）中选择 **Network（网络）>NAT**。

3 对你的策略配置进行修改，使系统能允许 PPTP 用户通过外部接口进行连接。如果需要使用 WebBlocker 对远程用户的访问权限进行控制，应将 PPTP 用户添加到控制 WebBlocker 的策略中（如 HTTP 代理）。

## 从不同的 Firebox 创建出站 PPTP 连接

如有必要，你可以通过一个不同的 Firebox 创建一个 PPTP 连接。例如，如果一位远程用户要访问客户配备有 Fireboxμƒoffice，该用户可以使用 PPTP 创建该 Office 与其网络的连接。为使本地 Firebox 能正确允许出站 PPTP 连接，需要添加 PPTP 策略，并允许 Any-External（所有外部连接）使用 PPTP。有关激活策略的详情，请参阅本指南的 “*配置策略*”章节。

# 第 23 章　用 WebBlocker 控制网站访问

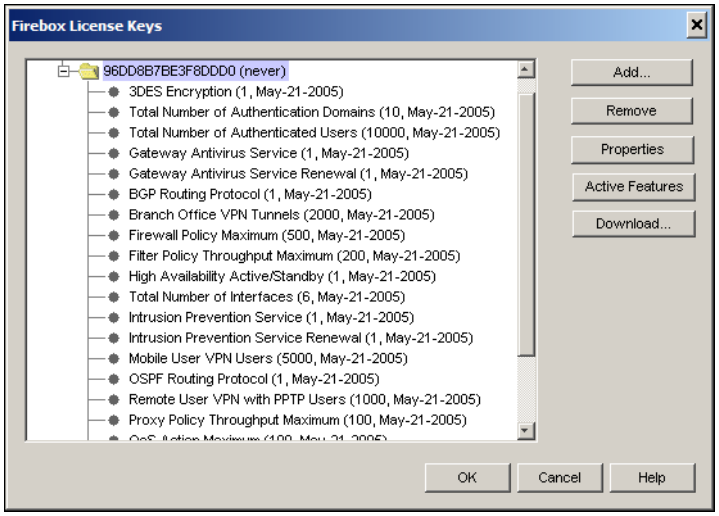
WatchGuard® Fireware® 的 WebBlocker 用 HTTP 代理服务器对 web 数据流进行控制。你可以设定精确的上网时限，仅允许用户每天在此时限内浏览互联网。你也可以设定受禁网站种类，禁止用户访问受禁网站。

## 安装软件许可

要安装 WebBlocker，你必须取得一个 WebBlocker 授权码并到 LiveSecurity 网站注册。注册后，LiveSecurity 将向你提供一个新的功能密钥。

安装该功能密钥需要进行以下操作：

1　在 Policy Manager（策略管理器）中选择 **Setup（设置）**>**Licensed Features（许可功能）**。
屏幕将出现 Firebox License Keys（Firebox 许可密钥）对话框。




2　点击 **Remove（删除）**，删除当前功能密钥。
你必须在安装新密钥前将包括 WebBlocker 在内的整个功能密钥完全删除。

3 点击 **Add（添加）**。

4 在 **Add Firebox Key（添加 Firebox 密钥）**对话框中，键入或粘贴你的许可密钥。你可以点击 **Import（导入）**，将密钥导入你的电脑或网络，然后点击 **OK（确认）**。
许可密钥将出现在 Firebox License Keys（Firebox 许可密钥）对话框中。

# 使用 WebBlocker 启动

在安装 WSM 时，你可以在 WatchGuard® 管理工作站上安装 WebBlocker Server（WebBlocker 服务器）。你也可以在一个不同的电脑上安装 WebBlocker Server 软件。具体安装方法与安装 WSM 软件的流程一样，但是需要选中 WebBlocker Server 组件。

可支持 WebBlocker 的操作系统是 Windows 2000 及 Windows 2003。

**注释**

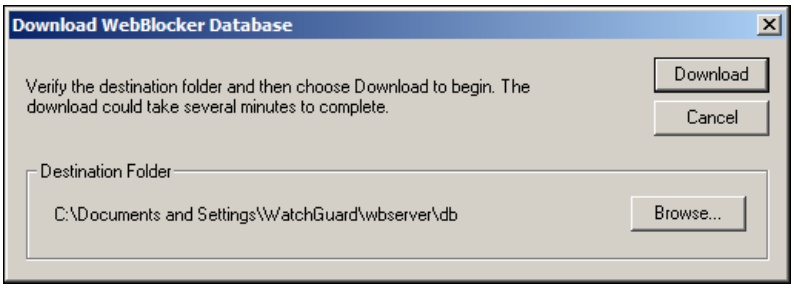
如果你将其中一个 WSM 安装到了一台使用个人防火墙（而非 Microsoft Windows 防火墙）的电脑上，你必须打开各个服务器的端口，使其能够连接到防火墙。要允许连接到 WebBlocker Server，你需要打开 UDP 端口 5003。如果你使用的是 Microsoft Windows 防火墙，你有必要对配置进行修改。详情请参阅 “*开始使用*”章节。

在配置 WebBlocker 前，必须下载 WebBlocker 数据库。

1 在屏幕底部的工具条上右键点击 WebBlocker Server 图标。

2 选择 **Get Full Database（获取完整的数据库）**。
屏幕将出现 Download WebBlocker Database（下载 WebBlocker 数据库）对话框。

3 选择 **Download（下载）**，下载新数据库。




**注释**

WebBlocker 数据库超过 95MB。连接速度将决定数据库的下载速度，因此该数据库的下载时间可能会超过 30 分钟。请确定硬盘有至少 200MB 的可用空间。

你可以随时使用 WebBlocker 进行以下操作：

- 下载新版数据库
- 查看数据库状态
- 启动或停止服务器

在对 WebBlocker 数据库进行增量更新前，必须首先让 WebBlocker Server 停止提供服务。具体操作为在 WatchGuard 工具条上右键点击 WebBlocker Server 图标，选择 **Stop Service（停止服务）**。

### 自动下载 WebBlocker 数据库

保持 WebBlocker 始终处于最新更新状态的最好办法是用 Windows Task Scheduler（Windows 计划任务程序）。你可以用 Windows 计划任务程序对 “updatedb.bat”程序进行调整，该程序是系统在 WSM8/bin 目录中为你自动创建的程序。

1 打开 **Scheduled Tasks（计划任务）**。要打开使用 Windows XP 的 Windows Task Scheduler（Windows 计划任务程序），需要点击 **Start（开始）**，点击 **ALL Programs（所有程序）**，将鼠标指向 **Accessories（附件）**及 **System Tools（系统工具）**，然后点击 **Scheduled Tasks（计划任务）**。

2 点击 **Add Scheduled Task（添加计划任务）**。

3 Scheduled Tasks（计划任务）向导将被启动。点击 **Next（下一步）**。

4 屏幕将显示程序列表。点击 **Browse（浏览）**。

5 进入 C:\Program Files\WatchGuard\wsm8\bin。选择 **updatedb.bat**。

6 选择执行此任务的时间间隔。我们推荐每天对数据库进行更新。如果你的宽带资源偏低，你可以调低更新频率。点击 **Next（下一步）**。

7 键入程序启动的时间及频率。由于更新时必须停止 WebBlocker Server 的运行，因此我们建议你将计划更新任务安排到非繁忙时段。

8 选择开始日期。点击 **Next（下一步）**。

9 键入使用该程序的用户名及口令。确定此用户有权访问必要的文件。点击 **Next（下一步）**。

10 点击 **Finish（完成）**。

## 激活 WebBlocker

在 HTTP 代理策略中使用 WebBlocker 之前，必须用 Activate WebBlocker（激活 WebBlocker）向导激活该功能并建立基础配置。具体操作为：

1 要使用 WebBlocker，在 WSM 中选择 Firebox®。

2 选择 **Tools（工具）>Policy Manager（政策管理器）**。

或者，
也可以在 WSM 工具条上选择 Policy Manager（策略管理器） Policy Manager（策略管理器）图标。

3 在 Policy Manager （策略管理器）中选择 **Tasks （任务）>WebBlocker>Activate （激活）**。
Activate WebBlocker Wizard （激活 WebBlocker 向导）将被启动。


4 点击 **Next （下一步）**。

5 按照向导的指示进行点击操作，并输入向导要求的各种信息。向导将弹出以下界面：

### 为 WebBlocker 选择策略

如果仍未对 HTTP 代理策略进行定义，则该界面不会出现。在此情况下，向导将为你创建一个 HTTP 代理策略。

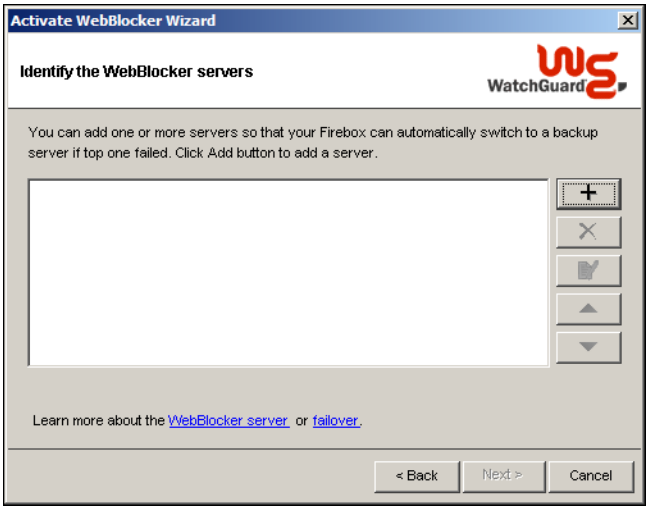
如 HTTP 代理策略已被创建到 Firebox，此界面将在列表中显示这些策略。从该列表中选择激活 WebBlocker 所需的代理策略。如果未选择任何策略，则系统将在 WebBlocker 中创建一个新的 HTTP 代理策略。

### 识别 WebBlocker 服务器

必须至少对一个 WebBlocker Server 进行配置。要添加 WebBlocker Server，点击加号 (+)。在 **Server IP （服务器 IP）**下一栏键入 WebBlocker Server 的 IP 地址。如有必要，修改端口编号。

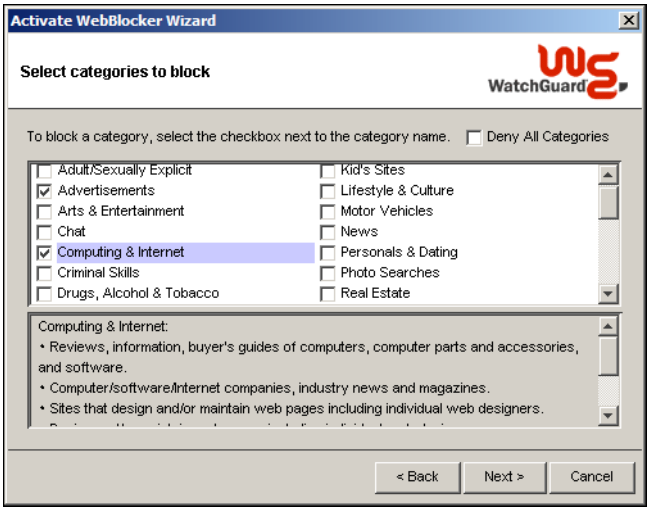
你可以添加多个 WebBlocker Server，以便在无法连接到主服务器时， Firebox 可以连接到备用服务器。主服务器是指列表中的主服务器。

在完成向导提示的操作后，如果需要添加 WebBlocker Server，则需要选择 **Setup**（**设置**）**>Actions**（**对策**）**>WebBlocker**。在 **Servers**（**服务器**）选项卡中添加服务器。




## 选择受禁网站的类别

**选**择想禁止的网站类别的复选框。阅读类别描述，选择相应的复选框。在选中一个复选框后，该复选框相对应的网站类别描述将出现在界面的底部。如果你想禁止用户访问界面中列示出的所有网站类别，则应该选择 **Deny All Categories**（**禁止所有类别**）。



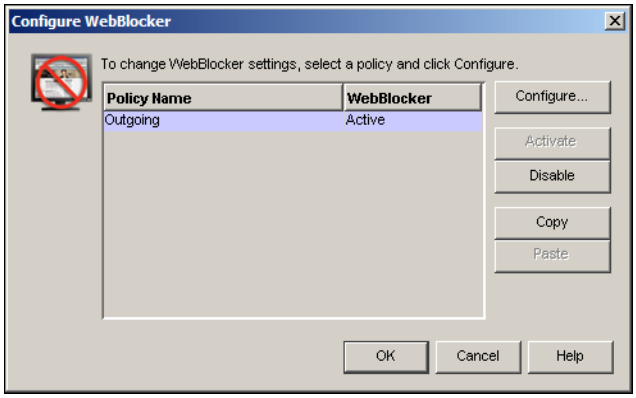

**注释**

如果要禁止用户试图避开 WebBlocker 而访问匿名网站，你应该在 WebBlocker 中禁止 Remote Proxies（远程代理）类别。

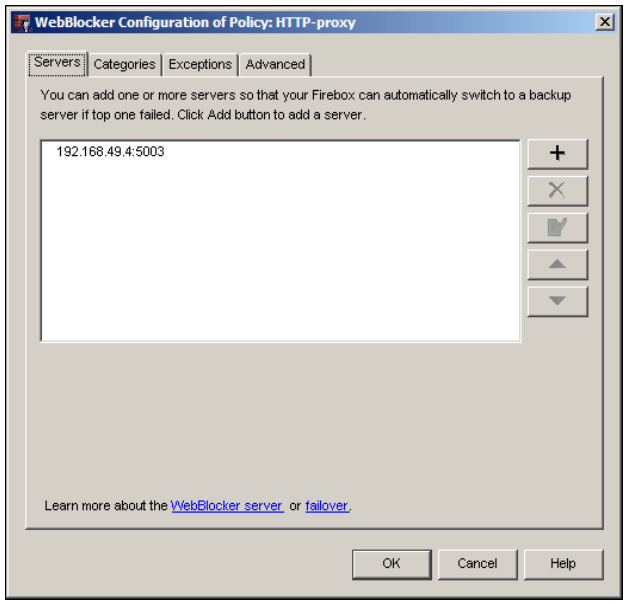
# 配置 WebBlocker

你在使用 Activate WebBlocker Wizard （激活 WebBlocker 向导）激活 WebBlcoker 并创建出基础配置后，你可以对 WebBlcoker 的更多设置选项进行配置。

1 在 Policy Manager （策略管理器）中选择 **Tasks （任务）>WebBlocker>Configure （配置）**。
屏幕将出现 Configure WebBlocker （配置 WebBlocker）对话框，并在对话框内显示已经创建的 HTTP 策略。




2 选择你想配置的策略并点击 **Configure （配置）**。
屏幕将出现该策略的 WebBlocker Configuration （WebBlocker 配置）对话框。




**WebBlocker Configuration （WebBlocker 配置）**对话框包括服务器、类别、例外及高级设置的配置选项卡。

## 添加新服务器

你可以添加多个 WebBlocker Server，以便在无法连接到主服务器时， Firebox® 可以连接到备用服务器。主服务器是指列表中的第一台服务器。你无法为一个配置添加超过五台 WebBlocker 服务器。

1 点击加号 (+)，添加一台服务器。
屏幕将出现 Add WebBlocker Server（添加 WebBlocker 服务器）对话框。

2 在 **Server IP**（**服务器 IP**）的下一栏键入 WebBlocker Server 的 IP 地址。键入端口号。

## 选择受禁网站的类别

在你使用 Activate WebBlocker Wizard（激活 WebBlocker 向导）时，选择你想禁止的网站类别。你可以使用该对话框对原始配置进行修改。选择你想禁止的网站类别的复选框。阅读类别描述，选择相应的复选框。在选中一个复选框后，该复选框相对应的网站类别描述将出现在界面的底部。如果你想禁止用户访问界面中列示出的所有网站类别，则应该选择 **Deny All Categories**（**禁止所有类别**）。

**注释**

如果要禁止用户试图避开 WebBlocker 而访问匿名网站，你应该在 WebBlocker 中禁止 Remote Proxies（远程代理）类别。

## 定义 WebBlocker 例外

你可以为 WebBlocker 添加例外情况。你可以添加被允许或禁止的网站，使其作为 WebBlocker 网站类别的例外。你添加的网站仅适用于 HTTP 数据流。他们不能被添加到 Blocked Sites List（受禁网站列表）。

定义的例外主要基于 URL 模式，而非 IP 地址。你可以让 Firebox 禁止同一 URL 的网站。通过，让 Firebox 寻找 URL 模式更为方便。URL 模式不包括前缀 “http://”。要在所有网站上查找匹配的 URL 路径，该模式必须有一个前缀 “/*”。

URL 中的主机可以采用 HTTP 请示中规定的主机名或服务器的 IP 地址。尽管你可以在某个模式下使用子网（如 10.0.0*），但此时网络地址并未得到支持。

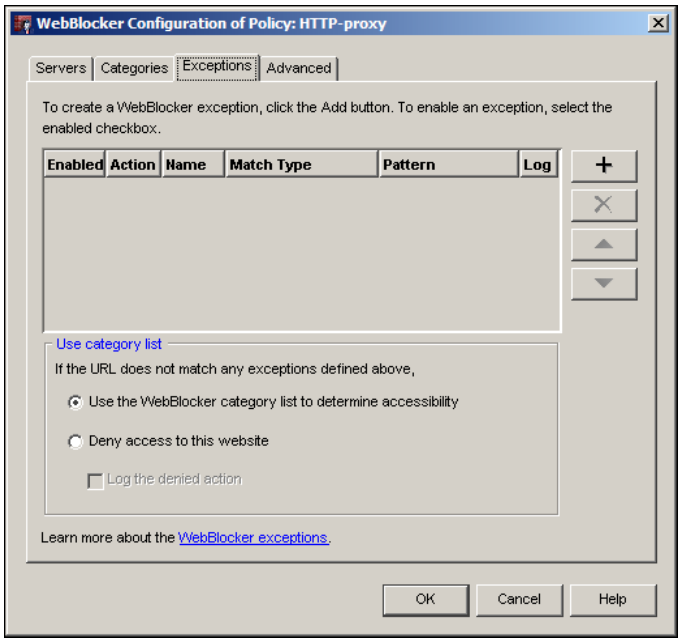
如果是 80 端口的服务器，请不要将此端口包括在内。如果是非 80 端口的服务器，你可以添加 “:ports”，例如：10.0.0.1:8080。你也可以为此端口采用一个通配符，例如：10.0.0.1:*，但是该通配符不适用于 80 端口。

你可以使用 URL 的任何部门创建 WebBlocker 例外。你可以针对某一网站设置必须禁止的端口号、路径名称或字符串。例如，如果由于存在不当图片，你仅需要禁止 www.sharedspace.com/ ~ dave，你应该键入 “www.sharedspace.com/ ~ dave/*”。如此操作，你可以使用户能够浏览 www.sharedspace.com/ ~ julia，让你的用户能够看到此页面的信息。

要禁止在路径中含有 “sex” 文字的 URL，你可以键入 “*/*sex*”。要禁止在路径中含有 “sex” 文字的 URL 或主机名称，你可以键入 “*sex*”。

你可以在 URL 中禁止各种端口。例如，禁止访问 URL http://www.hackerz.com/warez/index.html:8080。该URL会让浏览器使用TCP 8080端口上的HTTP协议，而非默认的TCP 80，因此你可以禁止与 *8080 匹配的端口。

1 点击 **Exceptions（例外）**选项卡，为 WebBlocker 网站类别创建例外。




2 点击加号 (+)，添加一个新的例外规则。

3 选择 **Action（对策）**栏，进入 **Action（对策）**下拉列表。选择让 WebBlcoker 允许或禁止所选的例外。

4 在 **Name（名称）**文本框中为例外键入一个名称。

5 点击 **Match Type（匹配类型）**栏，进入 **Match Type（匹配类型）**下拉列表：

模式匹配：确定 Drop（删除）了前缀 “http://”，并在添加了后缀 “/*”。

精确匹配：选择该选项可以实现字符对字符匹配。如果你定义的例外是允许访问 www.yahoo.com，当用户键入 “www.yahoo.com/news”时，该请求会被拒绝。

正则表达式：支持 Shell 命令表中使用的通配符。

6 在 **Pattern（模式）**文本框中键入你想将其识别为例外的模式。

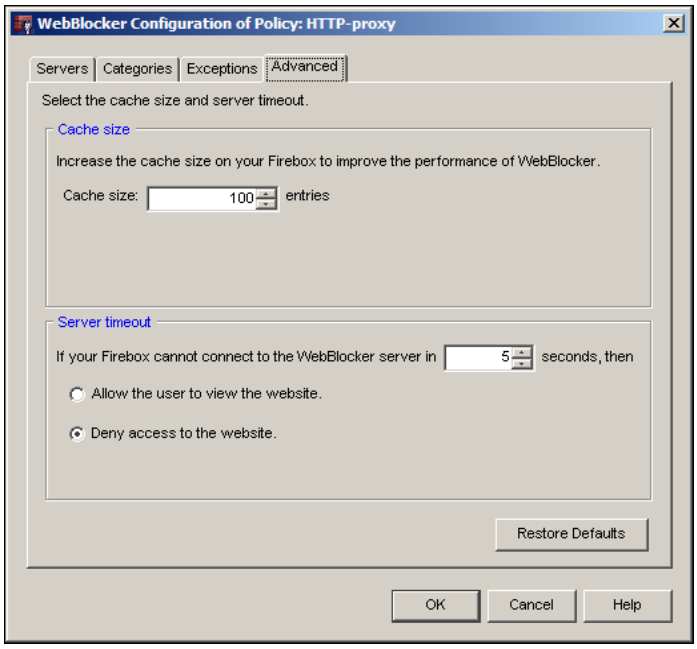
7 如果你想在 WebBlocker 限制或允许某次例外访问时向你发送日志消息，请点击 **Log（日志）**复选框。

8 要激活例外，请点击 **Enabled（被激活）**复选框。

9 如果所访问的 URL 与你配置的例外不符，你可以在 **Use category list（使用类别列表）**项下对该此访问进行设置。如果你希望让系统通过该此访问，请点击顶部的单选按钮。如果你想阻止该此访问，则可以点击底部的单选按钮。如果你阻止了该此访问，你可以选择单选按钮下方的复选框，为该此访问发送一条日志消息。

### 定义高级 WebBlocker 选项

1 要对高级 WebBlocker 选项进行配置，请点击 **Advanced（高级）**选项卡。




2 你可以调整 **Cache size（缓存值）**，提高 WebBlocker 的性能。使用箭头改变缓存中的条目数量或键入一个条目数。

3 你可以设置一个超时数值以及在服务器超时时系统的默认操作程序。如果你想在服务器超时时继续允许访问该网站，请选择 **Allow the user to view the website（允许此用户访问该网站）**。如果你想禁止该网站，请选择 **Deny access to the website（禁止访问该网站）**。.

## 为 WebBlocker 设置对策时段

你可以为策略设置操作时段。你可以使用下拉列表中的预定义设置或创建自定义时段。你可以为各个时段定义需要在此时段内禁止的网站。例如，你可以在正常的营业时间禁止访问体育类网站，但是允许用户在午间、晚间及周末访问这些网站。

要为某一策略设置时段，你需要：

1 打开并编辑该策略，然后点击 **Advanced（高级）**选项卡。

2 从下拉列表中选择一个时段，或点击 New/Clone（新增 / 复制）图标创建新的时段。详情请参阅 50 页的 “*创建时段*”。

3 对使用该时段的 HTTP 策略进行配置。

你也可以配置两项 HTTP 策略，但仅为其中的一项创建时段。每一策略使用 HTTP 代理对策中的以下。每一 HTTP 代理对策与 WebBlocker 对策（至少两项）中的其中一项相对应。

# 第 24 章　配置 spamBlocker

不受欢迎的电子邮件（垃圾邮件）正在以惊人的速度填充我们的普通收件箱。大量的垃圾邮件会削弱宽带流量，降低员工的劳动生产率并浪费网络资源。 WatchGuard® spamBlocker™ 采用行业领先的 Commtouch® 模式探测技术，可以在你的互联网网关有效阻止垃圾邮件并防止其进入你的电子邮件服务器。 spamBlocker 在检测垃圾邮件攻击时是检测电子邮件的模式，而非内容，因此它可以检测到任何语言、格式或加密方法的邮件。

## 关于 spamBlocker

在安装 spamBlocker™ 时，你必须获得：

- 一个 spamBlocker 许可密钥证书
- 一个基于 Firebox® 的 SMTP 电子邮件服务器
- 一个 SMTP 代理策略
- 在 Firebox 中配置好的 DNS。在 Policy Manager（策略管理器）中选择 **Network（网络）>Configuration（配置）**。点击 **WINS/DNS** 选项卡并键入 Firebox 所使用的用于识别主机名的 DNS 服务器 IP 地址。

### spamBlocker 对策

Firebox 使用 spamBlocker 对策（actions）对判定为垃圾邮件的电子邮件消息进行处理。 Firebox 可以：

- **拒绝** – 阻止垃圾电子邮件被发送到电子邮件服务器，而且不向发件人作出任何答复。
- **标识** – 将电子邮件标识为垃圾或非垃圾电子邮件，并允许该电子邮件进入电子邮件服务器。有关 spamBlocker 标识的详情，请参阅后续章节。
- **允许** – 允许垃圾电子邮件进入 Firebox，而且不对其进行标识。

### spamBlocker 标识

Firebox 可以将 spamBlocker 标识添加到电子邮件的主题行。你可以对 spamBlocker 标识进行配置，自定义添加的标识。以下示例显示了在主题行被标识为垃圾邮件的电子邮件。此添加的是默认标识：*** 垃圾邮件 ***。

主题：***SPAM*** Free auto insurance quote（***SPAM*** 免费的汽车保险报价）

以下示例显示的是自定义标识：SPAM （ 垃圾邮件 ）

主题：[ SPAM] You"e been approved!（[ 垃圾邮件 ] 你已通过审查！）

### spamBlocker 类别

spamBlocker 将检查电子邮件的模式是否与 spamBlocker 数据库中储存的模式匹配。spamBlocker 将电子邮件分为三类：垃圾邮件、群发邮件及疑似垃圾邮件。 spamBlocker 根据在电子邮件中探测到的模式数量，将电子邮件划分到上述类别中。

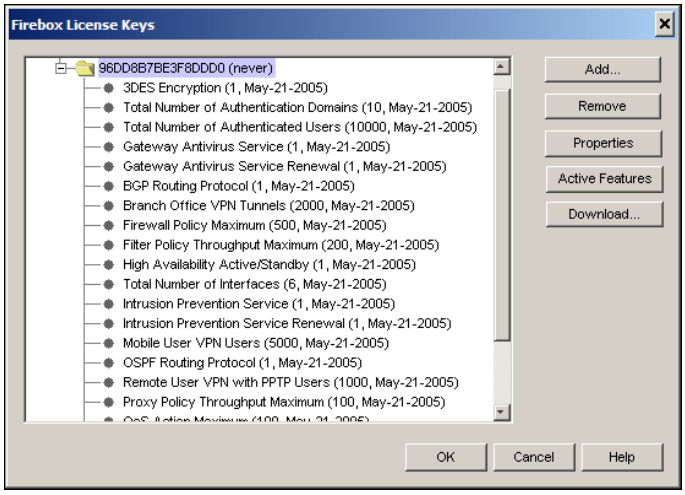
- *Spam （垃圾邮件）*：包括从已知垃圾邮件散播点发送的电子邮件。我们推荐针对此类电子邮件使用 Deny （ 拒绝 ）对策。
- *Bulk （群发邮件）*：包括不是从已知垃圾邮件散播点发送的但的确与垃圾邮件结构相匹配的电子邮件。我们推荐针对此类电子邮件使用 Tag （ 标识 ）对策。
- *Suspect （疑似垃圾邮件）*：是指貌似正常电子邮件但可能隐藏垃圾邮件攻击的电子邮件。通常，这些邮件是合法的电子邮件消息。我们推荐针对此类电子邮件使用 Tag （ 标识 ）对策。

## 安装软件许可

安装 spamBlocker™ 时，你必须取得一个 spamBlocker 密钥并将其注册到 LiveSecurity 网站。注册后， LiveSecurity 将向你提供一个新的功能密钥。

安装该功能密钥需要进行以下操作：

1 在 Policy Manager（策略管理器）中选择 **Setup（设置）>Licensed Features（许可功能）**。
屏幕将出现 Licensed Features（许可功能）对话框。




2 点击 **Remove（删除）**，删除当前功能密钥。
你必须在安装新密钥前将包括 spamBlocker 在内的整个功能密钥完全删除。

3 点击 **Add（添加）**。

4 在 **Add Firebox License Key（添加 Firebox 许可密钥）**对话框中，键入或粘贴你的许可密钥。你可以点击 **Import（导入）**，将密钥导入你的电脑或网络，然后点击 **OK（确认）**。
许可密钥将出现在 Licensed Features（许可功能）对话框中。

## 激活 spamBlocker

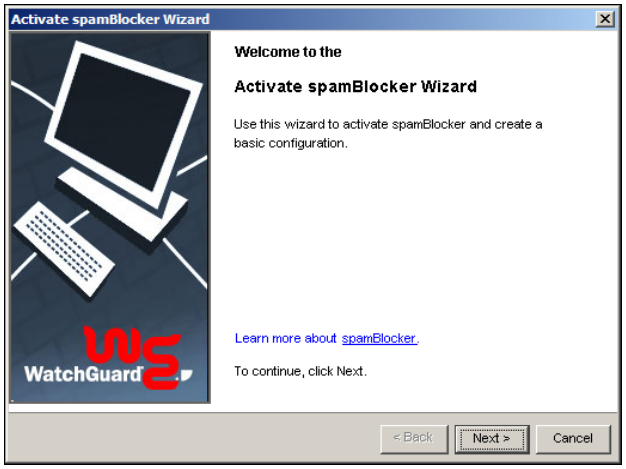
要激活 spamBlocker™，你需要使用向导启用该功能，并建立基础配置。

1 在 WSM 中选择将要使用 spamBlocker 的 Firebox。

2 选择 **Tools（工具）>Policy Manager（政策管理器）**。

或者，
你可以在 WSM 工具条上选择 Policy Manager（策略管理器）图标。

3 在 Policy Manager（策略管理器）中选择 **Tasks（任务）>spamBlocker>Activate（激活）**。
进入 Activate spamBlocker wizard（激活 spamBlocker 向导）。




4 按照向导的指示进行点击操作，并输入向导要求的各种信息。向导将弹出以下界面：

### 将 spamBlocker 设置应用到你的策略中

如果你的 Firebox 存在一个或多个已经定义的 SMTP 策略但并未启用 spamBlocker，此界面将出现。从列表中选择激活 spamBlocker 所需的代理策略。所有已将 spamBlocker 激活的策略将被显示为灰色。如果此时你未定义任何 SMTP 策略，此界面将不会出现。

### 创建代理策略

如果你的 Firebox 仍没有为 SMTP 创建的策略，此界面将出现。在此情况下，向导将为你创建一项 SMTP 代理策略。你必须至少有一个带有静态 IP 地址的外部接口。

输入电子邮件服务器的 IP 地址，创建一项 SMTP 策略。按照此向导创建的策略包含 **From（从）**字段的 “Any-External（任何外部接口）”及 **To（到）**字段的一条静态 NAT 输入项。静态 NAT 输入项使用在 Firebox 中配置的静态外部 IP 地址。它将为你在向导中输入的电子邮件服务器 IP 地址激活静态 NAT。如果默认的 NAT SMTP 策略不是你公司的最佳选择，你可以在使用向导之前，使用 Policy Manager（策略管理器）创建一个 SMTP 策略。

### 选择 spamBlocker 对策

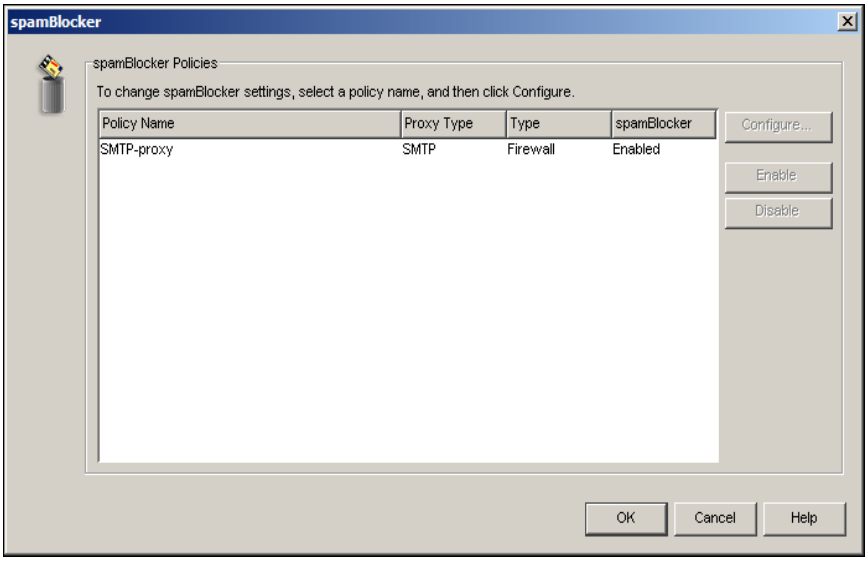
你可以使用此界面为划分为 SPAM（垃圾邮件）、Bulk（群发邮件）及 Suspect（疑似垃圾邮件）的电子邮件选择 spamBlocker 对策。

如果你想记录 spamBlocker 对某一电子邮件的应对日志消息，你可以选择 **Log（日志）**复选框。如果你不想记录日志消息，则应该清除 **Log（日志）**复选框。

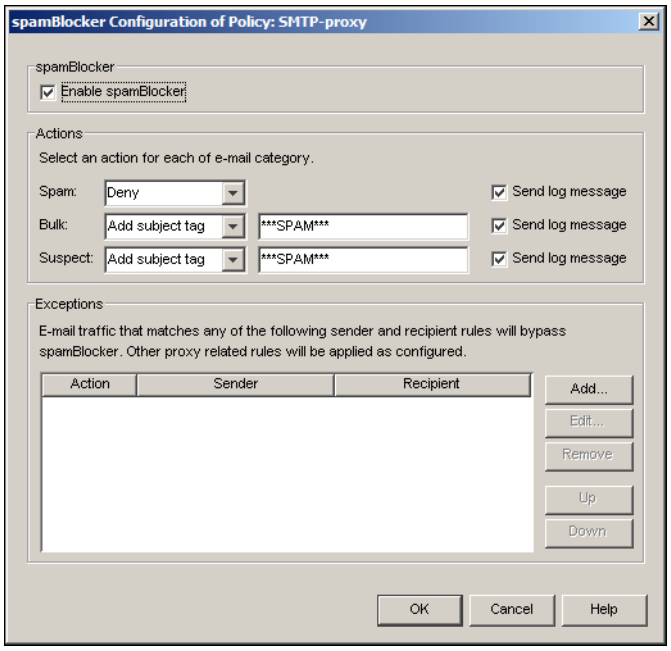
# 配置 spamBlocker

你在使用 Activate spamBlocker wizard （激活 spamBlocker 向导）激活 spamBlocker 并创建出基础配置后，你可以对 spamBlocker 的更多设置选项进行配置。

1 在 Policy Manager （策略管理器）中选择 **Tasks （任务） >spamBlocker>Configure （配置）**。
spamBlocker 对话框将与 SMTP 策略一同出现在列表中，并显示 spamBlocker 各项策略是否已被激活。




2 选择你想配置的策略并点击 **Configure （配置）**。
屏幕将出现该策略的 spamBlocker Configuration (spamBlocker 配置 ) 页面。




3 在你使用 Activate spamBlocker wizard （激活 spamBlocker 向导）时，你已经对垃圾邮件、群发邮件及疑似垃圾邮件设置了 spamBlocker 对策。你可以在此对话框中修改这些对策。

4 如果你想记录 spamBlocker 对某一电子邮件的应对日志消息，你可以选择 **Log（日志）**复选框。如果你不想记录日志消息，则应该清除 **Log （日志）**复选框。

5 确定 DNS 已在采用 spamBlocker 规则的 Firebox 中被激活。

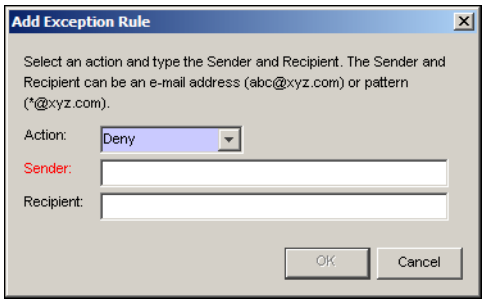
**注释**

如果你的 Firebox （使用 spamBlocker）与互联网之间存在任何边界防火墙，请勿禁止 HTTP 数据流。 HTTP 协议用于将各种请示从 Firebox 发送到 spamBlocker。

### 添加 spamBlocker 例外

有时， Firebox 会将正常的电子邮件识别为垃圾消息。如果你知道发件人的地址，你可以在 Firebox 中将该地址设定为例外地址，使 Firebox 不对该地址发出的消息进行检测。检测例外邮件时，spamBlocker 将检查 “mail from ( 邮件来自 ):” 字段，并不检查你在电子邮件中看到的 “From （来自）:” 抬头。如果你创建了一个例外规则，但该规则无法被正常执行，则应检验你输入的字段是否正确。

1 在 **spamBlocker Configuration （spamBlocker 配置）**对话框的 Exception （例外）中点击 **Add（添加）**。
屏幕将出现 Add Exception Rule （添加例外规则）对话框。




2 选择一个 rule action （应对策略）：**Allow （允许）、 Tag subject （标识主题）**或 **Deny （拒绝）**。

3 键入发件人及 / 或收件人。你可以键入整个电子邮件名称或使用通配符。

## 在电子邮件客户端为群发及疑似垃圾邮件创建规则

许多网络管理员允许将未被确定为垃圾邮件的电子邮件发送到指定的电子邮件收件人。然后，这些网络管理员会在他们的电子邮件客户端软件中设定各种规则，通过这些规则将标识为疑似或群发电子邮件放入一个电子邮件客户端的特殊文件夹中。以下流程将指示你如何设定 Microsoft Outlook 电子邮件客户端。有关如何在其他类型的电子邮件客户端中使用该流程的详情，请参照这些产品的用户文档。

### 在 Outlook 中将垃圾邮件或群发邮件发送到特殊文件夹

此流程将向你介绍在 Microsoft Outlook 中为群发及疑似垃圾邮件创建规则的步骤。你可以将标识为 “垃圾邮件” 或 “群发邮件” 的电子邮件直接发送到 Outlook 中的特殊文件夹。在你创建这些

文件夹后，你可以将可能是垃圾邮件的电子邮件排除在你的正常 Outlook 文件夹之外，但是如果有必要，你仍然可以查看这些电子邮件。

如果你使用另一种电子邮件客户端，你需要针对该产品检查你的用户文档。

在开始前，确定你将垃圾邮件及群发邮件的对策设置为 **Add Subject Tag（添加主题标识）**。你可以使用默认标识或创建自定义标识。以下步骤介绍如何使用默认标识创建文件夹。

1 从你的 Outlook Inbox（Outlook 收件箱）种选择 **Tools（工具）>Rules and Alerts（规则及警报）**。

2 点击 **New Rule（新规则）**，启动 Rules（规则）向导。

3 选择 Start from a blank rule（从空白规则开始）。

4 选择 **Check messages when they arrive（收到消息时进行检查）**。点击 **Next（下一步）**。

5 选择状态复选框：**when specific words in the subject（如果主题含有特定文字）**。然后在底部窗口点击特定文字，修改规则描述。在 **Search Text（搜索文本）**对话框中键入垃圾邮件标识（如 *****SPAM*****）。如果要使用自定义标识，请将自定义标识输入此处。点击 **Add（添加）**。点击 **OK（确认）**。

6 点击 **Next（下一步）**。

7 向导将询问你如何处置该消息。选择 **move it to the specified folder（将其移至特殊文件夹）**对话框。然后在底部窗口点击指定的文字，选择目标文件夹。

8 在 **Choose a Folder（选择一个文件夹）**对话框点击 **New（新建）**。在文件夹名称字段键入 **Spam**（垃圾邮件）。点击 **OK（确认）**。

9 点击 **Next（下一步）**两次。

10 要完成规则设定，为你的垃圾邮件规则键入名称。点击 **Finish（完成）**。

11 点击 **Apply（应用）**。

12 通过重复上述步骤为群发邮件创建一个规则 – 使用群发电子邮件标识。你可以将群发电子邮件发送到同一文件夹，或为群发电子邮件创建一个单独的文件夹。

## 报告假阳性及假阴性垃圾邮件

假阳性电子邮件是指被 spamBlocker™ 错误识别为垃圾邮件的合法邮件消息。假阴性电子邮件是指未被 spamBlocker 正确识别为垃圾邮件的垃圾邮件消息。如果发现了假阳性或假阴性电子邮件，你可以直接将分类错误报告给 Commtouch。你必须可以访问该邮件的信息，并将其上报。有关上报假阳性或假阴性电子邮件的详情，请访问：

https://www.watchguard.com/support/advancedfaqs/fw_spam-report.asp

## 监控 spamBlocker 的活动

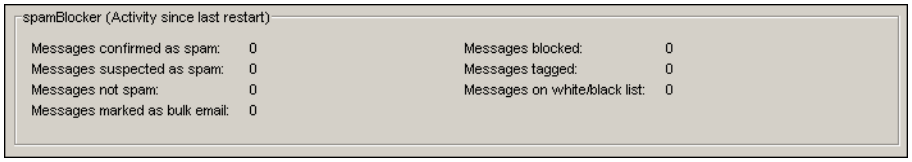
你可以使用 Firebox 系统管理器对 spamBlocker™ 的活动进行监控。

1 在 WatchGuard 系统管理器中选择你想监控其活动的 Firebox。

2 选择 **Tools（工具）>Firebox System Manager（Firebox 系统管理器）**。

或
在 WSM 工具条上点击 Firebox 系统管理器图标。

3 在 Firebox 系统管理器中点击 **Security Services （安全服务）选项卡。**
spamBlocker 统计数据将出现在界面底部。




## 用多项代理自定义 spamBlocker

你可以使用 spamBlocker™ 设定一个或多个 SMTP 代理服务。该功能允许你在公司中为不同的组群创建自定义规则。例如，你可以允许你的管理人员访问所有电子邮件，但对销售团队使用垃圾邮件标识。

如果你想通过 spamBlocker 使用多个 SMTP 代理服务，你的网络必须采用以下一种配置：

- 每一 SMTP 代理策略必须发送电子邮件至一台不同的内部电子邮件服务器。

或

- 你必须设置能够为每一 SMTP 代理策略发送电子邮件的外部资源。

**注释**

spamBlocker 不会检测外发 SMTP 电子邮件中的垃圾邮件。

# 第 25 章　享用基于特征的安全服务

网络黑客使用各种方法在互联网上肆意攻击各种电脑。进行攻击（本章称为入侵）的目的在于损坏你的网络、获得敏感信息或利用你的电脑攻击他人网络。

WatchGuard® 为你提供 Gateway AntiVirus（网关防病毒）/ 入侵防御服务（GAV/IPS），使你可以识别并阻止潜在入侵。入侵防御服务适用于所有 WatchGuard 代理协议，而 WatchGuard Gateway AntiVirus 适用于 SMTP、HTTP 及 TCP 代理协议。

识别到新的入侵后，系统将记录入侵病毒或攻击不同于其他病毒或攻击的特点。这些特点被称为特征。 GAV/IPS 使用这些特征探测病毒及入侵攻击。

新病毒及入侵方式在互联网上层出不穷。要确保 GAV/IPS 向你提供最大保护，你必须经常更新病毒或攻击特征。你可以对 Firebox® 进行设定，使其在 WatchGuard 中自动更新病毒及攻击特征。你也可以手动更新这些特征。

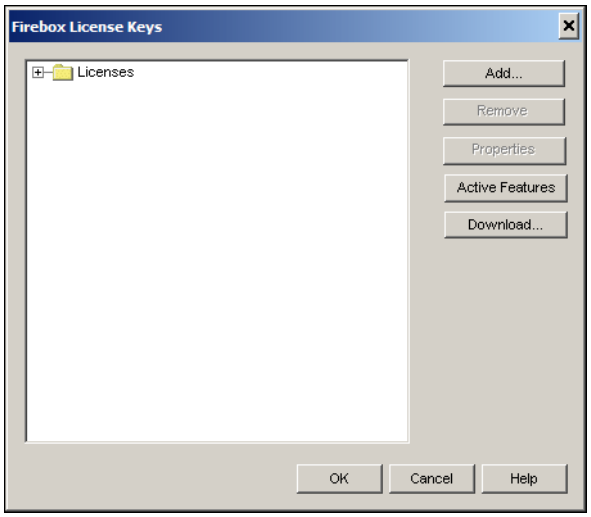
**注释**

WatchGuard 不保证本产品可以防范所有病毒或攻击，或防范某一病毒或入侵攻击对你的系统或网络的损坏。

# 安装软件许可

要安装 Gateway AntiVirus/ 入侵防御服务，你必须取得每一功能的许可密钥。

1 在 Policy Manager （ 策略管理器 ）中选择 **Setup （ 设置 ）>Licensed Features （ 许可功能 ）**。
屏幕将出现 Licensed Features （ 许可功能 ）对话框。




2 点击 **Add （ 添加 ）**。

3 在 **Add Firebox License Key （ 添加 Firebox 许可密钥 ）**对话框中键入你的许可密钥。你可以点击 **Import （ 导入 ）**将其导入到你的电脑或网络中。点击 **OK （ 确认 ）**。
许可密钥将出现在 Licensed Features （ 许可功能 ）对话框。

# 关于 Gateway AntiVirus

WatchGuard® Gateway AntiVirus (GAV) 可以在病毒进入你网络中的电脑之前将其有效阻止。 GAV 适用于 WatchGuard SMTP、 HTTP 及 TCP 代理协议。启动 GAV 后， SMTP、 HTTP 或 TCP 代理协议将对电子邮件及 web 数据流进行检测，并删除检测到的病毒。（ GAV 对 TCP 代理协议的设定是在 HTTP 代理协议对策 （ 由与其匹配的 TCP 代理协议对策推荐 ）中完成的。）

**注释**

如果你的公司未使用受 Firebox 保护的电子邮件服务器， GAV 不会启动电子邮件病毒防范功能。

如果你使用 SMTP 代理协议激活了 GAV， GAV 将检测到使用通常的电子邮件附着方式编码的病毒，具体包括 base64、二进制、 7 比特及 8 比特的编码技术。 GAV 不会检测未编码或 binhex 编码的消息， Firebox 将跳过这些类型的消息。

如果你使用 HTTP 代理协议激活 GAV， GAV 将检测到你试图下载的网页中的病毒。如果检测到病毒，用户的连接将自动中断。（ GAV 不会发出说明连接中断原因的通知 ）。

## 激活 GAV

在 SMTP 或 HTTP 代理策略中使用 GAV 之前，你必须启动 GAV 向导，激活该功能并创建基础配置。具体操作为：

1 在 WSM 中选择你想使用 GAV 的 Firebox。

2 选择 **Tools（工具）>Policy Manager（策略管理器）**。

或者，
你可以点击 WSM 工具条上的 Policy Manager（策略管理器）图标。

3 在 Policy Manager（策略管理器）中选择 **Tasks（任务）>GAV>Activate（激活）**。
进入 Activate Gateway AntiVirus wizard（激活 GAV 向导）。


4 点击 **Next（下一步）**。

5 完成向导。根据你是否已经在你的配置中使用了代理策略，该向导将显示不同的界面。例如，如果你没有使用代理策略，该向导将帮助你创建一个代理策略。你可以再次使用该向导对 GAV 进行配置，或者参照以下章节中的指示。具体界面为：

### 将 GAV 设置应用到你的策略中

此界面包括已经应用到你的 Firebox 中的代理策略列表。从列表中选择激活 GAV 所需的代理策略。所有已将 GAV 激活的策略将被显示为灰色。

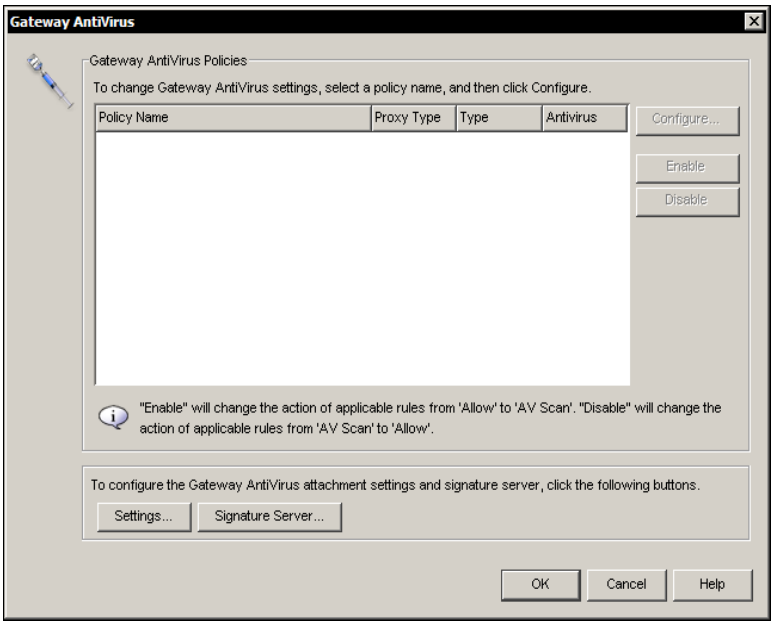
### 创建新代理策略

此向导将创建一项默认的 SMTP 策略，该策略为静态 NAT 策略。要创建此默认 SMTP 策略，你必须有至少一个带有静态 IP 地址或 PPPoE 的外部接口。即使你有多个外部接口，也仅可以创建一项策略。该策略的 **To（到）**字段是一个静态输入项（第一外部接口到指定邮件服务器 IP 地址的静态 IP 地址）。如果默认策略无法满足你的要求，你可以在使用向导之前在 Policy Manager（策略管理器）创建一个 SMTP 策略。

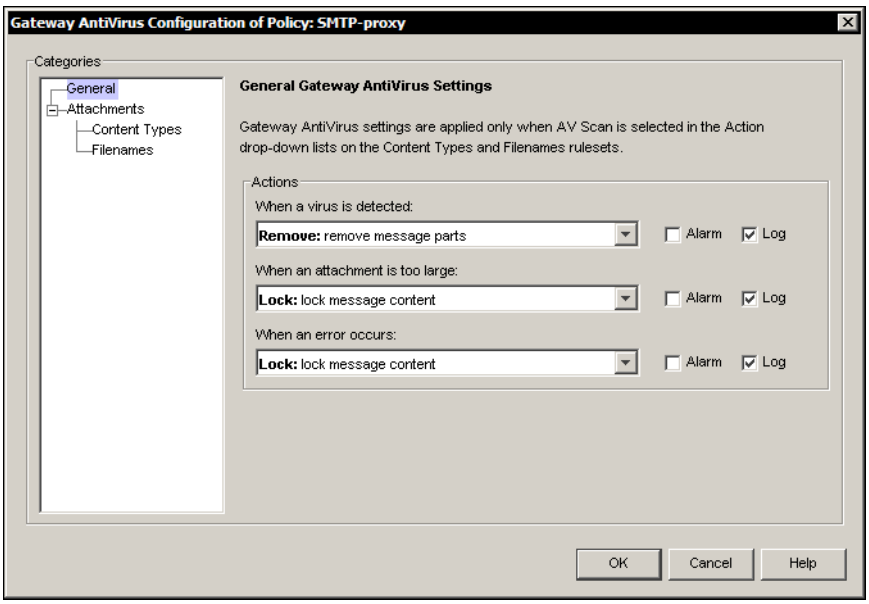
# 配置 GAV

你在使用 Activate Gateway AntiVirus wizard （激活 GAV 向导）激活 spamBlocker 并创建出基础配置后，你可以进一步修改已创建的配置。

1 在 Policy Manager （策略管理器）中选择 **Tasks （任务）>GAV>Configure （配置）**。
屏幕将出现 GAV 对话框，该对话框将显示已被创建的 SMTP、 HTTP 及 TCP 策略。




2 选择你想配置的策略，并点击 **Configure （配置）**。
屏幕将出现该策略的 General Gateway AntiVirus Settings （一般 GAV 设置）页面。



3 此对话框中的各个字段用于设置防范电子邮件病毒的必要对策。你也可以使用该此对话框，针对带有过大附件或 Firebox 无法扫描的电子邮件应采取的对策。在 **Actions （对策）**选项中，使用下拉列表为每一种状态选择 Firebox 的对策：

*Allow*

（允许）– 即使附件载有病毒，也允许将其发送给收件人。

*Drop*

（中断）– 去除附件并中断连接。系统不向邮件来源发出任何信息。

*Block*

（禁止）– 阻止附件，并将发件人的 IP 地址添加到 Blocked Sites （受禁网站）列表。

你可以将更多对策应用到 SMTP 代理协议。

*Lock*

锁定附件。如果是内容过大或 Firebox 无法扫描的文件，锁定将是一个不错的选择。被锁定的文件将无法被用户轻易打开。只有管理员才可以解锁。管理员可以使用不同的防病毒工具扫描该文件并检测附件内容。

*Remove*

（移除）– 移除附件并允许将消息发送到收件人。

**注释**

如果你将配置设置为 Allow （允许）附件通过，则你的配置不够安全。

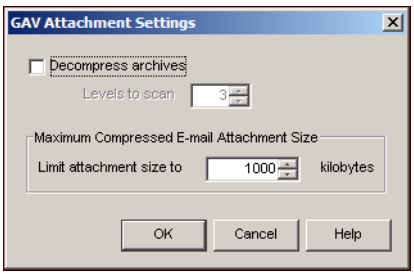
## 为防病毒应对举措创建警报或日志条目

警报是向用户告知代理协议规则正被应用到网络数据流中的一种机制。使用 General Gateway AntiVirus Settings （一般 GAV 设置）页面上的 **Alarm （警报）**复选框为防病毒应对举措创建警报。如果你不想为防病毒应对举措创建警报，你可以清除具体防病毒应对举措的 **Alarm （警报）**复选框。要成功使用警报功能，你必须设定在每一代理策略中将使用的警报类型。要设定将使用的警报类型，你需要打开代理策略进行编辑。在代理协议对策类别表中选择 **Proxy and AV Alarms （代理协议及 AV 警报）**。

如果你想记录某一防病毒应对举措的日志消息，为该防病毒应对举措选择 **Log （日志）**复选框。如果你不想记录某一防病毒应对举措的日志消息，你需要清除 **Log （日志）**复选框。

## 配置 GAV 引擎设置项

1 在 **GAV** 对话框中点击 **Settings （设置）**。

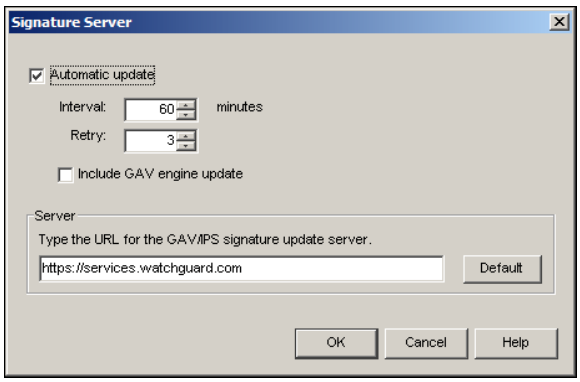


2 要扫描内部压缩附件，请选择 **Decompress archives （ 解压文档 ）**复选框。选择或键入压缩文件扫描级别的编号。
不能被扫描的压缩附件包括加密文件或使用某种我们不支持的压缩方式压缩的文件（ 如可保护密码的 Zip 文件 ）。使用 GAV>Configure （ 配置 ）对话框为 Firebox 设置用以处理无法扫描文件的对策。

3 为电子邮件输入以千字节为单位的最小容量。

## 配置 GAV 特征服务器

1 在 **Gateway AntiVirus （ GAV）**对话框中选择 **Signature Server （ 特征服务器 ）**。




2 要激活自动病毒特征更新功能，选择 **Automatic update （ 自动更新 ）**对话框。输入自动更新之间的间隔分钟数。

3 选择自动更新失败时重试的次数。

4 要在同样的间隔时间段更新 GAV 引擎，选择 **Include GAV engine update（ 包括 GAV 引擎更新 ）**对话框。

5 不要为 GAV/IPS 修改特征服务器的 URL，除非 WatchGuard 要求你如此操作。

6 点击 **OK （ 确认 ）**。

## 在 GAV 中应用多个代理协议

你可以在你公司的不同服务器中应用多个 SMTP 代理协议，查杀各种病毒。

使用 GAV 的每一代理协议均在该代理协议特有的选项中获得配置。例如，你可以为不同服务器或不同目的站的电子邮件设定不同的代理协议防病毒配置。你可以扣留由于过大而不能扫描的附件，使其不能到达某些用户，同时你也可以允许这些附件到达其他用户。

## 解锁被 GAV 锁定的附件

WSM 提供了一个可执行程序，通过该程序，你可以解锁被 GAV 锁定的附件：

C:\Program Files\WatchGuard\wsm8\bin\unlock.exe

要打开锁定文件，你需要进行以下操作：

1 打开一个命令提示。

2 键入：**Unlock （解锁）**<path to locked file>（到锁定文件的路径）

# 查看 GAV 状态及 GAV 更新

你可以在 Firebox System Manager （FSM）中的 **Security Services （安全服务）**选项卡中查看 GAV 状态并更新 GAV。

## 查看服务状态

通过查看 GAV 状态，你可以得知 GAV 保护功能是否仍然有效。你也可以查看病毒扫描器、病毒特征版本以及上次更新时间。

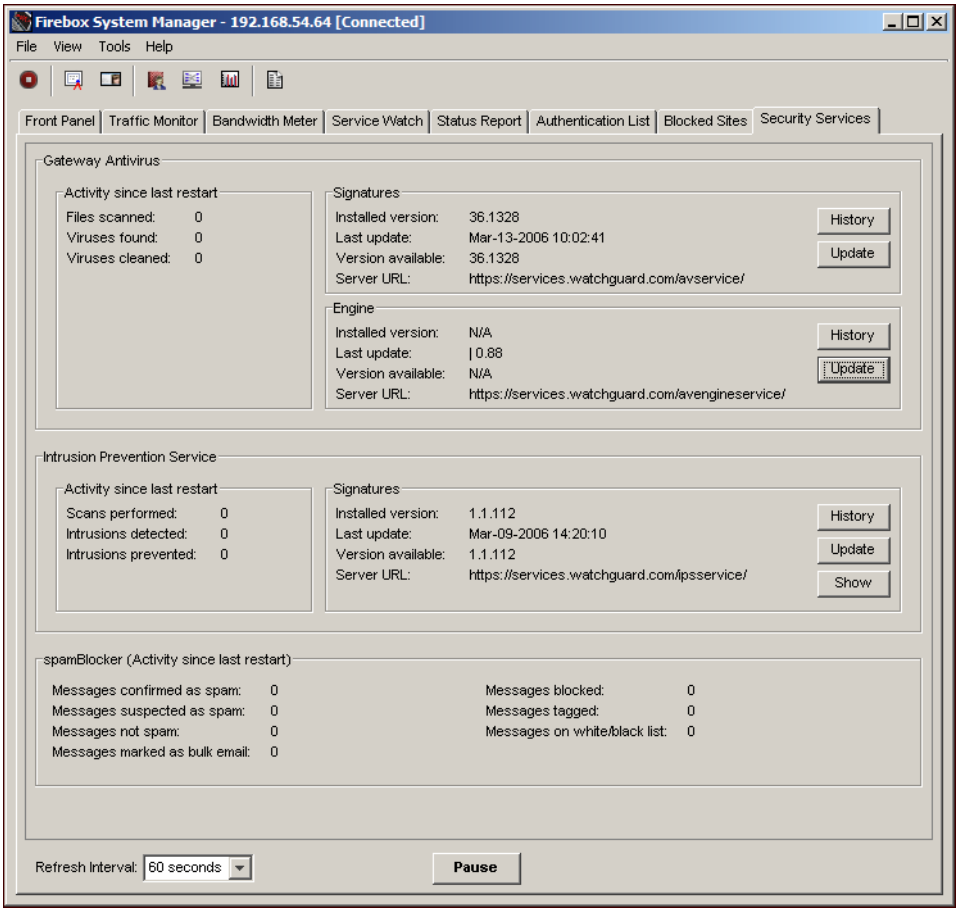
要查看服务状态，你需要：

1 从 WSM 中选择 Firebox。选择 **Tools （工具）>Firebox System Manager （FSM）**。

你也可以在 WSM 工具条上点击 Firebox System Manager （FSM）图标。

2 点击 **Security Services （安全服务）**选项卡。

Windows 将显示已安装安全服务的状态。必须安装这些功能的许可证照，便于查看状态信息。



### 手动更新 GAV 特征或 GAV 引擎

你可以将 GAV 设定为自动更新特征数据库或 GAV 引擎。你也可以手动更新特征数据库或 GAV 引擎。如果 Firebox 特征数据库或引擎已过期，系统将无法保护你免受最新病毒及攻击的入侵。要手动更新，你需要进行以下操作：

1 打开 Firebox System Manager（FSM）。

2 点击 **Security Services（安全服务）**选项卡。
屏幕将出现安全服务状态。

3 为你想要更新的服务点击 **Update（更新）**。你必须键入你的配置密码短语。
Firebox 将为 GAV 下载可取得的最新特征数据库或引擎。请参阅 Traffic Monitor（流量控制）。
如果无最征数据库或引擎，Update（更新）按钮将显示为无效。

### 更新防病毒软件

由于新型网络攻击总是层出不穷，因此你必须定期更新你的防病毒软件。如有必要，WatchGuard 会将更新程序发送到防病毒数据库或防病毒软件。在我们发出更新程序前，你将从 LiveSecurity 获得一份电子邮件。只要你认购的 GAV 仍在有效期内，你就有权访问所有上述更新程序。

如要下载软件更新程序，请在 www.watchguard.com/support 网站登入你的 LiveSecurity® 账户。

## 激活激活入侵防御服务（IPS）

网络黑客使用各种方法在互联网上肆意攻击各种电脑。进行攻击的目的在于损坏你的网络、获得敏感信息或利用你的电脑攻击他人网络。这些攻击又称为入侵。

你可以通过 IPS（入侵防御服务）使用 WatchGuard 代理协议查封各种网络攻击。Firebox Intrusion Prevention Service（Firebox® 入侵防御服务）将检查 DNA、FTP、HTTP 及 SMTP 数据流，其使用 TCP 代理协议扫描其他基于 TCP 的数据流。

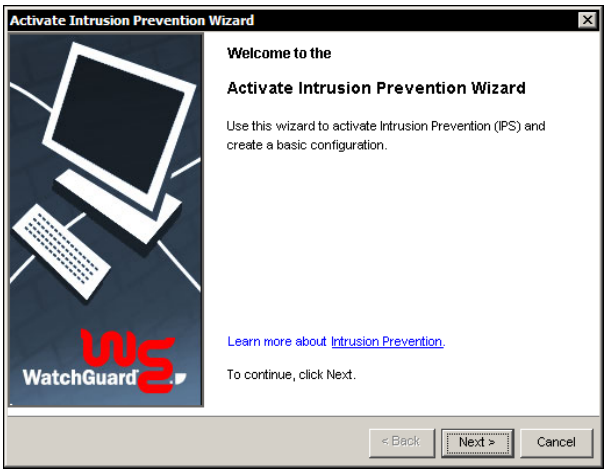
在一项代理策略中使用 IPS（入侵防御服务）之前，你必须启动 Activate Intrusion Prevention wizard（激活入侵防御向导），激活该功能并创建基础配置。具体操作为：

1 在 WSM 中选择将要使用 IPS（入侵防御服务）的 Firebox。

2 选择 **Tools（工具）>Policy Manager（策略管理器）**。

你可以在 WSM 工具条上选择 Policy Manager（策略管理器）图标。

3 在 Policy Manager（策略管理器）中选择 **Tasks（任务）>Intrusion Prevention（入侵防御）>Activate（激活）**。
进入 Activate Intrusion Prevention wizard（激活入侵防御向导）。




4 点击 **Next（下一步）**。

5 按照向导要求点击完成各项操作，并添加所需的信息。根据你是否已经在你的配置中使用了代理策略，该向导将显示不同的界面。如果你没有使用代理策略，该向导将帮助你创建一个代理策略。你可以再次使用该向导对 IPS（入侵防御服务）进行配置，或者参照以下章节中的指示。具体界面为：

### 选择需要激活的代理策略

此界面将显示你已在 Firebox 中定义的代理策略列表。从列表中选择激活 IPS（入侵防御服务）所需的代理策略。所有已将 IPS（入侵防御服务）激活的策略将被显示为灰色。

### 创建新代理策略

此界面显示当前并不存在对应策略的代理协议类型。例如，如果你已经创建了一项 SMTP 策略，该策略不会出现在列表中。
要创建一项策略，你需要选中对应的复选框。如果你选择 SMTP，请输入邮件服务器的 IP 地址。此向导将创建一项默认的 SMTP 策略，该策略为静态 NAT 策略。要创建此默认 SMTP 策略，你必须有至少一个带有静态 IP 地址或 PPPoE 的外部接口。即使你有多个外部接口，也仅可以创建一项策略。该策略的 **To（到）**字段是一个静态输入项（第一外部接口到指定邮件服务器 IP 地址的静态 IP 地址）。如果默认策略无法满足你的要求，你可以在使用向导之前在 Policy Manager（策略管理器）创建一个 SMTP 策略。

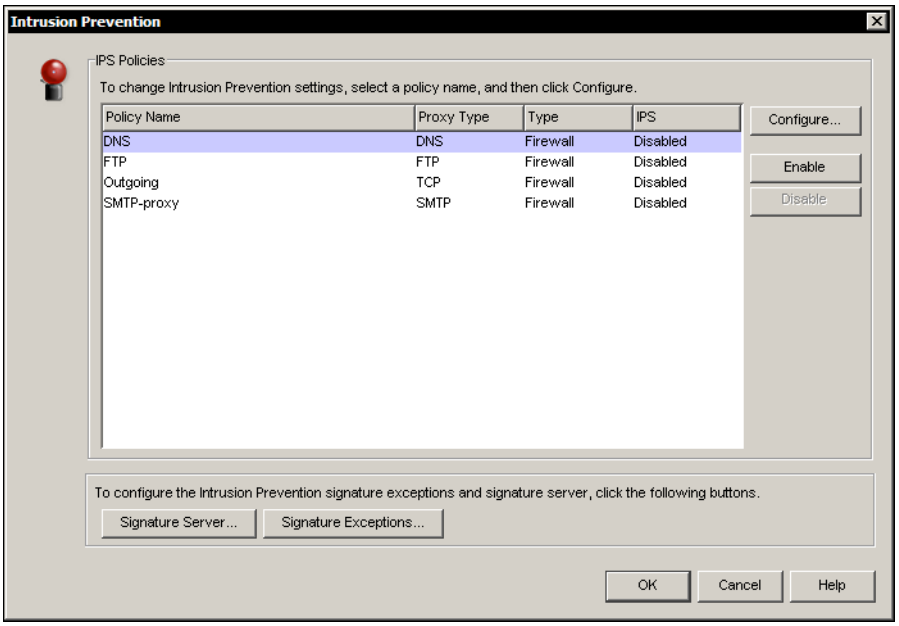
### 选择高级入侵防御设置（仅适用于 HTTP 及 TCP）

如果你使用向导添加一项 HTTP 或 TCP 策略，你可以选择保护系统免受即时通信软件（IM）、点对点（P2P）软件及间谍软件的侵扰。

# 配置入侵防御

你在用 Activate Intrusion Prevention wizard （激活入侵防御向导）激活 IPS （入侵防御服务）并创建出基础配置后，你可以对设定的配置进行进一步修改。

1 在 Policy Manager （策略管理器）中选择 **Tasks （任务）>Intrusion Prevention （入侵防御）>Configure （配置）**。
屏幕将出现 Intrusion Prevention （入侵防御）对话框，该对话框将显示已被创建的策略。




2 选择你想配置的策略，并点击 **Configure （配置）**。
屏幕将出现该策略的 General Intrusion Prevention Settings （一般入侵防御设置）页面。

## 入侵的严重性级别

入侵防御的策略设置通常将入侵严重程度划分为三个级别：

*High*
（高）– 允许远程访问或代码扩充的漏洞攻击，如缓存溢出、远程命令执行、密码泄漏、后门程序以及安全旁路。

*Medium*
（中）– 允许攻击者建立访问连接，允许将服务器端源代码泄漏给攻击者并拒绝访问合法用户的漏洞攻击。如：目录游走、文件 / 资源修楼、 DoS、 SQL 注入以及跨网站指令码（cross-site scripting）。

*Low*
（低）– 不允许攻击者建立访问连接、但允许其获得某一攻击所需的信息的漏洞攻击。例如，攻击者可以发送一条命令，要求获得操作系统信息、 IP 地址或网络拓扑结构。

通过漏洞攻击访问软件应用的攻击特征 （如没有具体内容的特征）也被定义为该级别。

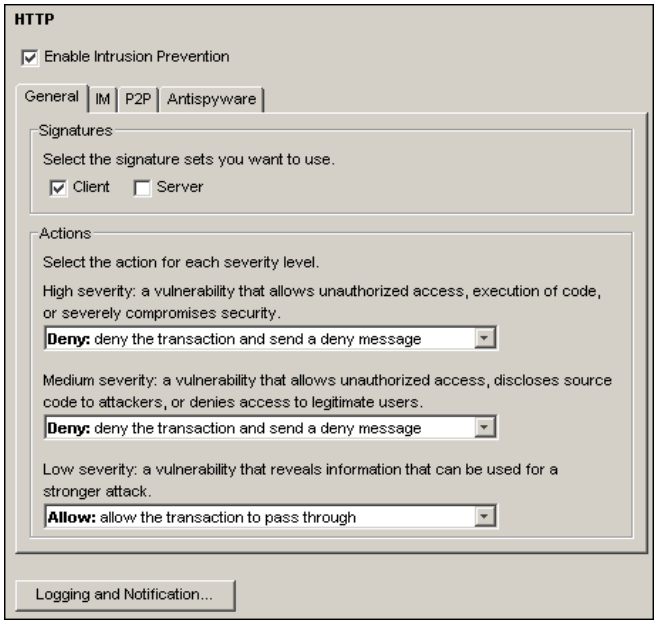
如果不存在十分详细的内容，通常被划分为高级别及中级别的攻击特征也将被划分为更低一级的级别。而且如果这些攻击特征很可能引起假阳性判断，则也将被划分到更低级别。

## 对 HTTP 或 TCP 进行入侵防御设定

HTTP 及 TCP 代理协议带有防范即时通信软件、点对点软件及间谍软件的选项。

如果你使用 TCP 及 HTTP 代理协议，你必须在 TCP 及 HTTP 代理协议中为即时通信软件、点对点软件及间谍软件设定对策，使这些对策应用到所有即时通信软件、点对点软件及间谍软件数据流中。

1 选择 **Enable Intrusion Prevention （激活入侵防御）**复选框。




2 （此项仅适用于 HTTP）在 **Signatures （特征）**项下点击一个或两个复选框，为 HTTP 客户端点及 / 或 HTTP 服务器端点应用更为精确的特征列表。

3 在 **Actions （对策）**选项中，使用下拉列表为每一严重性级别选择 Firebox 对策。

*Allow*

（允许）– 允许将某一数据包发送到其指定收件人，即使该数据包的内容与某一特征匹配。

*Deny*

（拒绝）– 拒绝某一数据包，并向发件人发送一个 TCP 复位数据包。

*Drop*

（中断）– 去除数据包并中断连接，但是不向发件人发送 TCP 复位数据包。

*Block*

（禁止）– 阻止数据包，并将发件人的 IP 地址添加到 Blocked Sites （受禁网站）列表。

### 防范对即时通信软件的使用

HTTP 代理协议的配置选项可以防范对即时通信软件的使用，如以下即时通信服务：

- AOL Instant Messenger （AIM）
- ICQ
- MSN Messenger
- Yahoo Messenger

1 在 HTTP 代理协议的 **IPS （入侵防御服务）**字段，点击 **IM （即时通信软件）**选项卡。

2 选择系统检测到即时通信软件时 Firebox 将采取的对策：Allow （ 允许 ）、 Drop （ 中断 ）、 Deny （ 拒绝 ）或 Block （ 禁止 ）。

3 选择 **IM Signature Categories （ 即时通信软件特征类别 ）**，为不同的即时通信服务启用各套特征。你也可以取消对个别服务的选择。

### 防范对点对点软件的使用

HTTP 代理协议的配置选项可以防范对点对点软件的使用，如以下点对点服务：

- BitTorrent
- eDonkey2000 (ed2k)
- GNUtella
- Kazaa
- Napster
- Phatbot

1 在 HTTP 代理協議的 IPS （ 入侵防御服務 ）字段，點擊 **P2P （ 點對點軟件 ）**選項卡。

2 选择系统检测到即时通信软件时 Firebox 将采取的对策：Allow （ 允许 ）、 Drop （ 中断 ）、 Deny （ 拒绝 ）或 Block （ 禁止 ）。

3 选择 **P2P Signature Categories （ 点对点软件特征类别 ）**，为不同的点对点服务启用各套特征。你也可以取消对个别服务的选择。

### 禁止间谍软件

HTTP 及 TCP 代理协议针对以下间谍软件，提供防范功能：

*Adware*

（ 广告软件 ）– 一种应用软件。在该软件运行时，系统将显示广告条。该软件有时载有危害性编码，在未获得用户授权或同意的情况下，记录某一用户的个人信息并将其发送给第三方。

*Dialer*

（ 拨号软件 ）– 一种应用软件。该软件可以劫持用户的调制解调器以及联网号，并将用户的电脑连接到不当网站。

*Downloader*

（ 下载器 ）– 一种下载并安装其他文件的程序，主要用于从指定的 web 或 FTP 站点下载文件。

*Hijacker*

一种恶意程序，该程序可以修改你的电脑浏览器设置，并强迫你访问你不打算浏览的 web 站点。

*Trackware*

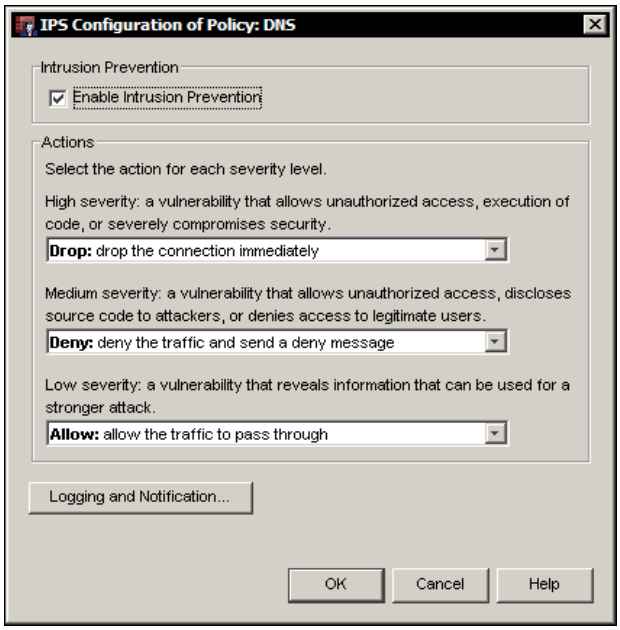
任何在未获得用户许可的情况下利用某一电脑的互联网连接发送个人信息的软件。

1 在 HTTP 代理服务器的 **Intrusion Prevention Services （ 入侵防御服务 ）**字段，点击 **Antispyware （ 防间谍软件 ）**选项卡。

2 选择系统检测到间谍软件时 Firebox 将采取的对策：Allow （ 允许 ）、 Drop （ 中断 ）、 Deny （ 拒绝 ）或 Block （ 禁止 ）。

## 对 FTP、SMTP 或 DNS 进行入侵防御配置

1 选择 **Enable Intrusion Prevention （ 激活入侵防御 ）**对话框。




2 为每一严重性级别选择以下一种对策：

*Allow*

（ 允许 ）– 允许附件通行。

*Deny*

（ 拒绝 ）– 拒绝接受附件，并向发件人发出拒绝消息。

*Drop*

（ 中断 ）– 去除附件并中断连接。系统不向邮件来源发出任何信息。

*Block*

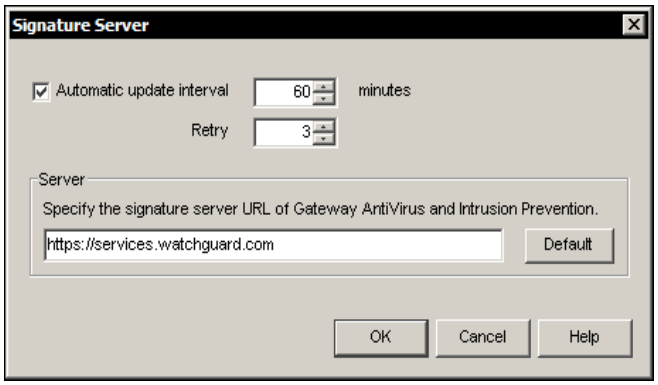
（ 禁止 ）– 阻止附件，并将发件人的 IP 地址添加到 Blocked Sites （ 受禁网站 ）列表

**注释**

如果你将配置设置为 Allow （ 允许 ）附件通过，则你的配置不够安全。

## 配置特征服务器

1 在 **Intrusion Prevention**（入侵防御）对话框中点击 **Signature Server**（特征服务器）。




2 要激活自动病毒特征更新功能，选择 **Automatic update**（自动更新）对话框。输入自动更新之间的间隔分钟数。

3 选择自动更新失败时重试的次数。

4 为 GAV/IPS 键入特征服务器的 URL。

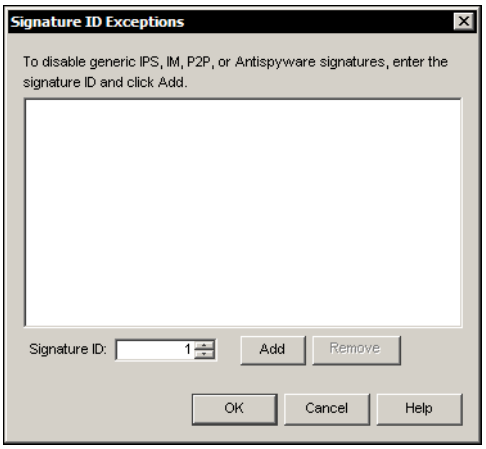
5 点击 **OK**（确认）。

6 选择 **File**（文件）**>Save**（保存）**>To Firebox**（到 **Firebox**）。

7 键入你的配置密码短语并点击 **OK**（确认）。

## 设定特征例外

1 在 **Intrusion Prevention**（入侵防御）对话框中点击 **Signature Exceptions**（特征例外）。屏幕将出现 Signature ID Exceptions（特征 ID 例外）对话框。



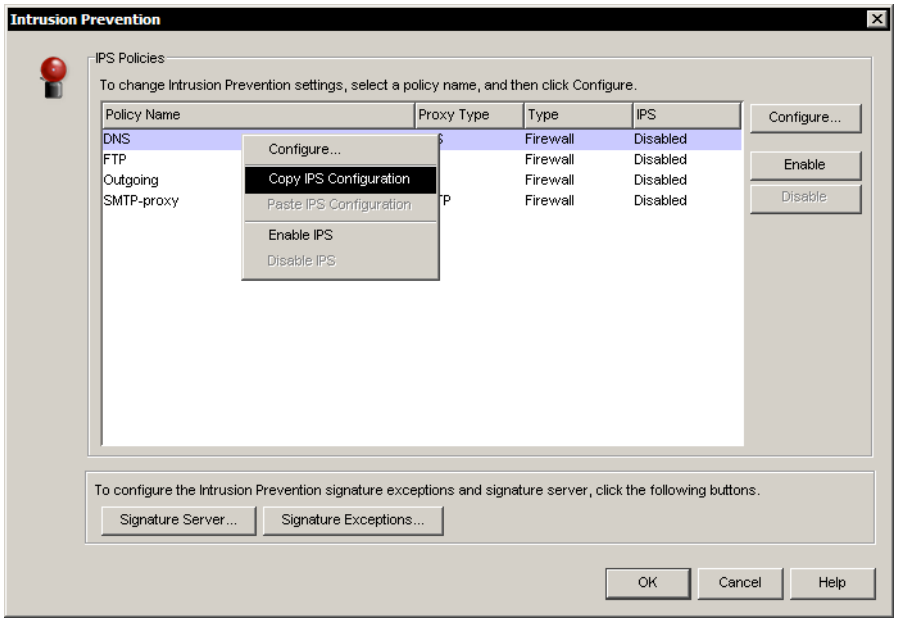

2 键入你想禁用的任何入侵防御服务、即時通信程序、点对点软件或反间谍软件。点击 **Add**（添加）。

### 将入侵防御设置拷贝到其他策略

在对一项代理协议进行入侵防御配置后，你可以将相同的配置拷贝到其他代理协议中。然而，该操作仅限于带有兼容入侵防御配置的策略。

- 在 FTP、 DNS 及 SMTP 策略之间
- 多个 TCP 策略之间
- 多个 HTTP 策略之间

1 在 **Intrusion Prevention （ 入侵防御 ）**对话框中选择你想拷贝其配置的代理协议，点击右键并选择 **Copy IPS Configuration （ 拷贝入侵防御配置 ）**。




2 在同一对话框中选择你想粘贴所选配置的目标代理协议，点击右键并选择 **Paste IPS Configuration （ 粘贴入侵防御配置 ）**。

## 入侵防御服务的查看及更新

你可以在 Firebox® System Manager （ FSM ）中的 **Security Services （ 安全服务 ）**选项卡中查看入侵防御服务并将其更新。

### 查看服务状态

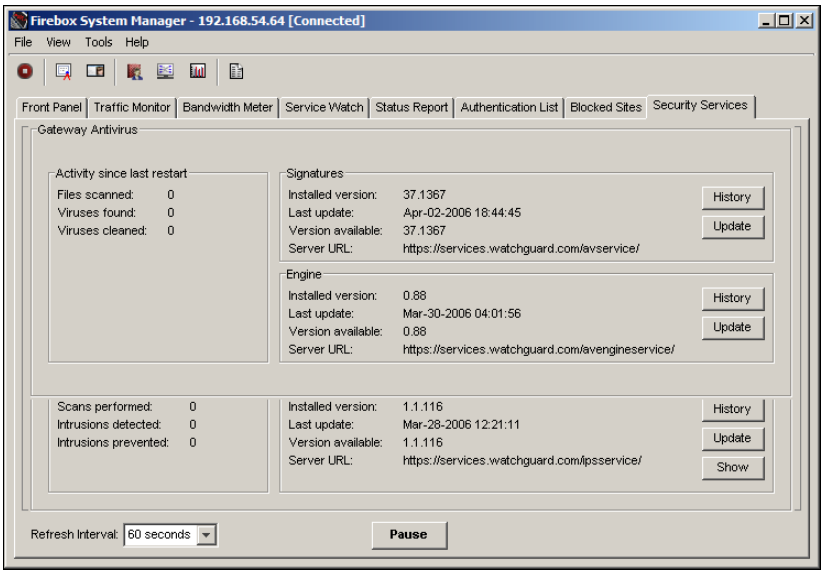
通过查看 IPS （ 入侵防御服务 ）状态，你可以得知 IPS （ 入侵防御服务 ）保护功能是否仍然有效。你也可以查看特征的版本。

要查看服务状态，你需要：

1 从 WSM 中选择 Firebox。选择 **Tools （ 工具 ）>Firebox System Manager （ FSM ）**。

也可以在 WSM 工具条上点击 Firebox System Manager （ FSM ）图标。

2 点击 **Security Services （安全服务）**选项卡。
Windows 将显示已安装安全服务的状态。必须安装这些功能的许可证照，便于查看状态信息。




3 点击 **History （历史）**查看先前更新特征数据库的日期、版本及状态。

## 手动更新特征

你可以将 IPS （入侵防御服务）设定为自动更新特征数据库。你也可以手动更新特征数据库。如果 Firebox 特征数据库已过期，系统将无法保护你免受最新病毒及攻击的入侵。

要手动更新，你需要进行以下操作：

1 打开 Firebox System Manager （FSM）。

2 点击 **Security Services （安全服务）**选项卡。
屏幕将出现安全服务状态。

3 为你想要更新的服务点击 **Update （更新）**。
Firebox 将下载可取得的最新特征数据库。请参阅 Traffic Monitor （流量控制）。
如果无最征数据库， Update （更新）按钮将显示为无效。

# 第 26 章 高级联网功能

**注释**

本章介绍的主要高级联网功能，即 " 服务质量 "（Quality of Service）、 OSPE 及 BGP 动态路由选择协议，仅可以在 Fireware® Pro 中实现。 Fireware 仅可以实现 RIP 动态路由选择协议。

高级联网功能旨在帮助 Firebox® 管理员更好、更有效地控制超大型或高流量网络。这些功能包括：

*Quality of Service （QoS）（服务质量）*

Fireware 的 QoS（服务质量）功能可以让你为各个策略设置优先传输队列、带宽限制以及联通速率限制。

*Dynamic routing （动态路由选择）*

除静态路由功能外， Firebox 也可以使用动态路由协议 RIP（版本 1 及 2）、 OSPF（版本 2）以及 BGP（版本 4）。这些路由协议允许对路由表进行动态修改。

## 创建 QoS（服务质量）对策

**注释**

本功能仅在 Fireware® Pro 中实现。

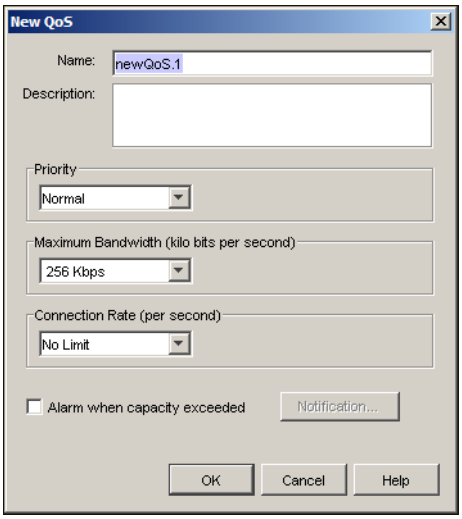
在存在大量主机的大型网络中，通过防火墙传输的数据量可能相当巨大。如果流量超过网络极限，数据包将阻挡。网络管理员可以使用 QoS（服务质量）防止在进行重要商业应用时发生数据遗失。例如，你可以将公司与各部门之间的数据流（如数据交换）设置为更高优先级，优于网上浏览或浏览的数据流。

通过 Fireware® Pro，你可以设置 QoS（服务质量）对策，并将其应用到各项策略中，确保重要数据流始终可以获得充足的宽带资源。

你也可以根据 QoS（服务质量）对策的参数，设置网络超载警报。你可以将警报设定为：Firebox® 向 SNMP 管理系统发出一份事件通知或向管理站发出一份电子邮件或弹出窗口形式的通知。

1 在 Policy Manager（政策管理器）中选择 **Setup（设置）>Actions（对策）>QoS（服务质量）**。
屏幕将出现 QoS（服务质量）对话框。


2 点击 **Add（添加）**。
屏幕将出现 New QoS（新增服务质量）对话框。




3 键入 QoS（服务质量）对策的名称及描述。

4 将 **Priority（优先级）**设置为正常，或在数据流需要优先处理时设置为高。
这些类别通常被称为队列。

5 使用 **Maximum Bandwidth（最大带宽）**下拉列表，设置或取消此对策的带宽限制。
为重要流量选择 No Limit（无限制），取消带宽限制，或选择每秒带宽的最大千字节。最大带宽设定完毕后，QoS（服务质量）对策将启动。

6 使用 **Connection Rate（连接速率）**下拉列表，设置 QoS（服务质量）对策启动前的每秒最大连接数。
在默认配置中，系统不对连接率进行任何限制。如果你选择 Custom（自定义），你可以键入最大连接率。设置完毕后，QoS（服务质量）对策将启动。

7 如果你想设置带宽或连接率超载或超量警报，你需要选择 **Alarm when capacity exceeded（超载警报）**对话框。你可以使用此警报确定一项策略是否需要更多宽带资源。点击 **Notification（通知）**，并参照 129 页的 “*设置日志及通知参数*”设置通知参数。

8 点击 **OK（确认）**。
新增对策将出现在 QoS Actions（服务质量对策）对话框中。

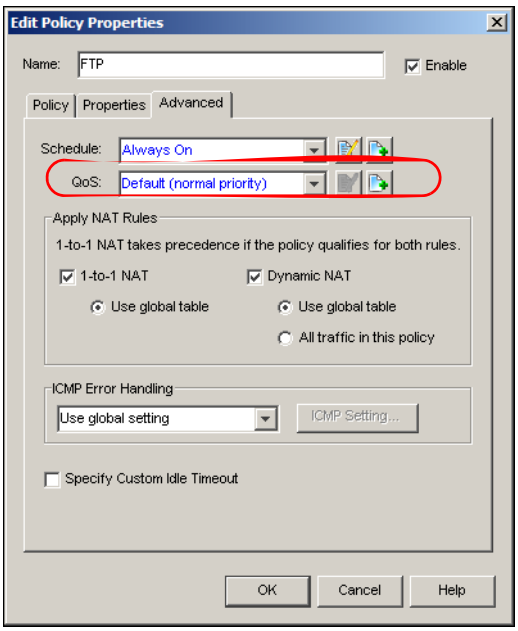
## 将 QoS（服务质量）对策应用到各项策略

创建 QoS（服务质量）对策完毕后，你可以将其应用到你在 Policy Manager（政策管理器）中配置的各项策略。具体操作为：

1 在 Policy Manager（政策管理器）中，双击你想为其添加 QoS（服务质量）对策的策略。

2 选择 **Advanced（高级）**选项框。

3 在 **QoS（服务质量）**下拉列表中选择将应用于策略的 QoS（服务质量）对策。




4 使用 **View（查看）/Edit（编辑）**或 **New（新增）/Clone（复制）**按钮（在 **Schedule** 和 **QoS** 字段的右边）修改 QoS（服务质量）对策的属性或为策略创建新的 QoS（服务质量）对策。

5 点击 **OK（确认）**。将修改内容保存到 Firebox。

## 在多重 WAN（广域网）中使用 QoS（服务质量）

在一项 QoS（服务质量）对策被应用到一项多重 WAN 策略后（而且已在循环模式下设置过多重 WAN），QoS（服务质量）对策中的最大带宽及连接率设置可以控制所有接口的总吞吐量及连接率。该操作包括为路由流量配置的所有外部接口，也包括暂停的外部接口。

在一项 QoS（服务质量）对策被应用到一项多重 WAN 策略后（而且已在循环模式下设置过多重 WAN），QoS（服务质量）对策中的最大带宽及连接率设置可以控制一个外部接口（该接口正在发送数据包）的吞吐量及连接率。

# 动态路由选择

路由选择协议是指各个路由器之间分享网络路由表中状态信息的语言。如果使用静态路由，路由表将被设置且不会发生改变。如果路由器在远程路径中运行失败，则数据包不会到达指定目的地。

动态路由允许路由表随路径的变化而改变。如果不能使用通向某一目的站的最佳路径，动态路由协议将修改路由表，使你的网络流量保持移动（如有必要）。Fireware® Pro 支持 RIP（版本 1 及 2）、OSPF 以及 BGP（版本 4）动态路由选择协议。Fireware 仅支持 RIP（版本 1 及 2）。

### 路由守护程序配置文件

要通过 Fireware 使用任何动态路由协议，你必须为你选择的路由守护程序导入或键入一份动态路由配置文件。你可以在此：

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

中查看每一路由协议的配置模版。

你可以在以下章节查看每一路由协议的受支持配置命令列表。以下命令的安排顺序与其在操作 配置文件中的顺序一致。

**有关配置文件的注释**：

- “!”及 “#”属于注释符号。如果单词的第一个字符为注释符号，则本行其它内容均为注释。如果注释符号不是单词的第一个字符，则可以将其解释为命令。
- 通常，你可以在行前使用单词 “no”，取消该命令。例如：“no network 10.0.0.0/24 area 0.0.0.0”可以在指定网络中取消主干区域。

# 使用 RIP

**注释**

可同时从 Fireware® 及 Fireware Pro 获得对本协议的支持。

RIP（路由信息协议）用于在自包含网络（self-contained network）（如公司局域网或私人广域网）中管理路由器信息。通过 RIP，网关主机会将其路由表每隔 30 秒发送到最近的路由器。随后，该路由器会将其路由表的内容发送到临近的其它路由器。

由于每隔 30 秒对整个路由表的传输将极大增加网络的负荷，且由于 RIP 表仅限于 15 路程段（hops），因此 RIP 是小型网络的最佳选择。OSPF 是大型网络的更佳代替方案。

## RIP（版本 1）

RIP（版本 1）通过在端口 520 上使用 UDP broadcast（UDP 发散性传输）向路由表发送更新信息。要创建或修改路由配置文件，请参见以下受支持的路由命令表。在配置文件中的章节顺序必须与此表中的顺序一致。你也可以使用此网页中的 RIP 配置文件示例：

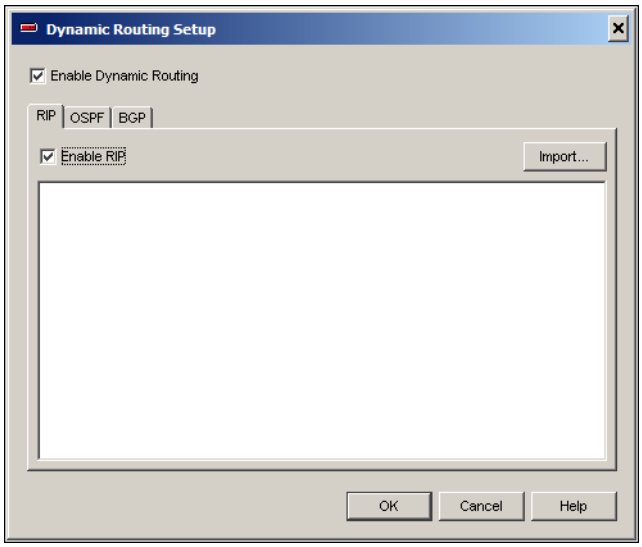
https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

| 项目 | 命令 | 描述 |
|---|---|---|
| 在接口上设置简单的密码或 MD5 认证 | | |
| | interface eth[N] | 为接口设置认证类型 |
| | ip rip authentication string [PASSWORD] | 设置 RIP 认证密码 |
| | key chain [KEY-CHAIN] | 设置 MD5 密钥链名称 |
| | key [INTEGER] | 设置 MD5 密钥编号 |
| | key-string [AUTH-KEY] | 设置 MD5 认证密钥 |
| | interface eth[N] | 为接口设置认证类型 |
| | ip rip authentication mode md5 | 使用 MD5 认证 |
| | ip rip authentication mode key-chain [KEY-CHAIN] | 设置 MD5 认证密钥链 |
| 配置 RIP routing daemon （路由选择端口监控程序） | | |
| | router rip | 激活 RIP 端口监控程序 |
| | version [1\|2] | 将 RIP 版本设置为 1 或 2 （默认版本 2） |
| | ip rip send version [1\|2] | 将 RIP 设置为发送版本 1 或 2 |
| | ip rip receive version [1\|2] | 将 RIP 设置为接收版本 1 或 2 |
| | no ip split-horizon | 禁用 split-horizon（横向隔离）；按默认值激活 |
| 配置接口及网络 | | |
| | no network eth[N] | |
| | passive-interface eth[N] | |
| | passive-interface default | |
| | network [A.B.C.D/M] | |
| | neighbor [A.B.C.D/M] | |
| 为 RIP 伙伴设备分配路由，并将 OSPF 或 BGP 路由注入 RIP 路由表 | | |
| | default-information originate | 与 RIP 伙伴设备共享最后可选路由（默认路由） |
| | redistribute kernel | 将防火墙静态路由重新分配到 RIP 伙伴设备 |
| | redistribute connected | 重新分配从所有接口到 RIP 伙伴设备的路由 |
| | redistribute connected route-map [MAPNAME] | 用一台路由映射表过滤器（映射表名称），重新分配从所有接口到 RIP 伙伴设备的路由 |
| | redistribute ospf | 重新分配从 OSPF 到 RIP 的路由 |
| | redistribute ospf route-map [MAPNAME] | 用一台路由映射表过滤器（映射表名称），重新分配从 OSPF 到 RIP 的路由 |
| | redistribute bgp | 重新分配从 BGP 到 RIP 的路由 |
| | redistribute bgp route-map [MAPNAME] | 用一台路由映射表过滤器（映射表名称），重新分配从 BGP 到 RIP 的路由 |
| 用路由映射表及访问列表（access lists）配置路由再分配过滤器 | | |

| 项目 | 命令 | 描述 |
|---|---|---|
| | access-list [PERMIT \| DENY] [LISTNAME] [A.B.C.D/M \| ANY] | 创建一份允许或拒绝对某一或所有 IP 地址进行重新分配的访问列表 |
| | route-map [MAPNAME] permit [N] | 创建一份路由映射表，为其命名并将优先级设置为 N |
| | match ip address [LISTNAME] | |

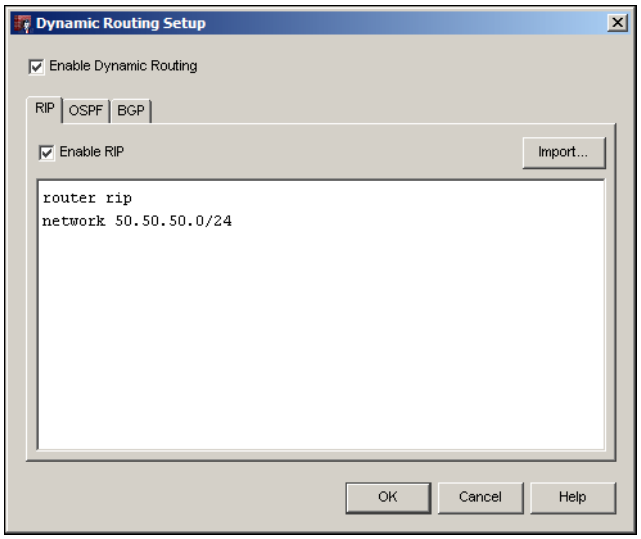
## 对 Fireware 或 Fireware Pro 进行 RIP （版本 1）配置

1 在 Policy Manager （政策管理器）中选择 **Network （网络）>Dynamic Routing （动态路由选择）**。
屏幕将出现 Dynamic Routing Setup （动态路由设置）对话框。




2 点击 **Enable Dynamic Routing （启用动态路由选择）**及 **Enable RIP （启用 RIP）**。

3 点击 **Import（导入）**，导入一份路由守护程序配置文件，或在文本框中键入你的配置文件。
如果点击 Import（导入），你可以浏览 RIP 守护程序配置模版的位置。具体位置为：C:\Documents and Settings\My Documents\My WatchGuard.

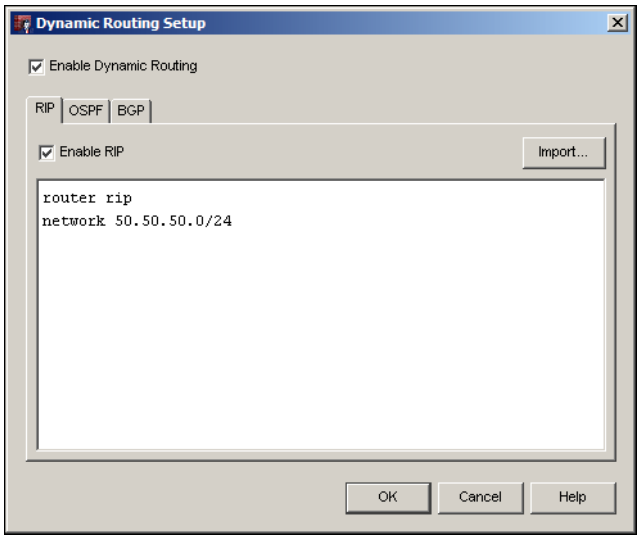



4 点击 **OK（确认）**。

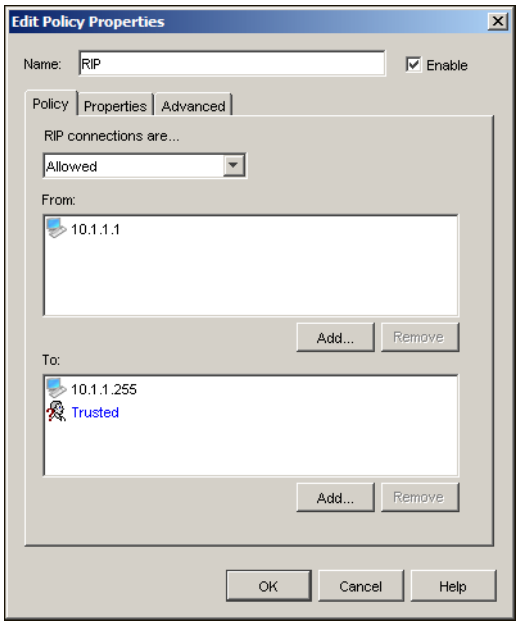
### 允许 RIP（版本 1）数据流通过 Firebox

你必须添加及配置一项策略，使其允许 RIP 从该路由器向网络发散性传输 IP 地址进行信息传输。你也必须将 Firebox® 的 IP 地址添加到 **To（至）**字段。

1 在 Policy Manager（政策管理器）中选择 **Edit（编辑）>Add Policies（添加策略）**。在数据包过滤器列表中选择 RIP。点击 **Add（添加）**。
屏幕将为 RIP 弹出 New Policy Properties（新策略属性）窗口。



2 在 **New Policy Properties（新策略属性）**对话框中对策略进行配置，使其允许从该使用 RIP 的路由器的 IP 或网络地址到其所连接的 Firebox® 接口的数据流通过。你也必须添加网络发散性传输 IP 地址。



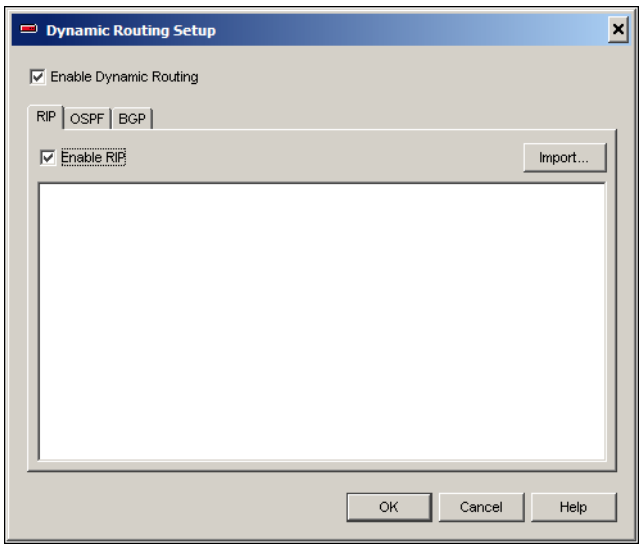

3 点击 **OK（确认）**。

## RIP（版本 2）

RIP（版本 2）使用多点传输发送路由表更新程序。要创建或修改路由配置文件，请参考 “*RIP（版本 1）*”章节中的受支持 RIP 路由命令表。使用网络 IP 地址的所有命令都必须包括子网掩码，否则 RIP（版本 2）将无法运行。在配置文件中的章节顺序必须与此表中的顺序一致。

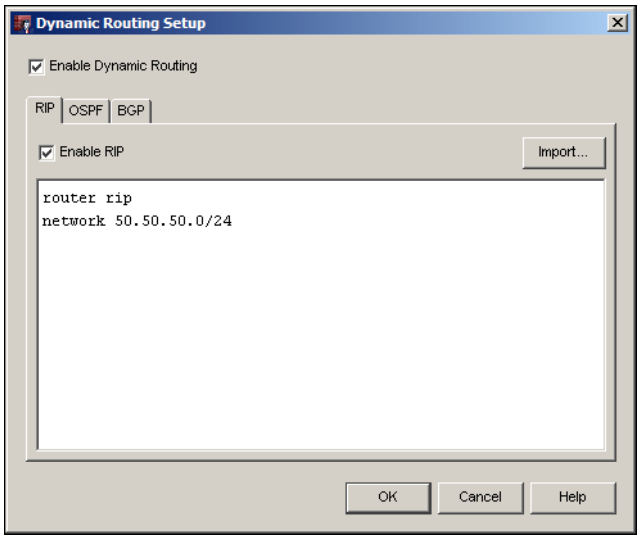
## 对 Fireware 或 Fireware Pro 进行 RIP（版本 2）配置

1 在 Policy Manager（政策管理器）中选择 **Network（网络）>Dynamic Routing（动态路由选择）**。
屏幕将出现 Dynamic Routing Setup（动态路由设置）对话框。




2 点击 **Enable Dynamic Routing（启用动态路由选择）**及 **Enable RIP（启用 RIP）**。

3 点击 **Import（导入）**，导入一份路由守护程序配置文件，或在文本框中键入你的配置参数。
如果点击 Import（导入），你可以浏览 RIP 守护程序配置模版的位置。具体位置为 :C:\Documents and Settings\My Documents\My WatchGuard。



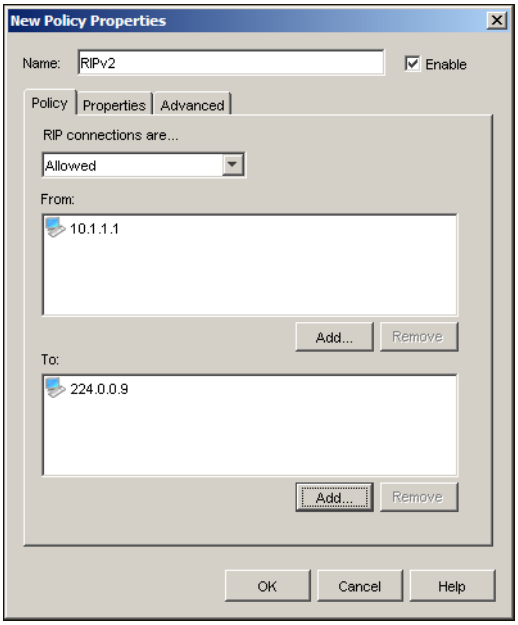

4 点击 **OK（确认）**。

### 允许 RIP（版本 2）数据流通过 Firebox

你必须添加及配置一项策略，使其允许 RIP（版本 2）从（激活 RIP[ 版本 2] 的）路由器向（为 RIP[ 版本 2]）预留的多点传输 IP 地址进行多点传输。

1 在 Policy Manager（政策管理器）中选择 **Edit（编辑）>Add Policies（添加策略）**。在数据包过滤器列表中选择 **RIP**。点击 **Add（添加）**。
屏幕将为 RIP 弹出 New Policy Properties（新策略属性）窗口。

2 在 **New Policy Properties（新策略属性）**窗口对策略进行配置，使其允许从该使用 RIP 的路由器的 IP 或网络地址到多点传输地址 224.0.0.9 的数据流通过。




3 点击 **OK（确认）**。

## 使用 OSPF

**注释**

仅可以从 Fireware® Pro 获得对本协议的支持。

OSPF（优先开放最短路进）是用于较大型网络中的内部路由器协议。使用 OSPF 后，路由器在发现路由表的任何变动或检测到网络中的任何变动时，将立即向网络中的所有其它路由器发出多点更新数据。 OSPF 与 RIP 的不同之处在于：

- OSPF 仅发送路由表的修改部分，而 RIP 每次发送整个路由表。
- 当 OSPF 的信息改变时，它仅发送多点传输数据。而 RIP 每隔 30 秒发送整个路由表。

你需要了解的有关 OSPF 的重要提示：

- 如果存在多个 OSPF 区域，必须将其中一个设置为 0.0.0.0（主干区域）。
- 所有区域必须临近主干区域。如果不临近，你必须为主干区域配置一个虚拟链接。

## OSPF 守护程序的配置

要创建或修改路由配置文件，请参见以下受支持的路由命令类别。在配置文件中的章节顺序必须与此表中的顺序一致。你也可以使用此网页中的 RIP 配置文件示例：

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

| 项目 | 命令 | 描述 |
|---|---|---|
| **配置接口** | | |
| | ip ospf authentication-key [PASSWORD] | 设置 OSPF 认证密码 |
| | interface eth[N] | 为接口设置属性 |
| | ip ospf message-digest-key [KEY-ID] md5 [KEY] | 设置 MD5 认证密钥 ID 及密钥 |
| | ip ospf cost [1-65535] | 为接口设置连接成本（见下文的 OSP 接口成本表） |
| | ip ospf hello-interval [1-65535] | 设置发送呼叫数据包（hello packet）的时间间隔；默认值为 10 秒 |
| | ip ospf dead-interval [1-65535] | 设置从临近设备上次呼叫之后到将其拒绝（declaring it down）之前的时间间隔；默认值为 40 秒 |
| | ip ospf retransmit-interval [1-65535] | 设置链接状态公告（LSA）重传之间的时间间隔；默认值为 5 秒 |
| | ip ospf transmit-delay [1-3600] | 设置发送 LSA 更新所需的时间；默认值为 1 秒 |
| | ip ospf priority [0-255] | 设置路由优先级；数值越高，则更具备成为指定路由（DR）的条件 |
| **配置 OSPF 路由选择端口监控程序** | | |
| | router ospf | 激活 OSPF 端口监控程序 |
| | ospf router-id [A.B.C.D] | 为 OSPF 相互设置路由 ID；如果未设置，路由器将确定其自己的 ID |
| | ospf rfc 1583compatibility | 激活 RFC 1583 兼容功能（可以导致路由环路） |
| | ospf abr-type [cisco\|ibm\|shortcut\|standard] | 有关此命令的更多信息请参阅 draft-ietf-abr-alt-o5.txt |
| | passive interface eth[N] | 在 interface eth[N] 上禁用 OSPF 公告 |
| | auto-cost reference bandwidth [0-429495] | 设置全程成本（global cost）（见下文的 OSPF 成本表）；请勿使用 “ip sopf[COST]” 命令 |
| | timers spf [0-4294967295][0-4294967295] | 设置 OSPF 进度延迟及持续时间 |
| **在网络中激活 OSPF**<br>*The “Area” variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z]. | | |
| | network [A.B.C.D/M] area [Z] | 为区域 0.0.0.Z 在网络 A.B.C.D/M 上通告 OSPF |
| **为骨干区域或其它区域配置属性**<br>*The “Area” variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z]. | | |
| | area [Z] range [A.B.C.D/M] | 创建区域 0.0.0.Z 并为该区域设置有类网络（范围与接口网络及掩码的设置应该相匹配） |

| 项目 | 命令 | 描述 |
|---|---|---|
| | area [Z] virtual-link [W.X.Y.Z] | 为区域 0.0.0.Z 创建虚拟连接邻居 |
| | area [Z] stub | 将区域 0.0.0.Z 设置为占位程序（stub） |
| | area [Z] stub no-summary | |
| | area [Z] authentication | 为区域 0.0.0.Z 激活简单的密码认证 |
| | area [Z] authentication message-digest | 为区域 0.0.0.Z 激活 MD5 认证 |
| **重新分配 OSPF 路由** | | |
| | default-information originate | 与 OSPF 共享最后可选路由（默认路由） |
| | default-information originate metrics [0-16777214] | 与 OSPF 共享最后可选路由（默认路由） |
| | default-information originate always | 与 OSPF 共享最后可选路由（默认路由） |
| | default-information originate always metrics [0-16777214] | 与 OSPF 共享最后可选路由（默认路由） |
| | redistribute connected | 重新分配从所有接口到 OSPF 的路由 |
| | redistribute connected metrics | 重新分配从所有接口到 OSPF 的路由 |
| **用访问列表及路由映射表配置路由重新分配功能** | | |
| | access-list [LISTNAME] permit [A.B.C.D/M] | 创建一份允许分配 A.B.C.D/M 的访问列表 |
| | access-list [LISTNAME] deny any | 限制分配任何上述未指定的路由映射表 |
| | route-map [MAPNAME] permit [N] | 创建一份路由映射表（MAPNAME），为其命名并将优先级设置为 N |
| | match ip address [LISTNAME] | |

## OSPF 接口成本表

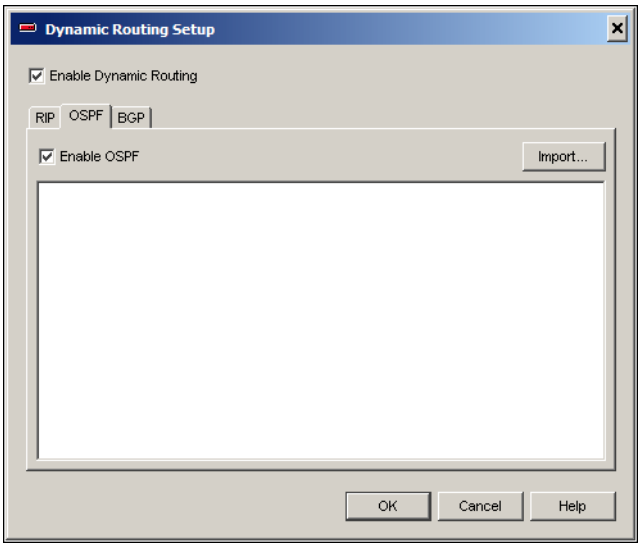
OSPF 协议可以发现两点之间的最有效路径。OSPF 将查看接口连接速度、各点之间的路程段数量以及其它尺度。在默认状态下， OSPF 使用某一设备的实际连接速度计算某一路由的总成本。例如：如果你的千兆字节防火墙连接到一台 100M 的路由器，你可以手动设置接口成本，以实现最大效率。使用 OSPF Interface Cost（OSPF 接口成本）本表中的数字，手动将接口成本设置为与实际接口成本不同的数值。

| 接口类型 | 带宽（比特 / 秒） | 带宽（bytes/ 秒） | OSPF 接口成本 |
|---|---|---|---|
| 以太网 | 1G | 100M | 1 |
| 以太网 | 100M | 10M | 10 |

| 接口类型 | 带宽（比特 / 秒） | 带宽（bytes/ 秒） | OSPF 接口成本 |
|---|---|---|---|
| 以太网 | 10M | 1M | 100 |
| 调制解调器 | 2M | 200K | 500 |
| 调制解调器 | 1M | 100K | 1000 |
| 调制解调器 | 500K | 50K | 2000 |
| 调制解调器 | 250K | 25K | 4000 |
| 调制解调器 | 125K | 12500 | 8000 |
| 调制解调器 | 62500 | 6250 | 16000 |
| 串口 | 115200 | 9216 | 10850 |
| 串口 | 57600 | 4608 | 21700 |
| 串口 | 38400 | 3072 | 32550 |
| 串口 | 19200 | 1636 | 61120 |
| 串口 | 9600 | 768 | 65535 |

## 对 Fireware Pro 进行 OSPF 配置

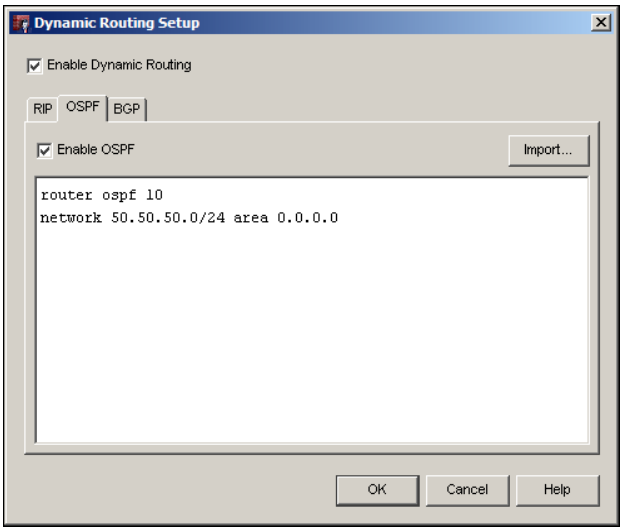
1 在 Policy Manager（政策管理器）中选择 **Network**（网络）**>Dynamic Routing**（动态路由选择）。
屏幕将出现 Dynamic Routing Setup（动态路由设置）对话框。




2 点击 **OSPF** 选项框。

3 点击 **Enable Dynamic Routing**（启用动态路由选择）及 **Enable OSPF**（启用 **OSPF**）。

4 点击 **Import（导入）**，导入一份路由守护程序配置文件，或在文本框中键入你的配置参数。
如果点击 Import（导入），你可以浏览 OSPF 守护程序配置文件的位置。具体位置为：C:\Documents and Settings\My Documents\My WatchGuard。



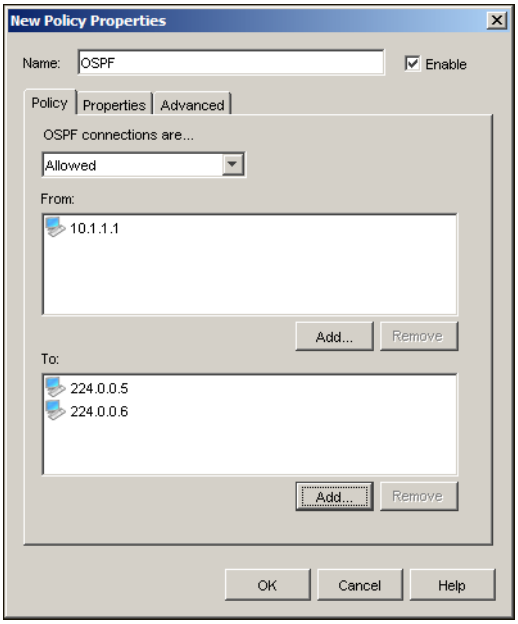

5 点击 **OK（确认）**。

## 允许 OSPF 数据流通过 Firebox

你必须添加及配置一项策略，使其允许 OSPF 从（激活 OSPF 的）路由器向（为 OSPF）预留的多点传输 IP 地址进行多点传输。

1 在 Policy Manager（政策管理器）中选择 **Edit（编辑）>Add Policies（添加策略）**。在数据包过滤器列表中选择 **OSPF**。点击 **Add（添加）**。
屏幕将为 OSPF 弹出 New Policy Properties（新策略属性）窗口。

2 在 **New Policy Properties（新策略属性）**窗口对策略进行配置，使其允许从该使用 RIP 的路由器的 IP 或网络地址到多点传输地址 224.0.0.5 及 224.0.0.6 的数据流通过。点击 **OK 确定**。




# 使用 BGP

**注释**

仅可以从 Fireware Pro® 获得对本协议的支持。

BGP（边界网关协议）是一款由路由群使用的可测量动态路由协议，用于共享路由信息。 BGP 是一种在网络上使用的路由协议。 BGP 使用路由参数或 “属性”定义路由策略，并营造稳定的路由环境。 BGP 允许你为你的网络及资源优选多个网络路径，因此可以向你提供冗余路径并增加你的正常运行时间。

当其中一台主机检测到修改内容后，使用 BGP 的主机群将使用 TCP 发送更新的路由表信息。 BGP 使用无类别域间路由选择（CIDR）技术减小因特网路由表的大小。 Fireware Pro 中的 BGP 路由表被设定为 32K。

一般 WatchGuard® 客户的 WAN 大小最适合 OSPF 动态路由。如果存在多个因特网网关， WAN 也可以使用 EBGP（外部边界网关协议）。 EBGP 允许你充分利用多归路网络可能出现的冗余。

要通过 ISP 加入 EBGP，你必须取得一个 ASN（自治系统编号）。你必须从下表中的其中一个区域注册点取得一个 ASN。取得你自己的 ASN 后，你必须联系每一 ISP，取得其各自的 AS 编号以及其它必要信息。

| 区域 | 注册名 | 网站 |
|---|---|---|
| 北美 | ARIN | www.arin.net |
| 欧洲 | RIPE NCC | www.ripe.net |
| 亚太 | APNIC | www.apnic.net |
| 拉丁美洲 | LACNIC | www.lacnic.net |
| 非洲 | AfriNIC | www.afrinic.net |

## BGP 守护程序的配置

要创建或修改路由配置文件，请参见以下受支持的路由命令类别。在配置文件中的章节顺序必须与此表中的顺序一致。你也可以使用此网页中的 BGP 配置文件示例：

https://www.watchguard.com/support/advancedfaqs/fw_dynroute-ex.asp

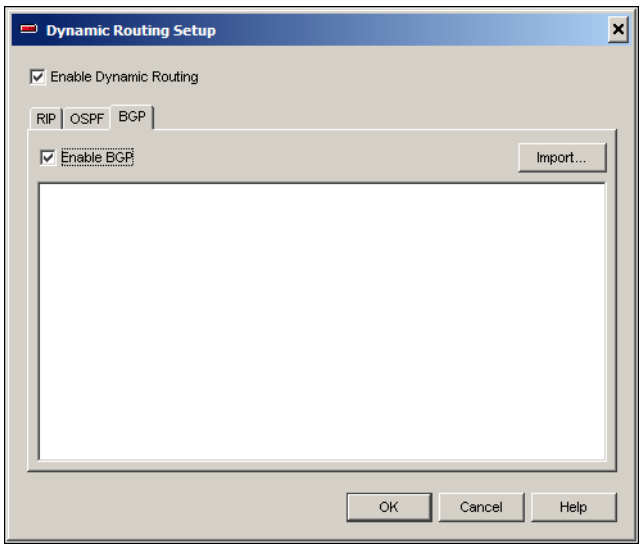
请勿使用你未从你的 ISP 取得的 BGP 配置参数。

| 项目 | 命令 | 描述 |
|---|---|---|
| **配置 BGP 路由选择端口监控程序** | | |
| | router bgp [ASN] | 激活 BGP 端口监控程序并设置独立系统编号（ASN）；由 ISP 提供 |
| | network [A.B.C.D/M] | 在网路 A.B.C.D/M 上广播 BGP |
| | no network [A.B.C.D/M] | 在网路 A.B.C.D/M 上禁止 BGP 广播 |
| 设置相邻路由（neighbor）属性 | | |
| | neighbor [A.B.C.D] remote-as [ASN] | 将临近路由（neighbor）作为远程 ASN 的成员进行设置 |
| | neighbor [A.B.C.D] ebgp-multihop | 在使用 EBGP 多跳（multi-hop）功能的另一网络中设置 neighbor |
| | neighbor [A.B.C.D] version 4+ | 为与 neighbor 的通信设置 BGP 版本（4,4+,4-）；默认值为 4 |
| | neighbor [A.B.C.D] update-source [WORD] | 为 TCP 连接设置使用特殊接口的 BGP 会话 |
| | neighbor [A.B.C.D] default-originate | 将默认路由传播到 BGP neighbor[A.B.C.D] |
| | neighbor [A.B.C.D] port 189 | 将自定义 TCP 端口设置为与 BGP neighbor[A.B.C.D] 通信 |
| | neighbor [A.B.C.D] send-community | 设置伙伴设备发送社区（peer send-community） |
| | neighbor [A.B.C.D] weight 1000 | 为 neighbor[A.B.C.D] 路由设置默认重量 |
| | neighbor [A.B.C.D] maximum-prefix [NUMBER] | 设置此 neighbor 允许的最大前缀数 |
| Community Lists | | |
| | ip community-list [<1-99>\|<100-199>] permit AA:NN | 指定接受独立系统编号及网络编号（由冒号分开）的社区 |

| 项目 | 命令 | 描述 |
|---|---|---|
| 伙伴设备过滤程序 | | |
| | neighbor [A.B.C.D] distribute-list [LISTNAME] [IN\|OUT] | 为伙伴设备设置分配列表及方向 |
| | neighbor [A.B.C.D] prefix-list [LISTNAME] [IN\|OUT] | 将与入站广告或出站广告匹配的前缀列表应用到该 neighbor |
| | neighbor [A.B.C.D] filter-list [LISTNAME] [IN\|OUT] | 将独立系统路径访问列表匹配到入站路由及出站路由 |
| | neighbor [A.B.C.D] route-map [MAPNAME] [IN\|OUT] | 将路由映射表匹配到入站路由及出站路由 |
| 将路由重新分配到 BGP | | |
| | redistribute kernel | 将静态路由重新分配到 BGP |
| | redistribute rip | 将 RIP 路由重新分配到 BGP |
| | redistribute ospf | 将 OSPF 路由重新分配到 BGP |
| 路由反射 | | |
| | bgp cluster-id A.B.C.D | 如果 BGP 集群器有多个路由反射器，对该集群器进行配置 |
| | neighbor [W.X.Y.Z] route-reflector-client | 将路由器作为 BGP 路由反射器进行配置，并将指定 neighbor 作为其客户端进行配置 |
| 访问列表及 IP 前缀列表 | | |
| | ip prefix-list PRELIST permit A.B.C.D/E | 设置前缀列表 |
| | access-list NAME [deny\|allow] A.B.C.D/E | 设置访问列表 |
| | route-map [MAPNAME] permit [N] | 与 “匹配” 及 “设置” 命令连用，此命名为路由的重新分配定义条件及对策 |
| | match ip address prefix-list [LISTNAME] | 匹配指定的访问列表 |
| | set community [A:B] | 匹配指定的社区列表 |
| | match community [N] | 为独立系统路径设置优选值 |
| | set local-preference [N] | 设置自治系统路径 |

### 对 Fireware Pro 进行 BGP 配置

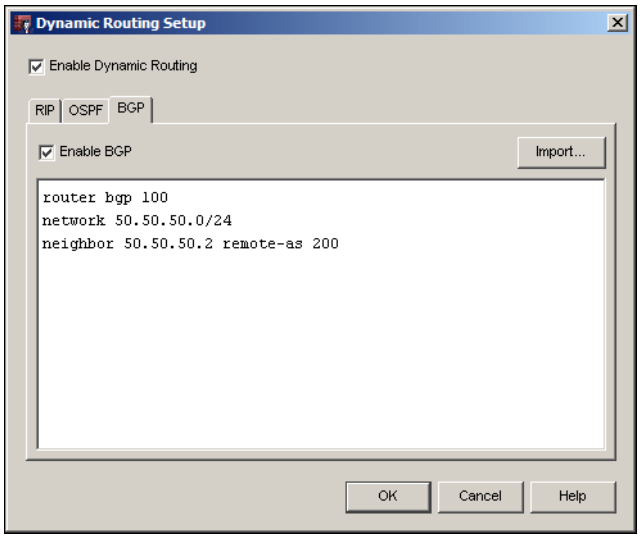
1 在 Policy Manager（政策管理器）中选择 **Network（网络）>Dynamic Routing（动态路由选择）**。
屏幕将出现 Dynamic Routing Setup（动态路由设置）对话框。




2 点击 **BGP** 选项框。

3 点击点击 **Enable Dynamic Routing（启用动态路由选择）**及 **Enable BGP（启用 BGP）**。

4 点击 **Import（导入）**，导入一份路由守护程序配置文件，或在文本框中键入你的配置参数。
如果点击 Import（导入），你可以浏览 BGP 守护程序配置文件的位置。具体位置为：C:\Documents and Settings\My Documents\My WatchGuard。



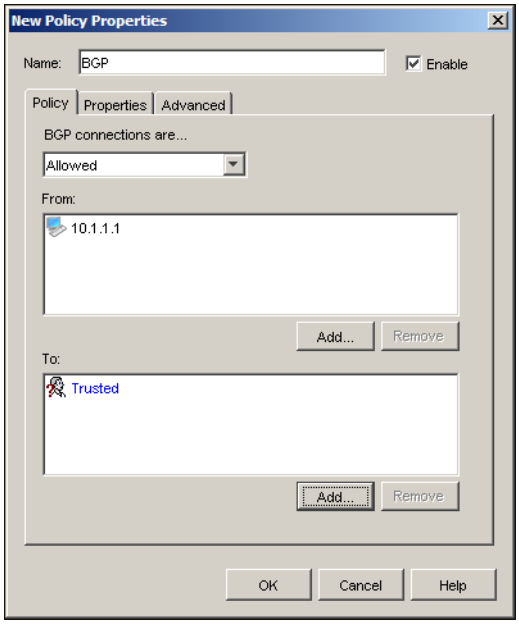

5 点击 **Select a BGP Configuration（选择一份 BGP 配置）**文件。点击 **OK（确认）**。

## 允许 BGP 数据流通过 Firebox

你必须添加及配置一项策略，使其允许从认可网络到 Firebox® 的流量通过。这些网络必须与你在你的 BGP 配置文件中定义的网络相同。

1 在 Policy Manager（政策管理器）中选择 **Edit（编辑）>Add Policies（添加策略）**。在数据包过滤器列表中选择 BGP。点击 **Add（添加）**。
屏幕将为 BGP 弹出 New Policy Properties（新策略属性）窗口。

2 在 **New Policy Properties（新策略属性）**对话框中对策略进行配置，使其允许从该使用 RIP 的路由器的 IP 或网络地址到其所连接的 Firebox 接口的数据流通过。点击 **OK（确认）**。



# 第 27 章　高度可用性（HA）

**注释**

High Availability（高度可用性）功能仅可以从 Fireware® Pro 获得。

High Availability（高度可用性）（HA）是指某一网络在出现硬件或软件问题时持续正常运行的能力。当你为网络添加冗余时，便排除了一个漏洞点。

WatchGuard® HA 功能实现了在容错配置中安装两台 Firebox® 设备。配置包括一台作为主设备的 Firebox 及一台作为辅助设备的 Firebox。其中一台 Firebox 将始终处于运行状态，而另一台则处于备用状态。上述两台 Firebox 被称为 “Peers（伙伴设备）”，他们经常相互发送消息，通告其各自的状态。

发生容错转接时，备用系统将被激活。被激活后，该 Firebox 将始终处于运行状态，直到系统掉线自动激活处于备用状态的另一 Firebox。

本章介绍两种 HA 配置方法。如果将要进行 HA 配置的 Firebox 设备是 Firebox X Core 或 Peak e 系列设备，则应选用第一种方法。如果两台 Firebox 设备是 Firebox X Core 或 Peak 设备，而非 e 系列设备，你可以使用第一或第二种方法。

## HA 要求

实现 HA 功能的要求：

- 在每对 HA 设备中，将一台 Firebox 作为主 Firebox。我们建议你将已获得最多许可功能及载量的 Firebox® 用作主 HA 设备。
- HA 配置中的两台 Firebox 必须为同一型号，并使用同一版本的软件。如果软件版本不同，你必须升级使用旧版软件的 Firebox，使两台 Firebox 相互匹配。使用旧版软件的 Firebox 必须取得软件升级许可。
- 必须将主 HA Firebox 的每一有效接口连接到网络集线器或接线器，同时辅助 HA Firebox 上与该接口对应的接口也将连接到该集线器或接线器。
- 当你在一个 HA 集群中连接两台 Firebox 设备时，你需要将每一台 Firebox 上最高编号端口之间的电缆线连接起来。如果你正在配置 Firebox 之间的两条 HA 连接，请使用每一台 Firebox 上的两个最高编号端口。我们建议你在配置上述两条 HA 连接之后，将各个端口连接起来。

- 如果两台HA Firebox设备中的其中一台是由管理服务器创建及管理的VPN隧道的VPN端点，则 HA 功能无法正常实现。
- 你不能将一台 WatchGuard 管理服务器安排在作为HA集群组成部分的一台网关Firebox之后。

**注释**

要实现 HA 功能，系统必须有一个或多个转用于 HA 同步的接口。

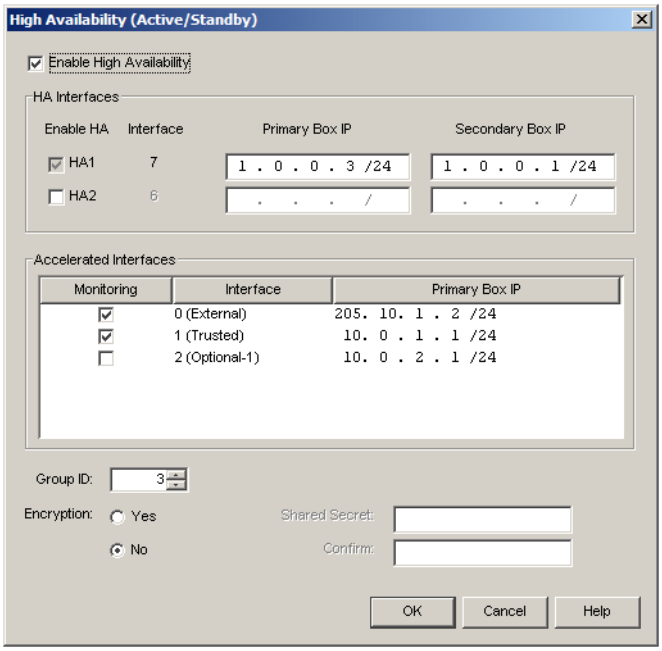
## 选择一台 HA Firebox

激活 HA 功能时，每对 Firebox 设备中的每一台 Firebox® 必须取得使用同一版本 Fireware® 应用软件的功能密钥。我们建议你将已获得最多许可功能的 Firebox 用作主 Firebox。如果你为 HA 设备组购买了升级软件，你必须在 LiveSecurity 网站激活该升级软件时，将该升级软件应用到主 Firebox 的序列号。 HA 设备组中的两台 Firebox 将同时使用主 Firebox 的许可功能。

如果你使用获得 VPN 认证证书的 IPSec VPN 隧道，辅助 Firebox 必须获得其自己的 IPSec VPN 证书。发生容错转接时，只有管理服务器证书将从主 Firebox 拷贝到辅助 Firebox。

## 为 Firebox X e 系列设备配置 HA 功能

1 在主 HA Firebox 的 Policy Manager（政策管理器）中选择 **Network（网络）**>**High Availability（高度可用性）**。
屏幕将出现 HA 对话框。




2 选择 **Enable High Availability（启用高度可用性功能）**对话框。

3 为接口选择 **HA1（高度可用性 1）**对话框，启动高度可用性功能。

4 在 **Primary Box IP**（**主 Box IP**）文本框中，你可以修改你想修改的默认 IP 地址。此 IP 地址应源自预留或未分配的网络。此 IP 地址将成为该接口的永久性 IP 地址。

5 在 **Secondary Box IP**（**辅助 Box IP**）文本框中，键入同一子网的 IP 地址。
如果你想修改默认的主 Firebox IP 地址，请勿修改默认的辅助 box IP 地址。

6 如果你想使用辅助 HA 接口，选择 **HA2** 对话框，将其激活。
HA2 接口属于可选项。

7 你可以选择你想监控其物理连接状态的接口。Firebox 将监控选中的界面，并启动 HA 容错转接（如果该接口不处于运行状态）。点击临近接口名称的对话框，激活监控功能。清除临近接口名称的对话框，关闭对某一接口的监控。
推荐监控所有启用的设备。

8 使用 **Group ID**（**群组 ID**）数值控制在网络中识别此 HA group（群组）。如果你在同样的网络中使用多个 HA 设备组，则每组设备的此数值必须不同。

9 点击 **Yes**（**是**）单选按钮对各组 Firebox 之间的 HA 流量进行加密。通常，此操作并非必要性操作，而且会占用更多资源。
或点击 **No**（**否**）单选按钮不对各组 Firebox 之间的 HA 流量进行加密。

10 （如果你选择了 **Yes**[ 是 ] 单选按钮）在 **Shared Secret**（**共享密钥**）字段键入共享密钥，对各组 Firebox 之间的 HA 流量进行加密。在 **Confirm**（**确认**）字段再次键入共享密钥。

11 将此配置保存到正在运行中的 Firebox。

12 关闭 Policy Manager（政策管理器）。

## 配置辅助 HA Firebox

辅助 HA Firebox 必须：

- 与 主 HA Firebox 的型号一致。
- 取得有效的功能密钥。

在你为实现主 HA 功能而激活辅助 Firebox 后，你必须首选使用 Web Quick Setup Wizard（Web 快速安装向导）在 Firebox 中安装 Fireware® 及基础配置。在按照 Web Quick Setup Wizard（Web 快速安装向导）操作完毕后，将该台 Firebox 置入你的网络。

## 启用 HA 功能

在对主 HA Firebox 及辅助 HA Firebox 进行配置后：

1 为你选定将其作为辅助 HA 设备的 Firebox 打开 Firebox 系统管理器。

2 选择 **Tools**（**工具**）**>High Availability**（**高度可用性**）**>Enable as Secondary**（**作为辅助设备启用**）。
屏幕将出现 Confirm Enable as Secondary（确定作为辅助设备启用）对话框。

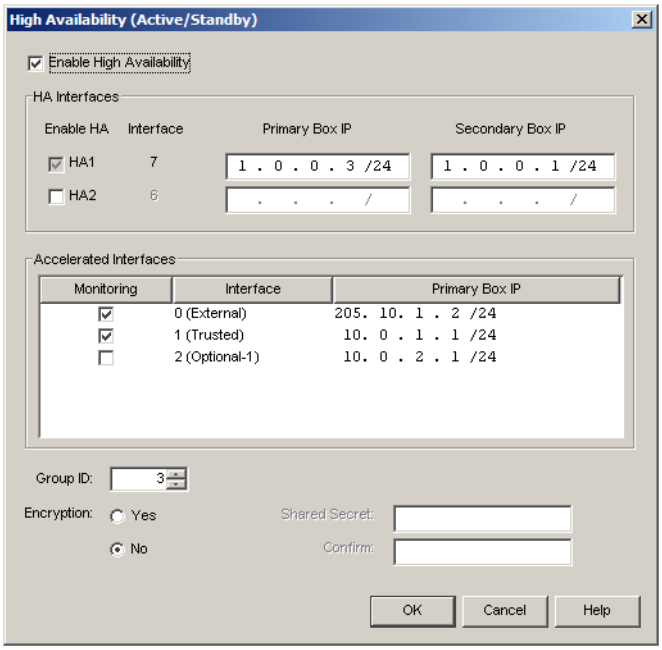

3 点击 **Yes**（**是**）将 Firebox 恢复到其默认状态，并在 HA 设备组中将其设定为辅助 HA Firebox。
你必须为辅助 HA Firebox 键入配置密码短语。

4 使用跨接电缆将一台 Firebox 的 HA1 接口（eth7）连接到另一台 Firebox 的 HA1 接口。如果 HA2（eth6）被启用，也需要同时连接两个 HA2 接口。

5 为主 HA Firebox 中打开 Firebox 系统管理器，并选择 **Tools（工具）>High Availability（高度可用性）>Synchronize Configuration（同步配置）**。收到系统提示后，键入配置口令。
你将看到 “高度可用性功能已被激活” 的消息。

## 为 Firebox X（非 e 系列）设备配置 HA 功能

1 在 Policy Manager（政策管理器）中选择 **Network（网络）>High Availability（高度可用性）**。
屏幕将出现 HA 对话框。




2 选择 **Enable High Availability（启用高度可用性功能）**对话框。

3 为接口选择 **HA1** 对话框，启动高度可用性功能。

4 在 **Primary Box IP**（主 Box IP）文本框中，你可以修改默认 IP 地址。此 IP 地址应源自预留或未分配的网络。此 IP 地址将成为该接口的永久性 IP 地址。

5 在 **Secondary Box IP（辅助 Box IP）**文本框中，键入同一子网的 **IP** 地址。

6 选择 **HA2** 对话框，将 HA2 接口激活。
HA2 接口属于可选项。

7 使用 **Group ID（群组 ID）**数值控制在网络中识别此 HA group（群组）。如果你在同样的网络中使用多个 HA 设备组，则每组设备的此数值必须不同。

8 点击 **Yes（是）**单选按钮对各组 Firebox 之间的 HA 流量进行加密。通常，此操作并非必要性操作，而且会占用更多资源。
或
点击 **No（否）**单选按钮不对各组 Firebox 之间的 HA 流量进行加密。

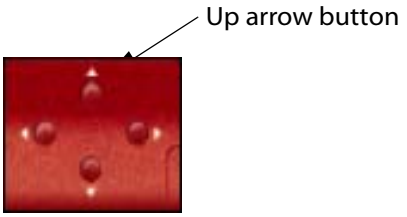
9 如果你选择了 **Yes**[ 是 ] 单选按钮在 **Shared Secret（共享密钥）**字段键入共享密钥，对各组 Firebox 之间的 HA 流量进行加密。在 **Confirm（确认）**字段再次键入共享密钥。

10 将此配置保存到正在运行中的 Firebox。

11 关闭 **Policy Manager（政策管理器）**。

12 使用跨接电缆将一台 Firebox 的 HA1 接口（eth5）连接到另一台 Firebox 的 HA1 接口。如果 HA2（eth4）被启用，也需要同时连接两个 HA2 接口。

13 将辅助设备设置为安全模式。具体操作为：关闭该台 Firebox，然后在你按住 Firebox 前面板上的 up arrow（上箭头）按钮时，再次将其打开。




14 开启 Firebox 系统管理器，并连接到主 Firebox。

15 选择 **Tools（工具）>High Availability（高度可用性）>Synchronize Configuration（同步配置）**。收到系统提示后，键入配置密码短语。
你将看到 “高度可用性功能已被激活” 的消息。

## 手动控制 HA 功能

尽管 HA 操作通常为自动进行，你仍然可以手动操作某些功能。

### 强制性转接

你可以手动进行强制性转接。届时，备用系统将立即被激活。

在 Firebox 系统管理器中，选择 **Tools（工具）>High Availability（高度可用性）>Force Failover（强制性转接）**。

### 同步配置

如果一台 Firebox 被关闭或与同组的另一台伙伴 Firebox 失去连线时另一台 Firebox 的配置发生变化，则你必须对配置进行同步处理。

在 Firebox 系统管理器中，选择 **Tools（工具）>High Availability（高度可用性）>Synchronize Configuration（同步配置）**。

### 重新启动伙伴设备

你设定的新 HA 配置仅对运行中的 Firebox 有效。要重启伙伴 Firebox，你必须从运行状态下的 Firebox 发出启动命令：

在 Firebox 系统管理器中，选择 **Tools（工具）>High Availability（高度可用性）**>Restart Peer **（重启伙伴设备）**。

**注释**

如果 Firebox 处于高 CPU 及流量状态，而且你使用 Firebox 系统管理器控制 HA 操作，你可能会收到一条错误的 “超时（time-out）消息”。在此情况下，此操作可能已经完成，因此该消息可能不正确。

### 备份 HA 配置

如果是一台用于 HA 功能的 Firebox，你仅可以在其处于运行状态时备份此 Firebox 的 flash 图象，原因是备份图象包括在容错转接之前并不存在于辅助设备中的系统及策略信息、证书以及许可。要创建正在运行 Firebox 的备份图象（.fxi），你需要：

1 在 Policy Manager（政策管理器）中选择 **File（文件）>Backup（备份）**。
2 键入配置密码短语。点击 **OK（确认）**。
3 键入并确认加密密钥。该密钥用户加密备份文件。
键入便于记忆的加密密钥。
4 浏览或键入备份文件的位置。点击 **OK（确认）**。
备份文件将被创建。
5 备份完成后点击 **OK（确认）**。

## 在 HA 配置中升级软件

如果你需要为正在运行中的 Firebox® 安装软件， HA 配置中的备用 Firebox 不会自动升级。你必须分别升级每一 Firebox。首先应升级运行状态中的 Firebox。重新启动后，备用 Firebox 将被激活，然后你可以对其进行升级。你无法在备用模式下升级 Firebox 中的软件。

## HA 与基于特征的安全服务

Gateway AntiVirus 及入侵防御服务（IPS）的特征数据库不会在运行及备用状态下的设备之间实现自动同步更新。

如果在防病毒及入侵防御服务已被激活的情况下发生了将备用 Firebox® 激活的系统事件，则此装备的防病毒及入侵防御服务特征数据库可能不是最新版本（尤其是当该设备长期处于备用状态时）。在数据库实现更新前，新病毒或 IPS 攻击可能会绕过你的 Firebox 进入你的系统。

要避免此问题，你应该启动 GAV 及 IPS 特征数据库定期更新功能，并尽量提高定期更新频率。如有可能，应在容错转接事件发生后立即手动更新特征数据库。

## HA 与 Proxy Sessions（代理会话）的使用

当默认配置的 HA 功能被激活时，所有 TCP 会话（TCP sessions）将在容错转接事件发生后完全断开。用户必须手动重新建立所有交互式或持久性会话。发生上述状况的原因是 HA 伙伴设备之间并未储存 proxy session 的状态记录，而且默认配置将向所有会话提供一份默认 TCP 代理协议。数据包过滤器会话将得到保留，但数据包并不是按照默认配置运行。你可以考虑为你想转接的 telnet、ssh 或任何其它策略将特定的数据包过滤器策略添加到你的配置中。注意 IPS 与这些新策略不兼容。

# 附件 A 版权和许可

## WatchGuard Firebox 软件终端用户许可协议

重要提示 – 请在使用 WatchGuard 软件前仔细阅读以下内容 :

本 WatchGuard Firebox 软件终端用户许可协议 （ 本协议 ）是你 （ 个人或单个实体 ）与 WatchGuard Technologies, Inc.（ WatchGuard ）之间为 WatchGuard Firebox 软件产品达成的合法协议。上述 WatchGuard Firebox 软件产品包括电脑软件组件 ( 无论是否单独安装到电脑工作站或 WatchGuard 硬件产品或包括在 WatchGuard 硬件产品之内的组件 )、相关媒体、印制材料、在线或电子文档、该等文档的更新或修订版本 （ 包括从 WatchGuard LiveSecurity Service[ 或类似媒介 ] 获得的文档 ）( 以下统称为 “软件产品”）。 WatchGuard 同意授予你使用**软件产品**的许可，但前提是你必须接受本协议中的所有条款。请仔细阅读本协议。对**软件产品**的安装或使用将构成你已完全同意本协议条款的事实。如果你不同意本协议中的条款， WatchGuard 将不会许可你使用软件产品，而且你无权享有**软件产品**的任何权利。若发生上述情形，(1) 如果软件产品是与硬件产品一起认购的，则应立即将**软件产品**及硬件产品连同支付凭证归还从其处获得**软件产品**及硬件产品的授权经销商，以获得全额退款，或 （ 2 ）如果**软件产品**是单独认购的，则应立即将该**软件产品**的许可密钥连同支付凭证归还 (i) 你从其处获得**软件产品**的授权经销商，或归还 (ii)WatchGuard （ 如果是直接从 WatchGuard 认购 ），以获得全额退款。 WatchGuard 硬件产品认购受制于单独的协议以及包括在 WatchGuard 硬件产品包及 / 或有关的用户说明性文件中的有限硬件担保声明。

1. 所有权及许可。**软件产品**受各种版权法、国际版权条约以及其它知识产权法规及条约的保护。本协议是一份许可协议，而非销售协议。所有**软件产品** （ 包括但不限于置入**软件产品**的所有图象、照片、动画、视频、音频、音乐、文本及小程序 （ applet ））、附带印制材料以及软件产品拷贝件的所有权及版权均归 WatchGuard 或其许可方所有。本协议明确规定了你的**软件产品**使用权， WatchGuard 保留所有未在本协议中明确授予的其它权利。无论何种情形，均不构成 WatchGuard 对其在美国版权法或任何其它法律或条约中所享有权利的放弃。

2. 经许可的使用。你将被授予以下**软件产品**权利 :

(A) 你可以在任何单独场所中的单件 WatchGuard 硬件产品上安装并使用**软件产品**，也可以在多台工作站电脑中使用**软件产品**。

(B) 若同时在多件 WatchGuard 硬件产品中使用软件产品，你须必须为每一新增的 WatchGuard 硬件产品购买一份软件产品拷贝件。若你按照上句的要求为新增的 WatchGuard 硬件产品安装**软件产品**拷贝件，但没有安装包含在该 WatchGuard 硬件产品中的附加**软件产品**拷贝件，则你同意按照本协议的条款及条件使用与新增 WatchGuard 硬件产品一起提供的任何软件。如果需要在每一件新增的 WatchGuard 硬件产品中使用更新或修订版本的**软件产品**，你也必须继续保持从 WatchGuard LiveSecurity Service （ 或其同等机构 ）认购产品。

(C) 除了 2(A) 章节规定的拷贝件外，你可以拷贝一份**软件产品**，但仅可作为备份或存档而用。

3. 受禁使用。若无 WatchGuard 的明确书面许可，你不得 :

(A) 使用、拷贝、修改、合并或传输任何任何**软件产品**拷贝件或印制材料，但本协议另有规定的出外;

(B) 除原有软件产品出现损坏或缺失的情形之外，以其它任何目的使用或允许他人使用**软件产品**的任何备份或存档拷贝件;

(C) 转用、出借、租赁或出租软件产品;

(D) 将许可转让予任何第三方，但以下情形出外 :

(i) 永久性转让，

(ii) 第三方同意本协议的条款及条件，且

(iii) 你没有留存**软件产品**的任何拷贝件。

(E) 对**软件产品**进行逆向工程、拆卸或解码。

4. 有限保证。在你从 WatchGuard 或其授权经销商处获得**软件产品**之日起为期九十 （ 90 ）天内，WatchGuard 提供以下有限保证 :

(A) 媒体。在正常使用中，光盘及文档不会出现材料或工艺缺陷。如果光盘及文档与本保证不符，（ 作为你的唯一补救方案 ）你可以将有缺陷的光盘或文档退回 WatchGuard （ 必须带有认购日期凭证 ），免费取得替换品。

(B) 软件产品。**软件产品**将与随附的文档完全吻合。如果**软件产品**与本保证不一致，（ 作为你的唯一补救方案 ）你可以将所有的**软件产品**及文档连同认购日期凭证及问题说明文件退回给你从其处取得**软件产品**的经销商，由该经销商自行决定向你提供新版软件产品或全额退款。

**权利放弃**。以上第 4.4(A) 及 4(B) 章节中规定的 WatchGuard 保证、义务及责任以及你可享有的补救方法均为排他性保证、义务、责任及补救方法，而且将取代 WatchGuard 及其授权许可方的所有明示或暗示的其它保证、义务及责任以及所有其它你以合法形式或其它形式在出现**软件产品** （ 包括但不限于任何暗示的适销性保证以及产品适用于特定用途的保证、任何在履约过程、交易过程或商业使用过程中出现的暗示性保证、任何不侵权保证、任何有关本软件产品可以满足你的要求的保证、任何不中断或无错误运行保证、任何由于 WatchGuard 及其授权许可方的过失 [ 无论是主动或被动 ] 或失误侵权行为而引起的义务、责任、权利、索赔或补救要求**以及**任何针对本**软件产品**造成、引发或导致的损失而提起的义务、责任、权利、索赔或补救申诉 ）不合规或有缺陷时可从 WatchGuard 及其授权许可方取得的明示或暗示性权利、索赔及补救措施，同时也将构成你对上述保证、义务及责任以及权利、索赔及补救措施的放弃。

**责任范围**。 WatchGuard 应对**软件产品**担负的赔偿责任 （ 无论是在合同、民法或其它项下；也无论是否存在错误、过失、严格赔偿责任或产品责任约定 ）在任何情况下均不得超出你购买本产品的价款。即使未能执行约定的补救措施，上述赔偿责任范围也将有效。在任何情形下 （ 即使 WatchGuard 已获悉可能会出现下述损害 ）， WatchGuard 均不对任何与本保证或本软件产品的使用有关或相关的间接、特殊、偶发或后果性损害 （ 包括但不限于商业利润损失、商业中断或商业信息流失 ）向你或任何第三方 （ 无论是否涉及本协议或任何侵权行为 [ 包括被动、主动或转嫁的过失责任及严格赔偿责任及过失 ] ）负责。

5. 美国政府的有限权利。本**软件产品**与**有限权利**一起提供。美国政府或任何机构或其媒介在使用、复制或披露本**软件产品**时必须遵从 DFARS 252.227-7013 **技术、数据和计算机软件权利**条文中第 (c)(1)(ii) 小节或 （ 如果适用 ） 48 C.F.R. 52.227-19 **商业计算机软件 – 有限权利条文**第 (c)(1) 及 (2) 小节的限制。本**软件产品**由 WatchGuard Technologies, Inc. 制造 （ 营业地址：505 5th Ave. South, Suite 500, Seattle, WA 98104。）

6. 出口控制。你同意不将本**软件产品**直接或间接转让予任何《美国出口管理法》及其有关法规禁止向其转让本**软件产品**的国家。

7. 终止。如果你未能遵守本协议的规定、或销毁了你持有的所有本**软件产品**的拷贝件或自愿将本**软件产品**归还 WatchGuard，本许可以及你使用本**软件产品**的权利将自动终止。本协议终止后，你必须销毁所有本**软件产品**的拷贝件以及你所持有的所有相关文档。

8. 其它条款。本协议受华盛顿实体法管辖并由其释义 （ 但不包括《联合国国际货物销售合同公约 1980》）。本协议构成本**软件产品**双方之间的完整协议，而且将取代任何先前有关本**软件产品**的订单、通讯文件、广告或声明。你对本**软件产品**的使用将构成已认同本协议条款的事实。如果本**软件产品**的使用人是某一实体，则该实体的协议签署人必须保证及声明：（ A ）此人是代表该实体签署本协议的合法授权代表，且有权代表该实体接受本协议中的条款； (B) 该实体有绝对权利、法人资格或其它有关资质达成

本协议，并履行其在本协议项下的义务； (C) 本协议的达成及对本协议的履行不会侵犯与该实体存在和约关系的任何第三方的合法权益。未在制成书面文件后经 WatchGuard 签署，对本协议的任何改动均不生效。

版本 : 050309

## WatchGuard Technologies, Inc. 附加产品 / 服务客户协议 / 终端用户许可协议

重要提示：本附加产品 / 服务客户协议 / 终端用户许可协议 （ 本协议 ）是你 （ 客户 ）与 WatchGuard Technologies, Inc.（ WatchGuard ）之间达成的合法协议。如果需要认购下述 WatchGuard 附加产品 / 服务（ 附加产品 / 服务 ）或续订 / 升级你的附加产品 / 服务，你必须首选阅读本协议，并按照本协议的提示接受本协议的条款及条件。如果你不接受本协议的条款，我方将不受理你的认购、续订 / 升级请求，而且你无权获得附加产品 / 服务或你的续订 / 升级请求将被拒绝。如果你想拒绝本协议，你可以按照本协议有关章节的提示操作，拒绝接受本协议。如果你拒绝接受本协议，你的认购将不能完成。在此情况下，你应该将附加产品 / 服务的许可密钥 （ 定义如下 ）连同认购日期凭证退回至授权经销商，或退回至 WatchGuard （ 如果直接从 WatchGurad 购买 ），以获得全额价款补偿。

WatchGuard 与用户兹同意如下 :

1 **定义**。作为本协议的一方（ 客户 ），以下加黑条款的释义如下: “**附加产品 / 服务**是指 WatchGuard 向其购买同等产品 / 服务 （ 如果适用，也包括服务级别 ）的客户广泛提供的而且 WatchGuard 可随时对其进行修改的软件许可及可续订认购服务 （ 见 “许可密钥” ），该等许可及服务包括软件、威胁特征、信息或其它物件 / 服务的提供 / 取得。**软件**是指任何 WatchGuard 软件，具体包括电脑软件组件 （ 无论是否单独安装到某一计算机工作站或某一 WatchGuard 硬件产品或包括 / 预安装在 WatchGuard 硬件产品中 ）、相关媒介、印制材料、在线或电子文档、任何上述组件、媒介、印制材料及文档的更新程序或版本 （ 包括从 WatchGuard LiveSecurity Service 或同等来源接收到的产品 / 服务 ）以及附加产品 / 服务。**许可密钥**是指向客户提供的证明客户对附加产品 / 服务的认购、续订 / 升级 （ 若适用 ）的许可证密钥或其它书面或在线文档。**威胁特征**是指用于扫描及识别已知网络威胁的信息 （ 如：病毒特征、入侵防御特征 ）。”。

2 **附加产品 / 服务:** 在本协议有效期内，WatchGurad 将向客户提供**附加产品 / 服务**。客户必须同意: (i) 仅按照许可密钥明确规定 WatchGuard 产品数量使用一件 / 项**附加产品 / 服务** （ 以及所有与**附加产品 / 服务**相关的益处 ），而且为新增的将从**附加产品 / 服务**中受益的 WatchGuard 产品购买更多**附加产品 / 服务**； (ii) 仅按照许可密钥明确规定 WatchGuard 产品数量使用**附加产品 / 服务**的一款续订 / 升级版本（ 以及所有与**附加产品 / 服务**续订 / 升级版本相关的益处 ），而且为新增的将从**附加产品 / 服务**续订 / 升级版本中受益的 WatchGuard 产品购买更多续订 / 升级版本。

3 **附加产品/服务费**。客户将向WatchGuard支付适当的**附加产品/服务费**，并为所有购买的**附加产品/服务**的续订 / 升级版本支付适当的**附加产品 / 服务**续订 / 升级版本费， WatchGuard 可不时修改上述两项费用的具体金额。无论本协议是否在初定有效期或续订有效期到期前按照第下述第 6 节的规定提前终止，WatchGuard 均不会向客户退回**附加产品 / 服务**费及**附加产品 / 服务**续订 / 升级版本费。

4 **有效期**。除非按照第 5 节的规定延续有效期，或按照第 6 节的规定提前终止本协议，否则本协议的有效期 （ **“有效期”** ）自客户接受本协议并同意认购**附加产品 / 服务**及**附加产品 / 服务**续订 / 升级版本之日开始，至**许可密钥**中规定的到期日结束。 **WatchGuard Firebox 软件终端用户许可协议** （ 该等协议适用于所有下述与**附加产品 / 服务**相关的软件 ）的有效期应以各个终端用户许可协议中确定的有效期为准。

5 **续订**。WatchGuard 可不时制定不同的续订要求，当客户按照该等续订要求付款后，将获得与第 5 节规定续订服务同样有效的续订服务。无论是否存在上述条款，如果客户的 WatchGuard 产品已被停用，或 WatchGuard 不再提供相应的**附加产品 / 服务**， WatchGuard 将不再向客户提供续订服务。

6 **终止**。如果协议任何一方造成对本协议的实质性违反或未能在收到书面违约通知后十五 （ 15 ）天内弥补违约后果，则协议另一方有权终止本协议。如果用户未能缴纳任何到期费用，则 WatchGuard 有权立即终止本协议。

7 **软件许可**。用户明确同意严格按照 **WatchGuard Firebox 软件终端用户许可协议**、（ 若适用 ）与该等软件相关的 WatchGuard 软件终端用户许可协议的条款及条件以及本文用作参考的条款及条件，将附加产品 / 服务相关的所有软件作为 “软件产品” 使用。

8 **权利放弃**。免责声明。 WatchGuard 保证将按照本协议的所有要求，向客户提供**附加产品 / 服务**。WatchGuard 不作出其它任何形式的保证或担保，包括但不限于任何明示或暗示的适销性保证以及**附加产品 / 服务**适用于特定用途的保证，或作为部分**附加产品 / 服务**或与**附加产品 / 服务**一同提供的有关任何威胁特征、信息或其它物件 / 服务（或其更新版本）的准确性、可靠性或完整性的保证。WatchGuard 不对任何由于使用或信赖作为部分附加产品 / 服务或与**附加产品 / 服务**一同提供的**附加产品 / 服务**或任何威胁特征、信息或其它物件 / 服务而引起的损失负责。本段（第 8 段）中第一句的保证为排他性保证，并将取代 WatchGuard 的所有明示或暗示的其它保证、义务及责任以及所有其它你可以以合法形式或其它形式从 WatchGuard 取得的与**附加产品 / 服务**（包括但不限于任何暗示的适销性保证以及**附加产品 / 服务**适用于特定用途的保证、任何在履约过程、交易过程或商业使用过程中出现的暗示性保证、任何不侵权保证、任何有关**附加产品 / 服务**可以满足你的要求的保证、任何不中断或无错误运行保证、任何由于 WatchGuard 的过失 [ 无论是主动或被动 ] 或失误侵权行为而引起的义务、责任、权利、索赔或补救要求**以及**任何针对本软件产品造成、引发或导致的损失而提起的义务、责任、权利、索赔或补救申诉），或威胁特征、信息或其它物件 / 服务的准确性、可靠性及完整性有关的明示或暗示性权利、索赔及补救措施，同时也将构成你对上述保证、义务及责任以及权利、索赔及补救措施的放弃。一些司法管辖权不允许排除暗示性保证，因此不适用于客户。有限保证向客户提供特殊法律权利，而且客户也可以享有其它权利，该等权利随司法管辖权的不同而有所差异。

9 **责任范围**。WatchGuard 应对**附加产品 / 服务**担负的赔偿责任（无论是在合同、民法或其它项下；也无论是否存在错误、过失、严格赔偿责任或产品责任约定）在任何情况下均不得超出你购买**附加产品 / 服务**的价款。即使未能执行约定的补救措施，上述赔偿责任范围也将有效。在任何情形下（即使 WatchGuard 已获悉可能会出现下述损害），WatchGuard 及其供应商均不对任何与本保证或**附加产品 / 服务**的使用有关或相关的间接、特殊、偶发或后果性损害（包括但不限于商业利润损失、商业中断或商业信息流失）向你或任何第三方（无论是否涉及本协议或任何侵权行为 [ 包括被动、主动或转嫁的过失责任及严格赔偿责任及过失 ]）负责。某些司法不允许使用上述限定性或排他性条款，因此不适用于客户。

10 **权利保留**。WatchGuard 及其授权许可方兹保留其在作为部分**附加产品/服务**或与**附加产品/服务**一同提供的威胁特征、信息及其它物件 / 服务中的所有权以及其它一切权利，以及与该等威胁特征、信息及其它物件 / 服务相关的所有版权、商标权及其它专属权利。除非本协议另有明确规定或 WatchGuard 另有明确书面授权（包括出版 WatchGuard 有关根据 “公开来源” 许可而使用任何威胁特征的条款及条件），你不得复制、再版、张贴、传输或分发作为部分**附加产品 / 服务**提供的威胁特征、信息或其它物件 / 服务。

11 **完整协议**。本协议连同 WatchGuard 许可密钥、 WatchGuard Firebox 软件终端用户许可协议、任何随同**软件**授权客户使用的软件用户终端许可协议、以及任何客户与 WatchGuard 达成的在上述协议出现出现争议或不一致时应明确以其条款及条件为准的协议，将构成客户与 WatchGuard 之间的完整协议，并将取代先前或暂时性的与**附加产品 / 服务**有关的所有书面或口头陈述、声明及协议。如果客户已经购买了在附加 WatchGuard 产品中使**附加产品 / 服务**的权利，本协议将取代所有先前达成的适用于**本附加产品 / 服务**的用户协议 / 终端用户协议，而且客户在使用本**附加产品 / 服务**时均须以本协议的条款为准。对本协议的任何改动仅在协议双方签署书面文件后方可生效。

无论是否与法律原则存在冲突，本协议均受华盛顿法律管辖并由其释义。协议双方同意华盛顿国王郡（King County）的法院为本协议的唯一法院。未经 WatchGuard 事先书面同意，客户不得（通过法律操作或以其它方式）转让本协议。本协议对双方各自承继人或受让人均具有约束力，并将符合双方各自承继人或受让人的利益。若协议任何一方违反或未能履行本协议的任何规定或未能行使本协议项下的任何权利，均不应视作或解释为该方已放弃或愿意放弃履行上述规定或行使上述权利。若协议任何一方由于不可抗力原因（延迟或未能付款的原因除外）而延迟或未能履行其在本协议项下的义务，协议任何一方均不得将其视作违约。

如果你同意本协议的条款，请按照本协议相关章节提示的方式表示你已同意接受本协议。如果你不同意本协议的条款，请按照本协议相关章节提示的方式表示你拒绝接受本协议。你同意接受本协议后将构成以下陈述及保证：(A) 同意接受本协议的个人是代表客户签署本协议的合法授权代表，且有权代表客户接受本协议中的条款；(B) 客户有绝对权利、法人资格或其它有关资质达成本协议，并履行其在本协议项下的义务；(C) 本协议的达成及对本协议的履行不会侵犯与该客户存在和约关系的任何第三方的合法权益。

版本：050309

### 版权及商标权



### 专利

美国专利号：6,493,752 ； 6,597,661 ； 6,618,755 ； D473,879。其它专利待决。

# Licenses

Some components of the WatchGuard System Manager software distribute with source code covered under one or more third party or open source licenses. We include below the full text of the licenses as required by the terms of each license. To get the source code covered under these licenses, please contact WatchGuard Technical Support at:

- 877.232.3531 in the United States and Canada
- +1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

## SSL Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

### OpenSSL License

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”
THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### Original SSLeay License

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-2003 Eric Young (eay@cryptsoft.com)
All rights reserved.
This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes’ SSL.
This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).”

4. The names “mod_ssl” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called “mod_ssl” nor may “mod_ssl” appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).”

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Apache Software License, Version 2.0, January 2004

Some components of the WatchGuard System Manager software are distributed with a version of the Apache web server and other source code under the Apache software license.

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and
(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.
You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

## PCRE License

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. The PCRE is a library of

functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## GNU Lesser General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU Lesser General Public License (LGPL).

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the “Lesser” General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”). Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.
For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.
7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

## GNU General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU General Public License (GPL).

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Sleepycat License

Some components of the WatchGuard System Manager software are distributed with a version of the BerkeleyDB covered under the Sleepycat software license.

Copyright (c) 1990-2004

Sleepycat Software. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs.

THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1990, 1993, 1994, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1995, 1996

The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Sourcefire License

In addition to the copyright and license information found earlier in this Appendix, signature updates provided as part of the Gateway AV/IPS Subscription are subject to this license agreement:
SOURCEFIRE,INC.
VERSION 1.1.1
THE VRT CERTIFIED RULES ARE MADE AVAILABLE TO YOU BY SOURCEFIRE, INC. ("SOURCEFIRE") UNDER THE TERMS OF THIS VRT CERTIFIED RULES LICENSE AGREEMENT (THE "AGREEMENT"). BY CLICKING THE "ACCEPT" BUTTON BELOW, OR BY INSTALLING OR USING THE VRT CERTIFIED RULES, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT CLICK THE "ACCEPT" BUTTON, AND DO NOT INSTALL OR USE ANY PART OF THE VRT CERTIFIED RULES.
1. Definitions
1.1. "Commercial Purpose" means the use, reproduction or distribution of (i) the VRT Certified Rules or any Modification, or any portion of the foregoing, (ii) a Compilation that includes, in whole or in part, the VRT Certified Rules or any Modification that in either case is intended to result in a direct or indirect pecuniary gain or any other consideration or economic benefit to any person or entity involved in such use, reproduction or distribution. Examples of a Commercial Purpose, include without limitation, (v) integrating the VRT Certified Rules with other software or hardware for sale, (w) licensing the VRT Certified Rules for a fee, (x) using the VRT Certified Rules to provide a service to a third party, (y) selling the VRT Certified Rules, or (z) distributing the VRT Certified Rules for use with other products or other services.
1.2. "Compilation" means a work which combines the VRT Certified Rules or any Modification or portions thereof with any services, programs, code or other products not governed by the terms of this Agreement.
1.3. "Improvements" shall mean a Modification to a VRT Certified Rule (or to a modified VRT Certified Rule) that corrects a bug, defect, or error in such rule without affecting the overall functionality of such VRT Certified Rule (or Modification thereof).
1.4. "Modifications" means any alteration, addition to or deletion from the substance or structure of the VRT Certified Rules or any Modifications of such, including, without limitation, (a) any addition to or deletion from the contents of a file containing Original Code or previous Modifications of either; (b) any derivative of the VRT Certified Rule or of any Modification; or (c) any new file that contains any part of the VRT Certified Rule or Modifications.
1.5. "Permitted Use" shall have the meaning given such term in Section 2.1.
1.6. "Restricted Activities" shall have the meaning given such term in Section 2.1.
1.7. "Snort® Registered User" shall mean an individual who has registered or subscribed on www.snort.org to use the VRT Certified Rules.
1.8. "VRT Certified Rules" means those Snort® rules (in text form, source code form, object code form and all documentation related thereto) that have been created, developed, tested and officially approved by Sourcefire. These rules are designated with SIDs of 3465 - 1,000,000, except as otherwise noted in the license file.
1.9. "You" (or "your") means an individual exercising rights under this Agreement issued under Section 7. For legal entities, "you" includes any entity which controls, is controlled by, or is under common control with you or any such entity you are acting on behalf of. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than forty percent (40%) of the outstanding shares or beneficial ownership of such entity.
2. Sourcefire License Grant.
2.1. Grant of License; Permitted Use. Subject to the terms and conditions of this Agreement, Sourcefire hereby grants you a world-wide, non-exclusive license to do any of the following with respect to the VRT Certified

Rules: (a) use and deploy the VRT Certified Rules on management consoles and sensors that you manage (over which you have administrative control); (b) use and deploy the VRT Certified Rules on behalf of your employer on its internal management consoles and sensors (e.g., where a valid employer-employee relationship exists between you and a legal entity); (c) modify the VRT Certified Rules and use those Modifications consistent with paragraphs (a) and (b) above; (d) distribute those VRT Certified Rules and any Modifications generally available to Snort® Registered Users on a limited basis to other Snort® Registered Users; (e) distribute any Improvement generally available to Snort® Registered Users on mailing lists commonly used by the Snort® user community as a whole; (f) reproduce the VRT Certified Rules as strictly necessary in exercising your rights under this Section 2.1; and (g) Make the VRT Certified Rules (or any Modification) available to your or your employer's consultants, agents and subcontractors for the limited purpose of exercising your rights under this Section 2.1 provided that such use is in compliance with this Agreement. Paragraphs (a) through (g) are collectively referred to as the "Permitted Uses". All rights not granted under this Agreement are reserved by Sourcefire.

2.2. Limitations on License; Restricted Activities. You recognize and agree that the VRT Certified Rules are the property of Sourcefire, contain valuable assets and proprietary information and property of Sourcefire, and are provided to you under the terms and conditions of this Agreement. Notwithstanding anything to the contrary in this Agreement, You agree that you shall NOT do any of the following without Sourcefire's prior written consent: (a) use, deploy, perform, modify, license, display, reproduce or distribute the VRT Certified Rules or Modifications (even if merged with other materials as a Compilation) other than as allowed under a Permitted Use; (b) sell, license, transfer, rent, loan, use, modify, reproduce or disclose the VRT Certified Rules or any Modifications thereto (in whole or in part and whether done independently or as part of a Compilation) for a Commercial Purpose; (c) post or make generally available any VRT Certified Rule (in whole or in part or any Modifications thereto) to individuals or a group of individuals who have not agreed to the terms and conditions of this Agreement, provided, however, that nothing in this Section 2.2(c) shall preclude the Permitted Use in Section 2.1(e); (d) share any user authentication information and/or password provided to you by Sourcefire with any third party to allow such party access your snort.org account or to otherwise access the VRT Certified Rules; (e) alter or remove any copyright notice or proprietary legend contained in or on the VRT Certified Rules. Paragraphs (a) though (e) of this Section 2.2 are collectively referred to as the "Restricted Activities").

2.3. Reproduction Obligations. You agree that any embodiment of the VRT Certified Rules permitted under this Agreement will contain the notices set forth in Exhibit A. In addition, to the extent you make any copies of or distribute the VRT Certified Rules or any Modifications under this Agreement, you agree to ensure that any and all such copies of shall contain: (a) a copy of an appropriate copyright notice and all other applicable proprietary legends; (b) a disclaimer of any warranty consistent with this Agreement; and (c) any and all notices referencing this Agreement and absence of warranties.

3. Modifications; Derivative Works.

In the event you create a Modification, the use, reproduction and distribution of such Modifications shall be governed by the terms and conditions of this Agreement. Additionally, you hereby grant Sourcefire and any other licensee of the VRT Certified Rules an irrevocable, perpetual, fully paid-up, world-wide, royalty-free, non-exclusive license to use, reproduce, modify, display, perform and distribute such Modifications (and the source code thereto), provided, however, that you and any recipient of such Modifications must include: (a) the original copyright notice and all other applicable proprietary legends; (b) the original warranty disclaimer; (c) the original notices referencing this Agreement and absence of warranties; and (d) a prominent notice stating that you changed the VRT Certified Rulese (or any Modification thereto) and the date of any change.

4. Distribution Obligations.

4.1. General. The source code version of the VRT Certified Rules (or any Modification thereof) may be distributed only under the terms of this Agreement, and you must include a copy of this Agreement with every copy of the VRT Certified Rules you distribute.

4.2. Required Notices. You must duplicate the notice in Exhibit A in each file of the source code. If it is not possible to put such notice in a particular source code file due to its structure, then you must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If you created one or more Modification(s) you may add your name as a contributor to the notice described in Exhibit A. You must also duplicate this Agreement in any documentation for the source code where you describe recipients' rights or ownership rights relating to the VRT Certified Rules. To the extent you offer additional warranty, support, indemnity or liability obligations, you may do so only on your own behalf, and not on behalf of

Sourcefire. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by you alone, and you hereby agree to indemnify and hold Sourcefire harmless for any liability incurred by Sourcefire as a result of any warranty, support, indemnity or liability terms you offer.

5. Inability to Comply Due to Statute or Regulation.

If it is impossible for you to comply with any of the terms of this Agreement with respect to some or all of the Original Code due to statute, judicial order, or regulation then you must: (a) comply with the terms of this Agreement to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

6. Application of this Agreement.

This Agreement also applies to code to which Sourcefire has attached the notice in Exhibit A and to related Modifications created in Section 3.

7. Versions of the Agreement.

7.1. New Versions. Sourcefire may publish revised and/or new versions of the Agreement from time to time. Each version will be given a distinguishing version number.

7.2. Effect of New Versions. Once VRT Certified Rules has been published under a particular version of the Agreement, you may always continue to use it under the terms of that version. You may also choose to use such VRT Certified Rules under the terms of any subsequent version of the Agreement published by Sourcefire. No one other than Sourcefire has the right to modify the terms applicable to Original Code.

8. DISCLAIMER OF WARRANTY.

THE VRT CERTIFIED RULES AND MODIFICATIONS ARE PROVIDED UNDER THIS AGREEMENT ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE VRT CERTIFIED RULES OR THE MODIFICATIONS ARE FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE VRT CERTIFIED RULES AND MODIFICATIONS IS WITH YOU. SHOULD ANY VRT CERTIFIED RULES OR MODIFICATIONS PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT SOURCEFIRE) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT. NO USE OF ANY VRT CERTIFIED RULE OR ANY MODIFICATION IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

9. Termination.

9.1. This Agreement and the rights granted hereunder will terminate automatically if you fail to comply with any or all of the terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the VRT Certified Rules which are properly granted shall survive any termination of this Agreement. Provisions which, by their nature, must remain in effect beyond the termination of this Agreement shall survive.

10. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU OR SOURCEFIRE BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, SECURITY BREACHES OR FAILURES, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATIONS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

11. License Compliance.

You may be requested by Sourcefire to provide a certificate, signed by your authorized representative, that you are using the VRT Certified Rules consistent with a Permitted Use. In the event your use of the VRT Certified

Rules is not in compliance with a Permitted Use, or if you otherwise violate the terms of this Agreement, Sourcefire may, since remedies at law may be inadequate, in addition to its other remedies: (a) demand return of the VRT Certified Rules; (b) forbid and enjoin your further use of the VRT Certified Rules; (c) assess you a use fee appropriate to your actual use of the VRT Certified Rules.

12. United States Government Users.

If the VRT Certified Rules or Modifications are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in the VRT Certified Rules and Modifications shall be subject to Sourcefire's standard commercial terms and only as set forth in this Agreement; and only with "Limited Rights" and "Restricted Rights" as defined the federal regulations if the commercial terms are deemed not to apply.

13. Miscellaneous.

This Agreement represents the complete agreement concerning subject matter hereof. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This Agreement shall be governed by Maryland law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. Any litigation relating to this Agreement shall be subject to the jurisdiction of the state and Federal Courts serving Greenbelt, Maryland, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. You hereby submit to jurisdiction and venue in such courts. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this Agreement. Headings and section references are used for reference only and shall not be used to define, limit or describe such section.

EXHIBIT A - VRT Certified Rules License Agreement

The contents of this file are subject to the VRT Certified Rules License Agreement 1.1 (the "Agreement"). You may not use this file except in compliance with the Agreement. You may obtain a copy of the Agreement here. Software distributed under the Agreement is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the Agreement for the specific language governing rights and limitations under the Agreement. The developer of the VRT Certified Rules is Sourcefire, Inc., a Delaware Corporation.

## Expat-MIT HTML Parser Toolkit License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Curl Software MIT-X License



**Note**

# 附件 B WatchGuard 文件位置

本附件向你介绍由 WSM 软件保存的公用数据文件的位置。由于我们可以对 Windows 操作系统（OS）进行配置，将该等目录文件保存于不同的磁盘驱动器，因此你必须根据你电脑上的 Windows 配置，了解该等文件的准确位置。

你可以对日志文件进行配置，将其保存到不同于其它安装文件的目录下。如果你改动了日志文件的默认位置，该等默认位置将不再适用。

如果你使用的是非英语版本的操作系统，你必须转换目录名称（如：“Documents and Settings”或 “Program Files”），使其匹配你的操作系统语言。

| 文件类型 | 位置 |
|---|---|
| 用户创建数据 | My Documents\My WatchGuard（用户创建的数据包括 Firebox 配置文件、许可文件以及证书等。很多情况下， WSM 软件在 My WatchGuard 文件夹中创建子文件夹，用于保存该等文件。） |
| 用户创建数据（共享） | C:\Documents and Settings\All Users\Shared WatchGuard |
| Firebox® 配置文件 | My Documents\My WatchGuard\configs |
| Firebox 日志文件 | C:\Documents and Settings\WatchGuard\logs |
| 报表文件 | C:\Documents and Settings\WatchGuard\reports |
| 证书 | My Documents\My WatchGuard |
| WatchGuard® 应用程序 | C:\Program Files\WatchGuard\wsm8 |
| 共享应用程序库 | C:\Program Files\Common Files\WatchGuard\wsm8 |
| 管理服务器数据 | C:\Documents and Settings\WatchGuard\wmserver |
| 认证中心数据 | C:\Documents and Settings\WatchGuard\wmserver\wgca |
| WebBlocker 服务器数据 | C:\Documents and Settings\WatchGuard\wbserver |
| 后期产品更新图象 | C:\Program Files\Common Files\WatchGuard\resources |
| 帮助文件（Fireware） | C:\Program Files\WatchGuard\wsm8\help |
| 帮助文件 (WFS) | C:\Program Files\WatchGuard\wsm8\wfs\help |

# 默认文件位置

下列表格介绍 WatchGuard 软件应用程序及服务器在寻找其数据文件或用户创建数据文件（如 Firebox 配置文件）的默认位置。在某些情况下，该等默认位置将随着软件应用程序打开某一类似文件的具体位置而改变。在此情况下，软件应用程序将记忆上次读 / 写类似文件的位置，并优选该位置。

由于我们可以对 Windows 操作系统（OS）进行配置，将该等目录文件保存于不同的磁盘驱动器，因此你必须根据你电脑上的 Windows 配置，确定该等文件的准确位置。

你可以对日志文件进行配置，将其保存到不同于其它安装文件的目录下。如果你改动了日志文件的默认位置，该等默认位置将不再适用。

如果你使用的是非英语版本的操作系统，你必须转换目录名称（如：“Documents and Settings”或 “Program Files”），使其匹配你的操作系统语言。

**Fireware 应用软件策略管理器**

| 操作 | 文件类型 | 默认位置 |
|---|---|---|
| 读 / 写 | Firebox 备份文件 | C:\Documents and Settings\All Users\Shared WatchGuard\backups |
| 读取 | 产品升级图象 | C:\Program Files\Common Files\WatchGuard\Resources\Fireware |
| 读取 | 受禁网站 | My Documents\My WatchGuard |
| 读取 | 受禁网站例外 | My Documents\My WatchGuard |
| 读 / 写 | Firebox 配置文件 | My Documents\My WatchGuard\configs |
| 读 / 写 | Firebox 许可文件 | My Documents\My WatchGuard\configs |
| 读取 | 初始许可导入 | My Documents\My WatchGuard |
| 写入 | MUVPN .wgx 文件 | C:\Documents and Settings\All Users\Shared WatchGuard\muvpn |

### Fireware 应用软件策略管理器

| 操作 | 文件类型 | 默认位置 |
|---|---|---|
| 读取 | 日志通知 | Current working directory |
| 读取 | 垃圾邮件规则导入 | Current working directory |
| 写入 | 保存的备份文件 | C:\Documents and Settings\All Users\Shared WatchGuard\backups |
| 写入 | MUVPN SPDs (.wgx) | C:\Documents and Settings\All Users\Shared WatchGuard\muvpn |
| 读取 | 受禁网站导入 | Current working directory |

### WFS 应用软件闪盘（Flash Disk）管理

| 操作 | 文件类型 | 默认位置 |
|---|---|---|
| 读 / 写 | 备份图象 | C:\Documents and Settings\All Users\Shared WatchGuard\backups |

### 历史报告

| 操作 | 文件类型 | 默认位置 |
|---|---|---|
| 读 / 写 | 报表定义 | C:\Documents and Settings\WatchGuard\report-defs |
| 读 / 写 | 汇报图 | C:\Program Files\WatchGuard\wsm8\reports\graphics\<report .jpg/.gif files> |

# 附件 C 策略类型

本章节介绍与 Fireware® 应用软件一起提供的预定义政策、其协议以及端口。本文也介绍可能对某些政策的安全性造成影响的特殊情形。

在本章节中，政策被分为两组 – 受数据包过滤器控制的政策及受代理协议控制的政策。

## 数据包过滤政策

数据包过滤器用于检查每一数据包的源头及目标站。过滤器将根据的数据包的来源及目标地址是否可信，选择允许或拒绝该数据包。

### 所有政策

如果仅选用 Any（所有）策略，你将允许两个指定受信 IP 或网络地址之间的数据流自由通行。Any（所有）政策将在 Firebox® 中开启一个 “空洞”，让指定主机间的数据流自由通过。我们建议仅为一条 VPN 中的数据流启用 Any（所有）策略。

Any（所有）政策与其它政策不同。例如，如果你仅允许通往某一指定主机的 FTP，则所有通往其它主机的 FTP 会话（sessions）将被该政策拒绝（除非你也配置了其它 FTP 政策）。 Any（所有）政策与其它政策不同，不会产生拒绝行为。

除非在 **From** 或 **To** 列表中使用了制定的 IP 地址、网络地址、主机别名、组名、或用户名，否则你也不能使用 Any（所有）策略。

#### 特征

- 互联网协议：所有协议
- 端口号：所有端口

## AOL

AOL （ 美国在线 ）专用协议允许通过 TCP/IP 网络访问 AOL。 AOL 用户必须在经过特殊配置后使用 TCP/IP，而非调制解调器。

### 特征

- 互联网协议：TCP
- 端口号：5190

## archie

archie 是用于查找 FTP 服务器中文件的搜索协议。我们建议你为 archie 提供可取得的 web 接口。你可以从：
ftp://microlib.cc.utexas.edu/microlib/mac/info/archie-servers.txt
匿名 FTP 获得 archie 服务器当前列表。外部主机可能会被欺骗。 Firebox 可能无法确定这些数据包是否来自正确的位置。在来访 archie 连接被拒绝后，你可以通过配置 Firebox，将源 IP 地址添加到受禁网站列表中。 archie 同样适用于所有常用日志选项。

### 特征

- 互联网协议：UDP
- 端口号：1525

## auth

服务器坚定协议 （ AUTH ）目前又名标识协议 （ IDENT ）。有关此政策的详细信息请参阅 IDENT。

## BGP

边界网关协议 （ BGP ）是广泛应用于大多数因特网的路由协议。 BGP 是一项高度可配置协议，可将冗余添加到来自及通往各个局域网的链接。我们建议你仅在你已经在 Fireware 配置的动态路由协议中启用并配置了 BGP 的情况下，使用此服务。

### 特征

- 因特网协议：TCP 或 UDP
- 端口号：179

## Citrix

Citrix 或独立计算体系结构 ( ICA ) 是由 Citrix 软件应用程序 ( 如 Winframe 及 Metaframe Presentation Server （ MPS ）) 使用的一种应用协议。Winframe 从不同类型的客户端 （ 使用 TCP 端口 1494 ）提供访问 Windows 电脑的权限。 Citrix MPS 3.0 用户使用在 TCP 端口 2598 上带有 Session Reliability 的 ICA。如果你使用 Citrix MPS，你必须为 TCP 端口 2598 添加一项自定义政策。添加 Citrix 政策之后，你的网络安全可能会承担一定风险，因为该协议允许远程用户在未经验证的情况下通过防火墙访问你的电脑。可对 Winframe 或 MPS 造成威胁的入侵包括各种拒绝服务式攻击。我们建议你通过设定 VPN 选项为 ICA 连接提供更多的安全保障。 Winframe 同样适用于所有常用日志选项。

### 特征

- 互联网协议：TCP
- 端口号：1494

有关添加 Citrix ICA 政策的详细信息，请参阅 Knowledge Base （知识库）中的 Advanced FAQs （常见高级问题）。请访问 www.watchguard.com/support 并登陆 LiveSecurity Service。

## Clarent 网关

Clarent 公司向主流通讯公司及服务提供商提供 IP 电话技术服务。 Clarent 产品允许在因特网上的 Clarent 网关之间进行 IP 语音传输。此政策支持 Clarent v3.0 或后期产品。

Clarent 产品使用两套端口，一套服务于网关对网关通讯（UDP 端口 4040、4045 及 5010），另一套服务于网关对命令中心通讯（UDP 端口 5001 及 5002）。将 Clarent 命令政策应用到于网关对命令中心通讯。

仅允许从指定外部网关到你的网关或命令中心的入站连接。

Clarent 也支持 PCAnywhere 管理功能。详情请参阅 PCAnywhere 政策注释。

由于 Clarent 网关政策仅根据网络地址判断是否允许数据流进入防火墙，因此使用 Clarent 网关政策将给你的网络安全带来一定风险，故而不能将其用作完全可信的验证方法。此外，在此配置下，你的 Clarent 服务器可能会接收拒绝服务式攻击。若有可能，我们建议你通过设定 VPN 选项，增强 Clarent 网关连接的安全性。

### 特征

- 互联网协议：UDP
- 端口号：4040、 4045、 5010

## Clarent 命令

Clarent 公司向主流通讯公司及服务提供商提供 IP 电话技术服务。 Clarent 产品允许在因特网上的 Clarent 网关之间进行 IP 语音传输。此政策支持 Clarent v3.0 或后期产品。

Clarent 产品使用两套端口，一套服务于网关对网关通讯（UDP 端口 4040、4045 及 5010），另一套服务于网关对命令中心通讯（UDP 端口 5001 及 5002）。将 Clarent 命令政策应用到于网关对命令中心通讯。

仅允许从指定外部网关到你的网关或命令中心的入站连接。

Clarent 也支持 PCAnywhere 管理功能。详情请参阅 PCAnywhere 政策注释。

由于 Clarent 命令政策仅根据网络地址判断是否允许数据流进入防火墙，因此使用 Clarent 网关政策将给你的网络安全带来一定风险，故而不能将其用作完全可信的验证方法。此外，在此配置下，你的 Clarent 服务器可能会接收拒绝服务式攻击。若有可能，我们建议你通过设定 VPN 选项，增强 Clarent 命令连接的安全性。

### 特征

- 互联网协议：UDP
- 端口号：5001、 5002

## CU–SeeMe

CU-SeeMe是一款用于通过因特网进行视频会议的软件应用程序。要保证CU-SeeMe能通过Firebox正常运行，你必须确定你所处的网络未使用外发动态 NAT。为来访及向外连接配置 CU-SeeMe 政策。

CU–SeeMe 协议允许你为来访及向外连接配置此政策。通过使用正确的端口，CU–SeeMe 协议允许你使用 CU-SeeMe 2.X 及 3.X 版本。 CU-SeeMe2.X 版本适用于 UDP 端口 7648 而 CU-SeeMe 3.X 版本适用于 UDP 端口 7648、 UDP 端口 24032 （供 H.323 会议使用）及 TCP 端口 7648 （视频会议目录文件）。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：UDP 7648、 UDP 24032、 TCP 7648

## DHCP 服务器或 DHCP 客户端

动态主机配置协议 （DHCP）可以向某一网络中的各个设备分配动态 IP 地址。

### 特征

- 互联网协议 （2）：TCP
- DHCP 服务器端口号：68
- DHCP 客户端端口号：67

## DNS

域名服务 （DNS）可以使主机名称与 IP 地址匹配。 DNS 政策在默认的配置中启用。 DNS 政策允许 UDP DNS 数据流以及 TCP 区域传输按照指定的方式进行。 DNS 适用于所有常用日志选项。

### 特征

- 互联网协议：TCP （适用于服务器 – 服务器传输）及 UDP （适用于客户端 – 服务器查询）
- 端口号：TCP 53 及 UDP 53

## Entrust

Entrust Authority Public Key（Entrust 权限公共密钥）应用协议可以将公共密钥传递给受信任的第三方组织，供验证使用。

### 特征

- 互联网协议：TCP
- 端口号：709、 710

## finger

finger 是一项用于在某一指定主机上获取用户信息的应用协议。黑客们很容易使用此信息做出对你不利的行为。我们不建议你在受信接口上安放 finger 服务器。

### 特征

- 互联网协议：TCP
- 端口号：79

## FTP

文件传输协议（FTP）用于在因特网上传输文件。 FTP 数据包过滤器不适用于为任何数据流设置的 FTP 代理协议规则。要对 FTP 数据流进行代理协议配置，请使用 FTP 代理政策。我们建议你仅允许在 Firebox 后部的公共 FTP 服务器中使用 FTP。

外部主机可能会被欺骗。 Firebox 可能无法确定这些数据包是否来自正确的位置。在来访 archie 连接被拒绝后，你可以通过配置 Firebox，将源 IP 地址添加到受禁网站列表中。包含在 WSM 中的数据包过滤器及代理政策可以处理被动及主动性会话（sessions）的数据隧道。 FTP 适用于所有常用日志选项。

### 特征

- 互联网协议：TCP
- 端口号：FTP 使用两款端口：供控制连接使用的 TCP 20 及供数据传输使用的 TCP 21。随客户端配置的不同， TCP 21 可以成为来访或外发连接。如果是来访连接， 21 为源端口，而目标端口将随机选定。

## Gopher

Gopher 是明尼苏达大学（University of Minnesota）开发的一种数据检索协议。由于大多数用户都使用 HTML，因此 Gopher 的使用率较低。

### 特征

- 互联网协议：TCP
- 端口号：70，但是可以对服务器进行配置，使其适用于其它端口

## GRE

一般性路由封装协议（GRE）一般与点对点隧道协议（PPTP）连同使用，用于在各个客户端之间或客户端与服务器之间创建虚拟专用网络（VPN）。

### 特征

- 互联网协议：GRE
- 协议号：47

## HTTP

HTTP 数据包过滤器不会将已设置的 HTTP 代理规则应用到任何数据流中。要对 HTTP 数据流进行代理协议配置，请使用 HTTP 代理政策。我们建议你仅允许在 Firebox 后部的公共 HTTP 服务器中使用 HTTP。

外部主机可能会被欺骗。 Firebox 可能无法确定这些数据包是否来自正确的位置。在来访 HTTP 连接被拒绝后，你可以通过配置 Firebox，将源 IP 地址添加到受禁网站列表中。 HTTP 适用于所有常用日志选项。

### 特征

- 互联网协议：TCP
- 端口号：80

## HTTPS

HTTPS 是 HTTP 协议的安全及加密版本。该客户端及 web 服务器将在 TCP 端口 443 上建立加密的会话（session）。由于此 session 已被加密，因此系统无法使用一项代理协议检查数据包的内容。此政策使用数据包过滤器检查该连接。

### 特征

- 互联网协议：TCP
- 端口号：443

## HBCI

家庭银行计算机接口 （HBCI）是为银行客户及金融产品制造商制定的一项标准。

### 特征

- 互联网协议：TCP
- 端口号：3000

## IDENT

识别协议（IDENT）是用于使 TCP 连接与某一用户名相匹配的一种协议。使用 IDENT 频率最高的是大型公众 SMTP 及 FTP 服务器。 IDENT 可被用于日志记录，但是由于黑客可以通过修改他们的服务器让该等服务器发回不正确信息，因此你不能信任 IDENT 提供的信息。 IDENT 使用 “虚假” 信息来掩藏内部用户信息。

当你使用 SMTP 及来访静态 NAT 时，你必须将 IDENT 添加到你的策略管理器中。对 IDENT 进行配置，使其允许通往 Firebox 的数据流。此操作将使邮件消息能够从 Firebox 后台区流向许多（使用 IDENT 识别其它邮件服务器身份的）因特网 SMTP 服务器，并将允许这些服务器通过 Firebox 将消息退回到其发件人。

如果你没有使用动态 NAT，应允许 IDENT 应用到你的电子邮件服务器中。
尽管黑客可以使用 IDENT 收集用户名称，但我们仍推荐将 IDENT 政策设置为允许进 / 出 Firebox。

#### 特征

- 互联网协议：TCP
- 端口号：113

### IGMP

因特网组管理协议（IGMP）是一套因特网 IP 多点传输标准，用于控制单一网络上多点传输群组中的主机成员关系。

#### 特征

- 互联网协议：IGMP

### IKE

因特网密钥交换协议是为密钥管理制定的一套标准协议。

#### 特征

- 互联网协议：UDP
- 端口号：4500 及 500。 UDP 4500 仅用于 NAT 穿越。

### IMAP

因特网邮件访问协议（IMAP）是一种从远程电子邮件服务器取得电子邮件或布告栏消息的应用层协议。你可以在许多位置（如家庭、工作地点或笔记本电脑）访问储存于 IMAP 服务器的电子邮件，而无需移动消息。

#### 特征

- 互联网协议：TCP
- 端口号：143

### IPSec

安全因特网协议（IPSec）是一套网络安全或网络通讯数据包层协议的框架。它是一种带加密功能的 VPN 隧道协议。

#### 特征

- 互联网协议：UDP、封装安全载荷（ESP）及验证头（AH）
- 端口号：UDP 500 及 UDP 4500

## IRC

因特网中继交谈（IRC）是一种因特网在线交谈系统。要使用 IRC，你必须取得 IRC 客户端及因特网接入条件。 IRC 客户端是你电脑上的一个软件应用程序，用于向 IRC 服务器发送消息或从 IRC 服务器接收消息。 IRC 服务器会确定将所有消息发送到聊天会话中的所有用户。

### 特征

- 互联网协议：TCP
- 端口号：6667

## Intel Video Phone

Intel Video Phone 是一种基于 H.323 的实时多媒体应用程序。H.323 是为 TCP/IP 网络在线会议制定的一款国际标准。此政策不会过滤危险内容，也不支持 QoS 或 rsvp 协议。此外，此政策也不支持 NAT。

### 特征

- 互联网协议：TCP
- 端口号：1720、 522

## Kerberos V 4 及 Kerberos V 5

Kerberos 网络认证协议是一款由麻省理工学院（MIT）开发的认证系统。通过使用安全认证，Kerberos 可以让两台电脑在开放式网络中交换保密信息。

### 特征

- 互联网协议：TCP 及 UDP
- Kerberos v 4 端口号：UDP 750
- Kerberos v 5 端口号：TCP 88 及 UDP 88

## L2TP

第二层隧道协议（L2TP）是 PPP 协议的扩充版本， L2TP 可以让 ISPs 在虚拟专用网络中运行。

### 特征

- 互联网协议：UDP
- 端口号：1701

## LDAP

轻型目录访问协议（LDAP）是为使用在线目录服务提供的一款开放式标准协议。可与因特网传送协议（如 TCP 等）一起使用此协议。你可以使用 LDAP 访问独立于操作系统的目录服务器或 X.500 目录文件。

### 特征

- 互联网协议：TCP
- 端口号：389

## LDAP–SSL

TLS/SSL 上的轻型目录访问协议（LDAP-SSL）适用于 Windows2000，可在你访问 Active Directory（活动目录）时提供更多安全保障。

### 特征

- 互联网协议：TCP
- 端口号：636

## Lotus Notes

Lotus Notes 是一个在线会谈、数据库及电子邮件客户端 / 服务器平台。Lotus Notes 也用于创建及使用文件。此政策可以启用专有 Lotus Notes 协议。由于该协议使用封装及隧道并向内部数据提供访问权限，因此我们不建议受信网络以外的地址使用 Lotus Notes 政策。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 1352、 UDP 1352

## MSSQL– 监视器

Microsoft SQL 监视器用于坚实 Microsoft SQL 数据库。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 1434、 UDP 1434

## MSSQL– 服务器

Microsoft SQL 服务器通常用于建立与 Microsoft SQL 数据库的远程连接。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 1433、 UDP 1433

## MS Win Media

Microsoft Windows Media 服务器是 Microsoft 开发的用于提供单点数据流的一款专有协议，该协议可以激活使用户能够向前、向后或停止回访单点传输数据流的双向连接。

### 特征

- 互联网协议：TCP
- 端口号：1755,80

## NetMeeting

NetMeeting 是 Microsoft 公司开发的能够使用户组在因特网上召开电话会议的一款产品。该产品包括在 Microsoft 的 Internet Explorer 网络浏览器之内。此政策基于 H.323 协议，不会过滤危险内容，也不支持 QoS 或 rsvp 协议。此外，此政策也不支持 NAT。

### 特征

- 互联网协议：TCP
- 端口号：1720,389

## NFS

网络文件系统（NFS）协议是 Sun Microsystems 开发的一款客户端服务器软件应用程序。 NFS 允许所有网络用户访问储存在不同类型电脑上的共享文件。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 2049、 UDP2049

## NNTP

网络新闻传输协议（NNTP）用于传输 Usenet （世界性的新闻组网络系统）新闻稿件。

使用 NNTP 的最佳方法是将内部主机设为内部新闻服务器，而将外部主机设为新闻输送服务器（news feeds）。大多数情况下，必须双向启用 NNTP。如果你运行的是公众新闻输送服务器，你必须允许所有外部主机进行 NNTP 连接。 WatchGuard 不能确定此等数据包是否来自正确的位置。

当某一来访 NNTP 连接造拒绝后，你可以通过配置 Firebox，将源 IP 地址添加到受禁网站列表。NNTP 适用于所有常用日志选项。

### 特征

- 互联网协议：TCP
- 端口号：119

## NTP

网络时间协议（NTP）是一款可控制本地计时的基于 TCP/IP 的协议。它可以将你的电脑时钟调整到与因特网其它电脑时钟同步。

### 特征

- 互联网协议：UDP 及 TCP

- 端口号：TCP 123 及 UDP 123

## OSPF

优先开放最短路径（OSPF）是为 IP 网络开发的一款基于链路状态运算法则的路由协议。由于 OSPF 提供幅度更小、频率更高的路由表更新，使网络更加稳定，因此正在快速取代 RIP 在因特网中的应用。

### 特征

- 互联网协议：OSPF
- 协议号：89

## pcAnywhere

pcAnywhere 是一款用于与 Windows 电脑建立远程连接的软件应用程序。要激活此协议，请添加 PCAnywhere 政策。然后，允许因特网上必须访问内部 pcAnywhere 服务器的主机访问内部 pcAnywhere 服务器。

由于 pcAnywhere 允许数据流在不受验证的情况下通过防火墙，因此 pcAnywhere 政策并不十分安全，可能使你的网络安全承担一定风险。此外，你的 pcAnywhere 服务器可能接收各种拒绝服务式攻击。我们建议你通过设定 VPN 选项为你的网络提供更多的安全保障。

### 特征

- 互联网协议：UDP 及 TCP
- 端口号：UDP 22、 UDP 5632、 TCP 5631、 TCP 65301

## ping

你可以使用 ping 确定是否能够找到某一主机，并确定该主机是否仍在网络中运行。要寻找基于 DOS 或基于 Windows 的路由追踪数据包，请配置 ping 政策。

外发 ping 是排除故障的有效工具。我们不建议你启用访问你受信网络的 ping 连接。

### 特征

- 互联网协议：ICMP
- 协议号：1

## POP2 及 POP3

POP2 及 POP3（邮局协议）是一款通常用于从 POP 服务器取得用户电子邮件的电子邮件传输协议。

### 特征

- 互联网协议：TCP
- 端口号：109（POP2）及 110（POP3）

## PPTP

PPTP 是带加密功能的 VPN 隧道协议。PPTP 使用一个 TCP 端口（供协商及验证 VPN 连接使用）以及一项 IP 协议（供数据传输使用）在 VPN 中连接两台伙伴设备。对 PPTP 政策进行配置，使其允许从因特网主机到因特网网络 PPTP 服务器的访问连接。由于 NAT 不能转发 IP 协议，因此 PPTP 不能访问主机的静态 NAT。由于此政策将激活 PPTP 服务器的一条隧道，而 Firebox 无法在隧道中检查数据包，因此必须对此政策的使用加以控制。请确定使用的是最新版本的 PPTP。

### 特征

- 互联网协议：TCP
- PPTP 协商端口：1723

## RADIUS 及 RADIUS–RFC

拨入用户远程认证服务（RADIUS）可以让远程用户安全访问公司网络。 RADIUS 是在所有服务器均可取得的中心用户数据库中为用户、远程访问服务器及 VPN 网关保存验证信息的客户端服务器系统。对网络的认证仅在一处位置进行。 RADIUS 使用验证密钥，该验证密钥可以识别访问 RADIUS 客户端的验证请求。

在 RFC 2865 中， RADIUS 使用的服务器端口将从端口 1645 变为 1812。请确定你所选的政策与你的设备相匹配。

### 特征

- 互联网协议：UDP
- RADIUS 政策端口号：UDP 1645
- RADIUS-RFC 政策端口号：UDP 1812

## RADIUS–Accounting 及 RADIUS–ACCT–RFC

拨入用户远程认证服务（RADIUS） Accounting（帐目管理）政策向网络（该网络使用 RADIUS 验证）管理员提供帐目管理信息。 RADIUS 是在所有服务器均可取得的中心用户数据库中为用户、远程访问服务器及 VPN 网关保存验证信息的客户端服务器系统。在经验证的会话（session）开始或停止时， RADIUS 服务器也将得到通知。此信息有益于帐户管理。

在 RFC 2866 中， RADIUS 使用的服务器端口将从端口 1646 变为 1813。请确定你所选的政策与你的设备相匹配。

### 特征

- 互联网协议：TCP
- RADIUS 帐户管理政策端口号：UDP 1646
- RADIUS-ACCT 政策端口号：UDP 1813

## RDP

Microsoft 远程桌面协议（RDP）为服务器上运行的 Windows 软件应用程序提供通过网络连接实现的远程显示及输入功能。

### 特征

- 互联网协议：TCP
- 端口号：3389

## RIP

路由信息协议（RIP）是路由产生早期开发的一款链接状态路由协议。RIP 的有限性使其不合适因特网应用，但 RIP 是小型网络的不错选择。我们建议你在使用此服务时首先在 Fireware 配置的动态路由程序中激活并配置 RIP。

### 特征

- 互联网协议 UDP
- 端口号：520

## RSH

远程 Shell（RSH）用于访问远程主机电脑的命令行。由于 RSH 未被加密，因此我们建议你在未使用 VPN 时不要允许任何 RSH 通过 Firebox 来访。

### 特征

- 互联网协议：TCP
- 端口号：514

## RealPlayer G2

媒体串流协议 v7 及 v8。

### 特征

- 互联网协议：TCP
- 端口号：554,80

## Rlogin

远程登陆（Rlogin）是一种 UNIX 命令，该命令允许经批准的用户登陆到网络中的其它 UNIX 电脑。登陆后，用户可以进行主机准许的所有操作，如读取、编辑或删除文件。由于 Rlogin 未被加密，因此我们建议你不要允许来访 Rlogin 通过 Firebox。

### 特征

- 互联网协议：TCP
- 端口号：513

## SecurID

RSA SecurID 双因素认证为用户验证流程提供更多安全保障。SecurID 由 Security Dynamics Technologies, Inc. 开发，可以使用 SecurID 令牌（ tokens ）生成代码及 ACE/ 服务器软件，对代码进行确认。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 5510、 UDP 5500

## SMB （ Windows 网络连接服务 ）

Windows 使用服务器信息块（ SMB ）共享文件、电脑、打印机及其它网络资源。

如果你设置了复制功能（ replication ），你可以查看许多要求在端口 135 上使用端口映射器服务的请求。如果此端口不能使用， SMB 将开始使用端口 42。详情请参阅供 DCE-RFC 以及 DCE-RPC 代理协议章节。

**注释**

通过 Firebox 的 SMB 并不安全，因此除非是使用了 VPN 连接，否则我们不建议你使用 SMB。应仅在无其它可选解决方案时使用这些配置选项，并在政策设置中指定内部及外部主机。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：UDP 137、 UDP 138、 TCP 139、 TCP 445、 UDP 445

## SMTP

SMTP 数据包过滤政策允许 SMTP 数据流（ 电子邮件 ）通过，而无需使用 SMTP 代理协议。

### 特征

- 互联网协议：TCP
- 端口号：25

## SNMP

简单网络管理协议（ SNMP ）用于收集远程电脑的信息，并对其进行配置。 SNMP 存在风险。许多因特网攻击均使用 SNMP。由于 SNMP 在被激活后，可能会修改某一网络，因此你应该仔细检查各个可选项以及所有连接的记录日志。

### 特征

- 互联网协议：UDP
- 端口号：161

## SNMP–Trap

简单网络管理协议（SNMP）捕获器（traps）是 SNMP 代理器（如：路由器）向网络管理站发送的通知消息。这些消息一般用来汇报必须进行检查的重要事件。

### 特征

- 互联网协议：UDP
- 端口号：162

## SQL*Net

Oracle 为其 SQL*Net 软件提供一个端口。此端口的默认值为 1526/tcp 或端口 1521/tcp。或者，将 tnsnames.ora 文件修改为端口。要允许 SQL*Net 通过 Firebox，请使用 tcp 协议以及 ignore 客户端端口为 SQL*Net 服务器使用的端口安装一项政策。然后对从允许外部主机到 SQL*Net 服务器的来访连接进行设置。

### 特征

- 互联网协议：TCP
- 端口号：1521、 1526

## SQL 服务器

SQL 服务器用于访问 Sybase Central 以及 SQL Advantage 软件。

### 特征

- 互联网协议：TCP
- 端口号：10000

## ssh

安全 Shell（ssh）是一款允许远程登陆、命令控制及电脑之间文件传移的免费应用程序协议。 ssh 提供强大的认证功能及安全（加密）连接。由于 ssh 比 telnet、 rssh 及 rlogin 等协议更加安全，因此我们推荐使用 ssh。

你可以从 www.ssh.com 取得 UNIX 的各种版本，并可以在 F-Secure (http://www.f-secure.com) 查看 Windows 可使用的各种 UNIX 版本信息。

### 特征

- 互联网协议：TCP
- 端口号：22

## Sun RPC

Sun 远程过程调用（Sun RPC）是 Sun Microsystems 为 Sun 网络文件系统中客户端及服务器之间的连接开发的一款协议。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 111 及 UDP 111

## syslog

syslog 是一款用于在 UNIX 主机上记录操作系统事件的政策。syslog 数据通常在防火墙中激活，用于从防火墙外部的主机收集数据。

在默认的 Firebox 配置中， syslog 端口的状态为禁用。要允许一台日志主机收集多台 Firebox 的日志数据，你需要：

- 从 Blocked List （受禁端口）列表中删去端口 514；
- 将 WatchGuard 日志政策添加到 Policy Manager （策略管理器）

**注释**

允许 syslog 数据流通过 Firebox 通常并不是安全举措。黑客有可能用日志条目充塞 syslogs。如果 syslog 已满， syslog 将更加难以检测出网络攻击。此外，磁盘经常会被数据充满，无法有效记录网络攻击。

### 特征

- 互联网协议：UDP
- 端口号：514

## TACACS

TACACS 用户认证是使用用户账户对用户进行验证，让其进入拨号上网调制解调器池的一套系统。TACACS 无需在 UNIX 系统上保存账户拷贝件。 TACACS 不支持 TACACS+ 或 RADIUS。

### 特征

- 互联网协议：UDP
- 端口号：49

## TACACS+

TACACS+ 用户认证是使用用户账户对用户进行验证，让其进入拨号上网调制解调器池的一套系统。TACACS+ 无需在 UNIX 系统上保存账户拷贝件。 TACACS+ 支持 RADIUS。

### 特征

- 互联网协议：TCP
- 端口号：49

## TCP

此政策充当所有 TCP 连接的默认政策，而且其它政策可以覆盖 TCP 政策。除非 TCP-UDP、 TCP 或 TCP 政策也在 Policy Manager （ 策略管理器 ）中实现相应配置，否则与 Policy Manager （ 策略管理器 ）中指定政策不符的 TCP 连接不会成功实现。由于 FTP 仅适用于 FTP 政策，因此，此政策不会激活 FTP。

## TCP–UDP

此政策充当所有 TCP 及 UDP 连接的默认政策，而且其它政策可以覆盖 TCP 政策。除非 TCP-UDP、UDP 或 TCP 政策也在 Policy Manager（策略管理器）中实现相应配置，否则与 Policy Manager（策略管理器）中指定政策不符的 TCP-UDP 连接不会成功实现。由于主动模式 FTP 仅适用于 FTP 政策，因此，此政策不会激活主动模式 FTP。

## UDP

此政策充当所有 UDP 连接的默认政策，而且其它政策可以覆盖 TCP 政策。除非 UDP、TCP-UDP 或 TCP 政策也在 Policy Manager （ 策略管理器 ）中实现相应配置，否则与 Policy Manager （ 策略管理器 ）中指定政策不符的 TCP-UDP 连接不会成功实现。

## telnet

telnet 政策用于登陆到远程电脑。其效用几乎与拨号访问一样，但 telnet 连接在整个网络中进行。

### 特征

- 互联网协议：TCP
- 端口号：23

## Timbuktu

Timbuktu是一款用于访问Windows电脑的远程控制及文件传输软件。该协议使用TCP端口1417以及UDP 端口 407。添加 Timbuktu 政策并允许因特网上必须访问内部 Timbuktu 服务器的主机访问内部 Timbuktu 服务器。

由于 Timbuktu 允许数据流在不受验证的情况下通过防火墙，因此 Timbuktu 政策并不十分安全，可能使你的网络安全承担一定风险。此外，你的 Timbuktu 服务器可能接收各种拒绝服务式攻击。我们建议你通过设定 VPN 选项为你的网络提供更多的安全保障。

### 特征

- 互联网协议：TCP、 UDP
- 端口号：UDP 407、 TCP 1417

## Time

Time 政策几乎与 NTP 相同，用于实现你的电脑时钟与网络上其它主机时钟的同步。与 NTP 相比，Time 在广域网 （ WAN ）中通常没有 NTP 准确及有效。

### 特征

- 互联网协议：TCP、UDP
- 端口号：TCP 37、 UDP 37

## traceroute

traceroute 是一款可以创建网络地图（ maps ）的软件应用程序，用于排除网络故障、消除网络路由故障以及查看网站的因特网服务提供商。 WatchGuard traceroute 政策仅控制基于 UNIX 及基于 UDP 方式的 traceroute。如果是基于 DOS 或基于 Windows 的 traceroute 数据包过滤器，请使用 ping 政策（ 请参阅第 42 页的 “*ping*”）。

traceroute 使用 ICMP 及 UDP 数据包创建网络路径，并使用 UDPTTL 字段从原点与目标点之间的每一路由器及电脑上发送后数据包（ back packets ）。如果你允许 traceroute 进入某一网络，可能会让黑客乘机生成一份你的专用网络地图。但是，外发 traceroute 有利于排除网络故障。

### 特征

- 互联网协议：UDP
- 端口号：33401-65535

## UUCP

UNIX 至 UNIX 拷贝（ UUCP ）是一款可以让一台电脑向另一台电脑发送文件的 Unix 工具及协议。由于用户经常使用 FTP、 SMTP 及 NNTP 传输文件，因此用户对该工具的使用并不频繁。

### 特征

- 互联网协议：TCP
- 端口号：540

## WAIS

广域信息服务（ WAIS ）是一款可以帮助你在因特网上找到文件的协议。 WAIS 最初由 Thinking Machines Incorporated 开发。一些网站用 WAIS 查找可搜索目录，但是 WAIS 的使用频率并不高。WAIS 是在 ANSI Z39.50 搜索协议基础上创建的，因此 239.50 及 WAIS 是指同一技术。

### 特征

- 互联网协议：TCP
- 端口号：210，但是与 HTTP 服务器非常相似，服务器可以在（ 而且经常在 ）其它端口配置。

## WinFrame

Citrix ICA 是 Citrix 为其软件应用程序（ 包括 Winframe 产品 ）使用的一款协议。Winframe 允许从不同类型的客户端访问 Windows。 Citrix 为其 ICA 协议使用 TCP 端 1494。在默认状态下， Citrix 使用的是 Session Reliability, 会将 ICA 协议改变为使用 TCP 2598。如果你使用 Citrix MPS，你必须为 TCP 端口 2598 添加一项政策。

由于 WinFrame 允许数据流在不受验证的情况下通过防火墙，因此 WinFrame 政策并不十分安全，可能使你的网络安全承担一定风险。此外，你的 WinFrame 服务器可能接收各种拒绝服务式攻击。我们建议你通过设定 VPN 选项为 CIA 连接提供更多的安全保障。 WinFrame 适用于所有常用日志选择。

### 特征

- 互联网协议：TCP
- 端口号：1494

## WG-Auth

WatchGuard® 认证政策允许用户通过认证进入 Firebox。

### 特征

- 互联网协议：TCP
- 端口号：4100

## WG-Firebox-Mgmt

WatchGuard Firebox 管理政策允许客户自定义配置，并允许监控各种 Firebox 连接。我们建议你仅允许管理站使用此政策。此政策通常安装在受信接口上。

### 特征

- 互联网协议：TCP
- 端口号：4103、 4105、 4117、 4118

## WG-Logging

WatchGuard 日志政策仅在辅助 Firebox 必须访问一台 Firebox 受信接口上的日志主机时方有使用的必要。如果仅有一台 Firebox，则无必要使用此证。

### 特征

- 互联网协议：TCP
- 端口号：4107、 4115

## WG-Mgmt-Server

当你使用 WatchGuard 管理服务器安装向导配置一台管理服务器时，向导会自动将此政策添加到网关 Firebox。此政策将控制通往管理服务器的来访连接。

### 特征

- 互联网协议：TCP
- 端口号：4110、 4112、 4113

## WG–SmallOffice–Mgmt

WatchGuard 小型办公室管理政策允许你从 WatchGuard 系统管理器建立一条到 SOHO 及各个 Edge Firebox 的安全连接。

### 特征

- 互联网网协议：TCP
- 端口号：TCP 4109

## WG–WebBlocker

WatchGuard WebBlocker™ 政策允许通向 WebBlocker 服务器的各种连接。

### 特征

- 互联网协议：TCP、 UDP
- 端口号：TCP 5003、 UDP 5003

## WHOIS

WHOIS 政策提供有关网站及网络管理员的信息，通常用于查找不同网站的管理员。要过滤 WHOIS 数据流，请添加一项允许连接到 WHOIS 服务器的 WHOIS 政策（如 :rs.internic.net）。

### 特征

- 互联网协议：TCP
- 端口号：43

## X11

X Windows 系统协议带有各种用于创建图形桌面的组件（包括窗口、颜色、画面及界面）。X11 也提供用户与电脑输入设备（如：鼠标、键盘等等）之间的连续互动事件记录。

### 特征

- 互联网协议：TCP
- 端口号：6000-6063

## Yahoo Messenger

Yahoo Messenger 协议是一种即时通信工具。

### 特征

- 互联网协议：TCP
- 端口号：5050,80

# 被代理政策

本章节回顾由 WatchGuard Firebox 系统提供的被代理政策。代理政策可以打开数据包，去除数据包内容中的受禁数据类型，并使用代理协议的源头及目标站重新组装该数据包。
配置及激活代理协议的方式与你添加数据包过滤政策的方式一样。

## DNS

域名服务（DNS）可以使主机名称与 IP 地址匹配。 DNS 代理政策将检查 DNS 数据包的内容，使你的网络免收黑客侵扰。它可以对在 DNS 查询中允许的操作类型加以限制，并在查询名称中寻找指定模式。

### 特征

- 互联网协议：TCP 及 UDP
- 端口号：TCP 53 及 UDP 53

## FTP

FTP 是指文件传输协议，用于在因特网上移传各种文件。

### 特征

- 互联网协议：TCP
- 端口号：20（命令隧道）、 21（数据隧道）

## HTTP

**HTTP 是指全球网络（WorldWide Web）用来在因特网上传输 / 交换信息的安全超文本传输协议。**

**注释**

WatchGuard 政策“HTTP 代理”与 HTTP 缓存代理（caching proxy）不同。HTTP 缓存代理控制的是 Web 数据的缓存。如果你使用外部缓存代理，你必须（通过添加政策）允许使用所有你公司所必须的外发政策。如果设置为不允许，外发 TCP 连接将不会正确运行。

### 特征

- 互联网协议：TCP
- 端口号：80（但服务器可以在任何端口上运行；常见的选择是 8080 ；安全套接层 [SSL] 连接通常在端口 443 上进行）

## SMTP

简单邮件传输协议（SMTP）是用于传输及接收电子邮件的因特网标准协议。 SMTP 服务器通常为公众服务器。
当你使用来访静态 NAT 及 SMTP 时（见第 32 页 “auth”），你必须将一项 auth 政策添加到策略管理器中。对 auth 进行配置，使其允许来访 auth 进入 Firebox。此操作将使外发邮件消息能够从

Firebox 后台流向因特网上使用 auth 的多台 SMTP 服务器。SMTP 允许这些服务器通过 Firebox 将消息发回发件人。

我们推荐你启用来访 SMTP 记录功能，但是此功能可能导致大量的日志数据。要在不使用 SMTP 代理的情况下让 SMTP 正常运作，你需要在策略管理器中创建一项使用 TCP 协议及端口 25 的新政策。

### 特征

- 互联网协议：TCP
- 端口号：25

## TCP 代理

TCP 代理政策在端口 80 上为 HTTP 提供配置选项，并添加一条规则，该规则在默认状态下允许从 Firebox 后台网络到 Firebox 外部网络的 TCP 连接。TCP 代理规则将确定所有源自 Firebox（所有端口）后台的 HTTP 数据流均被 HTTP 代理规则所代理。

我们建议你仅将 Firebox 后台的公众 HTTP 服务器配置为允许 HTTP。外部主机可能会被欺骗。WatchGuard 可能无法确定这些数据包是否来自正确的位置。

在通向 Firebox 后台主机的 HTTP 连接造到拒绝后，你可以通过配置 WatchGuard，将源 IP 地址添加到受禁网站列表中。按照与你配置 HTTP 代理一样的方式配置参数及 MIME 类型。

# 索引

## 符号



## 数字



## A

# B

# C

# D

# E

# F

# G



# H

# I

# K



# L

# M

# N

# O



# P

# Q



# R

# S

# T

# U



# V

# W

# X



# Y