卓豪（北京）技术有限公司

Firewall Analyzer 快速用户手册

Firewall Analyzer 用户快速使用指南

技术支持部

本文档旨在帮助用户快速熟悉产品使用的方法。

目录

简介

Firewall Analyzer 是基于 Web 的防火墙/VPN/代理服务器的日志分析解决方 案，它内置 Syslog 服务器来存储、分析日志并生成报表。防火墙分析仪提供防火墙流量、安全违反以及其它情况的日报、周报、月报以及年报。有助于网络管理员在网络威胁发生之前，主动地管理网络安全，以防止网络滥用。同时可有效地管理带宽需求、监视 Web 站点访问，确保员工适当地使用网络。

Firewall Analyzer 的功能：

1. 容量规划（带宽是否起到了有效的作用）
2. 故障诊断（在网络中，哪些链路和主机出现异常）
3. 流量分析（带宽流量趋势）
4. 日志分析

系统安装

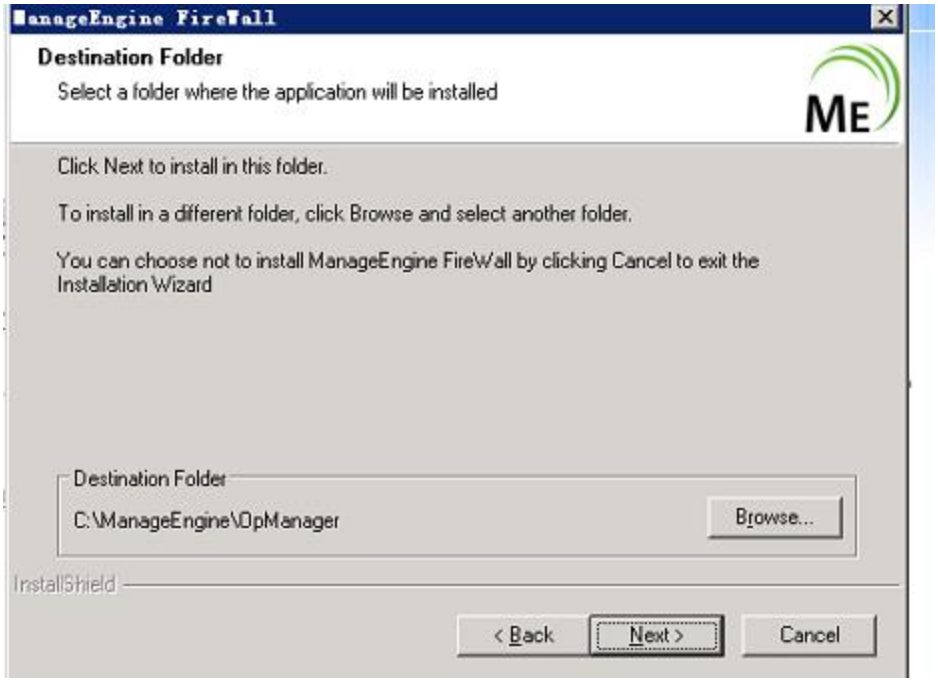
1. 最小系统要求
   - 2.80 GHz, 64-bit (x64) Xeon® 处理器或同级别的其它处理器
   - 4 GB RAM
   - 50 GB 硬盘空间
2. 下载安装包（推荐使用 Windows64 位系统）

   下载的安装路径：

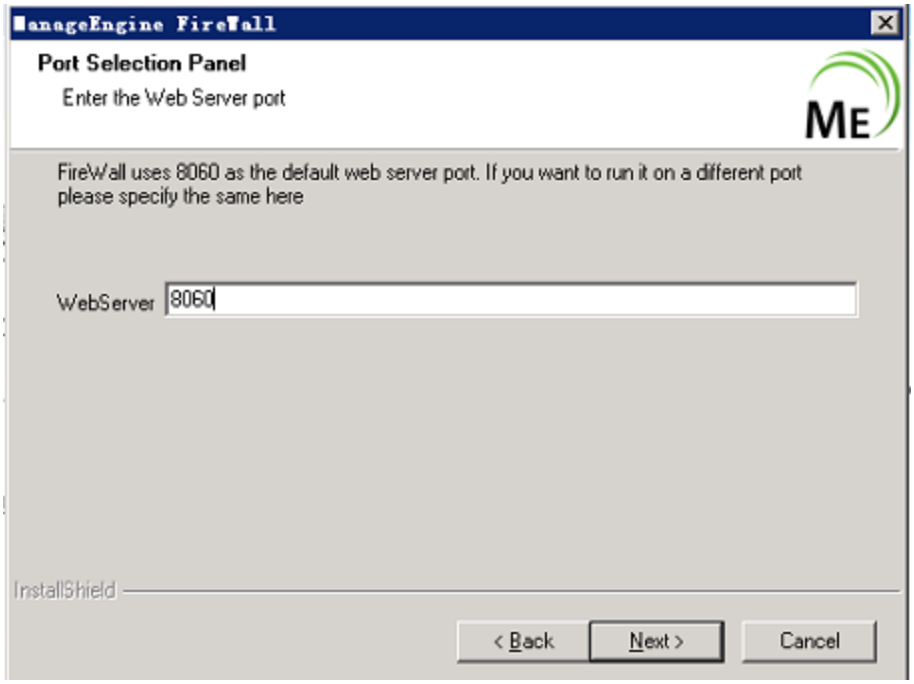
   https://www.manageengine.cn/products/firewall/download.html
3. 安装的关键步骤

   Windows：

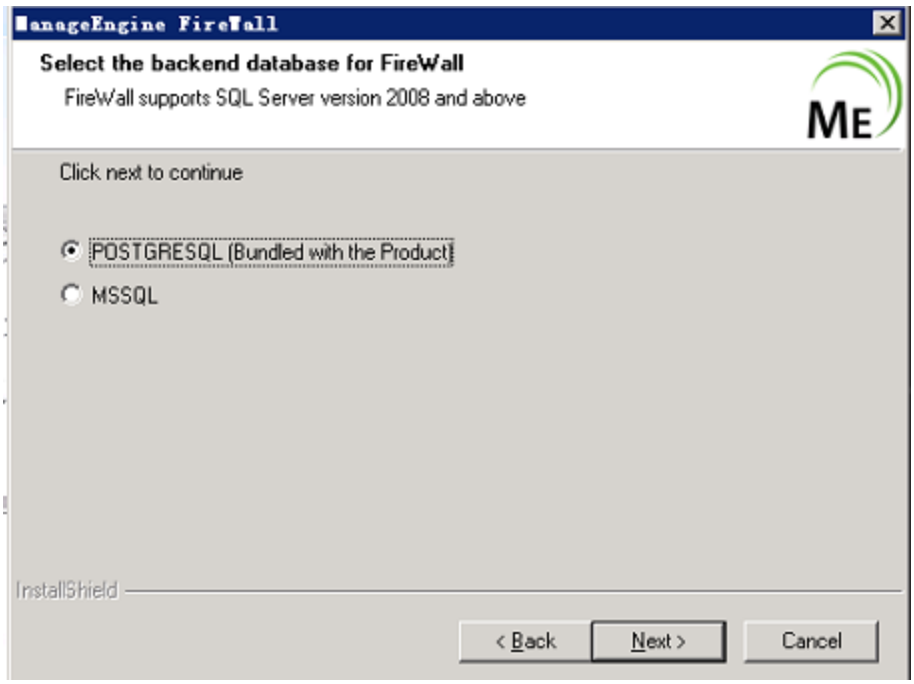
   1) 选择安装路径



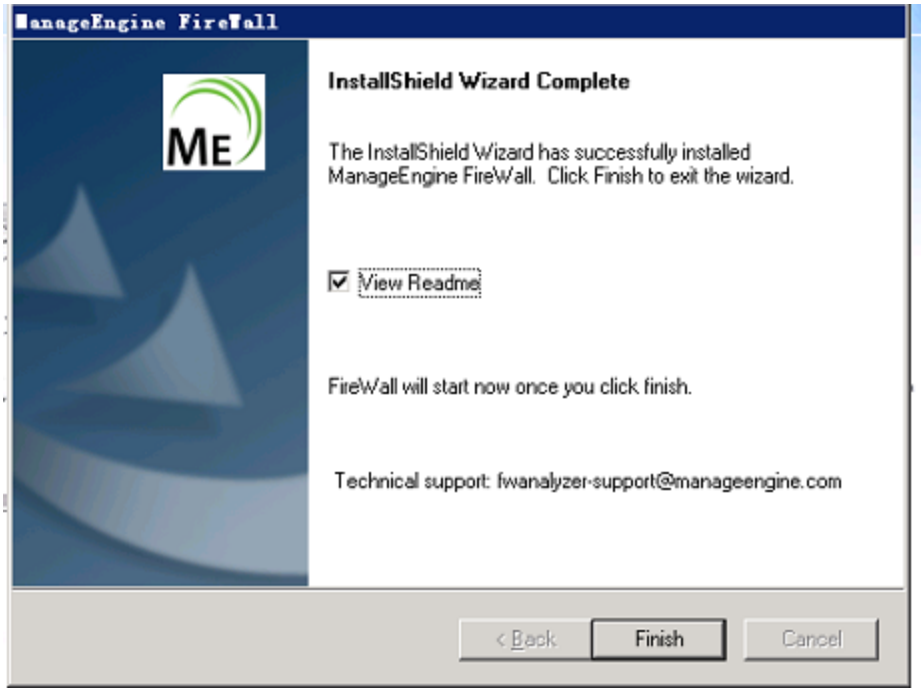
   2) 选择端口号 (其 Web 服务器的端口号)。



3) 选择数据库。可以选择该产品内置的 PostgreSQL 数据库，或者您环境中的微软 SQL Server 数据库。



4) 安装完成。点击完成按钮后将开始启动该产品。首次启动花费时间稍长，完全启动大约需要 5 分钟。



Linux：

1) 使用命令执行以下操作

   chmod a+x ManageEngine_FirewallAnalyzer_64bit.bin

2) 执行以下操作进行安装（如果没有图形界面，请在命令后面加上--console）

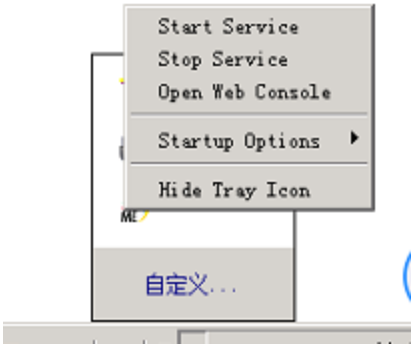
   ./ ManageEngine_FirewallAnalyzer_64bit .bin

3) 按照向导提示，进行一步一步安装。

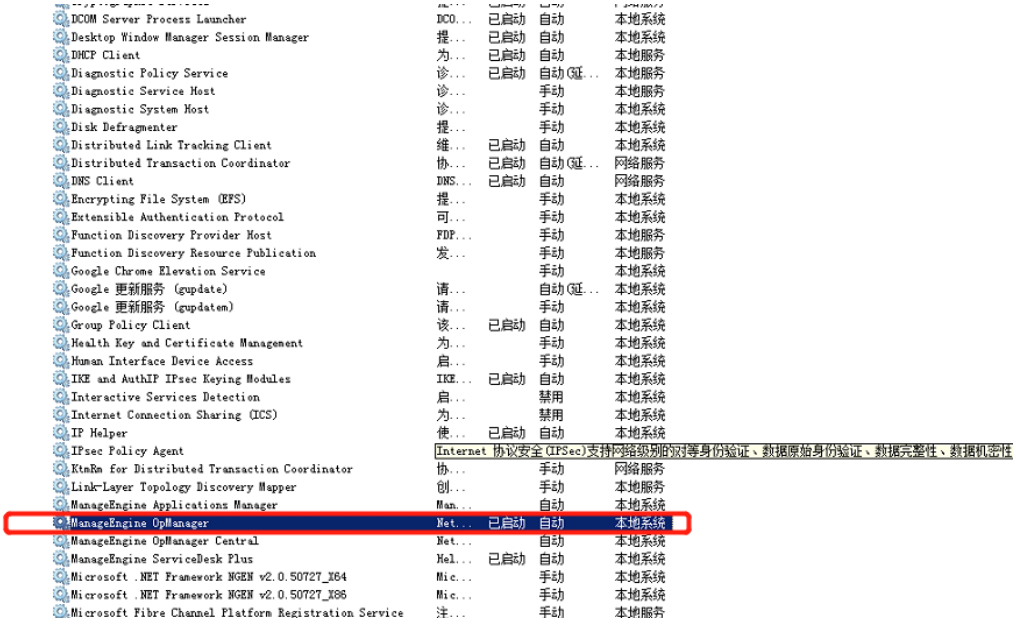
启动 Firewall Analyzer

可以通过如下方式之一启动：

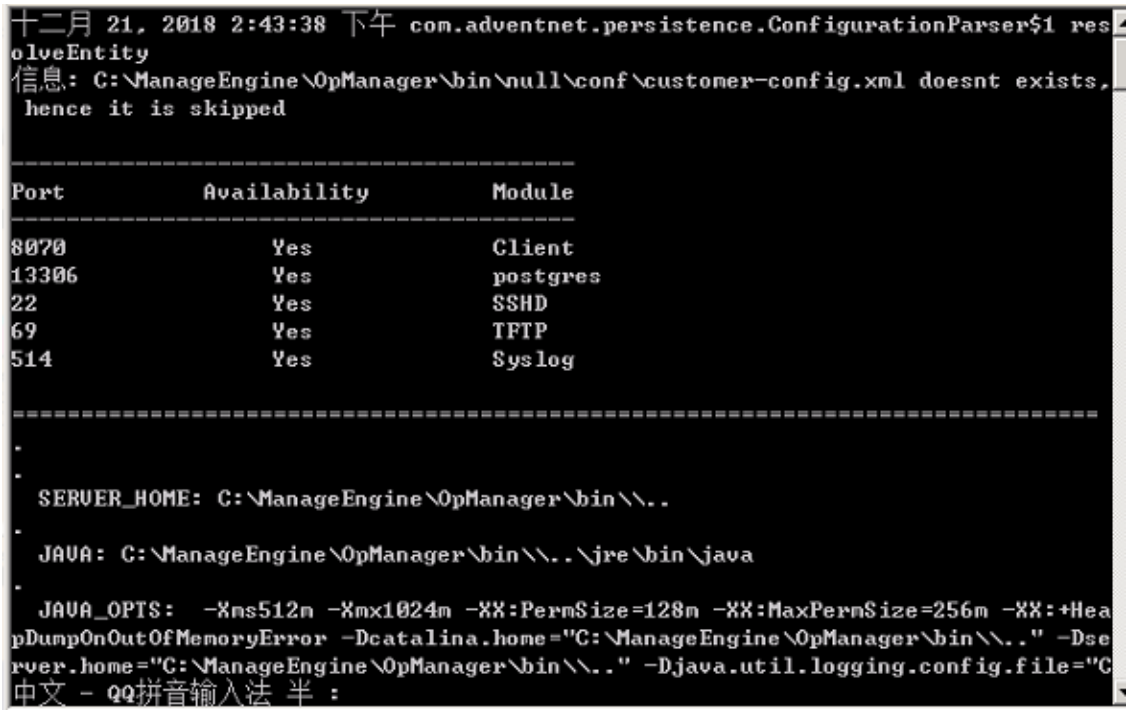
1. 桌面图标启动：双击桌面上的 Firewall Analyzer 图标启动；



2. 服务启动：打开 windows 的服务，在服务列表中找到 ManageEngine Opmanager 服务，打开其属性并点击‘启动’；



3. 进入到 Firewall Analyzer 的安装根目录，进入 bin 文件夹，双击 run.bat 或者通过命令提示符运行 run.bat：

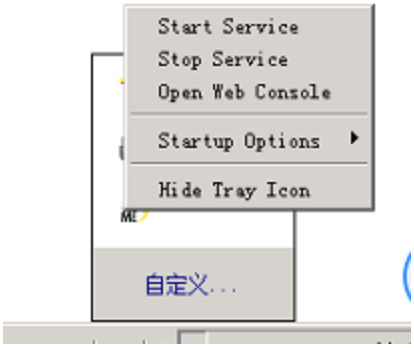


如果采用第三种方式启动，该命令窗口则保持当前状态，如果该窗口被关闭或者用户使用 ctrl+c 来中断操作，那么 Firewall Analyzer 会自动关闭。

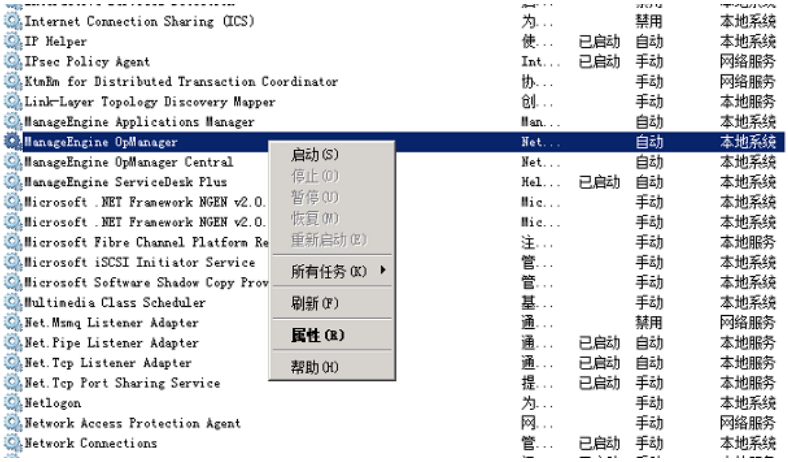
关闭 Firewall Analyzer

可以通过如下方式关闭：

1. 右击系统托盘中的 Firewall Analyzer 图标，在弹出的选项中选择“Stop Service”



2. 打开 windows 系统的服务列表，关闭 Firewall Analyzer 的服务；



登录 Firewall Analyzer

在启动完成后用户便可以访问客户端登录 Firewall Analyzer。Firewall Analyzer 基于 B/S 架构开发，所以支持基于 WEB 页面的访问，所以用户可以打开浏览器，在地址栏中输入：

http://server:port

来访问 Firewall Analyzer 的客户端，其中链接中的‘server’是指 Firewall Analyzer 所安装的服务器的 DNS 名称或者 IP 地址，端口就是在安装的过程中配置的 web 端口，比方说 Firewall Analyzer 服务器的 DNS 名称叫 fwaserver，IP 地址为 192.168.1.12，web 端口使用的是 8060，那么我们可以通过访问

http://fwaserver:8060

或者

http://192.168.1.12:8060

来访问 Firewall Analyzer 的客户端。当然，如果用户在 Firewall Analyzer 服务器上访问 Firewall Analyzer 的客户端，可以使用:

http://localhost:8060

来进行访问。

如何添加设备

防火墙分析仪监听 UDP 端口(默认 1514)以接收 syslog。当 Firewall Analyzer 收到来自设备的日志后将开始分析日志并把对应设备自动添加到资源清单中。所以安装并启动该产品后，要在设备上配置 syslog 输出。Firewall Analyzer 支持的 syslog 和配置方式如下：

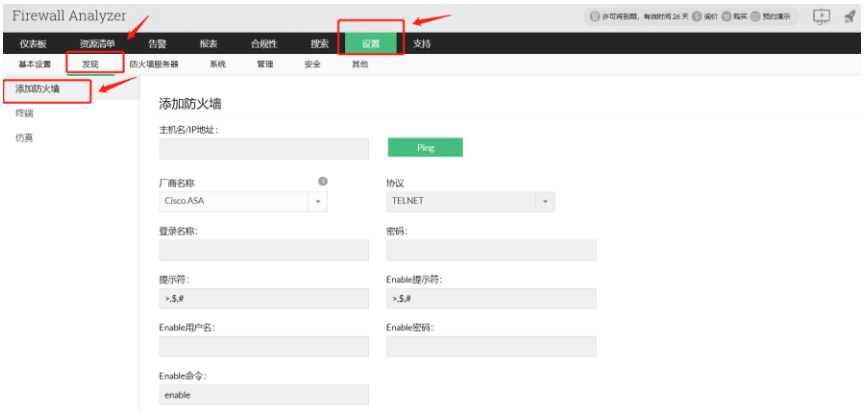
配置防火墙：
https://www.manageengine.cn/products/firewall/help/configure-firewall/configure-firewall.html

配置代理服务器：
https://www.manageengine.cn/products/firewall/help/configure-proxy-server/configure-proxy-server.html

1. 发现设备

   除了按照上面的说明手动配置防火墙日志的输出，还可以通过 Firewall Analyzer 来上传命令。操作步骤如下：

   1) 点击设置--->点击发现--->添加防火墙
   2) 填写主机名或 ip 地址--->选择厂商--->选择协议（ssh 或 telnet）



   3) 如果选择供应商为 Cisco ASA 或 Cisco PIX，则输入登录凭据，即登录凭据、登录名、密码、提示、启用用户名、启用密码和启用命令。

4) 如果您选择供应商为 Juniper SRX 或 FortiGate 或 SonicWALL 或其他人，则输入登录凭据，即登录名、密码和提示。

5) 点击“显示命令“查看将要上传的命令，如果需要可以修改命令。最后点击”执行命令“在把 syslog 导出命令上传到设备并执行。

2. 导入日志文件

导入的日志文件链接允许您通过 FTP 从本地计算机或远程导入日志文件。“导入日志文件”页面显示导入的日志文件列表，以及导入日志文件的主机和导入状态等详细信息。下面是设置导入日志文件的步骤：

1) 点击设置--->点击导入日志文件

2) 点击导入文件

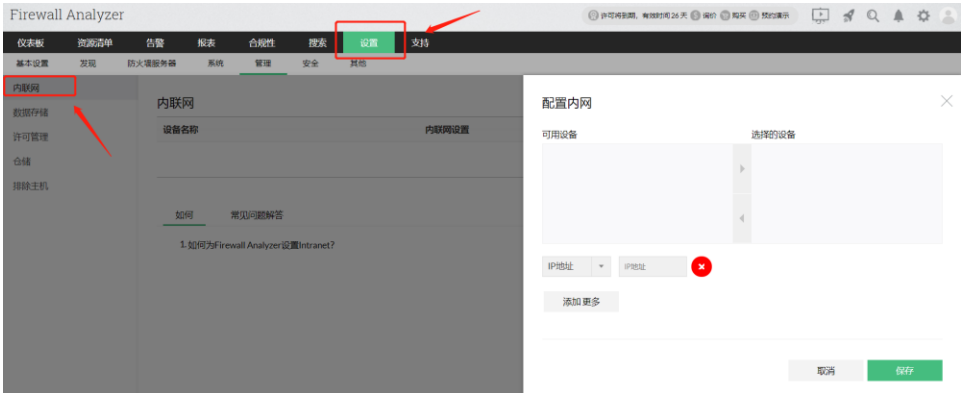

导入日志
本地主机
远程主机
文件位置：（文件最多尺寸：1 GB。）
浏览
忽略未解析 / 乱码记录
作为虚拟防火墙
192.168.0.144
将此日志文件映射到现有设备
取消
导入

关键配置

1. 配置内网

防火墙分析器包括指定网络的选项，或用于识别防火墙后面机器的一系列 IP 地址。此步骤叫做内网设备。通过添加位于您的网络(LAN)中的计算机或 IP 地址，您可以识别和区分在您的网络中生成的通信量和来自您网络或以您的网络以外为目的地的通信量。下面是设置内联网的步骤：

1) 点击设置--->点击内联网--->点击配置所有设备



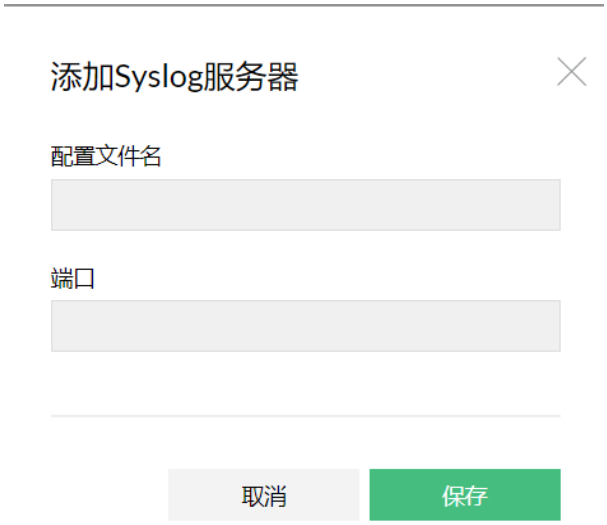
2) 单击“配置所有设备”链接菜单选项，为所有设备设置 Intranet。单击每个列出的防火墙，将使您能够为每个防火墙配置(Intranet)专用网络或 IP 范围或 IP 地址。

2. 增加 syslog 监听端口

1) 防火墙分析器中的 syslog 服务器的默认侦听器端口为 1514。如果防火墙将日志文件导出到这些端口之一，则不必设置任何虚拟 syslog 服务器。

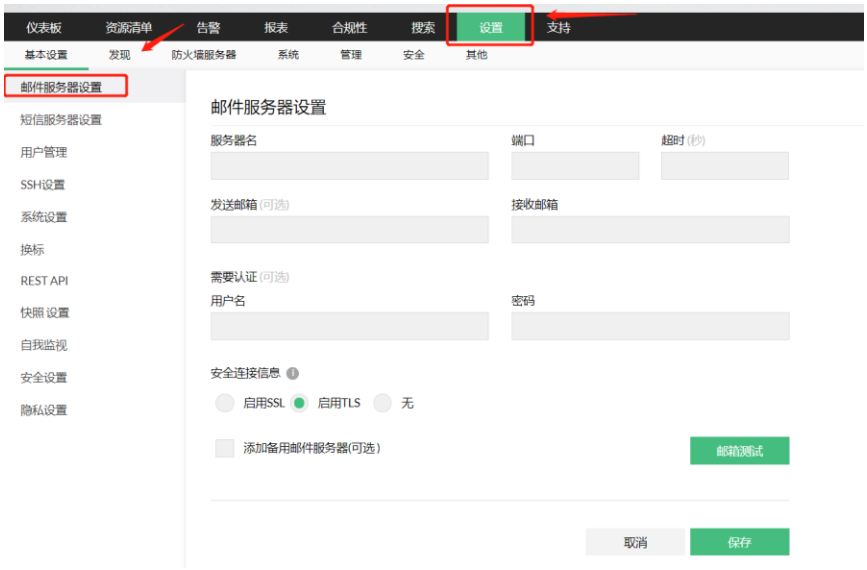
2) 增加 syslog 服务器

点击添加按钮



3. 配置邮件服务器

只有配置了邮件服务器才能接收到邮件告警通知和计划报表。



实时告警

1. 添加配置告警配置文件：

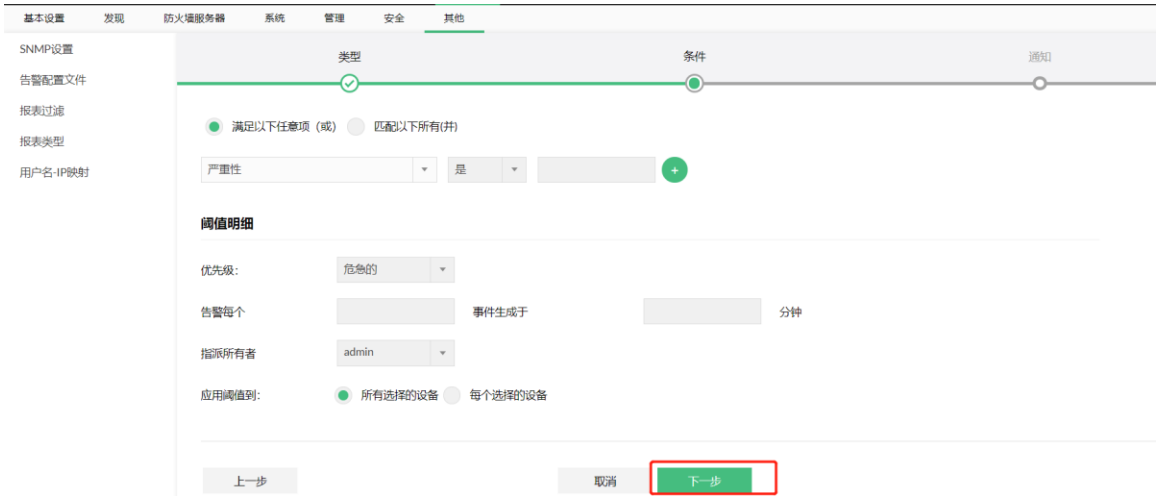
每当生成匹配特定条件的事件时，就会触发告警，警报配置文件允许定义这样的特定标准，并在触发相应的警报时通过电子邮件通知。

添加配置告警文件的步骤如下：

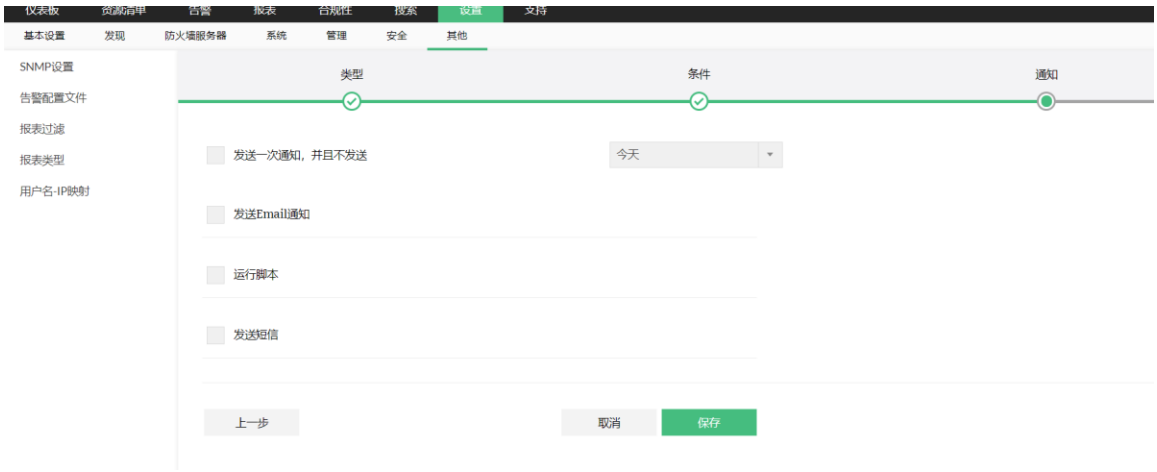
1) 点击设置--->点击配置告警文件--->点击添加

2) 选择设备，点击下一步

3) 选择好条件，点击下一步



4) 选择通知的方式



报表

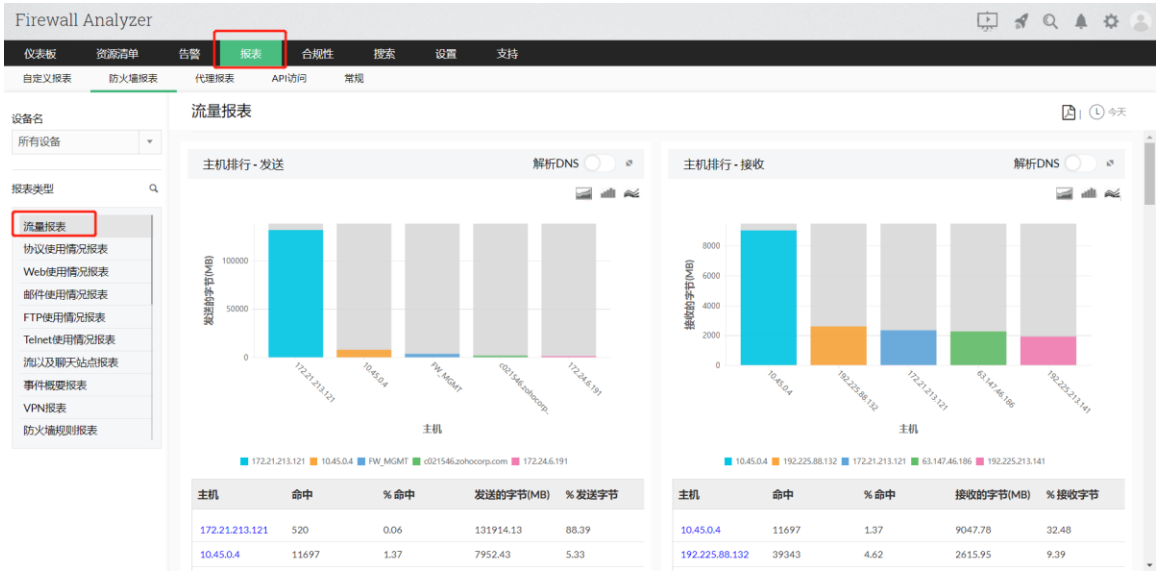
1. 报表的类型

- 实时报表
- 流量报表
- 协议使用情况报表
- Web 使用情况报表
- 邮件使用情况报表
- FTP 使用情况报表
- Telnet 使用情况报表
- 流媒体及聊天报表
- 事件综合报表
- VPN 报表
- 防火墙规则报表
- 入站/出站流量
- Intranet 报表
- Internet 报表
- 安全报表
- 病毒报表
- 攻击报表
- 垃圾信息报表
- 协议趋势报表
- 流量趋势报表

- 事件趋势报表
- 管理报表
- VPN 趋势报表
- URL 分类报表
- 防火墙变更管理报表

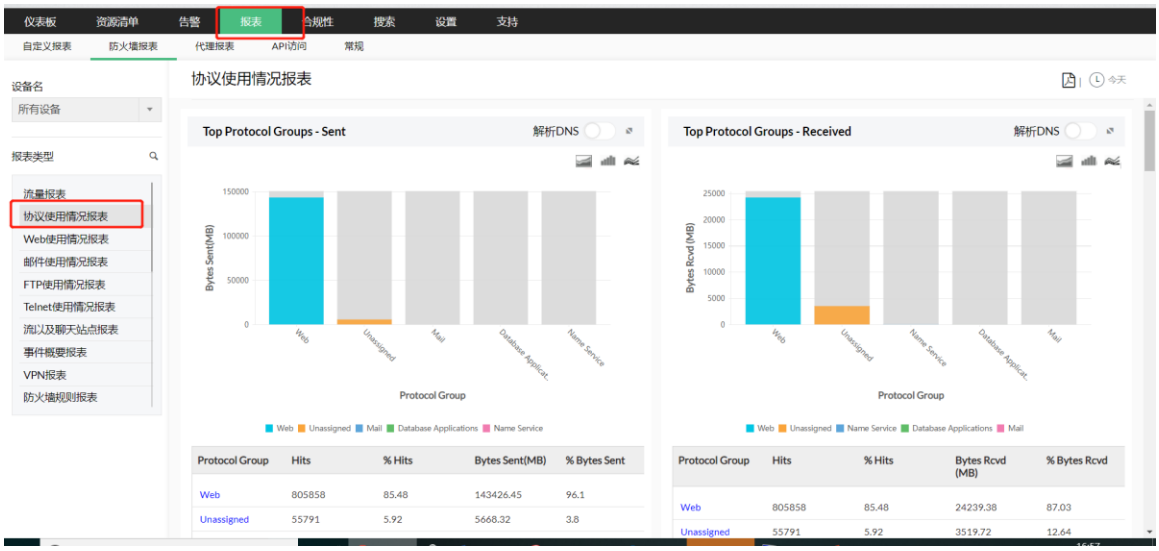
2. 流量分析报表

- 流量报表能基于设备接收和发送的流量，显示带宽的使用情况。
- 协议组排行，主机排行，工作时间和非工作时间分布流量



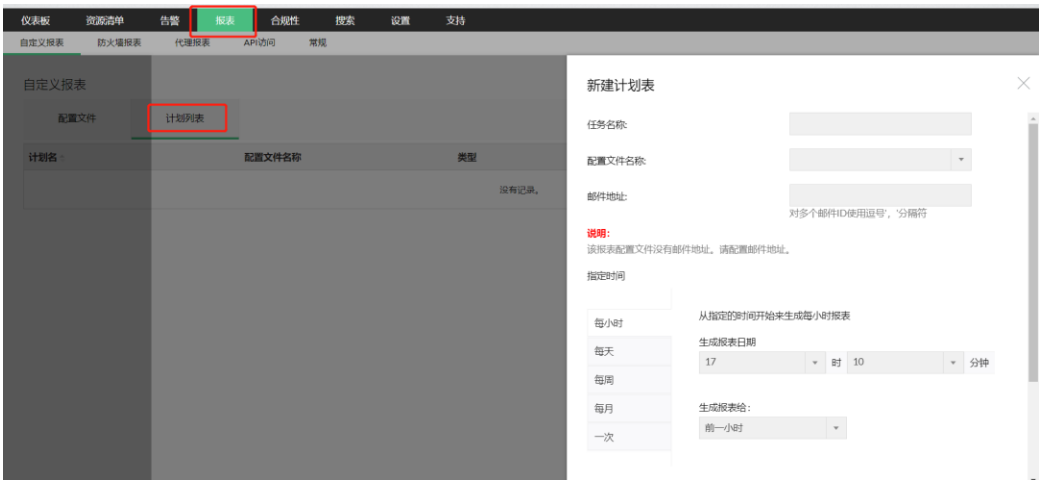
3. 协议使用情况报表

- 基于流量所使用的协议，显示带宽的使用情况
- 协议排行，主机排行，会话排行，工作时间和非工作时间流量分布。



4. 创建计划任务

通过指定计划，自动按时发送报表。



5. 搜索报表

此功能提供了许多选项，使搜索更加精确，并获得更多有用的结果。允许从存储在数据库中的索引、归档和处理防火墙日志中的原始防火墙日志进行搜索。

6. 设置日志过滤器

包含过滤器是过滤日志数据到报表的匹配条件。除外过滤器是把日志数据排除在报表外的匹配条件。除了选择指定过滤器来生成报表外，还可以添加、选择、编辑或删除过滤器。

产品文档

关于更详细的说明可参见用户手册：

网站：https://www.manageengine.cn/products/firewall/help/index.html

在线演示: http://demo.fwanalyzer.com

技术支持: mes@zohocorp.com.cn

电话：4006608680