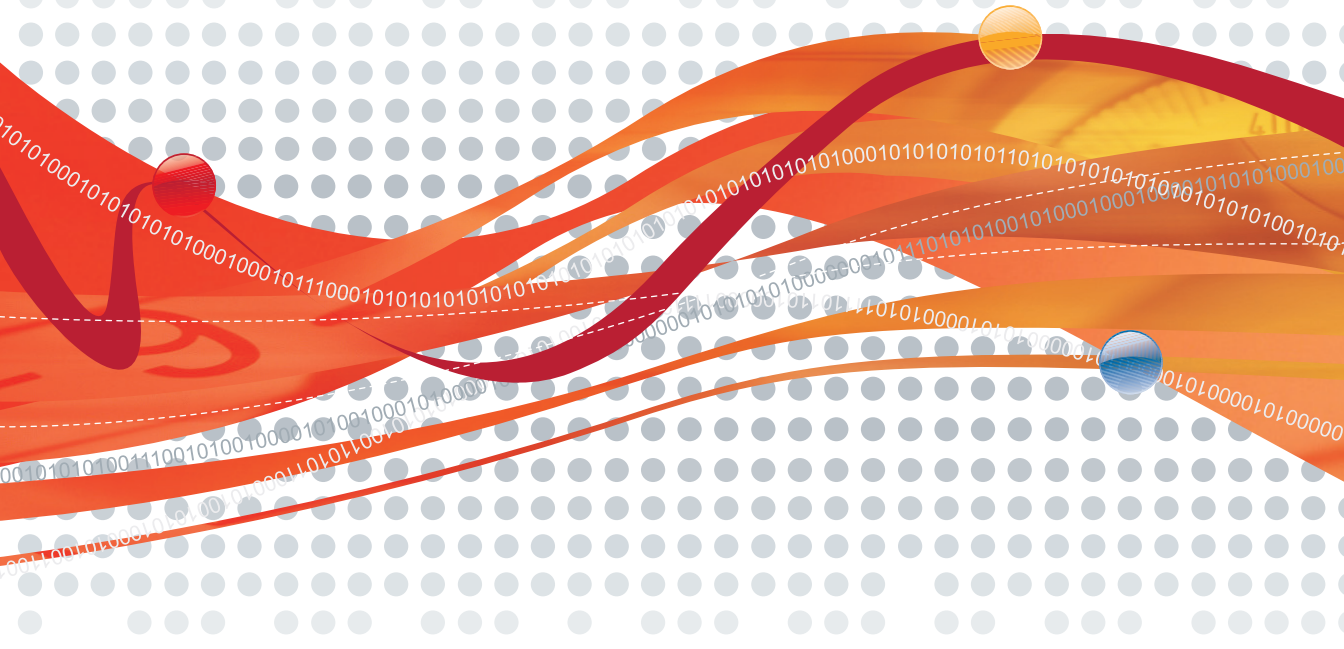
TREND MICRO

OfficeScan™ Corporate Edition 8.0

针对企业台式机与网络服务器的综合性集成安全方案

安装与部署指南



Endpoint Security

文档部分编号 OSCM83235/70529

发布日期：2007 年 6 月

受美国专利号 5,623,600、5,889,943、5,951,698 和 6.119,165 保护

趋势科技防毒墙网络版的用户文档介绍该软件的的主要功能和在您的产品环境中的安装指导信息。安装或使用该软件前先读一遍用户文档。

联机帮助文件和趋势科技 Web 站点上的在线知识库中有关于如何使用软件中的特定功能的详细信息。

趋势科技始终将设法改进其文档。如果您对此文档或任何趋势科技文档存有疑问、注释或建议，请访问 docs@trendmicro.com 与我们联系。

请在以下站点评估此文档：

www.trendmicro.com/download/documentation/rating.asp

目录

第 1 章： 规划服务器安装

安装需求 1-1

防毒墙网络版服务器需求 1-2
Web 控制台要求 1-3

产品版本与密钥 1-3

完全版和评估版 1-3
注册码和激活码 1-4

安装注意事项 1-5

防毒墙网络版服务器的位置 1-5
远程安装 1-6
服务器性能 1-6
专用服务器 1-7
不受支持的客户机平台 1-7
域编号 1-7
客户机编号 1-8
网络通信 1-8
程序文件放置 1-10
第三方防病毒应用程序 1-10

必需的安装信息 1-10

防毒墙网络版端口 1-12

其他安装节点 1-12

计算机无需重新启动 1-12
其他防毒墙网络版程序 1-13
客户机设置 1-13
Apache Web 服务器 1-13

规划试验部署 1-14

选择试验站点 1-14
创建还原计划 1-14
部署您的试验 1-14
评估您的试验部署 1-14

已知兼容性问题 1-15

Microsoft Small Business Server 1-15
Microsoft Lockdown 工具和 URLScan 1-15
Microsoft Exchange 服务器 1-15
SQL 服务器 1-16
Internet Connection Firewall (ICF) 1-16

第 2 章： 安装和升级防毒墙网络版服务器

安装或升级防毒墙网络版服务器 2-2

执行静默安装 2-10

从评估版升级 2-12

从控制管理中心升级 2-12

安装后任务 2-19

验证服务器安装或升级 2-20
更新防毒墙网络版组件 2-21
检查缺省设置 2-21
使用 Client Mover for Legacy Platforms 2-23
还原或重新安装后恢复设置 2-26
将防毒墙网络版注册到控制管理中心 2-28
安装插件管理器 2-28

卸装服务器 2-29

第 3 章： 规划客户机安装

安装需求 3-1

更新代理需求 3-5

安装方法 3-5

摘要 3-7

第 4 章： 安装和升级防毒墙网络版客户机

执行全新安装 4-2

从 Web 安装页安装 4-2
与 “登录脚本安装”一起安装 4-3
与客户机打包程序一起安装 4-6
从防毒墙网络版 Web 控制台安装 4-14
从客户机磁盘映像安装 4-16
与漏洞扫描程序一起安装 4-17

升级防毒墙网络版客户机 4-18

从第三方防病毒应用程序迁移 4-18

自动客户机迁移 4-19

从 ServerProtect 标准服务器迁移 4-20

系统需求 4-20
安装 ServerProtect 标准服务器迁移工具 4-20

安装后的任务 4-23

验证客户机安装、升级或迁移 4-23
启动组件更新 4-26
使用 EICAR 测试脚本测试防毒墙网络版 4-27

卸装客户机 4-28

从 Web 控制台卸装 4-29
运行客户机卸装程序 4-29

第 5 章： FAQ 和故障排除

常见问题 (FAQ) 5-1

故障排除资源 5-4

情况诊断工具 5-4
安装日志 5-4
服务器调试日志 5-6
客户机调试日志 5-7
知识库 5-8

解决安装问题 5-8

客户机安装 5-8
从第三方防病毒软件迁移 5-12
客户机卸装 5-14
服务器卸装 5-17
Apache Web 服务器 5-19

第 6 章： 与趋势科技联系

技术支持 6-1

加速您的支持呼叫 6-2

趋势科技知识库 6-3

TrendLabs 6-3

安全信息中心 6-4

将可疑文件发送给趋势科技 6-5

文档反馈 6-5

附录 A: 示例部署

基本网络 A-1

多个站点网络 A-2

总公司部署 A-5
远程站点 1 部署 A-5
远程站点 2 部署 A-6

第 1 章

规划服务器安装

本章中的主题：

- *安装需求*（第 1-1 页）
- *产品版本与密钥*（第 1-3 页）
- *安装注意事项*（第 1-5 页）
- *必需的安装信息*（第 1-10 页）
- *防毒墙网络版端口*（第 1-12 页）
- *其他安装节点*（第 1-12 页）
- *规划试验部署*（第 1-14 页）
- *已知兼容性问题*（第 1-15 页）

安装需求

以下为防毒墙网络版服务器和 Web 控制台的需求。

防毒墙网络版服务器需求

表 1-1. 防毒墙网络版服务器需求

资源	需求
操作系统	• 带有 SP 3 或 4 的 Microsoft™ Windows™ 2000 Server • 带有 SP 3 或 4 的 Microsoft Windows 2000 Advanced Server • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 32 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 64 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 R2 32 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 R2 64 位版 • Microsoft Windows Storage Server 2003 32 位版 • Microsoft Windows Storage Server 2003 64 位版 • Microsoft Cluster Server 2000 • Windows Compute Cluster Server 2003
硬件	• 800MHz Intel™ Pentium™ 处理器或其相当的处理器 • 512MB 内存 • 1GB 磁盘空间 • 网络接口卡 (NIC) • 颜色为 256 或更高时支持分辨率为 800 x 600 的显示器
Web 服务器	• Microsoft Internet Information Server (IIS) 在 Windows 2000 上：V5.0 （SP 3 或 4） 在 Windows Server 2003 上：V6.0 • 对防毒墙网络版服务器和 Cisco NAC 策略服务器都仅支持 Apache 2.0.54。
其他	• 可访问服务器计算机的管理员或域管理员权限 • 对于安装在服务器计算机上的 Microsoft 网络，允许 “文件和打印机共享”

注意： 如果计划在安装防毒墙网络版服务器的同一台计算机上安装 Cisco™ Trust Agent (CTA)，则不要在 Windows Server 2003 x64 版上安装防毒墙网络版服务器。有关 CTA 需求的详细信息，请参阅 *《管理员指南》*。

Web 控制台要求

表 1-2. Web 控制台要求

资源	需求
硬件	• 300MHz Intel Pentium 处理器或同等处理器 • 128MB 内存 • 30MB 可用磁盘空间 • 颜色为 256 或更高时支持分辨率为 800 x 600 的显示器
浏览器	Microsoft Internet Explorer™ 5.5 SP 1 或更高版本

产品版本与密钥

完全版和评估版

安装防毒墙网络版的完全版或免费的评估 （试用）版。

- **完全版：**包括所有产品功能和技术支持，并在许可证到期后提供一个宽限期 （通常为 30 天）。如果宽限期到期后未续定许可证，则将不能获得技术支持及执行组件更新。扫描引擎将仍然使用过期组件扫描计算机。这些过期组件可能不能完全保护您不受最新安全风险的侵扰。可以通过在到期前或到期后购买维护续定来续定许可证。

- **评估 （试用）版：**包括所有产品功能。您可以随时将评估版升级为完全版。如果在试用期结束时未升级，则防毒墙网络版将禁用组件更新、扫描和所有客户机功能。

注意： 两个版本都需要不同类型的激活码。如果没有激活码，请注册您的产品。

注册码和激活码

安装过程中，防毒墙网络版将提示您输入防病毒、损害清除服务 ™（可选）和 Web 威胁防护服务的激活码。

如果没有激活码，则使用产品附带的注册码在趋势科技 Web 站点注册并接收激活码。防毒墙网络版主安装程序将自动重新定向到趋势科技 Web 站点：

http://www.trendmicro.com/cn/support/pr-trial/PR-FAQ1.htm

如果注册码和激活码都没有，请与趋势科技销售代表联系（请参阅*与趋势科技联系*（第 6-1 页））。

注意： 对于注册问题，请参考 http://www.trendmicro.com.cn/corporate/techsupport/subwizard/case.asp。

安装注意事项

计划安装防毒墙网络版服务器时请考虑以下因素：

- *防毒墙网络版服务器的位置*（第 1-5 页）
- *远程安装*（第 1-6 页）
- *服务器性能*（第 1-6 页）
- *专用服务器*（第 1-7 页）
- *不受支持的客户机平台*（第 1-7 页）
- *域编号*（第 1-7 页）
- *客户机编号*（第 1-8 页）
- *网络通信*（第 1-8 页）
- *程序文件放置*（第 1-10 页）
- *第三方防病毒应用程序*（第 1-10 页）

防毒墙网络版服务器的位置

防毒墙网络版适用于各种网络环境。例如，可以在防毒墙网络版服务器和其客户机之间放置一个防火墙，或将服务器和所有客户机都放在单个网络防火墙之后。如果服务器和其客户机之间有防火墙，则配置该防火墙以允许客户机和服务器侦听端口之间的网络通信（有关详细信息，请参阅*防毒墙网络版端口*（第 1-12 页））。

注意： 有关解决在使用网络地址转换的网络上管理防毒墙网络版客户机时可能遇到的潜在问题的信息，请参阅 *《管理员指南》*和防毒墙网络版服务器联机帮助）。

远程安装

通过远程安装可以在一台计算机上启动安装程序，但却是在另一台计算机上安装防毒墙网络版。如果执行远程安装，则安装程序会分析目标计算机是否满足服务器安装需求。

确保安装可以继续：

- 确保您对目标计算机具有管理员权限。
- 注意计算机的主机名和登录凭证 （用户名和密码）。
- 确保计算机满足防毒墙网络版服务器系统需求。有关详细信息，请参阅*安装需求*（第 1-1 页）。
- 如果使用 Microsoft IIS 服务器作为 Web 服务器，则请确保版本为 5.0 或更高。如果选择使用 Apache Web 服务器，并且如果目标计算机中没有该服务器，安装程序将自动安装此服务器。

服务器性能

企业网络需要的服务器规格比中小型企业所需规格更高。理想状况下，防毒墙网络版服务器计算机应该至少有 2GHz 的双处理器和大于 1GB 的内存。

单个防毒墙网络版服务器可以管理的联网计算机客户机的数量取决于多个因素，如可用服务器资源和您的网络拓扑。请与趋势科技代表联系以帮助您确定服务器可以管理的客户机数。

带有 2GHz 双处理器和 2GB RAM 的防毒墙网络版服务器通常可以管理 3000 到 5000 台客户机。

专用服务器

选择要托管防毒墙网络版服务器的计算机时，请考虑以下因素：

- 计算机可以处理多少 CPU 负载？
- 计算机还会执行什么其他功能？

如果目标计算机有其他用途（例如，用作应用程序服务器的计算机），则趋势科技会建议选择不运行关键应用程序和占用大量资源的应用程序的计算机。

不受支持的客户机平台

防毒墙网络版不再支持 Windows 95、98、Me、NT 和 IA64 体系结构。如果打算升级此版本的防毒墙网络版，且客户机运行这些操作系统：

- 不要将所有的防毒墙网络版服务器都升级到此版本的防毒墙网络版。
- 指定一个未升级的防毒墙网络版服务器以管理这些客户机。
- 升级前，请打开 Web 控制台，并将这些客户机移动到指定的服务器。在防毒墙网络版 7.3 中，可以通过单击**客户机 > 移动**来访问“移动客户机”窗口。

如果已升级防毒墙网络版，但是没有将不受支持的客户机移动到未升级的服务器，则请参阅 *使用 Client Mover for Legacy Platforms*（第 2-23 页）以获取指导信息。

域编号

防毒墙网络版中的域是一组共享相同配置并运行相同任务的客户机。通过将客户机分组为域，可以同时对所有域成员配置、管理和应用相同的配置。

防毒墙网络版域与 Windows 域不同。一个 Windows 域中可以有几个防毒墙网络版域。

为了管理方便，请规划要创建几个防毒墙网络版域。可以根据所属部门或执行的功能为客户端计算机分组。另外，对更易受感染的客户机进行分组，并对它们应用更安全的配置。

客户机编号

如果联网计算机运行不同的 Windows 操作系统，则检查运行一个特定 Windows 版本的计算机数。使用此信息确定您的环境中最适合的客户机部署方法。

单个防毒墙网络版服务器可以管理的客户机数：

- 具有 2GB 的 RAM 和 2GHz 双处理器的防毒墙网络版服务器：3000 到 5000
- 具有 4GB 的 RAM 和 3GHz 双处理器的防毒墙网络版服务器：5000 到 8000

网络通信

规划部署时，请考虑防毒墙网络版产生的网络流量。执行以下操作时服务器会产生网络流量：

- 连接到趋势科技 ActiveUpdate 服务器以检查和下载更新的组件
- 通知客户机下载更新的组件
- 通知客户机配置的更改

执行以下操作时客户机会产生网络流量：

- 启动

- 手动或根据时间表更新组件
- 更新设置和安装 hotfix
- 在漫游模式和普通模式之间切换

组件更新过程中的网络通信

更新组件时，防毒墙网络版会产生大量的网络通信。要减少在组件更新过程中产生的网络通信，防毒墙网络版将执行组件复制。防毒墙网络版不下载更新的完全版病毒码文件，而是只下载 “增量”病毒码 （完全版病毒码文件的较小版本），下载后将其与旧的病毒码文件合并。

定期更新的客户机只下载增量病毒码，大约为 500KB 到 900KB。否则，可能必须下载大于 20MB 的完整病毒码文件。

趋势科技将定期发布新的病毒码文件。但是，一旦检测到常规损坏并存在积极传播的病毒/恶意软件后，趋势科技会立即发布新的病毒码文件。

更新代理和网络通信

如果客户机和防毒墙网络版服务器之间的网络有 “低带宽”或 “大流量”部分，则可以将选定的防毒墙网络版客户机指定为其他客户机的更新源。这将帮助分摊向所有客户机部署组件的负担。

例如，如果远程办公室有 20 台以上的计算机，则将指定一个更新代理以从防毒墙网络版服务器复制更新，并充当本地 LAN 上其他客户端计算机的本地分发点。有关更新代理的详细信息，请参阅*《管理员指南》*。

Trend Micro Control Manager 和网络通信

Trend Micro Control Manager™ 管理趋势科技产品与服务，和网关、邮件服务器、文件服务器和企业桌面级的第三方防病毒和内容安全产品。控制管理中心基于 Web 的管理控制台通过网络为防病毒和内容安全产品与服务提供单个监控点。

使用控制管理中心从单个位置管理多个防毒墙网络版服务器。互联网连接快速且可靠的控制管理中心服务器可以从趋势科技 ActiveUpdate 服务器下载组件，并将这些组件部署到互联网连接不可靠或无互联网连接的一个或多个防毒墙网络版服务器。

有关控制管理中心的详细信息，请参阅 *《管理员指南》*。

程序文件放置

在防毒墙网络版服务器安装过程中，在客户机上指定安装程序文件的位置。接受缺省客户机安装路径或对其进行修改。除非有强制性原因（如磁盘空间不足）要更改，否则趋势科技建议使用缺省设置。

缺省客户机安装路径为 C:\Program Files\Trend Micro\OfficeScan Client。

第三方防病毒应用程序

趋势科技强烈建议从要安装防毒墙网络版服务器的计算机移除第三方防病毒和反间谍软件应用程序，因为这些应用程序会阻止防毒墙网络版服务器的成功安装或影响其性能。

注意： 防毒墙网络版不能卸装任何第三方防病毒产品的服务器组件，但是可以卸装客户机组件 （有关详细信息，请参阅*从第三方防病毒应用程序迁移*（第 4-18 页））。

必需的安装信息

安装过程中，主安装程序会提示您以下信息：

- **代理服务器详细信息：**如果代理服务器可处理网络上的互联网网络通信，则从趋势科技 ActiveUpdate 服务器下载最新组件时请指定防毒墙网络版服务器要使用的代理服务器信息。

- **控制台密码：**通过指定一个密码阻止对防毒墙网络版 Web 控制台的未授权访问。
- **客户机软件安装路径：**指定主安装程序要将防毒墙网络版程序文件复制到的位置。

防毒墙网络版端口

防毒墙网络版有两种类型的端口：

- **服务器侦听端口（HTTP 端口）：**该端口用于防毒墙网络版服务器 Web 控制台。缺省情况下，防毒墙网络版将使用以下端口之一：
  - **IIS 服务器缺省 Web 站点：**与您的 HTTP 服务器的 TCP 端口相同的端口号
  - **IIS 服务器虚拟 Web 站点：**8080 (HTTP) 和 4343 (HTTPS)
  - **Apache 服务器：**8080
- **客户机侦听端口：**随机生成的端口号，客户机可通过此端口从服务器接收命令。

可以在安装过程中修改服务器侦听端口，或者安装后在防毒墙网络版 Web 控制台上修改。不能修改客户机侦听端口。

警告！ *许多黑客和通过 HTTP 传播的病毒 / 恶意软件攻击将使用端口 80 和 / 或 8080，因为多数组织都会把这些端口号用作 HTTP 通信的缺省传输控制协议 (TCP)。如果当前使用缺省端口号，则趋势科技建议使用其他端口号。*

其他安装节点

计算机无需重新启动

安装防毒墙网络版服务器不需要计算机重新启动。安装完成后，立即配置服务器，并将客户机安装到联网计算机。如果使用 IIS Web 服务器，则安装程序将自动停止，并在 Web 服务器安装过程中重新启动 IIS 服务。

警告！ *在运行 IIS 锁定应用程序的计算机上安装 Web 服务器可能阻止成功安装。请参阅 IIS 文档以获取详细信息。*

其他防毒墙网络版程序

可以在防毒墙网络版服务器安装期间或安装后启用防毒墙网络版防火墙，并安装面向 Cisco NAC 的策略服务器。

提示： 趋势科技强烈建议在非高峰时段安装防毒墙网络版以将对网络的影响最小化。

客户机设置

升级到此版本的防毒墙网络版时可以保留客户机设置，并且如果要重新安装防毒墙网络版服务器，则可以使用这些设置。有关知道信息，请参阅*还原或重新安装后恢复设置*（第 2-26 页）。

Apache Web 服务器

安装防毒墙网络版服务器时可以安装 Apache Web 服务器。缺省情况下，管理员帐户是在 Apache Web 服务器上创建的唯一帐户。如果黑客控制了 Apache Web 服务器，则趋势科技建议创建运行 Web 服务器的另一个帐户以防止危及防毒墙网络版服务器的安全。

有关 Apache Web 服务器升级、修补程序和安全问题的最新信息，请参考 http://www.apache.org。

规划试验部署

执行全规模部署前，趋势科技建议在受控的环境中执行试验部署。试验部署提供一个机会确定功能组件的工作方式和完全部署后可能需要的支持级别。它还给您的安装团队一个机会预演和净化部署过程，并测试您的部署计划是否满足贵组织的防病毒和反间谍软件动机。

有关示例防毒墙网络版部署，请参阅*示例部署*（第 A-1 页）。

选择试验站点

选择与您的生产环境相匹配的试验站点。尝试模拟可充分演示您的生产环境的网络拓扑类型。

创建还原计划

如果安装或升级过程出现问题，趋势科技建议创建灾难恢复计划或还原计划。

此过程应该考虑本地企业策略和技术特性。

部署您的试验

检查适合您特殊环境的部署方法。有关详细信息，请参阅*安装和升级防毒墙网络版服务器*（第 2-1 页）。

评估您的试验部署

创建试验过程中遇到的成功列表和失败列表。相应地识别潜在缺陷和计划。包括总产品部署计划中的此试验评估计划。

已知兼容性问题

本部分将解释兼容性问题（如果在带有特定第三方应用程序的同一台计算机上安装了防毒墙网络版服务器）。请参考在安装防毒墙网络版服务器的同一台计算机上安装的第三方应用程序文档。

Microsoft Small Business Server

在同时运行 Microsoft Small Business Server™ 和 Microsoft Internet Security Acceleration 服务器 (ISA) 的计算机上安装防毒墙网络版前，写下 ISA 使用的服务器端口。缺省情况下，防毒墙网络版服务器和 ISA 都使用端口 8080。

安装防毒墙网络版服务器时选择另一个服务器侦听端口。

Microsoft Lockdown 工具和 URLScan

如果使用 Microsoft IIS Lockdown 工具或 URLScan，则防毒墙网络版配置 (.ini)、数据 (.dat)、动态链接库 (.dll) 和可执行文件 (.exe) 的防盗装置可能会阻止防毒墙网络版客户机和服务器之间的通信。

要阻止 URLScan 干预客户机 - 服务器通信，请停止防毒墙网络版服务器上的 World Wide Web Publishing 服务，修改 URLScan 配置文件以允许上面指定的文件类型，然后重新启动该服务。请参阅防盗工具文档以获取其他信息。

Microsoft Exchange 服务器

如果选择在服务器安装过程中安装防毒墙网络版客户机，则防毒墙网络版需要访问客户机要扫描的所有文件。由于 Microsoft Exchange 服务器在本地目录中排列消息，因此这些目录需要从扫描中排除以允许 Exchange 服务器处理电子邮件消息。

防毒墙网络版可自动将所有 Microsoft Exchange 2000/2003 目录从扫描中排除。此设置在 Web 控制台设置（**联网计算机 > 全局客户机设置 > 病毒 / 恶意软件扫描设置**）。

有关 Microsoft Exchange 2007 的信息，请参考 http://technet.microsoft.com/en-us/library/bb332342.aspx 以获取例外详细信息。

趋势科技 ™ 防毒墙群件版 ™ for Microsoft Exchange 可以保护您的 Exchange 服务器不受病毒 / 恶意软件和其他潜在威胁的危害。有关防毒墙群件版 for Microsoft Exchange 的信息，请参阅趋势科技 Web 站点 (http://www.trendmicro.com.cn/) 或与您的销售人员联系。

SQL 服务器

还可以扫描 SQL 服务器数据库。但是，这可能会降低访问数据库的应用程序的性能。趋势科技建议将 SQL 服务器数据库及其备份文件夹从实时扫描中排除。如果需要扫描数据库，则在非高峰时段执行手动扫描以将扫描的影响最小化。

Internet Connection Firewall (ICF)

Windows Server 2003 将提供一个名为 Internet Connection Firewall (ICF) 的内置防火墙。如果启用了防毒墙网络版防火墙，则趋势科技会强烈建议移除任何第三方防火墙应用程序。但是，如果想运行 ICF 或任何其他第三方防火墙，则可将防毒墙网络版侦听端口添加到防火墙例外列表（有关侦听端口的信息，请参阅*防毒墙网络版端口*（第 1-12 页）；有关如何配置例外列表的详细信息，请参阅您的防火墙文档）。

第 2 章

安装和升级防毒墙网络版服务器

安装 / 升级场景：

- *安装或升级防毒墙网络版服务器*（第 2-2 页）
- *执行静默安装*（第 2-10 页）
- *从评估版升级*（第 2-12 页）

注意： 有关完全版和评估版之间差别的详细信息，请参阅*产品版本与密钥*（第 1-3 页）。

- *从控制管理中心升级*（第 2-12 页）

建议的安装后任务：

- *验证服务器安装或升级*（第 2-20 页）
- *更新防毒墙网络版组件*（第 2-21 页）
- *检查缺省设置*（第 2-21 页）

- *使用 Client Mover for Legacy Platforms* （第 2-23 页）

  注意： 仅当客户机运行不受支持的平台（包括 Windows 95、98、Me、NT 和 IA64 体系结构）时，才执行此任务。

- *还原或重新安装后恢复设置* （第 2-26 页）
- *将防毒墙网络版注册到控制管理中心* （第 2-28 页）

  注意： 控制管理中心注册仅适用于新安装的防毒墙网络版服务器。

- *安装插件管理器* （第 2-28 页）

其他任务：

- *卸载服务器* （第 2-29 页）

安装或升级防毒墙网络版服务器

可以本地或远程执行全新安装或升级前一版本的防毒墙网络版。此版本的防毒墙网络版支持从 V7.3、7.0、6.5 和 5.58 升级，但不支持从趋势科技中小企业网络安全版或网络与邮件安全版升级。

重新安装或升级到此版本的防毒墙网络版时可以保留您的客户机设置。请参阅*还原或重新安装后恢复设置* （第 2-26 页）以获取详细信息。

趋势科技建议升级前从防毒墙网络版服务器删除所有日志文件。如果想要保留这些日志文件，请先将它们保存到其他位置。

下面是安装窗口（按顺序排列）和本地或远程安装或升级防毒墙网络版的任务列表。有关窗口特定信息和指导信息，请在可应用的“安装”窗口单击**帮助**。

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
欢迎使用	✓	✓	✓	✓
授权合约书 *任务：*同意该授权合约书。	✓	✓	✓	✓
安装目标 *任务：*选择是要本地安装还是远程安装。	✓	✓	✓	✓
预扫描 *任务：*确定安装前是否扫描目标计算机。 如果执行预扫描： • 本地安装：单击**下一步**时扫描。 • 远程安装：实际安装过程中扫描。	✓	✓	✓	✓
安装状态 （计算机分析）	✓		✓	
安装路径 如果执行远程全新安装和升级，则将显示此窗口。但是，您在此处指定的设置仅适用于远程全新安装。对于远程升级，防毒墙网络版将使用前一版本的设置。 *任务：*使用缺省安装路径或指定一个新路径。	✓	✓		✓

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
代理服务器设置 如果执行远程全新安装和升级，则将显示此窗口。但是，您在此处指定的设置仅适用于远程全新安装。对于远程升级，防毒墙网络版将使用前一版本的设置。 *任务：*如果将代理服务器设置用于客户机 - 服务器通信，则请指定代理服务器设置。否则，请跳过此步。	✓	✓		✓
Web 服务器设置 如果执行远程全新安装和升级，则将显示此窗口。但是，您在此处指定的设置仅适用于远程全新安装。对于远程升级，防毒墙网络版将使用前一版本的设置。 如果从防毒墙网络版 5.58 进行本地升级，则还将显示此窗口。 *任务：*选择是使用 IIS 还是 Apache Web 服务器，然后配置 HTTP 端口和 SSL 设置。	✓	✓	✓	✓
计算机识别 如果执行远程全新安装和升级，则将显示此窗口。但是，您在此处指定的设置仅适用于远程全新安装。对于远程升级，防毒墙网络版将使用前一版本的设置。 *任务：*确定防毒墙网络版客户机是否按其域名或 IP 地址识别服务器计算机。	✓	✓		✓
注册 *任务：*使用产品附带的注册码注册防毒墙网络版，然后获取激活码。如果已注册并接收到了激活码，请跳过此步。	✓	✓	✓	✓

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
激活 *任务：*请输入产品服务的激活码。	✓	✓	✓	✓
远程安装目标 *任务：*指定要安装防毒墙网络版的目标计算机。		✓		✓
远程安装计算机分析 *任务：* • 单击**分析**以便安装程序可以确定目标计算机是否满足安装需求。 • 要将选定的计算机保存到文本文件，请单击**导出**。		✓		✓

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
安装其他防毒墙网络版程序 • 如果防毒墙网络版客户机存在于目标计算机上，则服务器安装后安装程序将自动升级客户机。 • 如果趋势科技防毒墙服务版 ™ 存在于目标计算机上，请在安装防毒墙网络版客户机前将其卸装。 • 如果未激活防病毒服务，则 Cisco NAC 程序不可用。 • 可以跳过安装防毒墙网络版客户机和 Cisco NAC 程序，然后在服务器安装后安装它们。对于防毒墙网络版客户机的安装，请参考*安装和升级防毒墙网络版客户机*（第 4-1 页）。对于 CTA 安装，请打开 Web 控制台并转至 **Cisco NAC > 代理部署**。对于策略服务器安装，请从您的防毒墙网络版安装软件包运行安装程序。 • 请参阅《管理员指南》以了解有关 Cisco NAC 的详细信息。 **任务：** • 选择要安装的程序。 • 如果安装了 Cisco Trust Agent (CTA)，请指定代理证书文件的位置（如果证书可用；如果不可用，请与您的趋势科技代表联系）。	✓	✓	✓	✓

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
Cisco Trust Agent 安装 / 升级 • 如果执行了全新安装，则仅当在前一窗口中选择安装 Cisco Trust Agent 时才显示此窗口。选择要安装到客户机的 CTA 软件包。 • 如果升级了，则仅当先前安装了 CTA 时才显示此窗口。选择是否要将 CTA 升级到当前版本 (2.1)。如果升级了，请选择 CTA 升级软件包。 • 如果在服务器安装期间未选择安装 CTA，则仍可以使用 Web 控制台安装它。	✓		✓	
Cisco Trust Agent 许可证 *任务：*同意该授权合约书。	✓		✓	
全球病毒跟踪 *任务：*确定是否要加入 “趋势科技全球病毒跟踪计划”。	✓	✓		
管理员帐户密码 *任务：*指定密码以执行以下操作： • 访问 Web 控制台 • 卸载和卸装防毒墙网络版客户机	✓	✓		
客户机安装路径 *任务：*接受缺省客户机安装设置或指定其他设置 • 客户机安装路径 • 防毒墙网络版服务器将用于与客户机进行通信的端口号 • 客户机安全级别	✓	✓		
启用防火墙 仅当激活防病毒服务时，才显示此窗口。	✓	✓	✓	✓

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
启用评估模式 仅当激活 Web 威胁防护服务时，才显示此窗口。	✓	✓	✓	✓
程序文件夹快捷方式 *任务：*接受缺省文件夹名称或指定一个新名称。还可以选择现有文件夹，以便安装程序向其添加程序快捷方式。	✓			
安装信息 *任务：* • 检查安装信息是否正确。 • 单击**返回**修改设置。	✓	✓	✓	✓
防毒墙网络版服务器安装	✓	✓	✓	✓
策略服务器安装 如果选择安装面向 Cisco NAC 的策略服务器，则将显示此窗口。显示的后续策略服务器安装窗口包括： • 欢迎使用 • 授权合约书 • 安装目标 • Web 服务器选择 • Web 服务器设置 • 策略服务器控制台密码 • ACS 服务器认证密码 • 策略服务器安装 • 安装完毕	✓			

表 2-1　　安装窗口和任务

窗口 / 任务	全新安装（本地）	全新安装（远程）	升级（本地）	升级（远程）
防毒墙网络版服务器安装完毕 *任务：* • 查看自述文件。 • 打开 Web 控制台可开始配置防毒墙网络版设置。请参阅*更新防毒墙网络版组件*（第 2-21 页）以获取详细信息。				

执行静默安装

如果服务器都使用相同的安装设置，则可静默安装多个防毒墙网络版服务器。静默安装包括两个过程：

1. 可通过运行 “安装”向导和将安装设置记录到一个 .iss 文件来创建响应文件。所有使用响应文件静默安装的服务器都将使用这些设置。

   重要：

   - “安装”向导只显示本地安装 （全新安装或升级）的窗口。有关将显示的相关窗口，请参阅 *安装或升级防毒墙网络版服务器*（第 2-2 页）。
   - 如果打算将防毒墙网络版服务器升级到此版本，请确保从安装有防毒墙网络版服务器的计算机创建响应文件。类似地，如果打算执行全新安装，则请从未安装防毒墙网络版服务器的计算机创建响应文件。

2. 从命令提示符运行安装程序，并将安装程序指向响应文件的位置以用于静默安装。可以使用静默安装过程将防毒墙网络版从先前版本升级。此过程与全新安装类似。

将服务器安装配置记录到响应文件：

注意： 此过程不安装防毒墙网络版。它只把服务器安装配置记录到响应文件。

---

1. 打开一个命令提示符，并键入防毒墙网络版 Setup.exe 文件的目录。例如，“CD C:\OfficeScan installer”。

2. 输入 setup.exe -r。 -r 切换命令该程序把安装详细信息记录到响应文件。

3. 在 “安装”向导中，请遵循安装步骤。完成这些步骤后，在 %windir% 中检查响应文件 (setup.iss)。

运行静默安装：

1. 将安装软件包 （包括所有安装文件和文件夹，还有 setup.exe 文件）和 setup.iss 复制到目标计算机。

2. 在目标计算机中，打开一个命令提示符，然后键入 setup.exe 文件的目录。

3. 键入 setup.exe -s -f1{ 路径 }setup.iss -f2{ 路径 }setup.log。

   例如：C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log

   其中：

   - **-s**：命令安装程序执行静默安装
   - **-f1{ 路径 }setup.iss**：响应文件的位置。如果该路径中包括空格，则会以引号 (") 结尾。例如， -f1"C:\osce script\setup.iss"。
   - **-f2{ 路径 }setup.log**：安装后安装程序将创建的日志文件的位置。如果该路径中包括空格，则会以引号 (") 结尾。例如， -f2"C:\osce log\setup.log"。

4. 按 **Enter** 键。 Setup.exe 将静默地把服务器安装到计算机。

5. 要确定安装是否成功，请检查目标计算机上的防毒墙网络版程序快捷方式。如果快捷方式不可用，请重试安装。

从评估版升级

您的评估 （试用）版快到期时，防毒墙网络版将在 “摘要”窗口中显示一条通知消息。可以将防毒墙网络版通过 Web 控制台从评估版升级为完全版，而不会损失任何配置设置。当有完全版许可证时，将收到一个注册码或激活码。

从评估版升级：

1. 打开防毒墙网络版 Web 控制台。
2. 单击**管理 > 产品许可证**。将显示 “产品许可证”窗口。
3. 如果有激活码，则请在**新激活码**字段中输入它，然后单击**激活**。

   如果没有激活码，则单击**在线注册**并使用注册码获取激活码。

从控制管理中心升级

可以升级 Trend Micro Control Manager 服务器可以管理的多个防毒墙网络版服务器。

支持的版本：

- 防毒墙网络版服务器：
  - 5.58，带有控管中心代理 2.51
  - 7.0，带有控管中心代理 2.53
  - 7.3，带有控管中心代理 2.55
- 控制管理中心服务器：2.5, 3.0, 3.5

升级前准备：

- 控制管理中心服务器
- 要升级的防毒墙网络版服务器 （请确保升级过程中服务器计算机已启动和运行。）
- 此防毒墙网络版版本的安装软件包
- 有效激活码
- 加密工具，如 SecurePass™
- **UpgradeEncryptOSCESrvAgent.zip** 文件

> **注意：** 要获取此文件，请与趋势科技代表联系，或访问 http://solutionfile.trendmicro.com/SolutionFile/24290/en/UpgradeEncryptOSCESrvAgent.zip。

从控制管理中心升级防毒墙网络版：

1. 从安装软件包将所有防毒墙网络版安装文件和文件夹复制到防毒墙网络版 5.58 或 7.x 服务器计算机中的临时文件夹。假设临时文件夹名称为 “OSCE8”。
2. 在带有加密工具的计算机上，创建包括所有防毒墙网络版 5.58 或 7.x 服务器的文件并为其加密。
   a. 创建一个名为 pass.csv 的文件，然后输入防毒墙网络版服务器计算机的主机名称和管理员帐户 （用户名和密码）。可以将防毒墙网络版 5.58 和 7.x 服务器包括在列表中。

      例如：

      计算机 01、管理员、密码 01

计算机 02、管理员、密码 02

计算机 03、管理员、密码 03

b. 打开命令提示符，然后转到加密工具的目录。

c. 输入加密工具名称，随后加 /e 或 /d 命令，然后再加 pass.csv. 的位置和文件名。 /e 命令加密该文件， /d 命令解密该文件。

示例用法：

- 如果 securepass.exe （加密工具名称）和 pass.csv 在同一目录上：

  securepass.exe /e pass.csv

- 如果这两个文件在不同目录上：

  securepass.exe /e C:\temp\pass.csv

d. 将 pass.csv 复制到步骤 1 中创建的文件夹。

3. 在防毒墙网络版 5.58 或 7.x 服务器计算机上创建一个响应文件。

注意： 创建响应文件时，输入一个有效的完全版或评估版激活码。如果输入了一个评估版激活码，请记住升级后将其更改。

---

a. 打开一个命令提示符，然后转到步骤 1 中创建的临时文件夹。

b. 输入 **setup -r**，然后按 **Enter** 键。

c. 在打开的 “安装”向导中，遵循本地升级步骤。有关要显示的升级窗口，请参阅 *安装或升级防毒墙网络版服务器* （第 2-2 页）。完成这些步骤后，在临时文件夹中检查响应文件 (setup.iss)。

注意： 此过程不安装防毒墙网络版；只将服务器安装配置记录到响应文件。

d. 将 setup.iss 重命名为：

- setup558.iss （如果从防毒墙网络版 5.58 升级）
- setup700.iss （如果从防毒墙网络版 7.x 升级）

4. 使用工具 （如 WinZip）将步骤 1 中创建的文件夹归档。如果我们使用步骤 1 中的示例临时文件夹名称 (OSCE8)，则归档文件名应该为 OSCE8.zip。

a. 注意归档文件的大小（以字节计算，不是在磁盘上的大小）。在控制管理中心服务器计算机中修改 server.ini 文件时，将需要此信息。要检查文件大小，请右键单击归档文件，然后单击**属性**。

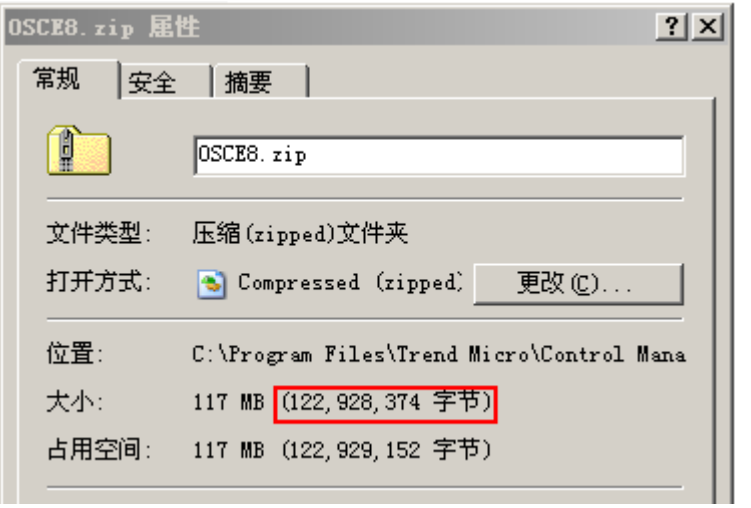


FIGURE 2-1. 样本归档文件的文件大小

b. 将归档文件复制到控制管理中心服务器计算机中下面的文件夹内：\WebUI\download\activeupdate\Product。

5. 将 UpgradeEncryptOSCESrvAgent.zip 文件也复制到控制管理中心服务器计算机中下面的文件夹内：\WebUI\download\activeupdate\Product。

6. 注意 UpgradeEncryptOSCESrvAgent.zip 文件的大小 （以字节计算）。

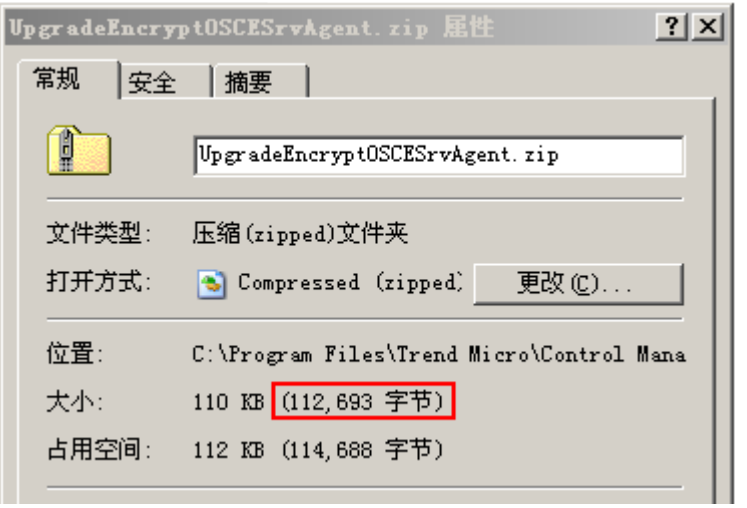


FIGURE 2-2. UpgradeEncryptOSCESrvAgent.zip 文件的大小 （只作为样本，请勿复制）

7. 在控制管理中心服务器计算机的 \WebUI\download\activeupdate 文件夹中打开 **server.ini** 文件。

8. 在 server.ini 文件中修改以下内容：

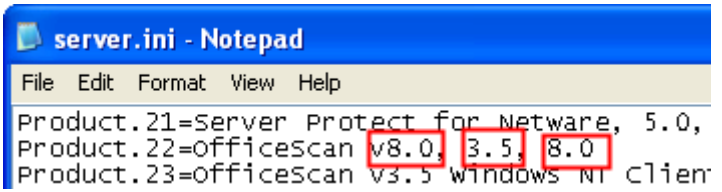


FIGURE 2-3. server.ini 文件中的变量

其中：

- **V8.0** 是防毒墙网络版安装软件包的版本
- **3.5** 是受支持的最低版本
- **8.0** 是受支持的最高版本

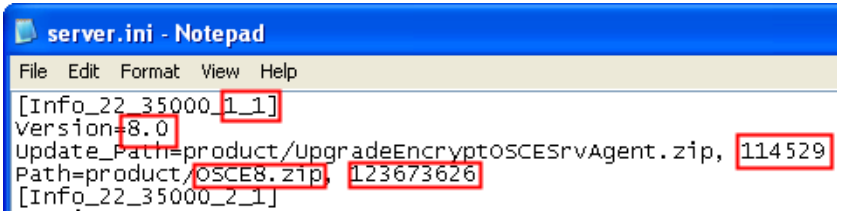


FIGURE 2-4. server.ini 文件中的变量

其中：

- **1_1** 是防毒墙网络版的英语版本

注意： 日语版本为 1_4。

- **8.0** 是防毒墙网络版安装软件包的版本
- **114529** 是 UpgradeEncryptOSCESrvAgent.zip 文件的大小（以字节计算）

注意： 此值只是个示例。请获取实际文件的大小。

- **OSCE8.zip** 是归档文件名称

注意： 这是在步骤 4 中创建的示例文件名。请使用您的归档文件的实际文件名。

- **123673626** 是 OSCE.zip 文件的大小 （以字节计算）

注意： 此值只是个示例。请获取实际文件的大小。

9. 打开控制管理中心控制台，然后转至**产品 > 任务 > 部署程序文件**。

   由控制管理中心管理的相应防毒墙网络版服务器开始升级。例如，如果从防毒墙网络版 5.58 服务器计算机创建归档文件，则仅列在 pass.csv 中且包含在产品目录实体中的防毒墙网络版 5.58 服务器会升级。如果服务器为防毒墙网络版 7.x 服务器，则重复步骤 1 到 9。

安装后任务

趋势科技建议执行以下安装后任务：

- *验证服务器安装或升级* （第 2-20 页）
- *更新防毒墙网络版组件* （第 2-21 页）
- *检查缺省设置* （第 2-21 页）
- *使用 Client Mover for Legacy Platforms* （第 2-23 页）

注意： 仅当客户机运行不受支持的平台（包括 Windows 95、98、Me、NT 和 IA64 体系结构）时，才执行此任务。

- *还原或重新安装后恢复设置* （第 2-26 页）
- *将防毒墙网络版注册到控制管理中心* （第 2-28 页）

注意： 控制管理中心注册仅适用于新安装的防毒墙网络版服务器。

- *安装插件管理器*（第 2-28 页）

验证服务器安装或升级

完成安装或升级后，验证以下内容：

- Windows 开始菜单上的防毒墙网络版程序快捷方式
- “添加或删除程序”窗口中的当前安装的程序列表，该列表应该包括 “趋势科技防毒墙网络版服务器”。
- Web 控制台连接：
  - http://{ 防毒墙网络版服务器名称 }:{ 端口号 }/OfficeScan
  - *或者如果使用 SSL*：https://{ 防毒墙网络版服务器名称 }:{ 端口号 }/OfficeScan

  其中 { 防毒墙网络版服务器名称 } 是防毒墙网络版服务器的名称或 IP 地址。
- 包括在 Windows 服务中的防毒墙网络版服务：
  - 防毒墙网络版主服务 （应该正在运行）
  - 面向 Cisco NAC 的趋势科技策略服务器 （如果已安装）
- 运行防毒墙网络版进程：
  - OfcService.exe
  - DBServer.exe
- 安装日志：OFCMAS.LOG （在 %windir% 中）

- 注册码：
  HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan
- Program 文件夹 :{ 安装驱动器和文件夹 }\Trend Micro\OfficeScan

更新防毒墙网络版组件

安装或升级后，立即用最新的防毒墙网络版组件更新服务器。

注意： 本部分向您显示如何执行手动更新。有关预设更新和更新配置的信息，请参阅防毒墙网络版服务器联机帮助。

更新防毒墙网络版服务器：

1. 打开防毒墙网络版 Web 控制台。
2. 在主菜单上，单击**更新 > 服务器 > 手动更新**。将显示 “手动更新”窗口，该窗口显示了当前组件、其版本号和最近更新日期。
3. 选择要更新的组件。
4. 单击**更新**。服务器将检查更新服务器是否有更新的组件。将显示更新进度和状态。

检查缺省设置

防毒墙网络版按缺省设置安装。如果这些设置与您的安全需求不一致，则请在安装防毒墙网络版客户机前在 Web 控制台上修改然后保存设置。有关 Web 控制台上可用设置的详细信息，请参考联机帮助和 《管理员指南》。

扫描设置

防毒墙网络版提供几种类型的扫描来保护您的客户机免受安全风险的侵扰。可以通过转至**联网计算机 > 客户机管理 > 设置 > { 扫描类型 }** 从 Web 控制台修改扫描设置。

- **实时扫描：**防毒墙网络版实时扫描文件。如果防毒墙网络版没有检测到安全风险，则用户可以继续打开或保存文件。如果防毒墙网络版检测到一个安全风险，则显示内容为文件名和特定安全风险的通知消息。
- **手动扫描：**用户在客户机控制台中启动对病毒 / 恶意软件的手动扫描后，手动扫描会立即开始。扫描时间的长度取决于要扫描文件的数量及客户端计算机的硬件资源。间谍软件 / 灰色软件的扫描时间和范围取决于您或（具有手动扫描配置权限的）客户机用户指定的扫描方法。可以选择在 Web 控制台的“手动扫描设置”页中使用的扫描方法。
- **预设扫描：**预设扫描和手动扫描的扫描行为相似。唯一的区别是预设扫描在预设的日期和时间自动运行。使用预设扫描在客户机上使例行任务扫描自动化并提高扫描管理效率。
- **立即扫描：**立即扫描和手动扫描是同一类型的扫描。唯一的不同是您使用 Web 控制台远程启动立即扫描，而用户在其客户端计算机上本地运行手动扫描。

全局客户机设置

防毒墙网络版提供了几种类型的设置，可适用于注册到该服务器上的所有客户机，或者具有特定权限的所有客户机。可以通过转至**联网计算机 > 全局客户机设置** 来从 Web 控制台修改全局客户机设置。

客户机权限

缺省客户机权限包括在客户机控制台上显示**邮件扫描**和**工具箱**选项卡。通过转至**联网计算机 > 客户机管理 > 设置 > 权限和其他设置**来从 Web 控制台修改缺省客户机权限。

使用 Client Mover for Legacy Platforms

此版本的防毒墙网络版不再支持 Windows 95、98、ME、NT 和 IA64 架构。如果您有运行这些平台的客户机，并已将其升级到此版本的防毒墙网络版：

- 防毒墙网络版服务器会停止管理不受支持的客户机。这些客户机的状态将变为 “断开连接”。
- 防毒墙网络版服务器会将这些客户机的信息保存到防毒墙网络版安装文件夹中的 **unsupCln.txt** 文件。通常，该文件路径是 C:\Program Files\Trend Micro\OfficeScan\PCCSRV \Private\unsupCln.txt。
- 请确保您有较早版本的防毒墙网络版服务器，该服务器将管理不受支持的客户机。
- 在已升级的防毒墙网络版服务器中，运行名为 Client Mover for Legacy Platforms 的工具可将客户机移动到较早的防毒墙网络版服务器版本。该工具会通知客户机其他防毒墙网络版服务器将管理它们。接收到通知的客户机将注册到该服务器。该工具还可以验证客户机移动是否成功。

将客户机移动到较早版本的防毒墙网络版服务器：

1. 在带有已升级的防毒墙网络版服务器的计算机上运行 Client Mover for Legacy Platforms (clientmover.exe)。可以从防毒墙网络版安装文件夹访问此工具，通常为：

C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Admin\Utility\ClientMover。

2. 在命令窗口中，使用以下格式键入命令：ClientMover [/P:ExportDataPath] [/S:ServerIP:port] [/N]

   例如：

   ClientMover /P:"C:\Program Files\TrendMicro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:1.2.3.4:21112 /N

   其中：

   /P：包含客户机信息的文件 (unsupCln.txt) 的路径和文件名。通常，该路径是：C:\Program Files\Trend Micro\OfficeScan\3PCCSRV\Private\unsupCln.txt。

   /S：将管理客户机的先前版本防毒墙网络版服务器的 IP 地址和端口号

   /N：通知客户机然后将其移动到先前版本的防毒墙网络版服务器的命令；与 /V 命令结合使用

3. 使用 /V 命令可验证该工具是否已移动客户机。

   例如：

   ClientMover /P:"C:\Program Files\Trend Micro\OfficeScan\PCCSRV\Private\unsupcln.txt" /S:1.2.3.4:21112 /V

   其中：

/V：验证该工具是否已成功移动客户机的命令。此命令会将已升级的防毒墙网络版服务器的 IP 地址与较早版本进行比较。如果 IP 地址相同，则该工具将无法移动客户机。

4. 检查结果：

   a. 访问结果日志，该日志位于 C:\Program Files\Trend Micro\OfficeScan\
   PCCSRV\Private\。日志文件名称的格式如下：
   unsupcln.txt.log.{date_time}

   例如：unsupcln.txt.log.20061201_162502

   b. 在同一文件夹中，验证防毒墙网络版是否已经更新且已经备份了 unsupcln.txt 文件。备份文件名是 unsupcln.txt.bak。

以下是已更新文件 unsupcln.txt 中的一条示例条目：

---

f50bb480-5abf-11db-ab38-000c292c4a67 1518338314 21112 0

其中：

客户机 GUID：f50bb480-5abf-11db-ab38-000c292c4a67

客户机的 IP 地址：1518338314（十进制）= 0x5A80010A（十六进制）

0A.01.80.5A（十六进制）= 10.1.128.90（十进制）

客户机通信端口：21112

结果：0，或任意以下值：

0 = 通知已完成

1 = 客户机通知成功

2 = 客户机通知不成功

3 = 验证成功

4 = 验证不成功

以下是 unsupcln.txt.log.{date_time} 文件中的一条示例条目：

---

f50bb480-5abf-11db-ab38-000c292c4a67 10.1.128.90:21112
无法发送通知。请检查网络或客户机状态。

其中：

客户机 GUID：f50bb480-5abf-11db-ab38-000c292c4a67

客户机的 IP 地址和通信端口：10.1.128.90:21112

结果：无法发送通知。请检查网络或客户机状态。

5. 使用 /F 命令可以不检查当前客户机状态而强制通知或验证。

还原或重新安装后恢复设置

可以保存防毒墙网络版数据库和重要配置文件的副本以还原您的防毒墙网络版程序。如果遇到问题且想要重新安装防毒墙网络版，或者想要回复到先前的配置，则可能想要执行此操作。

还原或重新安装后恢复程序设置：

1. 将防毒墙网络版服务器数据库备份到防毒墙网络版程序目录外的一个位置。

   通过防毒墙网络版 Web 控制台执行数据库备份 （**管理 > 数据库备份**）。有关指导信息，请参阅 *《管理员指南》*或防毒墙网络版服务器联机帮助。

   警告！ *不要使用任何类型的备份工具或应用程序。*

2. 从 \Program Files\Trend Micro\OfficeScan\PCCSRV 文件夹手动备份以下文件和文件夹：

   - **ofcscan.ini**：全局客户机设置
   - **ous.ini**：包括防病毒组件部署的更新源表
   - **Private 文件夹**：包括防火墙和更新源设置
   - **Web\tmOPP 文件夹**：包括爆发阻止设置
   - **Pccnt\Common\OfcPfw.dat**：包括防火墙设置
   - **Download\OfcPfw.dat**：包括防火墙部署设置
   - **Log 文件夹**：包括系统事件和连接验证日志
   - **Virus 文件夹**：包括隔离的文件
   - **HTTDB 文件夹**：包括防毒墙网络版数据库

3. 卸装防毒墙网络版 （请参阅*卸装服务器* （第 2-29 页））。

4. 执行全新安装 （请参阅*安装或升级防毒墙网络版服务器* （第 2-2 页））。

5. 主安装程序完成后，请停止目标计算机上的防毒墙网络版服务。

   a. 打开 “Windows 服务”窗口 （单击**开始 > 运行**并键入 **services.msc**）。

   b. 从列表中选择**防毒墙网络版主服务**，右键单击然后选择**停止**。

6. 将备份文件复制到目标计算机上的 \PCCSRV 文件夹。这将覆盖防毒墙网络版服务器数据库与相关文件和文件夹。

7. 重新启动防毒墙网络版服务。

将防毒墙网络版注册到控制管理中心

如果想要控制管理中心管理新安装的防毒墙网络版服务器，则安装后请将防毒墙网络版注册到控制管理中心。可以通过转至**管理 > 控制管理中心设置**来从防毒墙网络版 Web 控制台执行此操作。有关该过程，请参阅联机帮助。

安装插件管理器

可用之后，使用插件管理器可以开始使用在产品的发布版本之外开发的插件程序。插件管理器将在防毒墙网络版 Web 控制台上显示适用于防毒墙网络版服务器和防毒墙网络版客户机的插件程序。从 Web 控制台安装和管理上述程序，包括将客户机插件程序部署到客户机。

通过在 Web 控制台的主菜单上单击**插件管理器**来下载和安装插件管理器。按照“安装”窗口来完成安装。成功安装插件管理器后，检查可用的插件程序。

注意：

- 插件管理器不支持远程安装。必须在防毒墙网络版服务器计算机上打开 Web 控制台并从其安装插件管理器。

- 除可用磁盘空间外 （插件管理器至少需要 200MB），插件管理器与防毒墙网络版服务器的系统需求相同。
- 客户机插件管理器管理客户机的插件程序，在防毒墙网络版客户机安装或升级后可自动安装。它的系统需求与客户机程序相同。仅有的额外需求是 Microsoft XML Parser (MSXML) V3.0 或更高版本。

卸装服务器

防毒墙网络版可使用卸装程序安全将防毒墙网络版服务器从您的计算机移除。移除服务器前应移除所有客户机。

卸装防毒墙网络版服务器：

1. 在防毒墙网络版服务器计算机上，单击**开始 > 程序 > 趋势科技防毒墙网络版服务器 > 卸装防毒墙网络版**。

   将显示确定窗口。

2. 单击**是**。服务器卸装程序将提示您输入管理员密码。
3. 键入管理员密码，然后单击**确定**。服务器卸装程序将开始移除服务器文件。将显示确定消息。
4. 单击**确定**关闭卸装程序。

第 3 章

规划客户机安装

本章中的主题：

- *安装需求*（第 3-1 页）
- *更新代理需求*（第 3-4 页）
- *安装方法*（第 3-4 页）

安装需求

以下是在运行 Windows 2000、XP、Server 2003 和 Vista 的计算机上安装防毒墙网络版客户机的需求。

表 3-1　　客户机的系统需求

资源	需求
Windows 2000	

表 3-1　　客户机的系统需求

资源	需求
操作系统	• 带有 Service Pack 3 或 4 的 Microsoft Windows 2000 • Microsoft Cluster Server 2000
硬件	• 300MHz Intel Pentium 处理器或同等处理器 • 128MB 内存 • 200MB 可用磁盘空间 • 颜色为 256 或更高时支持分辨率为 800 x 600 的显示器
其他	如果执行 Web 安装，则需要 Microsoft Internet Explorer 5.0 或更高版本
Windows XP/2003 32 位版	
操作系统	• 使用 Service Pack 1 或 2 的 Microsoft Windows XP Professional 32 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 32 位版 • 带有或不带有 Service Pack 1 或 2 的 Microsoft Windows 2003 Web Edition, 32 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 R2 32 位版 • Microsoft Windows Storage Server 2003 32 位版 • Windows Compute Cluster Server 2003
硬件	• 300MHz Intel Pentium 处理器或同等处理器；还支持 AMD™ x64 或扩展的 64 位内存技术 (EM64T) 处理器体系结构 • 128MB 内存 • 200MB 可用磁盘空间 • 支持分辨率为 800 x 600 颜色为 256 的监视器
其他	如果执行 Web 安装，则需要 Microsoft Internet Explorer 6.0 或更高版本
Windows XP/2003 64 位版	

表 3-1　　客户机的系统需求

资源	需求
操作系统	• 使用 Service Pack 1 或 2 的 Microsoft Windows XP Professional 64 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 64 位版 • 带有或不带 SP 1 或 2 的 Microsoft Windows Server 2003 R2 64 位版 • Microsoft Windows Storage Server 2003 64 位版 • Windows Compute Cluster Server 2003
硬件	• Intel x64 处理器， AMD x64 处理器 • 128MB 内存 • 200MB 可用磁盘空间 • 支持分辨率为 800 x 600 颜色为 256 的监视器
其他	如果执行 Web 安装，则需要 Microsoft Internet Explorer 6.0 或更高版本
Windows Vista	
操作系统	• Microsoft Windows Vista Business 32 位版 • Microsoft Windows Vista Enterprise 32 位版 • Microsoft Windows Vista Ultimate 32 位版 • Microsoft Windows Vista Business 64 位版 • Microsoft Windows Vista Enterprise 64 位版 • Microsoft Windows Vista Ultimate 64 位版
硬件	• 800MHz Intel Pentium 处理器或同等处理器；还支持 AMD x64 或扩展的 64 位内存技术 (EM64T) 处理器体系结构 • 1GB 内存 • 200MB 可用磁盘空间 • 支持分辨率为 800 x 600 颜色为 256 的监视器
其他	如果执行 Web 安装，则需要 Microsoft Internet Explorer 7.0 或更高版本

注意： 禁用 Windows XP 计算机上的**简单文件共享**，那么用户可成功安装防毒墙网络版客户机程序 （请参阅 Windows 文档来获取指导信息）。

更新代理需求

表 3-2 更新代理的系统需求

资源	需求
操作系统	Windows 2000、 XP、 Server 2003 和 Vista
硬件	**处理器：**800MHz Intel Pentium 或同等处理器 **内存：** • 512MB （Windows 2000、 XP 和 Server 2003） • 1GB (Windows Vista) **可用磁盘空间：**700MB **其他：**颜色为 256 或更高时支持分辨率为 800 x 600 的显示器
更新请求容量	取决于计算机的硬件规格

安装方法

本部分提供不同客户机安装方法的摘要，以帮助您决定哪种方法最适合您的网络环境。所有安装方法都要求目标计算机上的本地管理员权限。

Web 安装页面

指导贵组织中的用户转到 Web 页面并下载客户机安装文件 （请参阅*从 Web 安装页安装* （第 4-2 页））。

登录脚本安装

在未受保护计算机登录到网络时，自动将防毒墙网络版客户机安装到这些计算机（请参阅*与“登录脚本安装”一起安装*（第 4-3 页））。

客户机打包程序

创建和发送客户机安装或更新文件至客户机用户（请参阅*与客户机打包程序一起安装*（第 4-6 页））。如果使用客户机打包程序创建 MSI 软件包，您可使用 Active Directory™ 或 Microsoft SMS 部署该软件包。

有关详细信息，请参阅以下主题：

- *使用 Active Directory 部署 MSI 软件包*（第 4-10 页）
- *使用 Microsoft SMS 部署 MSI 软件包*（第 4-11 页）

远程安装

从 Web 控制台，在运行受支持的平台的计算机上安装客户机程序（请参阅*从防毒墙网络版 Web 控制台安装*（第 4-14 页））。

从客户机磁盘镜像

创建和复制防毒墙网络版客户机的镜像，然后部署到网络中的其他计算机（请参阅*从客户机磁盘映像安装*（第 4-16 页））。

趋势科技漏洞扫描程序 (TMVS)

运行趋势科技 ™ 漏洞扫描程序，以在未受保护的计算机上安装客户机程序（*与漏洞扫描程序一起安装*（第 4-17 页））。

摘要

表 3-3　　防毒墙网络版客户机安装方法

	Web 安装页面	登录脚本安装	客户机软件包	使用 Microsoft SMS 部署的客户机软件包	使用 Active Directory 部署的客户机软件包	远程安装	客户机磁盘镜像	TMVS
适合跨 WAN 部署	无	无	无	是	是	无	无	无
适合集中式管理	无	无	无	是	是	是	无	是
需求客户机用户的干预	是	是	是	是 / 无	是 / 无	无	无	无
要求 IT 资源	无	是	是	是	是	是	是	是
适合大规模部署	无	无	无	是	是	无	无	无
带宽消耗	高	高，如果客户机同时启动	低，如果已预设	低，如果已预设	高，如果客户机同时启动	高	低	高

第 4 章

安装和升级防毒墙网络版客户机

安装 / 升级场景：

- *执行全新安装*（第 4-2 页）
- *升级防毒墙网络版客户机*（第 4-18 页）
- *从第三方防病毒应用程序迁移*（第 4-18 页）
- *从 ServerProtect 标准服务器迁移*（第 4-20 页）

建议的安装后任务：

- *验证客户机安装、升级或迁移*（第 4-23 页）
- *启动组件更新*（第 4-26 页）
- *使用 EICAR 测试脚本测试防毒墙网络版*（第 4-27 页）

其他任务：

- *卸装客户机*（第 4-28 页）

执行全新安装

请先关闭任何运行在客户端计算机上的应用程序，再安装客户机程序。否则，完成安装过程可能需要更长时间。

从 Web 安装页安装

如果已经在运行 Windows 2000 Server 或 Windows Server 2003、具有 Internet Information Server (IIS) 5.0 或更高版本或 Apache 2.0 的计算机上安装了防毒墙网络版服务器，那么客户机用户可以从服务器安装期间创建的 Web 安装页安装客户机程序。指导用户转到 Web 安装页并下载客户机安装文件。

提示： 您可使用漏洞扫描程序来确定没有遵循那些用以从 Web 安装页安装的指令的用户（请参阅*使用漏洞扫描程序以验证客户机安装*（第 4-24 页）以获取详细信息）。

需求：

- 至少 Microsoft Internet Explorer 5.0 (Windows 2000)、 6.0 (Windows XP/Server 2003) 或 7.0 (Windows Vista) 且安全级别设置为允许 ActiveX™ 控件。
- 计算机上的管理员权限

从 Web 安装页上发送以下指令给用户以安装防毒墙网络版客户机。

从 Web 安装页安装：

1. 如果安装到运行 Windows Vista 的计算机上，请执行安装前的任务。有关详细信息，请参阅第 5-3 页。如果计算机不是运行 Windows Vista，请跳过这一步。
2. 打开 Internet Explorer 窗口，然后键入以下内容之一：
   - 具有 SSL 的防毒墙网络版服务器：

     https://{OfficeScan_server_name}:{ 端口号 }/officescan
   - 不具有 SSL 的防毒墙网络版服务器：

     http://{OfficeScan_server_name}:{ 端口号 }/officescan
3. 单击**对于联网计算机**下的链接。
4. 在显示的新窗口中，单击**立即安装**开始安装防毒墙网络版客户机。客户机安装即开始。

   安装后防毒墙网络版客户机图标将显示在 Windows 系统托盘中。

与 “登录脚本安装” 一起安装

“登录脚本安装”可以在无保护的计算机登录到网络上时，将防毒墙网络版客户机自动安装到这些计算机上。“登录脚本安装”会将名为 AutoPcc.exe 的程序添加到服务器登录脚本中。

AutoPcc.exe 可执行以下功能：

- 确定无保护的计算机的操作系统，并安装正确版本的防毒墙网络版客户机

- 更新程序文件和防病毒、防间谍软件和损害清除服务组件

注意： 客户端计算机必须属于域，才能通过登录脚本使用 AutoPcc。

使用 “登录脚本安装” 将 AutoPcc.exe 添加到登录脚本中：

1. 在用于运行服务器安装的计算机上，从 Windows “开始” 菜单中依次单击**程序 > 趋势科技防毒墙网络版服务器 { 服务器名 }> 登录脚本安装**。

   将加载**登录脚本安装**实用工具。将在控制台上以树形显示网络上的所有域。

2. 找到要修改登录脚本的服务器，选中该服务器，然后单击**选择**。该服务器必须是主域控制器，并且您必须具有管理员访问权限。“登录脚本安装” 将提示您输入用户名和密码。

3. 键入用户名和密码。单击**确定**继续。

   将显示 “用户选择” 窗口。“用户” 列表将显示登录到该服务器上的用户的概要文件。“选定的用户” 列表将显示要修改其登录脚本的用户配置文件。

   - 要修改单个或多个用户配置文件的登录脚本，从 “用户” 列表中选择这些文件，然后单击**添加**。
   - 要修改所有用户的登录脚本，请单击**添加全部**。
   - 要排除先前选择的一个用户配置文件，请从 “选定的用户” 列表中单击名称，然后单击**删除**。
   - 要重置选择，请单击**移除全部**。

4. 当所有目标用户配置文件都出现在**选定的用户**列表中时，单击**应用**。

   将显示一条消息提示您已成功修改了服务器登录脚本。

5. 单击**确定**。“登录脚本安装”将返回到其初始屏幕。

   - 要修改其他服务器的登录脚本，请重复步骤 2 到 4。
   - 要关闭 “登录脚本安装”，请单击**退出**。

注意： 当不受保护的 Windows 2000/XP/Server 2003 计算机登录到被您更改过登录脚本的服务器上时， AutoPcc.exe 会自动将防毒墙网络版客户机安装到该计算机上。

但是， AutoPcc.exe 不会自动将客户机安装到 Windows Vista 计算机上。用户需要连接到服务器计算机，导航到 \\{ 服务器计算机名 }\ofcscan，右键单击 **AutoPcc.exe**，然后选择**作为管理员运行**。

对于使用 AutoPcc.exe 的远程台式机安装：

- 计算机必须在 Mstsc.exe/ 控制台模式下运行。这强制 AutoPcc.exe 安装程序在会话 0 中运行。

- 将一个驱动器映射到 ofcscan 共享，然后从此点执行 AutoPcc.exe。

Windows 2000/Server 2003 脚本

如果您已经具有现有登录脚本，登录脚本安装会追加一条执行 AutoPcc.exe 的命令。否则，防毒墙网络版将创建一个名为 ofcscan.bat 的批处理文件，包含运行 AutoPcc.exe 的命令。

登录脚本安装将以下内容追加到脚本的末尾：

\\{Server_name}\ofcscan\autopcc

其中：

- { 服务器名 } 是防毒墙网络版服务器计算机的计算机名或 IP 地址

- “ofcscan”是服务器上的防毒墙网络版目录
- “autopcc”是将安装防毒墙网络版客户机的 AutoPcc 可执行文件的链接

登录脚本位置 （通过网络登录共享目录）：

- Windows 2000 服务器：\\{Windows 2000 服务器 }\{ 系统驱动器 }\WINNT\SYSVOL\domain\scripts\ofcscan.bat
- Windows Server 2003 服务器：\\{Windows 2003 服务器 }\{ 系统驱动器 }\windir\sysvol\domain\scripts\ofcscan.bat

与客户机打包程序一起安装

客户机打包程序可以将安装和更新文件压缩到自解压缩文件中，您可使用常规介质 （如 CD-ROM）发送给用户。用户收到软件包后，只需在客户端计算机运行安装程序。

当向低带宽远程办公室中的客户机上部署客户机安装或更新文件时，客户机打包程序作用突出。使用客户机打包程序安装的防毒墙网络版客户机，将向服务器报告客户机打包程序创建已安装软件包的位置。

客户机打包程序创建的自解压缩文件

- **可执行文件：**该类常用文件扩展名为 .exe。
- **Microsoft Installer(MSI) 软件包格式：**该类文件符合 Microsoft's Windows Installer 软件包说明书。可通过一般介质，或使用 Active Directory 和 Microsoft SMS 发送 MSI 软件包。请参阅*使用 Active Directory 部署 MSI 软件包*（第 4-10 页）和*使用 Microsoft SMS 部署 MSI 软件包*（第 4-11 页）以了解详情。有关 MSI 的更多信息，请参阅 Microsoft Web 站点。

客户端计算机需求

- 最少 160MB 可用磁盘空间
- Windows Installer 2.0 （运行 MSI 软件包）

使用客户机打包程序创建软件包

1. 在防毒墙网络版服务器计算机上，浏览到 \PCCSRV\Admin\Utility\ClientPackager。
2. 双击 ClnPack.exe 运行此工具。客户机打包程序控制台将打开。
3. 选择要创建的软件包类型：
   - **安装：**如果安装防毒墙网络版客户机程序，选择此项。该操作将创建一个可执行文件。
   - **更新：**如果只更新防毒墙网络版客户机组件，选择此项。该操作也将创建一个可执行文件。
   - **MSI 软件包：**如果创建符合 Microsoft Installer 软件包格式的软件包，选择此项。
4. 如果创建可执行文件，选择要创建该软件包的操作系统。
5. 从下列安装选项中选择：
   - **静默方式：**创建在客户端计算机后台安装的软件包，客户机注意不到，也不显示安装状态窗口。
   - **更新代理：**给予客户机充当更新代理的能力 （更新代理是帮助防毒墙网络版服务器部署客户机组件的备用服务器）。如果使用客户机打包程序安装了防毒墙网络版客户机程序，并且启用了**更新代理**选项，必须使用预设更新配置工具启用和配置预设更新 （请参阅*使用预设更新配置工具* （第 4-9 页））。

提示： 如果使用客户机打包程序安装防毒墙网络版客户机程序，并且启用更新代理选项，该客户机注册的任一台防毒墙网络版服务器都不能同步或修改以下设置：更新代理的权限、客户机预设更新、从趋势科技 ActiveUpdate 服务器的更新、从其他更新源的更新。

趋势科技建议，只在没有注册到任一台防毒墙网络版服务器的客户端计算机上安装和配置更新代理，以从防毒墙网络版服务器以外的源进行更新。如果要修改上述更新代理设置，使用客户机打包程序以外的其他客户机程序安装方法。

- **强制用最新版本覆盖：**用最新版本覆盖旧版本；只适用于选择**更新**作为软件包类型时。
- **禁用预扫描 （仅用于全新安装）：**禁用防毒墙网络版安装之前的文件扫描

6. 选择软件包里包含的防毒墙网络版客户机实用程序。
   - **Outlook 邮件扫描：**扫描 Microsoft Outlook™ 邮箱安全风险
   - **Check Point SecureClient 支持：**支持 Windows 2000/XP/Server 2003 平台的 Check Point™ SecureClient™
7. 选择安装软件包里包含的组件。
8. 再选择**源文件**，确保 ofcscan.ini 文件的位置正确。要修改该路径，单击以 … 浏览 ofcscan.ini 文件。缺省情况下，该文件在防毒墙网络版服务器的 \PCCSRV 文件夹下。
9. 在**输出文件**里，单击 … 指定要创建的客户机软件包的位置和文件名 （例如， ClientSetup.exe）。

10. 单击**创建**。客户机打包程序完成创建软件包时，将提示“成功创建软件包”消息。验证是否已成功创建软件包，请检查指定的输出文件夹。

11. 部署软件包。

    - 将软件包发送给用户，请他们在计算机上通过双击 .exe 或 .msi 文件运行客户机软件包。对运行 Windows Vista 的计算机，指导用户右键单击 .exe 文件，然后选择**作为管理员运行**。

      警告！ *仅把软件包发送给其防毒墙网络版客户机向创建该软件包的服务器报告的用户。*

    - 如果创建了 .msi 文件，您可使用 Active Directory 或 Microsoft SMS。请参阅*使用 Active Directory 部署 MSI 软件包*（第 4-10 页）或*使用 Microsoft SMS 部署 MSI 软件包*（第 4-11 页）。

使用预设更新配置工具

用预设更新配置工具启用并配置，使用客户机打包程序在充当更新代理的防毒墙网络版客户机上安装的预设更新。该工具只在安装了客户机打包程序的更新代理上可用。

使用预设更新配置工具：

1. 在安装了客户机打包程序的更新代理上，打开 Windows Explorer。
2. 转到防毒墙网络版客户机文件夹。
3. 双击 SUCTool.exe 运行此工具。预设更新配置工具控制台将打开。
4. 选择**启用预设更新**。
5. 指定更新频率和时间。
6. 单击**应用**。

使用 Active Directory 部署 MSI 软件包

您可利用 Active Directory 的功能将 MSI 软件包同时部署到多台客户端计算机。有关创建 MSI 文件的指导信息，请参阅 *与客户机打包程序一起安装*（第 4-6 页）。

使用 Active Directory 部署 MSI 软件包：

1. 打开 Active Directory 控制台。
2. 右键单击您要将 MSI 软件包部署到的组织单元 (OU)，然后单击**属性**。
3. 单击**组策略**选项卡中的**新建**。
4. 在计算机配置和用户配置之间选择一个，然后打开下面的**软件设置**。

   提示： 趋势科技建议使用**计算机配置**，而不使用**用户配置**，以确保无论哪个登录到该计算机的用户都可成功安装 MSI 软件包。

5. 在软件设置下面，右键单击**软件安装**，然后选择**新建**和**软件包**。
6. 查找并选择 MSI 软件包。
7. 选择部署方法，然后单击**确定**。

   - **指定：**下次用户登录到计算机（如果您选择用户配置）或计算机重新启动（如果您选择计算机配置）时， MSI 软件包将自动部署。此方法不需要任何用户干预。
   - **发布：**要运行 MSI 软件包，通知用户转到“控制面板”，打开“添加或删除程序”窗口，然后选择在网络上添加或删除程序的选项。显示防毒墙网络版客户机 MSI 软件包时，用户可继续安装客户机。

使用 Microsoft SMS 部署 MSI 软件包

您可使用 Microsoft System Management Server (SMS) 部署 MSI 软件包。但是，您必须在服务器上安装 Microsoft BackOffice SMS。

有关创建 MSI 文件的指导信息，请参阅 *与客户机打包程序一起安装*（第 4-6 页）。

注意： 如果您使用 Microsoft SMS 2.0 和 2003，以下指导信息将适用。

SMS 服务器需要先从防毒墙网络版服务器获取 MSI 文件，然后才能将软件包部署到目标计算机。

- **本地：**SMS 服务器和防毒墙网络版服务器在同一台计算机上
- **远程：**SMS 服务器和防毒墙网络版服务器在不同计算机上

要在本地获取软件包：

1. 打开 SMS 管理员控制台。
2. 单击**树**选项卡的**软件包**。
3. 单击**操作**菜单的**新建 > 软件包 （从定义）**。将显示 “从定义创建软件包向导” 的欢迎窗口。
4. 单击**下一步**。将显示 “软件包定义” 窗口。
5. 单击**浏览**。将显示 “打开” 窗口。
6. 浏览并选择由客户机打包程序创建的 MSI 软件包文件，然后单击**打开**。“软件包定义” 窗口将显示 MSI 软件包名称。此软件包将显示 “趋势科技防毒墙网络版客户机” 和程序版本。
7. 单击**下一步**。将显示 “源文件” 窗口。

8. 单击**总是从源目录获取文件**，然后单击**下一步**。

   将显示 “源目录”窗口，显示您要创建的软件包名称和源目录。

9. 单击**站点服务器上的本地驱动器**。

10. 单击**浏览**，然后选择包含该 MSI 文件的源目录。

11. 单击**下一步**。向导将创建软件包。完成此过程后，软件包名称将出现在 SMS 管理员控制台上。

要远程获得软件包：

1. 在防毒墙网络版服务器上，使用客户机打包程序创建具有 .exe 扩展名的 “安装”软件包 （不可创建 .msi 软件包）。有关详细信息，请参阅 *与客户机打包程序一起安装* （第 4-6 页）。

2. 在您要存储源文件的计算机上，创建一个共享文件夹。

3. 打开 SMS 管理员控制台。

4. 单击**树**选项卡的**软件包**。

5. 单击**操作**菜单的**新建 > 软件包 （从定义）**。将显示 “从定义创建软件包向导”的欢迎窗口。

6. 单击**下一步**。将显示 “软件包定义”窗口。

7. 单击**浏览**。将显示 “打开”窗口。

8. 浏览 MSI 软件包文件。此文件位于您创建的共享文件夹上。

9. 单击**下一步**。将显示 “源文件”窗口。

10. 单击**总是从源目录获取文件**，然后单击**下一步**。将显示 “源目录”窗口。

11. 单击**网络路径 （UNC 名）**。

12. 单击**浏览**，然后选择包含该 MSI 文件的源目录 （您创建的共享文件夹）。

13. 单击**下一步**。向导将创建软件包。完成此过程后，软件包名称将出现在 SMS 管理员控制台上。

要将此软件包分发至目标计算机：

1. 单击**树**选项卡的**公布**。

2. 单击**操作**菜单的**所有任务 > 分发软件**。将显示 “分发软件向导” 的欢迎窗口。

3. 单击**下一步**。将显示 “软件包” 窗口。

4. 单击**分发现有软件包**，然后单击您创建的 “安装” 软件包的名称。

5. 单击**下一步**。将显示 “分发点” 窗口。

6. 选择您要复制此软件包的一个分发点，然后单击**下一步**。将显示 “公布程序” 窗口。

7. 单击**是**公布此客户机 “安装” 软件包，然后单击**下一步**。将显示 “公布目标” 窗口。

8. 单击**浏览**选择目标计算机。将显示 “浏览集合” 窗口。

9. 单击**所有 Windows NT 系统**。

10. 单击**确定**。将再次显示 “公布目标” 窗口。

11. 单击**下一步**。将显示 “公布名称” 窗口。

12. 在文本框中键入名称和您对此公布的注释，然后单击**下一步**。将显示 “公布至子集” 窗口。

13. 选择是否将此软件包公布至子集。您可选择仅将此程序公布至指定集合或子集的成员。

14. 单击**下一步**。将显示 “公布时间表” 窗口。

15. 通过键入或选择日期和时间指定何时公布客户机 “安装” 软件包。

    如果您希望 Microsoft SMS 在特定日期停止公布软件包，请单击**是。此公布应到期**，然后在**到期日期和时间**列表框中指定日期和时间。

16. 单击**下一步**。将显示 “指定程序” 窗口。

17. 单击**是，指定此程序**，然后单击**下一步**。

    Microsoft SMS 将创建此公布并显示在 SMS 管理员控制台上。

当 Microsoft SMS 分发此公布程序（即防毒墙网络版客户机程序）至目标计算机时，每台目标计算机上都将显示一个窗口。指导用户单击**是**，然后遵循向导提供的指令，把防毒墙网络版客户机安装到他们的计算机上。

与 Microsoft SMS 一起安装时的已知问题

- SMS 控制台的 “运行时间” 列将显示 “未知”。
- 如果安装不成功， SMS 程序的监控程序上安装状态可能仍然显示安装已完成。有关如何验证是否成功安装的指导信息，请参阅*使用漏洞扫描程序以验证客户机安装*（第 4-24 页）。

从防毒墙网络版 Web 控制台安装

可以把防毒墙网络版客户机远程安装到已经连接到网络中的一台或多台 Windows XP、2000、2003 Server 和 Vista 计算机上。确保您对目

标计算机具有管理员权限，以执行远程安装。远程安装程序不会在正在运行防毒墙网络版服务器的计算机上安装防毒墙网络版客户机。

从防毒墙网络版 Web 控制台安装：

1. 如果安装到运行 Windows Vista 的计算机上，请执行安装前的任务。有关详细信息，请参阅第 5-2 页。如果计算机不是运行 Windows Vista，请跳过这一步。
2. 在 Web 控制台，单击**联网计算机 > 客户机安装 > 远程**。
3. 选择目标计算机。
   - **域和计算机**列表显示网络上所有的 Windows 域。双击域名以显示域下的计算机。选择计算机，再单击**添加**。
   - 如果你记得某特定计算机的名称，在页面上方的字段里输入计算机名称，再单击**搜索**。

   防毒墙网络版会提示您输入目标计算机的用户名和密码。请确保使用管理员账户用户名和密码才能继续。
4. 输入用户名和密码，再单击**登录**。目标计算机显示在**选定的计算机**表中。
5. 重复步骤 2 和步骤 3，添加多个计算机。
6. 准备好在目标计算机上安装客户机时，单击**安装**。将显示确认框。
7. 单击**是**，确认要在目标计算机上安装客户机。程序文件复制到每台目标计算机时，将显示运行窗口。

   完成一台目标计算机防毒墙网络版的安装后，该计算机名称从**选定的计算机**列表中消失，显示在**域和计算机**列表中，带红色复选标记。

当所有目标计算机带着红色复选标记显示在**域和计算机**列表中时，远程安装已完成。

注意： 如果安装到多台计算机上，防毒墙网络版会在日志中记录不成功的安装，但不会推迟其他的安装。单击**安装**后，不必监督安装程序。以后再检查日志以查看安装结果。

从客户机磁盘映像安装

通过磁盘镜像技术，可以使用磁盘镜像软件创建某个防毒墙网络版客户机的镜像并将其复制到网络中的其他计算机。

每个客户机安装程序需要一个全局唯一标识号 (GUID)，这样服务器就可以单独识别计算机。使用名为 imgsetup.exe 的防毒墙网络版程序来为每个复制创建不同的 GUID。

注意： 支持的 Windows 平台包括 Windows 2000、XP 和 Server 2003。此安装方法不支持 Microsoft Vista 和 x64 平台。

创建防毒墙网络版客户机的磁盘镜像：

1. 将防毒墙网络版客户机安装到计算机。可以使用此客户机作为磁盘镜像源。
2. 从防毒墙网络版服务器的 \PCCSRV\Admin\Utility\ImgSetup 文件夹中，将 ImgSetup.exe 复制到此计算机。
3. 在此计算机上运行 ImgSetup.exe。将在 HKEY_LOCAL_MACHINE 下创建一个 RUN 注册表键。
4. 使用磁盘镜像软件创建防毒墙网络版客户机的磁盘镜像。

5. 重新启动复制。 ImgSetup.exe 将自动启动并创建一个新的 GUID 值。客户机将会把这个新的 GUID 报告给服务器而服务器将为该客户机创建一个新的记录。

警告！ *为避免防毒墙网络版数据库中两个计算机具有相同的名称，请务必手动更改被复制的防毒墙网络版客户机的计算机名称或域名。*

与漏洞扫描程序一起安装

使用漏洞检查程序可以检测安装的防病毒解决方案，在网络上搜索未受保护的计算机，还可以将防毒墙网络版客户机安装到这些计算机。要确定计算机是否需要保护，漏洞扫描程序将对防病毒解决方案通常使用的端口执行 ping 操作。

本部分说明如何将防毒墙网络版客户机程序与漏洞扫描程序一起安装。有关如何使用漏洞扫描程序来检测防病毒解决方案的指导信息，请参阅*管理员指南*中的 “管理工具” 部分和防毒墙网络版服务器联机帮助。

注意： 可以在运行 Windows 2000 和 Server 2003 的计算机上使用漏洞扫描程序。

使用漏洞扫描程序，您不可将防毒墙网络版客户机安装到已经安装防毒墙网络版服务器的计算机上。

要使用漏洞扫描程序安装防毒墙网络版客户机：

1. 如果安装到运行 Windows Vista 的计算机上，请执行安装前的任务。有关详细信息，请参阅第 5-2 页。如果计算机不是运行 Windows Vista，请跳过这一步。

2. 在安装防毒墙网络版服务器的计算机上，打开 OfficeScan\PCCSRV\Admin\Utility\TMVS。双击 TMVS.exe。将显示趋势科技漏洞扫描程序控制台。
3. 单击**设置**。
4. 在**防毒墙网络版服务器设置**下，键入防毒墙网络版服务器名和端口号。
5. 选择**为不受保护的计算机自动安装防毒墙网络版客户机**。
6. 单击**确定**，开始检查网络上的计算机并开始防毒墙网络版客户机的安装。

升级防毒墙网络版客户机

您可从早期版本或评估版升级到防毒墙网络版完全版。当升级防毒墙网络版服务器时，一使用任何可用的安装方法执行客户机安装，客户机就会自动升级（有关安装方法的详细信息，请参阅 *安装方法*（第 3-4 页））。

您还可使用客户机迁移程序工具。请参阅 *管理员指南*和防毒墙网络版服务器联机帮助以了解详情。

从第三方防病毒应用程序迁移

从第三方防病毒软件到防毒墙网络版的迁移过程分为两步：防毒墙网络版服务器的安装，接下来是客户机的自动迁移。

注意： 如果使用客户机迁移程序将未升级的防毒墙网络版客户机移动到已经升级到此版本的服务器，客户机将自动升级。有关客户机迁移程序的详细信息，请参阅*管理员指南*和防毒墙网络版服务器联机帮助。

自动客户机迁移

自动客户机迁移是指用防毒墙网络版客户机替换现有的客户机防病毒软件。客户机安装程序将自动卸装现有软件并替换为防毒墙网络版客户机。

注意： 防毒墙网络版只卸装客户机，而不是服务器。

要检查防毒墙网络版自动卸装的应用程序，请打开 \Trend Micro\OfficeScan\PCCSRV\Admin 里的以下文件：tmuninst.ptn 和 tmuninst_as.ptn。

客户机迁移问题：

- 如果自动客户机迁移成功，但是用户安装防毒墙网络版客户机后使用时遇到问题，请重新启动计算机。
- 如果客户机安装程序提示您，不能在用户计算机上自动卸装现有的客户机防病毒软件，请执行以下任务：
  - 手动卸装现有的客户机防病毒软件。根据软件卸装过程，卸装后计算机可能需要 （或可能不需要）重新启动。
  - 使用*执行全新安装*（第 4-2 页）中介绍的任何一种安装方法，安装防毒墙网络版客户机。
- 如果客户机安装程序继续安装防毒墙网络版客户机，但是没有卸装任何现有的客户机防病毒软件，安装在同一台计算机上的两个客户

机软件之间可能会有冲突。既然这样，卸装两个软件，然后使用*执行全新安装*（第 4-2 页）中介绍的任何一种方法安装防毒墙网络版客户机。

从 ServerProtect 标准服务器迁移

ServerProtect 标准服务器迁移工具是一个基于 Windows 的工具，可帮助您将运行 ServerProtect 标准服务器的计算机迁移到防毒墙网络版客户机。

系统需求

ServerProtect 标准服务器迁移工具要求与防毒墙网络版服务器相同的硬件和软件规格。在 Windows 2000/XP/Vista/Server 2003 计算机上运行该工具。

成功卸装 ServerProtect 标准服务器后，该工具安装防毒墙网络版客户机。但是，该工具不会保存 ServerProtect 标准服务器设置并且不会将 ServerProtect 标准服务器设置迁移防毒墙网络版客户机设置。

安装 ServerProtect 标准服务器迁移工具

在防毒墙网络版服务器计算机上，打开 \OfficeScan\PCCSRV\Admin\Utility\SPNSXfr，并将文件 SPNSXfr.exe 和 SPNSX.ini 复制到 \PCCSRV\Admin。

使用本地 / 域管理员帐户来访问客户端计算机。如果使用权限不足的帐户（例如“Guest”或“标准用户”）登录到远程计算机，将无法执行安装。

使用 ServerProtect 标准服务器迁移工具：

1. 双击 SPNSXfr.exe 文件打开该工具。将打开 ServerProtect 标准服务器迁移工具控制台。

2. 选择防毒墙网络版服务器。防毒墙网络版服务器的路径将显示在防毒墙网络版服务器路径下。如果该路径不正确，单击**浏览**，然后在防毒墙网络版安装所在的目录中选择 PCCSRV 文件夹。
要使该工具在您下次打开该工具时再次自动查找防毒墙网络版服务器，请选中**自动查找防毒墙网络版服务器**复选框 （缺省选中）。

3. 选择要在哪个运行 ServerProtect 标准服务器的计算机上执行迁移，请在**目标计算机**下单击以下选项之一：

   - **Windows 网络树：**显示网络中的域树。要通过这种方法选择计算机，请单击要从中选择客户端计算机的域。
   - **信息服务器名称：**通过信息服务器名称搜索。要通过这种方法选择计算机，请在文本框中键入网络中信息服务器的名称。要搜索多个信息服务器，请在服务器名称之间输入半角分号 “;”。
   - **特定标准服务器名称：**通过标准服务器名称搜索。要通过这种方法选择计算机，请在文本框中键入网络中标准服务器的名称。要搜索多个标准服务器，请在服务器名称之间输入半角分号 “;”。
   - **IP 范围搜索：**通过 IP 地址范围搜索。要通过这种方法搜索计算机，在 “IP 范围”下输入 B 类 IP 地址范围。

   注意： 如果网络中的 DNS 服务器在搜索客户机时没有响应，则搜索将挂起。等待搜索超时。

4. 选择将运行 Windows Server 2003 的计算机加入搜索。

5. 选择重新启动运行 Windows Server 2003 的计算机。要使迁移在 Windows 2003 计算机上成功完成，必须重新启动计算机。选中此复选框确保其自动重新启动。如果您没有选中**重新启动 Windows Server 2003 计算机**复选框，迁移后您必须手动重新启动计算机。

6. 单击**搜索**。搜索结果将显示在 “ServerProtect 标准服务器”下面。

7. 单击要执行迁移的计算机：

   - 要选择所有计算机，请单击**全部选择**。
   - 要取消选择所有计算机，请单击**取消全选**。
   - 要将列表导出为 .CSV 文件，请单击**导出为 CSV 格式**。

   如果登录到目标计算机需要用户名和密码，请执行以下操作：

   a. 选择**使用组帐户 / 密码**复选框。

   b. 单击**设置用户登录帐户**。将显示**输入管理信息**窗口。

   c. 键入用户名和密码。

   d. 单击**确定**。

   e. 单击**如果登录失败则再次询问**以便在迁移过程中无法登录时，能够再次键入用户名和密码。

8. 单击**迁移**。

注意： ServerProtect 标准服务器迁移工具不能卸装控管中心代理 （防毒墙服务器版）。有关如何卸装代理的说明，请参考 ServerProtect 和 / 或控制管理中心文档。

安装防毒墙网络版客户机时，迁移工具客户机安装程序可能会超时，结果可能显示为失败。但是，可能已成功安装客户机。从防毒墙网络版 Web 控制台验证客户端计算机上的安装是否成功。

迁移在以下情况下会失败：
- 如果远程计算机无法使用 NetBIOS 协议或端口 455， 337 到 339 被封闭
- 如果远程客户机无法使用 RPC 协议
- 如果远程注册表服务停止

安装后的任务

趋势科技建议执行以下安装后任务：

- *验证客户机安装、升级或迁移*（第 4-23 页）
- *启动组件更新*（第 4-26 页）
- *使用 EICAR 测试脚本测试防毒墙网络版*（第 4-27 页）

验证客户机安装、升级或迁移

完成安装或升级后，验证以下内容：

- 客户端计算机的**开始**菜单中趋势科技防毒墙网络版客户机的快捷方式

- “趋势科技防毒墙网络版客户机”是否在客户端计算机控制面板的**添加或删除程序**列表中
- 包括在 Windows 服务中的防毒墙网络版客户机服务：
  - OfficeScan NT Listener
  - OfficeScan NT Firewall （如果安装过程中启用了防火墙）
  - OfficeScan NT Proxy Service
  - OfficeScanNT RealTime Scan
- 安装日志：以下位置中的 OFCNT.LOG：
  - %windir% （对于除 MSI 软件包之外的所有安装方法）
  - %temp% （对于 MSI 软件包安装方法）
- 使用漏洞扫描程序的安装状态 （请参阅下一部分）

使用漏洞扫描程序以验证客户机安装

还可以通过创建预设任务来使漏洞扫描程序自动化。有关如果使漏洞扫描程序自动化的详细信息，请参阅防毒墙网络版联机帮助。

注意： 可以在运行 Windows 2000 和 Server 2003 的计算机上使用漏洞扫描程序。

要使用漏洞扫描程序验证客户机安装：

1. 在防毒墙网络版服务器计算机上，打开 \OfficeScan\PCCSRV \Admin\Utility\ TMVS。双击 TMVS.exe。将显示趋势科技漏洞扫描程序控制台。
2. 单击**设置**。

3. 在**产品查询**下面，选中**趋势科技防毒墙网络版 / 安全管理服务器**复选框，然后指定该服务器用来和客户机通信的端口。

4. 选择是使用标准检索，还是快速检索。标准检索更准确，但花费较长时间来完成。

   如果单击**标准检索**，通过选择**在可用时检索计算机描述**（如果可能），可设置漏洞扫描程序尝试检索计算机描述。

5. 要自动将结果发送给您或贵组织中的其他管理员，请选择**通过电子邮件将结果发送给系统管理员**。然后，单击**配置**来指定电子邮件设置。

   - 在**收件人**中，键入收件人的电子邮件地址。
   - 在**发件人**中，键入您的电子邮件地址。这将使收件人知道该邮件是谁发送的。
   - 在 **SMTP 服务器**中，键入 SMTP 服务器地址。例如，键入 smtp.company.com。这是必需的信息。
   - 在**主题**中，键入邮件的新主题或接受缺省主题。

6. 单击**确定**来保存您的设置。

7. 要在不受保护的计算机上显示警报，请单击**在不受保护的计算机上显示通知**。然后，单击**定制**来设置警报消息。将显示“警报消息”窗口。在文本框中键入一条新的警报消息，或接受缺省消息，然后单击**确定**。

8. 要将结果保存为逗号分割值 (CSV) 数据文件，请选择**自动将结果另存为 CSV 文件**。缺省情况下，漏洞扫描程序将 CSV 数据文件保存在 TMVS 文件夹中。如果要更改缺省的 CSV 文件夹，请单击**浏览**，在计算机或网络上选择目标文件夹，然后单击**确定**。

9. 在 **Ping 设置**下，指定漏洞扫描程序将如何向计算机发送数据包和等待响应。接受缺省设置或在**数据包大小**和**超时**字段键入新的值。

10. 单击**确定**。将显示漏洞扫描程序控制台。

11. 在 IP 地址范围内手动运行漏洞扫描，执行以下操作：

    注意： 漏洞扫描程序只支持 B 子网 IP 地址范围。

    a. 在**手动扫描**中，键入要检查已安装的防病毒解决方案的计算机的 IP 地址范围。

    b. 单击**开始**，开始检查网络上的计算机。

12. 要在从 DHCP 服务器请求 IP 地址的计算机上手动运行漏洞扫描，执行以下操作：

    a. 单击**结果**框中的 **DHCP 扫描**选项卡。将显示**开始**按钮。

    b. 单击**开始**。漏洞扫描程序开始侦听 DHCP 请求并在计算机登录到网络时对其执行漏洞检查。

漏洞扫描程序检查网络并在**结果**表中显示结果。请验证所有台式机和便携式计算机都安装了客户机。

如果漏洞扫描程序找到任何不受保护的台式机和便携式计算机，请使用首选的客户机安装方法在那些计算机上安装客户机。

启动组件更新

通知您的客户更新其组件，以确保有抵御安全风险的最新防护。

注意： 本部分向您显示如何启动手动更新。有关自动更新和更新配置的信息，请参阅防毒墙网络版服务器联机帮助。

要部署组件至客户机：

1. 打开防毒墙网络版 Web 控制台。
2. 在主菜单上单击**更新 > 联网计算机 > 手动更新**。将显示“手动部署”窗口，显示组件、版本和上次更新时间段的摘要。
3. 选择目标客户机。可以更新带有过期组件的客户机或手动选择客户机。
   - **选择带有过期组件的客户机：**可选择是否包括与服务器保持有效连接的漫游客户机，然后单击**开始更新**。
   - **手动选择客户机：**选择此选项后，单击**选择**以从客户机树中选择特定客户机。选择要更新的客户机，然后单击客户机树顶部的**启动组件更新**。

   服务器开始通知每台客户机下载更新过的组件。

使用 EICAR 测试脚本测试防毒墙网络版

趋势科技建议使用 EICAR 测试脚本测试防毒墙网络版并确认其有效。EICAR，欧洲计算机防病毒研究所开发了测试脚本作为确认防病毒软件安装和配置是否正确的安全方法。请访问 EICAR Web 站点以获取详细信息：

http://www.eicar.org

EICAR 测试脚本是一种扩展名为 .com 的无害文本文件。它不是病毒并且不包含任何含病毒碎片，但大部分防病毒软件将其作为病毒来响应。使用该文件来模拟病毒事件，确认电子邮件通知且病毒日志正常工作。

警告！ *请勿使用真实病毒来测试您的防病毒产品。*

要使用 EICAR 测试脚本测试防毒墙网络版：

1. 启用客户机实时扫描。
2. 将以下字符串复制、粘贴到记事本或任何纯文本编辑器：

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

3. 将文件另存为 EICAR.com，存放到一个临时目录。防毒墙网络版立即检测到该文件。
4. 要检测网络上其他计算机，将 EICAR.com 文件附加到电子邮件中并发送到其中一台计算机。

注意： 趋势科技还建议测试 EICAR 文件的 ZIP 压缩版本。使用压缩软件压缩测试脚本，然后执行上述步骤。

卸装客户机

有两种方法可从客户机卸装防毒墙网络版程序：

- *从 Web 控制台卸装*（第 4-29 页）
- *运行客户机卸装程序*（第 4-29 页）

注意： 如果客户机还有 Cisco Trust Agent (CTA) 安装程序，则卸装防毒墙网络版客户机程序可能（或可能不能）移除 CTA。这取决于您对客户机 Cisco 代理部署所配置的设置（请参阅*管理员指南*和防毒墙网络版联机帮助以获取详细信息）。

从 Web 控制台卸装

您可使用 Web 控制台从网络中的计算机上卸装客户机程序。请注意，卸装客户机程序还移除选中客户机上的安全风险防护。

从 Web 控制台卸装客户机：

1. 单击防毒墙网络版 Web 控制台主菜单的**联网计算机 > 客户机管理**。将显示客户机树。
2. 在客户机树中选择要卸装防毒墙网络版客户机的客户机，然后单击**任务 > 客户机卸装**。
3. 单击“客户机卸装”窗口中的**启动卸装**。服务器将发送通知给该客户机。
4. 检查通知状态并验证是否有未收到通知的客户机。
   a. 单击**选择未通知的计算机**，然后再单击**启动卸装**立即将通知重新发送给未通知的客户机。
   b. 单击**停止卸装**，提示防毒墙网络版停止通知当前被通知的客户机。已经被通知并且已经执行卸装的客户机暂不处理此命令。

运行客户机卸装程序

如果授予用户卸装客户机程序的权限，指导他们从他们的计算机运行客户机卸装程序。有关详细信息，请参阅*管理员指南*和防毒墙网络版服务器联机帮助。

运行客户机卸装程序：

1. 在 Windows **开始**菜单上单击**程序 > 趋势科技防毒墙网络版客户机 > 卸装防毒墙网络版客户机**。将显示“防毒墙网络版客户机卸装”窗口，并提示输入卸装密码。

2. 键入卸装密码，然后单击**确定**。防毒墙网络版将通知用户卸装的进度与卸装完成。

用户不需要重新启动客户端计算机来完成卸装。

第 5 章

FAQ 和故障排除

本章中的主题：

- *常见问题 (FAQ)*（第 5-1 页）
- *故障排除资源*（第 5-4 页）
- *解决安装问题*（第 5-8 页）

常见问题 (FAQ)

我有几个关于防毒墙网络版注册的问题。在哪里能找到答案呢？

请参阅以下 Web 站点解答关于注册的常见问题：

http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionID=16326

哪些防毒墙网络版版本可升级到当前版本？

此版本防毒墙网络版支持从任何以下版本的升级：7.3、 7.0、 6.5 和 5.58。

此版本不再支持哪些操作系统？

此版本的防毒墙网络版不再支持 Windows 95、98、Me、NT 和 IA64 体系结构。

从终端服务 2000 上能把防毒墙网络版客户机从 V7.3 （具有修补程序）升级到 8.0 吗？

不能。防毒墙网络版 7.3 不支持终端服务。

在运行 Windows Vista 的计算机上安装防毒墙网络版客户机之前，要执行什么操作？

如果您要从 Web 控制台 （远程安装）或使用漏洞扫描程序来安装防毒墙网络版客户机，请在 Windows Vista 计算机上执行以下步骤。

1. 启用内置管理员帐户并为该帐户设置密码。
2. 禁用 Windows 防火墙。
   a. 单击**开始 > 所有程序 > 管理工具 > Windows Firewall with Advanced Security**。
   b. 设置针对域概要文件、私有概要文件和公共概要文件的防火墙状态为 “关闭”。
3. 打开 “Widnows 服务”窗口 （单击**启动 > 运行**，键入 **services.msc**），然后启动 **Remote Registry** 服务。
4. 使用内置管理员帐户和密码安装防毒墙网络版客户机。请参阅*从防毒墙网络版 Web 控制台安装* （第 4-14 页）或*与漏洞扫描程序一起安装* （第 4-17 页）来了解如何操作。

如果用户要从 Web 安装页安装防毒墙网络版客户机，指导他们执行以下操作：

1. 使用内置管理员帐户登录到计算机。
2. 打开 Internet Explore，然后单击**工具 > Internet 选项 > 安全**。缺省情况下， **Internet** 区域被选择。
3. 单击**自定义级别 ...**
4. 在 **ActiveX 控件和插件**下面，启用 **ActiveX 控件自动提示**。
5. 安装防毒墙网络版客户机。请参阅*从 Web 安装页安装*（第 4-2 页）来了解如何操作。

注意： 安装过程中，用户需要允许安装 ActiveX 控件，才能成功安装客户机。

防毒墙网络版在利用网络地址转换的网络环境中能起作用吗？

能。必须启用 NAT 环境中的预设部署以确保客户机能接收更新组件。请参阅*管理员指南*以获取详细信息。

能手动卸装防毒墙网络版服务器和客户机吗？

能。但是，趋势科技建议使用卸装程序来卸装防毒墙网络版服务器和客户机。请参阅*卸装服务器*（第 2-29 页）和*卸装客户机*（第 4-28 页）来了解如何操作。

仅当使用卸装程序遇到问题时，才执行手动卸装。请参阅*服务器卸装*（第 5-17 页）和*解决方法：手动卸装客户机。*（第 5-14 页）来了解如何操作。

如果我不想使用防毒墙网络版防火墙，该做些什么？

在防毒墙网络版服务器安装过程中，不要选择“防病毒功能”窗口的**启用防火墙**。

如果您已经在安装过程中启用了防毒墙网络版防火墙，也可以从 Web 控制台执行以下操作以禁用防火墙：

1. 转到**管理 > 产品许可证 > 其他服务**。
2. 在 “用于联网计算机的防火墙”中，单击**禁用**。
3. 从 Web 控制台注销，然后再次登录。

故障排除资源

情况诊断工具

趋势科技“情况诊断工具”(CDT) 会在发生问题时收集来自客户产品的必要调试信息。CDT 可自动打开和关闭产品的调试状态，以及根据问题类别收集必要文件。趋势科技将使用此信息解决与产品相关的问题。

要获得此工具及相关文档，请联系您的技术支持提供商。

安装日志

使用防毒墙网络版自动生成的安装日志文件来解决安装问题。

表 5-1　　安装日志文件

日志文件	文件名	位置
服务器本地安装 / 升级日志	OFCMAS.LOG	%windir%

表 5-1　　安装日志文件

日志文件	文件名	位置
服务器远程安装 / 升级日志	OFCMAS.LOG （在启动安装程序所在的计算机上） OFCMAS.LOG （在目标计算机上）	%windir%
客户机安装日志	OFCNT.LOG	%windir% （所有安装方法， MSI 软件包除外） %temp% （MSI 软件包安装方法）

服务器调试日志

您可先启用调试日志记录，再执行以下服务器任务：

- 卸装然后再次安装服务器。
- 将防毒墙网络版 8.0 升级到新版本。
- 执行远程安装 / 升级 （在启动安装程序所在的计算机上启用调试日志记录，而不是在远程计算机上）。

警告！ *调试日志可能会影响服务器性能并消耗大量的磁盘空间。仅在需要时才启用调试日志记录，并且如果不再需要调试数据时立即禁用它。如果日志文件变得很大，则移除日志文件。*

要在防毒墙网络版服务器计算机上启用调试日志记录：

1. 将位于 \PCCSRV\Private 的 “LogServer” 文件夹复制到 C:\。
2. 创建名为 ofcdebug.ini 且具有以下内容的文件：

   [debug]

   DebugLevel=9

   DebugLog=C:\LogServer\ofcdebug.log
3. 将 ofcdebug.ini 保存到 C:\LogServer。
4. 执行相应的任务 （也就是，卸装 / 重新安装服务器、升级到新服务器版本或执行远程安装 / 升级）。
5. 检查 C:\LogServer 中的 ofcdebug.log。

客户机调试日志

您还可先启用调试日志记录，再安装防毒墙网络版客户机。

警告！ *调试日志可能会影响客户机性能并消耗大量的磁盘空间。仅在需要时才启用调试日志记录，并且如果不再需要调试数据时立即禁用它。如果日志文件变得很大，则移除日志文件。*

要在防毒墙网络版客户端计算机上启用调试日志记录：

1. 创建名为 ofcdebug.ini 且具有以下内容的文件：

   [Debug]

   Debuglog=C:\ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1

2. 将 ofcdebug.ini 发送给客户机用户，指示他们将该文件保存到 C:\。

3. 每次客户端计算机启动时都将自动运行 LogServer.exe。指示用户在计算机启动后不要关闭打开的 LogServer.exe 命令窗口，因为这会提示防毒墙网络版停止调试日志记录。如果用户关闭命令窗口，他们可以通过运行位于 \OfficeScan Client 中的 LogServer.exe 再次启动调试日志记录。

4. 对于每个客户端计算机，可以检查 C:\ 中的 ofcdebug.log。

5. 要禁用防毒墙网络版客户机的调试日志记录，请删除 ofcdebug.ini。

知识库

本部分的某些解决方案会将您引导到趋势科技知识库。请确保您连接到 Internet，以打开知识库。

解决安装问题

- *客户机安装*（第 5-8 页）
- *从第三方防病毒软件迁移*（第 5-12 页）
- *客户机卸装*（第 5-14 页）
- *服务器卸装*（第 5-17 页）
- *Apache Web 服务器*（第 5-19 页）

客户机安装

问题 1：

防毒墙网络版客户机不能安装在运行 Windows XP 的计算机上。

解决方法：

在运行 Windows XP 的计算机上禁用**简单文件共享**（请参阅 Windows 文档来获取指导信息）。

问题 2：

安装 Windows 2003 Service Pack 1 后， Web 控制台远程安装窗口中的客户机树 （**联网计算机 > 客户机安装 > 远程**）不显示域和客户端计算机。

解决方法：

选项 1：更改 Internet 信息服务 (IIS) 管理器中的匿名用户帐户。

1. 单击**开始 > 所有程序 > 管理工具 > Internet 服务管理器**，打开 IIS 控制台。
2. 单击**防毒墙网络版**虚拟目录，选择**防毒墙网络版 > 控制台 > remoteinstallcgi**，然后双击 **cgiRemoteInstall.exe**。
3. 然后单击**文件安全性**选项卡中的**编辑 > 浏览 > 高级 > 立即查找**。
4. 选择管理员 （如果有），然后单击**确定**。
5. 双击 cgiGetNTDomain.exe。重复步骤 3 和步骤 4。
6. 双击 cgiGetNTClient.exe。重复步骤 3 和步骤 4。

选项 2：使用以下任一种安装方法安装防毒墙网络版：

- 登录脚本安装。请参阅*与 “登录脚本安装” 一起安装*（第 4-3 页）。
- Web 安装。请参阅*从 Web 安装页安装*（第 4-2 页）。
- 客户机打包程序。请参阅*与客户机打包程序一起安装*（第 4-6 页）。

问题 3：

一些客户端计算机即使在线时，也不会在“远程安装”窗口中显示（**联网计算机 > 客户机安装 > 远程**）。客户端计算机和服务器计算机在同一子网中，并可互相通信 （使用 ping 进行验证）。

说明：

这些计算机在网络中不显示。

解决方法：

通过启用 “网络连接”中的 “Microsoft 网络的文件和打印机共享”来使这些计算机在网络中显示。

问题 4：

包含防毒墙网络版客户机安装链接的 Web 安装页面不显示。

说明：

这些设置在 Internet 选项中可能配置错误。

解决方法：

在目标计算机上执行以下步骤：

1. 如果用户可下载客户机安装文件，但无法安装防毒墙网络版客户机，则请验证以下内容：
   - 用户在该计算机上是否具有管理员权限。
   - 目标计算机是否满足防毒墙网络版客户机安装的最小系统需求。
   - 计算机是否运行受支持的 Windows 操作系统。
2. 打开 Internet Explore，然后单击**工具 > Internet 选项**。

3. 单击**连接**选项卡，然后选择**局域网设置**。

4. 禁用**对于本地地址不使用代理服务器**。

5. 单击**确定**保存更改。

6. 使用 Web 安装页面再次安装防毒墙网络版客户机。

问题 5：

使用“登录脚本安装”安装防毒墙网络版客户机时，出现以下错误消息：

“错误 – 无法登录。请确保选择的服务器 { 服务器名 } 是 Windows 服务器，然后输入正确的用户名和密码”。

解决方法：

安装防毒墙网络版客户机时，使用具有域管理员权限的帐户。

问题 6：

如果您在防毒墙网络版 7.3 修补程序 2 中安装了 Check Point SecureClient 支持工具，然后升级到此版本，升级后工具的使用会有问题。

解决方法：

- 使用客户机打包程序来部署 Check Point SecureClient 支持。
- 从防毒墙网络版客户机控制台安装此工具。

从第三方防病毒软件迁移

问题 1：

防毒墙网络版客户机安装程序不能自动卸装安装在客户端计算机上的第三方防病毒软件。

说明：

防毒墙网络版客户机的安装程序利用第三方软件的卸装程序自动将其从客户端计算机移除，然后替换为防毒墙网络版客户机。自动卸装由于以下原因失败：

- 第三方软件的版本号或产品密钥不一致。
- 第三方软件的卸装程序不起作用。
- 第三方软件的某些文件丢失或损坏。
- 安装程序不能清除第三方软件的注册码。
- 第三方软件没有卸装程序。

解决方法：

- 手动移除第三方软件。
- 停止对第三方软件的服务。
- 卸载对第三方软件的服务或进程。

要手动移除第三方软件：

- 如果第三方软件已注册到 “添加或删除程序”

  a. 打开 “控制面板”。

  b. 双击**添加或删除程序**。

c. 从安装的程序列表中选择第三方软件。

d. 单击**删除**。

- 如果第三方软件没有注册到 “添加或删除程序”

a. 打开 Windows 注册表。

b. 转到 HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall。

c. 查找第三方软件，然后运行 UninstallString 的值。

d. 如果第三方软件的安装程序是 MSI 格式：

- 查找产品编号
- 验证产品编号
- 运行 UninstallString

注意： 某些产品卸装码在 “Product Key” 文件夹中。

要修改对第三方软件的服务：

1. 在安全模式下重新启动计算机。
2. 将服务启动从自动修改为手动。
3. 再次重新启动系统。
4. 手动移除第三方软件。

要卸载对第三方软件的服务或进程：

警告！ *如果执行错误，此过程可能导致对计算机的不良效果。趋势科技强烈建议您先备份系统。*

1. 卸载对第三方软件的服务。
2. 打开 Windows 注册表，然后查找和删除产品密钥。
3. 查找和删除运行密钥或运行服务密钥。

验证 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 中的服务注册码已被移除。

客户机卸装

问题 1：

使用客户机卸装程序不能卸装客户机。

解决方法：手动卸装客户机。

警告！ *此过程需要您删除注册码。执行此操作前，确保如果出现问题您知道如何恢复。对注册表进行错误更改可能导致严重的系统问题。对注册表进行任何修改之前总是备份副本。有关详细信息，请参阅注册表编辑器帮助。*

要手动卸装防毒墙网络版客户机：

1. 停止以下服务：
   - OfficeScan NT Firewall （如果已启用）
   - OfficeScan NT Listener

- OfficeScan NT Proxy Service
- OfficeScanNT RealTime Scan

2. 打开注册表编辑器。单击开始菜单的**开始 > 运行**，然后键入 **regedit**。

3. 转到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services，然后删除以下键 （如果有）：

   - ntrtscan
   - tmcfw
   - tmcomm
   - TmFilter
   - tmlisten
   - TmPfw
   - TmPreFilter
   - TmProxy
   - tmtdi

4. 转到 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro，然后删除以下键 （如果有）：

   注意： 对 64 位客户机，查找 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro。

   - CFW

- NSC
- OfcWatchDog
- Pc-cillinNTCorp 或 OfficeScanCorp （根据客户机）

5. 转到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，然后删除 **OfficeScanNT Monitor** 键。
6. 从 Windows 开始菜单中删除防毒墙网络版客户机快捷方式。
7. 转到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Uninstall，然后删除 **OfficeScanNT** 键。
8. 如果启用了防毒墙网络版防火墙，打开 “控制面板”，然后选择**网络连接 > 本地连接**。单击**属性**，然后卸装趋势科技通用防火墙驱动程序。
9. 重新启动计算机。
10. 删除包含防毒墙网络版客户机程序文件的目录。

问题 2：

使用 “按用户” 卸装方法不能卸装 Microsoft SMS 和 Active Directory 的组策略对象上的防毒墙网络版客户机。

说明：

防毒墙网络版客户机需要检查卸装密码。对 Microsoft SMS 和 Active Directory 上的 “按系统” 卸装，防毒墙网络版使用账户名跳过密码检查（SYSTEM 和 SMSCliToknAcct&）。但是，对 “按用户” 卸装，如果没有设置 “允许用户卸装防毒墙网络版客户机” 权限，防毒墙网络版不能跳过密码检查。

解决方法：

- 使用 “按系统” 安装和卸装以完成部署。
- 在 Web 控制台中，启用 “允许用户卸装防毒墙网络版客户机” 权限。

服务器卸装

问题 1：

使用服务器卸装程序不能卸装服务器。

解决方法：

手动卸装服务器。

警告！ *此过程需要您删除注册码。执行此操作前，确保如果出现问题您知道如何恢复。对注册表进行错误更改可能导致严重的系统问题。对注册表进行任何修改之前总是备份副本。有关详细信息，请参阅注册表编辑器帮助。*

要手动卸装防毒墙网络版服务器：

1. 从 Windows 服务窗口中停止防毒墙网络版主服务。
2. 从开始菜单中删除防毒墙网络版程序的快捷方式。
3. 删除 \Trend Micro\OfficeScan 目录中的文件。此操作将删除 DBBackup 和 PCCSRV 文件夹。
4. 删除 IIS 虚拟目录。
   a. 打开 Internet 信息服务控制台。您可从 Windows 开始菜单打开此控制台 （**开始 > 程序 > 管理工具 > Internet 服务管理器**）。
   b. 搜索并删除 **OfficeScan** 文件夹。
5. 删除防毒墙网络版注册码。
   a. 打开注册表编辑器。单击开始菜单的**开始 > 运行**，然后键入 **regedit**。
   b. 转到 HKEY_LOCAL_MACHINE\Software\TrendMicro，然后删除 **OfficeScan** 键。
   c. 转到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion Uninstall\，然后删除 **OfficeScan Management Console** 键。
   d. 转到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\，然后删除 **ofcservice** 键。

Apache Web 服务器

策略服务器和插件管理器使用 Internet 服务器应用程序编程接口 (ISAPI) 处理某些 Web 请求。ISAPI 与 Apache Web 服务器 V2.0.56 到 V2.0.59 以及 V2.2.3 到 V2.2.4 不兼容。

您可以恢复不支持的 Apache Web 服务器版本。例如，您可以将 V2.0.59 恢复到 V2.0.54。

将 Apache Web 服务器从 V2.0.59 恢复到 V2.0.54：

1. 将防毒墙网络版服务器或策略服务器升级到此版本。
2. 备份防毒墙网络版安装文件夹中 **Apache2** 文件夹中的以下文件：
   - httpd.conf
   - httpd.conf.tmbackup
   - httpd.default.conf
3. 从“添加 / 删除程序”窗口卸装 Apache 2.0.59。
4. 安装 Apache 2.0.54。
   a. 从 \PCCSRV\Admin\Utility\Apache 启动 apache.msi。
   b. 在“服务器信息”窗口中，输入所需信息。
   c. 在“目标文件夹”窗口中，通过单击“更改”并浏览到 \PCCSRV 更改目标文件夹。
   d. 完成安装。
5. 将备份的文件复制回 **Apache2** 文件夹。
6. 重新启动 Apache 服务。

第 6 章

与趋势科技联系

本章中的主题：

- *技术支持*（第 6-1 页）
- *趋势科技知识库*（第 6-3 页）
- *TrendLabs*（第 6-3 页）
- *安全信息中心*（第 6-4 页）
- *将可疑文件发送给趋势科技*（第 6-5 页）
- *文档反馈*（第 6-5 页）

技术支持

趋势科技向所有已注册用户（必须在购买续订维护后）提供一年的技术支持、病毒码下载和程序更新。如果您需要帮助或有任何问题，请随时与我们联系。我们也欢迎您提出宝贵意见。

Trend Micro Incorporated/ 趋势科技（中国）有限公司向所有已注册用户提供全球支持。

- 请登录 http://www.trendmicro.com/cn/support 获取中国技术支持办事处的列表。
- 请登录 http://www.trendmicro.com/download/zh-cn/ 获取最新趋势科技产品文档。

在中国，您可以通过电话、传真或电子邮件与趋势科技销售代表取得联系。

趋势网络科技 （中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

免费咨询电话：800-820-8876(021-63848622)

技术支持热线：800-820-8839(021-6100-6656)

传真：86-21-6384 1899

Web 地址：www.trendmicro.com.cn

电子邮件：service@trendmicro.com.cn

加速您的支持呼叫

联系趋势科技时，为加快问题解决的速度，请确保您可以提供以下详细信息：

- Microsoft Windows 和服务包版本
- 网络类型
- 计算机品牌、型号和连接到计算机的所有其他硬件
- 计算机的内存以及可用硬盘空间

- 对于安装环境的详细描述
- 所有给出的错误消息的准确文本
- 重现问题的步骤

趋势科技知识库

趋势科技知识库，在趋势科技 Web 站点进行维护，具有对产品问题大部分最新答案。如果在产品文档中无法找到答案，还可以使用知识库来提交问题。在以下站点访问知识库：

http://www.trendmicro.com/cn/support

趋势科技不断更新知识库的内容并且每天添加新的解决方案。但是，如果无法找到答案，可以在电子邮件中描述问题然后将电子邮件直接发送给趋势科技支持工程师，他们将分析该问题并尽快回复。

TrendLabs

TrendLabs^{SM} 是趋势科技的一个全球性防病毒研究及技术支持中心。TrendLabs 在三个大洲都有办事处，有超过 250 名研究员和工程师为您和每个趋势科技的客户提供不间断的服务和技术支持。

您可以信赖以下售后服务：

- 用于所有已知已得到控制的和正在传播的计算机病毒和恶意代码的定期病毒码更新
- 紧急病毒爆发技术支持
- 电子邮件访问防病毒工程师
- 知识库是趋势科技技术支持问题的联机数据库

TrendLabs 已获得 ISO 9002 质量体系认证。

安全信息中心

可以在以下趋势科技 Web 站点获取全面的安全信息：
http://www.trendmicro.com.cn/vinfo

可用信息：

- 当前正在传播或活动的病毒和恶意传播代码列表
- 计算机病毒谣言
- 互联网威胁预警

- 每周病毒报告
- 包括了已知病毒和恶意传播代码的名称和症状的全面列表的病毒百科全书。
- 术语表

将可疑文件发送给趋势科技

如果您认为有文件受到了感染但扫描引擎没有检测到或无法清除此文件，趋势科技支持您将此可疑文件发送给我们。有关详细信息，请参考以下站点：

http://www.trendmicro.com/cn/support/subwizard/overview

还可以向趋势科技发送任何您怀疑是网络钓鱼 Web 站点的 URL，或其他人所说的“带毒站点”（互联网威胁的源意向，例如间谍软件和病毒）。

- 将电子邮件发送到：virus_doctor@trendmicro.com.cn，并指定“网络钓鱼或带毒站点”为主题。
- 使用基于 Web 的提交表格：http://www.trendmicro.com/cn/support/subwizard/overview。

文档反馈

趋势科技始终寻求改进文档质量。如果您对此文档或任何趋势科技文档存有疑问、注释或建议，请转到以下站点：

http://www.trendmicro.com/download/zh-cn/default.asp

示例部署

本部分描述了根据网络拓扑和可用网络资源部署防毒墙网络版的最佳方法。在贵组织中规划防毒墙网络版部署时，可以将本部分作为参考。

基本网络

图 1-1 描述了防毒墙网络版服务器和客户机直接连接的基本网络。多数商业网络都有此配置，其中 LAN（和 / 或 WAN）访问速度为 10Mbps、100Mbps 或 1Gbps。在此情况下，满足防毒墙网络版系统需求且有足够资源的计算机是安装防毒墙网络版服务器的首选。

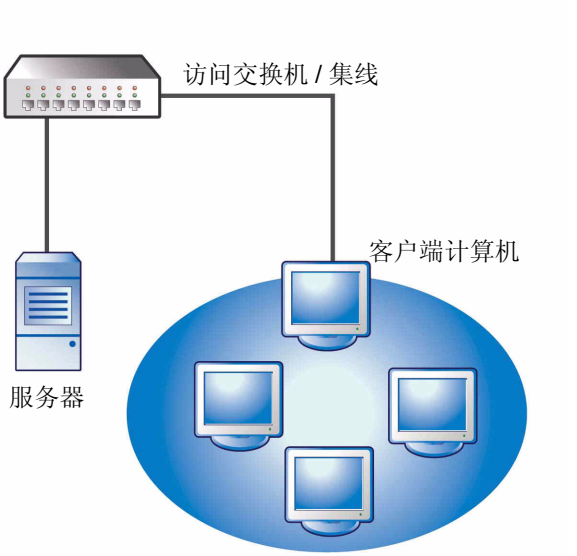


图 1-1　　基本网络拓扑

多个站点网络

对于带有多个访问点和多个不同带宽的远程站点的网络，根据办公室和网络带宽分析合并点，并确定其当前带宽使用率。这更清楚地描述了如何最佳部署防毒墙网络版。

图 1-2 描述了一个多站点网络拓扑。

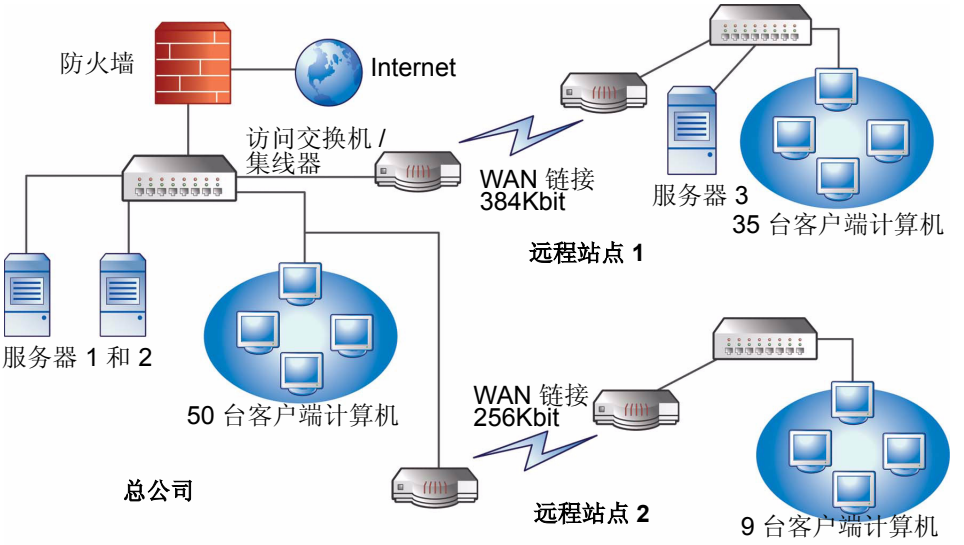


图 1-2 多个站点网络拓扑

网络信息：

- 营业时间内远程站点 1 WAN 链接的平均利用率大约为 70%。此站点上有 35 台客户端计算机。
- 营业时间内远程站点 2 WAN 链接的平均利用率大约为 40%。此站点上有 9 台客户端计算机。
- 服务器 3 只在远程站点 1 用作文件和该组的打印服务器。此计算机可能会安装防毒墙网络版服务器，但是可能不值得这些额外的管理开支。所有的服务器都运行 Windows 2000。网络使用 Active Directory，但是主要用作网络认证。
- 总公司中的所有客户端计算机、远程站点 1 和远程站点 2 都运行 Windows 2000 或 Windows XP。

任务：

1. 识别将要安装防毒墙网络版服务器的计算机。有关安装过程的信息，请参阅*安装或升级防毒墙网络版服务器*（第 2-2 页）。

2. 识别可用安装方法，并清除不满足需要的方法。请参阅*安装方法*（第 3-4 页）以获取详细信息。

   可能的安装方法：

   登录脚本安装

   如果 WAN 没有就绪，则登录脚本安装将正常进行，因为本地网络通信与此没有关系。但是，如果到每台计算机的数据传输大于 50MB，则此选项不可行。

   从 Web 控制台执行远程安装

   此方法对总公司中所有连接到 LAN 的计算机都有效。由于这些计算机上都运行 Windows 2000，因此将软件包部署到这些计算机非常容易。

   由于两个远程站点之间的链接速度较低，因此如果在营业时间部署防毒墙网络版，则此部署方法可能会影响可用带宽。可以在非营业时间，多数人不再工作时使用整个链接容量来部署防毒墙网络版。但是，如果用户关闭其计算机，则到这些计算机的防毒墙网络版部署将不会成功。

   客户机软件包部署

   客户机软件包部署似乎是远程站点部署的最佳选项。但是，在远程站点 2 没有本地服务器可适当简化此选项。深入考虑所有选项后，发现此选项可为多数计算机提供最佳范围。

总公司部署

最早在总公司实施的客户机部署方法是从防毒墙网络版 Web 控制台进行的远程安装。请参阅*从防毒墙网络版 Web 控制台安装*（第 4-14 页）来了解如何操作。

远程站点 1 部署

部署到远程站点 1 需要配置 Microsoft 分布式文件系统 (DFS)。有关 DFS 的详细信息，请参考 http://support.microsoft.com/?kbid=241452。配置 DFS 后，远程站点 2 处的服务器 3 需要启用 DFS，从而复制现有的 DFS 环境或创建一个新的 DFS 环境。

适当的部署方法是创建 Microsoft Installer 软件包 (MSI) 格式的客户机软件包，然后将该客户机软件包部署到 DFS 共享。请参阅*与客户机打包程序一起安装*（第 4-6 页）来了解如何操作。由于在下一次预设更新过程中将会把该软件包复制到服务器 3，因此客户机软件包部署有最小带宽影响。

还可以使用新的 Active Directory (AD) 策略。请参阅*使用 Active Directory 部署 MSI 软件包*（第 4-10 页）以获取详细信息。

将 WAN 上的组件更新的影响最小化：

- 指定一台客户机充当远程站点 1 的更新代理。要执行此操作，请打开 Web 控制台，然后转至**联网计算机 > 客户机管理**。在客户机树中，选择要充当更新代理的客户机，然后单击**设置 > 更新代理设置**。
- 指定更新代理后，在远程站点 1 中选择要从更新代理更新组件的客户机。要执行此操作，请转至**更新 > 联网计算机 > 更新源**。选择**定制更新源**，然后单击**添加**。在显示的窗口中，输入远程站点 1 中

的客户端计算机的 IP 地址范围，选择**更新源**按钮，然后从下拉列表中选择指定的更新代理。

远程站点 2 部署

关键问题是远程站点 2 为低带宽。但是，营业时间内 60% 的带宽都未占用。在营业时间内，带宽利用率为 40% 时，大约有 154 Kbits 的可用带宽可用。

安装防毒墙网络版客户机的最佳方法是使用与远程站点 1 处所使用的相同的 MSI 格式的客户机软件包。但是，由于没有可用的服务器，因此不能使用分布式文件系统 (DFS)。可以将运行 Windows 2000 或 XP 的计算机配置为 DFS 主机，但是这是在此文档的范围之外。您需要研究其他选项。

一个选项是使用第三方管理工具，该工具允许管理员在不访问的情况下在远程计算机上配置或创建共享。在单个计算机上创建此共享后，将该客户机软件包复制到共享所需的开支比将该客户机安装到九台计算机所需的开始少。

可以使用另一个 Active Directory 策略，但是这次也不会将 DFS 共享指定为源。

这些方法都将把安装网络通信保持为网络的本地通信，从而将 WAN 上的网络通信冲击最小化。

要将 WAN 上组件更新的影响最小化，还可以指定一台客户机充当更新代理。有关详细信息，请参阅远程站点 1 中的该过程。